
# Jelentés az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény hiányosságairól

II. rész

Strasbourg, 3 November 2010, november 3. T-PD-BUR(2010)09 (II) FINAL

Az adatvédelmi egyezmény Tanácsadó bizottságának Irodája (T-PD-BUR)
22. értekezlet
2010. november 15-17.

Szerzők:
Cécile de Terwangne, Professeur à la Faculté de Droit de l'Université de Namur,
Directrice de recherche au CRID
Jean-Philippe Moiny, aspirant du F.R.S.-FNRS
Chercheur au CRID
Avec la collaboration de :
Yves Poullet, Recteur de l'Université de Namur (FUNDP), Professeur à la Faculté de droit,
Directeur de recherche au CRID
Jean-Marc Van Gyzeghem, Senior Researcher au CRID

Nem hivatalos fordítás.

# Tartalomjegyzék

## Bevezetés

E jelentés célja, hogy azonosítsa azokat a területeket, ahol sajátos problémák merülnek fel a személyes adatok védelme elvei alkalmazásakor a technika új eredményei felhasználása folyamán.
A megfontolások összességükben a 108. Egyezménynek (Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során), valamint a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló, 2001. november 8-án kelt Kiegészítő Jegyzőkönyvének egyes rendelkezéseire vonatkoznak, különös tekintettel arra, választ adnak-e még napjainkban is a technika újabb eredményeivel kapcsolatos elvárásokra és aggályokra. Vajon e rendelkezések kielégítően garantálják-e még az adatok védelmét az Interneten, a Web 2.0 különféle alkalmazásai, a térbeli lokalizációs technikák, az adatcserék, az RFID csipek, a biometrikus azonosítás stb. tekintetében?
Evégből a jelentés két különböző részre tagozódik. Az első rész a 108. Egyezmény kihirdetése óta a technika terén bekövetkezett változásokat írja körül, feltárva e változásokkal kapcsolatos fontos jelenségeket, figyelmet fordítva az egyénnek a technika fejlődéséből fakadó új fajta sebezhetőségére. A jelentés második része a jelenlegi oldalakon olvasható. E részben elemezzük a 108. Egyezmény rendelkezéseinek szerepét az új fejlemények tükrében abból a célból, hogy azonosítsuk aktuális szövegezésük esetleges hiányosságait az adatok védelmét fenyegető új veszélyek és e védelemmel szemben jelentkező új elvárások tükrében.
Ez a jelentés bizonyos tekintetben felfogható úgy is, mint az a „L'autodétermination informationnelle à l'ère d'Internet" (Információs önrendelkezés az Internet-korban) című jelentés, amely a 108. Egyezmény adatvédelmi elveinek a távközlési világhálózatra való alkalmazásáról készített 2004-ben a Namuri Egyetem (Belgium) Informatika és Jog Kutató Központja az Európa Tanács megbízásából[1]. E tekintetben egyes részek teljes mértékben megőrizték érvényességüket, és eredeti szövegüket, szükség esetén formai kiigazításokkal, félkövéren kiemelve és aláhúzva idéztük.

## A 108. Egyezmény rendelkezéseinek konfrontációja az új technikai környezettel

Az elemzés a 108. Egyezmény, valamint a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló, 2001. november 8-án kelt Kiegészítő Jegyzőkönyve rendelkezéseinek a jelentés első részében tárgyalt új technikai környezettel való konfrontációjára irányul. Ennek a konfrontációnak a tükrében igazolható, hogy e rendelkezések még mindig megfelelő választ adnak-e az új kihívásokra és garantálják-e még az egyén megfelelő védelmét a személyes adatok kezelése során. E második, elemző rész célja tehát, hogy felfedje a védelemben jelentkező esetleges hiányosságokat.
Az elemzés az Egyezmény szövegére támaszkodik, logikailag követve annak szerkezetét.
Természetes, hogy elemzésünk tárgyával számos dokumentum foglalkozik, melyek közül többet különféle nemzetközi szervezetek fogadtak el, s melyek tápanyagát képezik a következő oldalaknak. Különös tekintettel voltunk az Európa Tanács, az Európai Unió, az OECD és az APEC szervezetei által kibocsátott dokumentumokra, köztük az EU irányelveire, az európai adatvédelmi biztos véleményeire, az európai adatvédelmi hatóságok csoportja (29-es munkacsoport) dokumentumaira, valamint az APEC e tárgyban legutóbb elfogadott

[1] Y. POULLET, J.-M. DINANT, avec la collab. de C. de TERWANGNE ET M.-V. PEREZ-ASINARI, «L'autodétermination informationnelle à l'ère de l'Internet», Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

regionális szövegére. Az Európai Emberi Jogi Bíróság és az Európai Unió Bíróság esetjogát, amennyiben elemzésünket segítik, ugyancsak figyelembe vettük.

# 1. Az Egyezmény tárgya és célja

## 1.1 Az Egyezmény célja: az adatok védelme

### *1.1.1 Az adatok védelme és a magánélet védelme*

Érdekes, hogy a 108. Egyezmény kezdettől fogva két jogot nevesített, mikor célját így határozta meg: „minden egyén számára (…) biztosítva legyen, hogy *jogait és alapvető szabadságjogait,* különösen a magánélethez való jogát tiszteletben tartsák a személyes adatainak gépi feldolgozása során”[2].

Az Egyezmény 1. cikkében kifejezetten jelzi, hogy az adatvédelem nem csupán a magánélet védelmét öleli fel. Egyéb jogokat és szabadságokat is figyelembe kell venni, például a szabad mozgást, a biztonságot, a lakhatást, a foglalkoztatottságot, a tájékoztatás és véleménynyilvánítás átláthatóságát stb. A multinacionális vállalkozások vagy államközi kapcsolatok hálózatai keretében létrehozott adatbázisok, lehetővé téve szolgáltatások igénybe vevői *a priori* profilírozását, az egyének diszkriminálásához vezethet, midőn lakást keresnek, információ után kutatnak, biztosítást kötnek vagy munkahelyet keresnek[3]. Másik példa a hagyományos fizetési módok egyre terjedő helyettesítése a hitelkártyával való fizetéssel, mely kártyák kibocsátói oligopolisztikus pozícióban vannak, ami megfontolás tárgyává teszi azt a hatást, mely az egyént éri mind a hitelkártya visszavonása vagy zárolása során a mozgás szabadságára, s mind inkább a kártyahasználat elemzésére nézve az egyén aktivitásának globális megfigyelése folytán.

Ha az adatok védelmének játéktere nem korlátozódik a magánélet kizárólagos védelmére, úgy kapcsolata ez utóbbival meglehetősen korlátozott. Az adatok védelme a magánélethez fűződő jogok kiterjesztése, amely a személyes autonómiában[4] vagy még inkább az önrendelkezési jogban[5] teljesedik ki, mindenek előtt a magánélet fogalmához hagyományos kapcsolódó bizalmasság követelményének értelmében. Az adatvédelem nem más, mint jog az információs önrendelkezéshez. A 108. Egyezmény vitathatatlanul ezt a megközelítést tükrözi, midőn rögzíti a polgároknak az adatkezelés feletti ellenőrzési jogosultsága érvényesítésének módjait, így a tájékoztatáshoz való jog és a mások által kezelt adatokhoz való hozzáféréshez való jog követelményét, meghatározva az adatkezelő jogainak korlátait mind közjogi, mind magánjogi adatkezelők esetében (törvényes cél, arányosság, biztonság, …) Egy negatívabb és korlátozóbb megközelítés, amikor a magánéletet védekező koncepciónak tekintjük, ennek ellenére felismerhető a különleges adatok esetében (az Egyezmény 6. cikke), érvényesítve a tiltás elvét, amely a polgár védelmét garantálja ilyen adatai bizalmas voltát érő támadásokkal szemben.

---

[2] A 108. Egyezmény 1. cikke (a szerzők kiemelése).

[3] E kérdésben lásd az Amazon „*diszkriminatív árazási*” gyakorlatát, melyre az amerikai fogyasztók egyesülete derített fényt, minek következtében a cég felhagyott vele.

[4] Az európai emberi jogi egyezmény 8. cikkében meghatározott, a magánélet védelméhez fűződő jogból levezetett személyes autonómia dimenziójának megvilágítására vonatkozóan lásd: Cour eur. D.H., *Pretty c. Royaume-Uni*, arrêt du 29 avril 2002, req. n° 2346/02 ; *Van Kück c. Allemagne*, arrêt du 12 juin 2003, req. n° 35968/97 ; *K.A. et A.D. c. Belgique*, arrêt du 17 février 2005, req. n° 42758/98 et 45558/99.

[5] Az EEJE 8. cikkében meghatározott, a magánélet védelméhez fűződő jogból levezetett önrendelkezési jogának vagy a személyes autonómia jogának kifejezetten elismeréséről lásd: Cour eur. D.H., *Evans c. Royaume-Uni*, arrêt du 7 mars 2006, req. n° 6339/05 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; *Tysiac c. Pologne*, arrêt du 20 mars 2007, req. n° 5410/03 ; *Daroczy c. Hongrie*, arrêt du 1er juillet 2008, req. n° 44378/05.

Az Európa Tanács Parlamenti Közgyűlése ebben a szellemben igyekezett elkészíteni 428. sz. Határozatát (1970). Következésképpen az Emberi Jogok Európai Egyezményének 8. cikkében garantált, a magánélet tiszteletben tartásához fűződő jogot e Határozatban a Közgyűlés 1970 januárjában a tömegkommunikáció módjáról és az emberi jogokról szólva úgy határozta meg, mint ami „jog az élet minimális beavatkozással való viteléhez". Közel harminc évvel e szöveg elfogadását követően a Közgyűlés azt így pontosította: „Tekintettel az adatok tárolását és felhasználását célzó új kommunikációs technikák megjelenésére, ezt a meghatározást ki kell egészíteni *az egyén saját adatai feletti ellenőrzés jogával*"[6].
Az Európai Unió Alapjogi Chartája, amely a Lisszaboni Szerződés hatályba lépése óta jogi kötelező erővel bír, élve a lehetőséggel – minden esetre pedagógiai okokból – különbséget tesz a magánélet (7. cikk) és az adatvédelem koncepciója (8. cikk) között[7].
A magánélet tiszteletben tartásához fűződő jogot autonomizálván az adatok védelméhez fűződő jog esetében számításba kell venni egyrészt az adatkezelő túlsúlyát az érintettel szemben, mely túlsúly az adatkezelő rendelkezésére álló adatok kezelésének kapacitásával kapcsolatos és napjainkban a technika fejlődése következtében drámaian megnövekedett, másrészt az adatkezelésnek a fentebb említett jogokra és szabadságokra gyakorolt hatását. A technikák, inkább választott konfigurációjuk, mint szükséges voltuk miatt, „nyomot" generálnak és konzerválnak a szolgáltatások felhasználásáról, és lehetővé teszik, a tíz évekkel (mondhatni huszonkilenc évvel) korábbihoz nem hasonlítható mértékű kezelési kapacitás révén az egyén és viselkedése megismerését, legyen e viselkedés egyéni vagy kollektív, személyes vagy anonim. Másképp fogalmazva az adatok felhasználása növeli az információ felett rendelkezők túlsúlyát egyénekkel szemben, legyen bár az egyén érintett avagy nem. A gyűjtött információ alapján kollektív döntés (például az adókulcs, egy betegség kezelési költségeinek megállapítása) vagy egyedi döntés (például hitel- vagy banki szolgáltatásra vonatkozó kérelem elutasítása) hozható.
Összefoglalva: a 108. Egyezmény nem esett a magánélet védelmét szolgáló adatok védelme területének csökkentése csapdájába, mely különösen hátrányos, ha e terület, mint olykor sajnos, nem öleli fel a klasszikus „right to be left alone"-t (vagyis a békén hagyáshoz való jogot), mint a bizalmasság követelményét. Vajon nem jelzi ez, hogy **mint evidenciát jobban figyelembe kell venni az adatvédelemhez fűződő jog koncepciójával kifejezett aggodalmakat? Fel kell-e ismernünk mint az Egyezmény hiányosságát, amely az 1. cikkben, az adatvédelem meghatározásában explicite nem említi az egyén ellenőrzésének szempontját az őt érintő személyes adatai felett?**
E szempont explicit említése pedagógiai célból kedvező hatást váltana ki abban az esetben, amikor a 108. Egyezmény az Európa Tanácshoz nem csatlakozott, harmadik országok érdekeit szolgálja, amelyek nem ismerik a „magánélet" koncepciójának az emberi jogok európai Bíróságának esetjogában kifejezett fejlődését, ami az Európa Tanács intézményeiben és az Európai Unió keretében is megjelenik. Ez egyébként azért is fontos, mert az Egyezmény preambuluma rögzíti, hogy az Egyezményt aláíró államok elismerik, hogy „szükség van a magánélet tiszteletben tartásához és a népek közötti szabad információáramláshoz fűződő alapvető érdekek összeegyeztetésére". A magánélet tehát az egyetlen magas rendű érdek,

[6] Parliamentary Assembly, Resolution 1165 (1998), Right to privacy (a szerzők kiemelése).

[7] 7. cikk: „A magán- és a családi élet tiszteletben tartása Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát és kapcsolattartását tiszteletben tartsák."
8. cikk: „(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.
(2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.
(3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie."

amely igazolja az elképzelt védelmi rendszert. Következésképpen kulcsfontosságú, hogy ezt a felfogást az tárgyhoz igazodó „modern" és specifikus jelentőségében értelmezzük.
Ennek az ellenőrzésnek vagy ennek az információ feletti uralomnak az önmeghatározás jegyében való felidézése világosan igazolhatja, hogy az Egyezmény nem több, mint egy defenzív eszköz, amely garantálni kívánja az adatok bizalmas voltát vagy tiltani egyes különleges adatok kezelését, de amely felettébb pozitív megközelítése annak, amit az információs önrendelkezési jog kinyilatkoztatásának nevezhetnénk.

*1.1.2 Az adatok és az emberi méltóság védelme*

Az Egyezmény nem tesz említést az emberi méltóság védelméről. **Az emberi méltóság úgy idézhető fel, hogy az Embert mint alanyt[8] nem szabad a megfigyelés vagy az ellenőrzés egyszerű tárgyára redukálni.**
Az európai emberi jog Bíróság nem tétovázott a magánélet tiszteletben tartásával kapcsolatos indokolásában kifejezetten az ember méltóságára támaszkodni, s erre alapozva kijelenteni, hogy „az ember méltósága és szabadság az Egyezménynek, nevezetesen 8. cikkének is a lényegét képezi."[9] Az Európai Közösségek (ma már Európai Unió) Bírósága is vezérelvnek nyilvánította az egyén elidegeníthetetlen méltóságának értékét, melyet jogi védelemben kell részesíteni. Egy transzszekszuális által kezdeményezett ügyben kinyilvánította: „Egy ilyen diszkrimináció tűrése egy ilyen személy tekintetében a méltóság és a szabadság tiszteletben tartása félreértéséhez vezetne, melyhez e személynek joga van, s melyet a Bíróságnak védenie kell."[10]
A francia adatvédelmi törvény már első cikkében kinyilvánítja, hogy „Az informatikának minden egyes polgárt szolgálnia kel. (…) Nem sértheti sem az emberi azonosságot, sem az alapvető jogokat, sem a magánéletet, sem az egyéni vagy a közösségi szabadságokat."[11] Jól látható, hogy e megfogalmazásban az emberi méltóság tiszteletben tartása iránt táplált gondoskodás fejeződik ki, az a felfogás, hogy az ember nem vethető alá a gépnek, még ha annak őt is kell szolgálnia, s nem veszélyeztetheti az egyén alapvető értékeit.
Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról[12] biztosítja a jogot arra, hogy a személy ne legyen alávetve egy gép által hozott döntésnek. Ez a jog – az emberi méltóság jegyében – minden személynek biztosítja, hogy ne terjedhessen ki rá olyan egyedi döntés hatálya, amely kizárólag automatizált feldolgozáson alapul[13].
**Az érintettet védő kiegészítő garanciáknak szentelt fejezetben javasolni fogjuk, hogy ez jelenjen meg mint az emberi méltóság lényeges követelménye. Ugyanígy javasolható, hogy ez utóbbi fejeződjék ki az Egyezményben körülírt adatvédelmi szabályok alapvető értékeiben.**

[8] Vö. Kant ünnepélyes megállapítása az emberi méltóságról: „Őt (az embert) nem szabad mások céljait szolgáló eszköznek tekinteni, sőt még saját céljait szolgáló eszköznek sem, hanem mint egy önmagában vett célt, vagyis mint aki méltósággal rendelkezik, melynek révén igényt tart arra, hogy személyét mások tiszteletben tartsák, s amely lehetővé teszi számára, hogy mindegyikükkel összemérje magát, és az egyenlőség talaján állva felbecsülje önmagát." (Doctrine de la vertu, p. 96-97) citée par J. FIERENS, « La dignité humaine comme concept juridique », Journal des tribunaux, 2002, p. 78.
[9] Cour eur. DH, Christine Goodwin c. RU, arrêt du 11 juillet 2003, req. no 28957/95, par. 90.
[10] C.J.C.E., 30 avril 1996, (P. v. S. and Cornwall County Council), par. 21-22.
[11] Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, modifiée en 2004,article 1er.
[12] Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.
[13] 95/46 irányelv 15. cikk, lásd lentebb.

A méltóságnak mint az adatok, sőt a magánélet védelmének[14] alapvető értékeként való felidézése kétség kívül szükség a technika egyes alkalmazásai tekintetében. Az információs rendszerek egyre növekvő mértékben valósítják meg a népesség és az egyének globális megfigyelését, az egyének viselkedését átláthatóvá tevő rendszereket hoznak létre, melyek ez emberi méltósággal ellentétesnek mutatkozhatnak.[15] Ezen túlmenően a profilképzés megjelenése lehetőséget ad arra, hogy az érintettre vonatkozó információk kombinációját mindenféle döntéshez felhasználják, ami súlyosan sérti a profilírozott egyén méltóságát.
A méltóság veszélyeztetésével egyébként világosan és többször foglalkozik annak az Ajánlásnak a tervezete, amely az adatvédelmet a profilképzéssel összefüggésben tárgyalja[16]. Két megfontolás felettébb egyértelmű: „14. Tekintettel arra, hogy a profilok felhasználása, még ha törvényes is, elővigyázatosság és sajátos biztosítékok nélkül súlyosan sértheti az emberi méltóságot, valamint egyéb alapvető jogokat és szabadságokat, ide értve gazdasági és társadalmi jogokat is; 20. Tekintettel arra, hogy az emberi méltóság és más alapvető jogok és szabadságok a profilképzéssel összefüggésben akkor, és csak akkor érvényesülhetnek, ha az egyén tisztességes és törvényes profilírozása területén valamennyi szereplő együttműködik."

