1.8. Adatvédelem és nyilvánosság

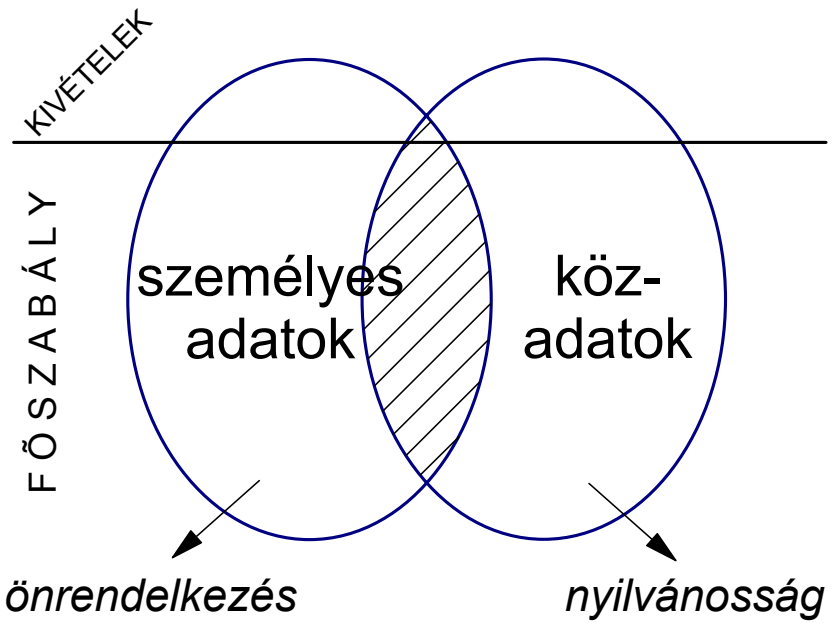
Szerző: Székely Iván

Lektor: dr. Vajda István

1.8.1. Alapmodellek

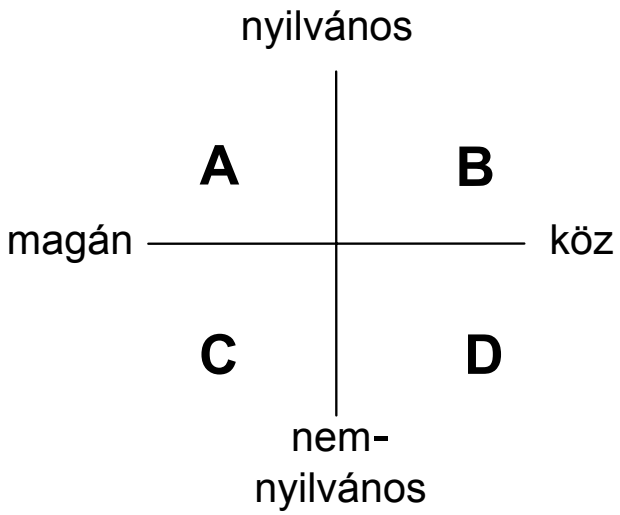
Az információktól a strukturált, visszakereshető formában rögzített adatokig és az adatoktól a kontextusba ágyazott, újraértelmezett információig terjedő teljes vertikum sajátos szempontú osztályozásának alapja az adatok és információk személyes, illetve közérdekű volta. E két alapkategória lefedi az információs rendszerekben kezelt és a távközlő hálózatokon továbbított adatok teljes körét (1.8.1. ábra). Noha ez a kategorizálás eltér a távközlés és az informatika területén szokásos műszaki-tudományos osztályozás logikájától, mégis olyan alapvető szabályokat vezet be, amelyek meghatározzák az adatkezelés kereteit és befolyásolják annak műszaki megvalósítását. E szabályok nem csupán jogi vagy társadalomtudományi jellegűek: az adatkezelés filozófiájától annak tételes alapelvein, a jog, a szabályozás és önszabályozás eszközein át az információs-kommunikációs technológiáig terjednek, s végső soron a korszerű adatkezelés közegében a nyilvánosság és titkosság alapvető kereteit határozzák meg.

