SZÉKELY IVÁN

# Privátszférát erősítő technológiák

Az információs társadalomban az egyén sorsa egyre inkább az „információs lenyomatától” függ. Az informatizálás egyik nemkívánatos hatása az, hogy az egyének elveszítik áttekintésüket és ellenőrzésüket személyes adataik sorsa fölött. A privátszférát erősítő technológiák (PET-ek) kifejlesztését az az igény szülte, hogy a technológia által okozott magánéleti erózió káros hatásait magával a technológiával is lehessen ellensúlyozni. Ez a tanulmány rendszerbe foglalja e technológiákat, bemutatja alkalmazási területeiket, technológiai hátterüket és a fejlődés irányát, és röviden áttekinti az alkalmazásukat ösztönző és gátló tényezőket.

**Kulcsszavak:** *privátszférát erősítő technológiák, PET, identitás-menedzsment, digital persona*

**Szerzői információ:**

Székely Iván
Társadalmi informatikus, az adatvédelem és az információszabadság multidiszciplináris területeinek nemzetközileg ismert szakértője és kutatója, az OSA Archívum főtanácsadója, a BME Információ- és Tudásmenedzsment Tanszékének docense. A szociológia kandidátusa. Az adatvédelmi biztosi hivatal egyik alapítója és 1995 és 1998 között főmunkatársa. Az Európa Tanács archívumi ajánlásának egyik kidolgozója; több nemzetközi civil szerveződés tagja. A BME mellett az ELTE Szociológiai Intézetében, a CEU-n és a Budapesti Kommunikációs Főiskolán indított új, interdiszciplináris jellegű kurzusokat. Számos tanulmány és szakkönyv szerzője, szerkesztője; az IKT-vonatkozású törvényhozás nemzetközi szakértője, kormányzati információs stratégiai dokumentumok társszerzője, a nyilvánosság és a titkosság témakörével foglalkozó nemzetközi kutatócsoportok aktív tagja.
E-mail: szekelyi@ceu.hu

**Így hivatkozzon erre a cikkre:**
Székely Iván. „Privátszférát erősítő technológiák”.
*Információs Társadalom* VIII, 1. szám (2008): 20–34.
*https://dx.doi.org/10.22503/inftars.VIII.2008.1.3*

Székely Iván

# Privát szférát erősítő technológiák

## Miért kell erősíteni a privát szférát?

Az információs társadalom jelenségeinek kialakulását, fejlődését lehetővé tevő és egyúttal indukáló információs-kommunikációs technológiák (IKT) hatásáról általában pozitív kép alakult ki a köztudatban, és még pozitívabb, optimistább képet sugallnak azok a közvetlen és közvetett reklámok, amelyek e technológiák elterjesztését, használatát népszerűsítik. Ez a hozzáállás magától értetődő a fejlesztők, terjesztők és szolgáltatók részéről, hiszen egyfelől alapvető üzleti érdekeik ezt diktálják a technológiai és szolgáltatási túlkínálat közegében, ahol elsősorban nem a felhasználói igények „húzzák" a technológia fejlődését, hanem az ipar és a kereskedelem igyekszik gerjeszteni a felhasználói igényeket; másfelől pedig ezt igényli a saját maguk és az általuk folytatott tevékenységek társadalmi elismertetése is, s ez a pozitív önkép beépül értékrendjükbe is. Érthető ez a megközelítés az üzleti világ részéről is, hiszen a vállalatok tevékenységének, versenyképességének egyre meghatározóbb eleme az IKT, ennek segítségével tudnak minél több információt szerezni, feldolgozni és üzleti céljaikra felhasználni ügyfeleikről, üzleti partnereikről és versenytársaikról. Az államigazgatás hozzáállása elvben – leszámítva az apparátus esetenkénti ellenállását – szintén pozitív, hiszen az IKT alkalmazása a modernizáció látványos eleme; növeli a hatékonyságot és az állam ellenőrző, információkezelő potenciálját, s erősítheti a polgárokkal fenntartott kapcsolatát.

Az IKT társadalmi hatásai tekintetében az információs társadalom kérdéseivel foglalkozó társadalomtudósok már árnyaltabban ítélik meg a helyzetet, többségük azonban nem értékmentesen, kívülálló megfigyelőként, hanem közvetlenül vagy közvetve pozitív értéktartalommal ítéli meg e hatásokat. E-demokráciáról sokat olvashatunk, e-diktatúráról – mint az IKT lehetséges felhasználási területéről – sokkal kevesebbet. A digitális szakadék növekedése vagy a magánélet határainak eróziója gyakran csak a teljesség kedvéért említett terület, afféle kötelező penzum az elemzésekben.

A kérdés ma már nem az, hogy használjunk-e számítógépeket, vagy sem, hanem hogy felismerjük-e azokat a nemkívánatos mellékhatásokat (hasonlóan a motorizációnak a környezetre és az egészségre gyakorolt hatásaihoz), amelyek ugyan nem gátolják meg a technológia használatát, de mindenképpen kezelést igényelnek. A színvonalasabb elemzések ma már nem azzal foglalkoznak, hogy jó vagy rossz irányba vezet-e a technológiavezérelt fejlődés – már lezárult az „áldás vagy átok", avagy az „Orwell vagy Athén" polarizálás korszaka –, hanem inkább azzal, hogy hogyan kezeljük ezeket a negatív vagy vitatható kimenetelű hatásokat. A technika „semlegességének" mítoszát (vagyis azt, hogy minden technológiai fejlemény eredendően semleges és értékmentes, ugyanúgy lehet jóra és rosszra használni, jó és rossz emberek kezébe adni) már talán csak a műszaki értelmiség egy része érzi maradéktalanul magáénak; egyre világosabbá válik, hogy már a termékek és szolgáltatások mögött rejlő technológia is alapvetően magán viseli kifejlesztőjének, megrendelőjének értékrendjét és érdekviszonyait. Örven-

detes kutatási fejlemény, hogy a kritikai megközelítést igénylő hatások elemzése napjainkban már nemcsak spekulatív szinten, absztrakt veszélyek felvázolásával történik, hanem konkrét forgatókönyvek elemzésével, valós és hipotetikus esettanulmányok feldolgozásával is.[1]

Az egyik olyan hatást, amelyet meglévő – kulturális értelemben nyugati típusú, demokratikus, jogállami – értékeink szempontjából legalábbis vitatható kimenetelűnek kell tekintenünk, és ezért kritikai elemzést igényel, az információkezelés folyamatosan megújuló eszközeinek és technikájának birtoklása fejti ki a hatalmi viszonyok megváltozására mikro- és makroszinten egyaránt. Információs viszonyrendszerben ritkán szerepelnek tökéletesen egyenrangú résztvevők, szinte mindig találhatunk erősebb és gyengébb felet, akár csak pillanatnyi viszonyukat tekintve is. Makroszinten jellemzően ilyen, információs szempontból gyengébb fél az állampolgár az állammal szemben, az ügyfél az üzleti szolgáltatóval szemben. Ha a gyengébb fél szemszögéből nézzük, az ő információs státusának egyik meghatározó eleme az, hogy milyen információkhoz fér hozzá másokról, a közszféráról, a külvilágról; a másik meghatározó eleme pedig az, hogy mások milyen információk birtokába kerülhetnek róla. Legújabb kori történelmi távlatban az egyén szempontjából az első elem dinamikája inkább evolúciónak tekinthető, a második eróziónak.