*1.1.3 Az adatvédelem más szabadságokat is támogat és szolgál*

Az, hogy a magánélet vagy még inkább az adatok védelme szabadságunk garanciája, magától értetődik. Ugyanígy, ha a véleménynyilvánítás vagy az egyesülés szabadságáról van szó, hogyan is képzelhető, hogy e jogok érvényesülhetnek, ha az egyén tudja, hogy kommunikációit megfigyelik, és olykor nem fejezheti ki magát anonim módon, ha a technika szisztematikusan nyomon követi üzeneteit? A tájékozódás szabadsága feltételezi, hogy az információ nem szűrhető, nem vezethet, különösen nem profilképzés céljából, az érintett tudta nélkül vagy ellenére, olyan információhoz, melyet mások szeretnének velünk elfogadtatni. Ennél is rosszabb, hogy a profilképzés e technikája arra indíthatja a profil képzőjét, hogy bizonyos szolgáltatásokat vagy információkat megtagadjon egy fogyasztótól, mert úgy véli, hogy kevésbé rentábilis számra, ha azokat a fogyasztó számára hozzáférhetővé teszi. E példák különféle, az emberi jogok európai Egyezményében szentesített szabadságok tekintetében megsokszorozódhatnak. Az adatok védelme vitathatatlanul számos egyéb szabadságot szolgál és garantál.
Mindazonáltal megtörténhet, hogy az adatok védelméről való gondoskodás sérti más szabadságok érvényesülését. Nevezetesen **az adatok védelmét egyensúlyba kell hozni a véleménynyilvánítás és kifejezés szabadságának feltétlen védelmével.**
Az Egyezmény preambuluma ezt implicite így idézi fel: „újra megerősítve ugyanakkor az információszabadság iránti elkötelezettségüket az országhatárokra tekintet nélkül; elismerve, hogy szükség van a magánélet tiszteletben tartásához és a népek közötti szabad információáramláshoz fűződő alapvető érdekek összeegyeztetésére", anélkül, hogy a 108. Egyezmény egyéb rendelkezése kifejezetten gondoskodna ennek az egyensúlynak a megteremtéséről. Az Egyezmény mindazonáltal törekszik ennek az egyensúlynak a létrehozására. Az adatvédelmi rendszer alól való kivételekre és annak korlátozására (amelyek nem érinthetik az adatbiztonsággal kapcsolatos kötelezettségeket) felhatalmazást adó 9. cikk előírja, hogy ettől csak akkor lehet eltérni, ha erről törvény rendelkezik, és az egy

[14] Erről lásd: J.H. REIMAN, "The Right to Privacy", in *Philosophical Dimensions of Privacy* 272, F.D. Schoeman ed., New York, 1984, 300 et ss.
[15] Vö. londoniak kamerás megfigyelése naponta 300 alkalommal; vagy kitűzőt viselő alkalmazottak, mely kitűző lehetővé teszi helyük meghatározását munkaidőben, s így következtetések levonását a munkához való hozzáállásukra vagy más, ugyancsak kitűzőt viselő munkatársakkal való kapcsolataikra nézve.
[16] Draft Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the T-PD at the 26th Plenary meeting, Strasbourg, 4 June 2010, disponible à l'adresse http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD%20documents/T-PDBUR_2009_02rev6_en_Fin%20_2.pdf

demokratikus társadalomban mások jogainak vagy szabadságjogainak védelme érdekében szükséges. A határátlépő adatáramlás rendszere (12. cikk és a kiegészítő Jegyzőkönyv) nem él a kivétel e lehetőségével. Mindazonáltal megengedi, hogy minden állam felhatalmazást adjon adatok rendszerint tiltott továbbítására, ha azt törvényes érdek felülmúlja. Könnyen elképzelhető továbbá, hogy a véleménynyilvánítás szabadsága az imént említett törvényes érdekek egyike. Még ha a kivételek rendszere minden kétséget kizáróan meg is engedi a véleménynyilvánítás szabadsága és az adatok védelme között jelentkező ellentmondás feloldását, talán nem szükségtelen kifejezetten felhívni az államokat arra, hogy összhangba hozzák e két, egymásnak ellentmondó érdeket. A 95/46 európai irányelv, jóllehet a 108. Egyezményhez hasonlóan lehetővé teszi a kivételeket, kifejezetten felhívja az államokat, rendelkezzenek a felmentésekről és kivételekről „a személyes adatoknak újságírás, vagy irodalmi, illetve művészi kifejezés céljából történő feldolgozása esetén", amennyiben azok „a magánélet tiszteletben tartásához való jognak a szólásszabadságra vonatkozó szabályokkal való összeegyeztetéséhez szükségesek"[17].

Az adatok védelmére alapozott, a véleménynyilvánítás és kifejezés szabadsága veszélyeztetésével kapcsolatos aggodalom mind a mai napig tükröződik az újságírói munka feltételeit védő egyes rendelkezésekben, különösen a mindig online világban. Mindazonáltal egyre inkább nélkülözhetetlennek látszik az adatvédelem és a véleménynyilvánítás szabadsága közötti egyensúly megteremtése. Ez a megfontolás különösen releváns az Internet világában, vitafórumai, blogjai és közösségi hálói tekintetében[18]. E médiumok használata manapság ténylegesen általánossá vált az önkifejezés, a közös cselekvés és a harmadik személyekkel való kapcsolatok terén. Mindez megvalósul az Internet, amely a kifejezés helye és eszköze mind a polgárok, mind azok tekintetében, akik azt „Web 2.0 a szabadidőre" névvel illetik[19]. A kommunikáció efféle körülményei között több szempontból lehetetlen tiszteletben tartani az adatvédelem szokásos rendszerét.

Az adatvédelmi törvények harmadik személyekkel szemben különféle követelményeket érvényesítő alkalmazása (tájékoztatási kötelezettség stb.) érzékeny problémát vet fel a véleménynyilvánítás és kifejezés szabadsága tekintetében, amely ekképpen korlátozottnak látszik.

Az európai Közösségek Bíróságának a Linqvist ügyben hozott döntése jól megvilágítja e tárgyat[20]. Szabad-e az Interneten személyes, közösségi vagy professzionális kapcsolatot létesíteni anélkül, hogy az a személyes adatok védelméről rendelkező törvényes követelményeknek megfelelne? A Bíróság szerint a körülmények figyelembe vételével mérlegelni kell a szabad véleménynyilvánítás joga gyakorlása korlátozásának arányos voltát mások jogai védelmére vonatkozó szabályok alkalmazásához képest. Ez a megfogalmazás homályos és az arányossággal kapcsolatos döntést igényel. Ez a döntés nehezen állítható az újságírói véleménnyel azonos alapra, azt akár hagyományosan, akár az Interneten értelmezzük, mely utóbbit e szabályoktól már megszabadították[21], továbbá mert a véleménynyilvánítás

[17] Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, 9. cikk.

[18] Lásd 29-es munkacsoport, WP 163, 5/2009. számú vélemény az internetes ismeretségi hálózatokról, 2009. június 12.

[19] Discours « l'Internet du futur: l'Europe doit jouer un rôle majeur» de Mme Reding, Commissaire européenne DG Société de l'Information et des Médias, à propos de l'Initiative «Futur de l'Internet» du Conseil Européen de Lisbonne (2 février 2009).

[20] C.J.C.E., 6 novembre 2003, (Lindqvist), C-101-01, *Rec*. p. I-12971, par. 43 et 44. Voy. la note d'observations de C. de Terwangne qui aborde amplement cette question : C. de TERWANGNE, « Arrêt Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 67 et s.

[21] Megjegyzendő, hogy a nemzeti jogszabályok változatosan rendelkeznek erről az egyensúlyról. (Vö. C. de Terwangne idézett cikke).

mindenkit megillető szabadsága szükségszerűen másokat is megillet. Ez utóbbiról időközben a CJCE ítéletet hozott, személyes adatok bármiféle, a „sajtónak" szánt nyilvános közzététele a kivételek rendszerébe tartozik[22].
A 108. Egyezmény elfogadását követően bekövetkezett technikai fejlődés egyúttal oda vezet, hogy **az adatvédelmi szabályok alkalmazása sérti a levéltitkot vagy a kommunikáció titkos voltát**. Ez az ellentmondás az elektronikus levelezés és más elektronikus cserék kapcsán jelentkezik. A levelezés ebben a formában az adatok automatizált kezelésévé alakul. Az átláthatóság követelménye, a hozzáférés joga és a helyesbítés joga akkor érvényesíthető, ha levelezést nem hagyományos módon, papíron folytatják (ami, az adatok strukturálása hiányában, még azon Felek adatvédelmi szabályaival érintett adatállományok körébe, amelyek az Egyezmény alkalmazását a nem automatizált állományokra is kiterjesztették). Következésképpen ezek a védelmi szabályok lehetővé teszik, hogy az elektronikus cserében megemlített harmadik személyek tudomást szerezzenek e csere tartalmáról, ami nyilvánvalóan sérti a levéltitkot vagy a kommunikáció titkos voltát. Az adatvédelem és a levéltitok vagy a kommunikáció titkos volta közötti ellentmondást a megfelelő kivételek rendszerében figyelembe kell vennie.
A forgalmi adatok felhasználása ugyancsak sérti a kommunikáció titkos voltát. Az ilyen felhasználást nagyon szigorú keretek közé kell foglalni[23].
Az adatvédelmi rendszer egyes szabályai ugyanakkor **sértik a tudományos kutatás szabadságát** is. A kutatás, főként az egészségügyi, olyan adatokat használ, amelyek – legtöbbször – úgy vannak kódolva, hogy nehéz, ha nem éppen lehetetlen azokat meghatározott természetes személlyel kapcsolatba hozni. A tudományos kutatók ezért szembesülnek a személyes adatok védelmére vonatkozó szabályok tiszteletben tartásának követelményével, mely szabályok gyakran számukra alkalmatlanok.
Gondoljunk tehát az érintett személyek különféle olyan jogaira, mint az adatokhoz való hozzáférés vagy azok helyesbítésének joga. A kutató vagy munkáltatója számára szinte lehetetlen választ adni a hozzáférésre irányuló igényre, hiszen nincs tudomása az adatokhoz kapcsolat fizikai személyről (csak kódolt adatokkal dolgozik, s nem ő, hanem egy harmadik személy ismeri a kód kulcsát). Ha a „személyes adatok" meghatározása kiterjedne az egyén minden olyan adatára, mellyel őt azonosíthatja valaki (például az adatokat felvevő orvos, de nem maga a kutató, aki csak kódolt adatokkal rendelkezik), ez a meghatározás és, *a contrario*, és az anonim adatokkal kapcsolatos felfogás, túl szigorúnak mutatkozhat, és a kutatás gátjává válhat. Ezt a felfogást ezért realista módon felül kell vizsgálni.

## 1.2 Hatály

### *1.2.1 A ratione personae kiterjesztése?*

Szükséges-e az egyén védelmén túlmenően védelmi szabályokat alkotni a profilképzésről[24]?
A profilképzés két szakaszban történik: először az egyén vagy az egyének alkotta közösség jellemzőinek azt körét határozzák meg, amely azok egy vagy több, tényleges vagy elvárt viselkedési módjával kapcsolatos, másodszor az egyén vagy a közösség ezt követő kezelése e jellemzők ismerete alapján.
A profilképzés jogi meghatározásának kérdése egy ajánlástervezet kidolgozásához vezetett, következésképpen e helyt nem tárgyaljuk.

[22] C.J.C.E. (gr. ch.), 16 décembre 2008, (Satakunnan Markkinapörssi Oy et Satamedia Oy), Affaire C-73/07, note C. de TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées », *R.D.T.I.*, 2010, n° 38, pp. 132-146.
[23] Lásd lentebb, 2.1.4 pont.
[24] Ilyen szabályozás létezik Svájcban és részben Norvégiában. Lásd L. BYGRAVE, *Data Protection Law*, Kluwer Law International, Information Law Series, Den Haag, 2002, pp.185 et s.

*1.2.2 Egy korlátozás*

**A 108. Egyezmény hatálya nem tartalmaz olyan korlátozást**, melyet az Európai Unió tagállamai valamennyi jogszabálya (a 95/46 irányelv rendelkezése alapján) tartalmaz. Az irányelv ugyanis nem alkalmazandó **„a természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett" személyesadat-feldolgozásokra**[25]. Az ilyen adatkezelés tehát ki van zárva az irányelvből és az azt átültető nemzeti jogszabályokból.
A kanadai törvény a személyes információk és elektronikus dokumentumok kezeléséről ugyancsak tartalmaz ilyen kivételt. 4. cikke 2. bek. (b) pontja szerint a védelmi rendszer nem alkalmazandó „arra az egyénre, aki személyes információkat gyűjt, használ fel vagy továbbít személyes vagy háztartási és bármely más célból".
Az APEC Adatvédelmi Kerete ugyanilyen típusú korlátozással határozta meg hatályát, éspedig a *személyes információ kezelője* meghatározásában körülírt kivétel alapján. Így e meghatározásból ki van zárva minden olyan egyén, „aki személyes, családi vagy háztartási ügyeivel kapcsolatos személyes információt gyűjt, tárol, feldolgoz vagy felhasznál"[26].
Egy ilyen kivétel érvényesítésének a fontosságát és nehézségeit az aktuális technikával, főleg a Web 2.0-val összefüggésben lentebb, a 7. részben taglaljuk.

# 2. Meghatározások

## 2.1 Aszemélyes adatok fogalma /2. cikk a) pont/

Az Egyezmény 2. cikk a) pontja szerint a személyes adatok körébe tartozik „bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik (adatalany)". Ez a meghatározás azóta klasszikussá vált, és az adatvédelmi jogeszközök többségében tükröződik. Mindazonáltal megjegyzendő, hogy az APEC ezt a megközelítést nem alkalmazza, s személyes adatoknak csak a (közvetve vagy közvetlenül) azonosító adatokat tekinti: „Az APEC Adatvédelmi kerete olyan személyes információkra vonatkozik, amelyek az egyén azonosítását lehetővé teszik. Felöleli továbbá azokat az információkat is, amelyek önmagukban e feltételnek nem tesznek eleget, de más információkkal együtt azonosíthatják az egyént."[27] Ez megközelítés nagyon korlátozott.

*2.1.1 Az azonosság: homályos fogalom a személyes adatok meghatározásában*

A személyes adatok fogalma az adatokkal érintett egyén azonosságán vagy „azonosíthatóságán" nyugszik. Az adatvédelem szabályai elvileg csak akkor alkalmazhatók, ha a kezelt adatok meghatározott személyre vonatkoznak. Mindazonáltal az azonosság fogalma kevésbé nyilvánvaló, amikor újabban alkalmazott technikákkal szembesülünk. Vajon az RFID címke, melyet egy öltözékre ragasztottak[28], személyes adatnak minősül-e, ha, legalábbis közvetlenül, egy tárgyra vonatkozik, éppúgy, mint az IP cím végső soron egy számítógépre és nem egy meghatározott felhasználóra vonatkozik?
Az azonosság fogalma homályos (vö. e jelentés első részében e tárgyban mondottak)

[25] 95/46 irányelv, 3.cikk (2) bek.
[26] APEC Privacy Framework (2004. november), Part II Scope, § 10. E rendelkezéshez fűzött kommentár ezt még jobban megvilágítja: „Az egyének gyakran gyűjtenek, tárolnak és használnak személyes információkat személyes, családi vagy háztartási célból. Gyakran feljegyzik noteszukba a címeket, telefonszámokat vagy készítenek családi hírleveleket. A Keret ezekre a személyes, családi vagy háztartási tevékenységekre nem alkalmazható." Forrás:
http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html
[27] APEC Privacy Framework, Part II Scope.
[28] Az RFID csipet először a Benetton ragasztott a termékeire.

Az azonosságot az iparban egyre felháborítóbb módon szűken igyekszenek értelmezni. Egy efféle értelmezés azzal az előnnyel jár, hogy kijátszhatják az adatvédelmi szabályokat, mivel kiüresítik a személyes adatok fogalmát.
Efféle szűk értelmezésre példa az Abacus[29] adatbank és a DoubleClick egyesítési szándéka. Az ember egyébként csak csodálkozik, hogy a DoubleClick „anonim[30]" profiljainak és az Abacus nevesített adatainak összekapcsolása technikailag lehetségesnek mutatkozott. Ez egészen egyszerűen azt jelenti, hogy a DubleClick, amely állítása szerint nem gyűjtött semmiféle, azonosítható személyre vonatkozó információt, mégis rendelkezett valamiféle, a kapcsolatot lehetővé tevő támponttal. Ez a nagyon is problematikus kapcsolat a hírhedt azonosító süti, melyet a DoubleClick személyi számítógépek millióiba ültetett be[31]. Elegendő egy láthatatlan hiperhivatkozást elhelyezni egy nevesített online űrlapra ahhoz, hogy a DoubleClick létrehozhassa ezt a kapcsolatot.
Az ipar jelenlegi törekvése[32] tehát, hogy a kapcsolati pontok és az egyszerű biográfiai adatok efféle társítását, mint egy nem meghatározható egyénre vonatkozó adatoknak tekintsék[33]. Az időben tartós kapcsolati pontokat általában személyes adatoknak ismerik el. Másfelől az egyénnek, vagy azoknak a javaknak, melyeket használ vagy birtokában tart megfigyelését és nyomon követését legtöbbször nem tekintik a magánélet megsértésének, ha a személy nem azonosítható vagy anonim marad (vagyis nem tudják a nevét vagy nem tudnak vele kapcsolatba lépni)[34]. Mintha viselkedésünk nem lenne azonosságunk önmagában konstitutív jellemzője.

### *2.1.2 Az „azonosíthatóság" jellemzői*

Említésre méltó az „azonosítható" jelző értelmezése, mely jelző egy természetes személyre vonatkozóan az „érintett személyt" jelenti. A 108. Egyezmény Indokolása szerint „azonosítható személy" az a személy, aki „könnyen" azonosítható, ami nem öleli fel a

---

[29] „egy együttműködésben résztvevők adatbankja, amely 1100 árukatalógust tartalmaz, s több mint 2 milliárd, gyakorlatilag valamennyi, árukatalógusból vásárló háztartás fogyasztói tranzakcióit", olvasható http://www.abacus-direct.com oldalon, 2004 májusában.

[30] http://www.doubleclick.net/company_info/about_doubleclick/privacy: *DoubleClick semmiféle, Önre vonatkozó, személyazonosításra alkalmas információt – nevet, címet, telefonszámot vagy e-mail címet – nem gyűjt.*

[31] A DoubleClick naponta több, mint egy milliárd bannerreklámot helyez el.

[32] A Microsoft Update-nek az információk bizalmas kezelésére vonatkozó nyilatkozata ugyanezt az utat követi. Miután kinyilvánítja, hogy a Web-hely a következő információkat gyűjti:

1. az alkalmazási rendszer verziószáma,
2. az Internet Explorer verziószáma,
3. azoknak a számítógépeknek verziószáma, melyekre a Windows Update a frissítéseket küldi,
4. a perifériák Plug and Play azonosítószáma,
5. a területi és nyelvi paraméter,

„adatvédelmi nyilatkozatában"
(http://v4.windowsupdate.microsoft.com/fr/default.asprögzíti: *„A Windows alkalmazási rendszer egy globálisan egyedi azonosítót (GUID, Globally Unique IDentifier) képez, melyet az Ön számítógépe tárol, hogy azt egyedi módon azonosítsa. A GUID nem tartalmaz semmi olyan információt, amely az Ön személyét azonosítja és az nem használható az Ön azonosítására."*

[33] Az első tanulmány a Safe Harbour (Biztonságos Kikötő) alkalmazásáról megvilágította, mi módon törekszenek az amerikai vállalkozások arra, hogy a személyes adatokat úgy értelmezzék, ami lehetővé teszi, hogy az adatkezelő az érintetteket azonosítsa. (J. DHONT, V.PEREZ, Y. POULLET with the assistance of J.REIDENBERG et L. BYGRAVE, Safe Harbour Decision Implementation Study, 19 April 2004, lásd http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm

[34] Lásd Privacy Policy of DoubleClick: arra a kérdésre, hogy „Hozzáférhetnek-e a felhasználók a Web-helyen róluk gyűjtött személyes információkhoz?", a Web-hely a következő választ adta: „Semmiféle személyazonosító információt nem gyűjtünk, tehát nincs mihez hozzáférni."

