

**Don't be evil – a Google
adatvédelmi politikája az
AdWords szolgáltatás
tükrében**

Jelige:

Thejack

Tartalomjegyzék

1.	Bevezetés	4
1.1.	A kutatás tárgya	4
1.2.	A dolgozat tagolása	4
1.3.	A kutatás módszere	5
1.4.	A kutatás célja	5
1.5.	A kutatás jelentősége, hasznosíthatósága	5
2.	A Google bemutatása	6
2.1.	A Google, mint a piac meghatározó szereplője	6
2.2.	Az AdWords szolgáltatás	7
2.2.1.	A reklámtevékenység fajtái	7
2.3.	Viselkedés alapú reklámozás	9
2.3.1.	A jelenség ismertetése	9
2.3.2.	Reklámozás elleni védelem	10
3.	A Szolgáltatás működése – Monitoring	10
3.1.	A monitoring fajtái	10
3.1.1.	Webtracking	10
3.1.2.	Cloud computing	11
3.1.3.	Cookie - Third Party Cookie	11
3.1.3.1.	Jogszabályi változások	12
3.1.3.2.	Az AdWords által használt cookie-k	14
3.2.	A monitoring tárgya – Combination of Data	15
3.2.1.	Fiókkal rendelkező felhasználók	18
3.2.2.	Fiókkal nem rendelkező felhasználók	18
3.2.3.	Passzív felhasználók	18
3.3.	Monitoring jogalapja – a Google Adatvédelmi Irányelve	18
4.	Európai Unió törekvések	20
4.1.	Az Adatvédelmi Irányelv	22
4.2.	Az e-Privacy Irányelv módosítása	23
4.2.1.	IP-címek	24
4.2.2.	A böngésző beállításai	25
5.	Az e-Privacy Irányelv implementálási problémája Magyarországon	25
6.	Interkontinentális együttműködés	27

7.	A lehetséges jövő – az új adatvédelmi csomag	29
7.1.	A reformtörekvések indokai	29
7.1.1.	Az adatalanyok jogainak erősítése	30
7.1.2.	A belső piaci dimenzió erősítése	31
7.1.3.	Az adatvédelem nemzetközi dimenziójának erősítése	31
7.2.	Az egyes elvekről	32
7.2.1.	A személyes adatok tárolásának megszüntetéséhez és a törléshez való jog	32
7.2.2.	Beépített és alapértelmezett adatvédelem	33
7.2.3.	Az érintett értesítése a személyes adatok megsértéséről	33
7.2.4.	Adatvédelmi hatásvizsgálat	33
7.2.5.	Az adatkezelő felelőssége	34
8.	Következtetések	34
8.1.	A lehetséges jövő	34
8.2.	Védelmi eszközök	35
8.3.	A munkacsoport ajánlása	35
8.4.	Társadalmi háttér	37
	Felhasznált Irodalom	40
	Felhasznált joganyagok	43

1. Bevezetés

1.1. A kutatás tárgya

Jelen dolgozat a Google 2012 márciusában megjelent legújabb adatvédelmi irányelvét vizsgálja az AdWords szolgáltatás sajátosságain keresztül. Az irányelv számos kérdést vet fel többek között az információs önrendelkezési jogok és a jogszerű adatkezelések területén, melyek minél előbbi válaszadást igényelnek.

A téma választásának oka a Microsoft döntése, amely alapján a 2012. október 26-án megjelent Windows 8 operációs rendszerbe integrált Internet Explorer 10-ben alapértelmezetté vált a „Do Not Track”¹ (továbbiakban: DNT) funkció. Ez a változás érzékenyen érintheti a Google-t, mert piaci tevékenységének meghatározó része épül a viselkedés alapú hirdetésekre. Az újítás a reklámtevékenységen kívül az adatgyűjtésre és adatkezelésre is hatással lehet.

1.2. A dolgozat tagolása

A munka hat fő részre osztható.

Az első rész a Google működéséről szól, nevezetesen a vállalatóriás stratégiájáról, illetve a meghatározó piaci szerep, és az AdWords kapcsolatáról. A szolgáltatás a különböző mechanizmusok segítségével, majd a viselkedésalapú reklámozás, mint fő tevékenységi kör életre gyakorolt hatásaival kerül bemutatásra.

A második fejezetben az elsőben elindított gondolatmenetet folytatva a monitoring tevékenység kerül részletes kifejtésre fajtái, tárgya, jogalapja szerint. Ezt követően az adatvédelmi irányelvek fejlődése kerül ismertetésre, melyből megismerhető a Google piaci stratégiájának fejlődése, változása.

A harmadik fejezet tárgyalja az említett stratégia megvalósításával szemben támasztott aggályokat az Európai Unió jogszabályok, irányelvek, állásfoglalások segítségével.

Ezután két kitekintés következik – először a hazai, majd a tengerentúli szabályozásra. Ebben a két részben az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) eltérő részletszabályai, valamint az Egyesült Államok és az Európai Unió közös adatvédelmi politikája kerül rövid bemutatásra.

¹ Ez jelzi a weboldalak, és az online hirdetési rendszerek felé, hogy az adott felhasználó részt kíván-e venni a hirdetési rendszerek működésének alapját adó felhasználói preferenciavizsgálatban, profilozásban vagy sem. Mind az öt piacvezető böngésző képest ezt a jelzést küldeni beállítástól függően, így a Chrome, a Firefox, az Internet Explorer, az Opera, és Safari.

FA hatodik rész egy lehetséges jövőképet vázol fel az Európai Bizottság által készülõben lévõ új adatvédelmi csomag tükrében.

1.3. A kutatás módszere

A dolgozatban nem a felhasználók jogai kerülnek a középpontba, hanem a Google, mint adatkezelõ, illetve egyes esetekben adatfeldolgozó. A kiindulópont a kezelés jogszerûségének vitatottsága, mivel a túlzott mértékû – és nem egyértelmû - monitoring tevékenységgel a Google Adatvédelmi Irányelve alapján a felhasználók adatai nincsenek teljes biztonságban. Az egyes fejezetek tárgyalása során a Google állt az adatkezelés vizsgálatának középpontjában, ez alapján kerültek felhasználásra az Európai Bizottság 29-es munkacsoportjának² állásfoglalásai, illetve az Uniós irányelvek. A cég teljes adatkezelõi tevékenységének vizsgálata meghaladná a dolgozat terjedelmi korlátait, így az AdWords szolgáltatás állt a kutatás középpontjában. Azért a reklámszolgáltatás, mert ez áll kapcsolatban a felhasználók valamennyi típusával (lásd bővebben 3.2. fejezet), illetve a személyiségprofilok kezelése itt jelenik meg a legtisztábban. Szükségszerû volt a legfrissebb joganyagok felhasználása, hiszen nem csak azok, hanem a jelenség elterjedése is a közelmúlt fejleménye.

1.4. A kutatás célja

A kutatás központi kérdése a Google Adwords magatartásalapú hirdetéseit által megvalósuló adatgyûjtés, illetve adatkezelés jogszerûsége. Kereskedelmi hasznossága nem vitatható, adatvédelmi szempontból azonban ez korántsem egyértelmû. A kutatás célja a kérdés részletes megválaszolása, illetve annak felhasználókra gyakorolt hatásainak adatvédelmi szempontból történõ elemzése.

1.5. A kutatás jelentõsége, hasznosíthatósága

Az internetezõk rendszeresen szembesülnek azzal, hogy a különbözõ oldalak, böngészõk adatokat kérnek tõlük,³ amiket a jobb felhasználói élmény érdekében jellemzõen kiadnak. Ennek következményeibe azonban nem gondolnak bele, ha mégis, nem tesznek ellene semmit, holott a DNT funkció mindenki számára alkalmazható védelmi eszköz.⁴ A dolgozat

² http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (2012.10.03.)

³ A Google AdWords tevékenységéhez hasonlóan gyakran ez is elmarad, és különbözõ technikai megoldások segítségével észrevétlenül gyûjtik a felhasználó adatait.

⁴ <http://www.hwsz.hu/hirek/48860> (2012.09.30.)

célja a Google, mint adatkezelő tevékenységének hiányosságaira és jogszerűtlenségeire történő figyelemfelhívás.

2. A Google bemutatása

A internet világában egy név az összes többi felett áll: Google. Az 1998-ban alapított cég nagy befolyással bír a mindennapos internethasználatra, a fogyasztók általános köre találkozik vele nap, mint nap.⁵ Tradicionálisan a kereső szolgáltatása tette világhírűvé, és normaalkotóvá a kereső technológia iparágában. A cég székhelye Kalifornia államban, Mountain Viewban van, de ez nem jelenti azt, hogy az európai székhelyek nem esnek az uniós adatvédelmi szabályozás hatálya alá. Az Európai Unió 23 hivatalos nyelvéből 22-n elérhető a szolgáltatás.⁶ Az európai központ Írországbán, Dublinban,⁷ két fő szerverközpontja pedig Belgiumban, és Finnországban van.⁸

Az elmúlt években a Larry Page és Sergey Brin által alapított óriás több alkalommal is bíróság elé került, de az esetek döntő többségében sikerrel védte meg álláspontját, és bizonyította, hogy továbbra is hű szlogenjéhez, a „don't be evil” mottóhoz.⁹ Legtöbbször a reklámszolgáltatása váltott ki összetett és bonyolult jogvitákat. Védjegyoltalmi ügyei miatt¹⁰ egy rendkívül széleskörű bírói gyakorlat és jogértelmezés alakult ki, amely ennek ellenére tartalmaz kifogásolható döntéseket.¹¹ A jogviták, valamint a gyakorlati alkalmazás során szembe kerülnek egymással a kereskedelmi, védjegyoltalommal bíró társaságok érdekei, valamint a felhasználók gyors és egyszerű információhoz jutáshoz való igényei.

2.1. A Google, mint a piac meghatározó szereplője

Az AdWords térhódítása forradalmasította a reklámpiacot az elmúlt években. Korábban csak felugró ablakokban, vagy oldalsávokban találkozott az internetező - többnyire zavaró - hirdetésekkel. A Google ezen változtatni akart, és egy sokkal hatékonyabb rendszert akart kidolgozni, amely megfelelt a piac által támasztott követelményeknek.¹² A keresésen alapuló reklámszolgáltatása 2007-ben a rádióon keresztül megvalósuló reklámok, 2011-ben pedig a

⁵ <http://www.google.hu/about/company/> (2012.10.15.)

⁶ kivéve a máltai

⁷ <http://www.google.com/about/jobs/locations/dublin/> (2012.10.12.)

⁸ Google Privacy Policy Legal Analysis (2012.09.18.)

⁹ <http://investor.google.com/corporate/code-of-conduct.html> (2012.10.12.)

¹⁰ Például az Egyesült Államokbeli Rosetta Stone v. Google ügy.

¹¹ Lendvai Zsófia: A Google AdWords szolgáltatása az Európai Bíróság előtt - (<http://www.sztnh.gov.hu/kiadv/ipsz/201008-pdf/02.pdf> 2012.09.25)

¹² David A. Vise & Mark Malseed, Inside the hottest business, media and technology success of our time: The Google story p117-118. 2005

televíziós reklámok bevételeit szárnyalta túl.¹³ A perszonalizált reklámok gazdaságélénkítő hatással bírnak, hiszen sokkal nagyobb a valószínűsége annak, hogy a felhasználó rákattint arra a hirdetésre, amely érdeklődési körével megegyezik. Erre helyezve a hangsúlyt az AdWords segítségével tökéletes személyiségprofilok hozhatók létre, amelyekben pontosan meghatározható az érdeklődési kör, ehhez pedig egy algoritmus segítségével egyszerűen hozzárendelhető az azonos témájú reklám.

2.2. Az Adwords szolgáltatás

A Google bevételeinek jelentős hányadát az AdWords szolgáltatásból szerzi. Az AdWords egy online aukciós rendszer szerint működik, ahol harmadik személyek (reklámozók) lefoglalhatnak különböző szavakat, amelyek felhasználó általi begépelését követően a reklámozó hirdetése jelennek meg az oldalsávon elkülönülve.¹⁴ A bevétel a reklámok differenciálásából adódik, a fizetett hirdetések prioritást élveznek az ingyenesekkel szemben. Maguk a szavak lehetnek általános kifejezések, vagy védjegyoltalom alatt álló márkanevek is.¹⁵ A hirdetések témák szerint is kategorizálva vannak, kiszűrve ezzel azokat a területeket, melyek a rendszeresen frissülő irányelv céljaival ütköznek. Ilyen területek például az abortusz, a fegyverkereskedelem, vagy a dohányreklámok.¹⁶ Az újdonságokról és változásokról a Google hivatalos blogján¹⁷ értesülhetnek a hirdetők. A szolgáltatást más kereső szolgáltatókra is kiterjesztették, ezzel is hatékonyabbá téve a személyiség profilok kialakítását, közvetetten pedig a szolgáltatás sikerét.

2.2.1. A reklámtevékenység fajtái

Az online reklámozásnak alapvetően két fajtája különböztethető meg: opt-in, illetve opt-out rendszerek. Opt-in rendszerben a felhasználónak csak akkor küldhető reklámlevél (úgy, hogy az ne számítson spamnek¹⁸), ha az e-mail cím tulajdonosa előzőleg engedélyt adott ilyen reklám célú levelek küldésére (például a levelezőrendszer regisztrációja során, vagy valamely weboldalon).

¹³ University of Arkansas Law Review: Technology law – Great Google-y Moogley: The effect and enforcement of clock fraud and online advertising

¹⁴ 68 Wash. & Lee Law Review: Lost in Translation: Repairing Rosetta Stone v. Google's Indecipherable Functionality Holding

¹⁵ <http://support.google.com/adwords/bin/answer.py?hl=hu&answer=1704410&topic=1713894&path=1710534&ctx=leftnav> (2012.10.15.)

¹⁶ <http://googleblog.blogspot.hu/2012/03/making-our-ads-better-for-everyone.html>

¹⁷ <http://adwords-hu.blogspot.hu/> (2012.10.12.)

