MÉSZÁROS JÁNOS

A személyes adat mint az adásvétel tárgya

Az Internet és az adatvédelem viszonya

A személyes adatok feldolgozása a számítástechnika fejlődésének köszönhetően jelentősen egyszerűbbé vált, melynek két fontos következménye van: egyrészt a személyes adatok egyszerűbben hasznosíthatóvá váltak, mellyel a pénzre cserélésük is egyszerűbbé vált, másrészt ennek következtében az országok jelentős részében folyamatosan születnek az egyre szigorúbb adatvédelmi jogszabályok.

Tanulmányom célja feltárni, hogy milyen negatív hatásai vannak, ha a személyes adatokra áruként tekintünk.

Az internet jelentősen eltér a korábbi kommunikációs csatornáktól, ezért az adatvédelem újfajta szabályozása vált szükségessé. Három olyan jellemzője van a világhálónak, mely jelentősen megnehezíti a hagyományos jogalkalmazást: a decentralizáltság, a nyitottság és a csomagkapcsolt működés.

Decentralizáltság alatt azt értjük, hogy nincs az internetnek egyetlen központi irányító egysége, melytől technikailag függene. Nincsen egyetlen olyan csúcsszerv, melynek befolyása lenne az összes vonalra, lehetősége lenne azt ellenőrizni.

Nyitott az internet, mivel bárki számtalan elérési útvonalon (számítógépek, telefonok és táblagépek milliói) csatlakozhat ahhoz, így gyakorlatilag nem lehet senkit „kitiltani" róla. Bárki, minimális technikai igények teljesítése mellett rákapcsolódhat.

Az internet csomagkapcsoltsága azt jelenti, hogy az információ csak a küldő és a fogadó gépén áll össze tényleges formában.[1]

A fogyasztók vásárlási és internetezési szokásaikról a világhálón folyamatosan adatokat gyűjtenek és elemeznek, gyakran titokban, melyet a következő esetek is szemléltetnek. Ha valamely internetes keresőoldalt használva árukra vagy szolgáltatásokra keresünk, akkor a kereséseink tárolásra kerülnek, és ahhoz kapcsolódó, személyre szabott hirdetéseket kaphatunk (például futócipők után olvasunk, majd megjelenik egy Adidas reklám).

Az ISACA[2] felmérése alapján az okostelefon-tulajdonosok közel 60 százaléka használja a készülék nyújtotta geolokalizációs (helymeghatározáson alapuló) alkalmazásokat, annak ellenére, hogy ezen programokkal kapcsolatban közismertek az adatvédelmi aggályok. Ilyen

---

[1] F. HATÓ Katalin: *Adatbiztonság, adatvédelem*. SZÁMALK Kiadó, Budapest, 2001. 14-15.

[2] Az ISACA (Information Systems Audit and Control Association, www.isaca.org) az Információ rendszer menedzserek és ellenőrök nemzetközi szakmai szervezete, amelyet 1969-ben alapítottak az Egyesült Államokban és világszerte 160 országban, 193 tagszervezettel, több mint 95.000 tagot számlál.

például, amikor az okostelefonunk egyik programja naplózza, hogy hol járunk, majd ebédidőben kapunk egy hirdetést valamely közeli étterem ajánlatáról.

Amikor egy hipermarketben hűségkártyát kapunk, valójában az adataink átadásáról van szó: nevünk, címünk és egyéb személyes adataink mellett tudomást szereznek a vásárlási szokásainkról. Ezzel olyan szenzitív adatokat is megtudhatnak rólunk, mint hogy allergiásak vagyunk-e valamire, vagy rendelkezünk-e betegséggel (például csak laktózmentes tej és egyéb gyógyhatású készítmények rendszeres vásárlása).

Az adatvédelmi szabályozásnak kihívást jelent, hogy az egyének cselekvése a forgalom szabadsága és az alapvető jogok védelmének határvonalán mozogjon, mivel az adatgyűjtéssel járó veszélyeket és előnyöket minden ember másképpen éli meg. Sokan nem tudnak a hátuk mögött zajló adatgyűjtésről, és jóhiszeműen adnak ki információkat magukról. Miattuk fontos, hogy a jogszabályok megfelelő tájékoztatási és további kötelezettségeket írjanak elő az adatkezelők számára.

Az érintettek jelentős része tud az adatkezelésről, azonban az adott szolgáltatásra szüksége van, ezért azt kénytelen elviselni. Számukra legfontosabb, hogy megfelelően legyen szabályozva az adataik célhoz kötött felhasználása.

Végül beszélhetünk egy olyan, javarészt fiatalokból álló csoportról, akik minél több szolgáltatást szeretnének használni a lehető legkevesebb korláttal. Őket nem érdekli a mobiltelefonon bekapcsolt helymeghatározás veszélye, hanem hogy minél több barátjuk értesüljön róla, hogy ők éppen a Mc'Donald's-ban gyülekeznek utolsó óra után.

Az érintetteket a jogszabályok többféle módszerrel is védik, melyek közül egyik legjelentősebb a megfelelő tájékoztatás kötelezettsége.

