HERBERT BURKERT

A privátszférát erősítő technológiák: tipológia, kritika, vízió

Tanulmányában Herbert Burkert a privát szférát erősítő technológiákat (Privacy-Enhancing Technologies, PETs) négy csoportra osztja: szubjektum-orientált koncepciók, objektum-orientált koncepciók, tranzakció-orientált koncepciók, és rendszer-orientált koncepciók. E kategóriák kialakulását elemezve az információ-egyensúly, az identitás és a bizalom lényeges szerepét emeli ki. Megközelítése heurisztikus módszert nyújt a PET-ek szerepének átfogó szemléletű vizsgálatához, ami rávilágít az információs társadalom szabályozási, politikai és társadalmi problémáira az adatvédelem terén.

Szerzői információ:

Herbert Burkert

Herbert Burkert német jogászprofesszor. PhD-fokozatát a Frankfurti Egyetemen szerezte. A svájci St. Galleni Egyetem Információs Jogi Kutató Intézet vezetője. Hírközlési jogot, média-jogot, internetjogot és közjogot oktat. Számos nemzetközi szervezet tagja, többek között az Európai Bizottság megbízásából az információs társadalom kérdéseivel foglalkozó jogi tanácsadó testület elnöke. A *Fraunhofer Kommunikáció- és Médiakutató Intézet* igazgatója. Számos európai és ausztráliai folyóirat szerkesztőségének tagja, az amerikai *BNA Electronic Commerce and Law Report* munkatársa.

Így hivatkozzon erre a cikkre:

Burkert, Herbert. „A privátszférát erősítő technológiák: tipológia, kritika, vízió”. *Információs Társadalom* V, 2. szám (2005): 98–113.

https://dx.doi.org/10.22503/inftars.V.2005.2.6

A folyóiratban közölt művek
a Creative Commons Nevezd meg! – Ne add el! – Így add tovább! 4.0
Nemzetközi Licenc feltételeinek megfelelően használhatók.

Herbert Burkert

A privát szférát erősítő technológiák: tipológia, kritika, vízió*

A „privát szférát erősítő technológiák" *(privacy-enhancing technologies, PETs)* kifejezés a személyazonosság védelmét célzó technikai és szervezési megoldásokra utal. Ezek a megoldások gyakran kötődnek a titkosításhoz (pl. digitális aláírás), az úgynevezett „vak-aláírásokhoz" vagy a digitális álnevekhez.[1]

A *PET*-eket el kell választanunk az adatbiztonságot szolgáló technológiai kérdésektől. A *PET*-ekről eddig folytatott vita egyik érdeme éppen az volt, hogy újra tisztázta az adatbiztonság korlátait a *privát szféra védelmének* szempontjából. Az adatbiztonságot szolgáló intézkedések az adatfeldolgozás biztonságossá tételét célozzák, függetlenül attól, hogy legitim-e maga a feldolgozás. Az adatbiztonság szükséges, de nem elégséges feltétele a privát szféra védelmének. A *PET*-ek alkalmazása ezzel szemben azt a törekvést szolgálja, hogy a személyes adatok felhasználását teljes egészében megszüntessék, vagy a személyes információ felfedésének jogát az illető személy kezébe adják, s így a *PET*-ek közelebb állnak a privátszféra védelmének társadalmi céljaihoz. Hogy valójában mennyire közelítik meg ezeket a célokat, arról lesz szó – többek között – ebben a fejezetben.

A *PET*-ek létrehozására irányuló elgondolások abból a felismerésből erednek, hogy a személyek közötti kölcsönhatások, illetve ezek megfigyelése során személyes információk halmozódnak fel. Ebből kiindulva felvázolhatjuk a *PET*-ek egy lehetséges tipológiájának struktúráját. Ha az említett kölcsönhatásokat olyan szubjektumok között végbemenő cselekvések sorozataként fogjuk fel, amelyek különböző rendszerekhez tartozó objektumokhoz kapcsolódnak, négyféle *PET*-koncepciót különböztethetünk meg:

– szubjektumorientált koncepciók,
– objektumorientált koncepciók,
– tranzakció-orientált koncepciók,
– rendszerorientált koncepciók.

Ezek közül a típusok közül eddig nem mindegyik képezte részletes vita tárgyát, és nem mindegyiket alkalmazzák a gyakorlatban, tiszta formájában pedig egyik koncepció sem valósult meg a gyakorlatban. Ez a tipológia tehát csupán heurisztikus eszközként szolgálhat, amely segít számba venni az ilyen rendszerek fő jellemzőit.

* Herbert Burkert: Privacy-Enhancing Technologies: Typology, Critique, Vision, in *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE*, 125–142 (Philip E. Agre & Marc Rotenberg, eds. MIT Press, 1997).

[1] További részletek találhatók a holland állam és az ontariói adatvédelmi hivatalok dicséretes együttműködése nyomán született munkában: *Privacy Enhancing Technologies*, 1995. A titkosítás kérdéseiről lásd továbbá Schneier (1995).

Szubjektumorientált koncepciók

A szubjektumorientált koncepcióknak az a céljuk, hogy megszüntessék vagy lényeges mértékben csökkentsék a cselekvő (vagyis egymással kölcsönhatásba lépő) szubjektumok személy szerinti azonosításának lehetőségét akár a tranzakciók során, akár a már létező adatokhoz fűződő kapcsolataikban.

E koncepciók szerint ez a cél elérhető úgynevezett *proxy*k (közvetítő technikai eszközök) alkalmazásával: a személyeket azonosítóval lehet ellátni. Ezek lehetnek nyomon követhetetlen azonosítók, legyen szó akár egy adott tranzakcióról, akár a tranzakciók sorozatáról vagy a szubjektumra, illetve szubjektumokra vonatkozó adatok együtteséről. Az azonosítók lehetnek állandóak, de minden egyes tranzakciót megelőzően újra is generálhatók. Az azonosítók létrehozása történhet előre megadott szabály szerint (ügyelve arra, hogy ez a szabály ne árulkodjon a személyazonosságról), és véletlenszerűen is. Maguk az azonosítók vagy visszakereshetők, vagy nem. Amennyiben visszakereshetők, a létrejövő kapcsolatok rendszerezhetők oly módon, hogy a rájuk vonatkozó szabályok ne sérüljenek. A visszakeresés folyamatára vonatkozó szabályok betartását különféle szervezetek és magánszemélyek (úgynevezett „megbízható harmadik felek") vagy olyan technikai rendszerek ellenőrzésére is bízhatjuk, amelyek csak meghatározott szabályok szerint létesíthetnek kapcsolatokat.

