Jelentés az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény hiányosságairól

I. rész

Strasbourg, 3 November 2010, november 3. T-PD-BUR(2010)09 (II) FINAL

Az adatvédelmi egyezmény Tanácsadó bizottságának Irodája (T-PD-BUR)
22. értekezlet
2010. november 15-17.

Szerzők:
Cécile de Terwangne, Professeur à la Faculté de Droit de l'Université de Namur,
Directrice de recherche au CRID
Jean-Philippe Moiny, aspirant du F.R.S.-FNRS
Chercheur au CRID
Avec la collaboration de :
Yves Poullet, Recteur de l'Université de Namur (FUNDP), Professeur à la Faculté de droit,
Directeur de recherche au CRID
Jean-Marc Van Gyzeghem, Senior Researcher au CRID

Nem hivatalos fordítás.

Tartalomjegyzék

1. Új távközlési mikrohálózatok

Századunk első évtizedében folyamatosan és egyre gyorsabban terjednek az új távközlési hálózatok, miközben az Internet növekedése a sebesség, a mobilitás és elérhetőség tekintetében ugyancsak tartós, legalábbis a fejlett országokban.
A különféle, kis hatótávolságú (néhány centimétertől néhány méterig) hálózatok, vagyis a mikrohálózatok, mindenek előtt a Wifi, az RFID és a BlueTooth, a közelmúltban jelentek meg, anélkül, hogy különösebb gondot fordítottak volna használóik adatainak és magánéletének védelmére.
A Wifi interfészek manapság rendszerint telepítve vannak a hordozható számítógépekben és egyre inkább a mobil telefonokban is. A gyakorlatban a „laptop" és a mobiltelefon konvergál egymáshoz. A laptoppal telefonálni is lehet (VoIP, pl. Skype), a mobil telefon pedig nemcsak telefonálásra használható, azzal az Interneten szörfölni, levelezni vagy közösségi hálózatokhoz hozzáférni is lehet. Ezek a hálózatok napjainkban különös veszélyt jelentenek, mert nem fordítanak kellő figyelmet a felhasználó nyomon követhetőségére vagy még inkább az ilyen távközlési hálózatokra csatlakozók emberi mivoltára. Ezeket a kockázatokat az alábbiakban foglaljuk össze.
- Az ellenőrzés megszűnése: a mikrohálózatokhoz nincs szükség vezetékes kapcsolatra, ami kikapcsolásukat problematikussá teszi, működésük még a tudatos felhasználó számára is átláthatatlan. Ez a probléma különösen kínos az RFID csipek esetében, melyek tápegység nélkül működnek, méretük parányi (néhány milliméter), így jelenlétüket a felhasználó alig veheti észre. Minthogy ezeket a csipeket leginkább üzletekben alkalmazzák lopások kiküszöbölésére, az alkalmazónak természetesen nem érdeke, hogy láthatóvá tegye, hiszen úgy a potenciális tolvaj azt letéphetné vagy megrongálhatná.
- A kapcsolat bizalmas jellegének hiánya: a három említett hálózat nincs szisztematikusan titkosítva. A Wifi esetében harmadik fél viszonylag könnyedén bekapcsolódhat egy vezeték nélküli terminál és a Wifi bázisállomás (hotspot) között folyó forgalomba, s megismerheti annak tartalmát.
- A nyomon követés lehetősége: még ha a kommunikáció titkosítva is van, a Wifi hotspot, az RFID csip vagy a mobil BlueTooth sztatikus elektronikus sorozatszáma rendszerint egyértelműen kiolvasható. Ezek az eszközök szerver típusúak, vagyis technikailag automatikus választ adnak a kapcsolat igényére, még ha az visszaélésszerű és tényleges következménye nincs is, kommunikálva globális egyedi azonosítójukat (GUID). Általában tehát technikailag lehetséges kiolvasni egy BlueTooth szériaszámot, egy WiFi kártya MAC (Medium Access Control) címét vagy egy RFID csip szériaszámát, még a kommunikációba való tényleges beavatkozás nélkül is.

