A privátszférát erősítő technológiák

Székely Iván

A Nemzeti Hírközlési és Informatikai Tanács (NHIT) „Információs Társadalom Technológiai Távlatai" (IT3) projektjének munkaanyaga[*]

Tézis: *A magánélet védelmét technológiai eszközökkel biztosító újabb egyedi módszerek kifejlesztését felváltja a PET-ek rendszerszerű alkalmazása és szabványos rétegként való beépülése az informatikai rendszerekbe.*

1. A témakör

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 adatalanyok tudta és beleegyezése nélkül kerül sor, és ez megfosztja az adatalanyokat 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 információs és kommunikációs technológiák (IKT)[1] és ezen belül az személyazonosítási technikák alkalmazásával.

A jogi szabályozás késve követi a technológiai fejlődést és önmagában nem is elegendő e problémák megoldására, ezért jöttek létre a privátszférát technológiai oldalról erősítő speciális technológiák (Privacy Enhancing Technologies, PET). A PET-ek jelentősége növekvőben van, s a vizsgált időszakban[2] elsősorban nem újabb megoldások kifejlesztése várható, hanem a PET-ek integrálása az identitásmenedzselésbe, illetve szabványos rétegként való beépülésük az informatikai alkalmazásokba.

2. A 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 adatalanyok rendelkezhessenek adataik sorsáról. 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. A rendeltetésszerűen használt PET-ek mindig a gyengébb felet

[*] A projekt munkaanyagai elérhetők a www.nhit-it3.hu honlapon. A tanulmány szerkesztett változata megjelent az *Égen-földön informatika – Az információs társadalom technológiai távlatai* c. kötetben (Typotex, 2008.)

[1] Lásd erről például az EPTA (Europan Parliamentary Technology Assessment) 2006. októberi jelentését „ICT and Privacy in Europe" címmel.

[2] Az IT3 projekt jelenlegi szakaszában a 2008–2018 közötti időszak technológiai távlataival foglalkozik.

– jellemzően az adatalanyt – védik az információs túlhatalommal bíró féllel szemben.[3] 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 korszerű PET-ek lényege az alábbi definíciókkal ragadható meg:

> „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."[4] (Koom *et al.* – Borking, 2004: 68)

> „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."[5] (van Blarkom – Borking – Olk, 2003: 33)

Ez utóbbi meghatározás a privátszférát 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.)

A PET megnevezés a technológiák szerteágazó csoportját fedi le, ennélfogva csoportosításuk is többféleképpen lehetséges. A legismertebb és egyúttal leginkább spekulatív jellegű csoportosítás Herbert Burkert nevéhez fűződik;[6] Burkert szerint 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.

[3] 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.

[4] A holland Alkalmazott Tudományos Kutatások Intézetének meghatározása.

[5] „A *privacy* és a privátszférát erősítő technológiák kézikönyve" meghatározása.

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

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.

Csoportosíthatók a PET-ek aszerint is, hogy melyik adatvédelmi alapelv[7] érvényesülését segítik elő. Egy további osztályozás szerint léteznek egyrésztvevős PET-ek (például a vállalati privacy-menedzsment rendszerek), központosított közvetítős rendszerek (például az *Anonymizer*), elosztott közvetítős rendszerek (*Crowds, Freedom Network*) és szerver-támogatású rendszerek (PET tartalmú digitális pénzrendszerek).

Ismét más felosztást eredményez, ha aszerint különböztetjük meg e technológiákat, hogy „technológia-alapúak", vagy „humán interakció" 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[8] elköltésével, forgatásával a pénzforgalomban részt vevő aktorok ne ismerhessék meg illetéktelenül a pénz birtoklójának, elköltőjének szokásait, ne következtethessenek anyagi helyzetére, ízlésére.[9] 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. 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. A szolgáltatók is hasonlóképpen meghatároznák

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

[8] 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.

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

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.[10]

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.

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 néhány 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 elektronikus levelezés illetéktelen harmadik fél általi lehallgathatóságát és követhetőségét megakadályozni hivatott I., majd II. típusú anonim remailerek,[11] az anonim böngészést lehetővé tevő web proxy-k, a speciális biometrikus rejtjelezést tartalmazó bioszkript (bioscrypt), valamint a digitális pénzrendszerekben alkalmazott számos protokoll, például a vak aláírás. A szolgáltatások szintjén megjelentek az anonim böngészők, a nymgenerátorok, az

[10] A valóságban a P3P-nek egy egyszerűsített változata valósult meg, amelyben a felhasználók nem határozzák meg saját profiljukat, csupán megnézhetik a szolgáltató profilját (ha a szolgáltató egyáltalán használja a P3P szabványos profil-meghatározó 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.