Ahhoz például, hogy egy hitelkártyarendszert szubjektumorientált PET-rendszerként állítsunk fel, eltávolíthatjuk a rendszerből a kártya tulajdonosának nevét és a kártya számára való hivatkozást (kapcsolatot), és ezeket az információkat olyan „adatszéfben" tárolhatjuk, amely csak az érintett személy engedélyével teszi őket hozzáférhetővé. Ebből a célból az információ titkosítható például egy nyilvános kulcson alapuló titkosító rendszerrel úgy, hogy az információ kinyeréséhez a bank és a számlatulajdonos kulcsára is szükség legyen. Ugyanezt megtehetjük a kártyához kapcsolódó bankszámlára vonatkozó információval is. Ez a módszer lehetővé teszi, hogy üzleti tranzakcióinkhoz – legalábbis a nem személyre szabott árucikkek és szolgáltatások esetében – egyfajta „hitelkártyát" használjunk anélkül, hogy a többi fél tudomást szerezne személyazonosságunkról.

Objektumorientált koncepciók

Az objektumorientált koncepciók abból a felismerésből erednek, hogy a tranzakciók gyakran cserejellegűek, és a „cserébe adott" objektumok olyan, az ujjlenyomatokhoz hasonló nyomokat viselnek magukon, amelyek lehetővé teszik a csereügyletben részt vevő személyek azonosítását. E szerint a koncepció szerint tehát a cél a csereobjektumok megszabadítása a nyomoktól anélkül, hogy magukat az objektumokat megsemmisítenénk. A csere leggyakoribb tárgya természetesen valamilyen fizetőeszköz. Az azonosítást legjobban megnehezítő fizetőeszköz a készpénz. Az objektumorientált koncepciók a készpénz vagy más csereobjektumok olyan elektronikus megfelelőit kívánják létrehozni, amelyek nem teszik lehetővé, hogy az objektumot bárki összeköthesse azzal a személlyel, aki azt beviszi a tranzakcióba. Ilyen elektronikus megfelelőnek számítana például egy készpénzért vásárolt, nem névre szóló kártyáról érkező elektromos impulzus. Az is elképzelhető, hogy a bank a hitelkártyára és a hozzá tartozó

bankszámlára vonatkozó azonosítók egymástól való elkülönítése helyett csak számsorozatokat bocsát a számlatulajdonos rendelkezésére, amelyek előre meghatározott összegekkel egyenértékűek, és ugyanolyan szabadon használhatók, mint a készpénz.

Tranzakció-orientált koncepciók

A tranzakció-orientált koncepciók, amelyek tudomásom szerint nem képezték széles körben folytatott viták tárgyát, legalábbis a *PET*-ekkel összefüggésben, a tranzakciós folyamat által hátrahagyott nyomokat célozzák meg anélkül, hogy közvetlenül foglalkoznának a csereobjektumokkal. (A nyomon követési folyamatokra sor kerülhet például a bankokban, amikor a pultnál végzett készpénzműveleteket videokazettára rögzítik, vagy amikor a készpénzes kifizetésről elismervény készül.)

A tranzakció-orientált koncepciók lényege az, hogy lehetővé tennék a rögzített adatok automatikus megsemmisítését. A tranzakciók során keletkező feljegyzések például előre megadott idő múltán automatikusan megszűnnének létezni. Ebben a kontextusban elképzelhető olyan technikai eszközök használata, amelyek lehetővé teszik az adatok és kisebb számítógépes programok kombinációit. Ezekről mostanában sokszor esik szó a szellemi termékekhez fűződő jogok kapcsán (ide tartoznak többek között az olyan elektronikusan rögzített felvételek vagy szoftverek, amelyek megsemmisítik önmagukat, ha a megadott időn belül nem történik fizetési kezdeményezés).

Rendszerorientált koncepciók

Végezetül elképzelhetünk a fent leírt elemek integrációját célzó koncepciókat is, olyan interakciós zónák létrehozására vonatkozóan, amelyekben a szubjektumok identitása rejtett, az objektumok nem viselik kezelőik „ujjlenyomatait", és magát az interakciót sem rögzítik semmilyen tárolásra alkalmas formában.

Az ilyen koncepciókra példa lehet a jelenlegi társadalomban a katolikus gyónás (ha elég nagy a templom), vagy a különféle krízisközpontokkal névtelenül folytatott kommunikáció. Elektronikus környezetben ezeknek a koncepcióknak leginkább egy olyan, két személy között folyó elektronikus levélváltás felel meg, melynek során mindkét fél igénybe vesz valamilyen, a kommunikáció névtelenné tételére alkalmas szolgáltatást, végül pedig megsemmisítik a kommunikáció minden nyomát.

Kísérlet a koncepciók bírálatára

A PET-tervezés eredményei

A *PET*-ek kidolgozásának szorgalmazói már a kezdet kezdetén felvetették a *PET*-ek tervezése során legelőször felteendő kérdést: Vajon szükség van-e egyáltalán a személyes adatokra? A *PET*-ek elérhetővé válása a legitimizáció terhét rója mindazokra, akik személyes adatokat kívánnak tárolni informatikai rendszereikben.

A *PET*-ek javára írható továbbá, hogy a „hozzájárulás" elvét megszabadítják a rá-nehezedő nyomástól. Túlságosan gyakran történik meg ugyanis, hogy a személyes adatok kezelésére felállítandó rendszerek tervezői úgy igyekeznek elkerülni az információ tárolásával kapcsolatos problémákat, hogy az alanyok beleegyezését kérik ahhoz. Ahelyett, hogy megpróbálnák elkerülni a személyes adatok használatát, vagy a speciális jogi feltételeknek megfelelő rendszert terveznének, igyekeznek egyszerűen megszerezni az alanyok hozzájárulását ahhoz, hogy személyes adataikat saját céljaikra felhasználhassák. A „hozzájárulási megközelítést" túlságosan gyakran alkalmazzák anélkül, hogy kielégítő módon elemeznék az adatalanyok előtt álló valós választási lehetőségeket. Ehelyett arra kérik őket, hogy válasszanak: vagy hozzájárulnak adataik felhasználásához, vagy lemondanak olyan előnyökről, kiváltságokról, jogokról és juttatásokról, amelyek közül nem egy alapvető fontosságú lehet számukra az adott helyzetben. A privátszféra védelmének kontextusában a hozzájárulás ráadásul tájékozottságon alapuló hozzájárulást jelent. A rendszerek üzemeltetői által megadott információ mennyisége ugyanakkor esetenként jócskán eltérő, az adatalany pedig hátrányban van, mert anélkül, hogy teljesen átlátná a rendszert és annak más rendszerekhez való kapcsolódását, nem is tudhatja, mennyi információra lenne szüksége. A *PET*-ek egyre szélesebb körben elérhetővé válásával eleve elkerülhetők az olyan helyzetek, amelyekben az adatalanyok hozzájárulását kell kérni, és azt ilyen tökéletlen módszerekkel szerzik meg.

Másrészt viszont biztosítani kell, hogy a *PET*-szemlélet ne szorítsa háttérbe a hozzájárulás elvének figyelembevételét. A *PET*-rendszerek nem helyettesítik a hozzájárulásra vonatkozó követelményeket. Használatukra nagy valószínűséggel olyan területeken kerül majd sor, ahol nincs választási lehetőség, vagyis amúgy sem lehetne valódi hozzájárulást szerezni, mert az illető személy az adott interakció során függő helyzetben van,[2] és ahol minden erőfeszítést meg kell tenni annak érdekében, hogy az információs rendszer a lehető legkevesebb kockázattal működjön.