Mivel az Európai Unióban, Magyarországon és a fejlett országok jelentős részében a célhoz kötöttség alapján személyes adatot kizárólag meghatározott célból, jog gyakorlása vagy kötelezettség teljesítése érdekében lehet kezelni, így vizsgálatom az Unió országait tekintve elméleti megközelítésű.[3] A kérdés különösen az Amerikai Egyesült Államokban aktuális, ahol a magánszféra védelmének megközelítése jelentősen eltér az európai modelltől, melynek alapja, hogy az USA-ban legfontosabb alkotmányos értékként az emberi szabadságot fogadják el, míg egy európai állampolgár az emberi méltóságot tekinti elsődlegesnek.

Az USA-ban a magánszféra védelme (rabszolgatartás történelméből eredően) a diszkrimináció tilalmára fókuszál és alig enged teret a magánfelek közötti viszonyok korlátozásának, míg az európai felfogás szerint az alapjogoknak az egész jogrendszert át kell hatniuk.[4] Az USA alkotmánya külön nem nevesíti a magánélet védelméhez való jogot, viszont több magánszférával kapcsolatos terület áll védelem alatt az alkotmánymódosítások[5] és a Legfelsőbb Bíróság döntései alapján.[6] Az USA jogrendszerében ezen felül tíz tagállam alkotmányában konkrétan szerepel a magánélethez való jog, továbbá két állam elismeri a keresetin-

[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
4. § (1) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.

[4] SZIGETI Tamás: Az információs hatalom korlátozása a tengeren innen és túl. *Infokommunikáció és jog* 33 (2009) 159.

[5] Szólás-, sajtó- és vallásszabadság (első alkotmánymódosítás). A megalapozatlan házkutatás elleni védelem (negyedik alkotmánymódosítás). A magántulajdon szentsége, önrendelkezés (ötödik alkotmánymódosítás).

[6] PÉTERFALVI Attila: *Adatvédelem és információszabadság a mindennapokban*. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2012. 29-31.

dításhoz való jogot magánszféra sérelme esetén.[7] Az Egyesült Államokban a személyes adatok védelméhez való jog nem vezethető le a magánélet védelmének alkotmányos jogából.

A felvázolt jogi háttér után nem meglepő, hogy az USA-ban európai értelemben vett adatvédelmi törvény és elkülönült adatvédelmi hatóság nem létezik,[8] így az Egyesült Államok nem éri el az Európai Unió (és a magyar adatvédelmi jogszabály) által előírt megfelelő védelmi szintet, melyet az Európai Bizottság, az európai törvények és adatvédelmi hatóságok a személyes adatok harmadik országba történő továbbításához feltételként szabnak meg.[9]

Bár az USA-ban nincsen elkülönült adatvédelmi hatóság, vagy személy, hasonló védelmi feladatokat lát el a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission) kereskedelmi célú adatkezelések esetén, továbbá a személyes adatok kezelését több szektorális jogszabály is lefedi.

Az érintett és a személyes adat fogalma

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.) határozza meg az érintett fogalmát: *bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy*.

A fogalomból eredően a szervezeteket nem illeti meg a személyes adatok tekintetében biztosított jogvédelem. Bár a meghatározásból nem tűnik ki, de érintett alatt csak élő személyek értendőek, mivel az információs önrendelkezési jog szükségképpen az adattal érintett élő személyt illeti meg. A meghalt személy adatainak védelméről, illetőleg a velük való rendelkezésről – az adattal vagy az adatkezeléssel összefüggő – külön jogszabályok rendelkeznek (például Polgári Törvénykönyv, levéltári és anyakönyvi jogszabályok). Bár a személyes adatok védelme nem illeti meg az elhunytakat, a helyzetük súlyozottan fontos, mivel a tudomány jelenlegi állása szerint mind az egy milliárd facebook felhasználó meg fog halni, és egy pillanat alatt bizarr vagy megrázó képekké válhatnak azok a családi, baráti fotók, vicces bejegyzések és ártatlan státuszüzenetek, melyek feltöltői elhaláloznak.

„Gyakorlatilag nem lehet törölni senkit és semmit egy komoly szerveren működő, alaposan megtervezett adatbázisból. Az ilyen adatbázisokban a törölt adatokat általában nem távolítják el, csak törölt állapotjelzővel látják el; aki a törlését kéri, nem lesz elérhető normál felhasználók számára, de adatai megmaradnak, így adminisztrátori jogosultsággal bármikor lekérhetők, vizsgálhatók, kereshetők. Az adatbázisok koherenciája megköveteli bizonyos rekordok megmaradását, ráadásul egy esetleges későbbi jogi vita miatt is szükség lehet bizonyos adatokra."[10]

---

[7] Privacy International PHR 2006-US United States of America, www.privacyinternational.org, (2010. 03. 02.)

[8] Adatvédelmi és információszabadság ügyekkel az USA Belbiztonsági Minisztériumának részlege foglalkozik (The Privacy Office of the U.S. Department of Homeland Security).