[11] Más elnevezéssel Cypherpunk és Mixmaster osztályú remailerek. (Jelenleg a III. típusú, ún. Mixminion remailerek képviselik a fejlesztés és az alkalmazások élvonalát.)

elektronikus levelezés bizalmasságát biztosító szolgáltatások, a süti (cookie) irtók, a kémprogram (spyware) irtók, a webpoloska (web bug) irtók és detektorok, 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 többszáz cég kínál az internetről közvetlenül letölthető vagy igénybe vehető saját fejlesztésű PET tartalmú terméket, illetve szolgáltatást. Az *Electronic Privacy Information Center* (*EPIC*) honlapján[12] például a „*Privacy Tools*" cím alatt tizenhat kategóriában mintegy kétszáz link található, amelyek mindegyike kipróbált termékekre, szolgáltatásokra, illetve magánélet-védő megoldásokra mutat, még ha nem is okvetlenül sorolnánk mindegyiküket a PET-ek körébe. E termékek és szolgáltatások funkcionalitása és minősége nagy szórást mutat. A 2001. 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 a 15 „régi" EU ország átlagában az egyéni felhasználók csupán 18 százaléka ismerte és 6 százaléka használta aktívan a PET tartalmú eszközöket és szolgáltatásokat; ezek az arányok ebben az időszakban az USÁ-ban magasabbak, Magyarországon pedig jóval alacsonyabbak voltak. Az Eurobarometer 2008. tavaszi vizsgálata azonban a helyzet alapvető változását mutatja: ugyanebben a 15 országban azok aránya, akik ismerik a PET eszközöket és szolgáltatásokat, 18-ról 43 százalékra (Portugáliában 64 százalékra) ugrott, az aktív használók aránya pedig 6 százalékról 25 százalékra (Dániában 49 százalékra). Kedvező fejlemény, hogy e vizsgálat szerint Magyarországon a PET-eket ismerők aránya elérte az 51 százalékot, az aktív használóké pedig a 18 százalékot.[13]

3. Folyamatban lévő kutatások, fejlesztések

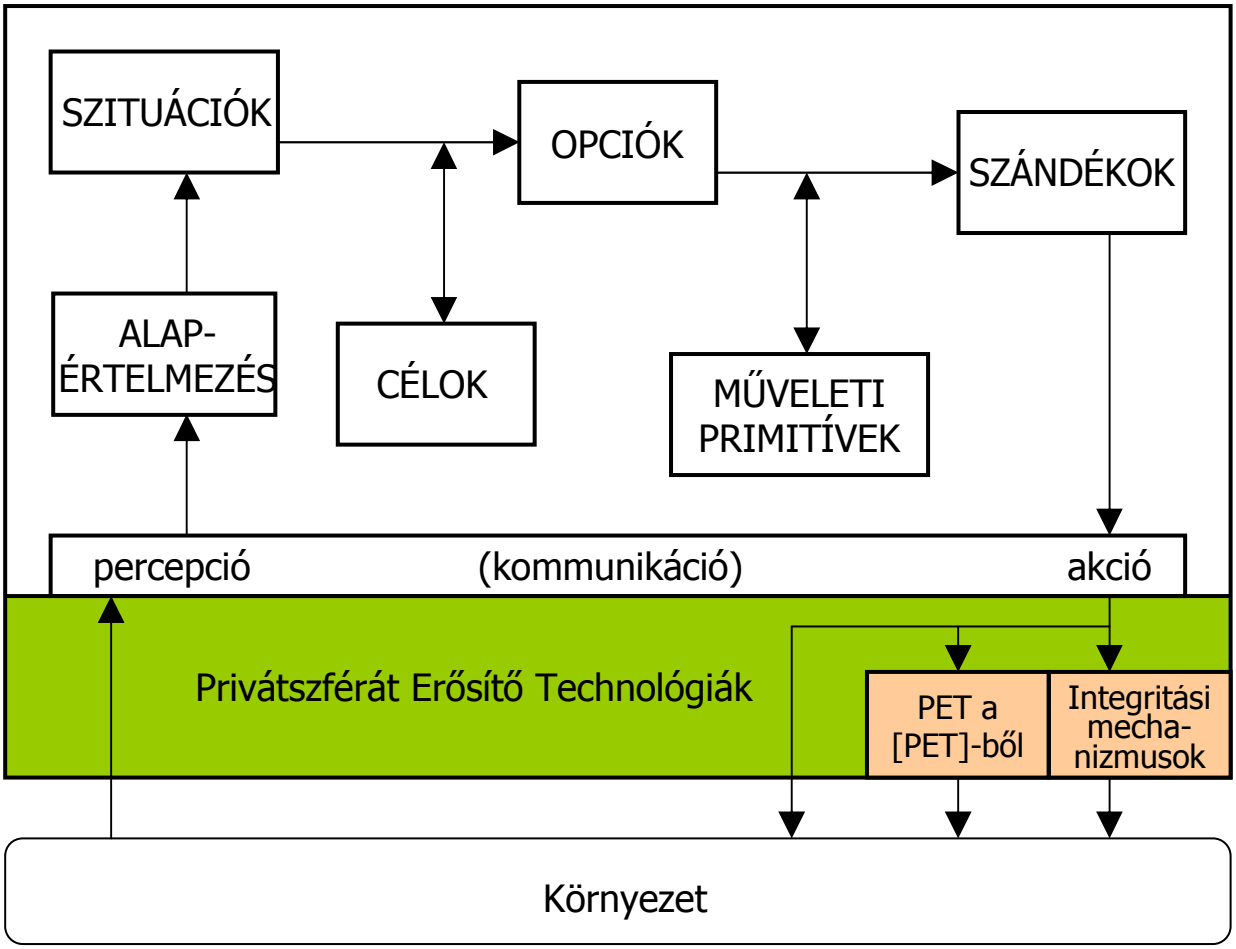
A jelenleg futó legjelentősebb PET vonatkozású európai uniós projekt a PRIME (Privacy and Identity Management for Europe)[14], illetve utóda, a PrimeLife (Privacy and Identity Management in Europe for Life)[15].