Ebben az erózióban kiemelt szerepe volt és van a mindenkori korszerű információs és kommunikációs technológiáknak. Warren és Brandeis korában az információ*szerzés* technológiája (telefónia, fotográfia) ért olyan fejlettségi fokra és alkalmazási szintre, ami megbontotta a magánélet addigi határait.[2] A második világháborút követő időszakban, a nagyszámítógépek polgári célú alkalmazásának idején az információ*feldolgozás* forradalmasodott (a lakosság nyilvántartása, az emberek adatainak kiterjedt elemzése), s ez tovább billentette az információs egyensúlyt a technológia birtoklói – az állam és az üzleti monopóliumok – javára. A jelenkor internetes, összehuzalozott világában pedig a két mozzanat, az információszerzés és -feldolgozás szétválaszthatatlanul összekapcsolódott: egyének milliói használnak olyan eszközöket és technológiákat, amelyek a rájuk vonatkozó információk gyűjtését és elemzését – és ennek felhasználásával tevékenységük, életük befolyásolását – az érintettek tudta nélkül végzik.

Ha a modern demokratikus jogállamok alkotmányait, adatvédelmi törvényeit, a nemzetközi szerződéseket, ajánlásokat, uniós irányelveket nézzük, akkor a kép megtévesztő lehet: az egyének *joga* arra, hogy a róluk szóló információkhoz – személyes adataikhoz – mások ne férhessenek hozzá korlátlanul, azokat ne használhassák az érintettek hozzájárulása vagy törvényi felhatalmazás nélkül, határozott történelmi fejlődést, a garanciák kiépülését mutatja. A *habeas corpus*tól a *habeas data*ig vagy az adatvédelemtől az információs önrendelkezésig ívelő fejlődés valóban impresszív, de csupán ellensúlyát képezi a magánélet eróziójának, amit jelentős részben maga az IKT tesz lehetővé. Ha csak egy pillantást vetünk e technológiák használatára az alkalmazások szintjén, a kor-

[1] E tekintetben különösen tanulságosak a *Safeguards in a World of Ambient Intelligence (SWAMI)* európai uniós kutatási projekt „sötét forgatókönyvei".

[2] A szerzőpáros 1890-ben írt híres tanulmányát, a *privacy*problematika megalapozó klasszikusát – amelyet igen sokan idéztek, de kevesen olvastak –, az *Információs Társadalom* 2005. évi 2. számában magyarul is megjelentette.

szerű és elterjedt eszközök és módszerek között találjuk az adattárházak építését (az élet átmeneti jelenségeiről szóló adatok történeti felhalmozását), adatbányászati módszerek (az eredeti adatkezelési célt meghaladó kifinomult elemzések) alkalmazását, az ügyfélkapcsolat-menedzsmentet (*CRM* – „ismerd meg ügyfeledet", „maximáld ügyfélértékét"), a felhasználók internethasználati szokásaiból profilok építését (és eladását más szolgáltatóknak), kéretlen elektronikus levelek tömegének küldését *(spam)*, a személyközi kommunikáció monitorozását (például webpoloskák, *cookie*-k útján) stb. Ehhez társulnak azok a divatos, személyes adatok tömeges kezelésén alapuló kapcsolatteremtő és -menedzselő szolgáltatások, amelyeket a felhasználók önként vesznek igénybe – ilyen például a *Facebook* vagy az *IWIW* –, az adataik feletti rendelkezés azonban kikerül a kezükből, s ez többnyire csak később tudatosul számukra.

Egyrészről azt láthatjuk, hogy egy fejlett társadalomban az egyének sorsa egyre inkább információs lenyomatuk *(information replica)* vagy digitális személyiségük *(digital persona)* sorsának függvénye – egyszerűen szólva annak, hogy „mi van róluk a gépben" –, másrészről pedig hangzatos kijelentéseket olvashatunk a magánélet haláláról, a *privacy* végéről. Vajon mindig és szükségképpen ilyen hatású-e a technológia? A privát szférát erősítő technológiák *(privacy enhancing technologies, PETs)* létrejötte és alkalmazása azt bizonyítja, hogy nem. Kifejlesztésüket éppen az az igény szülte, hogy az IKT által okozott magánéleti erózió káros hatásait ne csupán szabályozással, önszabályozással, az aktorok oktatásával, felvilágosításával, hanem magával a technológiával is lehessen ellensúlyozni.

## A PET-ek lényege, csoportosíthatósága

A PET-ek alapvető célja, hogy ne csak az adatokat általában, hanem az adatok *alanyait* is védjék a visszaélések ellen, és elősegítsék információs önrendelkezésük érvényesíthetőségét a korszerű IKT közegében. Ezért a PET-ek hangsúlyozottan nem „semleges" technológiák, „irányultságuk" van: a rendeltetésszerűen használt PET-eszközök és rendszerek mindig a gyengébb felet – jellemzően az adatalanyt – védik az információs túlhatalommal rendelkező erősebb féllel szemben. Természetesen nem mindig rendeltetésszerűen használják ezeket az eszközöket és rendszereket: számos adat mutat arra, hogy éppen az információs túlhatalommal rendelkező fél intézményei (például nyomozó szervek, diktatórikus országok hatóságai) használják ezeket saját kommunikációjuk biztonságosabbá tételére.

A teljesség igénye nélkül idézünk két definíciót, amelyek a PET-ek lényegét kívánják megragadni:

> „A PET olyan információs és kommunikációs technológiák gyűjtőfogalma, amelyek megerősítik az egyén magánéletének védelmét egy információs rendszerben azáltal, hogy megakadályozzák a személyes adatok szükségtelen vagy jogellenes felhasználását, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén ellenőrzését személyes adatai felett"[3] (Koom et al. – Borking 2004, 68).

[3] A holland Alkalmazott Tudományos Kutatások Intézetének meghatározása.

> „A PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs *privacy*t a személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, anélkül, hogy csökkentené az információs rendszer funkcionalitását"[4] (van Blarkom–Borking–Olk 2003, 33).

Ez utóbbi meghatározás a privát szférát erősítő technológiák fontos elemét tartalmazza: azt, hogy nem az eredeti funkcionalitás korlátozására, netán az egész rendszer használatának megakadályozására irányulnak, hanem megkísérlik leválasztani róla a személyes adatok „szükségtelen", „nemkívánatos" vagy „jogellenes" kezelését. (Ha egy informatikai funkció eleve a szükségtelen, nemkívánatos vagy jogellenes adatkezelésre irányul, akkor a PET-ek természetesen e funkció érvényesülésének meggátolására törekednek.)

