

# 19. PRIVÁT SZFÉRÁT ERŐSÍTŐ TECHNOLÓGIÁK (PET-EK)

Székely Iván

*A személyiségi jogokat technológiai eszközökkel is védő újabb egyedi módszerek kifejlesztését felváltja a PET-ek rendszerszerű alkalmazása és szabványos réteggént való beépülése az informatikai rendszerekbe.*

## **1. Megnevezés és rövid leírás**

Az információs társadalom technológiáinak alkalmazásszintű felhasználása számottevő részben azonosítható természetes személyekre vonatkozó, vagy velük kapcsolatba hozható adatok kezelésével történik. Az adatok gyűjtésére, továbbítására, elemzésére és felhasználására jellemzően az adatalányok tudta és beleegyezése nélkül kerül sor, és ez megfosztja az adatalányokat az adataik sorsa feletti rendelkezés lehetőségétől, leszűkíti társadalmi, gazdasági, politikai tevékenységükben a racionális választási lehetőségek körét. Ez a jelenség és problémakör szorosan összefügg az új személyazonosítási technikák alkalmazásával.

A jogi szabályozás késve követi a technológiai fejlődést és önmagában nem is elegendő a problémák megoldására, ezért jöttek létre a privát szférát technológiai oldalról erősítő speciális technológiák (PRIVACY ENHANCING TECHNOLOGIES, PET). A PET-ek jelentősége növekvőben van, s a vizsgált időszakban elsősorban nem újabb megoldások kifejlesztése várható, hanem a PET-ek integrálása az identitás-menedzselésbe, illetve szabványos réteggént való beépülésük az informatikai alkalmazásokba.

## **2. Jelenlegi helyzet**

A PET-ek olyan információs és kommunikációs technológiák, amelyek a korszerű IKT és az azon alapuló szolgáltatások funkcionalitását *megőrizve* biztosítják, hogy a személyes adatokat csak bizonyíthatóan törvényes és tisztességes célokra, a célokhoz szükséges és elégséges mértékben kezeljék, illetve, hogy az adatalányok rendelkezhessenek adataik sorsáról. A rendeltetésszerűen használt PET-ek mindig a gyengébb felet – jellemzően az adatalányt – védik az információs túlhatalommal bíró féllel szemben. Ez a túlhatalommal bíró fél lehet az államigazgatás valamely szervezete, lehetnek az üzleti szektor szervezetei, de magánszemélyek, illetéktelen

harmadik fél típusú megfigyelők és – elsősorban az internetes kommunikációban – több szervezetet magába foglaló közös adathasználó hálózatok is.

A PET-ek alapvető céljukat általában négy kritérium: az ANONIMITÁS, a PSZEUDONIMITÁS, a megfigyelhetetlenség (unobservability) és az összeköthetlenség (unlinkability) teljesítésével érik el. Aktív internethasználó esetében mind a négy kritérium jelentőséggel bír; passzív (nem közreműködő) adatalany esetében csak az első kettő. A PET-ek változatos technológiákat tartalmaznak: a Burkert-féle osztályozás szerint léteznek az adatalany személyét védő szubjektum-orientált technológiák, az eszközre összpontosító objektum-orientált technológiák, a hálózati tranzakciók adatkezeléseit korlátozó tranzakció-orientált, illetve rendszer-orientált technológiák. Egy másik osztályozás szerint vannak technológia-orientált PET-ek (például a mix net alapon működő rendszerek, mint az onion routing) és humán interakció orientált PET-ek (például a World Wide Web Consortium által kifejlesztett P3P, Platform for Privacy Preferences). Ismét más osztályozás szerint léteznek egyrésztvevős PET-ek (pl. vállalati privacy menedzsment rendszerek), központosított közvetítős rendszerek (pl. az Anonymizer), elosztott közvetítős rendszerek (Crowds, Freedom Network) és szerver-támogatású rendszerek (digitális pénz).

Kutatási konjunktúra (a későbbi technológiák és működő rendszerek alapjait képező matematikai, kriptográfiai, számítástechnikai megoldások kifejlesztése) elsősorban az 1980-as évtizedben, majd az ezredforduló körül, illetve az elmúlt egy-két évben volt tapasztalható. Az alkalmazások kifejlesztésének konjunktúrája az 1990-es évekre esett, zömében amerikai kezdeményezésre, amit ösztönzött az a próbálkozás, hogy az USA a személyes adatok kezelése terén ún. adekvát védelmi szintet érjen el az EU normái szerint.