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

[13] A tendenciák egyértelműek, azonban a számszerű adatok értékelésénél nem szabad megfeledkezni a módszertani problémákról, köztük arról, hogy az Eurobarometer vizsgálatai minden védelmi eszközt – akár egy egyszerű tűzfalat is – ebbe a kategóriába sorolnak.

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

[15] http://www.primelife.eu

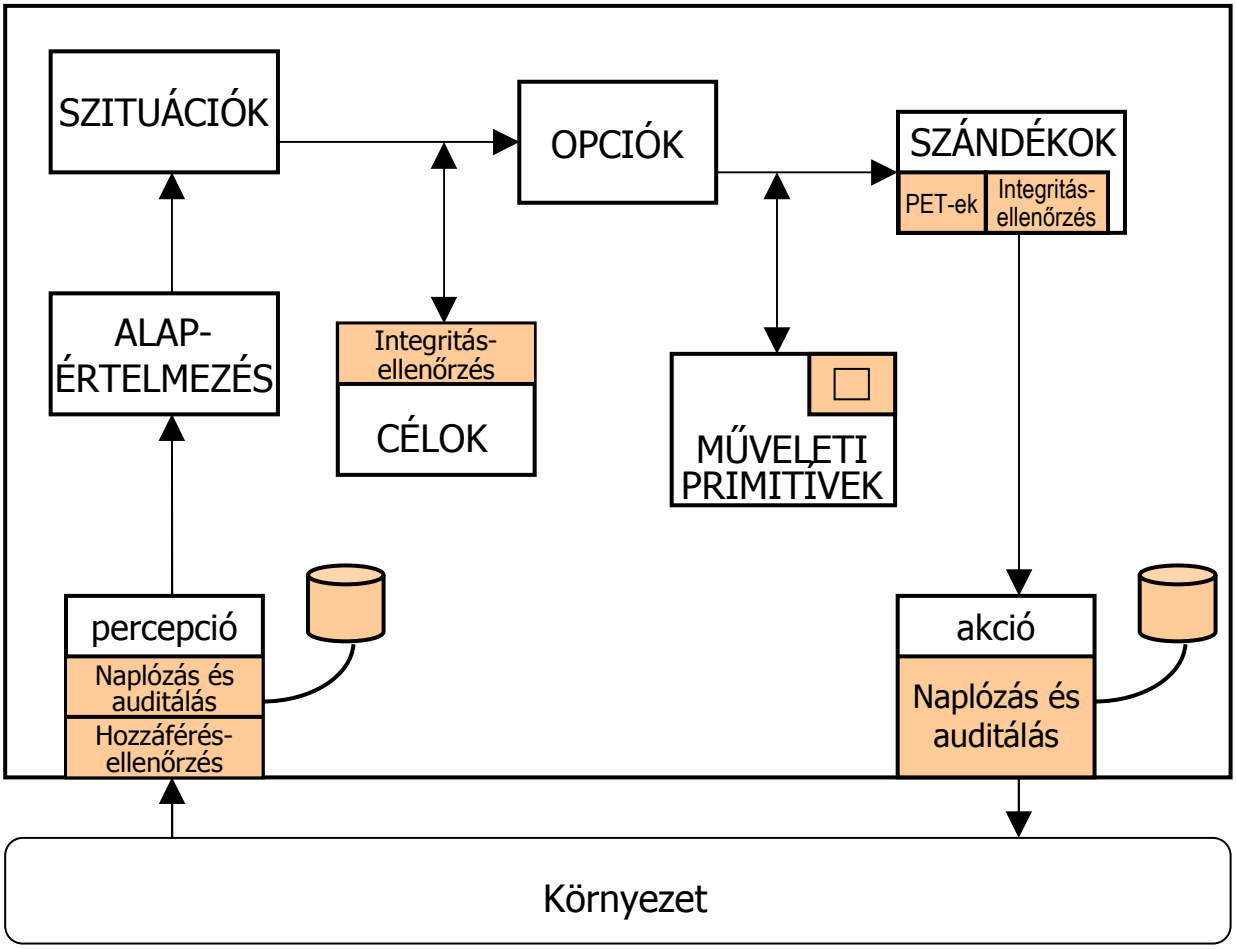


Intelligens ágens köré épített PET
(van Blarkom – Borking – Olk 2003 nyomán)