Ezekből az igen magas szinten általánosító meghatározásokból is sejthető, hogy a PET megnevezés a technológiák meglehetősen vegyes és szerteágazó csoportját fedi le. Ennélfogva e technológiák csoportosítása is többféleképpen lehetséges. A legismertebb és egyúttal leginkább spekulatív jellegű csoportosítás Herbert Burkert nevéhez fűződik.[5] Burkert szerint – aki maga nem technológus, hanem az információs társadalom és az IKT jogi vetületeinek teoretikusa – léteznek szubjektumorientált, objektumorientált, tranzakcióorientált és rendszerorientált koncepciók, illetve ilyen koncepciók alapján megvalósított technológiák. A szubjektumorientált koncepciók középpontjában az alany, a szubjektum áll; közvetlen céljuk, hogy megszüntessék vagy korlátozzák a cselekvő, egymással kölcsönhatásba lépő szubjektumok azonosításának lehetőségét, akár aktuális tranzakcióik során, akár korábban rögzített adataikhoz való kapcsolatukban. Erre szolgálhat például az egyszer használatos azonosítók, digitális fedőnevek alkalmazása. Az objektumorientált megoldások az eszközre, az objektumra összpontosítanak: olyan, bárki által használható, a használójáról „digitális ujjlenyomatokat" nem továbbító eszközök tartoznak ide, mint például az előre feltöltött telefonkártya, amellyel használójának (használóinak) telefonálási szokásait nem lehet monitorozni. A tranzakcióorientált PET-ek a hálózati tranzakciók során keletkező számtalan, az alany tevékenységének visszafejthetőségét, követhetőségét lehetővé tévő bejegyzés törlését, az adatláncolatok feldarabolását célozzák (például a rekordok automatikus törlésével); a rendszerorientált koncepciók pedig mindezen megoldások egységes rendszerbe szervezésén és alkalmazásán alapulnak.

Megkísérelhetjük más elvek alapján is csoportosítani a PET-eket, például aszerint, hogy melyik adatvédelmi alapelv[6] érvényesülését segítik elő. Egy további osztályozás szerint léteznek egy résztvevős PET-ek (például a vállalati privacymenedzsment-rendszerek), központosított közvetítős rendszerek (például az *Anonymizer*), elosztott közvetítős rendszerek *(Crowds, Freedom Network)* és szervertámogatású rendszerek (PET-tartalmú digitális pénzrendszerek).

[4] *A privacy és a privát szférát erősítő technológiák kézikönyve* meghatározása.

[5] A csoportosítást tartalmazó eredeti közlemény magyar fordítása ugyancsak az *Információs Társadalom* 2005. évi 2. számában jelent meg.

[6] A személyes adatok kezelésének tételes alapelvei – különböző csoportosításokban és lefedéssel – nemzetközileg elfogadottak; ilyen alapelv például a célhoz kötöttség vagy a személyes részvétel elve.

Ismét más felosztást eredményez, ha aszerint különböztetjük meg e technológiákat, hogy „technológiaalapúak" vagy humáninterakció-alapúak-e – más szóval, hogy az alkalmazott eljárás középpontjában valamilyen technológia áll-e (többnyire ilyenek a kriptográfiai protokollok), vagy a lényeg az emberi közreműködés lehetővé tételében (és így az információs önrendelkezés érvényesítésében) rejlik. Az előbbi csoportba sorolhatók például azok a PET-tartalmú digitális pénzrendszerek, amelyek biztosítják, hogy a digitális pénz[7] elköltésével, forgatásával a pénzforgalomban részt vevő aktorok ne ismerhessék meg illetéktelenül a pénz birtoklójának, elköltőjének szokásait, ne következtethessenek anyagi helyzetére, ízlésére.[8] Az utóbbi kategória példája a *Platform for Privacy Preferences (P3P)*, amelynek egy verzióját a *World Wide Web Consortium (W3C)*, az internet fejlődését alapvetően meghatározó szabványok, ajánlások, szoftverek és eszközök fejlesztésével foglalkozó szervezet koncepciója és megbízása alapján az Európai Unió Olaszországban működő egyesített kutatóközpontja *(Joint Research Centre)* fejlesztett ki. A *P3P* lényege, hogy a szolgáltató és a felhasználó közötti távkapcsolatot, melynek során a felhasználó személyes adatainak automatikus és általa ellenőrizhetetlen átadása zajlik, szabványos alkufolyamattá alakítsa. Amikor ugyanis egy felhasználó kapcsolatba lép egy távoli szolgáltatóval – például böngészőjével annak weboldalára lép –, akkor már a kapcsolat megteremtése pillanatában megindul a személyével kapcsolatba hozható adatoknak (vagyis a felhasználó személyes adatainak) az automatikus áramlása a szolgáltató felé. Ezt a folyamatot a felhasználó nem észleli és legfőképpen nem tudja befolyásolni. A *P3P eredeti víziója* egy olyan rendszer kifejlesztésére irányult, amelyben a felhasználó előre meghatározná adatkezelési preferenciáit, vagyis azt, hogy milyen adatkezelési gyakorlatot folytató szolgáltatókkal hajlandó kapcsolatot teremteni. E preferenciák vonatkozhatnak arra, hogy egyáltalán hozzájárul-e adatainak szerveroldali rögzítéséhez, kívánja-e ellenőrizni, módosítani, esetleg törölni saját adatait a szolgáltatónál, vagy megengedi-e a szolgáltatónak, hogy az más szolgáltatónak is továbbadja adatait; ha igen, mely adatait, milyen szolgáltatóknak stb. – mindezt szabványosan és egyszerűen, például *checkbox*ok bejelölésével. A szolgáltatók is hasonlóképpen meghatároznák saját adatkezelési profiljukat, és amikor a felhasználó beírja egy weboldal címét a böngészőjébe, a *P3P* még a kapcsolat megteremtése (és az adatáramlás megkezdődése) *előtt* összehasonlítja a két profilt, és csak akkor engedélyezi az automatikus kapcsolódást, ha azok azonosak.[9]

[7] Alapvető különbség a digitális eszközökkel távolról hozzáférhető és menedzselhető, de tulajdonképpen hagyományos számlapénz, másfelől a valódi digitális pénz között, hogy az előbbinél a pénz voltaképpen mindig a bankban marad, a digitális csatorna csak üzenetek, rendelkezések küldésére szolgál, míg az utóbbi esetben maga a digitális jelsorozat rendelkezik monetáris értékkel, vagyis a pénz a számítógépünkben, a kártyánkon, a szolgáltató szerverén van, és a készpénzhez hasonlóan adjuk át partnereinknek.

[8] Az ilyen rendszerek klasszikus példája az 1990-es években kifejlesztett és korlátozott körben elterjesztett *e-cash*.

[9] A valóságban a *P3P*-nek egy „lebutított" változata valósult meg, amelyben a felhasználók nem határozzák meg saját profiljukat, csupán megnézhetik a szolgáltató profilját (ha a szolgáltató egyáltalán használja a *P3P* szabványos profilmeghatározó programját), és *utólag* dönthetnek arról, hogy milyen speciális beállítást kívánnak alkalmazni a szolgáltatóra vonatkozóan, például tiltólistára helyezik. Ilyen *P3P* szolgáltatás található az *Internet Explorer* magasabb sorszámú verzióiban. A PET fejlesztői és alkalmazói közösségek egyre több kritikával illetik a *P3P* megvalósított változatát, és azt látszateredménynek, a PET-funkcionalitás szempontjából voltaképpen kudarcnak tekintik.