¹⁸ A spam a fogadó által nem kért, elektronikusan, például e-mailek keresztül tömegesen küldött hirdetés.

Magyarországon természetes személynek kizárólag ilyen opt-in módon küldhető üzleti reklámlevél az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (továbbiakban ekertv.) 3. § (1) bekezdése alapján.¹⁹

Az opt-out rendszer az opt-in ellentéte, amely szerint tárgytól, és gyakoriságtól függetlenül bárkinek küldhető kéretlenül is üzleti reklámlevél, amennyiben a felhasználó számára lehetőséget adnak a leiratkozásra.

Hazánkban a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (továbbiakban reklámtv.) alapján nem természetes személy esetén (tehát például egyértelműen céges e-mail címre küldött reklámüzenetnél) opt-out rendszer működik, így a címre csak akkor nem lehet levelet küldeni, ha azt a hirdetőnél előzőleg megtiltották. Természetes személy e-mail címénél az opt-in rendszer előírásai alkalmazandók.

A Google reklámtevékenysége összetett folyamat - különböző eszközöket használ eltérő célokra.²⁰ Az Európai Bizottság 29-es munkacsoportja 2012. február 2-án levelet²¹ küldött A Google Inc. elnök-vezérigazgatójának, Larry Pagenek, amelyben értesítette őt az új Adatvédelmi Irányelvvel kapcsolatos aggodalmáról, ezért felkérte a francia adatvédelmi hatóságot²², hogy segítsen a probléma feltárásában, és a lehetséges megoldások megtalálásában²³. A Google három pontban kifogásolta a vizsgálatot – megkérdőjelezte a CNIL bevonásának indokát, az vizsgálat során alkalmazandó jogot, illetve az eljárás menetét, és általános célját. A munkacsoport választ adott a kétségekre, amelyben hangsúlyozta, hogy a tagállamok adatvédelmi biztosai beleegyeztek, hogy a CNIL segítségével folyjon a vizsgálat, a jogszabályi háttér nem tagállami jog, hanem az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács által elfogadott 95/46/EK Adatvédelmi Irányelv, valamint hogy a vizsgálat célja annak igazolása, hogy a Google az európai adatvédelmi keretrendszer szerint jár el.

¹⁹ Információs társadalommal összefüggő szolgáltatás nyújtásának megkezdéséhez, illetve folytatásához előzetes engedély vagy bármely ezzel azonos joghatású hatósági határozat nem szükséges.

²⁰ <http://www.google.com/intl/en/privacy/ads/> (2012.10.18.)

²¹ A 29-es Munkacsoport 2012. február 2-i levele Larry Page-nek, a Google elnök-vezérigazgatójának http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf (2012.10.12.)

²² CNIL - Commission nationale de l'informatique et des libertés

²³ <http://www.out-law.com/en/articles/2012/october/future-of-eu-regulation-of-data-protection-previewed-in-google-privacy-policy-investigation-says-expert/> (2012.10.22.)

Ezt követően 2012. március 16-án egy kérdőívet küldött a Google-nek, melyben 69 kérdés szerepelt. A válasz két hét késéssel érkezett, és nem tartalmazott az összes kérdésre pontos választ. A hiányosságok miatt újabb kérdőívet küldött a Munkacsoport májusban. A júniusi válaszlévélben közölt információk sem voltak kellően világosak, ezért átmenetileg tisztázatlan marad a Google opt-out rendszert alkalmazó eljárásának néhány aspektusa.²⁴ Az AdWords szolgáltatás is opt-out jellegű, de kiegészül a DoubleClick cookie működésével, vagyis a megjelenő hirdetések eleve személyre szabottak.

A technikai/gazdasági kitekintés szükséges volt ahhoz, hogy átfogó képet kapjon az olvasó a szolgáltatás működéséről, felépítéséről, hiszen ezek elengedhetetlen ismeretek a probléma szakszerű feltárásához, értékeléséhez. A kiegészítő információk ismertetésének szükségessége Buddha tanításával támasztható alá: „Ahhoz, hogy megértsünk valamit, két fontos tényező szükséges. Az egyik a megelőző ismeretek, amikbe beépítjük az új ismeretet, s így értelmet adunk neki... Ha semmilyen ismerettel nem rendelkezünk, akkor nem tudnánk hova tenni az új ismeretet, nem lenne jelentése, sem jelentősége.”²⁵

A rendszer működése és sikeressége megkérdőjelezhetetlen kényelmet és előnyt biztosít a felhasználó számára, azonban ez csak látszólag ingyenes. A valóságban az internetező a privátszférájával, a magánéletével, szokásainak titkosságával fizet. A Google katalogizálja a személyes információkat, a kereséseket, a látogatott honlapokat.²⁶ Az ebből nyert adatok a viselkedés alapú reklámozás által történő felhasználás során válnak kiemelkedő jelentőségűvé.

2.3. Viselkedés alapú reklámozás

2.3.1. A jelenség ismertetése

Ez a jelenség a felhasználók internetezési szokásainak vizsgálatán alapszik, amelynek során a meglátogatott oldalak, gyakran használt kulcsszavak, online létrehozott tartalmak kerülnek tanulmányozásra annak érdekében, hogy a kiértékelés eredményeként létrejöjjön egy egyedi profil, amelyhez könnyedén hozzá lehet rendelni a hozzá illő reklámokat.²⁷

²⁴ Google Privacy Policy Legal Analysis (2012.09.18.)

²⁵ http://dharma.blog.hu/2010/02/18/ertett_ertelem (2012.10.20.)

²⁶ 39 Seton Hall Law Review: Regulating AdWords: Consumer Protection in a Market Where the Commodity is Speech

²⁷ A 29-es számú adatvédelmi munkacsoport 2/2010. számú véleménye a viselkedésalapú online reklámról (2010.06.22.)

Szakosodott cégek figyelik, mit keres, mire kattint, miről mond véleményt a felhasználó online, és ehhez társítják azokat a viselkedési jellegű hirdetéseket, amelyekre a leginkább fogékony lehet a felhasználó. Az elmúlt időszakban három nagy horderejű, több százmillió dollár összértékű üzletkötés - és az ezáltal támadt szakmai vita - is jelezte, hogy mekkora értéket tulajdonítanak a hirdető (és szoftverbeszállító) az ilyen szofisztikált információknak.²⁸

2.3.2. Reklámozás elleni védelem

Nem egyértelműen elfogadott módszer a felhasználók magatartásainak rögzítése és értékelése, ezért született meg a Do Not Track funkció, amely megadja a lehetőséget a felhasználónak a viselkedésalapú hirdetési rendszerből való teljes kilépéshez. A funkció létjogosultságát Gary Kovács, a Mozilla vezérigazgatója is indokolta: „*Nem a reklámok a rosszak, hanem amit tehetnek a követésből származó információval. A felhasználónak meg kell adni az ellenőrzés lehetőségét.*”²⁹ A funkciót elég egyszer bekapcsolni, használat közben minden oldalnak elküldi az opt-out üzenetet. A cookie alapú megoldásoknál azonban az opt-outot minden hirdetési hálózaton külön kell bekapcsolni, ráadásul ezt a műveletet a cookie-k törlését követően újra és újra el kell végezni. A Do Not Track egyértelmű hátránya, hogy passzív megoldás, vagyis a kiküldött üzenetnek a szerveroldalon kell reakciót kiváltania. A Google-nek nem érdeke megfosztania magát fő jövedelemforrásától.

3. A szolgáltatás működése – Monitoring

Ahol a viselkedés alapú reklámozással a reklámszolgáltatónak pontos adatai vannak arról, hogy a felhasználó milyen típusú honlapokat látogat, milyen szokásokkal rendelkezik, ott a reklámozónak jelentős mértékben megnő az esélye arra, hogy hirdetése elérje a célközönséget, és effektív legyen. A célhoz szükséges monitoring tevékenység tovább differenciálható fajtája, tárgya, jogalapja szerint.

3.1. A monitoring fajtái

A monitoring megvalósulása alapvetően három tevékenységre különíthető el: webtracking, cloud computing, illetve cookie-k. Az AdWords szolgáltatás cookie-k segítségével gyűjt

²⁸http://hirek.prim.hu/cikk/2012/08/22/szereted-ha_mindent_tudnak_rolad-utelagazas_elott_az_online_reklam (2012.10.10.)

²⁹ <http://www.hsw.hu/hirek/47215/do-not-track-adverticum-google-facebook-mozilla-firefox-web-reklam.html> (2012.10.12.)

információkat, de rendkívül szoros a kapcsolat a más módszerek, és az azokon keresztül gyűjtött adatok kezelése között.

3.1.1. *Webtracking*

Webtracking során a felhasználó adatait gyűjtik össze akár online, akár offline forrásból a hozzá való eljutás céljából.³⁰ A kommunikációs eszközök fejlődésével az adatok mennyisége is megnőtt, egyszerűbbé téve ezzel az azonosíthatóságot névtelen adatok esetén is. Az adatgyűjtés módszere nem világos a felhasználók számára, ezért befolyásolni, vagy megakadályozni sem képesek, így sokkal könnyebben ki vannak téve annak, hogy a róluk gyűjtött információkat akaratuk ellenére összegyűjtsék, közlégyék.³¹

3.1.2. *Cloud Computing*

A felhő alapú szolgáltatások az internet központú, online tárolt adatokra alapulnak, ezért jelentős gazdasági előnyt jelenthet az internet segítségével megosztott adatok gyors, egyszerű kezelése. A gazdasági hatásai mellett biztonsági előnyei is lehetnek: kis- és középvállalkozások juthatnak hozzá olyan technológiákhoz, amelyekre egyébként mérsékelt anyagi kereteik miatt nem lennének képesek.³² A „felhőben” tárolt adatok kezelését végző programok közvetlen a felhasználó irányítása alatt állnak, így azok az adott célra alkalmazhatók.³³

3.1.3. *Cookie – Third Party Cookie*

A Cookie egy információcsomag, amely közvetít a böngésző és a szerver között. Az általános ismertetőt követően az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK Irányelv³⁴ 5. cikkének 3. pontja szerint célra vezetőbb értékelni a Google által alkalmazott cookiek működését.

A cookie-nak több fajtája van, az AdWords esetében a harmadik személy által használt cookiek relevánsak. A 29-es munkacsoport sütik alkalmazásával kapcsolatos hozzájárulás alóli kivételekről szóló 4/2012-es állásfoglalása alapján az ilyen elnevezésű cookie-k félrevezetőek lehetnek, mert a személyes adatok feldolgozása vonatkozásában az Adatvédelmi Irányelv 2. cikkének f) pontja szerint „*harmadik személy az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely nem azonos az érintettel, az adatkezelővel,*

³⁰ Például: viselkedés alapú reklámozással.

³¹ Web tracking Privacy and data protection issues and recommendations

³² Working Paper on Cloud Computing - Privacy and data protection issues

³³ Például: naptár kezelése, telefonkönyv, jelentkezések.

³⁴ Elektronikus hírközlési adatvédelmi irányelv

a feldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy a feldolgozó közvetlen felügyelete alatt felhatalmazást kaptak az adatok feldolgozására.”³⁵

Ez alapján a cookie egy adatkezelőre utalna, aki különbözik a felhasználó által meglátogatott honlap üzemeltetőjétől. A felhasználók szempontjából azonban harmadik személy a kereső sávban megjelenő domain név. Ez alapján a harmadik személy által használt cookie-kat azon honlap üzemeltetője alkalmazza, amely olyan domain névhez tartozik, amely a felhasználó által meglátogatott honlaptól különbözik, függetlenül attól, hogy az entitás egy különböző adatkezelő, vagy sem.

3.1.3.1. Jogszábeli változások

A 2009/136/EK irányelv³⁶ által módosított Elektronikus hírközlési adatvédelmi irányelv (továbbiakban elektronikus hírközlési irányelv) 5. cikk (3) bekezdése³⁷ értelmében az előfizető, illetve felhasználó eszközében történő adattárolás, illetve az ott tárolt adatokhoz való hozzáférés (mint amilyen a cookie-t kezelő technológia) csak akkor lesz megengedett, ha a felhasználó teljes körű tájékoztatás alapján ehhez egyértelmű, előzetes hozzájárulását adta. Az elektronikus hírközlési irányelv értelmében ez a rendelkezés nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy amelyre az előfizető vagy felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.³⁸

A 29-es munkacsoport a 4/2012-es állásfoglalásában a fenti követelmények értelmezésével kapcsolatosan kifejti, hogy annak egyértelművé tétele érdekében mely cookie-k esetében nincsen szükség a felhasználótól előzetes hozzájárulás beszerzésére. A munkacsoport szerint ez két cookie típust érint, így az olyan sütik alkalmazását, melyek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás; illetve olyan sütiket,

³⁵ 95/46/EK Irányelv az egyének védelméről és az ilyen adatok szabad áramlásáról

³⁶ A 2002/22/EK Irányelv, 2002/58/EK Irányelv és a 2006/2004/EK rendelet módosításáról

³⁷ „A tagállamok gondoskodnak arról, hogy egy előfizető, vagy felhasználó végberendezésében történő adattárolás, illetve az ott tárolt adatokhoz való hozzáférés csak azzal a feltétellel legyen megengedett, ha az érintett előfizető vagy felhasználó a 95/46/EK Irányelvvel összhangban történő –többek között az adatkezelés céljairól szóló – egyértelmű és teljes körű tájékoztatás alapján ehhez előzetes hozzájárulását adta. Ez a rendelkezés nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás, vagy amelyre az előfizető vagy felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.”