Következtetés: ezek az új, széles körben elterjedt és a jövőben exponenciálisan növekvő számú hálózatok lehetővé teszik, hogy felhasználójuk tudta nélkül minden olyan terminált nyomon kövessenek, amelyre Wifi, RFID vagy BlueTooth interfészt telepítettek, még akkor is, ha a terminált szándékosan nem is aktiválták.

2. A térbeli helymeghatározás robbanásszerű elterjedése

Egy vezeték nélküli terminál azonosítója megszerezhető egy térbeli helymeghatározásra alkalmas számítógép, tipikusan egy GPS[1] rendszer által. Mivel ezek az új mikrohálózatok maguk is mind inkább az Internetre kapcsolódó terminálok, az Ipv4 dinamikus cím, amely véletlenszerűen és rendszeresen megújul, nem nyújt hatékony védelmet a távközlési hálózat igénybevevője részére a nyomkövetéssel szemben, s a használt mikrohálózat azonosítója vagy egyedi címkéje megszerezhető. Ezeknek a világhálóra kapcsolódó mikrohálózatoknak az elterjedése csendben és megkerülhetetlenül az egyén tartózkodási helyének meghatározásához vezet.
A térbeli helymeghatározás veszélyeit globálisan is elemezni kell. Többről van ugyanis szó, mint arról, hol tartózkodik adott pillanatban az egyén.
- Ha ezt a rendszert a fontos egyénekre alkalmazzuk, tudomást szerezhetünk arról, hogy kivel tartózkodik az adott helyen, és feltérképezhetjük családi, hivatásbeli vagy baráti kapcsolatait is.
- Számos helyszínnek különös jelentősége van, melynek ismerete átlépi az egyszerű információ határait. Egy városi főutca 25. sz. háza nem nagyon érdekes, kivéve, ha egy mecset, pszichiátriai klinika, helyi szakszervezet, rendőrség vagy bíróság címe.
- Az egyén mozgáspályája tevékenységének jellemzője. Annak ismeretében tudomást szerezhetünk arról, hogy megállt egy kirakat előtt vagy éppen kocog. Egy nagy árúházban az egyén mozgáspályája vásárlási szokásaira utal.
Ez a térbeli helymeghatározás ezen felül az online felhasználó viselkedésének – korábban már elemzett[2] – rendszeres megfigyelésével párosulhat. A két rendszer párosítását (online profil és térbeli helymeghatározás) technikailag megkönnyíti a térbeli helymeghatározó mikrohálózatnak az Internethez kapcsolt terminállal való összekapcsolása.

3. A süti invázió avagy a nyomon követhetetlenség megszűnése

A sütiket (cookies) arra találták ki, hogy a világháló használóit nyomon követhessék, függetlenül IP címének megváltozásától vagy ugyanannak a címnek több felhasználó közötti megosztásától[3]. Erre a nyomon követésre szükség lehet az elektronikus online tranzakciók céljára, de technikailag csupán az alkalmi sütik (session cookies) szolgálják ezt a célt. Márpedig napjaink problémája a megmaradó sütik, vagy harmadik felek sütijei, és azoknak a harmadik feleknek a megmaradó sütijei, akik transzklúzív módon megfigyelik a forgalmat. E

[1] A GPS ártatlanul passzív: egy GPS csip több ezer kilométer távolságban keringő geostacionárius műholdak által kibocsátott jeleket vesz, és semmiféle jelet nem bocsát ki. A csip folyamatosan kiszámítja, mekkora távolságra van a műholdtól, melynek pozícióját ismeri, és (néhány méternyi pontossággal) háromszögelési módszerrel kiszámítja saját pozícióját. Az adatvédelem problémája nem aGPS-sel magával kapcsolatos, hanem a GPS chipet tartalmazó terminállal, amely a térbeli lokalizációs adatokat tárolja és továbbítja.
[2] Poullet, Yves & Dinant Jean-Marc **Report on the application of data protection principles to the worldwide telecommunication networks** *Information self-determination in the internet era* Rapport d'expertise à l'attention du Conseil de l'Europe, Strasbourg, 2004
http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/
[3] A NAT (Network Adress Translation) rendszer a hotspot Wifi-k és az ADSL routerek többségében megjelenik, és lehetővé teszi, hogy több különböző felhasználó egyidejűleg az Internetnek ugyanazt a címét használja.