A személyes adatok felhasználásának csökkentésére irányuló „puha" társadalmi igényeket a *PET*-ek bevezetése átvitte a „kemény" rendszertervezési megfontolások szintjére.

Ebben a kontextusban a *PET*-ek a privátszféra védelmének elsősorban arra az alapelvére hívják fel figyelmünket, amelyet minden adatvédelmi törvény világosan megfogalmaz: személyes adatokat csak akkor szabad gyűjteni, ha ez *szükséges*.[3] Következésképpen a privátszférát védelmező aktivisták – annak a képességnek a birtokában, hogy a *PET*-ek részletes leírásaira mint *rendszertervezési specifikációkra* utaljanak – egy nyelven tudnak beszélni a rendszertervezőkkel; értékeiket és megfontolásaikat tehát képesek lefordítani a rendszertervezés nyelvére.[4] E lépés megtételével a privátszféra védelmét sürgető érvek már nem söpörhetők le az asztalról azzal, hogy „lefordíthatatlanok", vagy kívül esnek a tervezői kompetencián (és kötelezettségeken), illetve a „mérnöki szemléleten".

A privátszférával kapcsolatos kérdéseknek a tervezés szintjén való figyelembe vétele elengedhetetlen feltétele annak, hogy a privátszférával a *politika* szintjén foglalkoz-

[2] Egy ilyen rendszerre mutat be példát Elgesem (1996).
[3] Simitis (1994: 573–592).
[4] *Privacy Enhancing Technologies*, volume II, 26 ff.

zunk: a modern technika iránt elkötelezett társadalmakban a legitimációs stratégiák fontos eleme a képesség arra, hogy „tegyünk valamit". A *PET*-ek létrejöttével immár minden politikailag kívánatosnak tartott (és a személyes adatokkal kapcsolatos) rendszer felállítását meg kell indokolni, mégpedig annak alapján, hogy a tervezők milyen mértékben vették figyelembe a *technikai* szinten elérhető lehetőségeket abból a célból, hogy minimalizálják a személyes adatok előfordulását a rendszerben. Ennélfogva a személyes adatok tárolására vagy azok elérhetőségének növelésére irányuló politikai intenciók már nem takarózhatnak technikai szükségszerűségekkel, tervezési nehézségekkel vagy a rendszerekről alkotott rögzült felfogásokkal. Ehelyett világosan ki kell nyilvánítaniuk azt a *politikai szándékukat*, hogy azonosítható személyes adatokat tegyenek közzé. Ebből pedig az következik, hogy a korábbinál világosabban kimutatható a személyes adatok elérhetőségéből fakadó kockázatokkal kapcsolatos politikai felelősség.

A PET-tervezés korlátai

Ahhoz, hogy ne veszítsük el azt, amit a gyakorlati bevezetésről folytatott vitákban elértünk, az eredmények mellett szükség van az ilyen tervezői szemlélet korlátainak világos kimutatására vagy újrafogalmazására is. E korlátok egy része a tervek jellegéből fakad, és ezt a *PET*-rendszerek tervezői általánosságban el is ismerik. Más korlátok nem ugyanolyan mértékben találhatók meg a különböző rendszerekben, és a tervek megváltoztatásával kiküszöbölhetőek is lennének. Egyes korlátok külső eredetűek, és mindezeknek a korlátoknak a többségével már szembesültek is a *PET*-ek szószólói. A továbbiakban ezeket a korlátokat veszem tüzetesen szemügyre.

Belső korlátok

A PET-tervek négy belső korlátját az egyirányú perspektívában, az „azonosító információ" problémájában, a „rendszerperspektíva" kapcsán felvetődő általános problémákban, valamint a megvalósításuk alapjául szolgáló technikai jellegű előfeltevésekben látom.

Az egyirányú perspektíva

Jó néhány szubjektumorientált *PET*-koncepció arra a megfigyelésre épül, hogy a kölcsönhatások során az egyik fél rendszerint védelemre szorul a másik féllel vagy egy megfigyelőként működő harmadik féllel szemben. A védelmet kiérdemlő személyt általában olyan rendszer óvja, amely egyúttal lehetővé teszi számára, hogy azonosítsa a kölcsönhatásban részt vevő partnerét. Ezt a megközelítést nevezem „egyirányúnak". Az ilyen koncepciók a gyakorlatban egyfajta egyirányú névtelenséget biztosítanak. Annak eldöntése azonban, hogy a kölcsönhatás mely résztvevői jogosultak a védelemre, nem technikai, hanem normatív jellegű kérdés. Ha olyan normatív koncepciót követünk, mint amilyen például az erőegyensúly elve, akkor például az egyes vásárlókat a

gazdasági szempontból erős gyártókkal és szolgáltatókkal szemben védelemre szorulónak tekinthetjük. Ennek alapján figyelmünk olyan szolgáltatások fejlesztésére irányulhat, melyeknek az igénybe vétele során a fogyasztók dönthetnek arról, hogy azonosítják-e magukat, és ha igen, ezt milyen mértékben teszik meg – már ha ez az ötlet egyáltalán megvalósítható. (Az is elképzelhető, hogy a megrendelt áruhoz is névtelenségüket megőrizve szeretnének hozzájutni.) Azt ugyanakkor nem engednénk meg, hogy az eladó is hasonló eszközökkel éljen. De hogyan lehetünk bizonyosak abban, hogy megfelelően mértük fel az erőviszonyokat? Például az elektronikus adatcsere kontextusában könnyen elképzelhetők olyan helyzetek, amelyekben a vásárló szerepét egy hatékony szervezet tölti be, az eladó viszont olyan kis cég, amelynek a vásárló gazdasági hatalmával szemben legitim érdeke fűződik az önvédelemhez.

A példából két következtetést vonhatunk le. Nem szabad elfeledkeznünk arról, hogy az ebből a szempontból mégiscsak az adatbiztonsági rendszerekre hasonlító *PET*-ek alapjában véve technikai jellegű eszközök, és csak *követik* a normatív döntéseket.[5] A normatív döntést viszont meg kell hozni, s ezt a döntéshozatalt önmagában nem helyettesítheti a *PET*-koncepció. Ha ezt az egyirányú szemléletet vesszük alapul, akkor is el kell tehát *döntenünk*, hogy melyik fél jogosult a védelemre. Ebből következik, hogy a *PET*-ek bevezetésekor – legalábbis az esetek egy részében – óvatosnak kell lennünk, amikor ezeket a technológiákat egyszerűen a „privátszférát erősítő technológiáknak" nevezzük, holott valójában a személyek identitását védelmező *technikai* eszközökkel állunk szemben. Az pedig már más kérdés, hogy a privátszférát mint társadalmi értéket ez a védelem valóban erősíti-e. A *PET*-ekről folytatott vita segített rámutatni az adatbiztonsági koncepciók korlátaira, már amennyiben az adatbiztonság értékmentes (elképzelhető, hogy éppenséggel a rossz fajta kommunikációt tesszük biztonságossá). Óvakodnunk kell tehát attól, hogy a *PET*-ekkel kapcsolatban is elkövessük ugyanezt a hibát. Lehet, hogy nekünk tetsző módon erősítik a privátszférát, ám a nem kívánatos titkolózást is megkönnyíthetik.