Az 1990-es évekre kifejlesztett és termékek, szolgáltatások alapját képező PET-ek közé tartoznak az I., majd a II. típusú anonim remailerek, a web PROXY-k, a BIOSCRYPT, a digitális pénzrendszerekben alkalmazott számos protokoll, például a vak aláírás. A szolgáltatások szintjén megjelentek az anonim böngészők, a nym-generatorok, az elektronikus levelezés bizalmasságát biztosító szolgáltatások, a SÜTI (COOKIE) irtók, a kémprogram (SPYWARE) irtók, a webpoloska (web bug) irtók, személyes használatra tervezett adat- és hangrejtjelzők, a távoli ügyfélről gyűjtött adatok kezelését szabványosított alkufolyamattá alakító szolgáltatások, az elektronikus (kis)kereskedelemben az ügyfél, a bolt és a bank közötti kapcsolatot adatvédelmi szempontból kezelő szolgáltatások, anonim vagy részlegesen anonim digitális fizetési rendszerek, sőt ide sorolhatók a spam- és webreklám-szűrők és a személyes adatok kezelésére vonatkozó bizalmi védjegyek (trustmark) is. Megjelentek továbbá a személyes, illetve vállalati használatra kifejlesztett PET tartalmú és célú szolgáltatáscsomagok is, amelyek alkalmazása részben megoldja a több különböző fejlesztésű program egyetlen végberendezésre való telepítéséből adódó kompatibilitási és együttműködési problémákat.

Ma mintegy kétszáz 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. utáni anti-terrorista intézkedések hatására a szolgáltatások célközönsége az egyéni felhasználók mellett kibővült a vállalati felhasználókkal, és számos ingyenes szolgáltatás fizetősé vált. Ezzel együtt az Eurobarometer 2003-as felmérése szerint a 15 „rég” EU ország átlagában az egyéni felhasználók 18 százaléka ismeri és 6 százaléka aktívan használja

a PET tartalmú eszközöket és szolgáltatásokat; ez az arány alacsonyabb az USA adatainál és jóval magasabb a magyar adatokénál.

### 3. A várható fejlődés eredményének jellemzése

Már az ezredforduló körül látható volt, hogy új elven működő PET technológiák, illetve új megoldásokat alkalmazó szolgáltatások kifejlesztése rövid- és középtávon nem várható, a jelenlegi kutatások és fejlesztések inkább a meglévők tökéletesítésére, biztonságosabbá tételére, bizonyíthatóságára, támadások elleni védelmére irányulnak. Várható azonban a PET-ek rendszerbe állítása, szabványosítása és kísérlet szabványos réteggé váló beépítésükre az informatikai alkalmazásokba és rendszerekbe.

Jelentős felismerés, hogy az 1970-es és 80-as évek jogközpontú megoldási koncepciói és a 90-es évek – főként USA-beli – technológia-központú koncepciói után olyan új koncepciókat kell kidolgozni a személyes adatok megfelelő kezelésének biztosítására, amely a PET technológiákat jogi, társadalmi, kulturális és szervezeti szintű rendszerekkel szerves egységben alkalmazza. Más szóval: önmagában a technológia sem oldja meg a személyes adatok kezelésével kapcsolatos problémákat.



1. ábra: Várható fejlődés 2005-2015

Az önálló alkalmazások szintjén végzett kutatások és fejlesztések eredményei többek között a helyi hálózatokon alkalmazható PET-ek (pl. protokoll-anonimizálás), a matematikai bizonyíthatóság fejlesztése, a támadások elleni védelem erősítése, a fair anonim rendszerek, illetve a vállalati szintű adatkezelést támogató alkalmazások területén fognak megjelenni. A vizsgált időszakban várható, hogy a kis úttörő cégeket követő néhány eddigi nagy multinacionális szoftverfejlesztő után a többi nagy cég is megjelenik saját PET szolgáltatásokat nyújtó rendszerével, elsősorban saját vállalatirányítási rendszereibe való integrálás céljára.