A PET-ek alapvető céljukat általában négy kritérium: az *anonimitás*, a *pszeudonimitás*, a *megfigyelhetetlenség (unobservability)* és az *összeköthetetlenség (unlinkability)* vagylagos vagy konjunktív teljesítésével érik el. Leegyszerűsítve, az anonimitás azt jelenti, hogy az adatokat, illetve az adatok kezelésével járó eseményeket, cselekvéseket nem tudjuk egy meghatározott személlyel kapcsolatba hozni. A pszeudonimitás esetében van alanya az adatoknak, de az alany valós kilétét nem ismerjük; egy valós adatalanynak több fedőneve, profilja, virtuális személyisége is lehet. A megfigyelhetetlenség azt jelenti, hogy egy illetéktelen harmadik fél ne észlelhesse, hogy valaki egy távoli erőforrást használ, például nyílt hálózati kapcsolaton keresztül egy internetes folyóirat oldalait tölti le. Az összeköthetetlenség feltétele pedig az, hogy az illetéktelen harmadik fél akár észlelheti is a távoli erőforrás valaki általi használatát, azonban ne tudjon kapcsolatot teremteni az aktuális használat és az ezt megelőző vagy követő használatok között. Az összeköthetetlenség tehát megakadályozza a felhasználók szokásainak megfigyelését, profilírozását. Aktív internethasználók esetében mind a négy kritérium jelentőséggel bír; passzív (nem közreműködő) adatalany esetében – akinek csak az adatait használják, jellemzően a tudta és beleegyezése nélkül – értelemszerűen csak az első kettő.

## Alkalmazási területek, eszközök, szolgáltatások

Az egyik leggyakrabban végzett internetes tevékenység a weboldalak letöltése, olvasása, vagyis a böngészés. E tevékenység során nemcsak az elsődleges szolgáltató (a honlap fenntartója), hanem a hozzá kapcsolódó másodlagos szolgáltatók (például a hirdetések elhelyezői) is számos olyan adat birtokába jutnak a böngészést végzőről, amelyről egyrészt a böngésző nem is tud – vagy ha tudna, nem járulna hozzá –, másrészt nem szükségesek a szolgáltatás teljesítéséhez. Ha az illetéktelen és többnyire jogellenes megfigyelés csak a böngésző fogyasztói mozgásterét befolyásolja, akkor legfeljebb olyan üzleti praktikák alanyává válik, mint a dinamikus árazás.[10] Ha a felhasználói profil az érintett személy érzékeny adatait, például vallásos vagy más lelkiismereti meggyőződését, egészségi állapotát vagy szexuális szokásait tükrözi, akkor az érintett akár közvetlen vagy közvetett zsarolás áldozatául is eshet. Ha pedig az érintett valamely ország vagy politikai rendszer megítélése szerint tiltott tartalmakat, például nem engedélyezett híreket vagy politikai elemzéseket olvas az interneten, akkor ennek követése és nyilvántartása súlyos szankciókat is eredményezhet számára.

E probléma kezelésére fejlesztették ki az *anonim böngészőket*, amelyek azt hivatottak biztosítani, hogy sem a szolgáltató, sem a mögöttes szolgáltatók, sem pedig külső megfigyelők ne monitorozhassák a böngésző személyek kilétét, a böngészett tartalmakat, a böngészési szokásokat. E feladatot többnyire köztes számítógépek, ún. *proxy*k be-

[10] A „dinamikus árazás" eufemisztikus kifejezéssel jelölt gyakorlat azt jelenti, hogy az interneten vásárló felhasználó sohasem látja a szabott árakat, az árakat annak függvényében állapítja meg a szolgáltató, hogy a vevő a profilja alapján mennyire erős késztetést érezhet a termék vagy szolgáltatás megvételére. Hasonlattal élve, ez olyan, mintha a láthatólag éhes vendég étlapján magasabb árak jelennének meg, hiszen várhatóan úgyis fog rendelni. (Ez a legtöbb európai országban jogellenes; az elektronikus kereskedelmet szabályozó jogszabályok éppen az árak egyértelmű, előzetes megjelölését írják elő az interneten is – ahogy például a vendéglőknek is még a bejáratuk előtt kell bemutatniuk kínálatukat és áraikat.)

iktatásával oldják meg, amelyek a felhasználó „megbízásából" kérik le a megtekinteni kívánt oldalakat, a felhasználó személyét (internetes címét, használt eszközeinek azonosítóit) eltakarják a többi szereplő elől. Egy másik megoldás a csoportszintű anonimitás biztosítása, amelyben láthatók a csoport résztvevői és a lekért oldalak, de nem lehet a résztvevőket egyértelműen társítani a lekért weboldalakhoz. Természetesen az anonim böngészést lehetővé tevő programok, szolgáltatások korántsem tökéletesek; érdemes előzetesen tájékozódni a megbízhatóságukról.[11]

A böngészés jól ismert velejárói a „sütik" *(cookies)*, amelyek olyan kis szövegfájlok, amelyeket a szolgáltató helyez el a böngésző számítógépén, s így a következő kapcsolatfelvételkor már eleve bizonyos információk birtokában lesz a böngésző személyéről. Vannak „ártalmatlan", csupán a kapcsolat technikai fenntartását szolgáló sütik, amelyek a kapcsolat megszakadásával (például a weboldalról való eltávozással) automatikusan törlődnek, de vannak olyanok is, amelyek a felhasználó láthatatlan profiljának építését szolgálják. Számos PET-tartalmú program kínál sütikezelést – ezen a sütik törlését, szűrését, a felhasználó általi kontrollját értve –, s ehhez általában a sütihasonlat iróniáját kihasználó neveket választanak (*Cookie Cruncher, Cookie Jar, Burnt Cookies* stb.). Ugyancsak a böngészés során kerülünk – tudtunkon kívül – kapcsolatba a *webpoloskákkal (web bugs)*, amelyek megjelenési formájuk szerint 1 × 1 pixel méretű, áttetsző színű – tehát láthatatlan – képek. Elhelyezésük célja általában az, hogy egy illetéktelen harmadik fél monitorozhassa a szolgáltató és a felhasználó közötti kapcsolatot, vagyis azt, hogy ki mit néz vagy vásárol az interneten. Itt is léteznek „ártalmatlan" webpoloskák, amelyeket maga a szolgáltató vagy egy külső szervezet weboldal-látogatási statisztikák készítésére használ fel (bár a felhasználás éppen a láthatatlanság és érzékelhetetlenség miatt nehezen ellenőrizhető), és vannak e-maillel kombinált poloskák is, amelyek célja a fogyasztók titkos megfigyelése (Hullám 2005, 216). Egyes PET-tartalmú szolgáltatások e webpoloskák irtását, vagy legalábbis felismerését kínálják (ilyen például a Bugnosis fantázianevű program). A szolgáltatásoknak ebbe a családjába sorolhatjuk a *spyware-irtókat* is: ezek a szoftverek igyekeznek kiszűrni azokat a „kémprogramokat", amelyeket egyes szolgáltatók vagy külső megfigyelők azzal a szándékkal telepítenek észrevétlenül a felhasználók számítógépére, hogy ott információkat gyűjtsenek a tárolt adatokról, fájlokról, azok használatáról, a felhasználó hálózati kapcsolatairól, és ezeket az információkat rendszeresen továbbítsák megbízóiknak minden alkalommal, amikor a felhasználó a hálózatra kapcsolódik.