Az olyan politikai környezetekben (például az Egyesült Államokban), amelyeknek a kialakításában viszonylag kis szerepet játszik az információszabadság kultúrája, megtörténhetne az is, hogy a *PET*-eket hivatalnokok használják ellenséges környezetben tevékenykedő személyek védelmére. A hivatalnokok ebben az esetben követelhetnék, hogy az adminisztratív eljárások során az elektronikus aláírás intézménye védelmezze névtelenségüket, kilétükre pedig csak meghatározott feltételek teljesülése esetén és csak bizonyos eljárásbeli óvintézkedések megtétele után, például akkor derülhetne fény, ha az azonosítást bíróság rendeli el. Egy tisztán „papíralapú" környezetben a dolog ugyanolyan előnyökkel és hátrányokkal járna, mint ha például a rendőrök jelvényén nem a nevük, hanem csak egy szám szerepelne. Való igaz, hogy a *PET*-eket Európában még napjainkban is használják az adminisztratív titoktartás elveinek megerősítésére. A *PET*-ek nem mentesítenek attól, hogy a privátszférához fűződő jogokat és a hivatalok átlátható működésének szükségességét *értékítéletek alapján* mérlegeljük.

A *PET*-ek gyakorlati alkalmazása során tehát fokozott mértékben kell figyelembe vennünk a normativitás kérdését, éppen azért, hogy képesek legyünk kezelni a techno-

[5] A gondolat részletes kifejtése a *Privacy Enhancing Technologies* II. kötetének 26. oldalán olvasható.

lógia kétélű voltát. A *PET*-ek ugyanis alkalmasak lehetnek arra is, hogy a szervezetek kezében levő hatalom adott megoszlását *fenntartsák*, ahelyett, hogy az egyén kezébe adnának eszközt a szervezetek hatalmával szemben, és hozzásegítenék a szabadsághoz és a privátszférához fűződő jogainak érvényesítéséhez.

Azonosító információk

Egyes *PET*-koncepciók azon a lehetőségen alapulnak, hogy az egyénhez „kapcsolódó" információ elkülöníthető az egyént „azonosító" információtól, és ez a két különböző fajta információ külön is kezelhető. Mint fenti példánkból is kitűnt, egy bankkártya tulajdonosának a neve és a címe (az azonosító információk) elkülöníthetők a hitelkártya számától, és külön is tarthatók attól. A hitelkártya száma ugyanakkor jogi szempontból még mindig minősülhet személyes adatnak. Az Európai Parlament és a Tanács által 95/46/EC jelzéssel, 1995. október 24-én kiadott „Irányelv az egyének védelméről, a személyes adatok feldolgozásáról és az ilyen adatok szabad áramlásáról"[6] meghatározása szerint „személyes adatnak minősül [...] bármely információ, ami egy azonosított vagy azonosítható természetes személlyel (adatalannyal) kapcsolatba hozható"; továbbá „azonosítható személynek az minősül, aki közvetlenül vagy közvetve azonosítható, különösen egy azonossági számra való hivatkozás, illetve fizikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi azonosságára utaló egy vagy több tényező révén."[7] A probléma természetesen a „közvetve" kifejezésben rejlik: a hitelkártyaszámok konkrét személyhez kapcsolását vajon miért ne tekinthetnénk legalábbis „közvetett azonosításnak"? Az ilyesfajta problémák ugyanakkor elterelik a figyelmet egy jóval alapvetőbb kérdésről: azonosító információ létezhet akár a tudtunkon kívül is, és megtörténhet az is, hogy egy másik rendszer vagy környezet olyan kiegészítő információt szolgáltat, melynek segítségével egy csapásra azonosíthatóvá válunk. Az anonim adatok mögött rejlő személyek azonosításának lehetősége függ az azonosítás céljától, a hozzájuk kapcsolódó „rejtett információktól" és az esetleg más információs rendszerek által szolgáltatott „kiegészítő ismeretektől".[8] Ugyanakkor a rendszer tervezésekor rendkívül nehéz előre látni ezeket az összetevőket. Egy bizonyos *PET*-rendszer megtervezése önmagában még nem garantálja, hogy a rendszert csakis arra a speciális célra fogják felhasználni, amire megtervezték. Megeshet, hogy nem vagyunk eléggé tudatában a rendszer által hordozott rejtett információknak. Nem tudhatjuk bizonyosan, és nem is jósolhatjuk meg előre, hogy milyen más, a *PET*-ektől eltérő rendszerek léteznek már ma is, és milyen rendszerek jönnek létre azzal a céllal, hogy olyan „kiegészítő ismereteket" szolgáltassanak, amelyeknek a segítségével feltörhető a névtelenség és korlátozódik a *PET* elemeinek hatékonysága.

Tegyük fel, hogy létrehozunk egy olyan rendszert, amely tartalmazza egy megadott földrajzi területen élő kisebbség összes tagjának adatait. Ezt a jegyzéket „szub-

[6] *Official Journal*, L sorozat, 281/31, November 23, 1995.
[7] Az irányelv 2/A cikkelye.
[8] Burkert (1979: 63–73).

jektumorientált" *PET*-rendszerként működtetjük, vagyis a listán szereplők nevét és lakcímét minden más, a rendszer által szintén tárolt információtól (pl. nem, kor, foglalkozás és jövedelem) elkülönítve kezeljük. Legyen továbbá a rendszer célja az, hogy speciális szolgáltatásokat nyújtson a szóban forgó kisebbség tagjainak, például segítsen nekik iskolákat és könyvtárakat alapítani. Ha ebben az esetben kezünkbe kerül egy neveket és címeket tartalmazó lista, tudjuk róla, hogy a kérdéses jegyzéknek az azonosításra szolgáló részéből származik, és azt is tudjuk (hiszen hallottunk a jegyzékről), hogy a felsorolt személyek az illető kisebbség tagjai, annak ellenére, hogy a jegyzék „azonosító" és „statisztikai" része sem tartalmazhat semmiféle jelzést, ami a kisebbségre utalna. Ez a kiegészítő információ a rendszer definíciójának részét képezi. Tegyük fel továbbá, hogy más forrásból egyszer csak arról értesülünk, hogy a szóban forgó kisebbség tagjai között nagy arányban fordul elő egy bizonyos betegség vagy születési rendellenesség. Ebben az esetben címlistánk olyan egészségügyi jegyzékké válik, amely esetleg karanténintézkedések bevezetésére is felhasználható. Még ha nem is állnak rendelkezésünkre a nevek és a címek, és csupán a jegyzék statisztikai része van a birtokunkban, akkor is kielégítő pontossággal tervezhetjük meg karantének felállítására irányuló (vagy még ennél is diszkriminatívabb jellegű) intézkedéseket, hiszen ismerjük a földrajzi területet (ez része rendszerünk definíciójának), valamint a területről evakuálandó személyek pontos számát, korát és nemét is.[9]