Az egységes vállalati szintű privacy menedzsment rendszerek elterjedése elsősorban a fejlett adatvédelmi kultúrával rendelkező országokban (pl. Németország) várható. Ilyen célra szolgálnak például az IBM Enterprise Privacy Application Language (EPAL) alapján kifejlesztett rendszerek.

Három területen esélyes a PET-ek szervezeti határokon túlnyúló rendszerbe állítása: az identitás-menedzsmentben, amely az EU egyik támogatott fejlesztési iránya, a digitális pénz alapú fizetési rendszerekben (amennyiben a szolgáltatók érvényesíteni tudják önálló üzleti koncepcióikat a pénzügyi szervezetekkel szemben, az áttörés elsősorban a mikrofizetések terén lehetséges; ezek között vannak PET tartalmúak is), valamint a cégalapú bizalmi rendszerek válságát (ld. TRUSTe) megoldani kívánó, megbízható rendszerek, intézmények, eljárások kifejlesztésére irányuló EU kísérletekben; ezek közé tartoznak a PET tartalmúak is. Kérdéses a PET-ek alkalmazása a digitális jogkezelés (DRM) területén; a mikrofizetési rendszerek ott is elterjedhetnek, de a PET elem nem hangsúlyos, bár beépíthető lenne.

Az EU az i2010 programja részeként várhatóan 2006-os közzététellel e-government munkatervet készít, amelynek egyik kitűzött célja, hogy a tagországok 2010-re biztosítsák a személy- és dokumentumhitelesítés átjárhatóságát. Ennek megvalósítása nagyban érinti a személyes adatok kezelésének célhoz kötöttségi problémáit, valamint az adatok sorsának az adatalany általi átláthatóságát, az adatok feletti önrendelkezés érvényesíthetőségét. Adatvédelmi szempontból előnyös fejlemény, hogy az átjárhatóságot a jelenlegi elképzelések szerint nem centralizált, hanem „szövetségi” rendszerben kívánják megvalósítani. Az elektronikus kormányzati eljárások és szolgáltatások fejlesztése azonban gyakran párhuzamosan és nem összehangoltan történik a privátszférát erősítő technológiákkal, mind jogszabályi, mind technológiai szinten; ez a megállapítás érvényes a magyar viszonyokra is.

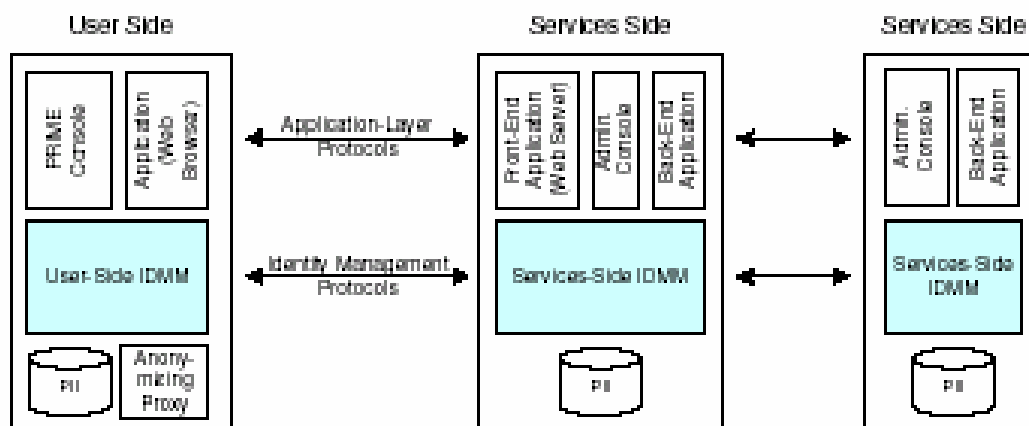
A privátszférát erősítő technológiák fejlesztésének egyik fő iránya az alkalmazásfüggetlen PET rendszerek és architektúrák létrehozása. Ilyen fejlesztések több egyetemen (pl. Karlstad, Drezda, Leuven, Aachen, Milano) és kutatóhelyen (pl. IBM Zürich, Centre National de la Recherche Scientifique [Franciaország], Joint Research Centre [Olaszország]) folynak, elsősorban az EU tagállamaiban.