tekintetben kétségtelenül a Google viszi el pálmát, amely a Google Analytics rendszerével gyűjti az Internet oldalak nagy többségének forgalmi – URL és tartalmi – adatait[4].
Mindemellett a böngésző – ugyan még kezdetleges – paraméterezése révén, a tudatos felhasználó blokkolhatja harmadik felek sütijeit. Hangsúlyozni kell, hogy a klasszikus böngészőkkel a transzkluzivitás nem blokkolható /vagyis a tartalom automatikus bekebelezése az Internet felhasználónak ismeretlen harmadik felek által (kontaktibilitás), valamint a forgalmi adatok továbbítása e harmadik felek oldalaira (megfigyelhetőség)/. Harmadik felek maradandó sütijeinek blokkolása csupán a nyomon követhetőség esetében hatásos. Két fontos esetet kell még megvizsgálnunk a nyomon követhetőség marginális ellenőrzése tekintetében.
Az első eset a tudatos felhasználónak az a lehetősége, hogy blokkolhatja a sütiket a WEB HTTP protokollja szintjén, amit a FLASH sütik megjelenése idézett elő. A Macromedia világszerte terjeszti a FLASH technikát plug-in formában, amelynek a böngészőkbe való telepítése általánosan elterjedt. Ez a plug-in sajátos felhasználásától függetlenül működő adatkezelő rendszer, akárcsak a sütik rendszere. Ebben az esetben a böngészővel eszközölt blokkolás totálisan működésképtelennek mutatkozik. A szakértő felhasználó a plug-in e szokatlan viselkedésére számos példát találhat, egy efféle plug-in ugyanis rendelkezik azzal a képességgel, hogy az adatokat kiolvassa és beírja a terminál tömegtárolójába. Mindemellett, mert a Flash sütiket kevéssé ismerik, és mert a blokkolás megtételéhez alapos technikai jártasság szükséges, az ilyen típusú blokkolást kevéssé használják.
A második eset a harmadik felek sütijeinek blokkolása a tudatos felhasználó által. A jelentős web helyek célzatosan törekszenek arra, hogy a mobil telefonok számára általában és különösen az Apple Iphone számára sajátos alkalmazásokat fejlesszenek ki. Miközben web helyüket klasszikus Firefox típusú böngészővel használják, sok vállalkozás (Amazon, FaceBook, Google, egyes újságok) saját alkalmazást fejleszt ki és terjeszt. Ezek az alkalmazások a HTTP protokollt használják, de a felhasználónak már nincs lehetősége arra, hogy blokkolja a sütiket, s még kevésbé a transzkluzivitást.
Ugyanide sorolható, hogy a MAC[5] cím szisztematikus befoglalása az Ipv6 címbe jelentősen és titkolva növeli a Web oldalakon böngészők nyomon követésének lehetőségét. Az IP cím megváltoztatása ellenére és az Ipv4 aktuális protokollal szemben minden Ipv6 cím tartalmazni fogja a számítógép hálózati kártyájának egyedi szériaszámát. Ez a kockázat jóval nagyobb, mint a harmadik felek megmaradó sütijei, melyet jelenleg nem eléggé vesznek figyelembe az adatvédelmi hatóságok. Az IPv6 protokollnak létezik egy olyan alternatívája, amely véletlenszerűen generál egy címet, s melyet már a W3C is elfogadott.

Általában tehát megállapíthatjuk, hogy erodálódnak azok a meglehetősen gyenge bástyák, melyek lehetővé teszik a tudatos felhasználónak az Internet hálózaton való nyomon követés elleni harcot.

4. A közösségi hálók

A múlt század végéig a levelezés és a csevegés (chat) volt a személyközi kommunikáció legnépszerűbb módja az Interneten, mára a korábbi blogok talaján kialakultak a közösségi hálók. Az innováció itt társadalmi jellegű: a blogok egy problematikára vagy egy sajátos tárgyra koncentrálódtak, a közösségi hálók pedig az egyénekre. E közösségi hálók hamarosan a személyes kapcsolatteremtés helyszínévé, az Interneten való ismerkedés eszközévé váltak.