³⁸ <http://www.dataprivacy.hu/archives/1086#more-1086> (2012.10.22.)

amelyre az előfizető vagy felhasználó által kifejezetten kért, az információs társadalommal összefüggő szolgáltatás nyújtásához a szolgáltatónak feltétlenül szüksége van.³⁹

Az első számú süti típus vonatkozásában a munkacsoport rögzíti, hogy az ott rögzített követelményeket szűken kell értelmezni és csak olyan sütikre vonatkozik a felmentés, amelyek a közlés-továbbításhoz nélkülözhetetlenek. Ennél fogva a közléstovábbítást csupán „elősegítő” sütikre ez a felmentés nem vonatkozik.

A második számú süti típus olyan adattárolásra vonatkozik, melyet az előfizető/felhasználó kifejezett magatartásával igényelt, és amely nélkül a szolgáltatás sem működne. Ezzel összefüggésben a módosító irányelv (66) preambulum bekezdése⁴⁰ mondja ki, hogy a kivételszabályt arra az esetre kell korlátozni, amikor adott, az előfizető vagy felhasználó által kifejezetten kért szolgáltatás jogszerű igénybevételéhez feltétlenül szükséges a technikai tárolás vagy hozzáférés. A munkacsoport szerint egy specifikus működési módot, illetve funkcionalitást kell érteni a „szolgáltatás nyújtása” kifejezés alatt, és értelemszerűen nem a szolgáltatások összességét. A munkacsoport osztályozta a cookie-kat, és véleményük szerint a harmadik személy által használt cookie-k feltehetően nem teljesítik a kivételszabályt.

Ebből kifolyólag amennyiben a honlap üzemeltető számára kétséges a kivételszabály alkalmazása, úgy a jogbiztonság érdekében javasolt annak megvizsgálása, hogy a felhasználó hozzájárulásának beszerzésére van-e lehetőség. Ez jelentős többletmunkával járna, ezért a reklámszolgáltatónak nem kellene minden egyes alkalommal beszerezni az érintett hozzájárulását, azonban az eredeti hozzájárulást időben korlátoznia szükséges, lehetőséget kell biztosítani az időponttól független, egyszerű visszavonásra, valamint szükséges egy ikon, szimbólum létrehozása, mely minden olyan honlapon jól láthatóan elhelyezésre kerül, ahol cookie-k telepítése, és így a felhasználók nyomon követése történik. Ez az ikon nemcsak

³⁹ A 29-es Munkacsoport süti alkalmazásával kapcsolatos hozzájárulás alóli kivételekről szóló 4/2012-es állásfoglalása

⁴⁰ Számos okból, ami lehet jogszerű (pl. bizonyos típusú cookie-k), de akár nemkívánatos betolakodás (pl. kémprogram vagy vírusok) céljából is előfordulhat, hogy harmadik felek információt kívánnak tárolni egy felhasználó berendezésén, illetve megpróbálnak hozzáférni az azon tárolt információhoz. Éppen ezért kiemelkedően fontos, hogy a felhasználók világos és átfogó információkkal rendelkezzenek, mielőtt olyan tevékenységekbe kezdenek, amelyek eredménye ilyen tárolás vagy hozzáférés-szerzés lehet. A tájékoztatást és az elálláshoz való jogot a lehető legfelhasználóbarátabb módon kell biztosítani. Az e kötelezettség alóli kivételt arra az esetre kell korlátozni, amikor adott, az előfizető vagy felhasználó által kifejezetten kért szolgáltatás jogszerű igénybevételéhez feltétlenül szükséges a technikai tárolás vagy hozzáférés. A 95/46/EK Irányelv vonatkozó rendelkezéseivel összhangban, amennyiben ez technikailag lehetséges, a felhasználó a böngésző vagy egyéb alkalmazás megfelelő beállításainak használatával is kifejezheti az adatkezeléshez való hozzájárulási szándékát. E követelmények betartatását a megfelelő nemzeti hatóságoknak történő megerősített hatáskörök megadásával kell hatékonyabbá tenni.

a cookie-k telepítésére és a nyomon követésre figyelmeztetne, hanem visszajelzést is adna az érintettnek beleegyezése érvényességéről.

3.1.3.2. Az AdWords által használt cookie-k

A Google AdWords szolgáltatásában két fajta cookie-t alkalmaz, melyek megfelelnek a harmadik személy által alkalmazott cookie-k követelményeinek. Ezek a PREF cookie, és a DoubleClick cookie. Előbbi elsősorban a személyiségprofilok kialakításában játszik kiemelkedő szerepet, miután válogatás nélkül gyűjt minden információt. Ez a cookie áll a Google adatgyűjtésének középpontjában. A cookie időtartama két év, amely automatikusan frissül, miután a felhasználó meglátogatja a google.com-ot. A Google megerősítette, hogy a cookie nem módosul, amikor a felhasználó ki- vagy belép a fiókjából - ez azt jelenti, hogy minden keresés dokumentálva van. A cég állítása szerint „*a nem azonosított felhasználóktól gyűjtött adatok külön vannak kezelve a fiókkal rendelkezőkétől*”.

Az 1995-ben alapított DoubleClick cég reklámok fejlesztésében és ellátásában nyújtott szolgáltatást olyan világcégeknek, mint a Coca-Cola, Motorola, vagy a Nike. 2008-ban több mint 3 milliárd dollárért a Google tulajdonába került. Jelentőségét jelzi, hogy sok más céggel ellentétben túlélte a dotcom buborékot.⁴¹ Ma reklámok feltöltése és a teljesítményük kiértékelése a fő profilja. Korábban támadások érték, hogy félrevezette a felhasználóit egy opt-out opcióval, amely valóban nem volt működőképes. A San Francisco IT konzultációs csoport szerint habár az opt-out hatással van a cookiekra, a DoubleClick nem engedi a felhasználói számára az opt-out opciót az IP-cím alapú követés esetében.

A Google állítása szerint „*a DoubleClick cookie nem fog összevonni adatokat azonosítható felhasználók adataival, kivéve, ha az opt-in opciót használják*”. E mellett kijelentették, hogy a szenzitív információkat nem fogják gyűjteni, így például a faji, nemi, vallási, szexuális beállítottságot tartalmazó adatokat. Ezen felül biztosítanak egy hirdetési szolgáltatást, amelyben a felhasználó beállíthatja az érdeklődési köreit, amelyek alapján a reklámok

⁴¹ Az 1995-2000 közötti időszakban a nemzetközi tőzsdéket az internet alapú üzleti modellel működő társaságok papírai hajtották. A hirtelen hanyatlás közvetlen kiváltó oka vélhetően a 2000. március 10-i hétvégét követő tőzsdenyitáskor beérkező CISCO, Dell és IBM részvényeire szóló többmilliárdos részvényeladási megbízás volt, ami pánikreakciót váltott ki és az internetpiacot örvénybe küldte. A krach 2,5 év alatt 5 ezer milliárd dollár vagyonszerzéshez vezetett. - <http://www.mb-partners.eu/cegerteklevel/258> (2012.10.19.)

megjelennek a képernyőjén. Ez regisztrált és nem regisztrált felhasználók számára egyaránt elérhető.⁴²

3.2. *A monitoring tárgya – Combination of Data*

A különböző szolgáltatásokon keresztül létrejövő felhasználók adatait tartalmazó adatsomagok az adatvédelem szempontjából újfajta feladatokat támasztanak az olyan releváns interneten jelenlévő óriások elé, mint a Google. Ugyan azzal érvel, hogy nem kötelező a szolgáltatásait igénybe venni, de a számok tükrében ez gyakorlatilag kivitelezhetetlen - az európai okostelefonok több mint 50%-án Android operációs rendszer fut;⁴³ a korábbi iOS verziók a Google Maps-et használják; az európai keresőpiac 90%-át a Google uralja,⁴⁴ és a három legnépszerűbb böngészőben⁴⁵ alapértelmezett kereső, amely a piac 60%-át lefedi. A Google népszerűségét a kiváló minőség biztosítja, ehhez azonban arra is szükség van, hogy a felhasználók ne foglalkozzanak a szükségesnél jobban adataik kezelésének indokoltságával, jogszerűségével.

A különböző szolgáltatások által létrejövő adatsomagok megnövelik az adatvédelem sikertelenségének kockázatát, mint például egy biztonsági rés elleni támadás. Adott szolgáltatás elleni támadás jogosulatlan belépést eredményezhet olyan adatokhoz, amelyek több, vagy az összes szolgáltatás adatgyűjtése során jöttek létre. Volt is hasonlóra példa a Google esetében, amikor a Gmail levelező szolgáltatását támadták sikeresen.⁴⁶ Ezen felül a személyiségprofilok kialakítása olyan kormányzat, igazságszolgáltatás, vagy jogvédő szervezetek által igényelt adatkezeléshez vezethet, amelyről a felhasználót nem értesítik.⁴⁷

A kockázat mértékét tovább növeli a Google visszatartási politikája, vagyis a garancia hiánya arra nézve, hogy időben törli az adatokat.

A 29-es munkacsoport kiemeli az Adatvédelmi Irányelv 1. cikk (1) bekezdését, amely szerint *“a tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében”*. Ezt az alapelvet az adatkezelés jogi alapjainak felbecsülésekor is

⁴² Google Privacy Policy Legal Analysis (2012.09.18.)

⁴³ <http://www.kantarworldpanel.com/Global/News/Android-maintains-Euro-dominance> (2012.10.20.)

⁴⁴ <http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&clearaf=1&qpaf=-000%09100%091%0D&qpcustomd> (2012.10.20.)

⁴⁵ Chrome, Firefox, Safari

⁴⁶ <http://techcrunch.com/2010/09/14/google-engineer-spying-fired/> (2012.09.28.)

⁴⁷ Ebben a témában a Google nem válaszolt a vonatkozó kérdésekre, illetve arra, hogy a jogvédő szervezetek megkeresései megtörténtek-e.

figyelembe kell venni, ha az „*adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges*”.⁴⁸

A Google a szolgáltatásokból összegyűjtött adatokat széleskörűen értelmezi az adott szolgáltatás aktív, vagy passzív használatától függően. Az adatkezelés elemzése csupán egy lehetséges következtetés, mert a munkacsoport kérdéseire nem, vagy nem kielégítő válaszokat kaptak.

Az adatkezelés céljai különbözőek lehetnek. A szolgáltatásokból összegyűjtött adatok hatással vannak azok kezelésére, és lehetővé teszik az egyes szolgáltatások számára, hogy adatokat gyűjtsenek a saját tevékenységi körükön kívül más szolgáltatásokból is. A munkacsoport nyolc olyan szituációt azonosított, ahol a leírt jelenség előfordul.

1. Egyes szolgáltatások esetében a felhasználó kérheti, hogy az adatai legyenek összevontan kezelve. Indokolt az opció alkalmazása a Gmail, Google Calendar, és Google Contacts esetében találkozók megbeszélése, vagy e-mailek küldése esetén. Másik gyakran előforduló példa a Google közösségi hálója⁴⁹ és a Picasa webalbum adatainak összevonása. Ezekben az esetekben a felhasználó egyértelműen látja, hogy az adatai összevontan vannak kezelve, és nem csak az éppen aktuálisan használt szolgáltatásból származnak. A szolgáltatáshoz is hozzáférési joggal rendelkezik, és törölheti adatait. Hasonló eset, amikor a felhasználó a keresőben a kifejezésre érkezett találatok után a „képek”, vagy „térkép” opcióra kattint a pontos eredmények végett. A szolgáltatásokból összegyűjtött adatoknak köszönhetően a Google a következő alkalommal azonnal megjeleníti a képeket, vagy a térképet a szöveges találatok mellett. Az ilyen típusú szituációk a legtöbb Google által üzemeltett szolgáltatás használata során előfordulnak.

2. A szolgáltatást igénybe veszi a felhasználó, de az összegyűjtött adatok kezelése a tudta nélkül zajlik. Ilyen eset, amikor a szolgáltatás részlegesen más szolgáltatások által kezelt adatokon alapul - a személyre szabott keresés egy általános jelenség, amitől a felhasználók nem tartanak.⁵⁰ Ilyenkor a felhasználó azt tapasztalja, hogy az adatait összevontan kezelik más szolgáltatásokéval, de nem tudja pontosan megállapítani, hogy melyikből származnak, sem pedig a lehetséges következményeit.

⁴⁸ 7. cikk c) pont

⁴⁹ Google+

⁵⁰ A Google 2011-ben beépítette szolgáltatásába a “Szó szerint” eszközt, amellyel pontosan rá lehet keresni a beírt kulcsszóra: <http://support.google.com/websearch/bin/answer.py?hl=hu&hlrm=fr&answer=1734130> (2012.10.20.)

3. A Google védelmi célokból is összegyűjtheti az adatokat, ezáltal a szolgáltatásai biztonságát erősíti, például a felhasználói fiókok közötti kapcsolatok vizsgálatával.
4. Gyakori eset, amikor az összevont adatkezelés termékfejlesztési, vagy marketing szempontból innovációs célokat szolgál. A különböző csatornákon keresztül összegyűjtött adatokat a Google új termékek, szolgáltatások tervezésére használja. Ezek a termékek a már meglévő adatokon alapulnak – például a Google Now szolgáltatás, ahol egy képernyőn minden szükséges információ megjelenik az adott naphoz, így például az aktuális időjárás, a felhasználó által beállított főbb hírek, térkép a szintén aktuális forgalmi viszonyokkal, mikor indul a következő vonat a célhoz, stb. Kiegészítésként a szokásokat megtanulja a Google Now, így a későbbi alkalmazások során egyre pontosabb információkat tud adni.⁵¹
5. A szolgáltatásokból összegyűjtött adatok kezelése a Google Fiók alapját képezi. Ez a fiók az összes adatot tartalmazza, ami a különböző szolgáltatások során jön létre. Az új Google Adatvédelmi Irányelv kommunikációs kampánya során kiemelt szerepet kapott az egyetlen fiókba összegyűjtött felhasználóhoz kapcsolható információ.⁵² A fiók létrehozásának azonban nem szükségszerű feltétele az adatok összevonása. Több olyan online mechanizmus létezik,⁵³ amely engedélyezi egy szolgáltatásnak, hogy egy másik szolgáltatás meghatározott adataihoz hozzáférjen az adatok összevonása nélkül. Az sem indok az összevonásra, hogy a szolgáltatásokat ugyanaz a cég nyújtja. Mindenesetre ez a megoldás érdekes lehet a felhasználó számára, hiszen egy teljes képet kap a különböző szolgáltatásokban kezelt adatairól. Ehhez nyújt segítséget a Google Irányítópult.
6. Összevont adatokat szintén használnak reklámcélokra, például az AdWords szolgáltatás keretében.
7. Analitikai célokra is felhasználhatók a személyiségprofilból nyert adatok. A fájlmegosztás engedélyezésével a Google Analytics szolgáltatásában felhasználhatja azokat különböző értékelésekhez, elemzésekhez. A Google azt állítja, hogy ebben az esetben adatfeldolgozóként tevékenykedik, de nem tisztázta azt, hogy mi történik, amikor a látogató adatait, amit a felhasználók megosztanak a Google-lal nem kapcsolják össze azokkal az adatokkal, amik már szerepelnek róluk a rendszerben. Ha az összekapcsolás megtörténik, a Google mint adatkezelő jár el. Emiatt, valamint a biztonság növelése érdekében Németország módosította az adatvédelmi törvényét.