Koncepcionális értelemben a PRIME projektek előfutárának tekinthető a privacy-tartalmú szoftverágens, a PISA (Privacy Incorporated Software Agent) kifejlesztése, amely speciális intelligens ágensként képes a felhasználó képviseletében automatikus feladatvégrehajtásra komplex hálózati környezetben oly módon, hogy minimalizálja, illetve a feladat végrehajtásához szükséges és elégséges mértékűre csökkentse a felhasználó személyes adatainak kezelését. Ez a koncepció jelentős előrelépést jelentett a statikus identitás-védő (Identity Protector) alkalmazásokhoz képest.

A PRIME projektek végső célja, hogy az információs rendszerekbe egy middleware-szerű, alkalmazás- és platform-független réteget építsenek 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 a törléséről. Amint a projekt elnevezése is utal rá, központi eleme az

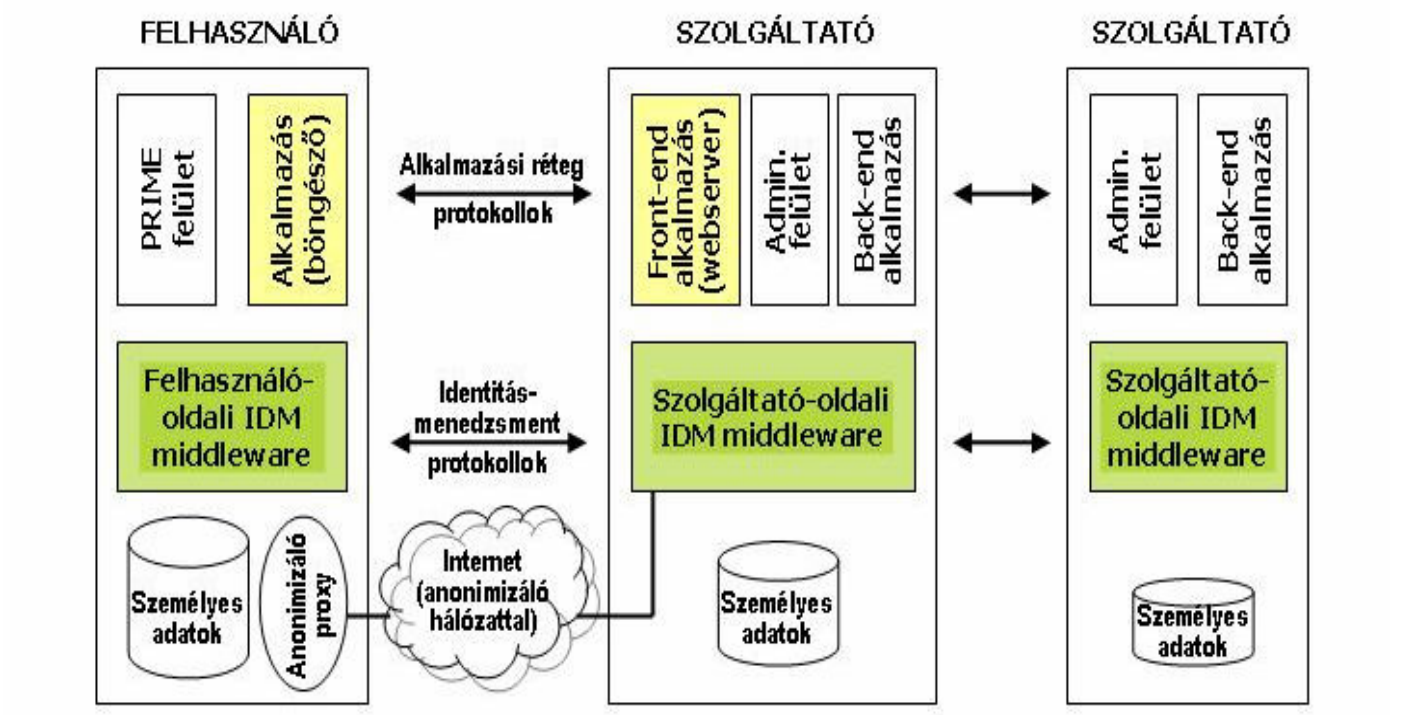
identitásmenedzselés. E kifejezés alatt általában azt értik használói, hogy miként tudja ügyfeleinek adatait minél jobban menedzselni az üzleti szolgáltató vagy a hatóság. A PRIME ezzel szemben *felhasználó-központú identitásmenedzselést* kíván megvalósítani, ahol – a jogszabályi korlátok között – maguk a felhasználók határozhatják meg adataik sorsát, és annak teljesítéséről automatikus rendszerek gondoskodnak.