#### **4. Szükséges technológiai előfeltételek**

A PET-ek fejlett, rendszerszerű alkalmazásának technológiai előfeltétele egyfelől a megfelelő számítástechnikai kapacitás (a kezdeti alkalmazások irreális számítási igénye ugyan megszűnt, de a PET-ek alkalmazása a számítási igény növekedését eredményezheti), másfelől a rendszerek kompatibilitásának biztosítása, közös informatikai infrastruktúrák létrehozása és működtetése.

## 5. Folyamatban lévő kutatások, fejlesztések

A jelenleg futó legjelentősebb PET vonatkozású európai uniós projekt a PRIME (Privacy and Identity Management for Europe).<sup>61</sup> A négyéves projekt 2004-ben indult, mintegy 20m euro közvetlen forrásból gazdálkodhat; résztvevői között található nagy szoftvercégek (IBM, HP), nagy alkalmazók (T-Mobile International, Lufthansa, Swisscom) és számos kutató és fejlesztőhely. A PRIME Framework a PET alapú identitás-menedzselés 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 történő, alkalmazásfüggetlen felhasználását teszi lehetővé. A PRIME Prototípusok felhasználói és szolgáltatói oldalra egyaránt készülnek, a PRIME forgatókönyvek pedig speciális alkalmazási környezetben (például repülőtéri biztonsági rendszerekben, távoktatásban) tesztelik az PET alapú identitás-menedzselés lehetőségeit.



2. ábra: A PRIME architektúra általános szintje  
(forrás: PRIME White Paper, 2005 július)

Észak-Amerikában a PET technológiákat más területekkel összefüggésben vizsgáló, integráló jellegű projektek közül kiemelkedik az „On The Identity Trail” című, amely kanadai vezetéssel észak-amerikai és nyugat-európai kutatókat és kutatóhelyeket tömörít. Három kutatási főiránya közül az első az ANONIMITÁS, az identitás és az autentikálás természetét vizsgálja, a második az alkotmányossági, jogi és politikai aspektusokra összpontosít, a harmadik pedig anonimizáló, azonosító, illetve hitelesítő technológiákat értékeli, illetve fejleszt.

Nemzetközi, „network of excellence” típusú szakmai műhely a Petworkshop, amely a PET-ek matematikai, kriptográfiai és számítástechnikai alapjainak legkiválóbb kutatóit, illetve kutatóhelyeit tömöríti és kutatási eredményeiről évi konferenciáin számol be. 2005. évi konferenciájukat Horvátországban rendezték, ami a régió felé nyitás (avagy a régió fogadókészsége) jeleként is értelmezhető.

<sup>62</sup> <http://www.prime-project.eu.org>

## **6. Az IKT más területeire való hatások bemutatása**

A PET-ek elterjedése minden olyan IKT alkalmazási területre hatással van, ahol azonosítható személyekkel kapcsolatba hozható adatok kezelése történik, például a közigazgatásban használt informatikai rendszerekre, az üzleti szféra adatkezeléseire, illetve az infrastruktúra-szerűen használt internetes szolgáltatásokra. Ezek a hatások azonban nem közvetlenül a technológiára, hanem azok alkalmazási környezetére vonatkoznak. A PET-ek használata ösztönzi az alkalmazások, illetve informatikai rendszerek közötti interoperabilitást, és várhatóan ösztönzi az alkalmazásfüggetlen PET rendszerek kifejlesztését.

A PET-ek használata ezen felül ösztönzi a matematikai és kriptográfiai kutatásokat és új szempontrendszert jelenthet az informatikai rendszerek architektúráinak tervezésében. Speciális kutatásokat, illetve hatásokat elsősorban a hitelesítési és azonosítási célú technológiák, illetve a biometrikus azonosító rendszerek területén (pl. BIOSCRYPT) indukálhat.

