COLIN BENNETT

Információpolitika és adatvédelem: a szabályozás nemzetközi fórumai

Bennett a személyes adatok védelmére kialakított európai és észak-amerikai jogi eszközöket hasonlítja össze. Mivel Amerikában az „információs privát szféra” (information privacy), Európában pedig a „személyes adatok” (personal data) védelmére eltérő szabályozási eszközöket alkalmaznak, elkerülhetetlennek látja egységes nemzetközi szabályozás kialakítását. A globális szabályozást ezen a különféle szereplők sokaságát, valamint igen változatos koordinációs és működési módozatokat magában foglaló komplex területen a szellemi tulajdon védelmének megoldásaihoz hasonlítja, a személyes adatok határokon átívelő továbbításának kereskedelmi kontextusában. Víziója szerint a globális szabályozás egyik lehetséges színtere a Világkereskedelmi Szervezet (World Trade Organization, WTO).

Szerzői információ:

Colin Bennett
Kanadai adatvédelmi szakértő, egyetemi tanár. PhD-fokozatát az Illinoisi Egyetemen szerezte. Kutatási területe az információs privát szféra és a személyes adatok védelmének összehasonlító elemzése nemzeti és nemzetközi szinten. Számos adatvédelemmel foglalkozó könyv és tanulmány szerzője. 1998-ban az Európai Bizottság számára készített jelentést az adatvédelem megfelelő szintjének kidolgozásáról.

Így hivatkozzon erre a cikkre:
Bennett, Colin. „Információpolitika és adatvédelem: a szabályozás nemzetközi fórumai”. *Információs Társadalom* V, 2. szám (2005): 75–97.
https://dx.doi.org/10.22503/inftars.V.2005.2.5

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

Colin Bennett

Információpolitika és adatvédelem: a szabályozás nemzetközi fórumai*

Ez a tanulmány egy előadás alapján készült, amelyet egy nemzetközi konferencián tartottam Chicagóban, 2002 októberében.[1] A konferencia a szellemi tulajdon kérdéseivel foglalkozott. Vendéglátóim előzékenyen repülőgéppel biztosították utazásomat Chicagóba, és ott tartózkodásom idején nagy vendégszeretetet tanúsítottak irántam. Fedezték a költségeimet, és szép tiszteletdíjat fizettek. Ez utóbbiak lebonyolítása érdekében a szervezők tájékoztattak, hogy költségeim megtérítése sokkal könnyebb lenne, ha rendelkeznék amerikai társadalombiztosítási számmal *(Social Security Number, SSN)*. Van-e ilyen számom? Ha nincs, kérvényezhetném-e, hogy legyen? Az utóbbi eshetőségre számos terjedelmes űrlapot kaptam. Érdeklődtem, bár hiába, hogy a kanadai társadalombiztosítási számom vajon megfelelhetne-e erre a célra, végül is a két ország között létezik adóegyezmény. Futólag még azt is fontolgattam, hogy kitalálok egy számot. Eszembe jutott, hogy a magánszféra védelmének egyes radikális szószólói írtak arról, hogy új, érvényes társadalombiztosítási számot hogyan lehet kitalálni, természetesen mások jogainak veszélyeztetése nélkül.

Az 1980-as évek elején azonban történetesen az Illinoisi Egyetem diákja voltam, ott készítettem el politikatudományi PhD-disszertációmat, és azokban az években ténylegesen volt társadalombiztosítási számom. Erre viszont nem tudtam visszaemlékezni, és úgy tűnt, hogy nincs már semmi olyan dokumentum a birtokomban, amelyen ez a szám szerepelne. Ugyanakkor rájöttem, hogy az Illinoisi Egyetem adminisztratív szervezetének a labirintusában valahol léteznie kell valami nyilvántartásnak, ami tartalmazza a számot. Így tehát megpróbáltam – sajnos sikertelenül – érintkezésbe lépni a régi tanszékemmel, majd valakivel a diákok tanulmányi eredményeit nyilvántartó osztályról *(Student Transcript Department)*. Ez utóbbitól azt a tájékoztatást kaptam, hogy igen, megvan a társadalombiztosítási számom, és ők azt valóban meg tudják küldeni a konferencia szervezőinek, tehát a közvetlenül előttem álló probléma megoldódott. Ez után azonban megkértem a nyilvántartási osztályt, hogy a számot küldjék meg nekem is, arra az esetre, ha a jövőben ismét szükségem lenne rá. A válasz érdekes volt számomra, mivel azt mondták, hogy az „én" számomat az egyetem adminisztrációján belül továbbíthatják, nekem azonban e-mail útján nem küldhetik meg. Kizárólag úgy juthatok hozzá, ha megrendelek egy hivatalos másolatot az indexemről vagy a diplomámról. Az előbbinek az ára öt dollár, az utóbbié pedig négy dollár. A megrendelést, amelyben e dokumentumok valamelyikét vagy mindkettőt igényelem, fax útján kellene hozzájuk el-

* A tanulmány a *Journal of Law, Technology and Policy* című folyóirat 2002. decemberi számában jelent meg először.

[1] Colin J. Bennett – Charles D. Raab: *A privát szféra védelmének szabályozása: stratégiai dokumentumok globális perspektívában. (The Governance of Privacy: Policy Instruments in Global Perspective.* Aldershot: Ashgate Press, 2003).

küldenem, önmagam megfelelő azonosításával és egy hitelkártyaszám megadásával, hogy a költségeket leszámlázhassák. Még azt is megmondták, hogy ezt ajánlatos lenne minél hamarabb megtenni, mert a nyilvántartási osztályon éppen akkoriban került napirendre az áttérés egy új adatbázis használatára, amely esetleg már nem fogja tartalmazni ezt a számot.

Ezt a történetet nem azzal a céllal mesélem el, hogy kifigurázzam az alma materemben keményen dolgozó egyetemi dolgozókat, és nem is azért, hogy hangsúlyozzam egy olyan helyzet abszurditását, amelyben valamilyen személyre vonatkozó információ könnyen átadható egy harmadik félnek, de magának az „adatalanynak" már nem. A lényeg annak a kérdésnek a vizsgálata, hogy vajon az *én* társadalombiztosítási számom megér-e öt dollárt. Ez kétségtelenül személyes információ, és a világ bármely magánszféra védelmére vagy az adatvédelemre vonatkozó törvénye szerint is az. Másrészt viszont én nem tettem semmiféle erőfeszítést annak érdekében, hogy létrehozzam ezt a számot. Nem belsőleg, nem olyan értelemben tartozik hozzám, mint ahogyan a vércsoportom vagy a genetikai összetételem a sajátom. Világos továbbá az is, hogy ez a szám nem az *én* tulajdonom. Hogyan is lehetne az, ha ismeretlen volt számomra? Csakúgy, mint több ezer más egyedi számot, amelyek valahol társítódnak a Colin J. Bennett névhez, és amelyek ismertek vagy ismeretlenek lehetnek számomra, ezt is egy bürokratikus szervezet hozta létre, adminisztratív célokra, és a társadalombiztosítási számok esetében az ilyen felhasználási célok sajnos egyre szaporodnak. A számnak nincs értéke számomra, kivéve olyan körülmények között, amikor az USA valamelyik közintézménye azonosítójaként igényt tart rá. Nyilvánvalóan nem ér meg öt dollárt. Nem ér egyetlen dollárt, még öt centet sem.

Az, hogy ehhez az információhoz nem csatolható pénzbeli érték, korántsem jelenti azonban azt, hogy számomra közömbösek lennének magának a számnak a felhasználási lehetőségei vagy a hozzáférhetősége. Sok horrortörténet kering arról, hogy egyes adatbázisokban érvénytelen vagy pontatlan társadalombiztosítási számok jelentek meg, és ez különféle jogok és szolgáltatások igazságtalan megtagadásához vezetett. Az Amerikai Egyesült Államokban például a hitelképesség-figyelő ügynökségek is ezt a számot használják. Ha a számomat összetévesztenék valamely hitelkockázati szempontból rossz megítélés alá eső személyével, s így megjelenne a hitelképesség-figyelő ügynökségek dokumentációjában, valószínűleg nem juthatnék többé hitelhez. A társadalombiztosítási számot felhasználják továbbá azonosítóként számos számítógépes nyilvántartási rendszerben és a kormányzat különböző szintjein működő hivatalok egymás közötti adatforgalmában, beleértve természetesen az adóhivatalt is. Bizonyára azonosítóként szolgál többek között az Illinoisi Egyetem öregdiákjainak nyilvántartásában. Ez az információ tehát nem az én tulajdonom, de rám vonatkozik. Igen sokféle olyan helyzet adódhat, amelyben a helyes információ illegális kezelése és a téves információ legális kezelése egyaránt súlyos következményekkel járhat az emberre nézve (Smith 1993).

Itt egy fontos különbséghez érkezünk, ami a szellemi tulajdon, illetve a privát szféra vagy a személyes adatok védelmére vonatkozó jog birodalmai között fennáll. Az előbbi feltételezi az információ tulajdonjogát, az utóbbi nem. E tanulmány első részében megpróbálom felvázolni azoknak a jogszabályoknak *(statutory law)* a keletkezéstörténetét, amelyeket Amerikában „a privát szféra védelme", Európában pedig az „adatvédelem" kategóriájába szokás sorolni. Ezután megmutatom, hogy a privát szférához

tartozó információk, az „információs privát szféra" *(information privacy)* védelmére vonatkozó szabályozás kialakulása és gyakorlati bevezetése óhatatlanul *nemzetközi* kérdéssé vált, és leírom azokat a különféle küzdőtereket, ahol ezekről a nemzetközi szabályokról tárgyalások folytak és ma is folynak. A privát szféra védelmének globális szabályozása ma különféle szereplők sokaságát, valamint igen változatos koordinációs és működési módozatokat magában foglaló komplex terület.