Ugyancsak a legelterjedtebb internetes tevékenységek közé tartozik a személyközi üzenetváltás, elsősorban az *e-mail*. Kevés internethasználó van tudatában annak, hogy az e-mailes üzenetküldés bizalmassági szintje közel áll a nyílt levelezőlapéhoz; és bár vannak az üzenet illetéktelen elolvasását nehezítő megoldások, a főnök vagy a rendszergazda általában nem tartozik az elektronikus levelek tartalmához nehezen hozzáférők közé. De nemcsak az üzenet tartalma, hanem a kommunikáló felek kiléte, üzenetváltásuk időpontja, gyakorisága, sorrendje, sőt néha a terjedelme is értékes információt nyújthat a lehallgatónak. Az *anonim remailerek* ezeknek az információknak az illetéktelenek előli elfedését célozzák. Olyan üzenet-továbbküldő szolgáltatásokról van szó,

[11] E témában magyar nyelvű összehasonlító elemzés is megjelent, lásd Gulyás Gábor György tanulmányát „Anonim-e az anonim böngésző?" címmel (Gulyás 2006).

amelyek akár a címzett elől is elfedik a küldő kilétét; ez a hatalom kritikájának ókori formája, a tömegből való „bekiabálás" modern megfelelőjeként funkcionálhat az internetes környezetben. Többnyire azonban a címzett ismeri a feladót, kettejük kapcsolatából csak a harmadik feleket kívánják kizárni.

A *remailerek* és a lehallgatásukra kifejlesztett technológiák fejlődése az elmúlt két évtizedben rabló-pandúr játékra emlékeztetett. A legelső, ún. *Cypherpunk* típusú *remailerek* csak a továbbítandó üzenet fejlécét cserélték le, s ezt a – szabadon reklámozott, tehát mindenki által ismert – *remailer* bemenetének és kimenetének figyelésével könnyen vissza lehetett állítani. A védekezésül bevezetett késleltetési időt (az üzenetek „pufferolását") a támadók a saját üzeneteikkel való elárasztással próbálták ellensúlyozni, amire a fejlettebb *remailerek* véletlenszerű sorrendben történő üzenettovábbítással reagáltak. A támadók által végzett üzenetsokszorozás ellen a *remailereknek* fel kellett ismerniük az azonos üzeneteket, és csak egy példányt volt szabad elfogadniuk belőlük – ez egyébként hasznos volt a *remailerekkel* való visszaélés egyik formája, a korai „levélszemét" *(spam)* kiszűrésére is. Az útvonalfigyelés megnehezítésére a *remailereket* láncba fűzték, méghozzá oly módon, hogy minden remailer csak a láncban utána következő remailer címét ismerte, a címzettét nem. Éppen ez a technika adott még egy lehetőséget a támadóknak: az ismeretlen tartalmú és címzésű üzeneteknek a *remailer*láncon való áthaladásuk során megjósolható mértékben csökkent a mérete, hiszen a továbbításra vonatkozó „elhasznált" parancsokat törölték a továbbított üzenetből. A csökkenő méretű üzenetek követése végül elvezethetett a címzetthez. E probléma megoldására jött létre a szabványos méretű és formátumú – ún. *Mixmaster* típusú – anonim üzenetcsomag; továbbfejlesztett, harmadik generációs típusukat *MixMinion* névvel illetik.

A *remailerek* használata – lényegükből fakadóan – ingyenes; hiszen ha a szolgáltató díjat akarna szedni a felhasználóktól, akkor neki is ismernie kellene kilétüket, ez pedig a *remailerek* kompromittálhatóságát eredményezné. A *remailer* szolgáltatás használatakor először le kell kérdezni az éppen aktív *remailerek* listáját, a felhasználónak választania kell egy programot; az üzenetküldő lánc már automatikusan alakul ki. Tekintettel az olykor jelentős – szándékos – késletetésekre, a *remailerek* nem a sürgős üzenetküldés, hanem a biztonságos és bizalmas kommunikáció eszközei.

A *bioszkript*[12] olyan technológia, amely nem egyetlen felhasználói tevékenységtípus védelmére irányul; alkalmazható például a személyazonosító adatok és más személyes adatok ideiglenes szétválasztására, ún. „anonim adatbázisok" felépítésére; használható az elektronikus levelezésben vagy az elektronikus kereskedelmi szolgáltatásokban. A bioszkript létrehozásához két kiinduló adatra: egy biometrikus és egy nem biometrikus adatra van szükség. A biometrikus adat célszerűen egy ujjlenyomat digitális képe, a nem biometrikus pedig egy kriptográfiai kulcs, egy azonosító kód vagy egy mutató (pointer), de akár egy haiku is lehet. A két adat összekódolásából jön létre a bioszkript, amelyet a biometrikus adattal mint afféle kulccsal lehet felnyitni, és így lehet hozzáférni a további alkalmazáshoz szükséges nem-biometrikus adathoz. A gyakorlatban a biometrikus adat ismételt produkálása az ujjlenyomat újbóli leolvasását jelenti, s így biztosítható, hogy az alkalmazás az érintett személyek jelenlétében és feltételezett hozzájárulásukkal történjék.

[12] *Bioscrypt*, a *biometric encryption* (biometrikus rejtjelezés) kifejezésből alkotott fantázianév.

A PET-ek sokszínűségét érzékeltetendő, említést kívánnak az internetes tartalomszolgáltatók által használható *bizalmi védjegyek (trustmarks)* is. Itt a technológiai elem csupán annyi, hogy ezeket a védjegyeket a megfelelő feltételek teljesülése (általában önbevallás és a használati díj befizetése) esetén le lehet tölteni és meg lehet jeleníteni a weboldalakon. Több internetes szolgáltatói ágazat alkalmaz bizalmi védjegyeket – az elektronikus kereskedelmi szolgáltatók például számos védjegyet használnak a fogyasztói bizalom erősítésére –, de vannak kifejezetten a személyes adatok kezelésére, illetve az információs *privacy* védelmére vonatkozó bizalmi védjegyek is. A legismertebb közülük a *TRUSTe*, amelynek „.org" végződésű honlapja profitorientált szervezetet takar, és amely korábban három védjegyet is forgalmazott: az első fokozatút azok használhatták, akik egyáltalán nem rögzítették a honlapjuk látogatóinak adatait, a második fokozatút azok, akik ugyan rögzítettek adatokat, de azokat nem adták tovább más szolgáltatóknak, a harmadik fokozatút pedig azok, akik rögzítettek is és továbbítottak is, de csak meghatározott adatokat, korlátozott körben, meghatározott további szolgáltatóknak. Paradox módon – és egyben jól illusztrálva a felhasználók naivitását – az első fokozatú védjegy használóin kívül mindegyik *TRUSTe* védjegyet használó szolgáltatónak csökkent a látogatottsága, csupán azért, mert korrekt módon felhívták a figyelmet adatrögzítési, illetve -továbbítási gyakorlatukra. Azok a szolgáltatók, akik egyáltalán nem hívták fel erre látogatóik figyelmét, sőt személyes adataikat korlátlanul megosztották másokkal, nem szenvedtek forgalomcsökkenést. Ma már csak egyetlen védjegy használatos – de még ezzel is vannak problémák: kiderült például, hogy egy *spyware*-eket telepítő cég honlapján is ott szerepelt a *TRUSTe* védjegy, ami alapjában megkérdőjelezte e védjegyek használatának értelmét.[13] A bizalmi védjegyek használata ezzel együtt is figyelemfelhívó (a szolgáltatók figyelmét is ráirányítja a felhasználók védelmének fontosságára), de önmagában nem oldja meg a személyes adatok ellenőrizetlen felhasználásának problémáit.