Intelligens ágensbe integrált PET
(van Blarkom – Borking – Olk 2003 nyomán)

A négyéves projekt 2004-ben indult; 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 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 környezetekben (például helyfüggő szolgáltatásokban, távoktatásban) tesztelik az PET alapú identitás-menedzselés lehetőségeit.



A PRIME architektúra általános szintje

A PRIME az előre definiált szabályok és a felhasználó preferenciáit tükröző szabályok automatikus végrehajtása mellett szerep-alapú privacy-védelmet (Role-Based Privacy, RBP) valósít meg. Ezzel voltaképpen a virtuális világban leképezi a „digitális személyiségek" számára azokat szerepeket, amelyeket az egyének, mint különböző társadalmi kontextusok résztvevői a valós életben betöltenek, például egyszer édesapák, máskor tanár urak, kedves vevők, gyerekkori osztálytársak, üzleti tárgyalópartnerek vagy köztisztviselők – és mindegyik szerepükhöz más személyes adataik kezelése indokolt, más adataiké pedig nem.[16] Ehhez pedig a különböző adatkezelési kontextusok felismerése és kontextus-függő adatkezelési aktusok végrehajtása szükséges.

Nemzetközi, „network of excellence" típusú szakmai műhely a korábban Petworkshop, jelenleg Petsymposium néven futó rendezvénysorozat,[17] amely a PET-ek matematikai, kriptográfiai és számítástechnikai alapjainak legkiválóbb

[16] És természetesen nem azért, mert bármilyen „félnivalójuk" vagy „titkolnivalójuk" lenne, ahogyan a különböző kontextusokból származó személyes adatok összekötésében, a profilépítésben és felhasználásban érdekelt felek érvelni szoktak.

[17] http://www.petsymposium.org

kutatóit, illetve kutatóhelyeit tömöríti és kutatási eredményeiről évenkénti konferenciáin számol be. Kutatási eredményeiket évente könyv formájában is kiadják;[18] számos tanulmányuk elektronikus formátumban is elérhető. (2005. évi konferenciájukat Horvátországban rendezték, ami a régiónk felé nyitás – avagy a régió fogadókészsége – jeleként is értelmezhető.)

A kutatások egyik aktuális vonulatát képezi a helyfüggő szolgáltatások magánszféra-védelmi aspektusainak vizsgálata és a megfelelő technológiák és alkalmazások kifejlesztése. (Ilyen szolgáltatás a PRIME alkalmazás-prototípusai között is szerepel.) A Location-Based Privacy, illetve Mobile Privacy elnevezés alá tartozó megoldások központi eleme az Onion Routing, Crowds vagy más típusú anonim útvonalválasztó protokollok mobil környezetre való adaptálása, vagyis annak biztosítása, hogy az egyéni felhasználó és partnere vagy szolgáltatója között egyedileg felépülő (és a kapcsolat bontását követően lebomló) útvonal mobil környezetben is létrejöhessen, és kellően stabil maradjon a kapcsolat tartama alatt, ugyanakkor védelmet biztosítson az illetéktelen harmadik felek információszerző kísérleteivel szemben. Ilyen protokoll például a Karlstadti Egyetem kutatói által fejlesztett Chameleon.

Egy másik aktuális kutatási-fejlesztési vonulat az útvonalválasztó és más PET alkalmazások kvázi-valós idejű környezetre való adaptálása. Már az anonim böngészésnél is zavaró lehet a felépülő-lebomló útvonalak létrehozásának és a szükséges kódolási-dekódolási folyamatok végrehajtásának számítás- és időigénye, de ez a probléma fokozottan jelentkezik az azonnali üzenetküldő és csevegő szolgáltatások esetében.