[9] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

8. § (1) Személyes adatot e törvény hatálya alá tartozó adatkezelő harmadik országban adatkezelést folytató adatkezelő részére akkor továbbíthat, vagy harmadik országban adatfeldolgozást végző adatfeldolgozó részére akkor adhat át, ha

a) ahhoz az érintett kifejezetten hozzájárult, vagy

b) az adatkezelésnek az 5. §-ban, illetve a 6. §-ban előírt feltételei teljesülnek, és – a 6. § (2) bekezdésében foglalt esetet kivéve – a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

[10] MERNYÓ Ferenc: Családi állapota: halott. *Népszabadság online*. 2010. július 24. (http://nol.hu/tudtech/csaladi_allapota_halott)

Ha egy élő ember törli a regisztrációját valamely internetes szolgáltatásról (például facebook), akkor az említettek alapján az adatai bár a nyilvánosság számára nem elérhetőek, de a szolgáltató szerverein jó ideig tárolva maradnak. Ebből következően a kapcsolat az adatok és az érintett között helyreállítható, így a szerveren tárolt adatok továbbra is személyes adatnak minősülnek az adatvédelmi gyakorlat szerint.

Az érintett fogalma után tárgyalandó a személyes adat meghatározása, mely az Infotv. alapján: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret, – valamint az adatból levonható, az érintettre vonatkozó következtetés.

A kapcsolatba hozhatóság az érintett és az adat közötti olyan viszony, amely meghatározza, hogy az adott esetben személyes adattal van-e dolgunk. Ha közvetetten sem állapítható meg a kapcsolat, a személyes adatok kezelésére vonatkozó szabályok nem alkalmazhatóak.

A számítógépeket az interneten egy négybájtnyi azonosító, az ún. IP-cím azonosítja. Az IP cím négy, 0-255 közötti értékű, ponttal elválasztott számból áll; például 112.183.2.1.

Ha a felhasználó fix IP-címet használ, számítógépét állandóan ugyanaz a cím azonosítja – ez az állapot tipikus azokban az esetekben, amelyeknél a számítógép kapcsolata a hálózattal állandó (kábeltelevíziós, bérelt vonali internetkapcsolat esetén). Böngészés közben valójában az történik, hogy az általunk megtekintett internetes oldalt letöltjük számítógépünkre, ahol a böngészőprogramunk (például Internet Explorer, Mozilla, vagy Google Chrome) meghatározott szabályok szerint megjeleníti azt. Böngészés közben történik azonban még valami, ami adatvédelmi szempontból lényeges: a webszerver – vagyis az a számítógép, amely a weboldalt tárolja, amelyről az oldalt saját gépünkre lehívtuk – az esetek többségében naplófájlban rögzíti a számítógépünk IP-címét és a megtekintés időpontját.[11]

Felmerül a kérdés, hogy ez a feljegyzett információ személyes adatnak minősül-e? A válasz igen, mivel közvetetten alkalmas az érintett azonosítására.

Kiemelendő, hogy a személyes adatminőség keletkezéséhez nem szükséges az érintett tényleges azonosítása, elég, ha csupán annak lehetősége fennáll. Az adatvédelmi gyakorlat az azonosíthatóság lehetőségét kiterjesztően értelmezi, így nem releváns, hogy az adatot megismerő személy képes-e azonosítani az érintettet. Így például az adószám attól függetlenül is személyes adatnak minősül, ha azt nem egy NAV alkalmazott tekinti meg.

A kiterjesztő értelmezés folytán személyes adatnak minősül az az adat is, amely csak másik adattal együtt lehet alkalmas egy személy azonosítására. Ebből következően a Kovács István név önmagában is személyes adatnak minősül, hiába él legalább több száz Magyarországon.[12]

Az célhoz kötöttség, mint adásvétel korlátja

Infotv. 4. § (1) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.

---

[11] JÓRI András: *Adatvédelmi kézikönyv*. Osiris Kiadó, Budapest, 2005. 98-110.
[12] PÉTERFALVI, 2012. 61-62.

A cél az adatkezelés legfontosabb része, melynek megváltozása új adatkezelést eredményez, amihez szükséges az érintett hozzájárulása. A célhoz kötöttség az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája.[13] Az adatgyűjtés célját annak megkezdése előtt meg kell határozni, valamint arról az érintettet megfelelően tájékoztatni kell, hogy megalapozottan dönthessen, miként rendelkezik személyes adataival, kiadja-e azokat. Az érintettel úgy kell közölni az adatfeldolgozás célját, hogy megítélhesse jogait és kötelezettségeit, továbbá a céltól eltérő felhasználás esetén élhessen jogaival.

A cél nélküli adatkezelés és adatraktározás jogszerűtlen, még az érintett hozzájárulásával is jogellenes. Az adatkezelés céljának meghatározottnak, konkrétnak és jogszerűnek kell lennie, így nem felel meg a célhoz kötöttség elvének, ha az adatgyűjtés célja túl tágan van megfogalmazva, egyedi célok nélkül. Magyarország az 1990-es évek elején az ország teljes lakosságát érintő adatfeldolgozó rendszert szeretett volna felállítani,[14] melyhez a az alábbi, semmitmondó célt határozta meg: „az állampolgár jogai érvényesítésének és kötelezettségei teljesítésének előmozdítása, az állami szervek, a gazdálkodó és társadalmi szervezetek, egyesületek, valamint magánszemélyek társulásai (a továbbiakban együtt: szervezetek) munkájának segítése".