Az ábrán látható *Székely-féle* (filozófiai-jogelméleti indíttatású) *modellben* mindkét alapvető adatkategóriára egy-egy főszabály vonatkozik: a személyes adatokra az önrendelkezés, a közadatokra a nyilvánosság. (E két fogalom jogi terminológiában használt megfelelője az információs önrendelkezés, illetve az információszabadság.) A vonal alatti területeken érvényesülnek a főszabályok, a vonal felett a kivételek. Az átfedő (satírozott) terület azon személyes adatokat tartalmazza, például a közfunkciót betöltő személyek e tevékenységével összefüggő személyes adatait, amelyekre nem az önrendelkezés, hanem a nyilvánosság főszabálya vonatkozik. A Székely-féle alapmodell kritikája, hogy nem jeleníthetők meg rajta a nem állami (üzleti, társadalmi) szervezetek adatkezelési viszonyai. Továbbfejlesztett változata ezért nem három, egymást részben átfedő körből vagy ellipszisből áll, hanem három hosszúkás, ívelt idom gyűrűjéből, ahol a szomszédos



idomok végei átfedik egymást. *Heller* és *Rényi* (szociológiai-tömegkommunikációs indíttatású) modelljében az információ magán–köz, és nyilvános–nem nyilvános attribútumai egymástól függetlenül, egy kétdimenziós koordinátarendszerben jelennek meg, s az így létrejövő négy tartományból kettőt "természetesnek", kettőt pedig magyarázatot igénylőnek, azaz kivételesnek tekinthetünk (1.8.1./b ábra).

Az adatok bárki számára, vagy csakis meghatározott személyek számára hozzáférhetővé tételét, és mások számára hozzáférhetetlenné tételét számos jog és érdek határozza meg. E jogok és érdekek testesülnek meg a hagyományos, nevesített titokkategóriákban, s érvényre juttatásukhoz az információs technológia mindenkori állásának megfelelő eszközök és eljárások tartoznak. Fontosabb nevesített titokkategóriák: üzleti titok, államtitok, szolgálati titok, magántitok, ügyvédi titok, orvosi titok, banktitok, gyónási titok stb. E kategóriák egy része (pl. orvosi titok) ráerősít a főszabályokra, más része (pl. államtitok) azok jelentős kivételeit képezik, s ennek megfelelően a modell különböző tartományaiban helyezhetők el. Általános jellemzőiket többnyire törvények és más jogszabályok, etikai kódexek tartalmazzák; konkrét alkalmazásukat e kereteken belül az információs rendszerek felelős kezelői határozzák meg. A személyes/közérdekű dichotómia azonban e titokkategóriák alkalmazásakor is érvényesül.