⁵¹ http://www.telefonguru.hu/hir/Bemutatjuk_a_Google_Now-t_2012-8-1 (2012.09.28.)

⁵² A korábbi Irányelvekben a Youtube fiók még külön szerepelt.

⁵³ Például: Facebook, Twitter

8. Összekapcsolt adatok egyetemek kutatási céljaira is felhasználhatók. Ebben az esetben az adatkezelőnek különböző előkészületi kötelezettségei vannak, mint például az anonimizálás, mintavétel stb.

Az ugyan egyértelmű, hogy a személyiségprofil szolgáltatások felhasználók általi használata során jön létre, szükséges megjegyezni azonban, hogy a felhasználóknak is több fajtája van, még tovább differenciálva ezzel a monitoring tevékenységet.

3.2.1. Fiókkal rendelkező felhasználók

A felhasználók egy rétegét a valamely Google szolgáltatásban felhasználói fiókkal rendelkezők köre alkotja. Ebben az esetben a Google minden információt begyűjt a felhasználóról, amelyek a szolgáltatás használata során keletkeznek, ezen felül azok az adatok is tárolásra kerülnek, melyek nyílt szolgáltatásban jönnek létre, például a Youtube, vagy a Maps használata során. A különböző módon keletkezett adatokat a Google cookie-k segítségével rendezi egy profilba.

3.2.2. Fiókkal nem rendelkező felhasználók

Nem regisztrált felhasználók esetében a legtöbbször az ún. PREF cookie segítségével gyűjt adatokat a Google, melyek nem a felhasználót azonosítják, hanem a felhasználó által használt böngészőben látogatott oldalakat.

3.2.3. Passzív felhasználók

A harmadik típusú (passzív) felhasználóknál az ún. DoubleClick Cookie segítségével gyűjt adatokat olyan oldalakon, amelyek alkalmazzák ezt a cookie-t. A Google állítása szerint *“nem hoz létre olyan adatokat, amelyek alapján megállapítható a személyazonosság”*, azonban azt elismeri, hogy az adatok között szerepelnek IP-címek, pontos földrajzi helyek, illetve meghatározható eszközök. A 29-es munkacsoport által elvégzett kutatások során nem volt megállapítható, hogy a PREF, illetve a DoubleClick cookie által gyűjtött adatokat együttes kezelik-e.

3.3. Monitoring jogalapja – a Google Adatvédelmi Irányelve

Adatvédelmi szempontból a Google legfontosabb dokumentuma a legújabb, 2012-es Adatvédelmi Irányelve. Ebben részletesen leírja a személyes adatok feldolgozásának módját, további információkhoz való hozzájutást biztosít, illetve bemutatja a különböző adatvédelmi eljárások működését.

A 2012. március 1-jén megjelent irányelvvel egy időben a Google létrehozott egy „Elvek és Irányelvek”⁵⁴ nevű oldalt, amely egy áttekintést,⁵⁵ az általános szerződési feltételeket, illetve a legfrissebb adatvédelmi irányelvet tartalmazza. Ezek mellett kiegészítő információk találhatók a reklámszolgáltatásról, a Google adatvédelemhez köthető alapelveiről, eszközeiről, blogjairól, videóiról, és Gy.I.K.-ról. Az oldal a legtöbb Google honlapról elérhető, ezzel is hangsúlyozva kiemelkedő fontosságát.

A rövidítés, illetve a kevésbé jogias és ezáltal jobban érthető nyelvezet volt a fő mozgóeleme az új Privacy Policy létrehozásának. A szabályozás maradt lineáris és beszámoló jellegű, a Facebookkal⁵⁶ ellentétben nem engedi az olvasónak a különböző információk közti navigálást, és nem különíti el az állításokat a gyakorlati példáktól. Felépítése nem különbözik az ezt megelőző, 2011. novemberi Privacy Policytől,⁵⁷ tartalmilag a legfontosabb újítás a több mint 60 termék specifikus adatvédelmi irányelv harmonizálása, általánosítása.

Az egyes szolgáltatások adatvédelmi irányelveinek egyesítésének első lépései a 2010. októberi irányelvben jelentek meg. Olyan termékek önálló szabályozásai szűntek meg, mint a Gmail, a Maps, vagy a Docs. Ez azzal járt, hogy a termékekhez kapcsolódó adatmegőrzési határidőkről szóló információk is elvesztek, mint például a Calendar,⁵⁸ a Google Docs,⁵⁹ vagy a Gmail⁶⁰ esetében. Utóbbinál érdekesség, hogy a saját szabályozása szerint az e-mail tartalma felhasználható volt reklámok személyre szabása céljából, de a 2011-es és 2012-es Irányelvekben⁶¹ ezek már nem szerepelnek.

2012-ben általánosításra került a termék specifikus adatvédelmi irányelvek egységesítő politikája, mert a Chrome, Chrome OS, Wallet és Books kivételével az összes szolgáltatásra az új irányelv vonatkozik. A felsoroltak mellett a más cégektől vásárolt szolgáltatások⁶² sem kerültek be a Privacy Policy hatálya alá.

⁵⁴ <http://www.google.com/policies/> (2012.10.15.)

⁵⁵ Az oldal tartalma e-mailekben és egyéb oldalakon is látható volt regisztrált felhasználók számára.

⁵⁶ <http://www.facebook.com/about/privacy/> (2012.10.23.)

⁵⁷ Ami a 2010. októberinek egy kisebb frissítése.

⁵⁸ Statisztikai adatok esetén 90 nap.

⁵⁹ 30 nap aktív szerveren, illetve 60 nap törlés után.

⁶⁰ 60 nap aktív szerveren fiók a törlése után.

⁶¹ Habár a Google ezt elmagyarázza más oldalakon:

<https://support.google.com/mail/bin/answer.py?hl=en&topic=1668949&hlrm=fr&ctx=topic&answer=6603> (2012.10.05.)

⁶² Például a Firefoxba integrált helymeghatározás.

Az Privacy Policy hosszának rövidítésére volt szükség a Google Buzz-ügy után, amely az Egyesült Államok Kereskedelmi Bizottsága (U.S. Federal Trade Commission, továbbiakban FTC) előtt zajlott. Az ügy a Google megtévesztő adatvédelmi politikája ellen indult. A FTC azzal vádolta a céget, hogy az megsértette saját adatvédelmi szabályozását, amikor a Gmail által gyűjtött információkat a felhasználó engedélye nélkül más célokra is felhasználta. Az új Irányelv ezt, és a hasonló vádak egyértelműen kizárja, hiszen bármely szolgáltatás során gyűjtött adatok felhasználhatók bármely másik szolgáltatásban (létező, vagy jövőben megjelenő).

Irányelveinek homogenizálása lehetővé tette a Google számára, hogy jogilag védetté tegye az adatvédelmi gyakorlatát és elkerülje a jövőbeni vádak. Hátrányos következménye azonban az összevonásnak az egyes szolgáltatások részleteiről szóló információk eltűnése. A Google nem volt képes kiállítani egy listát azokról a dokumentumokról, amelyeket visszavont.⁶³ A tény, hogy nem hozta létre ezt a dokumentumot megkérdőjelezi a Google szolgáltatásai feletti irányításának szintjét, és azok adatvédelmi politikáját.

A munkacsoport szerint mindegyik szolgáltatás egy önálló adatkezelési folyamat, akkor is, ha össze vannak kötve, és a felhasználónak képesnek kellene lennie arra, hogy világosan elkülönítse az egyes szolgáltatások adatkezelésének karakterisztikáját. A Google az új Privacy Policyben⁶⁴ információt nyújt arról, hogy adatkezelés címen mit tehet, valamint egy listát arról, amiket nem tehet. Utóbbiról az európai jogalkotás egy pontos felsorolást, és meghatározást igényel az adatkezelések összességéről.

4. Európai Unió törekvések

Az Európai Unió tagállamainak adatvédelmi hivatalai új ajánlásokat fogalmaztak meg arról, hogyan kellene alkalmazni az európai adatvédelmi ajánlásokat a cookie-k esetében. A szabályozás természetesen nem a beállításokat és bejelentkezési adatokat tároló cookiekkal foglalkozik, hanem azokkal, amik képesek a felhasználó böngészését követni és egyedi azonosítókkal látják el, teljes profilt építve a tevékenysége alapján.

Az új ajánlások élesen elválasztják, és teljesen külön kezelik az ártalmatlan, vagy viszonylag veszélytelen cookie-kat, amiket a weboldalak továbbra is telepíthetnek a felhasználó beleegyezése nélkül. A problémát a követésre alkalmas cookie-k indukálják, amiknek a

⁶³ A régebbi "fő" Irányelveket bemutatta ugyan, de a termékspecifikus szabályozásokat nem.

⁶⁴ Google Adatvédelmi Irányelve - <http://www.google.com/intl/hu/policies/privacy/> (2012.10.08.)

használatáról a 29-es munkacsoport szerint mindenképp értesíteni kell a weboldalaknak a felhasználókat. Az ajánlás külön kiemeli azokat a típusokat, amik a felhasználó teljes böngészését végigkövetik, hogy a szokásai alapján releváns hirdetéseket tudjon neki mutatni.

A korábbi ajánlásokkal ellentétben már jele sincs a kétértelműségnek, a szabályozók egyre pontosabban képesek megfogalmazni az irányelveket. Ennek hatására a hirdetési cégeknek sokkal nehezebb lesz észrevétlenül működni, ami jelentős mértékben visszavetheti az elérésüket, amennyiben az ajánlásokból előbb-utóbb kötelező erővel bíró direktíva lesz.

A szakmai anyag folyamatosan ellentéteket szít, és a különböző érdekcsoportok ugyanazokat a rendelkezéseket is képesek teljesen másképp értelmezni. A hirdetői csoportok legfontosabb vesszőparipája az értesítési kötelezettség. A hirdetőik szerint a felhasználónak számtalan eszköze van arra, hogy a követést korlátozza, s ezek többsége közvetlenül a böngészőből megtehető. Magyarországon az Adverticum már közel egy éve felismeri a böngészős opt-out lehetőséget és a felhasználónak csak egyszer kell kijelentkeznie, nem követik a továbbiakban.

A legtöbben a webes hirdetési piacot is féltik. Amennyiben valóban szigorú szabályokhoz kötné az Európai Unió a követő cookie-k használatát, az vélhetően sokat rontana a mostani állapotokon. Az IDATE kalkulációi szerint az európai webes hirdetési piac összességében 13,9 milliárd eurót tenne ki normális esetben, a korlátozások miatt ez biztosan kevesebb lenne. Az IAB⁶⁵ folyamatosan tiltakozik a szabályozás ellen, amellyel kapcsolatban Helene Chartier, az IAB France jelenlegi vezetője is felszólalt: *“Jelenleg így is és úgy is értelmezhetjük a szabályt”*. Szerinte az ilyen felvetések helyett sokkal inkább azon kellene az iparágnak dolgoznia, hogyan lehet a fogyasztókat kitanítani a célzott hirdetésekkel és azok előnyeiről.

„A már évek óta tartó huzavona azt bizonyítja, hogy Európának komoly problémái vannak ezzel a területtel és sajnálatos, hogy a bürokrácia vaskalapossága és a mindent szabályozni akarás miatt a világ legszigorúbb webes adatvédelmi szabályozása jön létre” - állítja az IAB. Ez a felhasználók számára is kényelmetlen lehet, de egyben az egész iparágot is visszavetheti, ami közvetetten akár az európai régió versenyképességét is negatívan érintheti.