Az információs privát szféra (information privacy)

Az információs privát szféra fogalma az 1960-as és 70-es években alakult ki Amerikában, körülbelül ugyanabban az időben, amikor a német *Datenschutz* szóból származó „adatvédelem" kifejezés bekerült az európai szakértők szótárába. Ennek értéke – egy olyan időszakban, amikor különféle európai, észak-amerikai és ausztrálázsiai államokban nagyarányú nemzeti adatintegrációs programok megvalósítását fontolgatták – elválaszthatatlanul összekötődött a számítógépek információfeldolgozási képességeivel, és avval a szükséglettel, hogy biztonsági berendezéseket kell kiépíteni. Ezek a programok ugyanis félelmet ébresztettek az emberekben, hogy mindentudó, „Nagy Testvér" jellegű kormányok jöhetnek létre, amelyek példátlan felügyeleti hatalommal rendelkezhetnek. A szakértők számos országban azzal kezdtek foglalkozni, hogy mit kellene tenni ez ellen. Ennek a kérdésnek a tanulmányozására bizottságokat hoztak létre Nagy-Britanniában, az Egyesült Államokban, Kanadában, Svédországban, Ausztráliában és másutt is. Az ekkor kifejtett elemzési erőfeszítések vezettek el a világ első „adatvédelmi" vagy „információs privát szféra" törvényeihez, s azután számos lépésen keresztül hasonlók születtek az egész világon (Bennett 1992, Bygrave 2002).

Noha az egyes államok főbb érdekei eltértek egymástól, a különböző országokban működő szakértők hasonlóan gondolkodtak, és szorosan együttműködő csoportjaikban általános konszenzus alakult ki a probléma megoldásához vezető legjobb út tekintetében. Az általános politikai cél minden országban az volt, hogy az emberek nagyobb ellenőrzést gyakorolhassanak a közintézmények (és néha magánkézben levő szervezetek) által róluk összegyűjtött, tárolt, feldolgozott és terjesztett információk fölött. Ez a cél leginkább az angol nyelvű országokban, valamint Európa kontinentális országaiban került előtérbe. Az információs önrendelkezés *(Informationsselbstbestimmung)* fogalma Németországban később fejlődött ki és kapott alapjogi státust. Az 1980-as évekre azonban már világszerte körvonalazódhattak azok a kulcsfontosságú alapfeltevések, amelyeken az adatvédelmi stratégiák fejlődése azóta is nyugszik. Ezek az alapfeltevések a következők:

Először is úgy tartják, hogy általában lehetetlen *a priori* meghatározni azokat az adatokat, amelyek belső természetüknél fogva nagyobb védelmet érdemelnek (ezek az úgynevezett „különleges" adatok), mivel inkább a különböző kontextusok, mintsem az adatok eltérő tulajdonságai vezetnek a privát szféra kockázataihoz. Ugyanaz az információ különféle kontextusokban igen különböző érzékenységi szintekre kerülhet. A nevem a telefonkönyvben esetleg nem érzékeny adat, ám a bankok hitelképességi feketelistáján vagy a szexuális zaklatással gyanúsítható személyek jegyzékén nagyon is érzékeny adat lehet. A társadalombiztosítási számom az egyetemi nyilvántartásban

esetleg nem érzékeny adat, de az adócsalók listáján feltétlenül az lenne. Ennélfogva a védelemre érdemes adattípusokat a jog legtöbbször nem tudja elhatárolni azoktól, amelyeket nem szükséges védeni, bár erre is voltak próbálkozások. Az információnak azokat a típusait, amelyeknek a privát szférában kell maradniuk, általában sem a közvélemény, sem a jogrend alapján nem lehet határozottan megkülönböztetni azoktól, amelyek nyilvánosan hozzáférhetővé válhatnak.

Másodszor, a privát szféra erősen szubjektív érték. A személyes információk védelmével kapcsolatos aggodalmak az idő, az igazságszolgáltatási körzetek, a különféle etnikai csoportok, a nemek és sok minden más szerint is mások és mások lehetnek. Egy név és egy lakcím a telefonkönyvben például közömbös lehet a legtöbb ember számára, de igen érzékeny információ lehet az olyan sebezhető személyek esetében, akik nem akarják, hogy megfigyelhessék őket vagy a nyomukra bukkanjanak. Ilyenek lehetnek például a bántalmazott feleségek, az abortuszt végző orvosok, a hírességek, a gyermekvédelmi szervek alkalmazottai, a rendőrtisztek és így tovább. Következésképpen a közvéleményt és a közérdeket szem előtt tartó jogi szabályozás nem jósolhatja meg előre, hogy melyek lesznek azok a személyes információk, amelyeknek a biztonságáért egy adott közösség valamely adott időszakban aggódni fog. A legtöbb, amit a privát szféra jogi védelme elérhet, mindössze annyi, hogy biztosítja az eljárási jogokat az emberek számára ahhoz, hogy ellenőrzést gyakorolhassanak a rájuk vonatkozó személyes információk fölött, amennyiben erre igényt tartanak. Így tehát a privát szférával kapcsolatos jogok és érdekek tartalmát maguknak az egyéneknek kell meghatározniuk, szubjektív módon és az adott körülményektől függően. Az adatvédelem szabályozása ennélfogva nem alapulhat alapvető, *szubsztanciális* elveken, hanem óhatatlanul inkább *procedurális* jellegű. Csak azokat a mechanizmusokat bocsáthatja rendelkezésre, amelyek segítségével az emberek érvényesíthetik a privát szférával kapcsolatos saját érdekeiket és igényeiket, *ha kívánják*.

Harmadszor, általános egyetértés van abban, hogy nem a szervezeteknek, vállalatoknak vagy más „jogi személyeknek", hanem az egyénnek vagy a „természetes személynek" kell leginkább védelemben részesülnie. Egyes társadalmak (például Skandináviában) megkísérelték egyesíteni a természetes és a jogi személyek jogait az adatvédelmi törvényeikben. Lényegében azonban általános egyetértés alakult ki abban, hogy az adatvédelmi szabályozás célja a nagyobb mértékű ellenőrzés biztosítása az egyén számára a személyével kapcsolatos információk fölött, amihez szükség van arra, hogy azt, akire az információ vonatkozik *(adatalany)*, megkülönböztessék attól, aki az információt kezeli *(adatkezelő)*. Ez a megkülönböztetés azonban semmi esetre sem egyértelmű, vagyis az egyén igen sok esetben egyszerre két sapkát is viselhet. Mindazonáltal a szabályozás mind az egyes országokban, mind nemzetközi szinten arra az alapfeltevésre építve fejlődött ki, hogy a különféle csoportoknak, vállalatoknak és más szervezeteknek a rájuk vonatkozó információval kapcsolatos érdekeit más jogi eszközökkel kell kezelni, mint az egyének érdekeit.

Ez pedig végső soron visszavezetett bennünket ahhoz a kérdéshez, amellyel kezdtem, nevezetesen, hogy a személyes információ tulajdonnak tekinthető-e, ami fölött az egyének tulajdonjoggal rendelkezhetnek. A klasszikus közgazdasági elmélet azt állítaná, hogy a tökéletlen piac kétféle módon korrigálható. Először is, a személyes információknak lehet olyan értéket adni, hogy a velük folytatott tranzakciók költségei és

az ilyen tranzakciókból eredő hasznok megfelelőbb arányban álljanak. Ám a jogban a személyes információt tulajdonként meghatározni, és ennek alapján a jogosulatlan információfeldolgozásra kereseti alapot definiálni igen nehéz. A fogyasztóknak lehet némi alkupozíciójuk valamely direkt marketinget folytató céggel szemben, amely adatlistákkal akar kereskedni, a polgárok azonban nincsenek alkupozícióban, ha például olyan hatósági felhatalmazásokkal vagy más, potenciálisan a privát szférába való behatolásra alkalmas adatgyűjtési módszerekkel kerülnek szembe, amelyeknek az elutasítása állami szankciókat vonhat maga után. A privát szféráról folyó viták kezdetén éppen a kormányzati szervek hatásköre volt az, ami a legjelentősebb kihívásokat jelentette.

Nehezen lehetett tehát kitérni egy olyan következtetés levonása elől, hogy az egyensúlyhiányt csupán szabályozási beavatkozással lehet korrigálni. Következésképpen az információs privát szféra védelmét kezdetben általában nem egyéni döntési kérdésként, hanem a közérdeket szem előtt tartó jogalkotás-politikai problémaként definiálták. Később, ahogy ennek az uralkodó szemléletnek a bírálatai felszínre kerültek, a személyes adatok feldolgozásának a gazdasági szektorban folytatott gyakorlata is ugyanilyen fontos kérdéssé vált. Továbbá, ahogy az interneten zajló kommunikáció és az e-kereskedelem egyre inkább kiemelkedő szerepre tett szert, változatos piaci alapú megoldások kerültek napirendre, amelyek mindegyike arra az alapfeltevésre épült, hogy a személyes információnak tulajdonérték adható, ami a személyes információk piacán belül áruba bocsátható és forgalmazható (Rule & Hunter 1999; Lessig 1999). Az ilyen fajta érveknek azonban igen csekély hatásuk volt azokra a szakértőkre és törvényhozókra, akik az 1970-es években az információs privát szféra problémájával viaskodtak.

Ezeket az alapfeltevéseket nem minden tudós és kommentátor fogadta el. Mindegyiket hosszabb ideje, mélyre hatóan vitatják. Az elemzés szempontjából ennél a sarkalatos pontnál az a legfontosabb, hogy a privát szféra védelmének stratégiája – az információs privát szféra problémájának természetét illetően általánosan elfogadott alapfeltevések eredményeként – egy bizonyos irányvonalat követett. Az eddig kidolgozott stratégiai válaszok (az adatvédelmet vagy az információs privát szféra védelmét biztosító törvények) életbe léptetéséhez legtöbbször az vezetett el, hogy az elitek közös álláspontra jutottak annak a problémának a természetét illetően, amellyel szembesültek. Ezek a liberális alapelvekre épülő közös alapfeltevések minden fejlett ipari államban mélyreható és széleskörű politikai következményekkel jártak. Abból kiindulva tehát, hogy mindannyian rendelkezünk az információs privát szférához való joggal, igényekkel vagy érdekekkel, hogyan lehet olyan rendszert kialakítani, ami megvédelmezi ezeket a jogainkat?