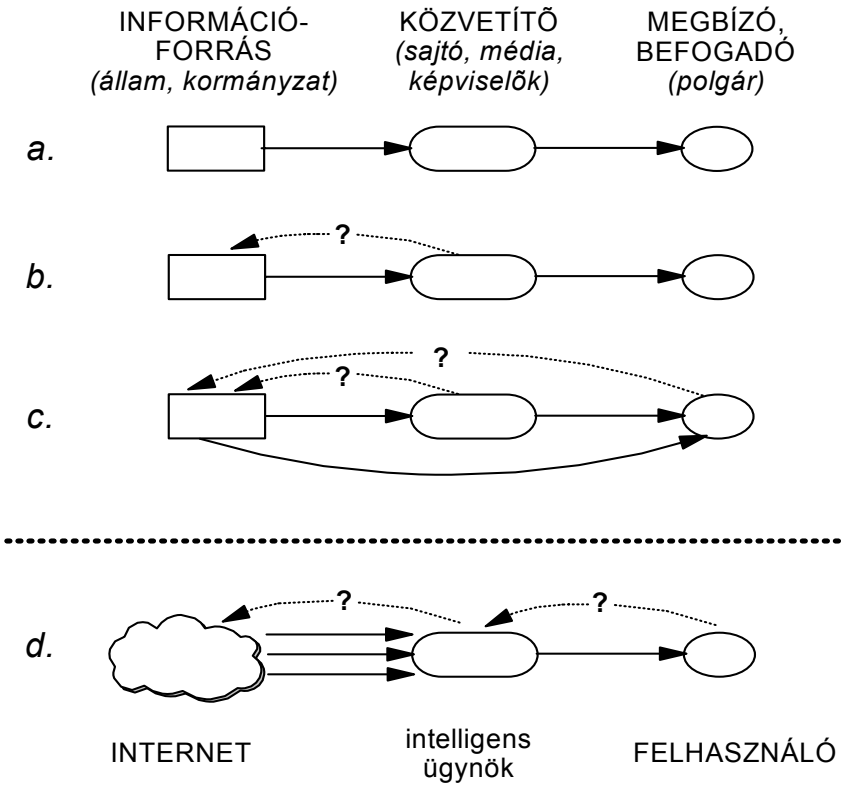


1.8.1./b ábra

Érdemes megjegyezni, hogy a fenti adatkezelési kategóriák és főszabályok már jóval a gépi adatfeldolgozás és a korszerű távközlés megjelenése előtt kialakultak, aktualitásukat azonban ezek elterjedése jelentősen erősítette. A mindenkori korszerű informatika és távközlés alkalmazása ugyanis számos elméleti és gyakorlati problémát vet fel az egyén és az információs hatalom, vagy más kapcsolatrendszerben az állam és az állampolgár, az üzleti szféra és az ügyfél, vagy általánosságban az információs szempontból erősebb és gyengébb fél viszonyában. E problémák egyik fő ága a személyes magánszféra információs határainak megváltozásából, az információs hatalom *mint az egyént ellenőrző és befolyásoló tényező* koncentrálódásából, a másik fő ága az egyén társadalmi részvételét meghatározó információs státusának megváltozásából, az információs hatalom *mint közinformációkat kezelő monopólium* koncentrálódásából ered.

Míg az információs önrendelkezés biztosításának történelmi folyamatát egyensúlyi állapotok és azoknak az új ICT által indukált felbomlási szakaszai sorozataként értelmezhetjük, az információszabadság elvi és gyakorlati megvalósulását evolúciós folyamatként. [1.8.2.]

A közinformációhoz való hozzáférés evolúciós modellje



1.8.2. ábra

Az *a.* szakaszt, leegyszerűsítve, a *képviseleti demokrácia* információs modelljének tekinthetjük: a képviselő (és az átvitt értelemben a polgárt képviselő sajtó) eljuttathatja a közinformációkat azok forrásától a befogadókig. A *b.* szakasz a *sajtószabadság* modellje: a "képviselő" nemcsak közvetíthet, hanem privilégiumait kihasználva követelhet is információkat, s azokat eljuttathatja a befogadókig. A *c.* szakasz a ma aktuális *információszabadság* modellje: a befogadó maga is közvetlenül követelhet információkat és azokat a közvetítő kiiktatásával kaphatja meg. (Az információk közvetítése a korszerű ICT alkalmazásával vagy anélkül is történhet.)

Az információszabadság joga az internet használatának általánossá válásával a *dezintermediáció* illúzióját veti fel. A közvetítők kihagyása azonban nemcsak azért illúzió, mert a globális hálózaton (jogszerűen) eleve csak az az információ található meg, amit oda valaki a nyilvános hozzáférés biztosítása céljából feltett, hanem azért

is, mert a felhasználó két alapvető problémával: a mennyiségi és a minőségi problémával szembesül. E problémák részleges orvoslására született reintermediációs megoldások egyike a *d.* szakasznál ábrázolt *intelligens ügynök* alkalmazása, ahol a személyre szóló tudásbázist tartalmazó ügynök előszelektálja, mintegy előemészti a befogadó által kért információt. (Meg kell jegyezni azonban, hogy a közinformációkhoz való hozzáférés megkönnyítésére alkalmazott ügynök egyúttal a felhasználó manipulálásának egyik leghatékonyabb, ma még kevéssé ellenőrizhető eszköze.) Itt az "internet" természetesen csak virtuális információforrás, mögötte valódi forrás áll; a szereplők megváltozását a szaggatott vonal jelzi.

1.8.2. Meghatározások

Az adatkezelés fenti attribútumaihoz kapcsolódó fogalmak egységes használata ma már általános követelmény a korszerű információs és távközlő szolgáltatásokban. (Magyarországon még ma is születnek színvonalas művek téves/elavult fogalomhasználattal, s a műszaki értelmiség körében az adatvédelem/adatbiztonság fogalom-páros ma is sok esetben félreértések forrása.) Az alábbiakban a legfontosabb fogalmak rövid meghatározását adjuk a nemzetközileg elfogadott terminológia alapján.