Az Alkotmánybíróság megsemmisítette, mivel a célja „alkalmatlan arra, hogy az adatfeldolgozásnak bármiféle irányt vagy határt szabjon, azaz hogy célhoz kötöttségről egyáltalán beszélni lehessen"[15]

Az adatkezelésnek minden szakaszában meg kell felelnie a céljának, mely nem csak az adatkezelő és harmadik személyek relációjában kötelező szabály, hanem az adatkezelő szervezetén belül is. Ebből következően az adatkezelő szervezetében is csak azok férhetnek hozzá az személyes adatokhoz, akiknek ez feltétlenül szükséges, és munkájuk az adatkezelés céljához kapcsolódik, (például az áruházak pontgyűjtő rendszeréhez a számlázási osztály hozzáférhet, de az árubeszerzési osztály elvileg nem), mely által az adatkezelés nem lép ki az előre meghatározott mederből.

A Földhivatal az ingatlan-nyilvántartás alapján nem adhat információt arról, hogy egy konkrét személynek mennyi és milyen értékű ingatlanjai vannak, csupán egy konkrét ingatlan adatait adhatja ki, mivel az ingatlan-nyilvántartás célja az ingatlanforgalom biztonságának garantálása, nem pedig a lakosság vagyonának nyilvántartása.

Fontos megjegyezni, hogy a célhoz kötöttség közérdekű adatokra[16] nem értelmezhető, azok bárki számára cél nélkül hozzáférhetőek, szabadon felhasználhatóak.

Az Európai Parlament és a Tanács 95/46/EK irányelve szerint a tagállamoknak van lehetősége arra, hogy másodlagos célra is megengedjék az adatkezelést, amennyiben az elsőd-

---

[13] 15/1991. (IV. 13.) AB határozat.

[14] Az állami népességnyilvántartásról szóló 1986. évi 10. számú törvényerejű rendelet, valamint a Minisztertanácsnak e törvényerejű rendelet végrehajtására kiadott 25/1986. (VII. 8.) MT számú rendelete és 102/1990. (VII. 3.) MT számú rendelete.

[15] 15/1991. (IV. 13.) AB határozat.

[16] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § 5. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

leges adatkezeléssel összefügg, azzal releváns, így például,[17] ha az adatkezelő ügyféladatbázisát saját marketingre használja fel.[18] A magyar adatvédelmi szabályozás viszont nem engedi meg a másodlagos, releváns adatkezelést, a célhoz kötöttséget szigorúan és szűken értelmezi.

4. § (2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

A szükségesség elve alapján csak olyan személyes adat kezelhető, mely a cél eléréséhez elengedhetetlen, így például egy autó vásárlásához nem szükségesek az egészségügyi adataink. Legszemléletesebb példa a szükségesség elvére a bankok és biztosítók által a kockázatelemzéshez kért személyes adatok, melyek között különleges adatok[19] is vannak: személyi azonosító adatokon túl a kereset, betegség, házasság fennállása, házastárs keresete, további hitelek fennállta, életbiztosítás megléte, stb.

Az adatkezelés célja az ügyfél hitelképességének vizsgálata, mely által a hitelintézet képet kaphat az ügyfél vagyoni és családi helyzetéről. A bank minél több információt kap a potenciális ügyfélről, annál személyre szabottabb ajánlatot tud számára nyújtani, mely adott esetben pozitív hitelelbírálást és kedvezőbb kamatokat is jelenthet.

A Toysmart-ügy

Az utóbbi évtizedek alatt hatalmas mennyiségű rendszerezett, elektronikusan nyilvántartott személyes adat cserélt gazdát cégek adásvétele, egyesülése, szétválása és újraszervezése során. A cégek számára nagy jelentőséggel bír a személyes adatok birtoklása, mely számukra profittá konvertálható egyre könnyebben, köszönhetően a feldolgozáshoz szükséges technika elérhetőségének.

Az ügy rövid tényállása

A Toysmart[20] egy online játékkereskedő cég volt az Egyesült Államokban, melynek a Disney volt a többségi tulajdonosa. A Toysmart 2001-ben csődbe ment, és legjelentősebb megmaradt vagyona a felhasználói listája volt, melyet megpróbált eladni, de azt a sorozatos botrányok és hosszas procedúra után a bíróság végül nem engedte.

Az ügy részletes leírása

Mikor a Toysmart bejelentette, hogy befejezi a tevékenységét, megbíztak egy végrehajtással és árverezéssel foglalkozó céget (The Recovery Group), valamint meghirdették a Wall

[17] JÓRI, 2005. 217.

[18] Az Európai Parlament és a Tanács 95/46/EK irányelve, 6. cikk:
(1) A tagállamok rendelkeznek arról, hogy a személyes adatok:
b) 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;
c) gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek;

[19] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § 3. különleges adat:
a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

[20] A Toysmart 1999 januárjában kezdte meg a játékok kereskedelmét, majd 1999 szeptemberében szerezte meg a TRUSTe tanúsítványt.

Street Journalban és a Boston Globe-ban a felhasználói adatbázisukat, mely tartalmazta az ügyfeleik nevét, címeiket, fizetési adatait és információkat gyermekeikről.[21]

Mivel a Toysmart online cég volt, így nem rendelkezett „hagyományos" elárverezhető vagyonnal, számottevően nem volt ingatlan és ingó vagyona. Az egyetlen értékes tulajdona a vevőkörről megszerzett adatbázisa volt.

A listát 50.000 dollárért hirdették meg, mely csupán kis része volt a Toysmart teljes, 18 millió dollárnyi adóságának, azonban hatalmas károkat okozhatott volna az online kereskedelemnek, mivel a sikeres tranzakció kikövezte volna az utat más internetes cégek előtt is, akik pénzzé tették volna adatbázisukat.