személyek „nagyon bonyolult módszerekkel” való azonosíthatóságát[35]. Ez az értelmezés nem kielégítő. A személy azonosítására használt módszerek bonyolultságának követelménye nem elegendően világos. Napjainkban a „nagyon bonyolult” módszerek technikai szempontból többé nem szükségszerűen esnek kívül az értelmezés hatályán.
A profilképzésről készített ajánlás már nem idézi fel az azonosítás módszere bonyolultságának követelményét, inkább azoknak a módszereknek a gazdagságát, amelyek alkalmazása az egyén azonosításához vezetnek. Eszerint „Az egyén nem tekinthető ’azonosíthatónak’, ha azonosítása ésszerűtlenül hosszú időt vagy munkaráfordítást igényel”[36].
**Törekedni kell egy megfelelő követelmény, egy olyan helyes gyakorlat meghatározására, mert ez a követelmény a személyes, és ellentéteként az anonim, adat fogalmának a kulcsa.** Ha például az a személy, aki egy adatalany azonosságát ismeri, egy titkosszolgálat foglalkoztatottja, s büntető szankció terhe mellett azt nem közölheti, tekinthető-e az adat azonosíthatónak? Valójában nem. Ám ugyanez-e a helyzet, ha a titoktartás szerződéses kötelezettség, megszegése büntetőjogilag nem szankcionálható.
A személyes adat fogalma igenis megérdemli, hogy határozottan tartalmazza azokat a formákat, amelyeket a technikai fejlődés következtében alkalmaznak. Nevezetesen tekintetbe kell venni az Internet-szolgáltatásokat nyújtó vállalkozások gyakorlatát.
E megfontolások keretében megjegyzendő, hogy egy olyan adat, mint a süti, az IP cím vagy a Globálisan Egyedi Azonosító (Global Unique Identifier) mint „személyes adat”[37] maga után vonja az Egyezmény rendelkezéseinek alkalmazását, s ettől fogva az érintett személyes azonossága felkutatásához vezethet, nem lenne más, mint a hozzáférés joga gyakorlásának megengedése, még ha erre az adatkezelő tevékenységéhez nincs is szükség. Másfelől e rendelkezéseknek mint az érintett tájékoztatása kötelezettségeként való alkalmazása azonosító hiányában lehetetlennek mutatkozhat.
Ezzel szemben problémát vethet fel, ha az IP címet és a GUI-t nem személyes adatként kezelik, mert kockázatot jelenthet ezeknek az adatoknak későbbi felhasználása az egyén profilja megalkotása, mi több, a vele való kapcsolat lehetősége vonatkozásában. E tekintetben megállapítható, hogy a világháló forgalma megfigyelésére szolgáló eszközök kombinálásával könnyedén körülírhatjuk egy gép és mögöttes felhasználója viselkedését. Így rekonstruálhatják az egyén személyiségét, hogy arra alapozva bizonyos, az egyénre szabott döntéseket alkalmazzanak. Anélkül, hogy ismernék az egyén „azonosságát”, vagyis nevét és címét, őt társadalmi-gazdasági, pszichológiai, filozófiai és más tulajdonságaival jellemezhetik, s rá nézve bizonyos döntéseket oly módon alkalmazzanak, hogy az egyén (vagy számítógépe) kapcsolati adatai már nem teszik szükségessé szoros értelemben vett azonosságának megállapítását. Másképp fogalmazva: az egyént érintő cselekvéshez már nincs szükség azonossága megismerésére.
Ezen túlmenően az új technikai környezetben az individualizálás előnyt élvez az azonosítással szemben. Kell-e azért tökéletesíteni a személyes adat meghatározását vagy mellé csatolni egy olyan meghatározást, amely már nem tartalmazza a személlyel kapcsolatos adatok közül azokat, melyekkel a személy azonosítható, hanem csak azokat, melyekkel individualizálható.
Érdekes megemlíteni hogy, még ha a személyes adatokat hasonlóan is határozza meg, az OECD Iránymutatáshoz csatolt Indokolása e felfogást olyan megvilágításba helyezi, ami

[35] Indokolás, 28. pont.
[36] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Appendix, 1. Definitions, a.
[37] A 29-es munkacsoport több alkalommal megismételte, hogy az IP címet önmagában személyes adatnak kell tekinteni (WP 136; WP 148; WP 150, Vélemény 2/2008 a magánélet védelméről és az elektronikus hírközlésről szóló 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) felülvizsgálatáról, 2008. május 15.

mellőzi az érintett személy azonosíthatóságát. Eszerint „Elvileg a személyes adatok olyan információt közvetítenek, amely közvetlenül egy *adott természetes személyhez* (a szerzők kiemelése) kapcsolható (például az anyakönyvi bejegyzés száma)".
A 2002/58 elektronikus hírközlési adatvédelmi irányelv meghatározza a forgalmi és a helymeghatározó adatok fogalmát (lásd alább), amely egyik esetben sem utal egy azonosított vagy azonosítható egyénre. E meghatározások alkalmazása azt jelenti, hogy elegendő egy végberendezéssel, vagy eszközzel létesített kapcsolat, mely által egy, e végberendezést birtokló személy, még ha nem is azonosított, veszélyeztetetté vagy jellemezhetővé válik, hiszen a 2002/58 irányelv hatálya rá is kiterjed[38].

*2.1.3 Biológiai és biometrikai adatok*

Az európai emberi jogi Bíróság megállapította, hogy az ujjlenyomat, a DNS profil és a sejtminta „az Európa Tanács 108. Egyezménye értelmében mind személyes adat"[39]. Ez az álláspont nem nyilvánvaló. Egy kis vér vagy kevéske nyál tehát személyes adat? Még is az elképzelhető, hogy egy sejtminta adatot tartalmaz, anélkül, hogy maga az lenne.
**Helyénvaló lenne tisztázni a személyes adat fogalmát a biológiai és biometrikai adatok tekintetében.**

*2.1.4 A forgalmi és a helymeghatározó adatok: egy sajátos rendszer?*

**Felfoghatjuk-e úgy a forgalmi és helymeghatározó adatokat mint olyan személyes adatokat, ami új, sajátos szabályozást igényel, s ezáltal a 2. cikkben felsorolt meghatározások közé iktatandó?**
A 2002/58 elektronikus hírközlési adatvédelmi irányelv ezeket az adatokat a következőképpen határozza meg[40]:

- „forgalmi adat: egy közlésnek az elektronikus hírközlő hálózaton keresztül történő továbbítása vagy erre vonatkozó számlázás céljából kezelt minden adat";
- „helymeghatározó adat: egy nyilvánosan elérhető elektronikus hírközlési szolgáltatás felhasználója végberendezésének földrajzi helyzetét jelző, az elektronikus hírközlő hálózatban vagy elektronikus hírközlési szolgáltatás keretében kezelt minden adat".

A helymeghatározó és a forgalmi adat sajátos meghatározását az ilyen adatok szisztematikus kezelésével járó veszélyek indokolják, hiszen azok felfedik a helyváltoztatást, a szokásos környezetet, a fogyasztási és az életviteli szokásokat[41]. Ezen felül az elektronikus szolgáltatások igénybe vevője, az értéknövelt szolgáltatások kivételével, viszonylag gyenge helyzetben van, hiszen a hálózat használata implicite feltételezi számos olyan technikai adat létrehozását, tárolását és továbbítását, melyek jelentése és potenciális felhasználása elkerüli figyelmét, s melyeknek útja egykönnyen nem követhető (a hálózatok működése a felhasználó számára nem átlátható).

[38] Lásd Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law, Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, p. 51.
[39] Cour eur. D.H. (Gr. Ch.), *S. et Marper c. Royaume-Uni*, arrêt du 8 décembre 2008, req. n° 30562/04 et 30566/04, par. 68.
[40] Az Európa Tanács R(99) 5. ajánlása a magánélet védelméről az Interneten ilyen típusú adatoknak sem a meghatározását, sem azokra vonatkozó különös rendelkezést nem tartalmaz.
[41] Ugyanebben a felfogásban lásd: A 29. munkacsoport véleménye 5/2005 a helymeghatározó adatok értéknövelt szolgáltatás nyújtására történő felhasználásáról, WP 115, 2005. november 25., 3. oldal: „Mivel az ilyen adatok kezelése – főként a szabad és névtelen közlekedés szempontjából – különösen kényes kérdés, az európai törvényhozás […] külön szabályokat fogadott el, amelyek szerint az értéknövelt szolgáltatáshoz szükséges helymeghatározó adatok kezelése előtt meg kell szerezni a felhasználók vagy előfizetők hozzájárulását, és a felhasználókat vagy előfizetőket tájékoztatni kell az ilyen kezelés feltételeiről".

A földrajzi helymeghatározással kapcsolatos kockázatokat az OECD a következő példával világítja meg: *„Egy mobil szolgáltató egy GPS (Globális Helymeghatározó Rendszer) rendszert vagy egy (a végberendezés által kiadott jeleknél kezdődő) háromszögelési rendszert használ fel a mobil felhasználó lokalizálására. A vállalkozás az előfizetőt érintő adatokat és lokalizációját eladja marketing vállalkozásoknak, hogy azok a mobil elfizetőnek hirdetéseket vagy személyre szabott üzeneteket küldhessenek. A mobil előfizető fel sem fogja, hogy ebben a rendszerben személyes adatait másoknak továbbítják, és hogy erre vonatkozó hozzájárulását nem adta meg. Megtörténhet, hogy a számára küldött információt számba veszik (például a közelben javasolt vásárlásokat illető SMS küldeményeket, vagy az Internetre kapcsolódás időpontját 'pop-up' üzenetek megjelenítése céljából). A felhasználót zavarja az a tény, hogy megtudhatják, hol tartózkodik, és nyugtalanítja, hogy az információt [rossz szándékú személyek] elfoghatják (ellophatják vagy eladhatják*[42]*"*.

Az egyén lokalizálása ugyanígy lehetséges nyomainak követésével, amelyeket például a hitelkártyája használatával vagy a tömegközlekedésben elektronikus jegyének érvényesítésével hagy. Ezeket a nyomokat mindazonáltal nem tekintjük a fentebb körülírt helymeghatározó adatoknak.

Ezzel szemben nagyon is helymeghatározó adatok azok, melyeket arra használnak fel, hogy feliratkozott személyeket felkutató szolgáltatásokat ajánljanak fel, (baráti csoportok vagy ismeretlenek, akik földrajzi közelségükben tartózkodó személyekkel szeretnének találkozni), s melyek – a *Find a friend* típusúak – sokasodnak, szükségessé téve a feliratkozott személyek folyamatos lokalizációját.

A helymeghatározó adatok tétjére való tekintettel, a 2002/58 irányelv *a priori* korlátozza az ilyen adatok kezelését, kivéve ha ahhoz a kellőképpen tájékozott érintett személy hozzájárul, mely hozzájárulását bármikor vissza is vonhatja.

Az OECD szerint helyes lenne, hogy a szolgáltatók „a gyűjtött helymeghatározó információkról világos tájékoztatást adjanak a fogyasztóknak, ide értve azok felhasználásának célját", valamint hogy „a fogyasztóknak lehetőséget adjanak arra, hogy az adatcserét harmadik személyekkel (szükséghelyzet kivételével) korlátozzák, és visszavonják azokra vonatkozó döntésüket, akikkel ezek az adatok cserélhetők"[43].

Az Egyesült Államokban a szolgáltatónak azt a lehetőségét, hogy az előfizető helymeghatározó adatait harmadik személyek részére továbbítsa, jogszabályok korlátozzák az ügyfelekre vonatkozó hálózati adatok felhasználását (Customer Proprietary Network Information, CPNI). Ezzel megegyezően a szövetségi hírközlési törvény 222. cikke megtiltja a vezeték nélküli végberendezések lokalizációs adatainak a továbbítását vagy felhasználását, mely adatokat a szolgáltató a távközlési szolgáltatás nyújtása során gyűjt az előfizető előzetes kifejezett hozzájárulása nélkül. Az előfizető hozzájárulásától csak kivételes szükséghelyzetben lehet eltekinteni (abból a célból, hogy előfizető sürgősségi hívására válaszolni lehessen). Ezen kívül a CAN SPAM törvény (Controlling the Assault of Non-Sollicited Pornography and Marketing) a címzett előzetes kifejezett felhatalmazása hiányában megtiltja a mobil szolgáltatónak, hogy kereskedelmi célú üzenetet küldjön az Interneten közvetlenül a vezeték nélküli végberendezésekre.[44]

### 2.2 Az adatállomány /2. cikk b)/ és a gépi feldolgozás /2. cikk c)/ fogalma

**A feldolgozás e meghatározása nem tartalmazza az adatok gyűjtését.** Ezt az alapvető műveletet a feldolgozás meghatározásából az Indokolás kifejezetten kizárja. Márpedig erre a

[42] OECD „Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce". OECD Miniszteri Értekezlet, Future of the Internet Economy, Seoul, 2008. június 20., oldal.
[43] Ugyanott, 20. oldal.
[44] Ugyanott, 23. oldal.

műveletre választ kell adnia a védelmi rendszerben részletezett követelményekre. Az 5. cikk ténylegesen előírja, hogy az adatok megszerzésének tisztességesnek kell lennie, például midőn információt gyűjtenek a Weben szörfölve vagy az Internet protokolljai révén, legalábbis a számítógép memóriájába. Minthogy az adatok rögzítése önmagában is feldolgozást jelent, megállapítható, hogy a gyűjtés tényével feldolgozás valósul meg.
Következésképpen: tekinthetjük-e ezt a szándékos kihagyást hiányosságnak?
Megjegyezzük, hogy az Európai Emberi Jogi Bíróság az adatok gyűjtését tárolásuktól megkülönböztetve kifejezetten beleveszi a magánélettel kapcsolatos műveletek körébe. Határozatában Antunes Rocha kiemeli, hogy az egyén „magánéletével kapcsolatos adatok gyűjtése, tárolása és az esetleges kommunikációja" az Egyezmény 8. cikk 1. bekezdésének alkalmazási körébe tartozik (Leander c. Suède, arrêt du 26 mars 1987, série A no 116, p. 22, § 48 ; Rotaru c. Roumanie [GC], no 28341/95, § 43, CEDH 2000-V). Még a publikus adatoknak is lehet magánéleti vonatkozásuk, ha azokat rendszeresen gyűjtik és tárolják közjogi szervek adatállományaiban (lásd Rotaru ügy), és „a 8. cikk értelmében beavatkozás az érintett magánéletébe, ha a hatóságok rá vonatkozó információt gyűjtenek, függetlenül attól, hogy ez a gyűjtés milyen formát ölt."[45]
**Szükséges-e újabb műveletekkel kiegészíteni** a gépi feldolgozás meghatározását? Esetleg az adatok továbbításával vagy összekapcsolásával?

### 2.3 Az adatállomány kezelője /2. cikk d)/

Az 108. Egyezmény 2. cikk d) pontja szerint az adatállomány kezelője: *„az a természetes vagy jogi személy, hatóság, hivatal vagy bármely más szervezet, amely a nemzeti jog szerint illetékes arra, hogy meghatározza az automatizált adatállomány célját, a tárolható személyes adatok fajtáját és az adatokkal végezhető műveleteket."*
Az „adatállomány kezelőjének" a 108. Egyezmény – indokolása szerint – *„kizárólag az adatállományért végső soron felelős személyt vagy szervet tekinti, és nem azokat a személyeket, akik a kezelési műveleteket végzik az adatkezelő rendelkezéseinek megfelelően"*[46].
Az „adatállomány kezelőjének" e meghatározását felül kell vizsgálni.
A meghatározásból kiviláglik, hogy a 108. Egyezmény az adatállomány kezelőjét úgy tekintette, mint akinek több szinten kell döntést hoznia: egyrészt meghatározza a létrehozandó adatállomány célját, másrészt az állományba kerülő adatokat a velük végezhető műveletekkel együtt. A hangsúly tehát e szereplő végső feladataira került.
Mindazonáltal úgy látszik, hogy ez a felfogás ma már nem illeszkedik az aktuális környezethez. Valóban érdekes hangsúlyozni, hogy napjainkban az adatállomány kezelőjének szerepe nem csupán egyetlen adatállományhoz kapcsolódik, hanem olyan kezelések együtteséhez, melyek központi elemévé vált. Ebben az összefüggésben indokolt az adatállomány-kezelő felfogását elmozdítani az adatfelelős irányába. Ezt hangsúlyozza a 29-es adatvédelmi Munkacsoport is: az adatállományokra alapozott felfogást el kell mozdítani a kezelés irányába, ami megengedi, hogy *„egy adatállományhoz kapcsolt statikus meghatározásról a feldolgozási tevékenységhez kapcsolt dinamikus meghatározásra térjünk át"*[47].
Ezzel a módosítással, ugyancsak lehetővé egyenlő módon integrálni és hatékonyabban kifejezni azt az elvet, mely szerint ez a szereplő felelős lenne a kezelést alkotó valamennyi láncszeméért, ami nagyobb védelmet nyújtana az érintettnek. Következésképpen az érintett lenne az egyetlen és kizárólagos szereplő, aki a teljes folyamat felett, az adatok gyűjtésétől azok megsemmisítéséig, ide értve anonimizálásukat is, ellenőrzést gyakorolhatna.

[45] Cour eur. D.H., *Antunes Rocha c. Portugal*, arrêt du 31 mai 2005, Req. no 64330/01, par. 65.
[46] A 108. Egyezmény indokolása, 32. pont.
[47] 29-es munkacsoport, 1/2010. számú vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról, 15. oldal.

Másfelől a gyakorlat jelzi, hogy az adatkezelő egyes helyzetekben két-, sőt háromfejű, mely helyzetet a 108. Egyezmény jelenlegi állapotában nem kezeli. Gondoljunk például a *cloud computing* vagy az *e-Health* platform esetére. Hasznos lenne talán tekintetbe venni egy vagy több személy közös munkájának az esetét, mint ahogyan azt a 95/46 irányelv teszi, még ha ez elkerülhetetlenül is felveti az alkalmazandó jog kérdését (lásd lentebb).

Helyénvaló ezután **tisztázni az Egyezmény aktuális szövegében rögzített kritériumot**: „az adatállomány kezelője illetékes arra, hogy meghatározza az automatizált adatállomány célját, a tárolható személyes adatok fajtáját és az adatokkal végezhető műveleteket" /2. cikk d)/. Ez a tisztázás az Egyezmény Indokolásában jelzett szellemben végezhető el, miszerint az adatállomány kezelőjének az Egyezmény „csupán azt a személyt vagy szervezetet tekinti, amely végső soron felelős az adatállományért, s nem azokat a személyeket, akik az adatállomány kezelője által meghatározott műveleteket hajtják végre"[48]. Az „adatállományért végső soron felelős" kritériuma bizonyosan helyes kritérium, mert összefüggésbe hozza azt, ami a gyakorlatban megjelent, s amit látni szeretnénk a felelős kezelő személyében, aki az adatok kezelése felett a tényleges ellenőrzést gyakorolja, akinek tényleges hatásköre van a kezelésre vonatkozó döntés meghozására.

Ez a tisztázás lehetővé tenné választ adni arra a kritikára, amely, a 95/46 irányelv keretében, a két kritérium koegzisztenciájával kapcsolatban jelentkezett. A felelős kezelő meghatározásának többféle kritériuma magától értetődően több felelős személy azonosításához vezethet, és ugyanígy több, egymással konkuráló nemzeti jog alkalmazásának problémájához is, ha az alkalmazandó jog kritériuma nem kapcsolódik a felelős kezelőhöz és annak telephelyéhez (mint a 95/46 irányelv esetében)[49]. Az Egyezmény 1981-ben hatályos változatában pedig hármas kritériumot találunk, amely az adatállomány felelősségi kérdéseit tükrözi: kérdéses, ki kompetens döntést hozni az automatizált adatállomány céljáról, az adatok fajtájáról és az adatokkal végezhető műveletekről.

Másodszor feltehetjük azt a kérdést, **milyen érdek fűződik egyéb olyan felfogások integrálása az Egyezménybe, amelyek megfelelnek mind a hagyományos, mind az újabban megjelent, a tárgyban szerepet játszó szereplőknek.**

Ezek a szereplők mindenekelőtt **adatfeldolgozók**, mely, széles értelemben, azokat a személyeket jelöli, akik az adatállomány kezelője/felelőse utasításai szerint dolgoznak, végrehajtva azokat a feladatokat, melyeket a kezelő/felelős nem maga végez. Az adatfeldolgozó tehát az adatállomány kezelőjétől különböző személy, aki az adatkezelés ráruházott (általában technikai) műveleteit végrehajtja. Az adatfeldolgozó döntő szerepet játszik nevezetesen a *cloud computing* környezetben.

Ahol egyáltalán létezik, ennek a felfogásnak az alkalmazása nem jár nehézséggel. Nem mindig különböztethető meg ugyanis nyilvánvalóan az adatállomány kezelője/felelőse és az adatfeldolgozó. Különösen ez a helyzet akkor, ha egy komplex szervezetről, például egy multinacionális vállalkozásról vagy egy vállalkozás-csoportról van szó.

Az újonnan piacra lépők között[50] találunk **hálózati operátorokat**, ide értve az Internet-hozzáférést szolgáltatókat is. Ők azok a kötelező, a hálózatot használók mint érintett személyek és az Internet számos szereplői közötti interfészek, amelyek a hálózat használata során a felhasználó tudtával vagy anélkül generált adatokat kezelhetik. Rájuk ruházhatók

[48] Indokolás, 32. pont.

[49] Ebben az értelemben fogalmaz meg kritikát D. KORFF, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010, pp. 60 et s.

[50] Lásd Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law, Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, p. 54.

olyan feladatok is, mint a hálózat használatával kapcsolatos veszélyek elhárítása, a szolgáltatások biztonságának garantálása, a hívó vonala azonosításának korlátozása, stb.
A **technikai** (nevezetesen böngészésre szolgáló) **informatikai eszközök szállítói** az új szintérnek ugyancsak részévé váltak. Megfontolás tárgyát képezheti, hogy őket is kötelezzék technikai szabványok alkalmazására, melyért felelősséget is kell viselniük (lásd alább a magánélet védelme követelményeit már a tervezés szakaszában figyelembe vevő Privacy by Design című részben).