A felsoroltak természetesen nem merítették ki az alkalmazási területek, illetve a PET-tartalmú eszközök és szolgáltatások teljes skáláját. Érdemes ellátogatni az *Electronic Privacy Information Center (EPIC)* honlapjára,[14] ahol a „Privacy Tools" cím alatt tizenhat kategóriában mintegy kétszáz link található, amelyek mindegyike kipróbált termékekre, szolgáltatásokra, illetve magánéletet védő megoldásokra mutat, még ha nem is okvetlenül sorolnánk mindegyiküket a PET-ek körébe. Az ott található felsorolás sem teljes, csupán jó válogatást és áttekintést nyújt a PET-ek köréből.

Ma több száz cég kínál az internetről közvetlenül letölthető vagy igénybe vehető saját fejlesztésű PET-tartalmú terméket, illetve szolgáltatást. E termékek és szolgáltatások funkcionalitása és minősége nagy szórást mutat. A 2001 szeptembere utáni antiterrorista intézkedések hatására a szolgáltatások célközönsége az egyéni felhasználók mellett kibővült a vállalati felhasználókkal, és számos ingyenes szolgáltatás fizetőssé vált. Ezzel együtt az *Eurobarometer* 2003-as felmérése szerint[15] a 15 „régi" EU-ország

[13] A botrányról többek között a http://www.epic.org/alert/EPIC_Alert_6.19.html címen olvashatunk; a történtek jó áttekintését adja McCarthy (1999).

[14] http://www.epic.org

[15] Special Eurobarometer, 2003, 54.

átlagában az egyéni felhasználók 18%-a ismeri és 6%-a aktívan használja a PET-tartalmú eszközöket és szolgáltatásokat; ezek az arányok az USA-ban magasabbak, Magyarországon pedig jóval alacsonyabbak.

## A technológiai háttér

E tanulmánynak nem feladata a PET-ek technológiai hátterének részletes ismertetése, azonban érdemes röviden áttekintenünk néhány jellemző megoldást. A PET-eket informálisan „egyszerű" és „bonyolult" technológiákra is felosztathatjuk: bonyolultaknak azok tekinthetők, amelyeknek az alkalmazásához speciális eszközök, szakértelem és nagy számítási kapacitás szükséges, a skála másik végén azok az egyszerű megoldások állnak, amelyeket akár két kockás füzet segítségével is meg lehet valósítani. A bioszkript például nyilvánvalóan a bonyolult, „elit" technológiák közé tartozik, saját, egyéni technológiai háttérrel és eszközökkel, míg az úgynevezett *kapcsolati kód* alkalmazásához akár még számítógép sem szükséges. A kapcsolati kód szerepe az, hogy az adatalanyokat egyértelműen azonosítsa két adatkezelés (vagy egy adatkezelés két szegmense) közötti kapcsolatban, ugyanakkor szegmentálja a személyesadat-köröket, amelyeket az egyes adatkezelők megismerhetnek. A kapcsolati kód alkalmazását egyébként a nagy állami nyilvántartások közötti adatkapcsolatban törvény is elrendeli Magyarországon,[16] de szervezeten belüli alkalmazásuk is hasznos lehet, például a személyazonosító adatoknak a többi személyes adatról való leválasztására. Az egyik adatállományban például a nevek és az egyedi kapcsolati kódok szerepelhetnek, a másikban csak a kapcsolati kódok és az érdemi adatok – így a túloldalon látszólag anonimizált egyedi adatsorokhoz juthatunk, amelyek személyes volta ugyan a kapcsolati kód segítségével bármikor helyreállítható, azonban személyes mivoltuktól ideiglenesen megfosztott formájukban alkalmasak arra, hogy kezelésük garanciákat nyújtson a személyes adatok „szükségtelen", „nemkívánatos" vagy „jogellenes" kezelése ellen.

Az anonim *remailerek* létező technológiai megoldások kombinációiból (szimmetrikus és aszimmetrikus rejtjelezés, a *remailerek* láncba fűzése, azonos üzenetek kiszűrése stb.) építették fel szabványos típusaikat, míg a bioszkript saját, innovatív technológiai megoldásokat fejlesztett ki.[17] Ugyancsak innovatív technológiai megoldásokat találhatunk a nyílt hálózaton kommunikáló zárt felhasználói csoportok tagjainak anonimitását biztosító rendszerekben. A csoport tagjai ismertek is lehetnek, mint ahogy a csoport tagjai által végzett tevékenységek összessége is, de a tagok és a tevékenységek összerendelése (például két tag kommunikációja) sem a csoporton belüli, sem azon kívüli megfigyelő számára elvben nem lehetséges. Az élővilágból vett példával érzékeltetve: egy ragadozó láthatja egy halraj minden mozgását, láthatja, hogy mekkorák a halak, de az egyedi hal megragadása nehézséget okoz számára. A gyakorlatban e rendszerek úgy teljesítik a meg-

[16] 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról.

[17] A bioszkript működésének részletes leírása magyarul is megjelent, lásd Jungbauer Alexandra és Somogyi Tamás „Bioszkript alkalmazása az elektronikus szavazásban" című tanulmányának függelékét (Jungbauer–Somogyi 2005, 269–274).

figyelhetetlenség és az összeköthetetlenség kritériumait, hogy akár a tagok és a központi szerverek közötti, akár a csoport tagjai közötti kommunikáció alkalomszerűen felépülő és lebomló útvonalakon valósul meg, rejtjelezett adatcserével, a tagok által működtetett számítógépek felhasználásával. Ilyen rendszer a *Crowds*, illetve annak új változata, a *Hordes*, valamint ilyen a hagymaszerűen egymásba ágyazott kódolási rétegeket alkalmazó *Onion Routing* és második generációs változata, a *Tor*. Akárcsak az anonim *remailereknél*, itt is az aktív résztvevők listájának lekérdezésével indul a kommunikáció, majd az egyszeri kommunikációs csatornákat a rendszer automatikusan építi fel. Ezek a rendszerek jól alkalmazhatók az anonim böngészőkben, de hasonló igény merült fel az azonnali üzenetküldő *(instant messaging)*, illetve csevegő *(chat)*-szolgáltatások terén is; itt az nehezíti alkalmazásukat, hogy a kommunikációs csatornák felépítését, lebontását, az üzenetek kódolását és dekódolását valós vagy kvázivalós időben kell megvalósítani. Ezeknél a szolgáltatásoknál ráadásul nemcsak az egyéni preferenciákat, hanem a csoportos, kollaboratív beállításokat is célszerű figyelembe venni (Gulyás 2007). Születtek már külön számítógépes nyelvek[18] is, amelyek célja szervezeti keretek között meghatározni és géppel értelmezhető módon végrehajtani a személyes adatok kezelésével kapcsolatos szabályokat az egyedi adatok szintjén.