A szabályozók irányelvei a kereskedők szerint rontani fogják az elektronikus kereskedelem teljesítményét. Az előzetes beleegyezési kérelmek miatt a felhasználói interakció jelentősen

⁶⁵ Interactive Advertising Bureau

hosszabbodhat és bonyolódhat. Iparági konszenzusra továbbra sem lehet számítani, a nyugat-európai webes ipar nagyobb szereplői kivétel nélkül kívánnak. Akik nem teljesen elutasítók, azok is igyekeznek az értesítés fogalmát a lehető legszélesebben értelmezni. Az alternatív megoldások közt értelemszerűen olyan eszközök vannak főleg, amit az átlagos felhasználó nem vesz észre, nem tud értelmezni, a híre nem ér el hozzá.⁶⁶ Egy felmérés szerint a brit webes cégek 80 százaléka elutasítja ezeket az irányelveket, és még akkor is ellenállna, ha büntetéseket helyeznének kilátásba.⁶⁷

Neelie Kroes, az Európai Bizottság digitális politikáért felelős biztosa a Centre for European Policy Studies⁶⁸ rendezvényén tartott beszédében egyértelművé tette, nem tűri, hogy a gazdasági érdekcsoportok használhatatlanná tegyék az elfogadás előtt álló új Do Not Track szabványt. A biztos aggodalmainak is hangot adott: *„Őszinte leszek - a szabványosítási eljárás nem a terveknek megfelelően alakul. Ami azt illeti, egyre jobban aggódom a késlekedés és a W3C által rendezett egyeztetések vargabetűi miatt. Tudom, hogy az Atlanti-óceán túlpartján, a Szövetségi Kereskedelmi Bizottságnál dolgozó kollégáim is osztják az aggodalmaimat. És hogy mi a legfőbb gond? A listám elején a DNT-szabvány felvizezése áll.”*

Ennek kapcsán elmondta, hogy *„a DNT-szabványnak elég átfogónak, és jelentőségteljesnek kell lennie ahhoz, hogy valódi előrelépést jelentsen az emberek magánéletének védelmében. Tudatos hozzájárulásra kell épülnie, és lehetővé kell tennie, hogy a felhasználók ellenőrizhessék a velük kapcsolatos információk felhasználását.”* Ugyan nem nevesített cégeket és szakembereket, beszédében mégis utalt egy szolgáltatásra, amely e dolgot bevezetőjében említett Internet Explorer 10 Do Not Track beállításait változtatja meg – *„a közelmúltban napvilágot látott beszámolók szerint az egyik népszerű webszerver olyan szolgáltatást mutatott be, amelynek lényege, hogy felülírja a DNT-t. Ez a felhasználók kívánságának semmibe vételét jelenti, amit meglehetősen aggasztónak és nemkívánatosnak találok. Az online vállalkozásoknak szem előtt kell tartaniuk az adatvédelmi követelményeket, különben nem lesznek képesek működni, mert az emberek nem fogják használni, amelyekben nem bíznak”*.⁶⁹

⁶⁶ <http://www.hwsz.hu/hirek/48535/europai-bizottsag-cookie-web-jog-maganszfera-privacy.html> (2012.09.20.)

⁶⁷ <http://www.hwsz.hu/hirek/48535/europai-bizottsag-cookie-web-jog-maganszfera-privacy.html> (2012.10.25.)

⁶⁸ <http://www.ceps.be/> (2012.10.15.)

⁶⁹ <http://computerworld.hu/kroes-elesen-tamadja-a-do-not-track-felvizezeset-20121012.html> (2012.10.12.)

4.1. Az Adatvédelmi Irányelv

A személyes adatok feldolgozása vonatkozásában a 95/46/EK Irányelv 1. cikkében céljai között határozta meg, hogy a „tagállamok az irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében.”⁷⁰ Ezen felül a „tagállamok nem korlátozhatják, és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását az (1) bekezdés értelmében biztosított védelemmel kapcsolatos indokok miatt.”⁷¹

A 3. cikk alapján az Irányelv hatálya kiterjed „a személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.” A tagállamoknak akkor kell a nemzeti jogukat alkalmazni, ha az adatfeldolgozás a területükön történik.⁷²

A 6. cikk rendelkezik az adatok minőségéről. Ez alapján „a személyes adatok feldolgozását tisztességesen és törvényesen kell végezni; gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon. A személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat; gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek; pontosak, és ha szükséges, időszerűek kell legyenek; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy a hibás vagy hiányos adatok, tekintettel gyűjtésük vagy további feldolgozásuk céljaira, törlésre vagy helyesbítésre kerüljenek; tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé...” Az adatkezelőnek további kötelezettsége az érintett – akitől a rá vonatkozó adatokat gyűjtik – tájékoztatása az adatkezelő személyéről, az adatfeldolgozás céljáról,

⁷⁰ 95/46/EK Irányelv 1. cikk (1)

⁷¹ 95/46/EK Irányelv 1. cikk (2)

⁷² 95/46/EK Irányelv 3. cikk (1) Ezen Irányelvet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

amelyre az adatokat szánják, illetve egyéb adatokról, mint például az adatok címzettjei, vagy az adatok helyesbítéséhez való jog.⁷³

4.2. Az e-Privacy Irányelv módosítása

A Google, és azon belül is az AdWords szolgáltatás adatkezelői tevékenységét reklámszolgáltatásából adódóan folytatja, így különös figyelmet fordított az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK Irányelv (továbbiakban hírközlési irányelv) módosítására. A módosítás előkészítése során született meg a 29-es munkacsoport által az „1/2009 vélemény a magánélet védelméről és az elektronikus hírközlési ágazatról szóló 2002/58/EK Irányelvet (elektronikus hírközlési adatvédelmi irányelv) módosító javaslatokról”. A munkacsoport véleményében kitért többek között a személyes adatok megsértésére, a bejelentési kötelezettségekre, az IP-címekre, valamint a nem kívánt tájékoztatásra és a böngészés beállításaira.

4.2.1. IP-címek

A munkacsoport egyetértett a bizottsági észrevételekben javasolt megfogalmazással, ahol külön hivatkoztak a munkacsoport munkájára. A dokumentumban újra hangsúlyozza korábbi véleményét,⁷⁴ amelynek értelmében a szolgáltatónak „*valamennyi IP-információt személyes adatként kell kezelnie, ha a biztonság talaján kíván maradni, kivéve, ha olyan helyzetben van, hogy teljes bizonyossággal el tudja dönteni az adatról, hogy az nem azonosítható felhasználóra vonatkozik*”. Az IP-címek legtöbb esetben azonosítható személyekre utalnak. Az azonosíthatóság az internetszolgáltató általi vagy egyéb eszközök révén további olyan azonosítók segítségével történő azonosíthatóságot jelent, mint például a cookie-k vagy a webes szolgáltatások igénybevétele, amelyek révén az adatalany közvetlen, vagy közvetett módon azonosíthatóvá válik.

Az adatvédelmi irányelv (26) preambulum bekezdése egyértelműen kimondja, hogy 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*”.

⁷³ 95/46/EK Irányelv 10. cikk

⁷⁴ A személyes adat fogalmáról szóló 4/2007 vélemény, valamint a keresőmotorokkal kapcsolatos adatvédelmi kérdésekről szóló vélemény

A személyes adatnak az adatvédelmi irányelvben található meghatározása személyekre vonatkozó adatokra, valamint arra utal, hogy az IP-címeket általában arra használják, hogy megkülönböztessenek felhasználókat, akik esetében például célzott reklám küldése vagy profil készítése keretében eltérő eljárást kell alkalmazni.

A munkacsoport egyetértett a Bizottsággal abban, hogy egy irányelv érdemi rendelkezése nem a legmegfelelőbb eszköz a probléma kezelésére, valamint hogy az „*irányelv által le nem fedett célokra*” utaló jelentési kötelezettség nem helyénvaló.

4.2.2. A böngésző beállításai

A munkacsoport ellenezte a Parlament által elfogadott módosítást, amely kimondta, hogy a böngésző beállításai előzetes hozzájárulásnak minősülnek. Eltekintve az abból adódó alaki problémától, hogy technológiailag specifikus nyelvezetet teremtett az e-Privacy Irányelv, a munkacsoportot aggasztotta a hozzájárulás fogalmának lerontása, valamint az átláthatóság ebből következő hiánya. A legtöbb böngésző olyan beállításokat alkalmaz, amelyek lehetővé teszik a felhasználó számára, hogy tájékozódjon a saját eszközeit érintő bármely tárolásról vagy hozzáférésről. Ennél fogva a böngészők beállításainak „*tiszteletben kellene tartaniuk a magánélet védelmét*”, de nem szolgálhatnak a felhasználó önkéntes, kifejezett és tájékoztatást követő hozzájárulásának gyűjtésére, ahogyan az az adatvédelmi irányelv 2. cikkének h) pontjában⁷⁵ áll.

A cookie-k tekintetében a munkacsoport úgy vélte, hogy a cookie-k kezelőjének kellene tájékoztatnia a felhasználókat az adatvédelmi nyilatkozatban és nem lenne szabad a böngésző (eredeti) beállításaira hagyatkoznia. Így a választott megfogalmazás nem korlátozódik a cookie-k kibocsátására, de kiterjed valamennyi olyan egyéb új technológiára, amellyel a felhasználó által a böngésző alkalmazása során gyakorolt viselkedést nyomon lehetne követni. A Munkacsoport a vélemény végén felszólította az európai jogalkotókat, hogy a véleményben kiemelt egyéb kérdések mellett mindenekelőtt azt vegyék fontolóra, hogy ki kellene terjeszteni a személyes adatok megsértése bejelentési kötelezettségének hatályát az információs társadalommal összefüggő szolgáltatásokra, mivel az elengedhetetlenül fontos hatást gyakorol az összes európai polgár személyes adatainak védelmére.

A módosítás végül a 2009/136/EK Irányelv által valósult meg, amelynek hatásairól a 3.1.3.1. fejezetben már volt szó.

⁷⁵ "az érintett hozzájárulása" az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítása, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához.

5. Az e-Privacy Irányelv implementálási problémája Magyarországon

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban Avtv.) helyébe lépő Infotv.-ből kitűnik, hogy a személyes adatok védelméről szóló szabályozásban jelentős változás nem történt. Ahogy az Avtv. úgy az Infotv. is összhangban áll az Adatvédelmi Irányelv rendelkezéseivel, így külön tárgyalást nem igényel.

A kisebb módosítások azonban mindenképp említést érdemelnek, mint például a 2. § (3) bekezdése,⁷⁶ amely a törvény hatályát kiterjeszti az unión kívüli adatkezelő által megbízott Magyarországon végzett adatfeldolgozásra. A személyes adatok védelme a 4. § (1) bekezdésében szigorodott – a „személyes adatot kezelni csak meghatározott célból...” megfogalmazást a „személyes adatot *kizárólag* meghatározott célból...” váltotta fel. Az adatbiztonság követelménye alapján az *„adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.”*⁷⁷

A 7. § (4)-(6) bekezdések szigorú feltételeket szabnak az adatállományok biztonságának megőrzése érdekében, úgy mint az automatikus adatfeldolgozó rendszerek jogosulatlan személyek által történő használatának megakadályozása, az adattovábbítás követelményei, vagy az ellenőrzések részletszabályai. A Google adatkezelési politikája szempontjából érdekesnek tűnik a (4) bekezdés, amely szerint *„a különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelkezhetőek”*. Ez alapján nem lenne lehetőség a személyiségprofilok kialakítására itthon, de a törvény engedi a külföldi adatfeldolgozást a 8. §-ban,⁷⁸ így a Google-nek lehetősége van kikerülni a magyar szabályozást.

⁷⁶ E törvényben foglaltakat kell alkalmazni, ha az Európai Unió területén kívül személyes adatok kezelését folytató adatkezelő az adatfeldolgozással Magyarország területén székhellyel, telephellyel, fiókteleppel vagy lakóhellyel, tartózkodási hellyel rendelkező adatfeldolgozót bíz meg, vagy itt lévő eszközt használ fel, kivéve, ha ez az eszköz csak az Európai Unió területén átmenő adatforgalom célját szolgálja. Az ilyen adatkezelőnek Magyarország területén képviselőt kell kineveznie.

⁷⁷ Infotv. 7. § (1) bekezdés

⁷⁸ 8. § (1) Személyes adatot e törvény hatálya alá tartozó adatkezelő harmadik országban adatkezelést folytató adatkezelő vagy adatfeldolgozást végző adatfeldolgozó részére akkor továbbíthat, ha ahhoz az érintett kifejezetten hozzájárult, vagy az adatkezelésnek az 5. §-ban (Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul...), illetve a 6. §-ban előírt feltételei teljesülnek, és a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

A 2009/136/EK Irányelv hazai átültetésével kapcsolatosan megállapítható, hogy a jogalkotó komoly hibát követett el, ugyanis az Irányelv 5. cikk (3) bekezdése, és az ott rögzített előzetes hozzájárulás követelménye kizárólag az elektronikus hírközlésről szóló 2003. évi C. törvénybe (továbbiakban Eht.) került átültetésre,⁷⁹ ennél fogva ez a követelmény csak elektronikus hírközlés területén alkalmazandó. Ezzel szemben információs társadalommal kapcsolatos szolgáltatásokra (ami fogalmilag sem rendelhető az elektronikus hírközlési szolgáltatás meghatározása alá) továbbra is az Ekertv. 13/A §⁸⁰ adatvédelmi szabályai irányadóak, amelyek az új módosítással ellentétben jóval tágabb körben teszik lehetővé a hozzájárulás alóli kivételek alkalmazását. A jogharmonizáció megteremtése érdekében tehát az Ekertv. nyilvánvalóan módosításra szorul.⁸¹

6. Interkontinentális együttműködés

Az Amerikai Egyesült Államok az Európai Gazdasági Térségből származó adattovábbítások esetén speciális helyzetben van, mivel az előbbi nem rendelkezik általános adatvédelmi szabályozással.⁸² Figyelembe véve az EU és az USA közötti kereskedelmi kapcsolatokat és a tömeges adattovábbításokat, az Amerikai Egyesült Államok Kereskedelmi Minisztériuma és az Európai Bizottság célul tűzte ki egy megfelelő egyezményes keret létrehozását, amelynek alapján amerikai adatkezelők az európai adatvédelmi irányelv követelményeinek – önszabályozás alapján – meg tudnak felelni. Ezek az ún. Safe Harbor adatvédelmi elvek, melyek irányelvnek való megfeleléséről 2000. július 26-án bocsátott ki határozatot⁸³ az Európai Bizottság.

Amerikai Egyesült Államokbeli adatkezelő, illetve adatfeldolgozó esetében többek között abban az esetben tekinthető biztosítottnak a személyes adatok megfelelő szintű védelme, amennyiben a személyes adatokat ún. Safe Harbor listán szereplő vállalat részére továbbítják.

A Safe Harbor elveknek való megfelelés önminősítés alapján történik, az érintett amerikai székhelyű vállalat önkéntes döntése alapján. Mivel csak vállalatok lehetnek alanyai a

⁷⁹ (4) Egy előfizetőnek vagy felhasználónak elektronikus hírközlő végberendezésén csak az érintett felhasználó vagy előfizető világos és teljes körű - az adatkezelés céljára is kiterjedő - tájékoztatását követő hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni.