A tisztességes információkezelés doktrínája

Mihelyt ezeket az alapfeltevéseket – más arra vonatkozó megfontolásokkal együtt, hogy a privát szférával kapcsolatos jogi szabályozást hogyan lehet és hogyan nem lehet kifejleszteni – elfogadták, azonnal működésbe lépett egy olyan logika, ami szükségképpen az alapvető eljárási jogok megfogalmazódásához vezet. Ezekből fejlődtek ki azután a „tisztességes információkezelés" elvei, amelyeknek logikusan néhány kulcsfontossá-

gú alapelv köré kellett összpontosulniuk. A tisztességes információkezelési gyakorlat történelmi eredetei rövid úton visszavezethetők az Európában és az Egyesült Államokban az 1960-as évek végén és a 70-es évek elején kidolgozott politikai elemzésekig (Bennett 1992: 95–115). Azok a szakértők, akik különféle országokon belül kísérelték meg ennek a kérdésnek a megoldását, valamennyien erős szükségét érezték annak, hogy tanulságokat szűrhessenek le más országokban működő kollegáik munkájából. A kölcsönös tanulás intenzív folyamata nemzetközi konszenzust hozott létre a privát szféra problémáinak politikai és jogi eszközökkel elérhető legjobb megoldását illetően.

Míg az elvek törvénybe iktatása változatos lehet, lényegüket tekintve mégis a következőkre redukálhatók (Bennett és Grant 1996: 6):

Az állami és a magán szervezeteknek egyaránt

- *elszámolásra kötelezhetőnek* kell lenniük a birtokukban levő valamennyi személyes információról;
- az adatgyűjtés előtt vagy avval egyidejűleg *meg kell határozniuk azokat a célokat*, amelyek érdekében feldolgozzák az információkat;
- személyes információkat (bizonyos speciális körülmények kivételével) kizárólag az egyén *tudomásával és beleegyezésével* szabad gyűjteniük;
- a személyes információk gyűjtését arra kell *korlátozniuk*, ami a közölt célok eléréséhez szükséges;
- a személyes információkat a közöltektől eltérő célokra nem szabad sem felhasználniuk, sem továbbítaniuk mások számára, kivéve az egyén jóváhagyása esetén *(a célhoz kötöttség elve);*
- csak addig szabad *megőrizniük* az információkat, ameddig szükséges;
- biztosítaniuk kell a személyes információk *pontosságát, teljességét és időszerűségét;*
- megfelelő *biztonsági berendezésekkel* védeniük kell a személyes információkat;
- *nyílt, átlátható* eljárási gyakorlatot kell követniük, vagyis nem tarthatnak fenn titkos információs rendszereket;
- az adatok pontatlansága, hiányossága vagy elavulása esetén biztosítaniuk kell az adatalanyok számára a rájuk vonatkozó személyes információkhoz való *hozzáférést*, és lehetőséget kell adniuk az adatok *helyesbítésére.*

Ezek az elvek mindazonáltal viszonylagosak. A privát szférához való jog – akárhogy is értelmezzük és bárhogyan fogalmazzuk is meg – nem abszolút jog, hiszen egyensúlyban kell lennie más, vele összefüggő jogokkal és a közösség iránti kötelezettségekkel, még akkor is, ha az „egyensúly" fogalma és a „mérlegelés" folyamatai meglehetősen homályosak (Raab 1999).

A tisztességes információkezelés elve explicit vagy implicit formában megjelenik minden nemzeti adatvédelmi törvényben, beleértve az USA, Ausztrália, Új-Zéland és Kanada törvényeit is, ahol ezeket nem adatvédelmi törvényeknek, hanem „a privát szférára vonatkozó törvényeknek" *(Privacy Acts)* nevezik. Megjelennek az önszabályozási rendelkezésekben és egyéb szabványokban, például a Kanadai Szabványügyi Társaság *(Canadian Standards Association)* által közzétett szabványokban is, amelyek a privát szektorra vonatkozó új kanadai adatvédelmi törvény alapját képezik (CSA, 1996). Az 1. függelék átfogó képet nyújt a személyes adatvédelmi törvényhozás állapotáról a világon 2001-ben. Bemutatja, hogy az adatvédelmi törvények életbe léptetése az

1980-as és 90-es években milyen gyorsan ment végbe az egész fejlett ipari világban, és hogy azok a társadalmak is, amelyeket többnyire a „fejlődő" jelzővel szoktak jellemezni, hasonló törvényeket kezdenek elfogadni.

E harmonizáció ellenére természetesen további viták folynak arról, hogy a tisztességes információkezelési gyakorlatok *(Fair Information Practices, FIPs)* doktrínája hogyan foglalhatók törvénybe. Viták folynak például az alábbi kérdésekről: Hogyan kell szabályozni a személyes adatok másodlagos felhasználását – fontossági mércék felállításán keresztül, vagy a törvényességi felügyeletet ellátó felelősökről való gondoskodás útján? Korlátozhatók-e az információgyűjtés alapjául szolgáló elvek? A szervezetek milyen mértékig legyenek kötelesek igazolni az adatok fontosságát az általuk képviselt speciális célok szempontjából? Melyek azok a körülmények, amelyek között nem elegendő az adatalanyok „hallgatólagos" hozzájárulása az adatok gyűjtéséhez és feldolgozásához, hanem „kifejezett" jóváhagyásukra van szükség? Milyen alapon lehet, illetve kell különbséget tenni az információ gyűjtése, felhasználása és továbbítása között? Csakugyan van-e értelmük ezeknek a megkülönböztetéseknek, és nem kellene-e mindezeket belefoglalni a „feldolgozás" gyűjtőfogalmába? Az, hogy ezeket a törvényalkotási kérdéseket – más, hozzájuk kapcsolódó kérdésekkel együtt – hogyan fogják megoldani, természetesen minden ország igazságszolgáltatásában mélyreható következményekkel jár a privát szféra védelmével kapcsolatos követelmények gyakorlati érvényesítésére nézve. A törvények különböznek egymástól annak a mértékében is, hogy mely szervezetekre terjednek ki: Észak-Amerikában és Ausztráliában történelmileg elsősorban a közszféra intézményeit szabályozták, míg másutt (különösen Európában) a szabályozás valamennyi szervezetre kiterjedt. Ezek a különbségek azonban gyorsan változnak, ahogy egyre több ország, köztük Kanada, Ausztrália és Japán is lépéseket tesz a privát szektor vagy a piaci szereplők gyakorlatának szabályozására. A törvények különbségeket mutatnak továbbá azt a mértéket tekintve is, amennyire a nem számítógépen tárolt dokumentumok (vagyis az iratrendező szekrényekben őrzött dossziék) kezelését szabályozzák. Ez a különbségtétel azonban szintén erodálódik.

A legfigyelemreméltóbb különbség a felügyelet és a szabályozás céljára létrehozott ellenőrzési eszközök tekintetében mutatkozik (Flaherty 1989). A „privát szféra" vagy a „személyes adatok" védelmére a legtöbb országban (az Egyesült Államok fontos kivételével) kisebb szervezeteket hoztak létre, különféle felügyeleti, tanácsadási vagy szabályozási hatáskörökkel. Némelyik ilyen szervezetnek erős hatósági és szabályozási hatalma van; mások inkább tanácsadó jellegű, „ombudsmanszerű" testületként működnek. Egyesek élén kollektív bizottságok állnak (például Franciaországban), másokat „a privát szféra védelméért felelős biztos" *(Privacy Commissioner)* vagy „adatvédelmi biztos" *(Data Protection Commissioner)* irányít. Egyes szabályozó rendszerekben az „önszabályozó" eszközök (például a vállalatok gyakorlatában alkalmazott szabályozások) fontosabb szerepet játszanak, mint másokban.

Végül meg kell jegyezni, hogy ez a mély és egyre növekvő konszenzus, ami a tisztességes információkezelés doktrínáját övezi, a mélységes szkepticizmus hátterével alakult ki, azt illetően, hogy a doktrína vajon ténylegesen meg tudja-e védeni a személyes privát szférát, és gátat tud-e vetni a felügyeleti eszközök kérlelhetetlenül emelkedő áradatának. Azok a szerzők, akik szélesebb szociológiai perspektívából vizsgálják a kérdést, folyamatosan hangoztatják aggodalmaikat amiatt, hogy az „információs privát

szférával" kapcsolatos mai törvényhozás inkább a személyes adatok feldolgozására lett kialakítva, mintsem annak korlátozására. David Lyon azt állítja, hogy „a *privát szféra* fogalma nem alkalmas annak a megjelölésére, ami a mai felügyeleti technológiákról folyó vitákban kockán forog" (Lyon 1994: 196). Azoknak a szempontjából, akik a túlzott mértékű felügyelet átláthatóvá tételében és korlátozásában érdekeltek, a privát szféra problémájának olyan formában való megfogalmazása, ami a privát szféra érdekei és a különféle szervezetek részéről a személyes információk iránt megnyilvánuló igények közötti megfelelő „egyensúlyt" próbálja meghatározni, aligha tekinthető a probléma mélyén meghúzódó kérdés helyes megközelítésének. Az adatvédelmi jogszabályok eredményezhetik a személyes adatok tisztességesebb és hatékonyabb kezelését és felhasználását, de nem vonhatják ellenőrzésük alá a modern szervezetek velük született csillapíthatatlan étvágyát az egyre apróbb részletekig terjedő személyes információkra. Ezeket az információkat pedig egyre inkább olyan tolakodó biometriai technológiák útján szerzik meg, amelyek megváltoztatják magukat az én és a külvilág között húzódó határokat is.

Már a viták korai szakaszában felismerték, hogy az információs privát szféra védelmét az egyes országok között mutatkozó ilyen különbségek dacára sem lehet egyszerűen belföldi problémának tekinteni. A személyes adatok országhatárokon túlra történő továbbításának fokozódó könnyedsége a nemzetközi harmonizációs erőfeszítések, valamint a határokon átívelő adatáramlások szabályozása terén ezekkel együtt járó törekvések érdekes történetét hozta létre. Az 1980-as években ezek a harmonizációs igények két nemzetközi egyezményben, az OECD 1981. évi irányelveiben *(Guidelines from the Organization for Economic Cooperation and Development)* és az Európa Tanács 1981. évi adatvédelmi egyezményében is tükröződtek. Az 1990-es években ezek a törekvések további megerősítést kaptak az Európai Unió 1995. évi adatvédelmi irányelvétől *(Directive on Data Protection)*, ami nagyobb mértékű védelmet biztosító követelményeknek megfelelően próbálja harmonizálni az európai adatvédelmi törvényeket, és ezeket érvényesíteni igyekszik minden olyan országban, ahol az Európai Unió állampolgárainak személyes adatait feldolgozhatják. Az adatvédelmi törvények tartalmát azóta az egész világon elsősorban ezek a dokumentumok szabják meg (Bennett és Raab 2003).