Természetesen a PET-ek megkerülésére, kompromittálására is irányulnak fejlesztések. Ezek közé tartozik például az olyan, forgalomelemzésen alapuló eljárások alkalmazása, amelyekkel a lehallgató vagy a személyes adatok „szükségtelen", „nemkívánatos" vagy „jogellenes" felhasználását kívánó fél statisztikai módszerek segítségével következtethet a kommunikáló felek kilétére vagy az adatok és a személyek kapcsolatára. E kompromittáló fejlesztések kritikus értékelése – és következésképpen a PET-ek további javítása és ellenállóbbá tétele – a PET-kutatók és -fejlesztők standard eszköztárába tartozik. Ugyanakkor vannak olyan új vagy terjedőfélben lévő technológiák, amelyeket a szakma általában a magánéletbe behatolónak, *privacy*invazívnak tart – ilyen például a rádiófrekvenciás úton kommunikáló csipet *(RFID)* tartalmazó bélyeg, igazolvány vagy kártya, amely tulajdonosának közreműködése nélkül is leolvasható, s így ellenőrizhető tulajdonosának mozgása, a nála lévő (*RFID*-vel ellátott) pénz mennyisége, vagy akár az (*RFID*-vel ellátott) alsóneműjének színe és mérete –, egyes kutatócsoportok mégis a *privacy*védelem új, felszabadító technológiáját látják benne.[19] Véleményük szerint a felhasználó által kontrollált működésű, PET-tartalmú *RFID*-eszközök erősíteni fogják a felhasználók önrendelkezését adataik sorsa felett.

## A fejlődés iránya

Mára nyilvánvalóvá vált, hogy a felhasználók rendelkezésére álló számos egyedi, széles skálán mozgó minőségű PET-tartalmú számítógépes program és szolgáltatás alkalmazása gyakorlati problémákat vet fel. A jól bevált magánéletvédő szolgáltatások

[18] A két rivális az IBM által kifejlesztett *EPAL (Enterprise Privacy Authorization Language)* és a Sun által támogatott *XACML (OASIS sXtensible Access Control Markup Language Standard)*. Összehasonlításukat – a Sun szemszögéből – lásd Anderson (2004) prezentációjában.

[19] Lásd Stephan Engberg kutatásait (Engberg–Harning–Jensen 2004) és az azokon alapuló termékeket (http://www.priway.com). Az RFIDsec védjegyű termék 2007 novemberében elnyerte Dániában az év informatikai terméke díjat (http://www.rfidsec.com).

egyre inkább fizetőssé válnak, ami nemcsak üzletileg, de a szolgáltatások szellemét tekintve is csökkenti a felhasználók szimpátiáját, s egyúttal – mint a magánélet védelmének más eszközei esetében is – csak a művelt, jogaikat ismerő, igényes felhasználóknak van valós esélyük e szolgáltatások igénybevételére, s nem azoknak, akik amúgy is kiszolgáltatottabbak az információs erőviszonyok között. Emellett a különböző fejlesztőktől, terjesztőktől letöltött és installált programok összeakadhatnak, egymás funkcionalitását akadályozhatják, s e problémát csak részben oldják meg a többfunkciós programcsomagok. Mindehhez járul a felületes, sietős, a kényelmet és a gyorsaságot a biztonság elé helyező felhasználók tömege, akik még a saját érdekükben sem hajlandók egy kattintással többet tenni kommunikációjuk biztonságosabbá tételére.

Ez a felismerés vezetett azokhoz az elképzelésekhez, amelyek automatikusan, közműszerűen kívánják végrehajtatni és ellenőriztetni az információs rendszerekkel a privát szféra védelmére vonatkozó szabályokat, s egyúttal felhasználócentrikus beavatkozási lehetőségeket nyújtani alkalmazóiknak. A legjelentősebb ilyen vonatkozású kutatási-fejlesztési projekt az Európai Unió *PRIME (Privacy and Identity Management for Europe)* projektje.[20] Ennek erénye, hogy nemcsak technológiát fejleszt, hanem vizsgálja bevezetésének várható társadalmi és gazdasági hatásait is. Végső célja, hogy az információs rendszerekbe *egy middleware*-szerű, alkalmazás- és platformfüggetlen réteget építsen bele, amely a felszín alatt elvégzi mindazokat a teendőket, amelyeket akár a jogszabályi előírások, akár az adatkezelő önszabályozása, akár az érintett adatalanyok egyéni preferenciái meghatároznak. Ha például egy adatot az adatkezelési cél teljesülésével törölni kell, a *PRIME*-réteg automatikusan követi az adat sorsát a különböző adatkezelőknél, és gondoskodik törléséről. Amint a projekt elnevezése is utal rá, központi eleme az identitásmenedzselés. Használói e kifejezés alatt általában azt értik, hogy miként tudja ügyfeleinek adatait minél jobban menedzselni az üzleti szolgáltató vagy a hatóság. A *PRIME* ezzel szemben felhasználó-központú identitásmenedzselést kíván megvalósítani, ahol – a jogszabályi korlátok között – maguk a felhasználók határozhatják meg adataik sorsát, és annak teljesítéséről automatikus rendszerek gondoskodnak.

A négyéves projekt 2004-ben indult és 2008-ban valószínűleg új projekt keretében folytatódik; résztvevői között találhatók nagy szoftvercégek *(IBM, HP)*, nagy alkalmazók *(T-Mobile International, Lufthansa, Swisscom)* és számos kutató- és fejlesztőhely, köztük a PET-kutatásban élenjáró Karstadi Egyetem és a Drezdai Műszaki Egyetem. A *PRIME Framework* a PET-alapú identitásmenedzselés összes technológiai és nem technológiai aspektusát összegezni kívánja, és meghatározza az alkalmazások jogi, társadalmi és gazdasági kritériumainak teljes körét. A *PRIME*-architektúra különféle PET-technológiák egységes rendszerben való, alkalmazásfüggetlen felhasználását teszi lehetővé. A *PRIME*-prototípusok felhasználói és szolgáltatói oldalra egyaránt készülnek, a *PRIME*-forgatókönyvek pedig speciális alkalmazási környezetekben (például helyfüggő szolgáltatásokban, távoktatásban) tesztelik a PET-alapú identitásmenedzselés lehetőségeit.

[20] http://www.prime-project.eu

## Ösztönző és gátló tényezők – avagy kik használják a PET-eket?

Látnunk kell, hogy a PET-ek elterjedését és tömeges alkalmazását egyfelől azok az üzleti érdekek gátolják, amelyek a személyes adatoknak az adatalanyok tudta és belegyezése nélküli felhasználására, elemzésére, értékesítésére irányulnak. Az ebben érdekelt cégek technikai, szervezési, marketing- és lobbieszközökkel igyekeznek olyan helyzetet teremteni, amely csökkenti a felhasználók esélyét, igényét vagy információit a PET-ek használatára vonatkozóan. Hasonlóképpen korlátozzák a PET-ek alkalmazását a szervezett bűnözés, illetve a terrorizmus ellen fellépő hatóságok és nemzetközi szervezetek, amelyeknek természetes szövetségese a biztonságtechnikai és informatikai ipar, és ahol a korlátozás mértéke nincs közvetlen összefüggésben a fenyegetettséggel. Végül a tapasztalatok azt mutatják, hogy a nonprofit alapon felállított és független infrastruktúra működtetését igénylő PET-rendszerek tartós fenntartása pénzügyi akadályokba ütközött. Megjegyzendő, hogy az elosztott közvetítős rendszerek esetében sem jött létre eddig az a kritikus felhasználói tömeg, amely a rendszerek működésének megbízhatóságát hosszú távon garantálná.