# 3. A védelem alapelvei

### 3.1 5. cikk: az adatok minősége, a cím nem megfelő volta

Az Egyezmény „Az adatok minősége" című 5. cikke rendelkezik a védelem kulcsfontosságú alapelveiről. E cikk címe azonban határozottan félrevezető. E rendelkezés tartalma valójában túlnyúlik az adatok szorosan értelmezett minőségén. Csupán a c) és a d) pont rögzít minőségi követelményeket (az adatoknak tárolásuk céljával arányban kell állniuk, és meg kell felelniük e célnak, azon nem terjeszkedhetnek túl; pontosaknak és időszerűeknek kell lenniük). Megszerzésük tisztességes és törvényes követelménye /a) pont/, továbbá a célhoz kötöttség elve (a célnak megfelelő felhasználás és a tárolás időbeli korlátozásának a követelménye) /b) és e) pont/ nem tekinthető minőségi követelménynek. Az Egyezmény Indokolása világosan kifejezi, hogy „E cikk különböző rendelkezései két fő szabályt rögzítenek. Egyrészt az adatoknak pontosnak, a célhoz illeszkedőnek kell lenniük, a célon nem terjeszkedhetnek túl. Másrészt felhasználásuknak is szabályszerűnek kell lennie."[51]
Annak a feltevésnek megfelelően, hogy az Egyezménynek a nemzetközi adatvédelmi rendszer modelljéül kell szolgálnia, elengedhetetlen, hogy szövegezése világos és szabatos legyen, nem megfeledkezve szöveg nevelői küldetéséről sem.
Az OECD-nek a magánélet védelmét és a személyes adatok határátlépő áramlását szabályozó Iránymutatása az adatminőség elve mellett a célhoz kötöttség és a korlátozott felhasználást elvét is tartalmazza. Az ENSZ Iránymutatás a számítógépi személyesadat-állományok szabályozásáról[52] megkülönbözteti a törvényesség és a tisztességesség elvét, a pontosság és a célhoz kötöttség elvét.

### 3.2 Az arányosság elve

**Az Egyezmény az arányosság elvének kifejezett meghatározását nem tartalmazza**, holott ez az az elv, mely szerint az adatkezelést kiváltó személy érdekeinek sérelme nem lehet aránytalan az adatkezelésért felelős érdekéhez képest. Ez az elv csupán abban fejeződik ki, hogy az adatok céljukon „nem terjeszkedhetnek túl", vagyis az adatok, még ha helyesek is, nem kezelhetők, mert ez felettébb sértheti az érintett érdekeit, még ha az a kezelésért felelős érdekét is képezi. Ugyanígy az a követelmény, mely az adatok gyűjtését a kizárólag helyes és megfelelő adatokra korlátozza, az arányosság elvének konkretizálódása abban az értelemben, hogy e követelmény szerint törekedni kell arra, hogy a sérelem a szigorúan szükséges mértéket ne haladja meg. A CEPD egyik véleményében ezt a felfogást fejezte ki, hangsúlyozva az érintett személy alapvető jogai és a különféle szereplők érdekei közötti egyensúly megőrzésének fontosságát, ami feltételezi a kezelt személyes adatok mennyiségének a lehető legnagyobb mértékű korlátozását.

[51] Indokolás, 40. pont.
[52] Guidelines for the Regulation of Computerized Personal Data Files (14 Dec. 1990).

Ez a felfogás értékeli, hogy **az Egyezmény 5. cikk b) pontjában rögzített célhoz kötöttség „legitim" követelménye összhangban van az arányosság követelményével.** Egy legitim cél nem okozhat nagyobb mértékű sérelmet, mint amit a kezelés érdeke jelent.
A kanadai törvény a személyes információ védelméről és az elektronikus dokumentumokról érdekes megfogalmazást tartalmaz az elfogadható kezelés célhoz kötöttségéről. Amint azt az 5. (3) pontjában előírja, „egy szervezet csak abból a célból gyűjthet, használhat vagy közölhet személyes információt, melyet egy értelmes személy a körülményekre való tekintettel elfogadhatónak tart". A törvény ily módon a létező érdekek egyensúlyának megteremtését igényli, méghozzá egy absztrakt egyén és nem egy adott helyzetben érintett egyén szintjén. Világos tehát, hogy az elfogadható cél mérlegeléséhez az értelmes személy a kezelés mellett és ellen szóló érveket veszi fontolóra, vagyis azokat hatásokat, melyeket helyzetére és érdekeire a kezelés gyakorolhat. Megemlítendő azonban, hogy, a kanadai példával ellentétben, az érdekek egyensúlyát mint az arányosság igazolásának fő szempontját, nem szabad magánéleti szempontra korlátozni, hanem ugyanígy tekintettel kell lenni egy magasabb rendű szempontnak is, amely a társadalom egészének érdekeit is felöleli.
**Kétség kívül indokolt és mindenesetre pedagógiailag is célszerű lenne az Egyezmény szövegében világosan megjeleníteni az arányosság elvének követelményét**. Napjainkban ugyanis kulcsfontosságúvá vált ennek a kötelezettségnek a rögzítése, ami gátat szabhat bizonyos, a technika fejlődéséből (nevezetesen az Interneten megvalósuló nem sejtett kezelésből) adódó kockázatoknak és az érintettnek az adatai kezeléséhez való hozzájárulása igen elterjedt (visszaélésszerű) mellőzésének. Ha egy hozzájárulás megléte egy kezelés törvényes voltát igazolhatja, úgy a létező érdekek és a megvalósított egyensúly örömmel üdvözölt biztosítékot nyújt, amikor a hozzájárulás gyakorta vélelmen alapul (az érintett nem kielégítő tájékoztatása, a hozzájárulásnak a feltételek módosítása elmaradására alapozott vélelmezése, stb.).
**Ezt a követelményt nem lenne szabad a kezelés céljára korlátozni, hanem el kellene rendelni az adatokon végzett valamennyi műveletre nézve.**
Genetikai adatok és digitális ujjlenyomatok esetében az európai emberi jogi bíróság leszögezte, hogy „az egyensúly megteremtése előnyeire nézve egyrészt e technikák széleskörű alkalmazását, másrészt a magánélet védelméhez fűződő lényeges érdekek érvényesítését eredményezheti"[53].
Az Európai Unió Bírósága már az első e tárgyban hozott ítéletében megállapította, hogy az emberi jogok európai Egyezménye 8. cikke a 96/46 irányelv sorai közül kiolvasható, amiből igazolható, hogy egy adatkezelés tekintetében e cikk 2. bekezdésében rögzített arányosság elvét tiszteletben tartja[54].

### 3.3 A hozzájárulás mint a kezelés törvényes alapja

**A 108. Egyezmény nem ad hivatalos helyt az érintett hozzájárulásának**. Ellentétben az Unió alapjogi chartája 8. cikkével és a 95/46 irányelvvel a hozzájárulást mint az adatkezelés törvényes alapját az Egyezmény nem szentesíti.

[53] Cour eur. DH (Gr. Ch.), *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. nos 30562/04 et 30566/04, § 112.
[54] Az EU Bíróságának a C-465/00., C-38/01. és C-139/01. sz. egyesített ügyekben hozott 2003. május 20-i ítélete (Österreichischer Rundfunk és társai): „Így a 95/46 irányelv [ ] alkalmazása érdekében azt kell megvizsgálni először, hogy egy olyan szabályozás, mint amilyen az alapügyekben szerepel, előírja-e a magánéletbe való beavatkozást, és adott esetben ez a beavatkozás igazolt-e az EJEE 8. cikke tekintetében." (72. pont); a Bíróság rámutat, hogy meg kell vizsgálni, a szóban forgó osztrák rendelkezés ilyen értelmezése megfelel-e az EJEE 8. cikkének: az elérni kívánt célokkal arányos-e. (80. pont). Ebben az értelemben mérlegelni kell az Osztrák Köztársaságnak a közalapok legkedvezőbb felhasználásának biztosításához [ ] fűződő érdekét, valamint az érintett személyek magánéletének tiszteletben tartását érintő veszély súlyosságát. (84. pont).

Kell ezt, ahogyan a kritikák teszik, hiányosságnak tekintetni a hozzájárulással kapcsolatos állandó panaszok tükrében, mely hozzájárulás bizonyos olyan kezelések törvényessége alapját képezi, melyeket a Web 2.0 és más szolgáltatásokat igénybevevő érintett személy tevékenysége vált ki[55]?
A hozzájárulás formája és feltételei ugyancsak nagy aggodalom forrásai, mint olyan helyzetekben, amikor egy Internet oldalon az adatok szolgáltató által javasolt felhasználásának feltételeit a szolgáltatás igénybe vevője nem ellenzi, mert számára „alantas", mert a „rákattintás", amire rákattinthatna, elmarad, a vélelmezett paramétereket nem módosítja. Mindezeket a hozzájárulás megfelelőjének tekintik.
A hálózatok átláthatatlansága, az a tény, hogy számos adatkezelés elkerüli az érintett figyelmét, és az a tény, hogy sokan nem teszik meg a kellő intézkedéseket a kezeléssel való érintettség elkerülése érdekében, aggályossá teszi ezt a vélelmezett hozzájárulást.
Minthogy a modern hálózatok interaktívak, a hozzájárulást egyszerűen mint a törvényesség alapvető kellékét kérhetjük számon, s egyúttal előnyben is részesíthetjük egyéb hagyományos alapvető kellékekkel, például az érdekek egyensúlyának megteremtésével szemben.
Ez a megfontolás egyeseket arra indít, hogy ezért a hozzájárulás elegendő lehet a kezelés legitimizálására. E tekintetben emlékeztetünk arra, hogy a World Wide Web Consortium (W3C) által kifejlesztett Platform for Privacy Preferencies (P3P, Személyes Adatvédelmi Beállítások Platformja)[56] ugyancsak azon a lehetőségen alapszik, hogy az Internet használó tárgyalhasson azzal a szolgáltatóval, aki nem teljesíti adatvédelmi beállításait, és ily módon megegyezésre jussanak, ami már az adott kezelés legitim alapját képezi. Jóllehet ezzel a tárgyalási lehetőséggel még mindig nem sokan éltek, legalábbis elektronikus úton, a P3P az ipar arra irányuló hajlandóságát igazolja, hogy módot ad a tárgyalásra az adatai felhasználásával érintett személynek. A magánélet védelme ily módon bizonyos mértékben alku tárgyát képezheti[57].
Márpedig a magánélet védelme nem egyszerűen magánügy, hanem igényt tart a társadalmi rendet érintő meggondolásokra, és megköveteli a közhatalmi szervek beavatkozásának lehetőségét és marginális ellenőrzését[58].

### 3.4 Az „inkompatitilis" kezelések

Az adatokon végzett műveletek „kompatibilitásának" elve megköveteli, hogy az adatok bármiféle felhasználása kompatibilis legyen az adatok felvételének céljával. A kompatibilitás követelménye megítélésekor azt kell megvizsgálni, hogy az adatokkal végzett műveletek nem sértik-e az érintett méltányos elvárásait.
Az APEC adatvédelmi kerete a felhasználás kompatibilitását a következőképpen fogalmazza meg: „Azt, hogy a cél kompatibilis-e a megjelölt vagy azzal összefüggő célokkal, aszerint az alapvető kritérium szerint kell eldönteni, hogy az adatok extenzív használata e céloknak

[55] Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, §§ 65-68.
[56] A 29-es munkacsoport ezzel kapcsolatos véleménye: Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), letölthető: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/1998_en.htm, e protokollról lásd J. CATLETT, « Technical Standards and Privacy : An open Letter to P3P Developers », disponible à l'adresse *: http://www.junkblusters.com/standards.html*
[57] Az adatkezelésnek a technika által így működtetett szerződéses viszonyairól lásd: P.M. SCHWARTZ, « Beyond Lessig's Code for Internet Privacy : Cyberespace, Filters, Privacy control and Fair Information Practices », *Wisconsin Law Review*, 2000, pp. 749 et s. ; M. ROTENBERG, « What Larry doesn't Get the Truth », *Stan. Techn. L. Rev*., 2001, 1, disponible sur le site : http://www.sth.Stanford.edu/STLR/Articles/01_STLR_1
[58] Lásd SCHWARTZ véleményét a fentebb idézett cikkben.

megfelel-e vagy e célokat szolgálja-e. A személyes információ felhasználása 'kompatibilis vagy összefüggő' célokra kiterjed például olyan esetekre is, mint a személyzet eredményes és hatékony igazgatását célzó központosított adatbázisok alkalmazása, az alkalmazottak bérlistáinak feldolgozása harmadik személyek által, vagy azoknak az adatoknak a kezelése, melyeket egy szervezet hitelnyújtás céljára gyűjtött ugyan, de e szervezettel szemben fennálló tartozások behajtásának célját is szolgálja."[59]

A technikai fejlődés gyorsulása, az informatikai eszközök kínálta új kezelési módszerek és a hálózaton elérhető adatok potenciálisan határtalan sokfélesége indokolja azt a kérdést, hogy a felhasználás, a másodlagos kezelés és a gyűjtés kompatibilitása a kezdetben rögzített céllal, továbbá a tiltás elvének tiszteletben tartását szolgáló módszerek szabályozása megfelelőnek tekinthető-e.

Ugyanígy az RFID, melyet a kereskedelmi vállalkozások kezdetben a nagy bevásárló központokban a lopások elleni harc eszközének tekintettek, a vásárlók viselkedésének elemzésére, profiljának képzésére stb. alkalmazott eszközzé vált. Egy alkotó tudós életrajzának és publikációinak rendelkezésre bocsátása munkásságának bemutatása céljából politikai vagy filozófiai osztályázását szolgálhatja. A bírósági ítéletek közzététele nagy adatbázisokban tudományos célt szolgál, s a jogi ismeretterjesztést segíti. Az azonban, hogy abban a peres felek vagy az ügytípusok szerint is kereshetünk, fekete listák felállításához vezethet (például alkalmazottakról, akik munkáltatójuk ellen bírósághoz fordultak vagy akiket elbocsátottak).

A javasolható szabályozásnak figyelembe kell vennie a másodlagos kezelés[60] érdekeit is. Kétségtelen, hogy ilyen esetekben a lehető legnagyobb mértékben meg kell követelni az adatok kódolását (az adatminimalizálás elve, lásd lentebb), vagy hozzájárulást kell beszerezni. Ennek hiányában megengedhető, hogy az az adatkezelő, amely másodlagos kezelést szándékozik megkezdeni, köteles legyen gondosan mérlegelni az érdekek egyensúlyát, e kezelés legitimitását, és tájékoztatni az érintetteket, legalább kollektíve.

A technikai megoldások tekintetében például a kereső motorok esetében álmodhatunk arról, hogy megadjuk a háló felhasználójának azt a lehetőséget, hogy maga határozza meg, mit ért a „kompatibilis" célon. Ekképpen a Web oldalakra felrakott „no robot" technikai rendszerek ennek a kereső motorok által való figyelembe vételét letiltják. A technikai megoldások másik példája: az Interneten gyűjtött adatok marketing célú felhasználása során az információközvetítők szolgáltatásaik felkínálásakor az Internet használók adatainak lehetséges felhasználásának kiválasztását marketing célokra ajánlják, stb.

## 4. Különleges adatok

A különleges adatok meghatározása az Egyezmény 6. cikkében felettébb széleskörű, s „a faji eredetre, a politikai véleményre, a vallásos vagy más meggyőződésre, valamint az egészségre, a szexuális életre *vonatkozó*" adatokat öleli fel (a szerzők kiemelése). Ez azt jelenti, hogy ebbe a kategóriába tartozik például a családnév, amely kétség kívül faji eredetre utal, valamint egy személy minden fényképe; és egy Interneten vásárolt, Koránról szóló könyv felfedheti vallásos meggyőződését, stb. Márpedig a nevek, fényképek és egyes vásárolt árucikkek mint különleges adatok szisztematikus kezelését nem lehet úgy érteni, mint amely nem tarthat számot egy különösen szigorú védelemre. Az ilyen adat nem más, mint a felelős kezelő birtokában tartott adatok joggal különlegesnek tekintett eleme (afrikai, arab, zsidó vagy japán származású személyek kiválasztása nevük alapján; tuszi, roma és egyéb típusú személyek

[59] IV. elv: A személyes információ felhasználása, 19. pont.

[60] Ekképpen egy elsődlegesen terápiai célt szolgáló egészségügyi adatbázist később felhasználhatnak tudományos kutatást szolgáló célokra, melynek révén új szolgáltatásokat javasolhatnak a betegek részére a rájuk vonatkozó adatok hatékonyabb értékelése által.

kiválasztása fényképük alapján), melyre a védelmi rendszert, mindenek előtt a kezelt adatokra épülő megkülönböztetés fokozott kockázatára való tekintettel nem készítették fel.
A különleges személyes adatok megőrzése egyrészt dicséretes. Ez ténylegesen lehetővé teszi különlegesnek tekinteni azokat az eseteket, melyekben semmiféle *a priori* különleges adat nem jelenik meg. Ezzel szemben amikor egy Internet használó a Google-lal keresi, hogyan utazhat Rómába, vagy vallásos könyvek után kutat, pápai enciklikát olvas stb., vallásos nézetei kifejezésének tekinthető.
Másrészt **jogszerűen megőrizni mindazt, ami különleges jellemzőt fed fel, oda vezet, hogy az adatok e kategóriájába roppant sok adat tartozna, melyeket az esetek többségében nem kezelnek különleges voltuknak megfelelően**. Ez szélsőséges és azzal a veszéllyel jár, hogy konkrét alkalmazás szintjén elveszi a különleges adatok meghatározásának értelmét. Megoldásul talán a meghatározás következő, árnyalatnyi módosítása kínálkozik: különleges adatként megőrizhetők „azok a személyes adatok, amelyeket a faji eredet, a politikai vélemény, vallásos vagy más meggyőződés feltárása céljából kezelnek, …".
**Érdemes fontolóra venni, nem kellene a különleges adatok körét, a technika fejlődése következtében jelentkező új kockázatokra való tekintettel, az alábbi két sajátos kategóriával kiegészíteni**:

- **azonosító számok** (a szorosan vett azonossághoz kapcsolva vagy e nélkül), amelyek lehetővé teszik sok adatbázis vagy adat összekapcsolását, s melyek általánossá váltak mind a magán-, mind a közjogi szektorban;
- **biológiai vagy biometrikai adatok**. Az európai emberi jogi bíróság világosan kifejtette, hogy ezek az adatok súlyos aggodalmat keltenek a magánélet védelme tekintetében. Véleménye szerint[61], tekintettel a sejtminták előreláthatóan növekvő használatára, hasonló adatok szisztematikus megőrzése eléggé súlyos beavatkozás a magánéletbe, következésképpen annak tiszteletben tartásához fűződő jogot sérti. Másrészt: „Azonkívül, hogy kiemelkedően személyes jellegű, a Bíróság megjegyzi, hogy a **sejtminták** számos, különleges információt tartalmaznak, nevezetesen az egyén egészségi állapotára nézve. Mi több, a minta magában foglal egy egyedi genetikai kódot, amely nagy jelentőségű mind az érintett, mint családja számára"[62]. Ami a **DNS profilokat** illeti, a Bíróság szerint[63] azok jelentős mennyiségű egyedi személyes jellegű adatot tartalmaznak, amelyek, minthogy objektív és megcáfolhatatlan jellegűek, lehetővé teszi a hatóságoknak, hogy a semleges azonosításon túlterjeszkedjenek (a DNS profil ugyanis egyének között fennálló genetikai kapcsolatok felfedése révén felhasználható az egy családhoz tartozás megállapítására). A **digitális ujjlenyomatot** illetően a Bíróság ugyancsak megállapította[64] (mely érvelés nagy valószínűséggel helytálló más fizikai azonosítók, pl. az írisz, a sziluett stb. tekintetében is), hogy „Általánosan elismert, hogy mind a sejtmintákból, mind a DNS profilokból, továbbá a digitális ujjlenyomatokból nyerhető információk megőrzése nagy hatással van a magánéletre. [ ] Mindazonáltal a digitális ujjlenyomat az érintett egyénről egyedi információkat tartalmaz, és megőrzésük az érintett hozzájárulása nélkül nem tekinthető semlegesnek vagy banálisnak. Ennél fogva a digitális ujjlenyomat megőrzése önmagában is felettébb aggályos a magánélet tiszteletben tartására nézve, s ezért sérti a magánélet tiszteletben tartásához fűződő jogot."