⁸⁰ Adatvédelem című fejezet

⁸¹ <http://www.dataprivacy.hu/archives/1086#more-1086> (2012.10.28.)

⁸² Az amerikai gyakorlatot a szektorális adatvédelmi megközelítés jellemzi.

⁸³ A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfeleléséről és az ezzel kapcsolatos gyakran felvetődő kérdésekről

programnak, társadalmi szervezetek ebben értelemszerűen ebben nem vehetnek részt, más adattovábbítási megoldást kell alkalmazniuk. A programban való részvétele esetén egy vállalat először csatlakozik egy ötanúsítási programhoz, ami megfelel a Safe Harbor elveknek vagy saját adatvédelmi (ön)szabályozásnak veti alá magát. Ezt követően kinyilvánítja az elveknek való megfeleléseit, melyet adatvédelmi szabályzatában is nyilvánosan közzétesz, továbbá minimális díj megfizetése mellett az USA Kereskedelmi Minisztériuma részére évente írásban kinyilvánítja (ötanúsítja), hogy az adatvédelmi elveknek megfelel, és ezáltal feltüntetésre kerül a Safe Harbor listán.

A Safe Harbor gyakorlati jelentőségét mutatja, hogy a legnagyobb amerikai adatkezelők, a Facebook, a Google,⁸⁴ Amazon, eBay illetve a legnagyobb amerikai vállalatok a Safe Harbor listán való szereplés útján biztosítják azt, hogy adatkezelésük megfelelően az európai adatvédelmi irányelv rendelkezéseinek (érdekesség, hogy az irányelvek maguk nem használják az „adatkezelő”, illetve „adatfeldolgozó” kifejezéseket⁸⁵).

Az EU-USA adattovábbításokat szabályozó Safe Harbor program tíz éves évfordulója nem volt kritikus felhangoktól mentes. A Safe Harbor működésében ugyanis komoly hiányosságok mutatkoztak, mivel a végrehajtás kizárólag az amerikai jogszabályok alapján történik meg, végső esetben az FTC végrehajtása útján, ami „megtévesztés” miatt szankcionálhatja az adatvédelmi elveknek való megfelelést tanúsító, de azoknak gyakorlatilag eleget nem tevő vállalatokat. A végrehajtás gyenge hatékonyságát mutatja, hogy az FTC részéről a tíz év alatt csupán hét esetben került sor eljárásindításra a Safe Harbor megsértése miatt, melyet a Schleswig-Holstein adatvédelmi hatóságának vonatkozó sajtónyilatkozata⁸⁶ is kiemel. A nyilatkozatban a tartomány adatvédelmi biztosa kiemeli, hogy haladéktalanul meg kellene szüntetni a Safe Harbor rendszert az annál tapasztalható széleskörű visszaélések miatt.⁸⁷

⁸⁴ „A Google megfelel az Amerikai Egyesült Államok Kereskedelmi Minisztériuma által meghatározott, az Amerikai Egyesült Államok és az EU viszonyára vonatkozó „Safe Harbor” keretszabályzat rendelkezéseinek, az Európai Unió tagországaiból és Svájcban származó személyes adatok gyűjtésére, használatára és megőrzésére vonatkozóan. A Google igazolta, hogy megfelel a „Safe Harbor” Adatvédelmi irányelvek értesítésre, választásra, továbbításra, biztonságra, adatintegritásra, hozzáférésre és végrehajtásra vonatkozó rendelkezéseinek.” - <http://www.google.com/intl/hu/policies/privacy/frameworks/> (2012.10.20.)

⁸⁵ http://www.huntonfiles.com/files/webupload/CIPL_Safe_Harbor_3.08.pdf (2012.10.20.)

⁸⁶ https://www.datenschutzzentrum.de/presse/20100723-safe-harbor_en.htm (2012.10.20.)

⁸⁷ <http://www.dataprivacy.hu/archives/133#more-133> (2012.10.20.)

7. A lehetséges jövő – az új adatvédelmi csomag

7.1. A reformtörekvések indokai

Az adatvédelmi irányelv felülvizsgálata hosszú ideje napirenden van. Ez a folyamat 2010. november 4. napjával fontos állomásához jutott, mivel az Európai Bizottság ekkor tette közzé az európai adatvédelmi irányelv módosításával kapcsolatos koncepcióját.

A Bizottság szigorúbb jogérvényesítést, adatvesztések tényének kötelező közzétételét, az direktíva implementációjának egységesebbé tételét, továbbá adatvédelmi jogsértésekre tekintettel büntető szankciók kötelező alkalmazását javasolta és a következő évben már konkrét jogszabályi javaslatot kívánt ezzel kapcsolatosan előterjeszteni. Azt azonban hangsúlyozták, hogy az új szabályozás a korábbihoz hasonlóan technológia-semleges marad. Ez az erőteljesebb harmonizáció az adatalanyok és egyéb érintett szereplők számára közel azonos jogokat és kötelezettségeket, kiszámítható jogi környezetet hozott az egységes piac nyújtotta lehetőségek jobb kihasználhatósága érdekében. Mindez kiegészült eltérő jogosítványokkal eljáró nemzeti adatvédelmi hatóságok munkájának egymáshoz való igazításával is.

A jelenleg is hatályos adatvédelmi irányelv felülvizsgálatát számos körülmény indokolja, közöttük az, hogy a szabályozás szövegét 1995-ben fogadták el, míg az adatkezeléssel kapcsolatos gyakorlatok azóta komoly változásokon estek át. Ezek közül kiemelendő az Internet tömegessé válása, az internetes keresők megjelenése, a tartalommegosztásra épülő web 2.0, a közösségi oldalak térhódítása, vagy akár a cloud computing alkalmazása. A nemzetközi adattranszferek mindennapossá váltak, gyakorlatilag irrelevánsnak tekinthető az adat kezelésének fizikai helye, mivel ugyanazon szervezet egyidejűleg több országban található szerveren is tárol személyes adatokat.

A Bizottság legfontosabb törekvése, hogy a továbbiakban is fenntartsa az Európai Unió adatvédelemhez fűződő jog érvényesítésével kapcsolatos vezető szerepét, ami sikertörténetnek tekinthető, ugyanis világszinten az adatvédelmi, illetve magánélethez fűződő jogokkal kapcsolatos konvergenciát eredményezett.⁸⁸ Itt említendő az Európai Emberi Jogi Egyezmény, továbbá a Lisszaboni Szerződéssel kötelező erejűvé vált Alapjogi Charta. Ez

⁸⁸ <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Dataprotection/Legislation> (2012.10.25.)

utóbbi 8. cikke⁸⁹ önálló jogként nevesíti az adatvédelemhez való jogot és a végrehajtás felügyeletéről is rendelkezik. Az adatvédelemhez fűződő jog mégsem önállóan áll, hanem a digitális korszakban legalább olyan fontos véleménynyilvánítás szabadságával való összefüggésben kell azt szemlélni és megfelelő egyensúlyt kell teremteni a különböző alapjogok között.

A célkitűzések kardinális pontjai közé tartozik az adatalanyok jogainak erősítése, a belső piaci dimenzió erősítése, az adatvédelem nemzetközi dimenziójának erősítése, valamint az egyes új elvek, úgymint a személyes adatok tárolásának megszüntetéséhez és a törléshez való jog, a beépített és alapértelmezett adatvédelem, az érintett értesítése a személyes adatok megsértéséről, az adatvédelmi hatásvizsgálat, vagy az adatkezelő felelőssége.

7.1.1. Az adatalanyok jogainak erősítése

A Bizottság az adatvédelmi irányelv fogalmainak koherens alkalmazását kívánja megerősíteni, mivel az irányelv fogalmainak rugalmas alkalmazása több esetben bizonytalansághoz vezetett, mind az adat alanyát megillető jogok, mind pedig az adatkezelői kötelezettségek vonatkozásában. Növelni szükséges az adatkezelési tevékenységek átláthatóságát, illetve meg kell teremteni annak kötelezettségét, hogy az adatalanyok részére a tájékoztatást egyértelműen és érthető, egyszerű nyelven adják meg, ideértve különösen a gyerekek személyes adataival kapcsolatos tájékoztatásokat. A transzparencia elvének bevezetése, illetve standard adatvédelmi tájékoztatók alkalmazása is a lehetőségek között szerepel.

Ezen kívül az adatvesztéssel kapcsolatos kötelező tájékoztatás⁹⁰ is bevezetésre kerülhet. A Bizottság erősíteni kívánja az adatelkerülés elvének hatékony alkalmazását, az adat alanyát megillető jogok gyakorlására vonatkozó konkrét jogosultságok (hozzáférés, helyesbítés, törlés) határidőkhöz és formához kötött gyakorlását, illetve a törléshez való jog hatékony érvényesítésének lehetőségét is. A tájékozott önkéntes bejegyzés feltételeinek egységes megteremtését is meg kell valósítani, mivel ezeket a követelményeket szintén eltérően

⁸⁹ Mindenkinnek joga van a rá vonatkozó személyes adatok védelméhez. (2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinnek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.

⁹⁰ Lásd bővebben: 7.2.3. pont.

értékelik az egyes tagállamokban. A Bizottság súlyos adatvédelmi jogsértések esetére büntetőjogi szankciók alkalmazását javasolja.

7.1.2. A belső piaci dimenzió erősítése

Az európai adatvédelemnek rendkívül erős belső piaci dimenziója van, mivel a tagállamok között a személyes adatok szabad áramlását is biztosítani kell. Ennek ellenére számos komoly eltérés tapasztalható a tagállami adatvédelmi jogok között, melynek egyik oka, hogy az Irányelv széles jogalkotási dimenziót biztosít a tagállamoknak, másrészt a tagállamok sokszor hibásan ültették át az Irányelv rendelkezéseit, ami nemzetközi társaságok számára jelentős adminisztratív terheket okoz. Éppen ezért elkerülhetetlen a további harmonizáció biztosítása. A magas és emiatt csökkentésre szoruló adminisztratív költségek között említendőek a tagállami bejelentési kötelezettségek, melyeket nemzetközileg aktív adatkezelőknek minden egyes országban teljesítenie szükséges.

Fontos az Irányelv hatályával kapcsolatos kérdések tisztázása, hogy melyik felügyeleti hatóság felelős az adatkezelés felügyeletéért. Az eltérő tagállami jogszabályi követelmények ugyanis konfliktushoz vezetnek különösen több tagállamban letelepedett adatkezelők vonatkozásában és sokszor lehetetlen az alkalmazandó jog megállapítása.⁹¹ Ezt tovább bonyolítja a globalizáció és a technikai fejlődés, mivel megállapítható, hogy az Internet korában gyakorlatilag jelentőségét veszítette az adatkezelés tényleges helye, mivel az gyakran meg sem állapítható. A Bizottság a jelzett problémák megoldására a kölcsönös elismerés elvének bevezetését, továbbá nemzetközi adatkezelők egyetlen tagállam adatvédelmi jogának történő alávetését javasolja, azonban ez sem akadályozhatná az adatalanyokat a saját joguk alapján megillető jogosultságok igénybevételeiben.

A Bizottság az adatkezelők felelősségnek megerősítését a felelősség elvének bevezetésével, magánélet-barát technológiák,⁹² továbbá a beépített adatvédelem⁹³ megkövetelésével valósítaná meg. Fontos szerep jutna az öntanúsítási rendszereknek, illetve az önszabályozásnak, ami hozzájárul az adatvédelmi szabályok hatékonyabb érvényesítéséhez.

7.1.3. Az adatvédelem nemzetközi dimenziójának erősítése

⁹¹ Az Infotv. az adatkezelés helyét, míg az Irányelv 4. cikke az adatkezelő letelepedésének helyét veszi alapul a hatály megalapozásának vonatkozásában.

⁹² Privacy Enhancing Technologies

⁹³ Lásd bővebben: 7.2.2. pont.

A nemzetközi adattovábbítással kapcsolatos szabályok azért jelentősek, mert a „megfelelő szintű védelem” megléte esetén gyakorlatilag megnyitja a lehetőséget a személyes adatok szabad forgalma előtt. A probléma a védelem elismerésével kapcsolatos, ugyanis ennek kritériumai nincsenek pontosan rögzítve. Így a Bizottság mellett a tagállamok is jogosultsággal rendelkeznek ennek megítélésében, ami tagállamonként eltérő gyakorlatot is jelenthet. Kiemelt fontosságú, hogy nemzetközi szinten fennmaradjon az Európai Unió vezető szerepe a személyes adatok védelmének nemzetközi biztosításában.⁹⁴

7.2. Az egyes elvekről

A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet) szóló adatvédelmi csomag javaslatában szereplő egyes új elvek, iránymutatások említést érdemelnek a Google adatkezelési magatartása kapcsán felmerülő bizonytalanságok miatt.

7.2.1. A személyes adatok tárolásának megszüntetéséhez és a törléshez való jog

A 17. cikk alapján „az érintett kérheti az adatkezelőtől a rá vonatkozó személyes adatok törlését, valamint az ilyen adatok további terjesztésétől való tartózkodást, különösen az érintett által gyermekkorában elérhetővé tett személyes adatok vonatkozásában, ha: az adatokra már nincs szükség az adatgyűjtés vagy más módon történő feldolgozás céljából; vagy az érintett visszavonta a feldolgozás alapját képező hozzájárulását, vagy lejárt az engedélyezett adattárolási időtartam, vagy a személyes adatok feldolgozásának nincs más jogalapja; vagy az érintett kifogásolja a személyes adatok feldolgozását; vagy az adatfeldolgozás egyéb okokból nem áll összhangban e rendelettel”.