A privát szféra védelmére létrehozott nemzetközi szabályozó rendszerek

Az Európa Tanács

Az Európa Tanács intézményei először az 1960-as évek végén váltak érdekeltté a privát szféra és a személyes adatok védelmének a kérdéseiben. Ekkor tanácsadási feladatokkal létrehoztak egy szakértői bizottságot annak tanulmányozására, hogy a modern számítástechnikai eszközök fejlődésével szembesülve hogyan lehet a legjobban megvédeni a privát szférát (Hondius 1975). Az 1970-es években hozott határozatok vezettek el a már említett, 108. számú egyezmény – a továbbiakban röviden Egyezmény – kidolgozásához „az egyének védelméről a személyes adatok automatikus feldolgozása során" *(Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data)*, amelyet 1980-ban elfogadtak, és 1981-ben előterjesztettek ratifikálásra.

Az európai konvenciók és egyezmények az Európa Tanács nem törvényerejű rendelkezései, és jogi státusukat egyszerűen azon államok akaratának köszönhetik, amelyek a dokumentumok aláírásával és ratifikálásával magukévá kívánják tenni őket. A ratifikáció azt jelenti, hogy az adott egyezmény elveit beépítik az adott ország törvényeibe, és a személyes információikkal való visszaélések esetén bármely ratifikáló ország állampolgárai – legalábbis elméletileg – jóvátételt követelhetnek a többi országban is. 2001. decemberéig a Tanács 41 tagja közül 33 aláírta és 25 ratifikálta ezt az Egyezményt.

Ez volt az első nemzetközi jogi dokumentum, amely rögzítette az *információs privát szférára* vonatkozó alapelveket. Ebben a tekintetben az Egyezmény mintaként szolgált azoknak az országoknak, amelyekben még nem volt adatvédelmi törvény. Az Európa Tanácsnak azonban nincs nemzetek fölötti jogi szervezete annak biztosítására, hogy az elveket a gyakorlatban is végrehajtsák. Ennélfogva nem állítható határozottan, hogy az Egyezmény ratifikálása egy közös minimális adatvédelmi szint tényleges garantálását jelenti. Továbbá – noha az Egyezmény arra törekszik, hogy a csatlakozó feleknél egyenlő szintet hozzon létre, és ennek révén biztosítsa a személyes adatok szabad áramlását a felek között – az adatok olyan országokba való továbbíthatóságának a megítélése, amelyek még nem írták alá az Egyezményt, a nemzeti jog hatáskörébe tartozik. Ez viszont aláássa a ratifikáló országoknak a személyes adatok címzettjeiként egymásba vetett kölcsönös bizalmát.

Az Egyezmény mint a személyes adatok nemzetközi áramlásának szabályozására szolgáló eszköz tényleges hatálya tehát korlátozott volt, és azóta ezt fel is váltotta az 1995. évi Európai Adatvédelmi Irányelv *(European Data Protection Directive)*, amellyel később részletesebben foglalkozom. Ez nem azt jelenti, hogy az Egyezmény feleslegessé vált, mert még mindig modellként szolgál az újonnan demokratizálódó államok számára, és alapdokumentumként segítségül hívták a személyes adatok védelmének szabályozásához olyan európai államközi szervezetekben is, mint például az *Europol*. Az Egyezmény értelmében a Tanács a következő években – miközben széles körben alkalmazott új kormányzati, társadalmi és gazdasági gyakorlatok és új technológiák alakultak ki, ideértve az internetet is – számos nagyhatású javaslatot fogadott el. Kidolgozott továbbá egy modellszerződést, amelyben körvonalazta mind az engedélyező, mind az engedélyekben részesülő felek kötelezettségeit az egyenlő adatvédelem biztosítására a nemzetközi adatáramlással összefüggésben.

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD)

Az OECD arénáján belül az 1970-es évek végén lehetett a világ első ízben tanúja olyan transzatlanti konfliktusoknak, amelyek az adatvédelem jogi szabályozása kapcsán robbantak ki. Az amerikai állásfoglalás a mellett az elv mellett, hogy az információk áramlását ritkán kell gátolni, sok európai szemében burkolt kísérletnek tűnt az USA világpiaci hegemóniájának védelmére. A másik oldalról viszont az „adatvédelem" címkéje mögött egyes amerikaiak be nem vallott protekcionista motívumokat láttak (Eger 1978). A magánélet védelméről és a személyes adatok határokon átívelő áramlásáról kiadott irányelvek *(Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data)* – a továbbiakban röviden Irányelvek (OECD 1981) – elfogadásával kap-

csolatos tárgyalások ennélfogva igen nehézkesen indultak meg és mindvégig heves viták közepette zajlottak (lásd Bennett 1992: 137).

Az Irányelvek alapjául a dokumentum előszavában rögzített alábbi feltevések szolgáltak:

- a tagországoknak – noha nemzeti törvényeik és jogrendszereik eltérőek lehetnek – közös érdekük fűződik a privát szféra és az egyéni szabadságjogok védelméhez, valamint az olyan alapvető, ám egymással versengő értékek összehangolásához, mint a privát szféra és a szabad információáramlás fenntartása;
- a személyes adatok automatikus feldolgozása és határokon átívelő továbbítása az országok közötti kapcsolatok új formáit hozza létre, és összeegyeztethető szabályozási és gyakorlat kifejlesztését kívánja meg;
- a személyes adatok határokon átívelő áramlása hozzájárul a gazdasági és társadalmi fejlődéshez;
- a privát szféra védelmére és a személyes adatok határokon átívelő áramlásaira vonatkozó belföldi törvényhozás esetleg gátolhatja az ilyen nemzetközi adatáramlásokat.

Az Irányelvek alkalmazása a személyes adatokra mind a közszférában, mind a versenyszférában azt a célt szándékozott elérni, hogy segítsen harmonizálni a nemzeti adatvédelmi törvényeket, és átfogó keretet nyújtson a nemzetközi adatáramlás elősegítéséhez. Az Irányelvek fontos konszenzust fogalmaztak meg a következő nyolc alapelv tekintetében: az adatgyűjtés korlátozása, adatminőség, a célhoz kötöttség, korlátozások használata, biztonsági intézkedések, nyíltság, egyéni részvétel és felelősségre vonhatóság.

A határokon átívelő adatáramlásokról szólva az Irányelvek 17. szakasza megállapítja:

„Az egyes tagországok tartózkodjanak attól, hogy korlátozzák a személyes adatok határokon átívelő áramlását a saját és egy másik tagállam között, kivéve, ha az utóbbi alapjában véve még nem tartja tiszteletben az Irányelveket, vagy ha az ilyen adatok újraexportálása megkerülné az ország magánéletre vonatkozó törvénykezését. Egy tagállam továbbá életbe léptethet bizonyos korlátozásokat a személyes adatok bizonyos kategóriáiban, ha a nemzeti magánéletre vonatkozó törvénykezése bizonyos specifikus szabályozásokat tartalmaz ezen adatok természetére vonatkozóan és ilyeneknek a másik tagállam nem tud megfelelő védelmet nyújtani."

A 18. szakaszban ugyanakkor ez olvasható:

„A tagállamok kerüljék, hogy olyan törvényeket, politikai irányelveket és gyakorlatokat léptessenek életbe a magánélet és a személyes szabadságjogok védelmének nevében, amik korlátokat szabnak a személyes adatok határokon átívelő áramlásának és amik túlmennek az ilyen védelem követelményein."*

Erőfeszítéseket tettek továbbá az OECD és az Európa Tanács egyezményei közötti szükségtelen eltérések elkerülésére is. Vannak azonban fontos különbségek, amelyeket érdemes megemlíteni. Először is, az Irányelvek elfogadása kifejezetten önkéntes jellegű. Nem von magával szankciót, ha akár egy ország, akár valamely szervezet nem alkalmazza őket, és nincs szankció arra az esetre sem, ha elfogadásuk után nem érvényesítik őket. Ezzel szemben az Egyezmény jogilag kötelező, legalábbis azokra az or-

* Az idézetek az Irányelvek szövegének *hivatalos* magyar változatából származnak. – *A ford.*

országokra nézve, amelyek ratifikálták, habár az egyes országok eleget tehetnek az általános követelményeknek oly módon is, hogy a saját politikai, adminisztratív és jogi rendszerüknek megfelelő végrehajtási és felügyeleti módszereket alkalmaznak. Másodszor, az Egyezmény kizárólag az automatizált adatfeldolgozásra vonatkozik, míg az Irányelvek általában a személyes adatok kezelésére vonatkoznak, tekintet nélkül az adatok feldolgozása során alkalmazott eszközökre.

Az 1980-as évek elején tehát ezt a két nemzetközi okiratot használták fel modellként a nemzeti törvényhozó testületek (Európában), és ezek szolgáltak mintául az önkéntesen alkalmazott gyakorlat kialakításához Európán kívül is. Mind az amerikai, mind a kanadai kormány megpróbálta nyomon követni, hogy saját társadalmaik milyen mértékig fogadták el az OECD Irányelveit, annak világos jelzése nélkül, hogy az „elfogadás" pontosan mit von magával, és természetesen bármely komoly elkötelezettség nélkül (Gellman 1993: 230). Az 1990-es években azonban a figyelem átirányult a számítógépes adatfeldolgozás biztonsági kérdéseire, és az információs rendszerek biztonságáról kibocsátott irányelvek *(Guidelines on the Security of Information Systems)* megtárgyalására (OECD 1992). Ez utóbbi, 2001-ben korszerűsített irányelveknek az volt a céljuk, hogy megteremtsék az igényelt kereteket az információs rendszerek elérhetőségének, integritásának és titkosságának biztosításához. Az OECD „csomagjának" harmadik elemét az 1997. március 27-én közzétett titkosítási irányelvek *(Guidelines for Cryptography Policy)* alkották, amelyeknek a kidolgozására a polgári célú kriptográfiai termékek exportjával kapcsolatban több évig folytatott heves nemzetközi viták után került sor (OECD 1997). Ez sem kötelező erejű egyezmény, de meghatározza azokat az alapvető kérdéseket, amelyeket az országoknak saját kriptográfiai jogszabályaik kialakításakor – nemzeti és nemzetközi szinten egyaránt – tekintetbe kell venniük.