Adatvédelem (data protection): a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. (Az adatvédelem fogalmilag csak személyes adatok esetében értelmezhető.)

Adatbiztonság (data security): itt használt értelmében az adatok jogosulatlan megszerzése, módosulása és tönkremenetele elleni műszaki és szervezési megoldások rendszere. (Az adatbiztonság személyes és nem személyes adatok esetében egyaránt értelmezhető.)

Röviden: az adatvédelem az *adatalanyok* védelme, az adatbiztonság maguké az adatoké.

Személyes adat: a meghatározható természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintett személlyel kapcsolatba hozható

következtetés. Személyes minőségét az adat mindaddig megőrzi, amíg kapcsolata az érintettel helyreállítható.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot vagy egyéb közfeladatot ellátó szerve vagy személy kezelésében lévő, a személyes adat fogalmába nem tartozó adat. (Az adat közérdekű mivoltában tehát nem annak deklarálása, nem az adatkezelő tulajdoni formája, hanem a közfunkció a döntő elem.)

Adatalany: az érintett személy, akivel az adat kapcsolatba hozható.

Adatkezelés: az alkalmazott eljárástól függetlenül a személyes adatok felvétele, tárolása, feldolgozása, hasznosítása, megváltoztatása, továbbítása, nyilvánosságra hozatala.

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül az alkalmazott eszköztől és módszertől.

Adatkezelő: az a természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, aki (amely) az adatkezelés célját meghatározza, a rá vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, aki (amely) az adatkezelő megbízásából személyes adatok feldolgozását végzi. (Adatkezelő és adatfeldolgozó tehát önálló szerv vagy személy; kapcsolatuk ma jellemző példája az *outsourcing.* Az adatkezelés jogszerűségéért az adatkezelő felel.)

1.8.3. Az adatvédelem alapelvei

Az információs önrendelkezés főszabálya és kivételei érvényre juttatásának következő szintjét a nemzetközileg elfogadott tartalmú, tételesen megfogalmazott adatvédelmi alapelvek képezik. Az alábbiakban az alapelveket az OECD Adatvédelmi Irányelveinek [1.8.2.] csoportosítását követve, kivonatosan ismertetjük.

1. *Az adatgyűjtés korlátozásának elve*

Személyes adatok gyűjtése csak törvényes és tisztességes eszközökkel, az adatalany tudtával és belegyezésével történhet.

2. Az *adatminőség elve*

Az adatoknak az adatkezelés céljával összhangban pontosnak, teljesnek és aktuálisnak kell lenniük.

3. A célhozkötöttség elve

Személyes adatokat csak előre meghatározott célból, csak a cél megvalósulásához szükséges mértékben és ideig lehet kezelni.

4. A *korlátozott felhasználás elve*

Az adatokat csak az adatalany hozzájárulásával vagy törvényi felhatalmazással lehet felhasználni.

5. A *biztonság elve*

Az adatokat a technika mindenkori állásának megfelelő ésszerű intézkedésekkel védeni kell a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás, sérülés és megsemmisülés ellen.

6. A *nyíltság elve*

Az adatkezelés tényének, helyének és céljának, az adatkezelő személyének, valamint az adatkezelési politikának nyilvánosnak kell lennie.

7. A *személyes részvétel elve*

Az adatalany megismerheti a rá vonatkozó adatokat, azokat (ha helyénvaló) helyesbítheti, kiegészítheti vagy töröltetheti.

8. A *felelősség elve*

Az adatkezelő a felelős a fenti elvek betartásáért, s bizonyítani kell tudnia az adatkezelés jogszerűségét.