[4] Egy Berkeley tanulmány 400 000 Webhelyet felölelő mintán végzett elemzésre alapozva kimutatta, hogy 2009 májusában 88%-uk használta a Google Analytics-et.
[5] Medium Access Control. Minden egyes periférikus Ethernet globálisan egyedi szériaszáma, pl. a kártyás és hotspot Wifi-ké, a hálózati kártyáké. A Bluetooth csipek gyakran annak az Ethernet kártyának a szériaszámát reprodukálják, amely e csipeket tartalmazó eszközökön található.

A fejlesztők hamarosan olyan speciális alkalmazásokat tettek lehetővé, melyek révén harmadik felek áttekinthetik a hálózatot és megtekinthetik a tárolt profilokat a felhasználók és a fejlesztők által definiált módon. Ezek a közösségi hálók rendszerint félrevezetően ingyenesek, hiszen használóik önmaguk közszemlére tételével fizetnek érte. A magánélet védelmének politikáját e hálózatokon rendszerint az üzemeltető szabja meg, aki megengedheti, hogy az érintett bizonyos mértékben meghatározza, a róla tárolt információból mennyit ismerhetnek meg harmadik felek.
A személyes adatok védelmét szolgáló jogszabályok a kezdetektől fogva bipoláris koncepcióra épültek: egyrészt a személyes adatokra, másrészt az „adatkezelő”-re vagy a „felelős kezelőre” koncentráltak. Ez a bipoláris felfogás mára túlságosan homályossá és korlátozottá látszik válni, s nem nyújt lehetőséget a magánélettel kapcsolatos hatékony jogszabályok megalkotására a technikájában és a gyakorlatában szüntelenül változó információs és kommunikációs társadalomban.

5. A személyes adat koncepciójának funkcionális megközelítése

Egy azonosított egyénnel kapcsolatos minden adat általában személyes jellegű: biográfiai vagy nyomkövető.
Az első esetben az egyénre vonatkozó adat bármi lehet, ami személyével kapcsolatos: pl. egy tény, egy cselekedet, egy mozgáspálya, egy vásárlás, mely ennek a személynek valamely tulajdonságát jellemzi, bár e tulajdonságon több egyén osztozik. Az a tény például, hogy valaki magyar vagy francia, valamennyi magyar vagy francia személyes adata. Etimológiai értelemben „biográfiai” adatról van szó, amely az egyén életének, pontosabban élete egy szeletének jellemzője. Itt tehát az egyén egy vagy több, adott kontextusban megjelenő tulajdonságának ismerete játszik szerepet.
A második esetben az egyénre vonatkozó adatok egyedi tulajdonságot vagy bizonyos változók egyedi értékét testesítik meg, melyek az egyént az adott népesség más egyéneitől valami módon megkülönböztetik. Így egy IP cím egy személyt egy adott pillanatban egyedi módon azonosít, az tehát egyedi azonosító (Unique Identifier)[6]. Ez az azonosító aligha problematikus, ha az egyént adott kontextusban azonosítja (bankszámla száma, kórházi, egyetemi hallgatói, állampolgári, munkavállalói azonosítója stb.). A gyakorlatban mindazonáltal ezek az azonosítók ritkán lokálisak, hamar globálissá, vagyis multikontextuálissá válnak. Következésképpen itt már globálisan egyedi azonosítókról (Global Unique Identifier) beszélhetünk. Az ilyen típusú azonosító lehetővé teszi ugyanannak a személynek a nyomon követését több, különböző kontextusban. Itt tehát ugyanannak az egyénnek a multikontextuális ismeretéről van szó.
Az adatok harmadik típusát a kapcsolati adatok képezik. Egy email cím, egy postacím, egy közösségi háló (üzenő) „falának” URL-je harmadik feleknek lehetővé teszi, hogy tartalmat küldjenek a kapcsolati adatukkal azonosított egyénnek. Így például egy email cím ismerete révén ugyanarra a személyre utaló WEB oldalakat azonosíthatunk. Az utóbbi típusú adatok lehetőséget adnak a kapcsolatteremtésre, vagy arra, hogy harmadik fél információtartalmat (éspedig marketing tartalmat) illesszen be egy postafiókba vagy egy képernyőre. Ebben a kontextusban természetesen marketingről van szó, pontosabban az egyén marketing tartalmakkal való befolyásolásáról.
Az adatok e funkcionális felosztása három típusú személyes adatot különböztet meg, melyek lényegbevágóan különbözőek. Még pontosabban a személyes adatok tulajdonságairól van szó.