Mindezek a követelmények – a privát szféra védelme, az adatbiztonság és a titkosítás – egy közös pontban találkoztak az 1990-es évek közepén, amikor az OECD egyik prioritásaként napirendre került az elektronikus kereskedelem témája, és ez számos váltást eredményezett az OECD retorikájában és politikájában egyaránt. Először is, a diskurzus a mai adattovábbítás interaktívabb, dinamikus és hálózati jellegének tükrözése felé hajlik. Másodszor, míg az 1970-es és 80-as években a törvényhozásra került a hangsúly, ma az a felismerés válik uralkodóvá, hogy – összhangban a mára már széles körű konszenzussal – a törvényi szabályozás mellett más megoldások sokaságára is szükség van, beleértve az önszabályozást, a privát szférát erősítő technológiákat, a szerződéses megoldásokat és a fogyasztók képzését (OECD 1999). Harmadszor, a privát szféra védelme ezekben a vitákban már nem a nemzetközi kommunikáció és kereskedelem gátjaként, hanem olyan szükséges feltételként szerepel, amelynek a megléte nélkül az emberek kereskedelmi tranzakciók lebonyolítására nem fogják felhasználni a nyílt hálózatokat.

Az Európai Unió fórumai

Az 1980-as évek végén már világosan láthatóvá vált, hogy az országok nem nagyon igyekeznek ratifikálni az 108. sz. Egyezményt, és jelentős jogi különbségek maradtak fenn azoknak az országoknak a törvényhozásai között is, amelyek ratifikálták az egyez-

ményt. Az OECD Irányelvei inkább az önszabályozási megoldások igazolásául szolgáltak, mintsem olyan módszerként, ami elősegítené a jó adatvédelmi gyakorlatok kialakítását az egész fejlett ipari világban. Az 1980-as évek végén azonban egyre világosabbá vált, hogy az adatvédelmi szabályok eltérései gátolhatják a személyes információk szabad áramlását az Európai Unió egész területén, és akadályt képezhetnek az egységes belső piac létrehozása előtt is, aminek a megteremtését 1992-re irányozták elő. Az adatvédelem megszűnt csupán emberi jogi kérdés lenni, és lényegileg összekapcsolódott a nemzetközi kereskedelem működésével is.

Ennek eredményeként született meg a mindmáig messze a legnagyobb hatású nemzetközi politikai dokumentum: az Európai Unió által kibocsátott „Irányelv a személyes adatok feldolgozására vonatkozóan az egyének védelméről és az ilyen adatok szabad áramlásáról" *(Directive on the Protection of Personal Data with Regard to the Processing of Personal data and on the Free Movement of such Data)* (EU 1995).[2] Ez a dokumentum – a továbbiakban röviden Irányelv – a fogalmazás és újrafogalmazás öt esztendeje után jelent meg végleges formában, amikor végigment az EU bonyolult és hosszadalmas döntéshozatali mechanizmusának valamennyi fokozatán.[3] Az Irányelv lényegét úgy érthetjük meg, ha ezt az okiratot a közszférában és a privát szektorban vezető szerepet játszó szereplők között kialkudott egyezség visszatükröződésének tekintjük.

Az Irányelvnek az a célja, hogy az Unió valamennyi tagországában magas szintű védelmet biztosítson az emberek privát szférájának, továbbá segítsen biztosítani az információ szabad áramlását az egész egységes piacon, a fogyasztók bizalmának előmozdítása és a tagországok szabályai közötti különbségek minimalizálása útján. Az Irányelv szövegének olvasója először is a célok és szándékok hosszadalmas felsorolásával találkozik, összesen 71 „mivel" kezdetű állítás formájában, amelyek arra szolgálnak, hogy az okiratot más értékek és szabályozási stratégiák kontextusába helyezzék, amelyek segítenek az értelmezésében, és azoknak az érdekeknek a sokaságát tükrözik, amelyek a tartalmát alakították. A tisztességes információkezelés elveinek ismerős csomagja, amelyben a korábbi nemzeti törvények és a nemzetközi egyezmények találkoztak, nem jelenik meg egyetlen könnyen hozzáférhető helyen sem. A jóváhagyás, az elérhetőség, a bejelentési kötelezettség, a biztonság stb. elvei bizonyára előfordulnak egyes cikkekben, de a dokumentum elsősorban jogi szöveg, amelynek a fő célja az, hogy irányt mutasson és segédletet adjon a nemzeti adatvédelmi törvények megfogalmazói számára.

> Az Irányelv – minden bonyolultsága mellett is – lemondott bizonyos mesterséges és elavult fogalmakról. Most például már alig van benne különbségtétel a közszférában, illetve a magán szektorban folyó adatfeldolgozás között. A korábbi fogalmazványok a

[2] Az Irányelv végleges szövege 1995 októberében az alábbi címen jelent meg: *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.* Brüsszel: OJ No. L281. 1995. október 24.

[3] Ez a folyamat – erősen leegyszerűsítve – az alábbi lépésekből állt: (1) A javaslat *(draft proposal)* kezdeményezése a tagországok kormányai által kinevezett 17 tagból álló Európai Bizottság részéről. (2) A tervezet véleményezése a tagországokból választott 518 tagú Európai Parlament és különféle parlamenti bizottságok által. (3) A tervezet revíziója a Bizottság által, a vélemények figyelembe vételével. (4) „Közös álláspont" kialakítására irányuló tárgyalás a miniszterek tanácsában (ebbe a végrehajtó testületbe a 12 tagország egy-egy súlyozott szavazattal rendelkező tagot delegál). (5) Az Európai Parlament végső jóváhagyása. (6) Közzététel.

személyes adatok feldolgozásának jogossága és az adatok tisztességes megszerzése tekintetében még megkülönböztették ezt a két szektort. Míg egyes jogszabályok csupán az „automatizált" adatfeldolgozásra vonatkoznak, az Irányelv hatálya alá tartozik „a személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető" (2. cikk, c pont). Az Irányelv megpróbálja továbbá elkerülni a mesterséges különbségtételt az információ gyűjtése, felhasználása és másokkal való közlése között, előnyben részesítve a „feldolgozás" fogalmát, amit kiterjeszt mindezekre a fázisokra, valamint más műveletekre is. A 108. számú Egyezményhez hasonlóan az Irányelv is tartalmaz specifikus feltételeket az adatok úgynevezett „különleges" formáinak meghatározására.

Az Irányelv – az Egyezménytől eltérően – meghatározza a tagországok „felügyelő hatóságainak" jellegét és funkcióját is. Minden egyes országnak gondoskodnia kell arról, hogy saját területén egy vagy több állami hatóság legyen felelős az Irányelv 28. cikke 1. bekezdésének megfelelően bevezetett nemzeti intézkedések végrehajtásának ellenőrzéséért. A felügyelő hatóságoknak teljesen függetlenül kell működniük, megfelelő hatáskörrel különféle vizsgálatok elrendelésére, beavatkozásra (különösen a feldolgozási műveletek megkezdése *előtt*), jogi eljárás kezdeményezésére, valamint a jogok és szabadságjogok *(rights and freedoms)* érvényesülésével, illetve az Irányelv hatálya alá tartozó adatfeldolgozási tevékenységek törvényességével kapcsolatos panaszok meghallgatására és kivizsgálására. A tagországoknak gondoskodniuk kell továbbá arról, hogy minden olyan adminisztratív intézkedés előkészítésekor, ami a privát szférát érintő következményekkel járhat, kikérjék a felügyelő hatóságok véleményét. Mindezeknek a kikötéseknek a teljesítése összességében nagyobb hatáskört biztosít a felügyelő hatóságok számára, és egyúttal nagyobb felelősséget ró rájuk, mint ami korábban számos európai adatvédelmi rendszerre jellemző volt.

A 29. és 30. cikk elrendeli egy tanácsadó munkacsoport *(Working Party)* létrehozását, amely minden egyes tagország felügyelő hatóságainak képviselőiből tevődik össze, kiegészítve az Európai Bizottság és az Unió más intézményeinek képviselőivel. Ennek a munkacsoportnak az a feladata, hogy tanácsokat adjon az Európai Bizottság számára a nemzeti törvények között mutatkozó eltérések, a harmadik országokban érvényesülő védelem szintje, az eljárási szabályok és az Irányelv esetleges kiegészítéseire vonatkozó javaslatok tekintetében. Az Irányelv előírásainak végrehajtását illetően a döntési hatáskör egy olyan testület kezében van, amit egyszerűen „a Bizottságnak" neveznek (*The Committee*, 31. cikk). Ez a tagországok képviselőiből áll, és elnöki tisztét az Európai Bizottság részéről delegált személy tölti be. A Bizottság az így kiépített mechanizmus révén fogadhatja el a Irányelv szellemében hozott határozatokat és szabályozásokat, különös tekintettel az Európai Unión kívüli harmadik országokban biztosított adatvédelem „megfelelő" szintjének meghatározására.

Egyes harmadik országok esetében az Irányelv területen kívüli implikációi komoly aggodalmakra adtak okot. A 25. cikkben az alábbi kikötések szerepelnek: „A tagállamoknak rendelkezniük kell arról, hogy a feldolgozásra kerülő vagy továbbítás után feldolgozásra szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha [...] az adott harmadik ország megfelelő védelmi szintet tud biztosítani. [...] A harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási mű-

velet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni." Különös figyelmet kell fordítani az adatok jellegére és felhasználási céljára, továbbá az „általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre." A 26. cikk ugyanakkor felsorol számos kivételt, amelyekre ez a rendelkezés nem alkalmazható.

Amennyiben a Bizottság megállapítja, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet, „a tagállamok megteszik a megfelelő intézkedéseket az azonos típusú adatoknak a szóban forgó harmadik országba irányuló továbbításának megakadályozására" (25. cikk, 4. bekezdés).* Ekkor a Bizottság „megfelelő időben tárgyalásokat kezdeményez a helyzet megoldására" (25. cikk, 5. bekezdés). Így tehát ha a Bizottság nem megfelelő szintű védelmet állapít meg, a tagországok nem egyszerűen engedélyt, hanem kifejezett utasítást kapnak arra, hogy megtiltsák az adatok továbbítását. Ez erősebb megfogalmazást jelent, mint azok, amelyek az OECD Irányelveiben vagy az Európa Tanács Egyezményében jelentek meg. Noha mind a két utóbbi okirat tartalmazza az „egyenlőség" elvét (ami alapos okkal nevezhető erősebbnek, mint a „megfelelőség"), egyik dokumentum sem követeli meg aláíróitól, hogy megakadályozza az adatok továbbítását olyan országokba, amelyek nem tudják a védelem egyenlő szintjét biztosítani.