A rendszerszemlélet

A *PET*-koncepciók vonzereje és talán egyik fő célja – mint korábban is említettem – az, hogy a rendszertervezők világképét veszik alapul, és a saját nyelvükön szólnak hozzájuk. A rendszertervezők szemlélete ugyanakkor absztrakción és azt követően valamilyen formalizáción alapul. Ez a szükségszerűen bekövetkező „szakmai torzulás" azzal a kockázattal jár, hogy a tervezők figyelmen kívül hagyják a rendszerek *egymáshoz való kapcsolódásait.* Egy személyes adatokat kezelő rendszer (vagy több ilyen rendszer) *PET*-eket alkalmazó rendszerré történő átalakításával elért eredmények kétessé válhatnak, ha csak egyetlen olyan fel nem fedezett (vagy szándékosan érintetlenül hagyott) rendszer is a színen marad, ami nem támaszkodik semmiféle *PET*-re. Mi több, az is előfordulhat, hogy több *PET*-rendszer együttesen – ha bizonyos módon kapcsolódnak egymáshoz – olyan nagyobb rendszert alkot, ami a szándékoltnál kevésbé, vagy egyáltalán nem erősíti a privátszférát.

Egy kisebbségi iskola vagy könyvtár tervezésénél alkalmazott rendszer *PET*-rendszerré való átalakítása során a privátszférát erősítő hatás nagy része elveszhet például abban az esetben, ha a kizárólag az adott közösség tagjai által olvasott újság előfizetőinek nyilvántartását tartalmazó fájl átalakítása elmarad.

Összegezve: nemcsak arról kell gondoskodni, hogy az egyes *PET*-rendszerek megfelelő tervek alapján készüljenek el, hanem arról is, hogy ezeknek a többi *PET* és nem *PET*-rendszer alkotta hálózatban játszott szerepe világosan azonosítható legyen.

[9] Bár a példa egyes olvasók számára ismerősnek tűnhet, valójában még mindig pusztán hipotetikus.

A technikai előfeltevés

Egyes *PET*-rendszerek azon a speciális, technikai jellegű megfigyelésen alapulnak, hogy a titkosításra és a titkosított anyagok dekódolására irányuló kísérletek száma között jelentős eltérés van. Számomra nem világos, hogy ez az egyensúlyhiány középtávon milyen mértékben fog megváltozni.[10] A múltban alkalmazott technológiák és a későbbi fejlemények azonban óvatosságra intenek.

Külső korlátok

A *PET*-koncepciók gyakorlati alkalmazása során nagy ellenállóképességű gazdasági, társadalmi és politikai erőkkel kell számolni. Ezzel kapcsolatban meg kell vizsgálnunk többek között az információgazdaság kérdéseit, a mobilizáció szükségességét és a privátszféra koncepcióját magát is.

Az információ gazdaságtana

Az információ gazdaságtanára utalni annyit tesz, mint újra hangoztatni, ami nyilvánvaló. A tranzakciós folyamat során kiadott személyes információ a megvásárolni kívánt termékért vagy szolgáltatásért járó fizetség részét képezi. Ha ez az információ hiányzik, a termék vagy a szolgáltatás ára valószínűleg megváltozik. A változás lehet átlátható, és a vásárlót „választás" elé állíthatják. Egy terméket vagy szolgáltatást kínáló cég esetleg magasabb árat kérhet, amelyben benne foglaltatik a rendelkezésére bocsátott személyes információ magasabb fokú védelme, másrészt azonban elképzelhető az is, hogy a vásárló kevesebbet fizet, de kiegészítő információkkal szolgál, amelyek hatékonyabbá tehetik a cég marketingstratégiáját, vagy lehetővé teszik számára, hogy az információ révén kiegészítő bevételre tegyen szert. Ha a versenyhelyzet nem tesz lehetővé ilyesfajta árváltozásokat, akkor talán a hirdetési és direkt marketing szakma gondolkodásmódjának kell megváltoznia. Tevékenységük kontextusában újra át kell gondolniuk a személyes információk felhasználásának szükségességére vonatkozó feltételezéseiket, és talán ennek a hatásait is számba kell venniük. A szokások megváltoztatásával járó nehézségeket nem szabad alábecsülnünk. A reklámipar és a direkt marketing – a közhiedelemmel ellentétben – a legkonzervatívabb ágazatok közé tartoznak, legalábbis ha azt a pénzmennyiséget tekintjük, amit ezek az ágazatok eddig a törvényi szabályozás elkerülésére költöttek.

Mobilizáció

A hagyományos közgazdasági megközelítések a fent leírtaknál általánosabb társadalmi jellegzetességekből indulnak ki. A társadalom modernizációja során a családok, a lakóközösségek, a munkahelyek és a kortárs csoportok társas kapcsolataiban keletkező

[10] Levy (1996: 128).

zavarokat a nyilvános és a privát szektorban is mobilizációs stratégiák kompenzálják. A kormányzatok, a közigazgatási intézmények, a politikai pártok, az egyházak, a vállalatok – csakúgy, mint a sarki zöldséges, a szemközti pizzéria és a fodrász is – folyamatosan mint egyént szólítják meg az embert, abból a célból, hogy újra meg újra kapcsolatot teremtsenek vele, hiszen az ilyen kapcsolatok instabillá váltak, és minden lehetséges alkalommal fel kell újítani őket.[11]

A mobilizáció mint társadalmi szükséglet erejét nem szabad lebecsülnünk. A mobilizáció nemcsak a mások bevonására való igényt elégíti ki, hanem a bevonódásra való igényt is. Nem csupán a kormányzatok törekednek arra, hogy ügyeikbe bevonják a polgárokat, hanem a polgárok is szeretnének bevonódni (vagy legalábbis úgy érezni, hogy sikerült bevonódniuk) a kormányzatok ügyeibe. Attól függően, hogy a mobilizáció milyen mérvű kötődést helyez kilátásba, és milyen erős az igény az ilyesfajta kötődésekre, még az is könnyen megtörténhet, hogy a *PET*-ek által kínált névtelenség elveszíti vonzerejét. Másrészt igaz az is, hogy a privátszférához kötődő értékek ellenállónak bizonyulnak a mobilizációs kísérletekkel szemben, különösen, ha az utóbbiak túl otrombák. Ez nagy valószínűséggel két egymással párhuzamos fejleményt eredményez: a mobilizációs technikák kifinomultabbá válnak, hogy legyőzzék a névtelenség iránti vágy által generált ellenállást, a *PET*-rendszerek pedig olyan „átjárókat" vagy „kapcsolókat" tartalmaznak majd, amelyeknek a felhasználásával az alany – feltéve, hogy az általa meghatározott feltételeket továbbra is teljesítik – elérhető marad.