[6] Ez általában igaz, feltéve, hogy a felhasználó nem használja a NAT rendszert. Egy NAT rendszer esetében, amely lehetővé teszi ugyanannak az IP címnek az egyidejű megosztását több személy (iskolatársak, családtagok, szálloda-vendégek stb.) között, az IP cím egy személycsoportot azonosít.

Egy email címből, pl. john.smith@coe.int, mindhárom típust felismerhetjük. Megtudjuk, email címét, továbbá nevét, s hogy az Európa Tanácsnál dolgozik. Egy böngészőbe írva címét egyéb kapcsolatairól is találhatunk információt, nem beszélve arról, hogy kapcsolatba is léphetünk vele, például marketing célból.
Régóta (túlságosan is?) hosszas viták folynak arról, személyes jelegű adatok-e az IP címek és a sütik. Hangsúlyozni kell, hogy e viták nyilvánvaló lényege a vállalkozásokon, különösen a multinacionális vállalkozásokon belüli téveszméknek tulajdonítható. Az EEJE 8. cikke nem az azonosított vagy azonosítható ember magánéletét védi. Minden személynek, még ha nem is azonosított vagy azonosítható, joga van erre a védelemre. A személyes adatok védelmének joga nem merül ki a magánélet védelmének jogával. Így például az emberek mindenütt jelenlévő kamerás megfigyelése köz- vagy magán területeken valójában beavatkozás a videón rögzített személy életébe, még ha arckifejezését elhomályosítva nem is azonosítható.
Másfelől, felfogásunk szerint, nincs olyan, az egyénre vonatkozó adat, amely őt nem azonosítja, legyen az bár nyomkövető, biográfiai, vagy nem teszi lehetővé, hogy vele kapcsolatba lépjünk.
Meg kell jegyezni, hogy e problémák némelyikét már tekintetbe vették egyes európai irányelvek, melyekkel megegyező megoldásokat az Európa Tanács kebelében nem ismerünk. Így például a 95/45/EK irányelv rendelkezik a tiltakozás jogáról a minden jogosultságot nélkülöző direkt marketinggel szembeni. A 2002/58/EK irányelv szabályozza az elektronikus küldemények gyakorlatát, s azt a kereskedelmi célra korlátozza, egyidejűleg előírva a hozzájárulás megszerzését vagy az érintett személy tiltakozási jogát. A 2006/24/EK irányelv teljes körűen meghatározza azokat a forgalmi adatokat, amelyeket – eltérően a 2002/58 irányelvtől – a szolgáltató megőrizhet. Stb.
Fel kell ismernünk, hogy az európai közösségi jog nagyobb pragmatizmusról tanúskodik, és mind a magánéletet, mind a személyes adatokat védi. Másfelől megjegyzendő, hogy az elektronikus levelezés védelme mind a természetes, mind a jogi személyekre vonatkozik.
Végül többé-kevésbé relevánsnak látszik az a kérdés, ez vagy az az adat személyes adat-e, ám később azonosítani kell azokat a kockázatokat is, amelyek az információs és kommunikációs technológiák használatával járnak adott kontextusban adott felhasználó esetében, és e kockázatokra elvi választ kell adni.
Felfogásunk szerint manapság a legérzékenyebbek a hardver Globális Egyedi Azonosítói (elektronikus sorozatszám) és a szoftver (süti), mert fizikailag hozzá vannak rendelve egy telekommunikációs terminálhoz, mely által lehetővé teszik ugyanannak a használónak több kontextusban való nyomon követését. Ennek az egyedi számnak a használatát a terminálra kellene korlátozni, s nem lenne szabad továbbítani a telekommunikációs hálózatba megfelelő garanciák nélkül.
A forgalmi adatok ugyancsak különleges szerepet játszanak. A európai jogban a forgalmi adatok anonimizálása vagy azonnali megsemmisítése a 2002/54 irányelvben rögzített követelmény. Ettől az általános elvtől a 2006/24 irányelv szerint a szolgáltatóknak el kell tekinteniük, s néhány adatot bűnüldözési és felderítési célból korlátozott ideig meg kell őrizniük. Meghökkentő az a tény, hogy a Google manapság valós időben tömegesen gyűjti az egyének Web-forgalmi adatait, és pedig kereskedelmi célból (a Google direkt marketingből származó bevétele 2007-ben 6 milliárd US dollárt tett ki[7]), miközben ilyen gyűjtés a telekommunikációs szolgáltatóknak kifejezetten tilos még a bűnüldöző szervek bűnüldözési és felderítési céljára is. Másképpen fogalmazva: az Internet egyik óriása jelenleg is gyűjt és *de facto* jobbára személyes adatokat kereskedelmi célra, holott mint szolgáltató nem lehet és nem