Az eladással több jogi és morális probléma is volt, az egyik, hogy a Toysmart adatvédelmi irányelvében (melyet a felhasználók számára regisztráláskor rendelkezésre bocsátott), kötelezte magát arra, hogy az adatokat harmadik személlyel nem osztja meg, azokat diszkréten kezeli.[22] Továbbá a Toysmart rendelkezett „TRUSTe"[23] tanúsítvánnyal és pecséttel, mely egy olyan szervezet, amely garantálja, hogy a pecsétjével és tanúsítványával ellátott cég a személyes adatokat és más információkat bizalmasan és jogszerűen kezeli.

TRUSTe pecsét

1. ábra: forrás: www.truste.com

A TRUSTe nem tudott közvetlenül keresetet beadni a bíróságra és eljárást indítani a Toysmart ellen, azonban a Szövetségi Kereskedelmi Bizottság[24] (Federal Trade Comission, továbbiakban FTC) figyelmét felhívta a jogsértésre, mely vizsgálatot indított és bíróságon megtámadta az ügyletet.[25]

A Szövetségi Kereskedelmi Bizottság keresetében azt állította, hogy a Toysmart *„unfair"* és megtévesztő üzleti magatartást és gyakorlatot folytatott, mely a kereskedelemre negatív hatással van. A Bizottság utasította a Toysmartot és keresetében kérte a bíróságot, hogy tiltsa meg a felhasználói lista eladását.

Az egyezség

A Szövetségi Kereskedelmi Bizottság és a Toysmart egy olyan egyezséget kötött, mely alapján a Toysmart eladhatta volna a felhasználói adatbázisát, viszont csak olyan kvalifikált vevőnek (*„qualified buyer"*), aki vagy amely elkötelezett a családbarát és tisztességes üzleti po-

[21] A Toysmart a felhasználók gyermekeiről is gyűjtött információkat egy online dinoszauruszos játék során, szüleik engedélye nélkül.

[22] „A személyes adatok, melyeket a látogatóink önként megadnak [...], harmadik személlyel megosztva soha nem lesznek. Minden információ, mely a Toysmart birtokába került, csupán a felhasználói élmény személyre szabására lesz felhasználva. Amikor Ön a Tosmart.com-on regisztrál, biztosítva lehet arról, hogy az Önnel kapcsolatos információkat bizalmasan kezeljük." Toysmart adatfelhasználási feltételek és irányelvek, 2012. 10. 21.

[23] A TRUSTe egy olyan nemzetközi cég, mely globálisan nyújt adatvédelemmel kapcsolatos megoldásokat és szolgáltatásokat. Ügyfelei közé tartozik többek között az Apple, Microsoft, Disney, eBay és a HP.

[24] A Szövetségi Kereskedelmi Bizottság egy szövetségi állami szerv az Egyesült Államokban, mely fogyasztóvédelmi és versenyhivatali hatósági feladatokat lát el (http://www.ftc.gov/).

[25] http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm (2013. 01. 10.)

litika mellett, valamint hasonló tevékenységi területen helyezkedik el és tiszteletben tartja a felhasználók jogait. A gyakorlatban ez azt jelentette, hogy csak másik online játékkereskedő cégnek adhatja el a Toysmart az adatbázisát.

Az egyezséggel több probléma is volt. Az egyik, hogy a Toysmart a felhasználóinak nem biztosított *„opt-out"* (tiltakozási, utólagos leiratkozási) lehetőséget, továbbá az egyezségről nem kérték ki a bíróság véleményét.

Később úgy módosították az egyezséget, hogy a Toysmart eladhatja a felhasználói adatbázisát egy másik Disney leányvállalatnak (a Buena Vistának), mely a megvásárlás után rögtön megsemmisíti a listát. Ennek az elsőre ésszerűtlen és a Disney számára előnytelen üzletnek a célja az volt, hogy a felhasználók és a Disney-t bíráló jogvédők megnyugodjanak, továbbá a Toysmart hitelezői is pénzt lássanak az ügyletből.

Tehát a módosított egyezség alapján a Buena Vista a listát megvásárolja, majd megsemmisíti, így az adatbázis gyakorlatilag sehol sem létezett volna.

A bíróság ítélete

A bíróság ítélete alapján végül a Buena Vistának úgy kellett a listát megvásárolnia, hogy az nem kerül át hozzá fizikailag, hanem a Toysmart megsemmisíti. Tehát a Toysmartnak a listát meg kellett semmisítenie, a Buena Vistának pedig fizetnie úgy, hogy nem kapott érte semmit.

Az ügy hatása az internetes kereskedelemre és a felhasználók bizalmára

Az üggyel kapcsolatos felháborodás rávilágított az internetes kereskedelem legnagyobb gátjára: a felhasználók bizalmatlanságára.