Az Európa Tanács részére 1999-ben készített elemzésében S. Simitis már úgy vélte, hogy a genetikai adatokat érdemes lenne felvenni a különleges adatok listájára. Véleménye szerint: „A lista korszerűsítésére a genetikai adatoknál nincs jobb példa. Alig beszéltek még róluk, amikor az első listát felállították. Manapság azonban kétség kívül nincs olyan adat, amely

[61] Cour eur. D.H., Van der Velden c. Pays-Bas, déc. du 7 décembre 2006, req. no 29514/05.
[62] Cour eur. D.H., *S. et Marper c. Royaume-Uni*, précité, par. 72.
[63] Cour eur. D.H., *S. et Marper c. Royaume-Uni*, précité, par. 75.
[64] Cour eur. D.H., *S. et Marper c. Royaume-Uni*, précité, par. 86.

hozzá hasonló átfogó információt tartalmazna az érintett személyről. A személyes adatok feldolgozásának kockázata soha korábban nem volt ilyen nyilvánvaló. Tekintet nélkül arra, hogy álláslehetőségekről, egészségbiztosítási szerződéskötésről vagy az egyén gyorsan növekvő áruvá válásának korlátairól van szó, a választ a genetikai adatok hozzáférhetősége adja. Egyetlen, különleges adatokat tartalmazó lista hagyhatja tehát figyelmen kívül a genetikai adatokat, anélkül, hogy komolyságát kétségbe ne vonnánk."[65]

# 5. Biztonság

## 5.1 A biztonság követelménye

Az Egyezmény 7. cikke nagyon szűkszavúan rendelkezik a biztonságról, azt lényegében az adatok megváltoztatására és bizalmas voltuk elleni támadásokra korlátozza. Célszerű lenne a biztonságot a „sértetlenség, rendelkezésre állás és bizalmasság" széles értelemben vett három követelményére alapozni, melyet az információs rendszerek biztonságára vonatkozó kilenc OECD irányelv (1992) is tartalmaz (felelősség, tudatosság, erkölcs, multidiszciplinaritás, arányosság, integráltság, alkalmazás, újraértékelés, demokrácia).

Ezen felül a hálózat biztonságának hiányában és a lehetséges jogosulatlan mesterkedések szaporodására való tekintettel szükségessé teszi, hogy az elektronikus kommunikációs szolgáltató értesítse a hálózat használóját szolgáltatásaival kapcsolatos kockázatokról.

Végül hangsúlyozzuk az önszabályozás fontosságát, vagyis szabályok kidolgozását, auditálási módszerek alkalmazását, nemzetközi szabványok követését stb. A biztonsági intézkedéseknek mind a szervezés, mind az információs rendszertechnikák tekintetében az adatvédelmi politika szerves részévé kell válniuk.

**A biztonsági intézkedéseknek nem csupán a jogosulatlan hozzáféréseket kell megakadályozniuk, hanem lehetővé kell tenniük azt is, hogy adataihoz való hozzáférés felett az érintett ellenőrzést gyakoroljon**. Az érintett ténylegesen csak akkor győződhet meg a biztonsági intézkedések hatékonyságáról és gyakorolhat ellenőrzést saját adatai felett, ha hozzáférhet azoknak a személyeknek az adataihoz, akik hozzáfértek az övéihez. Ebben a felfogásban döntött az európai emberi jogi Bíróság az *I c. Finlande* ügyben, elítélve ezt az államot azért, mert lehetővé tette egy állami kórháznak, hogy egy adatbiztonsági rendszert működtessen, amely nem tárolja az adatokhoz való utolsó öt hozzáférés nyomait, és amely ráadásul a hozzáférés minden nyomát törli, amint az adatokat archiválják[66].

Az Európai Közösségek Bírósága a maga részéről a *Rijkeboer* ügyben hozott ítéletében megállapította[67], hogy az adatok védelme azt is magában foglalja, hogy az érintett meggyőződhessen arról, hogy személyes adatait a jogosult címzettnek továbbították. A szükséges ellenőrzések végrehajtása céljából az érintettnek rendelkeznie kell a címzett vagy a címzett csoportok adataihoz, valamint a jelenben és a múltban továbbított információtartalomhoz való hozzáférés jogával. Ez felöleli azt a kötelezettséget, hogy az adatok címzettjeire, továbbá a lekérdezett vagy továbbított adatokra vonatkozó információkat egyaránt bizonyos ideig meg kell őrizni.

---

[65] S. Simitis, „Les données sensibles revisitées (1999)", Examen des réponses au questionnaire du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), Strasbourg, 24-26 novembre 1999.

[66] „[…] a vitatott egészségügyi adatokat tartalmazó rendszerben nem lehetett megállapítani a betegrekordok visszamenőleges használatát, mert az csak a legújabb öt vizsgálat adatait tartalmazta, és az információ törlődött, amikor az állományt archívumba visszahelyezték. Ezért a Megyei Közigazgatási Testület nem tudta megállapítani, hogy a panaszos és családja betegrekordjaiban tárolt információt harmadik, jogosulatlan félnek kiadták-e vagy ahhoz hozzáfért-e" (Cour eur. D.H., *I. v. Finlande*, 17 July 2008, appl. n° 20511/03, par. 41).

[67] C.J.C.E., 7 mai 2009, (Rijkeboer), aff. C-553/07.

A strasbourgi Bíróság az *I c. Finlande* ügyben hozott ítélete indokolásában vezérelvnek nyilvánította egyes (például egészségügyi) adatok bizalmas jellegét, hiszen ezek az adatok az érintett egyén számára nagyobb jelentőségűek, mely esetekben szigorúbb intézkedéseket kell tenni. **A biztonsági követelményeket valójában az adatok természetéhez, kezelésük körülményeihez és az érintettet ezzel kapcsolatban fenyegető kockázatokhoz kell igazítani**. A 2002/58 számú elektronikus hírközlési adatvédelmi irányelv 4. cikke ugyanilyen értelemben rendelkezik a kezelés biztonságáról: „[…] Tekintettel a legfejlettebb műszaki lehetőségekre és azok igénybevételének költségére, ezeknek az intézkedéseknek a felmerülő kockázatokhoz igazodó biztonsági szintet kell biztosítaniuk."
Az APEC Adatvédelmi Kerete ugyanígy lehetőséget ad a biztonsági követelmények enyhítésére. A VII., Biztonsági Intézkedések elve szerint: „22. A személyes adatokat kezelőnek a birtokában lévő személyes adatokat megfelelő biztosítékokkal kell védenie olyan kockázatokkal szemben, mint a személyes adatok elvesztése vagy a jogosulatlan hozzáférés, jogosulatlan megsemmisítés, felhasználás, módosítás, nyilvánosságra hozás és bármilyen más visszaélésszerű felhasználás. *Ezeknek a biztosítékoknak a kockázatokkal és az esetleges kár súlyúval, az adatok különleges jellegével és tárolásuk körülményeivel arányosnak kell lenniük, továbbá őket rendszeresen felül kell vizsgálni és újra kell értékelni* (a szerzők kiemelése).

### 5.2 A bizalmasság

Az adatok bizalmas jellegének kérdése hagyományosan a biztonság követelményeként jelenik meg.
Az elektronikus kommunikáció a jövőben alkalmazza a kommunikációban résztvevő személyek adatai kezelésének formáját, vagyis **az adatok bizalmas jellege biztosításának a követelménye konvergál a kommunikáció bizalmas jellege követelményéhez**. A bizalmas jelleg követelményeinek ez a konvergenciája úgy értelmezhető, hogy a hálózat interaktív technikája a jövőben lehetővé teszi e technikát használó személy számára, hogy a hálózathoz kapcsolt más személyekkel kommunikáljon, és ezt személyes célból tegye.
**A bizalmasság követelményét mind a kommunikációs tartalmára, mind a kommunikációt kísérő technikai adatokra, forgalmi adatokra és helymeghatározó adatokra is alkalmazni kell**.[68] Ezek az adatok tanúskodnak a kommunikáció létrejöttéről vagy létrehozásának kísérletéről, megjelölik a kezdeményezőt és a címzettet, a dátumot és az időpontot, az átvitt adatok méretét. A csatolt adatállomány tulajdonságait, a felhasználó földrajzi helyét stb.
Az adatok bizalmasságának azonban vannak határai. Az európai emberi jogi Bíróság szerint a jogalkotónak gondoskodnia kell azokról a jogszabályi keretekről, amelyek lehetővé teszik az Internet szolgáltatások bizalmas jellege és a közrend védelme, a bűnmegelőzés, valamint mások jogai és szabadságai védelmének összeegyeztetését. Egy, a Bíróság által tárgyalt ügyben[69] egy fiatal fiúra vonatkozó, szexuális jellegű tartalmat hoztak nyilvánosságra az Internet egy társkereső oldalán. Márpedig a kommunikáció bizalmas voltát védő, akkoriban hatályos finn jogszabályok sem a rendőrségnek, sem a bíróságnak nem engedték meg, hogy a szolgáltatót a tartalom szerzője azonosító adataihoz való hozzáférésre kötelezze. A Bíróság az EEJE sérelmét állapította meg, minthogy a bizalmasság tiszteletben tartásának megsértése a gyermek fizikai és erkölcsi jólétét veszélyezteti, következésképpen Finnország elmulasztotta az érintett magánéletének tiszteletben tartásához fűződő joga védelmét.

[68] Lásd 2002/58 irányelv, 5. cikk (1) bek., továbbá ugyanebben a felfogásban: Cour eur. D.H., *Copland c. Royaume-Uni*, arrêt du 3 avril 2007, § 44
[69] [69] Cour eur. DH, *K.U. c. Finlande*, arrêt du 2 décembre 2008.

### 5.3 A biztonság megsértése, jogosulatlan hozzáférés az adatokhoz

Az 2009. november 3-án kelt Madridi Nyilatkozat a magánélet védelméről alcímében – „Globális magán-életvédelmi szabályok a globalizált világban" – jelölve meg különös tartalmát, arra buzdítja az államokat, hogy „(7) **gondoskodjanak arról, hogy az egyéneket haladéktalanul tájékoztatást kapjanak, ha személyes adataikat gyűjtésük céljával összeegyeztethetetlen módon feltárják vagy felhasználják**". Értesíteni kell tehát az érintett személyt, ha személyes adataihoz harmadik – például egy kalózkodó – fél, behatolván egy szerverbe hozzáfért. Ugyancsak e kötelezettségnek kell eleget tenni azokban az esetekben, amikor a személyes adatokat elvesztik (melyeket pl. CD-ROM, USB kulcs vagy más, hordozható eszköz tárolnak), azokat – a célhoz kötöttség elvét vagy titoktartási kötelezettségét megsértve – a jogosult felhasználó figyelmetlenül vagy rosszindulatúan továbbítja (például amikor egy banki alkalmazott – bosszúból – banki adatokat tartalmazó állományt továbbít harmadik ország pénzügyi hatóságainak; egy politikai párt tagjai névsorának véletlen közzététele az Interneten; egy gyógyszer-kereskedelmi vállalkozás egy gyógyszer kockázataira figyelmeztető levele, amely megjeleníti mindazon személyes nevét és koordinátáit, akik ezt a gyógyszert szedik, …).

Az adatok biztonságának megsértése és jogosulatlan hozzáférésük esetén adandó tájékoztatásra vonatkozó kötelezettség az adatok védelmének fontos eleme: „A biztonság megsértéséről adott tájékoztatás segítheti az egyént, hogy megtegye a szükséges lépéseket a jogosulatlan hozzáférésből származó esetleges károk mérséklésére. A biztonság megsértéséről kötelezően adandó tájékoztatás ezen túlmenően arra ösztönzi a vállalkozásokat, hogy fejlesszék az adatbiztonságot és fokozzák azoknak a személyes adatoknak a kezelésével kapcsolatos elszámoltathatóságukat, melyekért felelősséget viselnek"[70] .

Az Egyesült Államokban az államok nagy többsége e tárgyban jogszabályt alkotott, s az adatvédelem sérelmével kapcsolatos rendelkezéseik azóta tükröződnek az európai közösségi jogalkotásban. Az EU 2002/58 elektronikus hírközlési adatvédelmi irányelvét módosító, 2009. november 25-én kelt 2009/136/EK irányelv „a személyes adatok megsértése" fogalmának értelmezésére egy külön rendelkezést iktatott be[71]. Azóta a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltató köteles az előfizetőt vagy magánszemélyt személyes adatai megsértéséről értesíteni[72].

---

[70] Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (2009/C 128/04), 10. pont.

[71] A személyes adatok megsértésének a fogalmát a módosított 2002/58 irányelv 2. cikk h) pontja a következőképpen határozza meg: „h) a személyes adatok megsértése: a biztonság olyan megsértése, amely a Közösségben nyilvánosan elérhető hírközlési szolgáltatások nyújtásával összefüggésben továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elveszítését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi."

[72] A módosított 2002/58 irányelv 4. cikk (3) bekezdése: „A személyes adatok megsértése esetén a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó illetékes szolgáltató indokolatlan késedelem nélkül bejelenti az illetékes nemzeti hatóságnak a személyes adatok megsértését.
Ha a személyes adatok megsértése várhatóan hátrányosan érinti az előfizető vagy magánszemély személyes adatait vagy magánéletét, akkor a szolgáltató erről az előfizetőt vagy magánszemélyt is indokolatlan késedelem nélkül értesíti.
Nem kell az érintett előfizetőt vagy magánszemélyt értesíteni a személyes adataival való visszaélésről, ha a szolgáltatásnyújtó a hatáskörrel rendelkező hatóságnak kielégítően igazolni tudja, hogy végrehajtotta a megfelelő technikai védelmi intézkedéseket, illetve, hogy ezen intézkedéseket alkalmazták a biztonság sérelmével érintett adatok tekintetében. Az ilyen technológiai védelmi intézkedéseknek értelmezhetetlenné kell tenniük az adatokat az azokhoz való hozzáféréshez engedéllyel nem rendelkező személyek számára.
Az érintett előfizetők vagy magánszemélyek értesítésére irányuló szolgáltatói kötelezettség sérelme nélkül, ha a szolgáltató még nem értesítette az előfizetőt vagy magánszemélyt a személyes adatok megsértéséről, az illetékes nemzeti hatóság kötelezheti erre, miután megfontolta a biztonság megsértésének várható hátrányos hatásait.

Ennek az értesítési kötelezettségnek a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatóra (legyen az távközlési vállalkozás vagy Internet-hozzáférést nyújtó szolgáltató) való korlátozását kritika érte. Mind az európai adatvédelmi biztos[73], mind a 29-es Munkacsoport úgy vélte, hogy a biztonság megsértésére vonatkozó értesítési kötelezettséget az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókra is ki kell terjeszteni (a fentebbi példák illusztrálják e kiterjesztés indokoltságát). Ezt a kötelezettséget elvileg tehát ki kellene terjeszteni az online bankokra, a hálózaton tevékenységet folytató vállalkozásokra, az online egészségügyi szolgáltatásokat nyújtó szolgáltatókra stb. „A rendelkezés hatályának az információs társadalommal összefüggő valamennyi szolgáltatásra történő kiterjesztése javítaná e vállalkozások elszámoltathatóságát, és hozzájárulna a társadalmi tudatosság növeléséhez, ami kétségkívül segítené a biztonsági kockázatok csökkentését[74]".
Ugyancsak kritika érte a biztonság megsértésére vonatkozó értesítés címzettjeinek korlátozása. Címzett ilyen értelemben a biztonság megsértésével végrehajtott hozzáféréssel érintett minden személy, s számukra az erről szóló értesítés hasznos lehet.
Az OECD, amikor elfogadta a „Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce" című dokumentumot[75], úgy vélte, hogy a mobil kereskedelem fejlesztésének keretében szükség lesz az adatvédelmi iránymutatás (1980) és az információs rendszerek és hálózatok biztonságát szabályozó iránymutatást (2002) újabb rendelkezésekkel kell kiegészíteni. A mobil szolgáltatókat fel kell szólítani arra, hogy az adatok biztonságára vonatkozó politikát folytassanak és olyan intézkedéseket hozzanak, melyekkel megakadályozható a jogosulatlan adattovábbítás és hozzáférés, és javasolják a fogyasztóknak, hogy hatékony jogorvoslattal éljenek, ha adataikhoz jogosulatlanul hozzáfértek vagy pénzügyi hátrányt szenvedtek.
Az OECD-nek az információs rendszerek és hálózatok biztonságát szabályozó iránymutatása[76] tartalmazza a **reagálás elvét**, mely szerint „a támadásnak kitett feleknek azonnal és egymással együttműködve kell cselekedniük a biztonság megsértésének megakadályozása, felfedése és válaszintézkedések foganatosítása érdekében". Az információs rendszerek és hálózatok interkonnektivitása hangsúlyozottan arra mutat, hogy a biztonság tömeges megsértésével okozott károk gyorsan növekszenek. Erre a fokozódó kockázatra ad választ a reagálás elve.

# 6. A érintettet védő további garanciák

## 6.1 Átláthatóság/értesítési kötelezettség

Az Egyezmény 8. cikke „az érintett védő további garanciákról" rendelkezik. Ezeket a garanciákat mint alanyi jogokat a nemzeti törvények is tartalmazzák. Az Egyezmény

---

Az előfizetőnek vagy magánszemélynek szóló értesítés tartalmazza legalább a személyes adatok megsértésének jellegét és azokat az információs pontokat, ahol az előfizető további felvilágosítást kaphat, továbbá intézkedéseket javasol a személyes adatok megsértése lehetséges hátrányos hatásainak enyhítésére. Az illetékes nemzeti hatósághoz intézett értesítés ezen túlmenően leírja a személyes adatok megsértésének következményeit és az annak orvoslására a szolgáltató által javasolt vagy megtett intézkedéseket."

[73] Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC, idézve fentebb, 22. és köv. pontok.

[74] A 29. cikk alapján létrehozott adatvédelmi munkacsoport, WP 150, Vélemény 2/2008 a magánélet védelméről és az elektronikus hírközlésről szóló 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) felülvizsgálatáról, 2008. május 15.

[75] OECD, Séoul, juin 2008.

[76] OECD Guidelines for the Security of Information Systems and Networks: towards a culture of security, 25 July 2002.

semmiféle különös kötelezettséget nem ró az adatkezelőre, ha az érintettnek ezeket a jogait nem érvényesíti.
Márpedig a védelmi rendszer nem foglal magába több garanciát, mint azokat, amelyek lényegében kizárólag az érintett kezdeményezésére épülnek. Az információs rendszerek különösen homályos környezetére tekintettel parancsoló szükségszerűség, hogy a felelős kezelő aktív átláthatóságra kötelezzék. Az érintett nem szerezhet tudomást egy olyan kezelésről, melynek létezését még csak nem sejti. Vajon hány átlagos érintett személy képes megálmodni, hogy azokat a szavakat, melyeket a kereső motorba ír, hónapokon át tárolják, méghozzá egy azonosítóval együtt[77]? Vagy hogy – mivel nagy teljesítményűek – tőle jókora távolságra elhelyezett, miniatűr kamerák veszik filmre? Vagy hogy forgalmazóik mágneses kulcsaik és kártyáik használatának nyomait megőrizvén mozgását követik? Hogy a kapu, melyen belépnek kiolvassa az útlevelében található RFID csipet? E példák jól jellemzik azokat a helyzeteket, amikor az érintett még csak nem is sejti, hiszen erről nem tájékoztatták, hogy adatait kezelik, s e helyzetek sajnos manapság egyre sokasodnak. **Elengedhetetlen tehát, hogy világos rendelkezéseket[78] hozzanak az adatok kezelésével érintett személy értesítésének kötelezettségről, mely kötelezettség a kezelést végző személyeket terheli**.
A Madridi Nyilatkozatban ugyancsak kifejezetten megjelenik az az igény, hogy a létrehozni javasolt egyetemes védelmi rendszer tartalmazza az adatok gyűjtőit terhelő kötelezettségek körét. A civil társadalom, a Nyilatkozat aláíróin keresztül „(1) Erőteljesen támogatja az adatkezelés tisztességes gyakorlatának megteremtését célzó globális keret létrehozását, amely *kötelezettségeket ró azokra, aki személyes információt gyűjtenek és kezelnek*, és jogokat állapítanak meg azok részére, akikről a személyes információt gyűjtenek”.[79]
Az APEC nemzetközi/regionális szinten legutóbb elfogadott jogeszköze előirányozza a személyes információt kezelőket terhelő értesítési kötelezettséget, melyet az Értesítés Elve cím alatt részletez[80]. Ez ehhez az elvhez fűzött kommentár erről így szól: „15-17. Az Értesítés Elvének érvényesítése biztosítja, hogy az egyén tudomást szerezhessen arról, milyen információt gyűjtenek róla és azt milyen célra használják. Az értesítéssel a személyes információt kezelők lehetővé teszik, hogy az egyén tájékozottabb döntést hozzon a szervezettel folytatandó érintkezésben. Ennek az elvnek az érvényesítését szolgáló általános módszerek egyike, amikor a személyes információt kezelők közleményt helyeznek el Web oldalaikon. Más helyzetekben, az intranet oldalakon elhelyezett közlemények vagy a működési szabályzatok mutatkoznak megfelelőnek.
Más tekintetben az érintett helyzetének jobbítása a cél, vagyis információs önrendelkezési jogai gyakorlásának biztosítása, amikor a kezelő kisebbíteni igyekszik e jogokat, megduplázván a terminál és a hálózat működésének az átláthatatlanságát. Ezeknek az új jogoknak az elismerése nélkülözhetetlen peremfeltétele annak, hogy az információs rendszerek használója ne veszítse el az információs környezet feletti uralmát biztosító ellenőrzés lehetőségét.