Az Irányelv elfogadását követően a 29. cikk alapján létrehozott Munkacsoport kibocsátott egy sor politikai nyilatkozatot annak tisztázására, hogy az Irányelv 25. és 26. cikkét hogyan kell értelmezni. A „megfelelő védelem" feltételezi nemcsak az előírt követelmények elfogadását, hanem azok tényleges érvényesítését is a gyakorlatban. Az „elfogadás" az alábbi elvek elfogadását foglalja magában: célhoz kötöttség, adatminőség és arányosság, átláthatóság, biztonság, hozzáférési jogok, helyesbítés és bírálat, valamint a további harmadik országokba irányuló továbbítás korlátozása. A Munkacsoport azonban – bizonyos strukturális követelmények meghatározása helyett – azokat az alapvető funkciókat részletezte, amelyeket az adatvédelmi rendszereknek be kell tölteniük (EU 1997: 7):

1. A szabályoknak való *megfelelés jó szintjének* biztosítása. (Egyetlen rendszer sem garantálhat 100 százalékos megfelelést, de egyesek jobbak, mint mások.) A jó rendszert általában az adatkezelők részéről kötelességeik magas szintű, tudatos vállalása, az adatalanyok körében pedig jogaik és az azok gyakorlására szolgáló eszközök magas szintű ismerete jellemzi. A szabályok tiszteletben tartásának biztosításához fontos követelmény a hatékony visszatartó szankciók megléte, valamint természetesen az ellenőrzést végző hatóságok, illetve az ellenőrök vagy független adatvédelmi felelősök közvetlen felülvizsgálati rendszerének a működése is.

2. *Támogatás és segítség nyújtása az egyéni adatalanyok számára* jogaik gyakorlásához. Az embereknek képesnek kell lenniük jogaik gyors és hatékony érvényesítésére anélkül, hogy ez visszatartó költséget jelentene számukra. Ennek biztosításához lennie kell valamilyen fajta intézményi mechanizmusnak, amely lehetővé teszi a panaszok független szervek által történő kivizsgálását.

3. *Megfelelő jogorvoslat* nyújtása a sértett fél részére abban az esetben, ha a szabályokat nem tartják be. Ez kulcsfontosságú elem, amelynek olyan független döntőbírósági

* A szó szerinti idézetek az Irányelv *hivatalos* magyar szövegéből származnak. – *A ford.*

rendszert kell magában foglalnia, amely lehetővé teszi a kártérítés kifizettetését és egyéb szankciók érvényesítését, ahol erre szükség van.

A fentiekben leírt egész folyamat során az amerikai adatvédelmi szabályok vezettek a legnehezebb dilemmákhoz. Amennyiben az európaiak úgy találnák, hogy az USA – annak dacára, hogy az amerikai gazdaság számos területén nem érvényesülnek kötelező erejű adatvédelmi szabályok – eleget tesz az Irányelv által előírt „megfelelőség" próbájának, ez aláásná az EU Irányelv hitelességét. Másrészt viszont ha az Irányelvet betű szerint érvényesítenék, akkor az adatáramlásokra vonatkozó széleskörű tilalmak komoly fennakadásokat okoznának a nemzetközi kereskedelemben és a nemzetközi utasforgalomban, és szinte bizonyosan transzatlanti kereskedelmi vitákhoz vezetnének. Ennek felismerése alapján magas kormányzati szintű párbeszéd folyt a *DGXV** akkori főigazgatója, John Mogg és az USA kereskedelmi miniszterhelyettese, David Aaron között, ami a „Biztonságos kikötő" egyezmény (Safe Harbor Agreement) megkötéséhez vezetett. Ennek az egyezménynek az a célja, hogy azokat az amerikai vállalatokat, amelyek eleget kívánnak tenni a „biztonságos kikötő" kritériumainak, rábírja bizonyos – a Szövetségi Kereskedelmi Bizottság *(Federal Trade Commission, FTC)* által jóváhagyott és számukra kötelezően előírt – adatvédelmi szabályok betartására. 2001. december 21-ig 148 amerikai vállalat kötelezte el magát a „Biztonságos kikötő" egyezményben foglalt adatvédelmi elvek mellett, amelyeknek a megsértése kitenné őket annak, hogy az *FTC* a saját hatáskörében a „tisztességtelen és megtévesztő" üzleti gyakorlat bélyegét üsse rájuk.[4]

A 25. és 26. cikk előírásainak a gyakorlatba való átültetését – és valójában az Irányelv egészét tekintve – számos gond fennmarad a „Biztonságos kikötő" követelményeinek elfogadása mellett is.[5] Az Irányelv (a 31. cikk bizottságának jóváhagyásával) a Bizottság hatáskörébe utalja a harmadik országokba irányuló adattovábbítás szabályainak a meghatározását, amelyeket az egész Európai Unióban alkalmazni kell. Legalábbis az a veszély azonban fennáll, hogy az EU kormányzati döntéshozatali folyamatainak kiszámíthatatlansága érinteni fogja a „megfelelés" megítélését is, ami valószínűleg össze fog keveredni olyan kérdések eldöntésével, amelyeknek semmi közük sincs az információs privát szférához. A politikai érdekszövetségek tehát elnyomhatják a racionális és jobban előrelátható adatvédelmi szabályozásra irányuló törekvéseket. Egy másik leselkedő gond az, hogy sem a felügyelő hatóságoknak, sem az adatkezelőknek nincs kellő energiájuk ahhoz, hogy tüzetesen tanulmányozzák más államoknak a személyes adatok kezelésére vonatkozó jogszabályait, és abban a kérdésben sem lehetünk teljesen nyugodtak, hogy az adatalanyok vajon ténylegesen gyakorolni tudják-e a privát szféra védelmét biztosító jogaikat. Az Irányelv nem oldja meg azt a központi dilemmát, amely áthatja a nemzetközi adatforgalom szabályozására az Egyezményben vagy a modellszerződések-

* *Directorate General XV,* az Európai Bizottságnak az egységes piac és a vállalati jogok kérdéseivel foglalkozó 15. sz. főigazgatósága. – *A ford.*

[4] A „Biztonságos kikötő" egyezmény valamennyi dokumentuma megtalálható a következő URL címen: http://www.export.gov/safeharbor

[5] Az Irányelv jelenlegi működésére vonatkozó vélemények egy Brüsszelben 2002 októberében tartott nagy konferencián kaptak nyilvánosságot. Lásd „A brüsszeli konferencia vitatja az EU adatvédelmi törvényeinek tervezett megváltoztatását". *(Brussels Conference Debates Changes to EU Data Protection Laws), Privacy Laws and Business* No. 65, November 2002.

ben korábban tett kísérleteket. Olyan ellenőrzési mechanizmus hiányában, amely biztosítaná, hogy a személyes adatokat valamely harmadik országban *ténylegesen* tisztességesen és törvényesen kezelik, a megfelelés elbírálása valószínűleg továbbra is „a törvény betűi szerint vagy más formális jellemzők elemzése alapján" fog történni, nem pedig empirikus úton (Raab és mtsai 1998).

Az európai törvényeknek a saját joghatóságukon kívüli tiszteletben tartásával kapcsolatban ugyanezek a gondok kerülnek felszínre abban az új irányelvben is, amelyet 2002 júliusában fogadtak el „a magánélet védelméről az elektronikus hírközlési ágazatban" (EU 2002). Ez az irányelv felvált egy korábbi hírközlési adatvédelmi irányelvet, és az interneten folyó kommunikáció tekintetében új szabályok sorát alkotja meg a privát szféra védelmére. Különösen ellentmondásosak benne azok a rendelkezések, amelyek az alábbi területekre vonatkoznak: a „forgalmi adatok" visszatartása; a „lokációs adatok" feldolgozása; továbbá a kéretlen kommunikáció, különösen az e-mail útján küldött *spam* ellenőrzése. Ezt az újabb irányelvet várhatóan 2003 októberéig kell beiktatni a tagállamok nemzeti törvényeibe.

A nemzetközi szabályozás arénái

Az adatvédelem gyakorlati megvalósításának folyamatában mutatkozó szakadék felismerése egyeseket arra a meggyőződésre vezetett, hogy az adatvédelem kérdésével a világ szabványügyi tervező és hitelesítő testületeinek kell foglalkozniuk, mert ezek az intézmények sok éves tapasztalattal rendelkeznek a „megfelelési szintek" megfigyelésében és különféle nemzetközi normák alapján történő mérésében. Az információbiztonsági szabványok néhány éven át perifériku s, ám fontos szerepet játszottak a privát szféra védelmében. Az 1990-es években azonban a nemzetközi szervezetek napirendjére került az a gondolat, hogy a privát szférával kapcsolatos elvek összességét illetően általánosabb kezelési szabványokra van szükség. Ez a gondolat – nagy vonalakban – azokból a tárgyalásokból származott, amelyeket a „Szabályozási minták a személyes információk védelmére" *(Model Code for the Protection of Personal Information)* című dokumentum kidolgozásáról a Kanadai Szabványügyi Társaság *(Canadian Standards Association)* égisze alatt folytattak Kanadában (CSA, 1996). A szabályozási minták közzététele számos kísérletet ösztönzött hasonló okmány kidolgozására a nemzetközi szintre vonatkozóan is, annak a gondolatnak a jegyében, hogy a privát szféra védelme – hasonlóan az *ISO 9000* minőségbiztosítási szabványok sorozatához – a „minőségbiztosítás" egyik elemének tekinthető.