Az üggyel kapcsolatos botrány után csökkent az Egyesül Államokban az internetes vásárlás iránti kedv, mely becslések alapján 2,8 milliárd dollár kiesést is okozhatott az internetes kereskedelem forgalmából csak 1999-ben.[26]

Több felhasználó is pert indított internetes kereskedők ellen különböző jogalapokkal, melyek közül leggyakoribb a szerződésszegés volt. Szerződésszegés esetén az Amerikai Kereskedelmi Kódex[27] alapján a bíróságok előtt a felhasználóknak azt kell bizonyítaniuk, hogy a kereskedők adatvédelmi irányelvei, melyeket regisztráció során elfogadtak, egy fogyasztó és vállalkozó között létrejött szerződés részének tekintendőek, mely alapján szerződésszegés történt.

A második leggyakrabban alkalmazott jogalap a felperesek kereseteiben a megtévesztés volt,[28] mely során azt kellett bizonyítaniuk, hogy az adatkezelési irányelvek hiányosak és megtévesztésre alkalmasak voltak.

Végül egyes államokban jogalapként szolgálhatott az is, ha az ott hatályos kereskedelmi szabályok megszegésével (megtévesztő üzletpolitika, fogyasztó megkárosítása stb.) vádolták az online kereskedőt.

A Toysmart ügy kapcsán felmerült a kérdés, hogy mit tehet a TRUSTe, ha ilyen jogsértés történik, és mennyire jelent biztonságot a tanúsítványa és pecsétje a honlapokon.

A TRUSTe gyakorlatilag három dolgot tehet, ha az ügyfeleinél jogsértést tapasztal:

1. Megfosztja az ügyfelet a TRUSTe tanúsítványtól és a pecsét használatától.
2. Az ügyféllel kötött szerződés megszegéséért bíróságon pert indít.
3. Fogyasztóvédelmi szerveknél és gazdasági versenyhivataloknál eljárást kezdeményez.

---

[26] Center for Democracy and Technology 1999-es felmérése alapján becsült összeg.
[27] United States Uniform Commercial Code U.C.C. § 1-201 (3).
[28] Restatement (2nd) of Torts, 537. §.

A tulajdonjogi és az alapjogi megközelítés

A Toysmart jogászai (és több cég jogi képviselője) amellett érveltek, hogy a személyes adatokat célszerű lenne árunak tekinteni, mellyel minden természetes személy szabadon rendelkezhetne és ellenszolgáltatásért egy megfelelő biztosítékokkal ellátott szerződésen keresztül átruházható, hasznosításra rendelkezésre bocsátható lenne (tulajdonjogi megközelítés).

A jogvédők és a bíróság szerint is ez a megközelítés teljesen téves volt, mivel a magánszféra és a személyes adatok védelme elsőbbséget élvez üzleti érdekekkel szemben. (alapjogi megközelítés).

A tulajdonjogi megközelítés szerint avval, hogy az online cégek megkapnák teljes körű rendelkezésre a felhasználók személyes adatait, a felhasználóknak csupán előnyére válna, mivel több szolgáltatást és kedvezményt kaphatnának érte, mely az érintettek részére pénzben mérhető előnyt is jelenthetne.

Az alapjogi megközelítés szerint ez azért téves feltevés, mert a cégek jelenleg is felhasználhatják a személyes adatokat célhoz kötött hirdetések elhelyezésére, és a kedvezmények nem lennének arányban a magánszféra korlátozásával.

A tulajdonjogi megközelítés abból a téves feltevésből indul ki, hogy minden személy szabadon képes belépni szerződésekbe és meghatározni annak feltételeit.

Az alapjogi megközelítés a valós életet hozza ellenérvként: az egyén (érintett, fogyasztó) a gyengébb fél, aki nincs tárgyalópozícióban a nagy vállalatokkal szemben. Az érintett döntési alternatívája a valós életben – különösen az online világban – az „elfogadom" és „elutasítom" lehetőségekre szűkül.

A személyes adatot árunak tekintők azzal érveltek, hogy az adatok „adásvétele" esetén is van az érintettnek több olyan (kötelmi) jogi védelme, mint az ellenszolgáltatás elve, ellenérték arányosságának elve, továbbá a jóhiszeműség és a rendeltetésszerű joggyakorlás követelményei.

A valós életben a felsorolt védelmek azért nem működnének, mert nincsen alkupozíció, és a vállalatok a jogi osztályaikon keresztül sokkal erősebb jogérvényesítési és tárgyalási pozícióban vannak, míg egy fogyasztónak jelentős anyagi és időbeli ráfordítást jelentene egy per lefolytatása, bizonytalan eredménnyel, addig ez egy vállalatnál a jogászok mindennapi feladata.

Azért is téves út a tulajdonjogi megközelítés, mert az érintett, miután a vállalat rendelkezésére bocsátotta a személyes adatait, már nem tudja követni azok útját és ellenőrizni, hogy kinek a birtokában vannak, kik tekintenek bele. Tehát az érintett a „szerződésszerű teljesítést" nem tudná vizsgálni.

A tulajdonjogi megközelítés enyhébb változatának megvalósulása

Az olvasható az Enliken honlapján „ha egy szolgáltatásért nem fizetsz, akkor Te nem a vásárló vagy, hanem maga az áru".[29]

Az Enliken[30] egy internetes tevékenységgel foglalkozó cég, melyet az Egyesült Államokban alapítottak 2011-ben, és célja, hogy a felhasználók hasznosíthassák a személyes adataikat egy sajátos módszer által, mellyel a felhasználók követni tudják adataik sorsát és még pénzt is kereshetnek (vagy takaríthatnak meg).