Ígéretes kutatások és fejlesztések folynak Dániában az általános vélekedés szerint eleve privacy-invazívnak tartott RFID technológia privátszféra-védő változatának megvalósítására. A legegyszerűbb megoldás szerint a fogyasztói termékekbe épített RFID bélyegeket a vásárlás után véglegesen alkalmatlanná kell tenni a további – az eredeti célhoz már nem tartozó – felhasználásra. Egy másik megoldás szerint a termékekbe épített, illetve egyes szolgáltatások igénybevételéhez kötött RFID bélyegeket deaktiválni lehet, majd egy későbbi időpontban (adatvédelmi garanciák megléte esetén) újból aktiválni és ezzel a termék vagy szolgáltatás életciklus-menedzsmentjének részévé tenni. A legfejlettebb koncepció szerint az RFID bélyegek használatának feltétele az ún. zéró-tudású eszköz-authentikálás (Zero-Knowledge Device Authentication).[19] Ezzel megoldható, hogy csakis a felhasználó aktív közreműködésével lehessen írni/olvasni az RFID bélyegeket, és azt is csak a kontextus által indokolt módon, vagyis a bélyegeken tárolt vagy a bélyeg használata által hozzáférhető személyes adatok kezelése az adatalany kontrollja alá kerül. Az ilyen RFID bélyeg alvó üzemmódban van mindaddig, amíg az arra feljogosított felhasználó nem lép kapcsolatba vele, anélkül, hogy a kapcsolatba lépés során közölt adatokból illetéktelen fél megismerhesse a feljogosított felhasználó személyazonosító vagy más személyes adatait. Az ilyen technológiát tartalmazó RFID bélyegek tömeges előállítására már létrejött az infrastruktúra és megkezdődött a gyártás.

[18] Lásd a Springer „Lecture Notes in Computer Science" sorozatát.

[19] Lásd Engberg – Harning – Jensen 2004

A privacy-barát RFID fejlesztések legújabb vonulatát az „RFID 2.0” eszközök létrehozása jelenti, amelyek a Web 2.0 alkalmazásokhoz idomulva újrakonfigurálható, kontextus-felismerő, hozzáférés-kontrollal rendelkező, intelligens mikroszámítógépeknek tekinti az RFID bélyegeket.

4. A várható fejlődés

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 rétegként való 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.

4. ábra: Várható fejlődés 2005-2018

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.

Tovább folytatódik a helyfüggő szolgáltatásokkal összefüggő PET-ek kutatása és fejlesztése; ezek eredményei elsősorban a szolgáltatások hálózati rétegét érintik. Megjelenik az azonnali üzenetküldő és csevegő szolgáltatásokban alkalmazható PET-megoldások új generációja, amely nemcsak nagyobb biztonságot és jobb erőforráskezelést nyújt, hanem a Web 2.0 szolgáltatásoknak megfelelően közösségi (csoportszintű) privacy menedzsmentet is lehetővé tesz.

Elsősorban alapkutatási szinten várható a kvantuminformatikai, ezen belül a kvantumkriptográfiai kutatások eredményeinek (például a kvantumkommunikáció lehallgathatatlanságának) PET szempontú vizsgálata, illetve ilyen alapokon működő alkalmazások koncepcióinak kidolgozása.

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. Érdekes fejlemény, hogy a Microsoft a kézirat lezárását megelőzően megvásárolta a pseudonym-ek használatán alapuló, biztonságos és letagadhatatlan digitális okmányok szabadalmait a Credentica cégtől.

Az egységes vállalati szintű privacy menedzsment rendszerek elterjedése elsősorban a fejlett adatvédelmi kultúrával rendelkező országokban (pl. Németország) várható. Ilyen célra alkalmazhatók például a privacy menedzsment céljait (is) szolgáló speciális nyelvek, elsősorban az IBM által kifejlesztett Enterprise Privacy Application Language (EPAL), illetve a Sun által kifejlesztett eXtensible Access Control Markup Language (XACML) alapján kifejlesztett rendszerek.

A PET-ek szervezeti határokon túlnyúló rendszerbe állítása elsősorban az alábbi területeken várható:

- az identitás-menedzsmentben, amely az EU egyik támogatott fejlesztési iránya; itt a PrimeLife és hasonló tárgyú kutatások a Web 2.0 szolgáltatásaihoz idomuló PET rendszereket hoznak létre, illetve valósítanak meg, várhatóan nyílt szabványok bevonásával, illetve nyílt forráskódú fejlesztések megvalósításával is;
- a digitális pénz alapú fizetési rendszerekben; feltéve, ha a nagy szolgáltatók (például mobilszolgáltatók, üzletláncok) érvényesíteni tudják önálló üzleti koncepcióikat a pénzügyi szervezetekkel szemben; az áttörés elsősorban a mikrofizetések terén lehetséges, amelyek 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 itt nem hangsúlyos, bár beépíthető lenne.

Az EU az i2010 programja részeként e-government munkatervet készített, amelynek egyik kitűzött célja, hogy a tagországok 2010-re biztosítsák a személy- és dokumentumhitelesítés átjárhatóságát. Ennek megvalósítása nagyban érinti a személyes adatok kezelésének célhozkötöttségi 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 interoperábilis rendszerben kívánják megvalósítani. Az elektronikus kormányzati eljárások és szolgáltatások fejlesztése azonban gyakran párhuzamosan és nem összehangoltan történik a privátszférát erősítő technológiákéval, mind jogszabályi, mind technológiai szinten; ez a megállapítás érvényes a magyar viszonyokra is.