A privátszféra koncepciója

A *PET*-rendszerek nagy része még mindig a privátszféra olyan felfogásán alapul, miszerint az névtelenséget, illetve – a fejlettebb rendszerekben – a névtelenség és az azonosíthatóság közötti tudatos választást, vagy (a még kifinomultabb rendszerekben) az anonimitás különböző fokozatai közötti szabad választási lehetőséget jelent, ennek a felfogásnak azonban megvannak a maga korlátai. A privátszféra ilyetén felfogása figyelmen kívül hagyja azt a tágabb fogalmat, amit „a privátszféra politikai szemléletének" nevezek. A privátszféra politikai szemlélete a névtelenség választhatóságát a szabadságjogok összességének szerves *részeként* kezeli, egyfajta speciális kommunikációs módként sok más lehetőség között, és arra törekszik, hogy a hagyományos privátszférát kombinálja az aktívabb, részvételre orientált elemekkel.[12] A privátszféra ilyen politikai jellegű felfogásának a *PET*-koncepciókra való alkalmazása kétféle következménnyel jár. Először is, a *PET*-rendszereket meg kell nyitni a részvételt elősegítő elemek előtt. Ebből következik, hogy a *PET*-ek tervezésébe és a társadalmi rendszerekbe való beillesztésük folyamatába be kell vonni azokat, akiket a fejlesztés szolgálni hivatott. Másodszor, a *PET*-rendszereknek az eddiginél több olyan kapcsolót és modult kell tartalmazniuk, amelyek minden szituációban megkönnyítik a választást. Ez a

[11] McKenna (1991).

[12] Bas van Stokkom (1995: 53) említ egy anekdotát, amely szerint Louis Brandeis „A magánszférához való jog" *(The Right to Privacy)* után meg kívánta jelentetni *A nyilvánosság kötelessége* (The duty of publicity) című munkáját is.

rugalmasság nemcsak a fent leírt mobilizációs nyomást tudná kezelni, hanem a politikai kommunikációs lehetőségek szélesebb körébe is integrálná a *PET*-eket. A jelenlegi politikai folyamatoknak már részét képezik ilyen kommunikációs módozatok: a demokrácia mint részvételen alapuló társadalmi rendszer például egyesíti a névtelen részvétel (titkos szavazások, névtelen politikai pamfletek stb.) és az azonosítható beavatkozás (petíciók, parlamenti felszólalások, magánindítványok, nyílt szavazások) lehetőségeit. Az ilyen folyamatokba bevezetett valamennyi technikai eszköznek legalábbis fenn kell tartania a létező választási lehetőségeket, és meg kell könnyítenie, hogy az egyének egyrészt élni is tudjanak ezekkel, illetve meg is változtathassák ezeket.

Ezzel nem azt akarom mondani, hogy a hagyományos *PET*-eknek a privátszféra politikai koncepciójában nem lenne helyük, vagy csak korlátozott használati értékük lenne. Ezeket inkább kiegészítő megoldásoknak tekinteném.

A privát szféra és a PET-ek szerepe

Amikor egy idevágó régebbi szöveggel foglalkoztam, amely a legelső adatvédelmi törvénnyel (Hesse szövetségi állam adatvédelmi törvényével) nagyjából egy időben született,* rábukkantam egy olyan írásra, amely felhívta a figyelmet arra, hogy az adatvédelmi törvényeket nemcsak adatbiztonsági intézkedéseknek kell kísérniük, hanem a privátszférát biztosító technikai rendszereket is létre kell hozni.[13] Ha jól emlékszem, az erről a kérdésről folytatott németországi vitát nem kísérte túlságosan nagy figyelem. Az adatvédelmi hivatalok éves jelentéseiben még azt az alapvető szabályt is csak ritkán, és szinte a mellőzésébe beletörődő módon említették, miszerint az a legjobb adatvédelem, ha személyes adatok tárolására egyáltalán nem kerül sor. Az elkövetkező években a legnagyobb figyelmet az adatvédelemmel kapcsolatos ismeretek nemzetközi terjesztésére fordították, s végül nagy türelemmel sikerült odáig eljutni, hogy egyes országokban hasonló törvényt léptessenek életbe. Azután minden erőfeszítés a törvénykezés megfelelő adminisztrációjára és a technikai fejlődéssel való lépéstartásra irányult.

Eluralkodott a megszokás. Európában ez a rutin azzal fenyeget, hogy megakadályozza a privátszféráról alkotott felfogás újraértékelését, pedig folyamatosan figyelemmel kell követnünk a privátszféra társadalmi (vagy inkább különböző társadalmakon belül érvényesülő) percepciójának változásait, és készen kell állnunk arra, hogy újra átgondoljuk normatív előfeltevéseinket. Általában éppen ezt teszi a jogtudomány értelmezése, bár nyilvánvaló, hogy ez nem csupán a jogtudomány feladata, hanem olyan kötelezettség, amelyet minden esetben vállalnunk kell, amikor társadalmi környezetekben technikai rendszereket tervezünk. Ebben a helyzetben hasznosnak tűnik, ha néha vetünk egy pillantást azokra az érzékelési mechanizmusokra, amelyek lehetővé teszik a privátszféráról alkotott felfogás alakulásának figyelemmel követését. Azt a hosszú időszakot követően, amelyben a társadalomtudományok alig foglalkoztak ezzel a felfogással, most a filozófia és általában a társadalomtudomány is mintha lassacskán

* A németországi Hesse szövetségi állam adatvédelmi törvénye 1970-ben lépett életbe. – *A ford.*

[13] Steinmüller (1970: 88).

változtatna a hozzáállásán.[14] A továbbiakban három olyan irányzatra kívánok rámutatni, amelyekről úgy gondolom, hogy a privátszféráról alkotott felfogás és a *PET*-ek, illetve a *PET*-ekhez hasonló tervezési koncepciók jövőbeli fejlődése szempontjából relevánsak lesznek. Ebben a kontextusban három elemmel foglalkozom: az információegyensúllyal, az identitással és a bizalommal.

Információegyensúly

Amikor információegyensúlyról beszélek, korántsem az információs *érdekek* egyensúlyára gondolok. Az információs érdekek kiegyensúlyozása a hagyományosabb felfogásra, vagyis egy olyan folytonos „társadalmi szerződés" feltételezésére épül, amely egyensúlyt kíván teremteni az „adatalanyok" és más személyek (például az „adatkezelők") érdekei, illetve a társadalmi érdekek (közbiztonság, az állam gazdasági jóléte stb.) között. Az „egyensúly" kifejezéssel az alábbiakban az adekvát módon elosztott információs forrásokra, illetve a kommunikációs technológiák és a tervezési folyamatok hozzáférhetőségére utalok.