---

[29] „If you are not paying for it, you're not the customer; you're the product being sold."http://enliken.com (2012. 10. 21.)

[30] http://enliken.com/ (2012. 10. 21.)

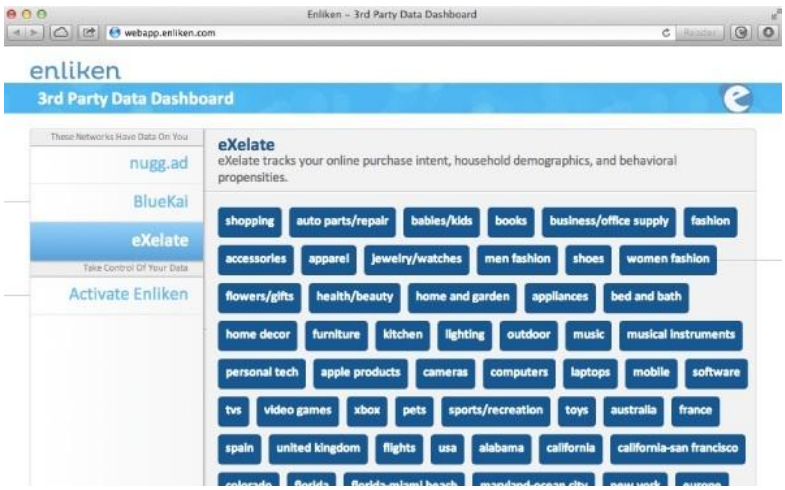
Interneten az érintettek használják többek között a szociális hálókat, videó megosztókat, híroldalakat és sok más ingyenes webes szolgáltatást, melyeken keresztül a cégek információt gyűjtenek róluk és azokat a felhasználják személyre szabott hirdetésekre, vagy eladják más cégeknek a felhasználók háta mögött. Nyilatkozatuk szerint ezt a folyamatot akarja megfordítani az Enliken.

Az Enliken szerint a felhasználók által önkéntesen átadott internetezési szokások és információk sokkal értékesebbek a hirdetők számára, mint a rejtetten, vagy „kéz alól" szerzett adatok tömege. Az Enliken módszere úgy működik, hogy a felhasználó feltelepít a számítógépére egy programot, mely megfigyeli a böngészési tevékenységét és azt naplózza.

A leírás alapján kizárólag olyan információkat rögzít a program, melyhez a felhasználó hozzájárult (például milyen weboldalakat nézett). A program a cég szerint más információkat (például magánlevelezést, szenzitív adatokat) nem rögzít, csak amelyekbe a felhasználó beleegyezett.

Az Enliken üzleti partnerei (például New York Times, Amazon) az Enlike programján keresztül látják, hogy a felhasználók mely oldalakat látogatják és milyenek az böngészési szokásaik, melynek ellenértékeként vásárlási kedvezményeket adnak a felhasználó részére, vagy ingyenes hozzáférést a fizetős tartalmakhoz.

Az program működés közben



2. ábra: forrás: www.gigaom.com

A felhasználói felületen be lehet állítani, hogy milyen adatokat kívánunk megosztani az Enliken-nel. Az Enliken koncepciója a legkényesebb kérdést is felveti: normális-e, hogy a hétköznapi felhasználók „aprópénzért" rendelkezésre bocsátják a személyes adataikat, melyek útját elméletileg tudják csak követni.

Az Enliken elmondása szerint egy tiszta és átlátható helyzetet teremtenek, melyet a felhasználó irányít és ő dönti el előzetesen (*opt-in*), hogy milyen adatokat kíván megosztani, melyeken kívül semmilyen más információ nem hagyja el a számítógépét. Úgy vélik, hogy ezáltal megteremthetnek egy előzetes beleegyezésen alapuló hirdetési rendszert, mely a fel-

használó számára hasznot és átláthatóságot biztosít, továbbá kedvező a vállalatoknak is, mert tiszta és értékes adatokat kaphatnak ahelyett, hogy kémkedniük kellene a felhasználók után.

Többen jártunk már úgy, hogy úszásról, tengerről olvastunk cikket, vagy ebben a témában küldtünk e-mailt, majd felbukkan egy hirdetés az akciós úszószemüvegekről. Az ilyen esetek több problémát is felvetnek, melyek miatt megrendül az internetes szolgáltatásokba vetett bizalom. Az példánál maradva, ha valaki a rákról és a rákos megbetegedés tüneteiről olvas egy életmóddal kapcsolatos oldalon, majd egy rákgyógyszerről kap hirdetést, már sokkal aggályosabb kérdéseket vet fel, mivel különleges adatokról van szó.

Az Enliken szerint ezt a kellemetlen helyzetet próbálja meg kezelni az ő megoldásuk: amikor interneten vásárolunk egy úszóruhát, akkor nem kapunk több hirdetést fürdőnadrágról, hanem egy valóban kedvezményes, személyre szabott ajánlatot egy úszószemüvegről olyan sportkereskedőtől, aki a hirdetésre vonatkozó engedélyt a mi beleegyezésünkkel kapta meg előzetesen.[31]

Az Enliken szerint a módszerük különösen a nagy vállalatoknak kedvez (Apple, New York Times), mert azok hajlamosabbak tisztességesen megszerezni és kezelni adatokat, mivel sokkal szabálykövetőbben kénytelenek viselkedni. Ennek következményeképpen kevésbé alkalmaznak adathalászatot és adatvásárlást, így az ő részükre nyitja meg a személyre szabott hirdetés lehetőségét az Enliken.