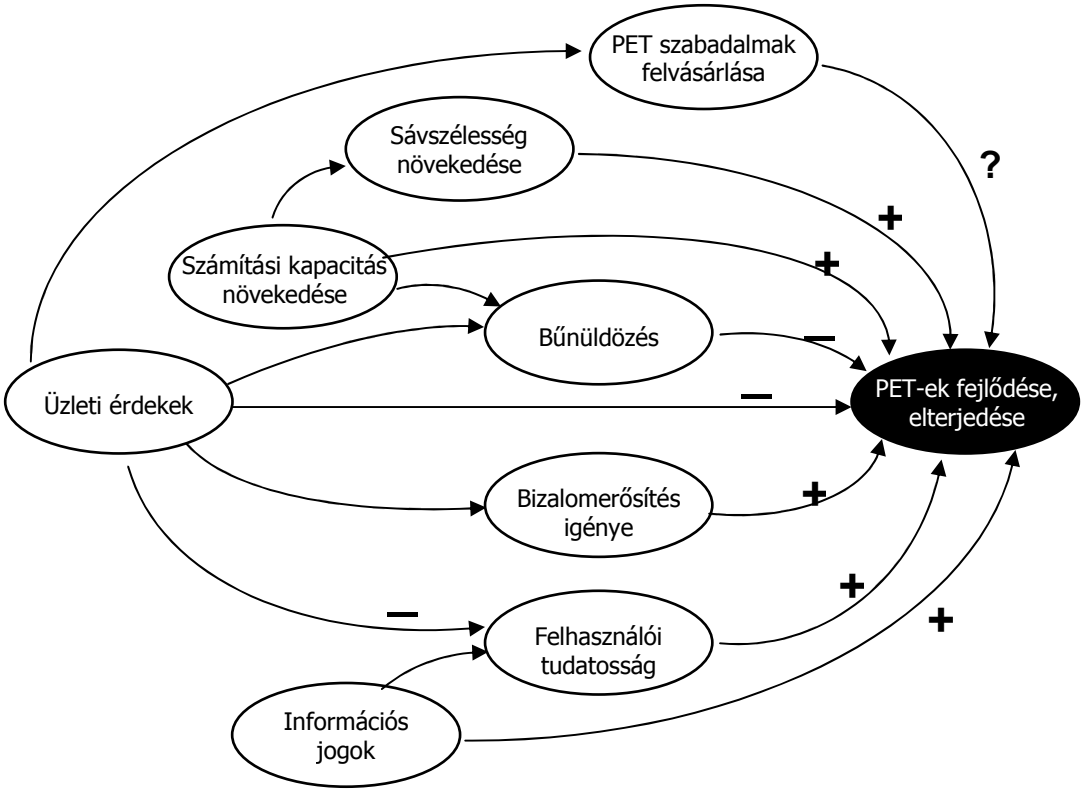
A privátszférát erősítő technológiák fejlesztésének egyik fő iránya az alkalmazásfüggetlen PET rendszerek és architektúrák létrehozása. Ilyen fejlesztések több egyetemen (pl. Karlstad, Drezda, Leuven, Aachen, Milano) és kutatóhelyen (pl. IBM Zürich, Centre National de la Recherche Scientifique [Franciaország],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

5. Befolyásoló tényezők

A PET-ek fejlett, rendszerszerű alkalmazásának technológiai előfeltétele a megfelelő számítástechnikai kapacitás: az alapfunkcionalitás teljesítéséhez járuló extra számításigény teljesítése a felhasználó számára nem vagy csak kevéssé érzékelhető késleltetéssel, illetve az ehhez szükséges sávszélesség biztosítása. A kezdeti PET alkalmazások irreális számításigénye ugyan megszűnt, de a PET-ek alkalmazása a számításigény növekedését eredményezheti. Ugyancsak előfeltétel a rendszerek kompatibilitásának biztosítása, közös informatikai infrastruktúrák létrehozása és működtetése. Az előfeltételek közé sorolható a megfelelő szakértelem és szemlélet rendelkezésre állása is; ehhez a szereplők – a felhasználók, a közigazgatási és üzleti döntéshozók, valamint a rendszereket tervező és üzemeltető informatikusok – oktatása és képzése szükséges.

A PET-ek elterjedését és tömeges alkalmazását gátolják egyfelől azok az üzleti érdekek, amelyek a személyes adatoknak az adatalanyok tudta és belegyezése nélküli felhasználására, elemzésére, értékesítésére irányulnak. Az ebben érdekelt cégek technikai, szervezési, marketing- és lobbi-eszközökkel 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.



5. ábra: Befolyásoló tényezők

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 történő 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 a belátható időszakban e rendszer kiépítésének csak az első fázisa valósulhat meg, így inkább bizalmi vagy PET szigetek létrejötte valószínűsíthető.