A folyamat először a nemzetközi szabványügyi szervezet *(International Organization for Standardization, ISO)* intézményeiben indult meg. A várható eredmények azonban – főleg bizonyos amerikai bázisú multinacionális üzleti érdekeltségek igen intenzív lobbi-tevékenységének következtében – nem születtek meg. Innen kiindulva az elgondolás átvándorolt a speciálisan európai szabványügyi testületekhez. Az Európai Szabványügyi Bizottság *(Comité Européen de Normalisation, CEN)*, amely Európán belül felelős a szabványok egyeztetéséért, az Irányelv 29. cikke alapján létrehozott munkabizottság támogatásával tanulmányozni kezdte egy nemzetközi szabvány bevezetésének lehetőségeit a privát szférára vonatkozóan.[6] Egy Brüsszelben 2000 márciusában tartott

nyílt konferencián azt javasolták, hogy a szabványosítási tevékenységet a következő három irányban kellene megkezdeni: 1. olyan általános adatvédelmi szabvány kidolgozása, amely operatív gyakorlati lépések megtételét határozná meg a szervezetek számára ahhoz, hogy megfeleljenek a releváns adatvédelmi törvényeknek, elsősorban az EU Irányelvének; 2. szektorspecifikus kezdeményezések sorozata, olyan kulcsfontosságú területeken, mint az egészségre vonatkozó információk és a humán erőforrás menedzsment; és 3. az *online* környezettel kapcsolatos feladatspecifikus kezdeményezések. Egy hivatalos döntés az európai Irányelv alátámasztása érdekében három szabványügyi testületnek *(CEN, CENELEC, ETSI)* mandátumot adott a további szabványosítási munka lehetőségeinek tanulmányozására. Innentől kezdve az irányítás „A privát szférával kapcsolatos európai szabványosítási kezdeményezés" *(Initiative on Privacy Standardization in Europe, IPSE)* hatáskörébe került.[7]

A javaslat támogatói azt állítják, hogy egy ilyen nemzetközi szabvány nagy figyelmet kapna és a nemzetközi normákhoz való igazodási erőfeszítéseket váltana ki a különféle nemzeti szabványügyi testületek részéről, mert az Európán kívüli üzleti partnerek számára megbízhatóbb és következetesebb módszert nyújtana ahhoz, hogy bizonyíthassák a nemzetközi adatvédelmi szabványoknak való megfelelésüket. Megbízhatóbb mechanizmust nyújtana továbbá az Irányelv 25. cikkének gyakorlati érvényesítéséhez is. Mint korábban említettem, a törvények és a szerződések alapos megvizsgálása önmagában nem nyújt kellő biztosítékot az európai adatvédelmi szervezetek számára azt illetően, hogy a fogadó országok joghatósági rendszerei valóban követni fogják az adatvédelmi szabályokat. Egy szabvány megkövetelt bevezetése, ami független és rendszeres ellenőrzést tételez fel, nagyobb bizonyosságot nyújtana abban a tekintetben, hogy a fogadó szervezetek – akárhol helyezkednek is el – „megfelelő" adatvédelmet alkalmaznak a gyakorlatban. Ez természetesen további erőfeszítéseket kívánna meg a „megfelelés" értékelése és az ellenőrzés hitelesítési rendszereinek harmonizálása terén is. Végső soron kölcsönös bilaterális és multilaterális elismerési egyezményeket kellene kötni annak biztosítására, hogy az adatvédelem „megfelelő" szintjének értékelésére hivatott belföldi rendszereket mindenütt tiszteletben tartsák. Ezek a kezdeményezések mindazonáltal igen nagy fokú ellenállással találkoztak a vállalatok és általában az információigényes szektorok részéről (Bennett, 2000). E tanulmány írása idején semmi esetre sem tekinthető tisztázottnak, hogy a személyes adatok védelme állandó jelleggel a szabványügyi tervező és hitelesítő testületek hatáskörébe fog-e kerülni.

Konklúzió: A privátszféra védelme és a világkereskedelem

Ezt az esszét egy anekdotával kezdtem, amelynek az volt a célja, hogy rámutasson a privát szféra és a szellemi tulajdon közötti különbségekre. Azt fejtegettem, hogy a privát szféra védelme ma önálló jogi terület, ahol egyre nagyobb számú kihirdetett jogsza-

[6] A privát szféra területén megvalósítandó szabványosításra vonatkozó kanadai kezdeményezésről alkotott 1/97. számú vélemény megtalálható:
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp2en.htm

[7] Az elérhető dokumentációt lásd: http://www.cenorm.be/isss

bállyal találkozunk, és ezek betartását az információs privát szféra biztonságáért felelős adatvédelmi hatóságok egyre nagyobb mértékben intézményesített hálózata ellenőrzi. Ezen túlmenően a privát szféra védelmének porondján megjelentek a nagyvállalati adatvédelmi felelősök és a privát szféra érdekében fellépő szószólók nemzetközi hálózatai, továbbá a kisebb vállalkozások sokasága is gondoskodik a privát szférát erősítő technológiák alkalmazásáról az aggódó fogyasztók érdekében. Számos országban igen sok ember érdekelt abban, hogy a privát szféra védelme továbbra is jelen legyen a nemzeti és nemzetközi politika napirendjén. Egy bizonyos vonás tekintetében azonban a privát szféra és a szellemi tulajdon védelmének kérdései közelítenek egymáshoz. A privát szféra védelme – csakúgy, mint a szellemi tulajdon védelme is – óhatatlanul kereskedelmi összefüggésekbe került, s ennélfogva előbb-utóbb valószínűleg be fogják illeszteni azoknak a kérdéseknek a szélesebb spektrumába, amelyekről a Világkereskedelmi Szervezeten *(World Trade Organization, WTO)* belül folytatnak tárgyalásokat, és ott hozzák meg a döntéseket. Idevágónak látszik tehát ezt a tanulmányt néhány arra vonatkozó gondolattal zárni, hogy az adatvédelem milyen helyet foglalhat el a nemzetközi kereskedelem szélesebb politikai palettáján.

Az amerikai megfigyelők számára az európai adatvédelmi mozgalom 1970-es évekre tehető kezdeteitől fogva aggodalmat okozott, hogy az európai törvények extraterritoriális rendelkezései felhasználhatók a vámmentes kereskedés akadályozására, azoknak az európai információs technológiai iparágaknak a védelmében, amelyeket az amerikaiak a sajátjaiknál kevésbé fejlettnek és kevésbé innovatívnak tekintettek. Az európai hátsó szándékokkal kapcsolatos retorika – ahogy az Európa Tanács, az OECD és az EU harmonizációs törekvései előre haladtak és az adatvédelem központi fontosságra tett szert a nemzetközi elektronikus kereskedelemben – még inkább felfűtötté vált. Maga az a kilátás, hogy az EU Irányelve esetleg megvédelmezheti az európai üzleti érdekeket az amerikai versennyel szemben – függetlenül a valódi, nyilvánvalóan szerteágazó és bonyolult európai indítékoktól – egész sorozatnyi izgalmas kérdést vet fel azt illetően, hogy ezek az európai szabályozások vajon sértik-e a világkereskedelem fennálló szabályait vagy nem. Swire és Litan (1998: 145) szerint azokat az amerikai vállalatokat, amelyek Európán belül kívánnak működni, az európai adatvédelmi törvények – a lehető legkevesebbet mondva is róluk – rá fogják kényszeríteni arra, hogy tartsák tiszteletben a szabályokat és fogadják el a személyes információk kezelésére alkalmazott módszereik korlátozásait. Swire és Litan hangoztatják továbbá, hogy az európai vállalatok inkább olyan belföldi információ-feldolgozó cégekkel fognak szerződéseket kötni, amelyeknél az Irányelv védelmi ernyője nem gátolja a személyes adatok cseréjét.

Az USA vagy bármelyik más nem európai állam bármilyen fellépése az adatvédelmi törvények protekcionista hatásai ellen igen nagy valószínűséggel az „Általános Egyezmény a Szolgáltatások Kereskedelméről" *(General Agreement on Trade in Services, GATS)* hatálya alá esne, ami azt jelenti, hogy az egyes államoknak különféle szektorok és tevékenységek tekintetében „elkötelezettséget" kell tanúsítaniuk „piacaik hozzáférhetővé tételére". Ha valamely személyes adat átvitele az ilyen elkötelezettségek valamelyikének a hatálya alá esik, akkor az EU köteles az amerikai vállalatokat ugyanolyan kedvezményekben részesíteni, mint az európaiakat. A *GATS* VI. cikkelye így fogalmaz: „Azokban a szektorokban, ahol konkrét elkötelezettséget vállaltak, minden Tagnak biztosítania kell, hogy valamennyi általános érvényű intézkedés, ami kihatással

van a szolgáltatások kereskedelmére, ésszerű, objektív és részrehajlástól mentes módon történjék". Az Irányelv alkalmazhatóságának bármilyen kétségbevonása tehát ekkor az „ésszerű" *(reasonable)* szó értelmezésétől függene (Shaffer 2000: 49). Továbbá, talán még fontosabb, hogy az Irányelv 25. és 26. cikkének rendelkezései értelmében az adatátvitel bármilyen tiltását pártatlanul kell alkalmazni. Így, ha az EU betiltaná az adatok kivitelét egy bizonyos országba, de egy másikba nem, ahol pedig ugyanolyan mértékben „nem megfelelő" az adatvédelem, akkor összeütközésbe kerülne a „legnagyobb kedvezményben részesülő országokra" vonatkozó klauzulával a *GATS* II. cikkelyében, ami a következőket mondja ki: „Minden olyan intézkedés esetében, ami ennek az Egyezménynek a körébe tartozik, valamennyi Tagnak azonnal és feltétel nélkül biztosítania kell, hogy bármely más Tag szolgáltatásai és szolgáltatói olyan kezelésben részesüljenek, ami nem kevésbé kedvező, mint amivel [az illető Tag] bármely más ország hasonló szolgáltatásait és szolgáltatóit kezeli."

A pártatlansági követelmény magyarázza az Irányelv 29. és 31. cikkeihez felállított bizottságok óvatos kísérleteit egy világos metodika kifejlesztésére a „megfelelés" értékeléséhez, valamint a harmadik országokban meglevő adatvédelem különféle aspektusainak átfogóbb, tapasztalatokra alapozott tisztánlátására irányuló törekvéseiket is (lásd Schwartz és Reidenberg 1996, Raab és mtsai 1998). Mindkét bizottság formálisan elkötelezte magát a diszkrimináció 2000-re tervezett eltörlése mellett. A 31. cikk bizottsága – az Emberi Jogok Európai Egyezményének *(European Convention of Human Rights)* rendelkezéseit idézve – megerősítette elkötelezettségét a diszkrimináció eltörlése, valamint „az egyenlőség általános elve mellett, ami különös hangsúllyal nyilvánítja ki a nemzetiség alapján történő diszkrimináció tiltását, és ami a Közösség jogrendszerének egyik alapvető elve." A bizottság a továbbiakban így foglalt állást: „Fontos, hogy képesek legyünk a különféle szituációk érdemeik alapján való megítélésére, és az egyenlő bánásmód elvét ne tekintsük valamiféle egyetlen modell harmadik országokra való rákényszerítésének".[8] Úgy tűnik tehát, hogy a szabályozás azon a megkérdőjelezhető feltevésen nyugszik, hogy a megfelelés értékelésére – pártatlan módon – különféle rugalmas módszereket lehet használni.