1.8.4. Nemzeti és nemzetközi szabályozás

Az adatvédelem következő szintjét a nemzetközi szerződésekben, irányelvekben és más dokumentumokban meghatározott feltételek és követelmények rendszere alkotja. A legfontosabb nemzetközi dokumentumok: az OECD Adatvédelmi Irányelvei, az Európa Tanács Adatvédelmi Egyezménye [1.8.3.] és az Európai Unió Adatvédelmi Direktívája. [1.8.4.] Megjegyzendő, hogy a magyar jogi szakirodalom a direktívát is általában "irányelv"-nek fordítja; az eredeti kifejezés megtartását az indokolja, hogy az irányelv (guidelines) követése nem kötelező, míg a direktívában (directive) foglaltak bevezetése a belső jogba igen.

Az 1980-ban született OECD irányelvek és az 1981-es ET egyezmény párhuzamosan készült, mindkettő tartalmazza az adatvédelmi alapelveket, de amíg az OECD irányelvek a határátlépő adatáramlás szükségességét (és annak garanciáit) hangsúlyozza, addig az ET egyezmény célja az információs jogok biztosítása a határátlépő adatáramlásban. További különbség, hogy az irányelvek követése csak ajánlott, az egyezmény betartása pedig kötelező a csatlakozó országok számára (Magyarország 1993-ban aláírta, 1997-ben ratifikálta és 1998-ban kihirdette az egyezményt).

Az 1995-ben, ötéves vita után elfogadott EU direktíva az adatkezelés azon közös, részletes szabályait határozza meg, amelyeket az EU tagállamoknak kötelező belső jogukba emelniük; ennek határideje 1998 októbere volt. Amelyik országnak volt korábbi adatvédelmi törvénye és gyakorlata, azt szükség esetén hozzá kellett igazítani a direktíva előírásaihoz, az újonnan hozott jogszabályok, tagfelvételre váró országokban is, már a direktíva szellemében készültek.

Ahogy Colin Bennett kanadai politológus már a nyolcvanas években felismerte, az adatkezelés terén nemcsak technológiai konvergencia, hanem "policy konvergencia" is tapasztalható. Fontos gyakorlati következményekkel jár azonban, hogy amíg az ET egyezmény a szerződő országok számára *azonos (ekvivalens) védelmet* ír elő, addig az EU direktíva csak *megfelelő (adekvát) védelmet*. Az egyezményen, és az EU tagországain kívüli, harmadik országba ugyanis csak akkor lehet korlátozások nélkül, például automatikus távközlő és információs rendszerek segítségével személyes adatokat továbbítani, ha a harmadik ország a megkövetelt adatvédelmi szintet képviseli. Az ekvivalens védelem azonos szabályozást és gyakorlatot követel, az adekvát védelem viszont eltérő szabályozási környezetben és alternatív eszközök és módszerek alkalmazásával is elképzelhető.

Az adekvát védelem problémája kiélezetten jelentkezik az EU és az Egyesült Államok vitájában. Az európai és az amerikai modell eltéréseit az *1.8.1.. táblázat* foglalja össze. Az európai modellt a nyugat-európai országok és a fejlettebb új demokratikus országok képviselik, az amerikai modellt (kisebb eltérésekkel) az USA, Ausztrália, Új-Zéland, valamint – korábban – Kanada.

Egy nem-adekvát védelmi kategóriába tartozó országgal szemben a személyes adatok határátlépő áramlásában korlátozásokat kell alkalmazni, s ez a globalizálódó információáramlás korszakában jelentős gazdasági és politikai

	Európai modell	Amerikai modell
Szektor:	magán + köz	köz
feldolgozás:	automatikus + manuális	automatikus
Lefedés:	Általános	mozaikszerű
ellenőr:	Van	nincs

1.8.1. táblázat. Adatvédelmi szabályozás

következményekkel járhat. Jelenleg az EU illetékes testületei, ellentmondó határozatok sora után, ideiglenes jelleggel adekvát adatvédelmi szintűnek fogadja el a Safe Harbor Principles elnevezésű, az adatkezelők önkéntes csatlakozásán és önkorlátozásán alapuló elvek követőinek tevékenységét, a csatlakozók száma azonban alacsony, az elvek megsértésének pedig nincs szankciója. Magyarország, Svájc után második EU-n kívüli országként 2000-ben hivatalosan megkapta az adekvát státust.