[7] E tárgyban lásd a Le Monde 2009. október 16-ai cikkét: „Bénéfices en forte hausse pour Google”, http://www.lemonde.fr/technologies/article/2009/10/16/benefices-en-forte-hausse-pourgoogle_1254699_651865.html

is olyan rendőri szerv, amely a közbiztonságot veszélyeztető esetekben azok felderítése céljából ilyen adatokhoz juthat.

6. Az adatkezelő

Mind a 95/46 irányelv, mind a 108. Egyezmény két, az adatkezelésért felelős személyt különböztet meg: a kezelés felelősét (adatkezelő) és adatfeldolgozót.
Ez a kategorizálás már nem látszik megfelelőnek. Az ICT világa specializálódik és újabb foglalkozások jönnek létre jelenleg és a jövőben egyaránt.
Ennek a rendelkezésnek a kiigazítására annak a társadalmi foglalkozásnak a funkciójára vonatkozó jogi rendelkezéseket kell hozni, amely gyűjti, tárolja vagy továbbítja az egyénnel kapcsolatos adatokat. Másrészt tudatában vagyunk annak, hogy ez a szabályozás jelenleg sérti a nemzetközi magánjog egyik problémáját. A fogyasztói jog mintájára az adatok védelme (amely egyre fontosabb szempontjává válik a fogyasztói jognak) nem lehetne az érintett és nem azoknak a társadalmi intézményeknek a védelme, amely az ő adatait tárolja és továbbítja? Ezt a kérdést részletesen a második részben tárgyaljuk.
A közvélemény nyomására egyes nagy szereplők (FaceBook, Google) néhányszor módosították a magánéletet illető politikájukat, de próba szerencse (trial and error) módszerük nem látszik kielégítőnek. Az Internet használó személyes adatai védelme és magánélete ellen intézett egyre kifinomultabb támadásokat az Internet nagy szereplőinek gazdasági érdekei motiválják, és felvetik azt a nem mellékes kérdést, hogy a társadalmi költségeket a közösség egésze viseli.
E kérdés jelentőségét megvilágítja az a tény, hogy az információs és kommunikációs társadalom számos eszközének (kereső motorok, közösségi hálók, elektronikus levelezés) finanszírozása a hirdetéseken nyugszik. A hirdetőknek az ingyenességet illető legsúlyosabb érve – elemzését követően – ingatagnak mutatkozik. Ha ezek a hirdetések finanszírozzák az Internetet, nyilvánvalóan fel kell tenni azt a kérdést, ki finanszírozza a hirdetéseket. A fogyasztó távolról sem kapja az internetet ingyenesen, hiszen valójában kétszer is fizet érte. Fizet mindenek előtt azzal, hogy profilírozhatóvá válik, adatait – tudtával vagy anélkül – elemezhetik és manipulálhatják. Másodszor akkor fizet, amikor megvásárolja az így hirdetett terméket vagy szolgáltatást, melynek végső ára a hirdetés költségét elkerülhetetlenül tartalmazza.
Sok szereplő alkotott véleményt a magánélet és a személyes adatok áruvá válásról. Napjainkban elismertnek látszik, hogy a magánélet védelme alapvető szabadság. És bizonyára azért, mert egy alapvető szabadságról van szó, s mert ez a magánélet, bizonyos mértékben és bizonyos feltételek mellet, pénzzé tehető. A képmáshoz fűződő jogok mintájára, melyet a szórakoztató ipar sztárjai pénzzé tesznek, minden egyént fel kellene jogosítani arra, hogy ne csak megtagadhassa vagy elfogadhassa a hirdetéseknek való kitettséget, hanem azt pénzzé is tehesse. Kívánatos lenne ezért, ha az információs és kommunikációs társadalom szolgáltatásainak igénybe vétele nem járna azzal a kötelező feltétellel, hogy elfogadjuk viselkedésünk elemzését és hirdetések megjelenítését, s ha az igénybe vett szolgáltatásért a fogyasztó fizethetne, Ezeket a hirdetéseket kizáró szolgáltatásokat a polgárok számára az Internet-hozzáférést biztosító szolgáltatók nyújtanák, az Internet-előfizetés díjában foglalt szerény anyagi hozzájárulás ellenében. Ha durván számba vesszük, milyen bevételt hoz ez valójában a Google részére, az érintett Internet használók tömegeinek figyelembe vételével megállapíthatjuk, hogy a Google szolgáltatásainak igénybe vételéért egy felhasználónak havonta körülbelül egy eurót kellene fizetnie, anélkül, hogy az jelentősen befolyásolná a Google bevételét.