Shaffer (2000) a fenti nehézségek ellenére is arra a következtetésre jutott, hogy bármely harmadik országban tett kísérlet az EU adatvédelmi szabályozásának figyelmen kívül hagyására valószínűleg nem járna sikerrel a WTO előtt, három ok miatt. Először is, azt lehet állítani, hogy az adatforgalom bármely tilalma éppen olyan károsan érintené az európai tulajdonban lévő és az Európai Unióban bejegyzett vállalatokat, mint amennyire az Unión kívülieket. Másodszor, az EU tevékenysége olyan közérdekű célok elérésére irányul, amelyeket a *GATS* – explicit formában – általános kivételként említ:

> Annak a követelménynek a fenntartásával, hogy ilyen intézkedéseket nem hoznak olyan módon, ami önkényes vagy igazolhatatlan diszkrimináció eszköze lehetne olyan országok között, ahol hasonló feltételek uralkodnak, vagy ami burkolt korlátozást jelentene a szolgáltatások kereskedelmére nézve, ez az Egyezmény semmiféle

[8] A 31. cikk bizottsága által 2000. május 31-én elfogadott szövegnek a diszkriminációval kapcsolatos része elérhető ezen a címen: http://www.export.gov/safeharbor/nondiscrimArt31May00.htm.

> feltételt nem foglal magában olyan intézkedések bevezetésének vagy végrehajtásának a megakadályozására, amelyek [...] szükségesek a jelen Egyezmény rendelkezéseivel összhangban álló törvények vagy szabályozások betartatásához, ideértve (ii) az egyének privát szférájának védelme érdekében a személyes adatok feldolgozásával és terjesztésével, valamint az egyénekre vonatkozó nyilvántartások és feljegyzések bizalmasságának védelmével kapcsolatos előírásokat. (*GATS*, XVI. cikkely)

Harmadszor pedig Shaffer azt állítja, hogy a viták rendezése során a *WTO* keretein belül minden egyeztető fórum vonakodna a felek lényeges anyagi érdekeit érintő határozatok meghozatalától, és inkább arra hajlana, hogy az eljárási kérdésekre koncentráljon. Ezt a beletörődő attitűdöt Shaffer véleménye szerint alátámasztja a *WTO* jelenlegi gyakorlatának alapjául szolgáló jogtudomány is.[9]

Semmiféleképpen nem áll módunkban megítélni, hogy ezek az előrejelzések vajon helyesnek fognak-e bizonyulni, de valószínűnek látszik, hogy egy bizonyos ponton, bizonyos körülmények között sor fog kerülni a nemzetközi adatvédelmi törvények próbára tételére a *WTO* apparátusán belül is. Az európai szabályozás amerikai bírálatainak kontextusában tekintélyes mennyiségű előzetes elemzés – érthető módon – már eddig is figyelembe vette ezeket a forgatókönyveket. Észben kell azonban tartanunk, hogy a határokon átívelő adatáramlással kapcsolatos rendelkezések megjelennek a legtöbb nemzet törvényeiben. Potenciális vitákra sor kerülhet tetszőleges számú kereskedelmi partner között, a világ szinte bármely térségében.[10] Éppen ezért valószínű, hogy a jövőben a nemzetközi kereskedelmi jog bonyolult, és az adatvédelmi szakemberek számára bizonyos mértékig ismeretlen világa lesz az egyik legfontosabb küzdőtér, ahol egyezkedések fognak folyni az adatvédelmi törvényekről.

[9] Különösen a garnélarákok és a tengeri teknősök esete, ami magával vonta az USA tilalmát a garnélarákok importjával szemben: e tilalom bevezetését az USA azzal indokolta, hogy Délkelet-Ázsiában nem tesznek eleget a tengeri teknősök védelmét szolgáló természetvédelmi előírásoknak (Shaffer 2000: 52).

[10] Érdemes megjegyezni, hogy a spanyol hatóságok 1999-ben, még az Irányelv hatályba lépése előtt majdnem hatvanezer dollárra megbüntették a *Microsoft* vállalatot azért, mert európai alkalmazottai köréből nem megfelelő módon gyűjtött adatokat egy amerikai honlapon, s ezzel megszegte a spanyol adatvédelmi szabályokat.

Függelék

Az információs privát szférával kapcsolatos törvények életbe lépése, régiónként[11]

	1970-es évek	1980-as évek	1990-es évek
Nyugat-Európa	Svédország (1973) Nyugat-Németország (1978) Dánia (1978) Ausztria (1978) Franciaország (1978) Norvégia (1978) Luxemburg (1978)	Izland (1981) Egyesült Királyság (1984) Finnország (1987) Írország (1988) Hollandia (1988)	Portugália (1991) Spanyolország (1992) Svájc (1992) Belgium (1992) Olaszország (1996) Görögország (1997)
Kelet-Európa			Szlovénia (1990) Magyarország (1992) Cseh Köztársaság (1992) Észtország (1996) Litvánia (1996) Lengyelország (1997) Szlovákia (1998) Lettország (2000)
Észak-Amerika	Egyesült Államok (1974)	Kanada (1982)	
Dél-Amerika			Chile (1999)
Ausztrálázsia		Új-Zéland (1982) Ausztrália (1988)	
Kelet-Ázsia		Japán (1988)	Dél-Korea (1994) Hong Kong (1995) Tajvan (1995)

Irodalom

Bennett, C. J. (1992): *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.

Bennett, C. J. (2000): *An International Standard for the Protection of Personal Information: Objections to the Objections*. Paper presented to the 2000 conference of *Computers, Freedom & Privacy* (CFP 2000). April 19, San Francisco, at: http://www.acm.org/pubs/articles/proceedings/cas/332186/p33-bennett/p33-bennett.pdf.

[11] Ez a táblázat azokat az első dátumokat mutatja, amikor az információs privát szférára vonatkozó, illetve adatvédelmi törvények meghozatalára sor került az egyes országokban, akár csupán a közszférában, akár mind a magánszektorban, mind a közszférában. A táblázat nem foglalja magában az olyan törvényhozási intézkedéseket, amelyeknek a hatálya nem terjed ki az egész országra. Nem tartalmazza továbbá az információszabadságra vonatkozó törvényeket, valamint az olyan törvényeket sem, amelyek kizárólag a magánszektorban működő vállalatok tevékenységét szabályozzák. A táblázatban nem szerepelnek a törvények hatályba lépését követő módosítások.

Bennett, C. J. – Grant, R. (eds) (1999): *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press.

Bennett, C. J. – Raab, C. (2003): *The Governance of Privacy: Policy Instruments in Global Perspective.* Aldershot: Ashgate Press.

Bygrave, L. A. (2002): *Data Protection Law: Approaching its Rationale, Logic and Limits.* The Hague, Kluwer International Law.

Canadian Standards Association (CSA) (1996): *Model Code for the Protection of Personal Information.* CAN/CSA-Q830-96, CSA, Rexdale, at: http://www.csa.ca.

Council of Europe (CoE) (1981): *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).* Strasbourg: Council of Europe.

Eger, J. M. (1978): Emerging Restrictions on Transnational Data Flow: Privacy Protection or Non-Tariff Trade Barriers? *Law and Policy in International Business,* Vol. 10, 1055–1103.

European Union (EU) (1995): *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.* Brussels, OJ No. L281, (The EU Data Protection Directive) (24 October 1995).

– (1997): *First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy.* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Brussels, at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp4en.pdf.

– (2002): *Directive 2002/58/EC of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.* Brussels, OJ EC L 201 (12 July 2002), 20.

Flaherty, D. H. (1989): *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.* Chapel Hill: University of North Carolina Press.

Gellman, R. M. (1993): Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. *Software Law Journal,* vol. 6, 199–231.

General Agreement in Trade and Services (GATS) (1994): *General Agreement on Tariffs and Trade.* Geneva: The World Trade Organization, at: http://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm.

Hondius, F. W. (1975): *Emerging Data Protection in Europe.* Amsterdam: North Holland Publishing.

Lessig, L. (1999): *Code and Other Laws of Cyberspace.* New York: Basic Books.

Lyon, D. (1994): *The Electronic Eye: The Rise of Surveillance Society.* Minneapolis: University of Minnesota Press.

Organisation for Economic Co-operation and Development (OECD) (1981): *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OECD, at: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

Organisation for Economic Co-operation and Development (OECD) (1992): *Guidelines for the Security of Information Systems.* Paris: OECD, at: http://www.oecd.org/dsti/sti/it/secur.

Organisation for Economic Co-operation and Development (OECD) (1997): *Cryptography Policy: The Guidelines and the Issues.* Paris: OECD, at: http://www.oecd.org/dsti/sti/it/secur.

Organisation for Economic Co-operation and Development (OECD) (1999): *Directorate for Science, Technology and Industry. Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks.* Paris: OECD, at: http://www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)12-final.

Raab, C. D. (1999): From Balancing to Steering: New Directions for Data Protection. In Bennett, C. J. – Grant, R.: *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press, 68–93.

Raab, C. D. – Bennett, C. J. – Gellman, R. – Waters, N. (1998): *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer.* Office for Official Publications of the European Commission, Luxembourg, at: http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/adequat.htm.

Rule, J. – Hunter, L. (1999): Towards Property Rights in Personal Data. In Bennett, C. J. – Grant, R. (eds.): *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press, 168–181.

Schwartz, P. – Reidenberg, J. (1996): *Data Privacy Law: A Study of United States Data Protection.* Michie, Charlottesville, VA.

Shaffer, G. (2000): Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U. S. Privacy Standards. *Yale Journal of International Law*, vol. 25, 1–88.

Smith, R. E. (1993): *War Stories: Accounts of Persons Victimized by Invasions of Privacy.* Privacy Journal, Providence, RI.

Swire, P. – Litan, R. (1998): *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* Washington DC: Brookings Institution.