## **7. Társadalmi-gazdasági hatások elemzése**

Az információs javak – köztük a személyes adatok – sajátos tulajdonságai miatt az adatalany kontrollja alól kikerült információk útja és felhasználhatóságuk lehetőségei a korszerű IKT közegében gyakorlatilag követhetetlenek. Ez a fejlemény a társadalom mikro- és makroszintjein hatalmi eltolódást okozott, a nagyobb adatszerző és -elemző lehetőségekkel rendelkező fél kezében egyre nagyobb képesség összpontosul érdekeinek érvényesítésére, az adatalanyok befolyásolására. Tekintettel az információs rendszerek tervezőinek, fejlesztőinek és üzemeltetőinek érdekviszonyaira, az informatikusok többsége (régiónk új demokráciáiban a túlnyomó többsége) számára a szakmai és anyagi érvényesülés egyedüli útja az „erősebb felek” megbízásainak teljesítése. Ezért az általuk kifejlesztett rendszerek többsége is az erősebb fél (az adatkezelő) érdekeit tükrözi. A PET-ek nem a már kifejlesztett és alkalmazott rendszerek, szolgáltatások működését gátolják, hanem azokat az adatalany érdekeit tükröző (és azok érvényesítését lehetővé tevő) elemekkel egészítik ki.

A PET-ek elterjedését és tömeges alkalmazását gátolják egyfelől azok az üzleti érdekek, amelyek a személyes adatoknak az adatalanyok tudta és beleegyezése nélküli felhasználására, elemzésére, értékesítésére irányulnak. Az ebben érdekelt cégek technikai, szervezési, marketing- és lobbierővel 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, amelyek természetes szövetségese a biztonságtechnikai és informatikai ipar, és ahol a korlátozás mértéke nincs közvetlen összefüggésben a fenyegetettséggel. Végül, a tapasztalatok azt mutatják, hogy azon PET rendszerek esetében, ahol

független infrastruktúra működtetésére van szükség, és ezeket nonprofit alapon állították fel, ott ezek tartós fenntartása pénzügyi akadályokba ütközött. Megjegyzendő, hogy az elosztott közvetítés rendszerek esetében sem jött létre eddig az a kritikus felhasználói tömeg, amely a rendszerek működésének megbízhatóságát hosszú távon garantálná.

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 ezen átrendeződés megállapítására. Ösztönzi továbbá az ipar és kereskedelem azon felismerése, 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 úton történő megszerzése általában nem járt eredménnyel, így üzleti szempontok is némi engedményre és technológiai változtatásra készítik az 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 bázisa lenne egy szabványosított PET réteg beépítése az információrendszerekbe. Feltételezhető azonban, hogy a vizsgált időszakban e rendszer kiépítésének csak az első fázisa történhet meg, így bizalmi vagy PET szigetek létrejötte valószínűsíthető.

## **8. Magyar vonatkozások**

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

A PET-ek elterjedésének üteme Magyarországon (és az új EU-tagországokban) jelentősen lassabbnak prognosztizálható, mint a fejlett európai demokráciákban, de még mindig magasabbnak, mint a kelet-európai régió országaiban, ahol ezek a technológiák a vizsgált időszakban 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 identitás-menedzsment projektben részt vesz, köztük a PRIME-ban is, és több magyar kutató fejlesztett ki egymástól függetlenül nemzetközileg elismert PET koncepciókat és alkalmazásokat. A magyar

hozzájárulás a privátszférát erősítő technológiák fejlődéséhez és elterjedéséhez azonban elsősorban nem fejlesztői, hanem alkalmazói szinten várható; pilot projektek, alkalmazási szigetek létrehozásával és a tapasztalatok visszacsatolásával az EU szervei felé. Ehhez a meglévő szakértelem és a szabályozási környezet kedvező feltételeket nyújt.

## **9. Következtetések**

A PET-ek alkalmasak arra, hogy a korszerű IKT alkalmazások funkcionalitásának megőrzése mellett javítsanak az adatalanyok információs státuszán. Jelentőségük nőni fog a vizsgált időszakban, bár nem a tömeges elterjedésük révén. Megjelennek a PET-eket alkalmazásfüggetlen szabványos réteggként tartalmazó rendszerek; ezek használatát az EU várhatóan támogatni fogja, de még kérdéses, hogy ki viseli a közös infrastruktúra kiépítésének és működtetésének költségeit. Magyarországot az alacsony felhasználói tudatosság, de kedvező szabályozási környezet és a megfelelő szakértelem megléte jellemzi; nemzetközi szerepvállalásunk elsősorban alkalmazói szinten várható.