7. Egy sikertörténet?

Felfogásunk szerint a modern mobil telefonhálózat példáját érdemes követni, hiszen annak technikájába szervesen beépítették a magánélet védelmét. A mobil telefonkészüléknek ugyanis tartalmaznia kell a hívószám kijelzés korlátozását (hiányát büntetés terheli, ilyen készüléket tehát lehetetlen árusítani). Ez a funkcionalitás minden felhasználónak, még a kezdőnek is, lehetővé teszi száma megjelenésének letiltását a hívott fél készülékén. Tudnunk kell azonban, hogy technikailag ezt a számot mindig továbbítják, mely lehetővé teszi, például a sürgősségi szolgálatok számára, bizonyos feltételek mellett és a törvény erejénél fogva, hogy e szolgáltatók hívása esetében a hívót azonosítsák.

A mobil telefonkészülékeknek ugyancsak van egy elektronikus szériaszámuk, az IMEI (International Mobile Equipment Identity). Ez a szériaszám átkerül a telefonhálózat üzemeltetőjéhez, és csak hozzá. A hálózat üzemeltetője technikailag nem továbbítja ezt a szériaszámot a távközlés címzettje mobil készülékére. Mindazonáltal a 2006/24 irányelv rendelkezése szerint ezt az azonosító adatot az üzemeltetőnek tárolnia kell. E technikai megoldások révén a felhasználó tényleges ellenőrzést gyakorolhat mobil telefonja felett. Megtilthatja hívószámának kijelzését, s így kezelheti nyomon követhetőségét és kontaktibilitását. Kommunikációját kódolják, így azt harmadik személy egykönnyen nem figyelheti meg.

Bizonyos egyetértést tapasztalhatunk a magánélet és a személyes adatok védelme elvei tekintetében /az adatvédelem ontológiája, a megfigyelhetőség, a nyomon követhetőség és a kontaktibilitás ellenőrzése, a célhoz kötöttség elvének tiszteletben tartása (az adatok összekapcsolása)/, amit a „privacy by design”-nal kapcsolatos számos kutatás is igazol.

Mi, akik a jelen kihívásaival szembesülünk, olyan törvényt szeretnénk látni, amely az információs és kommunikációs társadalom minden egyes szereplőjét különböző módon szólítja meg, igazodva ahhoz a szerephez, melyet játszik és azoknak az adatoknak a típusához, melyet kezel. Az információs világsztrádán olyan járműveket és technikákat kell alkotni, melyek valóra váltják a vezetőik védelmét szolgáló elveket. „Ha a technika problematikus, a problémára a technika adhat választ…”