[77] Lásd fentebb: személyes adat fogalma.
[78] Úgy gondolhatnánk, hogy az értesítési kötelezettség halványan ugyan, de megjelenik a 8. cikk a) pontjában, az államokra hagyva e kötelezettség határának és formájának meghatározását, mely pont rögzíti, hogy „Mindenkinek joga van arra, hogy tudomást szerezzen a személyes adatok automatizált állományáról, annak fő céljairól, valamint az adatállományt kezelő személyéről és szokásos lakhelyéről vagy székhelyéről”. A jelentés indokolása ilyen értelemben szól arról, hogy e rendelkezés számol azzal, hogy ezt az elvet a belső jogszabályok különféle formában fogják konkretizálni. Ekképpen „egyes államokban az adatkezelő nevét nyilvános névmutató tartalmazza. Más államokban, ahol a nyilvánosságnak nincs ilyen rendszere, a törvény előírhatja, hogy az adatkezelő nevét ki kell adni annak, aki azt kéri.” Azon a tényen kívül, hogy a rendszeres értesítési kötelezettség kétes (és nem egy nyilvános jegyzékben rögzített bejelentés útján) elrendelését nem idéztük az a) pontban meghatározott elvet érvényesítő példákban, ennek az elvnek a megfogalmazása nem feltétlenül elegendő utalás az önkéntes átláthatóság kötelezettségére, ami pedig nélkülözhetetlen a korszerű technikai realitásai közepette.
[79] Madridi Nyilatkozat, fentebb idézve (a szerzők kiemelése).
[80] Principle II Notice.

### 6.2 A hozzáférés joga

Az Egyezményben rögzített hozzáférés jogát több tekintetben szélesíteni lehetne.
Mindenekelőtt **az érintett hozzáférésének, maguknak az adatoknak a közlésén túl, ki kellene terjednie az adatok forrásához való hozzáférésre is**[81] . Ez az információ ténylegesen kulcsfontosságú, mert gyakran az adatok forrása éppen az, ami az érintettet nyugtalanítja, s benne kérdéseket vet fel (hogyan jutottak a közlésben megjelölt adatokhoz?). Másfelől az adatok forrásának ismeretében igazolható azok továbbításának vagy gyűjtésének jogszerűsége, továbbá lehetővé teszi, hogy az érintett adott esetben az adatok első kezelőjénél kifogással éljen (vagyis gátat szabjon a kiszivárogtatásnak, ha a kezelő jogosulatlanul terjeszti a kérdéses adatokat). Végül az adatok minőségével és helyesbítésével kapcsolatos problémák esetében a helyesbítést a forrásnál lehet foganatosítani, melynek révén a hibás adatok végzetes terjesztése elkerülhetővé válik.
A hozzáférés jogát ki kellene terjeszteni arra is, hogy **mindenki megismerhesse az őt érintő adatok automatizált kezelésének logikáját** (lásd lentebb, 6.5 pont).
Mindemellett biztosítani kellene, hogy jogai gyakorlása céljára az érintett is élvezhesse a technikának ugyanazokat az előnyeit (vagyis a hozzáférés, továbbá a helyesbítés és a tiltakozás jogát), melyeket az adatkezelő is élvez[82]. Lehetővé kell tenni az érintett számára is, hogy magán a hálózaton forduljon a felelős kezelőhöz, ha a kezelés helye az Internet. Ez nem más, mint a **kölcsönös előnyökhöz való jog**, ami a technika alkalmazóját arra kötelezi, hogy az internet-használók rendelkezésére bocsássa azokat az elektronikus megoldásokat, melyekkel az elektronikus technika használatával veszélyeztetett érdekeiket vagy jogaikat érvényesíthetik.
A hozzáférés joga (és egyéb jogok) gyakorlásának elősegítése érdekében továbbá **meg kellene engedni** a felelős kezelő által használt (bizonyos esetekben nem nominatív) **azonosító adatok ismételt felhasználását** az érintett jogainak gyakorlása céljából, ahelyett, hogy megkövetelnék azonossága okmánnyal való igazolását. Az így igazolt azonosság az esetek többségében nem fog megegyezni a tárolt azonosság adataival (egy süti például, amely polgári jogilag nem igazolja az érintettet, de a szükséges individualizálására ugyanolyan alkalmas).

### 6.3 A tiltakozás joga

Egyéb nemzetközi eszközökhöz hasonlóan (az OECD iránymutatásai, az ENSZ Iránymutatása[83] és az APEC Adatvédelmi Keretek) **az Egyezmény nem tartalmazza az érintett tiltakozási jogát**. A 95/46 európai irányelv azonban 1995 óta azoknak az alanyi jogoknak a körében rögzíti ezt a jogot, amelyek biztosítják az egyén számára, hogy adatai felett az információs önrendelkezési jog gyakorlása keretében rendelkezzék. A 2002/58

[81] A hozzáférésnek ezt a jogát a 96/46 irányelv 12. cikke garantálja: „A tagállamoknak biztosítaniuk kell minden érintett számára a jogot, hogy az adatkezelőtől: a) korlátozás nélkül, ésszerű időközönként, túlzott késedelem vagy költség nélkül: [ ] érthető formában értesítést kapjon az adatfeldolgozás alatt álló adatokról és azok forrásával kapcsolatos minden rendelkezésre álló információról […]".
[82] Y. POULLET, « Pour une troisième génération de réglementation de protection des données », in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain – Challenges of Privacy and Data Protection Law, Perspectives of European and North American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, pp. 57 et s.
[83] A tiltakozási jog bizonyos formájának egy megfogalmazása: „a megfelelő helyesbítés vagy megsemmítés joga az adatok jogosulatlan, illetéktelen vagy pontatlan tárolása esetében", e jog az érintett hozzáférésének elvéhez kapcsolódik /Guidelines for the Regulation of Computerized Personal Data Files (14 Dec. 1990)/. Idézve fentebb.

elektronikus hírközlési adatvédelmi irányelv különféle formákban ugyancsak tartalmazza ezt a jogot (lásd lentebb).
Ez a jog különösen fontos, amikor az adatok kezelése nem az érintett hozzájárulásán alapul. Az érintett, aki nem nyilváníthat véleményt a kezelés megkezdésekor, e jog alapján kifejezést adhat érveinek, hogy meggyőzze az adatkezelőt arról, mondjon le adatai kezeléséről. Ez a jog különösen fontos azokban az esetekben, amikor a felelős kezelő *a priori* maga mérlegelte a fennálló érdekeket, melyeket egyensúlyban lévőnek talált, s így úgy döntött, hogy az adatokat törvényesen kezelheti. A tiltakozás jogának köszönhetően az érintett vitathatja az egyensúlyt vitathatja, legalább is saját adatai tekintetében.
A technika mai környezetében, amikor az érintett tudta nélkül vagy hozzájárulása mellőzésével folytatott adatkezelések száma szakadatlanul növekszik, újra mérlegelni kell azokat a helyzeteket, melyekben garantálni kell az érintettnek azt a jogát, hogy adatai gyűjtése és felhasználása ellen kifogással éljen, kezelésüket kifogásolja, ha arról tudomást szerzett. Az is megtörténhet, hogy az érintettet a tervezett kezelésről tájékoztatták, de nem vették kellően figyelembe adatainak esetleges megváltozását vagy kezelésük hatását más, idővel jelentkező érdekekre. Ilyen esetekben a tiltakozás joga ugyancsak megfelelő megoldást kínál.
Ezt a jogot a 29-es Munkacsoport az adatvédelem kemény magjának részének tekintette, s azóta felkerült azoknak a védelmi elvek listájára, melyeket minden, magát „megfelelőnek" tartó adatvédelmi rendszernek tartalmaznia kell. A 12. számú munkaanyag, melyet az Unió tekintetében harmadik országok adatvédelmi rendszere megfelelősége elismerésének minimális feltételeit tartalmazza, melyek teljesülése esetén a védelem szintje megfelelőnek tekinthető, e feltételek egyikeként rögzíti: „Bizonyos esetekben (minden érintett számára) lehetővé kell tenni, hogy az őt érintő adatok kezelése ellen tiltakozzon".[84]
A tiltakozás joga különösen fontos egy olyan esetben, amikor keményen kitartanak az adatkezelés jogosultságának az érdekek kiegyensúlyozásán alapuló igazolása mellett, leginkább azért, hogy ne kelljen az érintettek előzetes hozzájárulását megszerezni, például a közvetlen üzletszerzés területén. Ezt a területet egyébként a 29-es Munkacsoport is tollhegyre tűzte, mely területen ugyancsak el kell ismerni a tiltakozás jogát: „Ha az adatokat közvetlen üzletszerzés céljára továbbítják, lehetővé kell tenni, hogy az érintett megtilthassa adatainak ilyen célt szolgáló felhasználásának bármely időpontban való kiadását."[85]
Amikor az üzletszerzés különösen tolakodó vagy költséges a fogyasztónak (például az automata telefonhívások[86], faxok vagy elektronikus levelek esetében), már nem a tiltakozás jogát kell biztosítani (opt-out), hanem a megcélzott fogyasztó hozzájárulásának a meglétét (opt-in)[87].
A Web működésének gazdasági modellje menten felveti azt a megfontolást, hogy biztosítani kell a tiltakozás jogát és lehetőségét annak, aki élni kíván vele. Ez a modell a kínált szolgáltatások többsége esetében az ingyenesség látszatára épül, mely szolgáltatásokat a tisztességesen vagy átlátszatlan módon gyűjtött, hatalmas mennyiségű személyes adatokkal táplált célzott hirdetésekkel finanszíroznak. A tiltakozás jogával élve az egyén visszautasíthatná ezt a modellt, amely adatai kezelésével, sokasodásával, összekapcsolásával jár, és előnyben részesíthetné a fizető modellt, ami lehetővé tenné számára, hogy közölt adatai felett rendelkezzék.
Ugyanígy, de nem a közvetlen üzletszerzés céljából tömegesen kezelt adatokra épülő gazdasági modell mentén, az adatok kezelése ellen való tiltakozás oda vezethetne, hogy a

[84] 29-es munkacsoport: WP 12, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 1998. július 24.
[85] 29-es munkacsoport: WP 12, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 1998. július 24.
[86] Automatizált hívó rendszerek és emberi beavatkozás nélküli kommunikáció.
[87] Lásd 2002/58 elektronikus hírközlési adatvédelmi irányelv, 13. cikk, nem kívánt tájékoztatás.

szolgáltatás tervezőjét, aki a felhasználót adatai kezelésére kényszeríti, arra kötelezzék, hogy szolgáltatásának egy olyan változatát fejlessze ki, amely a személyes adatok kezelése nélkül működik. Jó példa erre a tömegközlekedésben használt elektronikus kártya. Aki nem kíván egy szolgáltatónál nyomot hagyni arról, merre járt, azt tiltakozhasson ellene, ami a kérdéses szolgáltatóra róná szolgáltatása „nem azonosítható" változata felajánlásának kötelezettségét. Ezt a változatot olyan feltételek mellett kellene hozzáférhetővé tenni, hogy az a potenciális felhasználók érdekeit ne sértse. A párizsi metrón használható elektronikus menetjegy jól illusztrálja ezt a hipotézist, vagyis egy „azonosítható" és egy „nem azonosítható" szolgáltatás együttes lehetőségét[88].
A közvetlen üzletszerzésen és piackutatáson kívül eső területek egyikén, a 2002/58 irányelv rendelkezései szerint a hívott vagy hívó felhasználó letilthatja a hívóvonal és a hívott vonal azonosításának kijelzését, ami ugyancsak jó példa a tiltakozás elvének alkalmazására[89].
Ez a szöveg kevéssel korábban a tiltakozás jogának más értelmezését tartalmazta. Az irányelv 5. cikke (3) bekezdése szerint minden személyt tájékoztatni kellett végberendezésének minden távoli felhasználásáról (például sütikről vagy kémprogramokról), amit egyszerűen és ingyenesen visszautasíthatott. Manapság felhasználó végberendezésében történő adattárolás vagy az ott tárolt adatokhoz való hozzáférés csak azzal a feltétellel megengedett, ha az érintett ehhez egyértelmű és teljes körű, különösen az adatkezelés céljairól szóló tájékoztatás alapján előzetes hozzájárulását adta.
Másfelől a vásárolt árúra erősített RFID csipnek a vásárló által való deaktiválása[90] ugyancsak a tiltakozás elvének kinyilvánítása.
A forgalmi vagy a helymeghatározó adatok kezelése esetében a tiltakozás jogát ugyancsak meg kellene valósítani[91].

### 6.4 Jog a tiltakozásra gép által hozott egyedi döntésnek az egyénre való kiterjesztése ellen

Nem kívánatos az az egyénre erőszakolt döntés, amely kizárólag egy gép következtetésétől függ [92]. Márpedig a napjainkban egyre gyakrabban használt technika a döntést egy „számítógépre" és olyan algoritmusokra bízza, melyeket az egyénre szabott döntések meghozatalára alkalmaznak (s őt esetleg adócsalónak, az üzletszerzés címzettjének, vagy utazó terroristának tekintik). Ekképpen „az új technikák újabb veszélyeket hoznak magukkal: az egyre sokasodó és egyre könnyebben hozzáférhető adatok kiterjedt és folyamatosan terjedő automatikus elemzése az egyén számára azzal a kockázattal jár, hogy csupán tárggyá válik, melyet a számítógéppel képzett „profilok", valószínűségek és előrejelzések alapján kezelnek, anélkül, hogy az érintettnek lehetősége lenne a mögöttes algoritmus ellen tiltakozni. Az adatok szigorú védelme hiányában a „jelentős következménnyel" járó döntések /például alkalmazásba vétel megtagadása vagy állásinterjúra jelentkezés elutasítása; feltartóztatás egy államhatár átlépésekor vagy egy országba való belépés megtagadása; az egyén tolakodó megfigyelése és ezt követő esetleges letartóztatása stb.) indokaként egyre többször azt hozzák

[88] Lásd lentebb: 6.7 Az anonimitás joga.
[89] A 2002/58 irányelv 8. cikke: „A hívóvonal és a hívott vonal azonosításának kijelzése és korlátozása (1) Ha választható a hívóvonal-azonosítás kijelzésének lehetősége, a szolgáltatónak egy egyszerű eszköz alkalmazásával és díjmentesen fel kell ajánlania a hívó felhasználó számára a hívóvonal-azonosítás hívásonkénti letiltásának lehetőségét. A hívó előfizető számára ezt a lehetőséget vonalanként kell biztosítani. […] (4) Ha választható a hívott vonal azonosítása kijelzésének lehetősége, a szolgáltatónak egy egyszerű eszköz alkalmazásával és díjmentesen fel kell ajánlania a hívott előfizető számára a hívott vonal azonosításának a hívó felhasználó részére történő kijelzése letiltásának lehetőségét."
[90] Lásd lentebb a „nyomomat ne kövessék" joga.
[91] Lásd a 2002/58 irányelv 6. és 9. cikke, valamint az OECD „Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce", Seoul, 2008. június, 18. oldal.
[92] Vö. fentebb az ember méltóságáról mondottak.

fel, hogy a „számítógép azt mondta", s a döntést végrehajtó tisztviselők vagy alkalmazottak nem képesek arra kielégítő magyarázatot adni"[93].
A 95/46 irányelv példájára (15. cikk)[94] **meg kellene tiltani, hogy egy személyt jelentős mértékben érintő döntést, amelynek célja a rá vonatkozó egyes személyes szempontok kiértékelése, kizárólag automatizált feldolgozás alapján hozzanak meg**.
Egy ilyen tilalomnak kellene elismernie a korlátokat és kivételeket ott, ahol azt a kontextus és a kockázatok igazolják. Ekként a kereskedelem területén általánosan elterjedt a fogyasztó profiljának automatizált kiértékelése, amikor kölcsön- vagy biztosítási szerződés megkötésére kerül sor. A profilképzési technika alkalmazása a jövőben széles körben elterjed e korlátozott kereskedelmi kontextusban, és a minden honnan összehordott tekintélyes mennyiségű adatokból táplálkozik, amint arról fentebb szóltunk.[95] A kontextus tekintetében talán disztingválnunk kell. Egyes vizsgák (például a járművezetői engedély kiadását megelőző elméleti vizsgák, vagy egy állás elnyerésére kiírt pályázat) sikeres volta elbírálása is kizárólag automatizált döntésen alapszik. Az indokoltnak minősített kivételeknek mindig társulniuk kell azokkal az intézkedésekkel, amely a géppel szemben az emberi méltóságot garantálják, biztosítván az érintettnek legalább azt a jogát, hogy álláspontját hatékonyan érvényesítse.

### 6.5 Jog az adatfeldolgozás során alkalmazott logika megismerésére

Az Egyezményben nem találjuk azt a jogot, melyhez a technika mai állása mellett jelentős érdekek fűződnek, különösen a profilképzés exponenciálisan terjedő alkalmazása tekintetében. **Az adatok automatizált feldolgozása során alkalmazott logika megismerésének jogáról van szó** [96]. Ennek a 95/46 irányelvben biztosított garanciának az alkalmazása mondatta Marc Rotenberggel (EPIC – Electronic Privacy Information Center – Washington), hogy „Egy óriás alszik az EU irányelvben, s ez nem más, mint az adatfeldolgozás logikájának megismeréséhez való jog"[97].
Ez a jog mint vezérelv a profilképzésre vonatkozó ajánlástervezetben jelenik meg, s a megfontolandók sorában ez olvasható: „17. […[ tekintettel arra, hogy mindenki megismerheti a profilképzés logikáját, ám ez a jog nem sértheti mások jogait és szabadságait, s különösen nem az üzleti titkot vagy a szellemi tulajdon vagy a szoftvert védő szerzői jogot;" Ez a tervezett szöveg tehát rögzíti az ilyen információhoz való hozzáférés jogát (függelék 5.1.b. pont).
A kezelés logikájához való hozzáférés joga mellett, de ugyancsak azt a célt szolgálva, hogy az érintett ellenőrizhesse, mi a rá vonatkozó döntés alapja, a tárgyban elismert tekintélynek örvendő kanadai Pierre Trudel professzor javasolta, hogy **a magas fokú interaktivitásra és párbeszédre alkalmas hálózatok sajátos környezetében, a jogi keretek a jövőben kötelezzék a szervezeteket arra, hogy az érintettel közöljék azokat az adatokat, amelyeket egy egyedi döntés során tekintetbe vettek** [98]. Ez biztosíthatná az adatok

---

[93] LRDP Kantor Ltd, in association with Centre for Public Reform, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final report.
Forrás: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 2010. január, 2. oldal.
[94] E rendelkezés elemzését lásd: L. BYGRAVE, « Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling », *Computer Law & Security Report*, 2001, volume 17, pp. 17–24.
[95] Lásd az ajánlást a profilképzésről.
[96] Az európai irányelv, amely a 12. cikkben rendelkezik erről a jogról, hozzáteszi, hogy „legalább (…) automatizált döntések esetében".
[97] Marc Rotenberg at the International Conference on Privacy and Data Protection "Re-inventing Data Protection?", Brussels, 12 and 13 October 2007.
[98] P. Trudel, „Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'Etat en réseau", in *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nordaméricain – Challenges of Privacy and Data Protection Law, Perspectives of European and North*

pontosságát: „Így a személyes adatok bármiféle felhasználása során minden közhatalmi szerv[99] köteles az érintettel egyeztetni azokat az adatokat, melyekhez hozzáfért. Abban az esetben, ha ez szükséges az adatok minőségének biztosítására, az adatokat az érintett rendelkezésére kell bocsátani, hogy azok tartalmát ellenőrizhesse, és szükség esetén helyesbítési jogát gyakorolhassa.” [100] E kötelesség teljesítése tehát nem más, mint egy tervezett döntés alapjául szolgáló adatok jó szándékú rendelkezésre bocsátása. Ebben az értelemben ez nem a közlendő adatokra alkalmazott logika (a számítógépi program, az indokolás vagy a kritériumok), hanem a tekintetbe vett adatok maguk.