Erről a kérdésről újabban a távlözlési infrastruktúra kapcsán folynak viták, különösen a közszférában fellelhető információs források és a tömegtájékoztatás kapcsán. Sok szó esik a társadalmi kohézióról, az információ hozzáférhetőségéről és az elektronikus döntéshozatali folyamatokban való részvételről. Úgy látom, hogy a *PET*-ek jövőbeni fejlődésének releváns kérdései ebben a kontextusban két oldalról közelíthetők meg.

Először is, a *PET*-ek tervezési folyamatába az eddiginél közvetlenebb módon kell bevonni az egyes embereket, illetve az általuk választott képviseleti formákat. Annak a szükségességére már utaltam, hogy a privátszféráról alkotott hagyományos felfogást nyitottá kell tenni, amire a privátszféra politikai szemlélete adhat módot. Ebben az összefüggésben a *PET*-eket olyan „közművekként" is felfoghatjuk, amelyek tudakozódásra, részvételre ösztönöznek, és olyan döntéshozatali folyamatokat támogatnak, amelyek a hagyományos közművek irányítására jöttek létre. Az adatvédelmi ügynökségekre fontos szerep hárulhat az ilyen eljárások alkalmazásában a személyes információkat kezelő nagyméretű rendszerek, valamint az ezekbe beépített *PET*-komponensek tervezésénél és gyakorlati bevezetésénél egyaránt.

Másodszor, a *PET*-tervezés során figyelmet kell fordítani a részvételt igénylő folyamatokra is, különösen az „elektronikus demokrácia" kontextusában. A mobilizációhoz és a privátszféra különféle felfogásaihoz fűzött korábbi megjegyzéseim között felvetettem, hogy a túlságosan szűk értelmezés hajlamos figyelmen kívül hagyni a társadalom igényét a „bevonódásra", azt az igényt, hogy az egyént bátorítsák a politikai folyamatokban való részvételre, és hogy az egyén nyílt és azonosítható ellenvélemény-nyilvánítás, illetve elhatárolódó viselkedés révén hozzájárulhasson a társadalmi változásokhoz; vagyis ez a

[14] A politikatudományi és kortárs filozófiai trendek összefoglalását lásd például: Bennett (1996). A művészet területéről vett példák Julia Scher műveiből származnak.

[15] *MacIntyre v. Ohio Elections Commission*, 115 S. Ct. 1511 (1995); *Figari v. New York Telephone Company*, 303 N. Y. S. 2d. 245 (App. Div. 1969). Lásd továbbá Peritt (1996: section 6.2).

szűk értelmezés figyelmen kívül hagyja a „civil kurázsi" kinyilvánításának igényét. Másrészt az Egyesült Államok Legfelsőbb Bírósága egy közelmúltbeli határozatában újra megerősítette nemcsak a politikai viták során hallatott „anonim hangok" legitimitását, hanem ezeknek a politikai fontosságát is.[15] Szükségessé válhat tehát a politizáló individuum „digitális személyiségének"[16] rugalmas kezelése.

Identitás

A privátszférával kapcsolatos uralkodó felfogás egyik újabb keletű kritikai megközelítése azzal érvel, hogy a fogalom értelmezési tartományából hiányzik az identitás lényege. Az identitás nem állandó, hanem változik. Identitásunkat nem úgy alakítjuk ki, hogy másoktól elkülönítjük magunkat; identitásunk az, amit mások tudnak rólunk. Mások hatalmat gyakorolnak fölöttünk csupán azáltal is, hogy tudnak rólunk. Az, ahogyan mások látnak minket, nagyban befolyásolja azt, ahogyan mi látjuk magunkat. A ránk vonatkozó információ ebben az értelemben saját identitásunk alakítását jelenti. Ahhoz, hogy ilyen körülmények között biztosíthassuk az egyenjogúságot, be kell avatkoznunk már abba a folyamatba is, melynek során az információ befolyásolja a szubjektumot.[17] Ez a gondolat a közelmúlt társadalomelméleti munkáiból, és még inkább korábbi irodalmi művekből ismerősen csenghet,[18] ám a *PET*-eken eszközölhető változtatások tekintetében új perspektívákat nyit meg, és több lehetőséget kínál arra, hogy különféle nézőpontokból szemléljük magunkat. Ez visszavezet minket – ezúttal a politikai folyamatoktól eltekintve is – a *PET*-ekhez mint olyan rendszerekhez, amelyek eltérő társadalmi körülmények között a személyiség különböző megjelenési formáinak kezelését teszik lehetővé. Elképzelhető, hogy a *PET*-ek egyfajta „identitás-ügynökök" *(identity agents)* elektronikus kezelőivé válnak, és nyomon követik, hogy mit árulunk el magunkról, kinek, és milyen körülmények között. Így a *PET*-ek segítségével felidézhetjük, hogy például az interneten keresztül folytatott kommunikáció során mikor, kivel és hogyan viselkedtünk.

Bizalom

A *PET*-ek széles körű alkalmazásával kapcsolatban hangoztatott fő ellenérvek egyike az a szükségletünk vagy szokásunk, hogy önbizalommal felvértezve nézzünk szembe a lét bizonytalanságával, és megtartsuk vagy visszanyerjük biztonságunkat a bizonytalanság világában. Annak elemzésébe, hogy ez a trend vajon természetes velejárója-e azoknak a társadalmainkban végbemenő racionalizációs és iparosítási folyamatoknak, amelyek során oly sok kockázati helyzet alakul ki, hogy a biztonságra való igény folyamatosan új táptalajra lel, itt nem bocsátkozom bele.

[16] Clarke (1994).
[17] Poster (1995, 1990).
[18] Különösen Fernando Pessoa (1888–1935) művei.

A dolgok ilyetén alakulására válaszul kialakítható egyik lehetséges stratégia jegyében a társadalmi entitások közötti kapcsolatok fellazítását szorgalmazhatjuk, abból a célból, hogy e kapcsolatokat egymástól kevésbé függővé tegyük, és viszonylagos perspektívából szemlélhessük azokat a kritériumokat, amelyek – mint például a hatékonyság – minden társadalmi rendszert ugyanabba a logikai rendbe kényszerítenek.[19] Egy ilyen társadalmi modellben alapvető szerepet játszana a bizalom.[20]

A bizalom szót itt nem olyan értelemben használom, mint ahogyan a „megbízható harmadik fél" vagy a „megbízható rendszerek" kifejezésekben szokás. A jelen kontextusban inkább a működés szempontjából való megbízhatóság tűnik a megfelelő terminusnak: a szóban forgó rendszereknek adott valószínűségi határok között kell eleget tenniük bizonyos követelményeknek; arra hivatottak tehát, hogy megbízhatóak legyenek. Nem szükséges azonban, hogy az ilyen rendszerekben a szó hagyományos értelmében „megbízzunk". Ezek az adott valószínűségi határokon belül biztonságosak, használatukkal nem jár kockázat, vagy ha igen, az kiszámítható mértékű. A bizalom mint társadalmi jelenség fogalmához ugyanakkor hozzátartozik az is, ha a létező kockázat *ellenére*, tudatosan az interakció mellett döntünk. Az olyan jellegű kapcsolatok, amelyekben bizonyos (technikai vagy társadalmi természetű) eszközök szüntetik meg vagy csökkentik lényeges mértékben a kockázatot, alig hagynak teret a bizalom kinyilvánítására. Arra is kevés alkalmat nyújtanak, hogy az ember úgy érezhesse, bíznak benne és szükség van rá, illetve a részvételére. A társadalmat összetartó kötések ugyanakkor annál lazábbá válhatnak, minél kevesebb alkalommal érez így az ember.