A nemzetközi szinten meghatározott adatkezelési kritériumok azonban közvetlenül is alkalmazandók az adatkezelési rendszerek tervezésében és működtetésében: az adatalany hozzájárulásának három, az EU által meghatározott kritériumának (önkéntesség, határozottság, tájékozottság) például a webes felületű online adatkezelési rendszereknek is eleget kell tenniük. Hasonlóképpen, a személyes részvétel elvének érvényesíthetősége (például az egyénekkel kapcsolatba hozható tranzakciók elkülöníthetősége és visszakereshetősége) az adatalanyok átgondolt azonosítási rendszerének kialakítását igényli az adatbázisokban.

A *belső (nemzeti) jog* az adatvédelem soron következő szintje. A magyar szabályozás korszerű, az európai hagyományokat követi. Sajátossága, hogy az adatvédelmet és az információszabadságot egy közös törvény szabályozza. A szabályozás vertikuma az Alkotmánytól a keretjellegű Adatvédelmi törvényen [1.8.5.] át a szektorális adatvédelmi törvényekig, és rendeletekig terjed.

A nemzeti adatvédelmi jog érvényesülését független ellenőri intézmények ellenőrzik. Ezek hatáskörüket és legitimitásukat tekintve többfélék: lehetnek testületek, mint a francia CNIL (Commission Nationale de l'Informatique et des Libertés), egyszemélyi tisztségek, mint a brit Information Commissioner (korábban Registrar); választhatja őket parlament (Németország) vagy kinevezheti kormány (Hollandia); jogosítványaik lehetnek hatósági, bírói vagy ombudsmani jellegűek. A

magyar adatvédelmi biztost a másik két országgyűlési biztossal együtt 1995-ben választotta meg először a Parlament; jogosítványai ombudsmani jellegűek és mind az adatvédelem, mind az információszabadság területére kiterjednek. Tevékenységének súlypontját a panaszügyek kivizsgálása képezi, de hivatalból is indíthat vizsgálatot állami és magánszektorbeli adatkezelőknél egyaránt. Vizsgálatának eredményei ajánlások, amelyek követése jogi értelemben nem kötelező, elfogadottságuk aránya azonban magas. Véleményezi az adatkezelést érintő jogszabályok tervezetét és ellenőrzi az állam- és szolgálati titokká minősített adatok minősítésének indokoltságát. Titokfelügyeleti jogosítványa hatósági jellegű, visszaminősítésre vonatkozó felhívásait végre kell hajtani. [1.8.6.]

1.8.5. PET technológiák

Az adatvédelmi elvek és rendelkezések megvalósításának technológiai szintjét képviselő PET (Privacy Enhancing Technologies) összefoglaló néven ismert változatos információs és kommunikációs technológiákat abból a célból fejlesztették ki, hogy ne csak az adatokat, hanem az adatok *alanyait* is védjék a visszaélések ellen. A PET technológiák célja a tágabb technológiai környezet által okozott magánéleti sérelmek kifejezett csökkentése; közelebbről az, hogy az új technológiák által nyújtott előnyöket a személyes magánszféra további sérelme nélkül (vagy e sérelmeket legalább is mérsékelve) lehessen igénybe venni. A rendeltetésszerűen használt PET eszközök és rendszerek mindig a *gyengébb felet* (jellemzően az adatalanyt) védik az információs túlhatalommal rendelkező erősebb féllel szemben.

A PET technológiák többféle szempont szerint csoportosíthatók.

(a) A *Burkert-féle csoportosítás* [1.8.7.] szerint vannak

- szubjektum-orientált,
- objektum-orientált,
- tranzakció-orientált, és
- rendszer-orientált technológiák.

Az első esetben a technológia az adatalanyra irányul (pl. kártyabirtokosok anonimitásának biztosítása), a második esetben az eszközre (anonim fizetőeszközök), a harmadik esetben a hálózati tranzakció nyomainak eltüntetése a

cél, a negyedik esetben pedig több technológia rendszerszerű közös alkalmazásáról van szó.

(b) Más szempont szerint megkülönböztethetünk

- meglévő rendszerek biztonságát növelő technológiákat,
- új adattárolási és -hozzáférési technológiákat, és
- tranzakció-alapú technológiákat.

(c) Csoportosíthatjuk a PET technológiákat aszerint, hogy melyik adatvédelmi alapelv érvényesülését segítik elő.