### 6.6 A „nyomomat ne kövessék” joga

A „tárgyak Internete” kifejlesztésének következtében egyes szervezetek hivatalos dokumentumaiban új jog jelent meg, melyben „*right to be left alone*” új értelmezése tükröződik[101]. Ez a jog „a nyomomat ne kövessék” joga (*right not to be tracked*), amely az RFID csipek használatának exponenciálisan növekvő elterjedésére ad választ, ami mint „jog a csipek kiiktatására” fogalmazódik meg. Ez a jog „azt fejezi ki, hogy az egyénnek módjában kell állnia, hogy hálózati környezetével bármikor megszakítsa a kapcsolatot”[102].
Az európai Bizottság az RFID alkalmazásairól szóló Ajánlásában különböző magatartási formákat ajánl az RFID-alkalmazások jogszerű, etikailag, társadalmilag és politikailag is elfogadható tervezéséhez és üzemeltetéséhez a magánélet védelméhez való jog, valamint a személyes adatok védelmének biztosítása mellett. Az Ajánlás 11. pontja előírja, hogy „11. A kiskereskedőknek az árusítás helyén hatástalanítaniuk szükséges vagy el kell távolítaniuk az általuk használt alkalmazás címkéit, kivéve, ha a fogyasztók hozzájárulásukat adják a címkék üzemben tartásához, miután tájékoztatták őket a 7. pontban említett politikáról. A címkék hatástalanításán azt az eljárást kell érteni, amely megakadályozza a címke és a környezete közötti olyan kölcsönhatásokat, amelyekhez nem szükséges a fogyasztó aktív közreműködése. A címkék hatástalanítását vagy eltávolítását a kiskereskedőnek haladéktalanul és díjtalanul szükséges elvégeznie a fogyasztó számára. A fogyasztók számára lehetővé szükséges tenni a hatástalanítás, illetve eltávolítás eredményességének ellenőrzését.[103]
Az európai adatvédelmi biztos az RFID-nek a kereskedelem területén való használatával kapcsolatosan javasolja az árusítás helyén történő hozzájárulás lehetőségének biztosítását, amelynek értelmében az árusítás helyén a fogyasztási cikkeken található valamennyi RFID-címkét alapesetben hatástalanítanák.[104].

### 6.7 Az anonimitás joga

Számos, az Interneten végrehajtott cselekedetekre jellemző, hogy azokról különböző személyeknél nyomot hagynak. A való világban történtekkel szemben, az információs

---

*American Law*, M.V. Perez-Asinari et P. Palazzi (ed.), coll. Cahiers du CRID, n° 31, Bruxelles, Bruylant, 2008, p. 547.

[99] Ezt a megfontolást a hálózatra kapcsolódó állami szervek sajátos kontextusa indokolja, de valamennyi, a hálózatokon aktív szereplőre nézve tekintetbe kellene venni. (A szerzők megjegyzése.)

[100] P. Trudel, *op. cit.*, p. 547.

[101] A privacy első meghatározása óta a *„right to be left – ou let – alone”* ünnepélyes formulája világszerte elterjedt. *(*WARREN & BRANDEIS, *«* The Right to Privacy *»*, 4 *Harv. L. Rev.* 193 (1890)).

[102] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A tárgyak internete – Cselekvési terv Európáért, COM(2009) 278 végleges, 18.6.2009, 3. cselekvési irányvonal – A „csipek kiiktatása”.

[103] A Bizottság ajánlása ( 2009. május 12.) a magánélet- és adatvédelmi alapelveknek a rádiófrekvenciás azonosítás által támogatott alkalmazások területén történő alkalmazásáról, C(2009) 3200.

[104] Az európai adatvédelmi biztos véleménye az információs társadalom iránti bizalomnak az adatok és a magánélet védelme elősegítése révén történő erősítéséről, 2010. március 18, 56-70. pont.

sztrádán nem sétálhatunk, nem léphetünk be egy üzletbe, nem olvashatunk újságot vagy egy kereskedelmi hirdetés, anélkül, hogy ez ki ne tudódjék. Óhatatlanul érdeklődünk, mivel jár az afféle folyamatos átláthatóság, melyet kétség kívül nem tűrnénk a való világban.
Számos, nem kötelező erejű szöveg elismeri azt a jogot, hogy az ember határozzon anonimitása felől[105], midőn az új technikák kínálta szolgáltatásokat igénybe veszi. Az Európa Tanács Miniszteri Tanácsának Bizottsága R(99) 5 számú Ajánlásában[106] ugyanezt az elvet képviseli: „Az anonim fizetés és a szolgáltatások anonim igénybe vétele a magánélet védelmének legjobb módja", s egyúttal kiemeli a magánélet védelmét fokozó technológiákat (Privacy Enhancing Technologies), amely a piacon rendelkezésre áll.
**Az anonimitás értelmezését kétség kívül újra kellene definiálni**, és egyúttal olyan egyéb fogalmakat, mint az „azonosíthatatlan", csak akkor vegyünk elő, ha az anonimitásnak ez az értelmezése bizonytalannak mutatkozik. Nem annyira az abszolút anonimitást szeretnénk elérni, hanem az üzenet szerzőjének egyes személyekkel szembeni funkcionális „azonosíthatatlanságát"[107].
Aki a kommunikáció korszerű eszközeit használja, annak választási lehetőséget kellene biztosítani, hogy azonosíthatatlan maradjon mind az üzenet útjába beavatkozó harmadik felek vagy a kommunikáció e láncába beavatkozó szolgáltató számára, mind a kommunikáció egy vagy több címzettje számára, vagy legalább elfogadható áron gyakorolhassa választási lehetőségét.
Az óhajtott anonimitás vagy „funkcionális azonosíthatatlanság" mindazonáltal nem abszolút. Az egyén anonimitáshoz való joga szembe kerül az állam magasrendű érdekével, az állam korlátozásokat rendelhet el, amennyiben a korlátozások *„a nemzetbiztonság, a honvédelem, a közbiztonság, bűncselekmények vagy (egyes) vétségek megelőzése, vizsgálata, felderítése biztosításához szükségesek*". A vétségek legitim ellenőrzése és az adatok védelme között az egyensúlyt a „pszeudoazonosság" rendszerében találhatjuk, melyet speciális szolgáltatást nyújtó szolgáltató rendel az egyénhez kizárólag jogszabályban rögzített esetekben és olyan módon, ahogyan azt egy felhasználó valódi azonossága és pszeudoneve közti kapcsolatot létrehozni jogosult személy meghatározza.
A Madridi nyilatkozat az anonimitás megvalósítását célzó műszaki kutatások elmélyítésére ösztönöz. Javasolja „az adatok azonosíthatósága megszüntetésére irányuló technikai kutatások elmélyítését annak megállapítása céljából, hogy ilyen módszerekkel hatékonyan biztosítható-e a magánélet és az anonimitás védelme" (8. pont).
Az egyén anonimitáshoz való jogának garantálása nem csupán azt jelenti, hogy felajánljuk számára az adatokat azonosíthatatlanná alakító eszközöket nevezetesen azért, hogy a hálózatokon anonim módon navigálhasson. Ez egyúttal azt is garantálja, hogy az egyén a kínált szolgáltatások közül azt válassza, amely felhasználóit azonosításra nem kötelezi. Erre jó példa a tömegközlekedésben használt kártya. Egyes agglomerációkban a metrón vagy a buszon mágneskártyával is utazhatnak. Jó lenne ilyen rendszereket működtetni, s ahol a rendszer még a bérlettel vagy kártyával utazók azonosításával jár, beépítenék azt a lehetőséget, hogy aki nem kíván nyomot hagyni a közlekedési vállalkozásnál arról, merre járt, anonim

[105] E tárgyban lásd: S. RODOTA, "Beyond the E.U. Directive : Directions for the Future", in *Privacy : New Risks and opportunities*, Y. POULLET, C. de TERWANGNE et P. TURNER (ed.), coll. Cahiers du CRID, n° 13, Bruxelles, Bruylant, pp. 211 et s.
[106] Iránymutatás az „információs sztrádán" gyűjtött és kezelt személyes adatok védelmére (olvasható az Európa Tanács honlapján), és ugyanebben az értelemben: a 29-es munkacsoport „anonimitás az Interneten" című, 3/97 ajánlása. Vö. a belga adatvédelmi bizottságnak az elektronikus kereskedelemről szóló kezdeményezése (Avis n° 34/2000 du 22 novembre 2000, avis disponible sur le site de la Commission belge de la vie privée: http://www.privacy.fgov.be) kifejezetten felidézi, hogy vannak olyan mechanizmusok, amelyekkel egy üzenet küldője hitelesíthető, anélkül, hogy azonossága kötelező megadása szükséges lenne.
[107] E tárgyban lásd J. GRIJPINK et C. PRINS, "Digital Anonymity on the Internet, New Rules for anonymous electronic Transactions ?", 17 *CL&SR*, 2001, p. 378 et ss.

módon is közlekedhessen, esetleg elfogadható külön díj megfizetése ellenében (ha az ezzel kapcsolatos költségek ezt indokolják).

## 7. A 9. cikk: kivételek és korlátozások

Ahhoz, amit fentebb az Egyezmény hatályának korlátozásával kapcsolatban mondtunk, sok szerző szerint **egy általános kivételt is hozzá kellene tenni**, és pedig **a személyes adatok „családi, személyes vagy háztartási célra" való kezelése tekintetében**. Ezt joggal alátámasztja az az érv, hogy mások adatai védelmére hivatkozva nem sérthetjük annak intimitását, aki saját céljára kezel adatokat. E kivétel korlátját azonban annak a ténynek a figyelembe vételével kell megállapítani, mint azt az EEJB már idézett Linqvist ügyben hozott ítélete is mutatja, hogy egy internet oldalra feltett magánjellegű információ tagadhatatlanul a magán- vagy háztartási szférához tartozik, s meghatározhatatlan és megszámlálhatatlan személy részére hozzáférhető.
Egy efféle kivétel nagy jelentőségűvé vált a Web 2.0 és a Web exponenciálisan terjedő használatával, blogjaival, közösségi hálóival, Twitterjével s azokkal az egyénekkel, akik tartalmakat maguk szolgáltatnak (mely tartalmak gyakran információ formáját öltő személyes adatok, képmások vagy videók). A „szórakozás Internete", mint imént bemutattuk, tökéletesen illusztrálja a személyes és családi célok keveredését a vélemény nyilvánosságra hozásával, ami ellentmond a megosztott adatok „magánügyi" jellegének. Ennek a realitásnak a következmények, hogy a technika mai állása mellett magától értetődően és minden fenntartás nélkül nem lehet elfogadni vagy visszautasítani egy ilyen kivételt.
„Az általános probléma, hogy ha bármely magánszemélynek, aki az Internetre tartalmat tölt fel, teljes mentességet adunk az adatvédelmi követelmények alól, az könnyen a szabályok megkerüléséhez vezethet, és, a felhasználó által létrehozott tartalmak korában, alapvetően aláaknázná magát az adatvédelmet (és a magánélet védelmét), ráadásul túlzás lenne a jogszabály hatályának kiterjesztése minden ilyen egyénre, és pusztán számukat tekintve végrehajthatatlan. Kérdés, van-e középút, s megtaláljuk-e.[108]
**A 2. bekezdés a kifejezés vagy a véleménynyilvánítás szabadságával kapcsolatos kivételeket tartalmazza** (az adatvédelem és a véleménynyilvánítás vagy kifejezés szabadsága közötti helyes egyensúly elve). Egy ilyen kivétel megfogalmazását finoman kell mérlegelni, mivel a világ számos országában a sajtóra specifikus rendelkezések vonatkoznak, melyek alapján a sajtó az adatvédelmi elvek alkalmazása alól részleges vagy teljes mentességet élvez (például az európai országokban vagy Kanadában), s az Internet kontextusában újra kell gondolni. A Web 2.0 kibontakozása a sajtó eszméjének a felhígulásához és a zsurnalisztika szerepének elhalványulásához vezetett, a hírek és a közérdekű információk terjesztése és kommentálása már nem az újságírók és az újságok osztályrészét képezte.[109]
A statisztikára és a kutatásra vonatkozó 3. bekezdés csak a személyes adatokkal kapcsolatos veszélyt tekinti a kutatást és statisztikát korlátozó feltételnek. A statisztika és a tudományos kutatás esetében is szükség van óvintézkedésekre, még ha anonim vagy anonimizált adatokkal is dolgoznak, hiszen az egyén így képzett profilja felhasználásának lehetősége így is megmarad.

## 8. A felelősség

[108] D. KORFF, *Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, EC Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, WP 2, 20 January 2010, pp. 60 et s.
[109] E kérdéssel kapcsolatos fejtegetésekről lásd az EU bíróságának felettébb érdekes ítéletét:

A 108. Egyezmény semmiféle, az általa elrendelt védelmi szabályok betartásának felelősségére vonatkozó rendelkezést nem tartalmaz
Ezzel szemben az OECD-nek a magánélet védelmét és a személyes adatok határátlépő áramlását szabályozó Iránymutatása (1980) rögzíti a felelősség elvét, mely szerint: „Az adatkezelő legyen felelős azokért az intézkedésekért, melyek a fenti alapelveknek érvényt szereznek." Először van tehát szó arról, hogy a védelem elveinek érvényesítését az adatkezelőnek kell garantálnia.
Ennek a szövegnek az elfogadása óta eltelt idő megmutatta, mily fontos a felelősséget az adatkezelőre terhelni. Ez ténylegesen az adatvédelmi követelmények szervezeteken belüli figyelembe vételével jár. „A megfelelésnek az eseményt megelőző biztosítása kevésbé költséges, és kisebb terhet ró az érintettre, mint kényszerintézkedésekért a bírósághoz fordulni vagy más eszközökhöz folyamodni."[110]
A 29-es Munkacsoport egy röviddel ezelőtt elfogadott dokumentumában felhívja az Európai Bizottságot, hogy fogalmazza újra a 95/46 irányelvben rögzített felelősség elvét, kitartva amellett, hogy a védelmi szabályok érvényesítéséért viselt felelősség konkrét intézkedések foganatosításával jár. A 29-es munkacsoport erre alapozva javasolja, hogy a felelősség a jövőben együtt járjon az ilyen intézkedések foganatosítása igazolásának kötelezettségével: „ [ ] a felelősség törvényes elve kifejezetten megkövetelné a felelős adatkezelőtől, hogy megfelelő és hatékony intézkedéseket foganatosítson az irányelvben rögzített elvek és kötelezettségek betartásának garantálása tekintetében, melyeket igény esetén bizonyítania is kellene. Gyakorlatilag ezt azoknak a programoknak a fejlesztésével kellene megvalósítani, amelyek az adatvédelem hatályos elveit már alkalmazzák (ezeket olykor „megfelelőségi programoknak" nevezik)."[111] Ezzel megegyezően: „a felelősség elve megkövetelné a felelős adatkezelőtől, hogy belső mechanizmusokat alakítson ki, amelyek külső feleknek, például a nemzeti adatvédelmi hatóságoknak demonstrálnák megfelelőségüket. Végül annak igazolása, hogy alkalmas intézkedéseket tettek a megfelelőség biztosítására, jelentékenyen megkönnyítené az előírt szabályok végrehajtását.[112]
E megfontolások egyúttal a108. egyezményre is vonatkoztathatók.

## 9. A magánélet védelme követelményeit figyelembe vevő felfogás (Privacy by Design)

„A magánélet védelmére már kezdetben gondolkodnunk kell, amikor a védelem koncepcióját tervezzük, s nem amikor azt megvalósítjuk."[113]
Az az elv, amely „ magánélet védelmének tekintetbe vétele már a tervezéskor" (Privacy by Design) fordulat fejez ki, mindinkább mint napjaink körvonalazhatatlan követelménye jelenik meg, amely hatékonyan megvalósítja az adatok és a magánélet védelmét. **A magánélet védelme követelményének integrálása a tervezett rendszerekbe, termékekbe és szolgáltatásokba** már tervezésük első szakaszában már többször hangot kapott az Internet Governance Forúmon 2010. szeptemberében[114]. Az egész világról összegyűlt szereplők

[110] OECD Directorate for Science, Technology And Industry, Committee For Information, Computer and Communications Policy, Working Party on Information Security and Privacy, Report on Compliance with, and Enforcement of, Privacy Protection Online, DSTI/ICCP/REG(2002)5/FINAL, 12 February 2003.
[111] 29-es munkacsoport, 3/2010 vélemény az elszámoltathatóság elvéről, WP 173, 2010. július 13., 3. pont.
[112] 29-es munkacsoport, WP 168, 79. pont.
[113] Joseph ALHADEFF, vice president for Global Public Policy and Chief Privacy Officer for Oracle Corporation (Washington), at the Internet Governance Forum, Workshop "The Future of Privacy", Vilnius, 14 September 2010.
[114] Hugh STEVENSON, igazgatóhelyettes (International Consumer Protection Office of International Affairs, U.S. Federal Trade Commission): „Először is ösztönözzük az üzleti vállalkozásokat, hogy már kezdetben integrálják rendszereikbe a magánélet védelmét és a biztonságot. Úgy gondolom, hogy ez válasz a magánélet

véleménye szerint a Privacy by Design megfelelő hozzájárulás az adatok és a magánélet védelméhez.
Az európai Bizottság több alkalommal hangsúlyozta egy ilyen elv jelentőségét, nevezetesen jellegzetes alkalmazások (pl. a tárgyak Internete esetében: „Az IKT fejlődése már eddig is megmutatta, hogy [a bizalom és a magánélet kérdéseit] a tervezés szakaszában olykor negligálják, holott annak figyelembe vétele hiánya nehézségekkel és költségekkel jár, s tekintélyesen csökkentheti a rendszer minőségét. Fontos tehát, hogy a tárgyak Internete elemeinek kezdeti tervezésekor figyelembe vegyük a magánélet védelmét és a biztonság követelményét, mint a felhasználók igényei összességének egyik tényezőjét”[115]). A 29-es Munkacsoport és az európai adatvédelmi biztos ugyancsak úgy vélte, hogy e követelménynek jogszabályi formában kellene megjelenni.
Az OECD a maga részéről sokat fáradozott azon, hogy ösztönözze az adatvédelmet érvényesítő technikák alkalmazását. Az 1998. évi Miniszteri nyilatkozatában leszögezte, hogy a magánélet védelmét szolgáló technikák döntő szerepet játszanak azáltal, hogy lehetővé teszi az internet használónak a rá vonatkozó személyes információk fölötti fokozott ellenőrzést, továbbá választási szabadságának gyakorlását adatai felhasználása tekintetében. Az OECD tagállamai kormányai kötelezettséget vállaltak arra, hogy bátorítják a magánélet fokozott védelmét szolgáló technikák alkalmazását. A kormányok felszólították az OECD-t arra, hogy együttműködjön az iparral és a vállalkozásokkal a magánélet védelmének a világhálón való biztosítása érdekében.[116]
Itt kell említést tenni arról a meggondolásról, amely a termékek technikai konfigurálása során figyelembe veendő magánélet-védelmi szempontokra vonatkozik. Ez az az észrevétel, amelyet az Európai Bizottság által megrendelt, a magánélet védelmének a technikai fejlődés fényében jelentkező kihívásaival foglalkozó tanulmány szerzői fogalmaztak meg. A szerzők rávilágítottak arra, hogy ha a közösségi hálók vagy blogok internet oldalainak működtetőit jobb híján (default option) a magánélet védelmét szolgáló paraméterezésre kötelezik, megoldódna a személyes célokra irányuló használatra vonatkozó kivételek problémája (vö. a fentebb mondottak a kifejezés nyilvánossága eszközei, például az Internet használatának korlátairól). A szerzők szerint „lehetővé kellene tenni az adatvédelem szabályainak rugalmasabb alkalmazását az Interneten folytatott viszonylag jelentéktelen tevékenységek esetében. A problémát az okozza, hogy az Internetet szokásszerűen használókat alá akarják vetni valamennyi, az „adatkezelő” által alkalmazott szabálynak. És mi úgy gondoljuk, hogy e problémának a legjobb megoldása, ha szabályozzuk magánemberek által használt

---

védelmét és a rendszerfejlesztést bátorító megjegyzéseink egyikére.[…]” Ellen BACKLER (ügyvezető igazgató, AT&T), Rosa BARCELO, az európai adatvédelmi biztos jogi tanácsadója: „A másik jog,melyet támogatunk, a privacy by design joga. Ez jog szükséges ahhoz, hogy az adatvédelmi elveket ne csak a technikában vegyék figyelembe, hanem az egész szervezetben, s már a tervezés kezdetén egészen a folyamat befejezéséig.” Joseph ALHADEFF (a globális közpolitikáért felelős alelnök és adatvédelmi főnök, Oracel Corporation); az Internet Architecture Board, (IAB); Jon PETERSON (Neustar), Hannes TSCHOFENIG (Nokia Siemens Network), Bernard ABOBA (Microsoft): „Állásfoglalás: a magánélet védelmének fejlesztése az Interneten és a szabványosítási közösség szerepe”, műhely „A magánélet védelmének jövője” tárgyában: „Internet Engineering Task Force (IETF) hosszú időn gyűjtött tapasztalataira építve a szerzők meggyőződése, hogy a protokollok és architektúrák tervezésekor a magánélet védelmét fontos már kezdetben tekintetbe venni, s nem utólag felmerült gondolatként vesződni vele. […] A technikai munkát jogszabályokkal kell alátámasztani, és megfelelő megoldásokkal megsértésüktől elriasztani. Ha a vállalkozásokat a magánélet védelmének figyelembe vételére barátságos ösztönzőket állapítunk meg, úgy a játéktér is megváltozik majd” stb.