Ebben az értelemben a bizalomnak fontos szerepet kell majd játszania a társadalmi rendszerek, különösen pedig az informatikai rendszerek tervezése során. Ez az állítás nem pusztán normatív jellegű, hanem egyben előrejelzés is. Egy pillanatra eltávolodva a „titkos megfigyelés" réme által gyakran előidézett paranoiától,[21] szeretném, ha az olvasó részt venne egy úgynevezett „metanoia"-kísérletben,[22] ami segíthet megvilágítani a lényeget. Ha más szemmel tekintünk azokra az alkalmakra, amelyek során a számítógépes adatkezelés biztonsága valamilyen csorbát szenvedett, és félretesszük a gondatlanság, az ártó szándék és az emberi ostobaság által okozott eseteket (mivel a bizalomnak tudatosan szelektívnek kell lennie), akkor azt látjuk, hogy a fennmaradó esetekben valamilyen formában ténylegesen a bizalom nyilvánult meg. Az ember hajlamos megmosolyogni, esetleg semmibe venni az ilyen eseteket. Könnyen lehet azonban, hogy a bizalom kinyilvánításának ezekkel az eseteivel kapcsolatban meg kell változtatnunk a véleményünket, és a lenéző mosoly vagy a gúny nem azokat illeti meg, akik túlságosan megbíztak valakiben, hanem inkább azokat, akik rácáfoltak a bizalomra. Ebből a perspektívából nézve a fenti esetek arra hívják fel a figyelmet, hogy különféle elektronikus környezetekben még mindig milyen gyakran kerül sor a bizalom kinyilvánítására. Ez legalábbis jóval gyakrabban történik meg, mint amit a titkos eszközökkel megfigyelt társadalomról folytatott viták jelezni látszanak.

[19] Bennett (1995: 30).
[20] Burkert és Rankin (1989), Burkert (1994).
[21] Lyon (1994: 218).
[22] Senge (1990).

Talán a bizalom adja meg a választ a jól ismert megfigyelési paradoxonra is. (A megfigyelést irányítani kell, ugyanakkor minden megfigyelési szint egy újabbat kíván, ez pedig végtelen regresszióhoz vezet: a megfigyelés megfigyelésének a megfigyelése és így tovább.) Az ilyen mechanizmusok ellenében a társadalom működőképességét az embernek az a képessége biztosítja, hogy a társas kapcsolatok során be tudja építeni a tudatos kockázatvállalást (vagyis a bizalmat) ezekbe a rendszerekbe. A *PET*-ek – már amennyire úgy tervezik meg őket, hogy könnyedén, ugyanakkor tudatosan és szelektív módon fedhessük fel identitásunkat – segíthetnek abban, hogy szélesebb teret biztosítsunk a bizalmat létrehozó és fenntartó társadalmi mechanizmusoknak. Arra bátoríthatnak minket, hogy legalábbis az eddiginél gyakrabban fontolóra vegyük, kívánunk-e interakciót folytatni nem teljesen biztonságos környezetekben.

Konklúzió

A *PET*-eket tekinthetjük olyan technikai újításoknak, amelyek segítenek megoldani egy sor társadalmi és politikai problémát. Meglehet, hogy legfontosabb tulajdonságuknak az bizonyul majd, hogy sikeres gyakorlati bevezetésük érdekében kénytelenek leszünk visszatérni a *társadalmi innovációhoz*. Ez pedig elvezet bennünket minden társadalomtudós, jogász, törvényhozó és privátszféra-szakértő fő feladatához: az információs és kommunikációs technológiák által felvetett kihívást a társadalom megújuló képességével szemben megnyilvánuló kihívásként kell elfogadnunk. Az adatvédelem szabályozása történelmi példát nyújt az ilyen társadalmi megújulásra. A *PET*-ek segítségével további kihívásoknak felelhetünk meg.

Ez a fejezet „A huszonegyedik századi privátszféra víziója: megoldások nyomában" című konferencián (Victoria, British Columbia, 1996) elhangzott előadás átdolgozott változata.

Irodalom

Az információ és a privátszféra védelmének biztosa (Ontario, Kanada) és Registratiekamer (Hollandia) (1995): *Privacy Enhancing Technologies: The Path to Anonimity.* I–II. kötet.

Bennett, Colin (1995): *The Political Economy of Privacy: A Review of the Literature.* Kiadatlan tanulmány.

– (1996): The political economy of privacy.

Burkert, Herbert (1979): Die Eingrenzung des Zusatzwissens als Rettung der Anonymisierung? *Datenverarbeitung im Recht, 8.*

– (1994): Electronic Trust and the Role of Law: A European Perspective. In *13th World Computer Congress 1994.* Ed. K. Brunnstein. 2. kötet.

Burkert, Herbert – Rankin, Murray (1989. június 26.): *The Future of the OECD Privacy Protection Guidelines: Building trust in Electronic Data Networks (ICCP).* Párizs: OECD.

Clarke, Roger (1994): The digital persona and its application to data surveillance. *Information Society,* 10. no. 2.

Elgesem, Dag (1996): Privacy, respect for persons and risk. In Ess, C. (szerk.): *Philosophical Perspectives on Computer-Mediated Communication.* New York.

Levy, Steven (1996): Wisecrackers. *Wired*, 4.03
Lyon, David (1994): *The Electronic Eye: The Rise of Surveillance Society.* Minneapolis.
McKenna, Regis (1991): *Relationship Marketing.* London
Peritt, Henry H. (1996): *Law and the Information Superhighway.* New York.
Poster, Marc (1990): *The Mode of Information.* Chicago.
Poster, Marc (1995): *The Second Media Age.* Cambridge.
Schneier, Bruce (1995): *Applied Cryptography.* 2. kiadás. New York.
Senge, Peter M (1990): *The Fifth Discipline.* New York.
Simitis, Spiro (1994): Lob der Unvollständigkeit – Zur Dialektik der Trasparenz personenbezogener Informationen. In *Gegenrede: Aufklärung–Kritik–Öffentlichtkeit.* Ed. H. Däubler-Gmelin et al. (Baden-Baden).
Steinmüller, Wilhelm et al. (1970): *EDV und Recht. Einführung in die Rechtsinformatik.* Berlin.
Stokkom, Bas van (1995): Citizenship and privacy: A domain of tension. In *Privacy Disputed.* Eds. P. Ippel et al. Hága.