(d) Végül megkülönböztethetünk

- technológia-alapú, és
- humán interakció alapú
- PET-eket.

Fontos megjegyezni, hogy ugyanannak a halmaznak többféle szempont szerinti felosztásáról van szó. Néhány példa PET alkalmazásokra:

Bioscrypt. A biometrikus rejtjelezés (biometric encryption) két kiinduló elemből, egy biometrikus elemből (pl. digitalizált ujjlenyomat) és egy nem-biometrikus elemből (pl. kulcs, PIN vagy pointer) hozza létre a bioscryptet. A bioscryptes alkalmazások működtetésének feltétele a biometrikus elem forrásának produkálása, vagyis az adatalany jelenléte. A biometrikus rejtjelezés sajátos alkalmazásai közé tartozik az "anonim adatbázis", ahol a személyazonosító adatok és a lényegi adatok egy adatbázis mezőiben kvázi-véletlenszerűen vannak elszórva, s a köztük lévő kapcsolatot a bioscryptben lévő pointer tartalmazza. A (b) csoportosítás szerint új adattárolási és hozzáférési technológiáról van szó, amely a (c) szerint a célhozkötöttség elvének érvényesülését segíti elő. Felhasználható hálózaton történő személyközi kommunikáció résztvevőinek és az üzenet tartalmának illetéktelenek előli elrejtésére; ehhez a partnereknek közös bioscryptet kell előállítaniuk, amelyet bármelyikük biometrikus elemével (ujjlenyomatával) fel lehet bontani, s felszabadíthatják a bioscryptbe csomagolt szimmetrikus kulcsot. Felhasználható továbbá elektronikus kereskedelmi alkalmazásokban: itt három résztvevős adatkapcsolatról van szó (Bank, Ügyfél, Bolt), ugyancsak közös bioscrypttel, de a Bank itt ujjlenyomat vagy hasonló biometrikus elem helyett egy megfelelő bonyolultságú egyedi mesterséges mintázatot használ a bioscrypt előállításához.

Platform for Privacy Preferences (P3P). Internetes, jellemzően angol nyelvű elektronikus kiskereskedelmi alkalmazásokra kifejlesztett technológia, amely a távoli adatkezelő és az adatalany közti személyesadat-áramlást egy standardizált alkufolyamattá alakítja. Humán interakció alapú technológia, amely egyúttal a személyes részvétel elvének érvényesülését segíti elő (az adatalany tudtával és ellenőrzésével kerülnek adatai a távoli adatkezelő birtokába).

Anonim remailer. Elektronikus levelező szolgáltatások, amelyek nemcsak az üzenet tartalmát, hanem annak tényét, időpontját, gyakoriságát, résztvevőinek kilétét is elrejtik az illetéktelen megfigyelő elől. Fejlett (Mixmaster típusú) változataik az üzenetek késleltetését, véletlenszerű továbbítását, az azonos üzenetek kiszűrését, a remailerek láncbafűzését, valamint szabványos üzenetméretet és rétegesen kódolt formátumot alkalmaznak.

Digitális fedőnevek. Számos PET alkalmazás kínál internetes szolgáltatások felhasználóinak ún. *nym*-eket. Ezek az egyedi digitális fedőnevek az egyes adatkezelőkkel vagy bizonyos típusú szolgáltatókkal való kapcsolat állandó *alias*-aiként, vagy egyszer használatos azonosítókként használhatók fel.

Hitelesítés azonosítás nélkül. A pénzinformatikai alkalmazások céljára kifejlesztett PET technológiák egyik alapkérdése a "hitelesítés kontra azonosítás" problémája. Az elméleti kutatások és a létező rendszerek tapasztalatai egyaránt igazolják, hogy a bank mint adatkezelő lemondhat az ügyfelek tranzakcióinak teljes körű ismeretéről, s ez paradox módon erősíti a rendszer adatbiztonsági szintjét, egyúttal biztosítja a tranzakciók hitelességét. A két elvi megoldás egyike a tranzakció részekre bontása oly módon, hogy a hitelesítés a tranzakció egészén végigkövethető legyen, az azonosítás azonban mindig csak két-két pont között jöjjön létre, s az egyes pontokon az egyedi ügyfélazonosítón egyirányú (nehezen visszafejthető) átalakítás történjen. A másik megoldás az ismétlődő, triviális tranzakciók egyszer használatos digitális fedőneveken történő bonyolítása.