Ez a nagy vállalatok részére biztosított „lehetőség" azért kedvez a felhasználónak, mert így a legnagyobb és legmegbízhatóbb gyártóktól vásárolhat személyre szabott, kedvezményes ajánlatok alapján. A vállalatok számára ez a módszer a hirdetések hatékonysága miatt lehet vonzó, mivel az ilyen személyre szabott hirdetéseknél jelentősen nagyobb az esély arra, hogy a felhasználó a hirdetést megtekinti (CPM), vagy rákattint (CPC).[32]

Az Enliken programjának működését a fejlesztők olyan egyszerűre csinálták, hogy mindenki számára eladható legyen: a program beépül a böngészőbe (Internet Explorer, Mozilla Firefox, Google Chrome), és észrevétlenül működik addig, amíg nem akarunk beállításokat módosítani rajta.

Összegzés

Magyarországon az Alaptörvény emeli alapvető jogaink közé a személyes adatok védelméhez fűződő jogot, melynek részletszabályait sarkalatos törvény tartalmazza, valamint gyakorlati érvényesülését független hatóság biztosítja. Az Egyesült Államokban az adatvédelemnek sem a szabályozása, sem a kikényszerítése nincs így megvalósítva, bár az Európai

---

[31] http://www.adexchanger.com/data-exchanges/will-consumers-manage-their-data-enliken-makes-the-case/ (2013. 01. 21.)

[32] A bannerek (hirdetések a honlapokon) árazása 3 elterjedt módszert követ:

Időszaki árazás: adott időszakra (általában napra vagy hónapra) fix összeget kell fizetnie a hirdetőnek a reklámjaiért. Ezen módszert csak akkor érdemes választani, ha pontosan ismertek adott oldal látogatottsági statisztikái, és így az időszaki költséget lebontva CPM-re olcsóbban kijön egy megjelenés, mint egyébként. Tisztán ezt a módszert főleg kis, magáncélú oldalak alkalmazzák, illetve elvétve olyan portálok, melyeknél titkosak a látogatottsági statisztikák (komoly oldal sosem működik kizárólag ilyen alapon).

Megjelenés alapú árazás (CPM – Cost per mil): ez a legelterjedtebb árazási típus, amikor a banner 1000 megjelenésének van egy fix díja, például 5000 Ft, vagyis megjelenésenként 5 forint. De szokás egyszerűn AV (Ad View), azaz megjelenés díjat is megszabni (főleg Magyarországon). Ez a két fajta megadási mód egyenértékű.

Átkattintás alapú árazás (CPC – Cost per click): a leginkább hatékony és követhető megoldás a hirdetők részéről, de sajnos kevéssé elterjedt. Ekkor a hirdetőnek csak akkor kell fizetnie a hirdetésért, ha a látogatók ténylegesen rá is kattintottak, tehát „teljesítmény" alapon számolják adott reklám költségét.

Unióval való együttműködés céljából ez fokozatosan erősödik az adattovábbítás jogi akadályainak leküzdése céljából.

A mindennapi életünk során a leggyakrabban használt internetes oldalak Egyesült Államokbeli cégek tulajdonában állnak. Nem tudjuk és nem is akarjuk megkerülni őket, mivel a szolgáltatásaik fontosak és igényesek, azonban ennek ára van. A személyes adat mindennapjainkban ellenszolgáltatásként funkcionál: egy stabil és könnyen kezelhető e-mail rendszer (például gmail, hotmail) használatáért vagy szociális hálózathoz (például facebook) való csatlakozásért személyes adatainkat önként megadjuk, valamint annak gazdasági hasznairól (például facebook személyre szabott hirdetéseinek profitja) lemondunk.

A technológia fejlődésének köszönhetően Világunk leszűkült, melynek gazdasági és magánéleti előnyeit minden nap élvezzük, ám ezzel együtt a magánszféránk is csökkent, melyet a jogalkotónak és jogalkalmazónak védenie kell, különben a személyes adataink velünk együtt céltalan haszonszerzés tárgyává válnak.

JÁNOS MÉSZÁROS

Personal Data as Object of Sale Contract

(Summary)

Digital technology and the international flow of information affect our life significantly and it is difficult to regulate them. Toysmart, a dot-com company in the USA, which sold toys for children, went bankrupt June 2000. When the company went bankrupt, it wanted to sell the list of its costumer's personal data like other goods of the company when the ethical issues surrounding e-business came into sharp focus.

The Toysmart example is far from unique. In the past decade, large amounts of personal data changed hands or 'ownership', as part of merger-acquisitions, reorganizations and other strategic company movements. And there is more to come. With the importance of personalization services, it is clear that personal data and individual user profiles will be the key instrument in obtaining returns on the investment for the dot-com companies.

This article attempts to take account the philosophical and economic arguments for and against a property rights in privacy.

There are data protection authorities in the European Union and they have strong rights to protect the privacy which is a fundamental right. The privacy and the protection of the personal data are not guarded in the same way in the United States where the Federal Trade Commission can make some data protection measures.

The article wants to prove that the European human rights-oriented approach of the privacy can give better protection than the property approach of the privacy.