E pillanatban még kérdéses, hogy milyen hatással lesz a PET-ek alkalmazására a fent említett üzleti lépés, amelynek során a Microsoft felvásárolta a kutatásban és fejlesztésben élenjáró Credentica céget összes szabadalmával együtt,[20] amely a felhasználó-központú identitásmenedzselés egyik eszközét, a megbízható pseudonym-ek és digitális okmányok generálását és használatát garantálja termékeiben. Az egyik szcenárió szerint az óriáscég célja a saját szolgáltatásainak további terjedését gátló szabadalmak elzárása; a másik szcenárió szerint a Credentica termékei megjelennek majd a Microsoft által terjesztett termékekben és szolgáltatásokban.

6. Várható hatások

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. Megjelennek a kvantuminformatikai kutatásokban az eddigi hipotézisek, illetve kutatási eredmények PET célú alkalmazhatóságára irányuló vizsgálatok; ezekből potenciális PET-alkalmazások tervezése várható.

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 azonban nem a már kifejlesztett és alkalmazott rendszerek, szolgáltatások működését gátolják, hanem azokat az adatalany érdekeit tükröző (és azok érvényesítését lehetővé tevő) elemekkel egészítik ki. Ennek ellenére ennek az alapvető érdekkapcsolatnak a

[20] A Credentica mögött Stephan Brandt-nak, a Chaum utáni kriptográfus-generáció egyik legkiválóbbikának szabadalmai állnak.

megváltozása középtávon nem várható, legfeljebb az etikus információkezelés elveinek jobb ismerete az informatikai szakma egyes szegmenseiben.

Fejlett adatvédelmi kultúrával rendelkező országokból és/vagy multinacionális cégektől származó, PET tartalmú informatikai rendszerek az informatikai szakma figyelmét a területre irányíthatják és növelhetik szakmai tájékozottságukat. A jövőben sem az állami, sem az üzleti döntéshozók nem hagyhatják figyelmen kívül a személyesadat-kezelés szervezeti és technológiai következményeit és alternatíváit. Ez egyaránt vonatkozik az adatvédelmi hatásvizsgálat (Privacy Impact Assessment, PIA), illetve az adatvédelmi auditálás gyakorlatának terjedésére, valamint a PET-ek potenciális használatának vizsgálatára.[21]

Amennyiben a független ellenőrző hatóságok (Magyarországon az adatvédelmi biztos), illetve a civil szervezetek kellő propagandát nyújtanak a PET-ek laikusok általi használatához, beleértve azok kezelésének egyszerű elsajátíthatóságát, a lakosság tudatossága várhatóan növekedni, látszólagos érdektelensége csökkenni fog adatai sorsát illetően.

7. A hazai helyzet

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 nem változott lényegében, 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[22] 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 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

[21] Lásd például a holland belügyminisztérium „fehér könyvét": *„Privacy-Enhancing Technologies: White Paper for Decision-Makers"*.

[22] 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. – Lásd ebben a szerző tanulmányát a magyar lakosság adatvédelmi tájékozottságáról és attitűdjeiről az 1989–2006 időszakban.

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.

2008. tavaszának kedvező fejleménye, hogy létrejött a privátszférát erősítő technológiák első hazai internetes fóruma, a PET Portál és Blog. A fiatal műegyetemi kutatók kezdeményezésére, nemzetközileg ismert szakemberek támogatásával megvalósított független nonprofit szakmai portál célja, hogy a PET-ek témakörével kapcsolatos ismeretek, hírek, elemzések, publikációk és vélemények meghatározó magyar nyelvű fórumává váljon.

8. Összefoglalás

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 rétegként 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.

Hivatkozások

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.* PISA Consortium, The Hague.

Burkert, H.: Privacy-Enhancing Technologies: Typology, Critique, Vision. In: Agre, P.E. – Rotenberg, M. (eds.): *Technology and Privacy: The New Landscape.* MIT Press, 1997.

Engberg, S. J. – Harning, M. B. – Jensen, Ch. D. (2004): Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. *Second Annual Conference on Privacy, Security and Trust,* 2004 October, New Brunswick, Canada.

ICT and Privacy in Europe. Experiences from technology assessment of ICT and Privacy in seven different European countries. Final report, October 16, 2006, Europan Parliamentary Technology Assessment.

Koorn, R. (ed.) (2004): *Privacy-Enhancing Technologies: White Paper for Decision-Makers*. Ministry of the Interior and Kingdom Relations, the Netherlands.

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

Flash Eurobarometer 225, *Data Protection in the European Union. Citizens' perceptions. Analytical Report.* The Gallup Organization (February 2008)

Székely I.: Changing attitudes in a changing society? Information privacy in Hungary 1989–2006. In: Zureik, E. et al. (eds), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons,* McGill-Queen's University Press, Kingston, Ontario (előkészületben)