Adatok nyilvánosságra hozatala esetén az adatkezelőnek értesítenie kell a harmadik fél adatfeldolgozót, hogy az érintett kérte a személyes adat törlését.⁹⁵ A 29-es Munkacsoport is egyetért a tervezettel, mert ez erősítené a felhasználók saját adataik felett gyakorolt jogait.⁹⁶ Törlés helyett azonban bizonyos feltételek fennállása esetén a feldolgozás korlátozása is

⁹⁴ <http://www.dataprivacy.hu/archives/286> (2012.10.20.)

⁹⁵ 17. cikk (2) bekezdés: Amennyiben az (1) bekezdés szerinti adatkezelő nyilvánosságra hozza a személyes adatokat, a technikai intézkedéseket is beleértve megtesz minden ésszerű lépést, hogy – azon adatok vonatkozásában, amelyek nyilvánosságra hozatala az adatkezelő felelősségi körébe tartozik – értesítse az ilyen adatokat feldolgozó harmadik felet arról, hogy az érintett kérte a személyes adat bármely nyilvános internetes linkjének, másolatának vagy másodpéldányának törlését. Amennyiben az adatkezelő harmadik felet hatalmazott fel a személyes adatok nyilvánosságra hozatalára, az adatkezelő felelősséggel tartozik e nyilvánosságra hozatalért.

⁹⁶ A 29-es Adatvédelmi Munkacsoport 1/2012-es véleménye az adatvédelmi reform javaslatról

elégseges. Ennek kontrollálása érdekében a 17. cikk (7) bekezdése⁹⁷ speciális mechanizmusok alkalmazását írja elő.

7.2.2. Beépített és alapértelmezett adatvédelem

A 23. cikk szerint „az adatkezelő – a technika állására és végrehajtás költségeire tekintettel – mind az adatfeldolgozás módjának meghatározása, mind a feldolgozás során megfelelő technikai és szervezési intézkedéseket hajt végre oly módon, hogy az adatfeldolgozás megfeleljen e rendelet követelményeinek, és biztosítsa az érintettek jogainak védelmét”.

Ezt az előírást a (2) bekezdésben tovább differenciálja azzal, hogy a feldolgozás során kizárólag a konkrét célhoz szükséges adatok kerüljenek feldolgozásra, és a minimálisan szükséges időtartamot se lépje túl. Erre a bizottság egységes technikai előírásokat állapíthat meg.⁹⁸

7.2.3. Az érintett értesítése a személyes adatok megsértéséről

A 32. cikk (1) bekezdése tartalmaz előírást arra az esetre, ha „a személyes adatok megsértése várhatóan hátrányosan érinti az érintett személyes adatainak vagy magánéletének védelmét.” Ilyenkor „az adatkezelő a 31. cikk⁹⁹ szerinti értesítést követően indokolatlan késedelem nélkül tájékoztatja az érintettet a személyes adatok megsértéséről”. A tájékoztatásnak tartalmaznia kell a személyes adat megsértésének jellegéről szóló ismertetést, valamint egyéb javaslatokat.

7.2.4. Adatvédelmi hatásvizsgálat

„Amennyiben az adatfeldolgozási műveletek jellegük, alkalmazási területük vagy céljaik tekintetében különleges kockázatot jelentenek az érintettek jogaira és szabadságaira nézve, az adatkezelő vagy az adatkezelő nevében eljáró adatfeldolgozó elvégzi e tervezett adatfeldolgozási műveletek személyes adatok védelme tekintetében várható hatásának vizsgálatát”.¹⁰⁰

⁹⁷ Az adatkezelő olyan mechanizmusokat vezet be, amelyek biztosítják a személyes adatok törlésére és/vagy az adattárolás szükségességének időszakos felülvizsgálatára meghatározott határidő tiszteletben tartását.

⁹⁸ 23. cikk (4) bekezdés: A Bizottság az (1) és (2) bekezdésben rögzített követelményekre vonatkozó egységes technikai előírásokat állapíthat meg. E végrehajtási jogi aktusokat a 87. cikk (2) bekezdése szerinti vizsgálóbizottsági eljárással összhangban kell elfogadni.

⁹⁹ 31. cikk (1) bekezdés: Az adatkezelő a személyes adatok megsértése esetén indokolatlan késedelem nélkül, amennyiben lehetséges a személyes adatok megsértéséről való tudomásszerzéstől számított 24 órán belül értesíti a felügyelő hatóságot a személyes adatok megsértéséről. A felügyelő hatóság értesítését írásbeli indokolással kell ellátni, amennyiben arra nem 24 órán belül került sor.

¹⁰⁰ 33. cikk (1) bekezdés

A javaslat különleges kockázatként értékeli olyan feldolgozási műveleteket, mint például „a természetes személyre vonatkozó egyes személyes szempontok olyan módszeres és átfogó értékelése vagy különösen a természetes személy gazdasági helyzetének, tartózkodási helyének, egészségének, személyes igényeinek, megbízhatóságának vagy viselkedésének olyan elemzése vagy előrejelzése, amelyre automatizált feldolgozáson alapul, és amelyre az érintett személy tekintetében joghatással bíró vagy az egyént jelentős mértékben érintő intézkedések épülnek”. Hasonló kockázatot jelent a nyilvánosság számára hozzáférhető területek nyomon követése, különösen optikai-elektronikus eszközök nagyarányú alkalmazásával (videomegfigyelés).¹⁰¹

7.2.5. Az adatkezelő felelőssége

A 22. cikk (1) bekezdésével összhangban „az adatkezelő elfogadja azokat a politikákat és végrehajtja azokat a megfelelő intézkedéseket, amelyekkel biztosítja és igazolni tudja azt, hogy a személyes adatok feldolgozása e rendelettel összhangban történik”. A végrehajtandó intézkedések közé tartozik a dokumentáció vezetése, az adatvédelmi követelmények érvényesítése, az adatvédelmi hatásvizsgálat lefolytatása, a felügyelő hatóság előzetes engedélyezéséhez vagy előzetes konzultációhoz szükséges feltételek teljesítése, illetve az adatvédelmi tisztviselő kijelölése.

8. Következtetések

8.1. A lehetséges jövő

A Bizottság az Irányelvbe foglalt alapelvek fenntartásának és az alapjogok megfelelő érvényesítésének szükségességének elismerése mellett nem új Irányelvet kíván elfogadni, hanem a kor követelményeihez kívánja igazítani annak rendelkezéseit, hangsúlyozva azt, hogy az Irányelv technológia semleges megközelítését fenn kell tartani. Ez azonban a jelenlegi viszonyokhoz képest egy rendkívül szigorú szabályozást igényel, mivel a jogszabályalkotás sebessége nem képes felvenni a versenyt a technikai fejlődéssel. A lobbicsoportok várhatóan elérik céljukat, és enyhülni fog a tervezet, a fő kérdés azonban hogy milyen mértékben. Az adatkezelésről szóló rendelkezések kapcsán a Google is érintett és egyben érdekelt is a minél enyhébb szabályozás megszületésében, de nem csak az új adatvédelmi csomag jelent adatkezelési politikájára fenyegetést.

¹⁰¹ 33. cikk (2) c) pont

8.2. Védelmi eszközök

Jelenleg a felhasználók által alkalmazható védelmi eszköz a Do Not Track funkció bekapcsolása, ez azonban Balatoni Emese¹⁰² szerint nem érdeke a felhasználók jelentős részének, emiatt nem is számítanak a rendszerből történő tömeges kilépésre. A funkció bekapcsolásával a felhasználó véletlenszerű hirdetésekkel fog találkozni és semmilyen, korábbi viselkedéssel kapcsolatos egyedi tartalmat nem fog látni. Ez azt is jelenti, hogy a felhasználó gyakrabban kerül szembe zavaró, számára valószínűleg nem releváns reklámokkal, illetve a rendszer nem tartja számon a szokásait, a célzhatóság pedig erősen szűkül. Ettől függetlenül is integrálni kell a DNT-t, az érzékenyebb felhasználóknak ugyanis meg kell felelni.¹⁰³

Ugyanakkor ezeknek a felhasználóknak sem egyszerű eltűnni a Google mindent látó szemei elől. Egy nem regisztrált felhasználónak négy különböző opt-out eljárást kell teljesítenie, hogy ne kövessék többet – keresés, webhasználat, harmadik személy általi reklámok, illetve mobiltelefon mellőzése. Egy Google+ fiókkal rendelkezőnek ugyanez a cél hat eljárásból érhető el – az előzőek kiegészülve a böngészés előzményeinek törlésével, illetve a közösségi hálóról való kilépéssel. Fontos megjegyezni, hogy a Do Not Track teljes körű bekapcsolása nem jelenti a már megszerzett adatok azonnali törlését. A személyre szabott reklámok nem jelennek meg többé, de a cookie-k továbbra is gyűjtik az azonosításhoz szükséges adatokat.¹⁰⁴

8.3. A munkacsoport ajánlása

A 29-es munkacsoport vizsgálata – ideiglenes - zárásaként megfogalmazta kétélyeit az adatkezelés jogszerűségében. Szerintük „*a személyes adatok ilyen nagyfokú kombinációja nagy kockázatnak teszi ki a felhasználók magánszféráját, ezért a Google-nek módosítania kellene a gyakorlatát, amikor ilyen célból összegzi a felhasználói adatokat.*” A Google-nek intézett levelet az uniós adatvédelmi hatóságok mellett többek között Liechtenstein, Horvátország, valamint Kanada, és több ázsiai ország is aláírta.¹⁰⁵

A kutatás rámutatott többek között arra, hogy a Google nem ad megfelelő tájékoztatást a felhasználóinak, különösen az adatkezelések tárgyában. Ennek eredményeként a felhasználó képtelen megállapítani, hogy mely típusú adatait kezeli az általa használt alkalmazás, és

¹⁰² Az Adverticum ügyfélkapcsolati igazgatója

¹⁰³ <http://www.hwsz.hu/hirek/47215/do-not-track-adverticum-google-facebook-mozilla-firefox-web-reklam.html> (2012.08.22.)

¹⁰⁴ Google Privacy Policy Legal Analysis (2012.09.18.)

¹⁰⁵ <http://www.hwsz.hu/hirek/49209/google-adatvedelmi-privacy-europai-unio-jog.html> (2012.10.16.)

milyen célból. Az internetes cégeknek nem lenne szabad olyan adatvédelmi felszólításokat alkalmazniuk, melyek túl komplexek, jogi szaknyelvet használnak, vagy túl hosszúak. Az egyszerűsítés azonban nem vezethet oda, hogy a cégek megfedkezzenek kötelezettségeikről.

A különböző szolgáltatások által gyűjtött adatok együttes kezelése is aggályosnak minősül. Az új Irányelv megengedi a Google-nek, hogy minden adatot együttesen kezeljen, céltól függetlenül. Ehhez jogszabályi alap szükséges, és az adatgyűjtésnek az adatkezelés céljával meg kell egyeznie. Ezzel szemben a Google nem szerzi meg a felhasználó egyértelmű beleegyezését, a hatalmas adatbázisok fenntartásához fűződő érdekei semmibe veszik az alapjogokat és alapszabadságokat. Az adatgyűjtés megtörténik, azonban nem bizonyítja semmi, hogy az összegyűjtött adatok arányosak az adatkezelés céljával. Ebből kifolyólag szükséges a Google adatkezelési gyakorlatának megváltoztatása. Ezen túlmenően a Google az adatmegőrzési időszakok pontos meghatározására is képtelen volt.

A Munkacsoport ajánlásokat fogalmazott meg, amelyek legalább átmeneti megoldást nyújtanának a kifogásolt problémakörökre: háromszintű adatvédelmi tájékoztatási rendszer, melynek részei a tájékoztatás működésének bemutatása, az aktuális adatvédelmi szabályzat, illetve a termék specifikus szabályozások. E mellett interaktív prezentációkra van szükség, amelyek érthetően mutatják az adatvédelmi szabályozást a felhasználónak. A különös biztonságot igénylő adatokra történő figyelemfelhívás (tartózkodási hely, bankkártyaszám, telefonszám, stb.), valamint a passzív felhasználók tájékoztatása is elengedhetetlen követelmény a teljes tájékoztatás megvalósulása érdekében.

Az együttesen kezelt adatok céljainak és megvalósulásának tisztázása érdekében is ad tanácsokat a Munkacsoport, így az opt-out mechanizmusok egyszerűsítése azonosított, és nem azonosított felhasználók számára egyaránt; az együttes adatkezelés céljainak elkülönítése megfelelő eszközök segítségével; felhasználók általi kifejezett beleegyezés megszerzése; azonosított felhasználók számára lehetőség felajánlása, hogy mely szolgáltatásban legyenek bejelentkezve; passzív felhasználók esetén az együttes adatkezelés mértékének maximalizálása; az e-Privacy Irányelv 5. cikk (3) bekezdésének implementálása, valamint a német Google Analytics használatának minden országra történő kiterjesztése.

A munkacsoportnak nem célja a Google innovációs tevékenységének és kutatásainak korlátozása, viszont szükségesnek látja biztosítani a felhasználók információszabadsághoz kapcsolódó alkotmányos jogait.¹⁰⁶

A vállalat rövid közleményben hozta nyilvánosságra a levéllel kapcsolatos álláspontját. „Megkaptuk a jelentést és jelenleg is tanulmányozzuk. Az új adatvédelmi szabályzatunk annak az elkötelezettségnek a bizonyítéka, hogy megvédjük a felhasználóink adatait és nagyszerű termékeket hozunk létre. Biztosak vagyunk benne, hogy az adatvédelmi értesítéseink megfelelnek az uniós jogszabályoknak.”

Vagyis a Google nem ért egyet a munkacsoport állításaival, és ezzel lezártnak tekinti az irányelve körülötte vitát. Változatlan állapot mellett lehetséges következmény az egyes országok hatóságainak jogi eljárás indítása a változtatás kikényszerítésére.¹⁰⁷ Addig azonban még történhetnek technikai és jogszabályi változtatások, pontosabban jelenleg is zajlik a fejlesztés, illetve a felülvizsgálat.