Ugyanakkor a PET-ek elterjedését ösztönzi a demokratikus jogállamoknak, köztük az EU tagállamainak az a felismerése, hogy az IKT által felerősített hatalmi átrendeződés ellentétes ezen államok értékrendjével és alkotmányos jogrendszerével, valamint hogy a jog eszköztára – különösen a jelenlegi nemzetközi politikai viszonyok között – nem nyújt kellő védelmet a jelzett átrendeződés megállítására. Ösztönzi továbbá az ipar és kereskedelem azon felismerése is, hogy az elektronikus kereskedelmi és üzletviteli szolgáltatások tömeges elterjedésének alapvető gátja a felhasználói bizalom alacsony szintje, és ebben meghatározó a személyes adatok kezelésével kapcsolatos bizalmatlanság. A bizalom marketing útján való megszerzése általában nem járt eredménnyel, így üzleti szempontok is némi engedményre és technológiai változtatásra késztetik a jogi és etikai határokat átlépő adathasználókat. E tekintetben alapvető jelentőségű lehet az EU egységes bizalmi infrastruktúrájának kiépítése, amelyre még csak kezdeményezések léteznek, és amelynek technológiai bázisát egy szabványosított PET-rétegnek az információrendszerekbe való beépítése alkotná. Feltételezhető azonban, hogy belátható időn belül e rendszer kiépítésének csak az első fázisa valósulhat meg, így inkább bizalmi vagy PET-szigetek létrejötte valószínűsíthető.

Magyarországon a fejlett demokráciákhoz képest nyersebben és a szükséges ellensúlyok nélkül érvényesülnek azok az üzleti és hatalmi érdekek, amelyek a személyes adatok kezeléséhez, az adatalanyok feletti kontroll kialakításához fűződnek. Feltételezhető, hogy az adatalanyok körében a rendszerváltás körül közepesnek tekinthető tájékozottság adataik felhasználását illetően lényegében nem változott, azonban a tájékozottság valószínűleg nem követte az információtechnológiai változásokat, különösen a védelmi lehetőségek terén. Becslések szerint legfeljebb 1% körül van azon adatalanyok aránya, akik valamilyen PET-szerű technológiát alkalmaznak személyes számítógép-használatukban, szemben a nagyságrenddel magasabb nyugat-európai és észak-amerikai aránnyal. Ehhez járul a legújabb kutatások

szerint[21] a magyar lakosság nemzetközi összehasonlításban meglepően alacsony tudatossága és érdeklődése személyes adatainak sorsát illetően, és meglepően magas arányú elfogadási hajlandósága a magánéletét korlátozó technológiák, aktorok és módszerek iránt.

A PET-ek elterjedésének üteme Magyarországon (és az új EU-tagországokban) jelentősen lassúbbnak prognosztizálható, mint a fejlett európai demokráciákban, de várhatóan még mindig gyorsabb lesz, mint a kelet-európai régió országaiban, ahol ezek a technológiák a következő években várhatóan csak kuriózumként jelennek meg a magánfelhasználásban. Magyarországon a PET-ek használatát támogathatja az adatvédelmi jog- és intézményrendszer, valamint a professzionális informatikai oktatás színvonala, bár a lakossági használat növeléséhez a felhasználók és az adatkezelők oktatására is szükség lenne.

Magyarország szakértői szinten több európai uniós identitásmenedzsment-projektben vesz részt, köztük a *PRIME*-ban is, és több magyar kutató fejlesztett ki egymástól függetlenül nemzetközileg elismert PET-koncepciókat és -alkalmazásokat. A magyar hozzájárulás a privát szférát erősítő technológiák fejlődéséhez és elterjedéséhez azonban elsősorban nem fejlesztői, hanem alkalmazói szinten várható, kísérleti projektek, alkalmazási szigetek létrehozásával és a tapasztalatok visszacsatolásával az EU szervei felé; ehhez a meglévő szakértelem és a szabályozási környezet kedvező feltételeket nyújt.

## Hivatkozások


Anderson, Anne (2004): Privacy Policy Languages: XACML vs EPAL. *5th Annual Privacy & Security Workshop*, 29 October 2004.
http://www.cacr.math.uwaterloo.ca/conferences/2004/isw/slides/AnneAndersonpresslides.pdf

van Blarkom, G. W. – Borking, J. J. – Olk, J. G. E. (eds.) (2003): *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents.* College bescherming persoonsgegevens, The Hague.

Engberg, Stephan J. – Harning, Morten B. – Jensen, Christian Damsgaard (2004): Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. In: *The Second Annual Conference on Privacy, Security and Trust – PST.* New Brunswick, Canada, October 2004.

Gulyás Gábor György (2006): Anonim-e az anonim böngésző? Technológiák és szolgáltatások elemzése. In: *Alma Mater sorozat az információ- és tudásfolyamatokról 10.* Budapest, 2006. március, BME GTK Információ- és Tudásmenedzsment Tanszék.

Gulyás Gábor György (2007): Az anonimitás és a privacy kérdései a csevegőszolgáltatásokban. In: *Tanulmányok az információ- és tudásfolyamatokról 11.* Budapest, 2007. május, BME GTK Információ- és Tudásmenedzsment Tanszék, 137–157.

Hullám Gábor (2005): A web bug technológia – barát vagy ellenség? In: Székely Iván – Szabó Máté Dániel (szerk.): *Szabad adatok, védett adatok.* Budapest, 2005. március, BME GTK Információ- és Tudásmenedzsment Tanszék, 211–233.


[21] A Queen's Egyetem (Kingston, Kanada) által vezetett *Surveillance Project* keretében nyolc ország (Brazília, Egyesült Államok, Franciaország, Kanada, Kína, Magyarország, Mexikó, Spanyolország) kilencezer lakosának megkérdezésével végzett felmérés eredményeinek publikálása előkészületben van.

Jungbauer Alexandra – Somogyi Tamás (2005): Bioszkript alkalmazása az elektronikus szavazásban. In: Székely Iván – Szabó Máté Dániel (szerk.): *Szabad adatok, védett adatok*. Budapest, 2005. március, BME GTK Információ- és Tudásmenedzsment Tanszék, 235–274.

Koom, Ronald et al. – Borking, John (2004): *Privacy-Enhancing Technologies. White Paper for Decision-Makers*. KPMG Information Risk Management.

McCarthy, Jamie (1999): TRUSTe Decides Its Own Fate Today. http://yro.slashdot.org/yro/99/11/05/1021214.shtml?tid=95

Special Eurobarometer 196, Wave 60.0, *Data Protection*, European Opinion Research Group EEIG (September 2003).