1.8.6. . Adatvédelmi szakértelmek, teendők

A technológiai konvergencia és az online szolgáltatások terjedése szükségessé teszi az adatvédelmi követelmények gyakorlati érvényesítésének hozzáigazítását a változó technológiai, jogi és szervezeti környezethez. Különös

figyelmet igényel az adat és az adatalany közötti kapcsolatba hozhatóság kritériumainak rögzítése, a kapcsolat helyreállíthatóságának értelmezése, továbbá az adatkezelések összekapcsolhatósági feltételeinek, az adatalany online hozzájárulásának adatvédelmi szempontú biztosítása, valamint az adattovábbítás (különösen az automatikus adattovábbítás) feltételeinek meghatározása, a betekintési és törlési jog érvényesíthetőségének biztosítása, az adatkezelő és adatfeldolgozó viszonyának és funkcióinak meghatározása.

Az adatvédelmi követelmények érvényesítéséhez mind statikus, mind változó környezetben rendszerszemléletű, a tágan értelmezett informatikai, jogi és társadalomtudományi ismereteket magában foglaló szakértelem szükséges. Az adatkezelések adatvédelmi követelményeit, szervezeti szintű eljárási szabályait és felelősségi viszonyait célszerűen belső *adatvédelmi szabályzat* tartalmazza. Az adatkezelések adatvédelmi szempontú ellenőrzésének célszerű módja az *adatvédelmi auditálás,* amely egységes rendszerben vizsgálja a szervezet személyesadat-kezelésének folyamatát, az alkalmazott eljárásokat és technológiákat, a személyesadat-tartalmú termékeket és szolgáltatásokat. (Az adatvédelmi audit nem azonos az *adatbiztonsági* audittal, az utóbbinak egyes eredményei azonban részét képezik az adatvédelmi auditálás során vizsgált területeknek.) Előzetes adatvédelmi szempontú vizsgálatot indokolt végezni új személyesadat-kezelési rendszerek tervezésénél, felépítésénél. Az adatvédelmi státust rendszeresen ellenőrizni szükséges.

Irodalomjegyzék

[1.8.1.] Székely Iván: Az adatvédelem és az információszabadság filozófiai, jogi, szociológiai és informatikai aspektusai. Kandidátusi értekezés. Budapest, 1994.

[1.8.2.] Guidelines on the Protection of Privacy and Transborder Flow of Personal Data. Organisation for Economic Co-operation and Development (OECD), Paris 1980.

(Magyarul: Az OECD Tanács ajánlása a magánélet védelmét és a személyes adatok határátlépo áramlását szabályozó irányelvekre. In: INFORMATIKA ? JOG ? KÖZIGAZGATÁS, Nemzetközi dokumentumok I., InfoFilia, Budapest 1991., 5.1–5.39 old.)

[1.8.3.] Convention for the protection of individuals with regard to automatic processing of personal data. Council of Europe, Strasbourg, 28 January, 1981. European Treaty Series No. 108. (Magyarul: Egyezmény a személyiségnek a személyes adatok automatikus kezelésével kapcsolatos védelmérol. In: INFORMATIKA ? JOG ? KÖZIGAZGATÁS, Nemzetközi dokumentumok I., InfoFilia, Budapest 1991., 3.1–3.55 old.)

[1.8.4.] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities No. L 281/31, 23.11.1995

(Magyarul: Az Európai Parlament és a Tanács 95/46/EC Irányelve az egyénnek a

személyes adatok feldolgozásával kapcsolatos védelmérol és ezeknek az adatoknak

a szabad áramlásáról. Adatvédelmi Biztos Irodája, Budapest 1995.)

[1.8.5.] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

[1.8.6.] Az adatvédelmi biztos beszámolója 1995–96, 1997, 1998, 1999, 2000 Budapest.

[1.8.7.] Herbert Burkert: Privacy-Enhancing Technologies: Typology, Critique, Vision.

In: Agre, P.E. – Rotenberg, M. (eds.): Technology and Privacy: The New Landscape.

MIT Press, 1997.