8.4. Társadalmi háttér

Ahogy a bevezetőben említésre került, az IE 10 alapbeállításai segítenek a felhasználónak a bekapcsolt DNT funkcióval. A Google már meg is tette válaszlépését „Get your Google back” nevű kampányával. Ez visszaállítja a Google-t, mint alapértelmezett keresőt,¹⁰⁸ illetve a Chrome-ot, mint alapértelmezett böngészőt.¹⁰⁹ Ezzel megkerülve az Internet Explorert és a DNT-t továbbra is gyűjtheti a felhasználók adatait. Az azonnali válaszlépéstől eltekintve a Microsoft ezzel a döntésével a jogvédő szervezetek előtt kíván jó fényben feltűnni, a valóság azonban ennél árnyaltabb képet mutat.

A Windows 8 operációs rendszerbe új funkció került SmartScreen néven, amely alapértelmezettként be van kapcsolva. A funkció célja az összes program megfigyelése, amit a felhasználó az internetről telepíteni kíván, hogy értesíthessen, hogy biztonságos-e a program, vagy sem. Az eljárás gyakorlati megvalósulása a következő: a program internetről történő letöltése, és az installációs eljárás után a SmartScreen információt gyűjt a programról azonosítás céljából, majd az adatokat elküldi a Microsoft redmondi központjába. A központ ezután visszajelez, hogy a program rendelkezik-e a megfelelő tanúsítvánnyal.

¹⁰⁶ http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf (2012.10.28.)

¹⁰⁷ <http://www.hwsz.hu/hirek/49209/google-adatvedelmi-privacy-europai-unio-jog.html> (2012.10.16.)

¹⁰⁸ A Microsoft Bing nevű keresőmotorja helyett.

¹⁰⁹ <http://www.hwsz.hu/hirek/49259/google-search-app-chrome-windows-8.html> (2012.10.27.)

Ez az eljárás felvet néhány adatvédelmi kérdést. A Windows 8 úgy van beállítva, hogy azonnal adatokat küldjön a Microsoftnak program telepítés esetén. Ezáltal a Microsoft központi adatkezelővé és feldolgozóvá válik, amelynek következtében a nemzetbiztonsági szervek segítséget kérhetnek tőle. Még nagyobb aggodalomra adhat okot az a tény, hogy a SmartScreen és Microsoft közti kommunikációt hackerek is figyelhetik.¹¹⁰

2012. augusztus 27-én a VentureBeat-nek¹¹¹ adott nyilatkozatában a Microsoft szóvivője tagadta a vádakát – „*Megegyeztetjük, hogy nem készítünk adatbázist a használt programokról és a felhasználó IP-címéről. Mint minden online szolgáltatásban, az IP-címek fontosak a kapcsolat létrehozása szempontjából, de periodikusan töröljük ezeket az adatokat.*” Azt is kijelentették, hogy nem gyűjtenek adatokat targetált hirdetésekhez, illetve nem osztják meg azokat más cégekkel.¹¹²

A válaszban egy kételkedésre okot adó részlet van, mégpedig a „periodikus” kifejezés. Az adatok törlése ez alapján megtörténhet naponta, hetente, vagy akár évente. Ezek után csak bízni lehet abban, hogy a Microsoft igazat mond, és amit az egyik szolgáltatásával megad a felhasználónak, vagyis a személyhez fűződő adatai teljes védelmét, azt nem veszi el egy másikkal.

Az egyértelműnek tűnik, hogy a szabályozások alapján minimum megkérdőjelezhető a Google adatkezelő tevékenységének jogszerűsége, nem szabad azonban elfelejteni, hogy az Unió aggályai, valamint a személyek aggodalmai abban az értelemben alaptalanok, hogy még nem történt, vagy csupán nem került nyilvánosságra olyan jogsértés, amelyben a Google a saját, illetve a tagállami adatvédelmi szabályozásokat megsértette volna. A jövőre tekintve igény van az adatkezelők fokozottabb ellenőrzésére, mert a személyekről egyre több adatot kell kezelni, és ezek az adatok előbb-utóbb egyazon adatkezelő szervnél egyesülnek. Aki ennek lehetséges következményeitől tart, annak már évek óta lehetősége van a böngészője biztonságának fokozására. A jog nem küzdhet a végsőkéig olyan eszmékért, amelynek nincs, vagy elenyésző a társadalmi támogatottsága.

A társadalom jelentős része úgy tekint az adatvédelemre, mint egy feleslegre. Az adatkezelő cégek számviteli adminisztrációs kötelezettségként fogják fel, az emberek pedig egyáltalán

¹¹⁰ <http://log.nadim.cc/?p=78> (2012.08.26.)

¹¹¹ Innovációs technológiákkal foglalkozó, a New York Times által is elismert világhírű blog.

¹¹² <http://venturebeat.com/2012/08/27/microsoft-we-dont-harvest-windows-8-smartscreen-user-data/> (2012.10.10.)

nem foglalkoznak vele. Sokak szerint az adatvédelem csak a bűnözőket védi, az adatvédelem miatt nem lehet kamerarendszereket telepíteni, az adatvédelem miatt nem lehet a csaló munkavállalót lenyomozni.

Az emberek úgy szocializálódtak, hogy a magánlakásukba nem engednek be bárkit. Ha csöngetnek, megnézik, megkérdezik, kihez van szerencsájük, a látogató mit szeretne, és az információk birtokában meghozzák a döntést, beengedik-e a magánszférájukba vagy sem. Különös módon ez nem ilyen természetes, ha a személyes adatokról van szó, pedig ott is ez lenne az eljárás.

„Miért ne adnám meg az adataimat? Nincs semmi titkolnivalóm, semmi károm nem származhat belőle.” – mondhatja a szkeptikus. Ha nincs titkolnivalója, vajon beenged egy vadidegen embert a lakásba, hogy megnézzze este a kedvenc tv-sorozatát mellette helyet foglalva? Nem kér enni, sem inni, nem is beszélne, csak leülne a kanapéra, kárt nem okozva.

Amíg nem sikerül felismerni, hogy a személyes adat kezelése önmagában egy ember magánszférájába való behatolás, mely az érintettet – még ha nem is tudja – zavarja, addig szinte teljesen felesleges is konkrét jogszabályi rendelkezések betartásán fáradozni.¹¹³

¹¹³ <http://www.adatvedelmiszakerto.hu/2012/10/nincs-semmi-titkolnivalom-miert-is-fontos-az-adatvedelem/>
(2012.10.28.)

Felhasznált Irodalom

1. Dr. Jóri András: Adatvédelem és információszabadság a gyakorlatban - Complex Kiadó, Budapest 2010
2. Majtényi László: az információs szabadságok – adatvédelem és a közérdekű adatok nyilvánossága – Complex Kiadó, Budapest 2006
3. Gutwirth, Poullet, Hert: Data Protection in a Profiled World – Springer, UK 2011
4. Karen Lawrence Öqvist: Virtual Shadows – Your Privacy in the Information Society - The British Computer Society, Swindon UK 2009
5. David A. Vise & Mark Malseed, Inside the hottest business, media and technology success of our time: The Google story p117-118. 2005
6. Alex W. Cannon: Regulating AdWords - Consumer Protection in a Market Where the Commodity is Speech (In Seton Hall Law Review, Vol 39. (2009), p291-334.)
7. Amy Tracy: Technology law – Great Google-y Moogley: The effect and enforcement of click fraud and online advertising (In University of Arkansas at Little Rock Law Review, Vol. 32, (2010), p347-374)
8. A. J. Grey: Lost in Translation: Repairing Rosetta Stone v. Google's Indecipherable Functionality Holding (In Washington and Lee Law Review, Vol. 68, (2011), p1505-1554)
9. Lendvai Zsófia: A Google AdWords szolgáltatása az Európai Bíróság előtt (<http://www.sztnh.gov.hu/kiadv/ipsz/201008-pdf/02.pdf> 2012.09.25.)
10. Google Privacy Policy Legal Analysis (2012.09.18.)
11. <http://support.google.com/adwords/bin/answer.py?hl=hu&answer=1704410&topic=1713894&path=1710534&ctx=leftnav> (2012.10.15.)
12. <http://googleblog.blogspot.hu/2012/03/making-our-ads-better-for-everyone.html> (2012.10.20.)
13. <http://www.google.com/intl/en/privacy/ads/> (2012.10.18.)
14. <http://support.google.com/websearch/bin/answer.py?hl=hu&hlrm=fr&answer=1734130> (2012.10.20.)
15. <https://support.google.com/mail/bin/answer.py?hl=en&topic=1668949&hlrm=fr&ctx=topic&answer=6603> (2012.10.05.)
16. <http://investor.google.com/corporate/code-of-conduct.html> (2012.11.03.)
17. <http://www.google.com/policies/> (2012.10.15.)
18. <http://www.google.com/intl/hu/policies/privacy/> (2012.10.08.)

19. <http://www.google.com/about/jobs/locations/dublin/> (2012.10.12.)
20. <http://www.google.hu/about/company/> (2012.10.15.)
21. http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (2012.10.03.)
22. <http://adwords-hu.blogspot.hu/> (2012.09.20.)
23. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120202_letter_google_privacy_policy_en.pdf (2012.10.04.)
24. <http://www.out-law.com/en/articles/2012/october/future-of-eu-regulation-of-data-protection-previewed-in-google-privacy-policy-investigation-says-expert/> (2012.10.22.)
25. http://hirek.prim.hu/cikk/2012/08/22/szeretted-_ha_mindent_tudnak_rolad_-_utelagazas_elott_az_online_reklam (2012.10.10.)
26. Web tracking Privacy and data protection issues and recommendations
27. Working Paper on Cloud Computing - Privacy and data protection issues
28. <http://www.mb-partners.eu/cegerteklevel/258> (2012.10.19.)
29. <http://www.kantarworldpanel.com/Global/News/Android-maintains-Euro-dominance> (2012.10.20.)
30. <http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&clearaf=1&qpaf=-000%09100%091%0D&qpcustomd> (2012.10.20.)
31. <http://techcrunch.com/2010/09/14/google-engineer-spying-fired/> (2012.09.28.)
32. http://www.telefonguru.hu/hir/Bemutatjuk_a_Google_Now-t_2012-8-1 (2012.09.28.)
33. <http://www.facebook.com/about/privacy/> (2012.10.23.)
34. <http://www.ceps.be/> (2012.10.15.)
35. <http://computerworld.hu/kroes-elesen-tamadja-a-do-not-track-felvizezeset-20121012.html> (2012.10.12.)
36. http://www.huntonfiles.com/files/webupload/CIPL_Safe_Harbor_3.08.pdf (2012.10.20.)
37. https://www.datenschutzzentrum.de/presse/20100723-safe-harbor_en.htm (2012.10.20.)
38. <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Dataprotection/Legislation> (2012.10.25.)
39. http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf (2012.10.28.)

40. <http://log.nadim.cc/?p=78> (2012.08.26.)
41. <http://venturebeat.com/2012/08/27/microsoft-we-dont-harvest-windows-8-smartscreen-user-data/> (2012.10.10.)
42. http://dharma.blog.hu/2010/02/18/ertett_ertelem (2012.10.20.)
43. <http://www.adatvedelmiszakerto.hu/2012/10/nincs-semmi-titkolnivalom-miert-is-fontos-az-adatvedelem/> (2012.10.28.)
44. <http://www.hwsz.hu/hirek/48860> (2012.09.30.)
45. <http://www.hwsz.hu/hirek/49259/google-search-app-chrome-windows-8.html> (2012.10.27.)
46. <http://www.hwsz.hu/hirek/49209/google-adatvedelmi-privacy-europai-unio-jog.html> (2012.10.16.)
47. <http://www.hwsz.hu/hirek/47215/do-not-track-adverticum-google-facebook-mozilla-firefox-web-reklam.html> (2012.08.22.)
48. <http://www.hwsz.hu/hirek/48535/europai-bizottsag-cookie-web-jog-maganszfera-privacy.html> (2012.10.25.)
49. <http://www.hwsz.hu/hirek/48535/europai-bizottsag-cookie-web-jog-maganszfera-privacy.html> (2012.09.20.)
50. <http://www.hwsz.hu/hirek/49209/google-adatvedelmi-privacy-europai-unio-jog.html> (2012.10.16.)
51. <http://www.hwsz.hu/hirek/47215/do-not-track-adverticum-google-facebook-mozilla-firefox-web-reklam.html> (2012.10.12.)
52. <http://www.dataprivacy.hu/archives/1086#more-1086> (2012.10.28.)
53. <http://www.dataprivacy.hu/archives/133#more-133> (2012.10.20.)
54. <http://www.dataprivacy.hu/archives/286> (2012.10.20.)
55. <http://www.dataprivacy.hu/archives/1086#more-1086> (2012.10.22.)

Felhasznált joganyagok

1. 95/46/EK Irányelv az egyének védelméről és az ilyen adatok szabad áramlásáról
2. 2002/58/EK Irányelv az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről
3. 2009/136/EK Irányelv
4. A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről
5. Az új általános adatvédelmi rendelet javaslata COM(2012) 11 final – Brüsszel, 2012.01.25.
6. Google Privacy Policy Legal Analysis (2012.09.18.)
7. 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
8. 2003. évi C törvény az elektronikus hírközlésről
9. 2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól
10. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
11. A 29-es Munkacsoport 4/2007 számú véleménye a személyes adat fogalmáról, valamint a keresőmotorokkal kapcsolatos adatvédelmi kérdésekről
12. A 29-es Munkacsoport 1/2009 véleménye a magánélet védelméről és az elektronikus hírközlési ágazatról szóló 2002/58/EK Irányelvet módosító javaslatokról
13. A 29-es Munkacsoport 2/2010. számú véleménye a viselkedésalapú online reklámról
14. A 29-es Munkacsoport 1/2012-es véleménye az adatvédelmi reform javaslatáról
15. A 29-es Munkacsoport sütik alkalmazásával kapcsolatos hozzájárulás alóli kivételekről szóló 4/2012-es állásfoglalása