[115] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A tárgyak internete – Cselekvési terv Európáért, COM(2009) 278 végleges, 18.6.2009. június 18.

[116] OECD, Ministerial declaration on the Protection of privacy on global networks, 7-9 october 1998. Továbbá: Forum de l’OCDE sur les technologies protectrices de la vie privée (TPVP), 8 octobre 2001 ; OCDE, *Protection de la vie privée en ligne Orientations politiques et pratiques de l’OCDE* , Paris, 2003, pp. 273-383.

szolgáltatásokat, így a közösségi hálókat, a „blogoknak” szállást adó Web helyeket stb. E szállásadókat kötelezni kellene arra, hogy Web helyeiket és szolgáltatásaikat default option paraméterekkel és a magánéletet védő eszközökkel lássák el. A közönséges felhasználóknak, akik ezeket a Web helyeket használják anélkül, hogy módosítanák a default option paramétereket, biztosnak kellene lenniük abban, hogy nem sértenek semmiféle adatvédelmi jogot; ha e paraméterek nem védik a személyes adatokat, a paramétereket definiáló Web helynek kell viselnie a fő felelősséget.”[117]
Az adatvédelmi követelményeknek a termékekben és a szolgáltatásokban való figyelembe vételére és integrálására vonatkozó kötelezettségen túl (a gyűjtött adatok, az adatgyűjtők, az adatokhoz hozzáférők átláthatósága, a tájékozott hozzájárulás megszerzése, …) e kötelezettség mint vezérelv két különös szempontját kell megvizsgálnunk:

### 9.1 Az adatok minimalizálásának elve

A 108. egyezmény az adatkezelést azokra az adatokra korlátozza, melyek tárolásuk céljával arányban állnak, e célnak megfelelnek, ezen nem terjeszkednek túl, s e kötelezettséggel határt szab a gyűjtött adatok mennyiségének. E kötelezettséget az adatok minimalizálása elvének tekinthetjük. Ez elv azonban ennél messzebbre megy. Valójában a személyes adatok lehető legnagyobb fokú minimalizálására (vagyis a szigorú minimumra korlátozásra) vagy gyűjtésük mellőzésére hív fel.
A minimalizálás elvének megvalósítására különösen alkalmasak az anonimizálási vagy pszeudonimizálási technikák vagy a magánélet védelmét fokozó technikák (Privacy Enhancing Technologies – PET). E technikák már felismert korlátain[118] túl azonban nagyon hatékonyan érvényesíthetjük ezt az elvet, ha kevésbé technikai jellegű megoldásokhoz folyamodunk. Így megkövetelhetjük, hogy a különféle alkalmazások default option paraméterei a kezelt személyes adatok mennyisége tekintetében fokozzák, s ne gyengítsék a magánélet védelmét. Ez jobb híján oda vezethet, hogy a böngésző korlátozza felhasználó által a web helyekre küldött információk maximumát, vagy például egy közösségi háló nem teszi hozzáférhetővé az egész világnak a hálón tárolt információkat.
Az Európai Unió nemzeti adatvédelmi hatóságainak közössége javasolta, hogy a minimalizálásnak ezt az elvét a jövőben építsék be a jogszabályokba[119]. Az európai adatvédelmi biztos ugyanígy tett[120]. Az Európai Bizottság a maga részéről a magánélet

[117] LRDP Kantor Ltd, in association with Centre for Public Reform, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final report. Forrás: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 2010. január. 35. pont.
[118] „Más, az adatvédelmet fokozó módszerek, ide értve olyan technikai módszereket is, mint a titkosítás, anonimizálás, azonosságkezelő eszközök és más, (feltehetően) a magánélet védelmét fokozó (PET) technikák, még mindig kevéssé fejlettek, megvalósításuk és hatékonyságuk foka gyakran gyenge, alkalmazásuk módja hatástalanítja őket. Néhányuk nem több, mint fügefalevél. Más módszereken (mint az anonimizáláson) a fejlett technika kerekedik felül. Sokuk gyakran nem a kellő pillanatban, vagyis a tervezés szakaszában, kezeli a problémákat, vagy nem felhasználó-barát. Az új technikai környezetben még több és még kritikusabb figyelmet kell szentelnünk e módszereknek.” (*Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, 19. oldal.)
[119] A 29. cikk alapján létrehozott adatvédelmi munkacsoport, WP 150, Vélemény a 2/2008 a magánélet védelméről és az elektronikus hírközlésről szóló 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) felülvizsgálatáról, 2008. május 15.; Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, §53.
[120] Az európai adatvédelmi biztos véleménye az információs társadalom iránti bizalomnak az adatok és a magánélet védelme elősegítése révén történő erősítéséről, 2010. március 18. „[ ] javasolja a Bizottságnak, tegyen javaslatot egy, a beépített adatvédelemre vonatkozó általános rendelkezésnek az adatvédelemmel kapcsolatos jogi keretbe történő beépítésére.” (38. pont)

védelmét erősítő technológiák fejlesztésének támogatására irányuló programokat javasol, melyek végrehajtása a személyes adatok kezelésének csökkentéséhez vezet[121].

### 9.2 A magánéletre gyakorolt hatás vizsgálata

Ugyanígy javasolták azt is, hogy mielőtt egy termék vagy szolgáltatás (például RFID csip) fejlesztéséhez látnak, a tervezők kötelesek legyenek megvizsgálni, hogy a kérdéses termék vagy szolgáltatás milyen hatást gyakorol a magánélet vagy az adatok védelmének kockázataira[122]. Az Európai Bizottság szerint az értékelés részletezése szintjének igazodnia kell azokhoz a kockázatokhoz, amelyek az alkalmazás során a magánélettel kapcsolatosan merülnek fel.
A magánélettel kapcsolatos hatásvizsgálatokban újra felismerhetjük a jogok és érdekek kiegyensúlyozásának követelményét, amelynek minden adatkezelést meg kell előznie (vö. fenti 3.2 pont). A kiegyensúlyozás írásba foglalásának kötelezettsége garantálja, hogy ténylegesen figyelembe vettek valamennyi érdeket, lehetővé téve a kiegyensúlyozás eredményének könnyűszerrel való vitatását.
A hatásvizsgálatot legalább azokra a termékekre, szolgáltatásokra és információrendszerekre nézve kellene kötelezően elrendelni, amelyek jelentős kockázati hatást gyakorolnak a népességre.
Ugyanebben a felfogásban Ausztráliában: „A kormány javasolja, hogy a magánélet-védelmi biztos utasíthassa a szövetségi kormány ügynökségeit (de nem a vállalkozásokat), hogy egy olyan „új alkalmazás vagy egy meglévő fejlesztése" esetében a magánélettel kapcsolatos hatásvizsgálatot [Privacy Impact Assesment] nyújtsák be a biztosnak, amely a Biztos véleménye szerint 'jelentős hatást' gyakorol a személyes információk kezelésére, és – ha az ügynökség ezt elmulasztja, a Biztos jelenti a Miniszternek (kérdés, vajon közzé is teszi) (AusGov, 2009: 47-4)."[123]

## 10. Kiskorúak adatainak különleges védelme

A 108. Egyezmény semmiféle, a kiskorúak adatainak védelmére vonatkozó különleges rendelkezést nem tartalmaz. Márpedig fokozott kockázatnak vannak kitéve mind az Interneten, mind pedig mobiltelefonjuk használata során, ami talán **megérdemel egy hozzájuk igazított védelmet**. Ők az üzletszerzési akciók, a közösségi hálók vagy egyéb, ilyen szolgáltatásokat igénybe vevők csoportok, ilyen alkalmazások felhasználói körének tagjává válásra szóló meghívások céltáblái… Ugyanakkor nélkülözik az ítélőképességet és a kritikai szellemet, nem veszik figyelembe döntéseik következményeit, döntésük impulzív s nem előrelátó,…
Az OECD a „Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce" című dokumentumában[124] külön foglalkozott azokkal a szaporodó kockázatokkal, amelyeknek a gyermekek a mobil kereskedelem területén ki vannak téve. Az OECD e dokumentuma „Protection des données nominatives des enfants" (Gyermekek személyes adatainak védelme" cím alatt a következő ajánlást teszi:

---

[121] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak az adatvédelemnek a magánélet védelmét erősítő technológiák által történő ösztönzéséről, 2007. május 2., COM(2007)228 végleges.
[122] Lásd az európai adatvédelmi biztos véleménye (JO C 101, 23.4.2008, pp 1-12) és a Bizottság ajánlása (2009. május 12.) a magánélet- és adatvédelmi alapelveknek a rádiófrekvenciás azonosítás által támogatott alkalmazások területén történő alkalmazásáról, C(2009) 3200).
[123] G. GREENLEAF, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Country Study B.2 – Australia, January 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B2_australia.pdf, p. 33.
[124] OECD, Seoul, 2008. június.

Az országok kiegészíthetnék hatályos törvényeiket és szabályaikat a gyermekeket a mobil környezetben védő rendelkezésekkel. Az Egyesült Államokban például szövetségi törvény korlátozza 13 évesnél fiatalabb gyermekek személyes azonosíthatóságát lehetővé tevő adatok gyűjtését, felhasználását vagy közlését az online szolgáltatásokban. A törvény előírja továbbá az alkalmazott adatvédelmi gyakorlatról szóló tájékoztatást, a gyermekek személyes adatai gyűjtésére vonatkozó szülői hozzájárulást (bizonyos korlátozott kivételekkel), gyermekeikre vonatkozó személyes adatok megtekintését és törlését a szülők által, és az adatok biztonságát védő eljárások kötelező alkalmazását."[125]
A kiskorúak hozzájárulása nehézségeit már az „Információs önrendelkezés az Internet-korban" című jelentés is tárgyalta.[126] Rámutatott arra, hogy a kiskorúak hozzájárulása személyes adataik kezeléséhez sajátos problémákat vetnek fel. A hozzájárulást csak a törvény értelmében cselekvőképes személy adhatja meg. A kiskorú hozzájárulása szülői felhatalmazás hiányában nem elegendő, mégis – ítélőképességükhöz mérten – szükséges autonóm módon kifejezett hozzájárulásuk megszerzése a szülői hozzájárulás mellett.
Újabban az Internet interaktív szolgáltatásainak fejlődése tette ezeket az elveket aktuálissá. A gyermekek az Interneten jelen lévő legkülönbözőbb „árusok" privilegizált céltáblái, akik változatos módszerekkel gyűjtik az információkat, melyek alapján személyes információt nyújtanak, például meghívót játékversenyekre, belépési adatlapokat stb.
A szülői hozzájárulás ilyen információk küldéséhez tehát elengedhetetlennek látszik. Az amerikai „Children's Online Privacy Protection Act of 1998" (COPPA)[127] elrendeli, hogy a gyermekek adatait gyűjtő szolgáltatók kötelesek megszerezni a „hiteles szülői hozzájárulást", melynek meghatározása: „minden ésszerű (a rendelkezésre álló technika kínálta) módon törekedni kell arra, a tájékoztatóban körülírt jövőbeli gyűjtésre, felhasználásra és közlésre szóló felhatalmazás megszerzése mellett, hogy a gyermek szülője megkapja a szolgáltató tájékoztatását a személyes információk gyűjtéséről, felhasználásáról és közlésének gyakorlatáról, majd felhatalmazást adjon a személyes információk gyűjtésére, felhasználására és adott esetben közlésére, valamint ennek az információnak a későbbi felhasználására, még mielőtt azt a gyermektől gyűjtenék."

## 11. Specifikus védelem a jogokra és szabadságokra nézve különös kockázattal járó kezelések esetében

A 108. Egyezmény elfogadása óta bekövetkezett technikai fejlődés megmutatta, hogy egyes kezelések különös veszélyt jelentenek az érintett személyre nézve.
Azokról a kezelésekről lehet szó, amelyeket az állami szektorban végeznek, s amelyek – mivel az ország egész lakosságát vagy e lakosság fontos tagjait érintik – fokozott veszélyt jelentenek, s mivel kötelező érvényűek, az adatkezelés legitim okból való megtagadásának nincs helye. Az állami szektorban az adatállományok összekapcsolásának komoly kockázata is jelentkezik, minthogy több adatállomány ugyanazt az egyedi azonosító számot használja. E kockázatok tehát fokozzák azoknak a fentebb jellemzett adatállományoknak vagy adatkezeléseknek a veszélyeztetettségét, melyek számára egy nem specifikus azonosító szám használatát kellene elrendelni.
A magánszektor kezelései ugyancsak különös kockázatokkal járnak. Ilyen kezelések új technikai eszközökre épülnek (például RFID címkék, új térfigyelő rendszerek, arcfelismerés,

[125] Ugyanott, 21. oldal.
[126] Idézve fentebb.
[127] Sect. 1302(9). 1998. évi törvény a gyermekek online adatai védelméről. Olvasható a Federal Trade Commission honlapján: http://www.ftc.gov/ogc/coppa1.htm. A törvény e kötelezettségek alól néhány kivételt is tartalmaz.

testkép, biometrikus azonosítók, …), amelyek az ilyen eszközökkel megcélzott személyek érdekeit, jogait és szabadságait sérthetik.
**Helyes lenne előzetes óvintézkedéseket foganatosítni ilyen kezelések megkezdése előtt**. Ez az intézkedés előzetes ellenőrzés formáját ölthetné, mely ellenőrzést az adatvédelmi hatóság végez. Másik megoldás lehetne a kezelést tervező szervezet, intézmény vagy magánszemély kötelezése arra, hogy végezze el a kezelésnek a magánéletre gyakorolt hatásai vizsgálatát (vö. fenti 9.2 pont).

## 12. Jogorvoslat

Az utóbbi években napvilágra került megfontolások fényében javasolható, hogy **a 108. Egyezmény rendelkezzen arról, hogy jogi személyek az adatvédelmi szabályok megsértése esetén peres eljárást kezdeményezzenek**.[128] „[ ] meg kell érteni, hogy a magánélet és az adatok védelme területén adott személynek okozott sérelem önmagában általában nem elegendő ahhoz, hogy bírósági peres eljárást kezdeményezzen. Magánszemélyek önszántukból általában nem fordulnak bírósághoz, csak mert kéretlen üzenetet (spam) kaptak vagy nevüket helytelenül vették fel egy névjegyzékbe. Ez a módosítás lehetővé tenné, hogy a fogyasztók közös érdekeit képviselő fogyasztóvédelmi szervezetek vagy szakszervezetek nevükben bírósági eljárást kezdeményezzenek."[129]
Továbbá „fel kellene jogosítani jogi személyeket, például fogyasztóvédelmi szervezeteket és nyilvános elektronikus hírközlési szolgáltatókat arra, hogy bírósági eljárást kezdeményezzenek, ami erősíti a fogyasztók pozícióját és elősegíti az adatvédelmi jogszabályok betartását. Ha a jogsértő vállalkozásoknak fokozódik az a kockázata, hogy peres eljárással kell szembenézniük, valószínűleg többet fektetnek be abba, hogy betartsák az adatvédelmi jogszabályokat, ami hosszabb távon a magánélet és a fogyasztók védelmének javulását eredményezi."[130]
Az egyén jogai védelmének hatékonysága kérdésén túl annak elismerése, hogy jogi személyek jogosultak e tárgyban bírósághoz fordulni, vitathatatlanul hozzájárulhat e területen a védelem elvei alkalmazásának javulásához.

## 13. A magánélet és az adatok védelme tárgyában alkalmazandó jog – Az adatok határátlépő áramlása

### 13.1 Egy három részre „szakadt" környezet

Az alkalmazandó jog kérdését megelőzően fontos kiemelni az új technikai környezet jellemzőit, amelyek befolyásolják e kérdés megoldását. Ezek a jellemzők azzal a ténnyel kapcsolatosak, amelyet a környezet három részre szakadása okozott.
Az Internet manapság tömeges használata (e-mail, közösségi hálók, elektronikus kereskedelem) együtt jár az egyre nagyobb mennyiségű adat határátlépő áramlásával. Az informatika fejlődése, például a „cloud computing" (számítási felhő) az informatikai erőforrások tényleges helyhez kötöttsége megszűnéséhez vezet, az adatot – legyen az pénzügyi, személyes, üzleti stb. – ott kezelik, ahol – technikailag és gazdaságilag – a

[128] Lásd LRDP Kantor Ltd, in association with Centre for Public Reform, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final report. Forrás: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 2010. január. 109-111. pont.
[129] Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (2009/C 128/04), 89. pont.
[130] [130] Ugyanott, 92. pont.

leghatékonyabb, és az Internet segítségével az adat a földkerekség bármely pontjáról hozzáférhető. Az információs társadalommal összefüggő – egy vagy több országból eredő – szolgáltatásokat [131] már hosszabb ideje online nyújtják az egész világon, változatos szükségletek kielégítésére és változatos ügyfeleknek, akik vagy amelyek magánéleti vagy hivatásbeli célból cselekvő egyének, vállalkozások, gyermekek, átlag- vagy nagy emberek, hasznot hajtó cél nélküli egyesületek, állami szervezetek, szakszervezetek, kampányoló politikusok, kórházak, egyetemek stb. E szolgáltatások tekintetében egy két részre szakadás figyelhető meg: egyrészt környezetük (a szolgáltatók, a címzettek, a kezelés módszerei, a szolgáltatás hozzáférhetősége stb.) földrajzi helyét tekintve, másrészt a szereplőktől és a kezelt adatoktól függő jellegükre nézve (állami szereplők, magánéleti célból cselekvő természetes személyek, multinacionális vállalkozások stb.).
Egy ilyen környezet óhatatlanul a jogszolgáltatás vagy közhatalmi szervek (rendőrség, bíróság, pénzügyi hatóság, adatvédelmi hatóság stb.) nemzetközi kompetenciájának, valamint a tekintetbe vehető különféle tényállásokat szabályozó jog meghatározásának kérdéséhez vezet[132]. A jogi szabályok megállapítása és értelmezése e kérdések döntő szempontja, számos kulcsfontosságú célt kell megvizsgálni, köztük a területiség elve, a nemzetközi összhang, az egyén – alapvető vagy nem alapvető – jogainak hatékony védelme biztosításának és a jogbiztonságnak a követelménye.
A 108. Egyezmény és jegyzőkönyve – kötelező erejű nemzetközi szerződések – a személyes adatok gépi feldolgozását és ezzel kapcsolatosan az adatok határátlépő áramlását. Az imént ismertetett helyzet nemzetközi jellegére tekintettel az Egyezmény az Európa Tanács negyvenhét tagállama közül negyvenhárom [133] jogszabályai összhangját teremti meg. A jegyzőkönyvet (2001) napjainkig negyvenegy állam írta alá, közülük harminc ratifikálta is[134]. Másfelől az Európa Tanács minden tagállamára kötelező az EEJE 8. cikke, amely jelen esetben különösen lényeges. Megjegyzendő továbbá, hogy azok az országok is csatlakozhatnak a 108. Egyezményhez, amelyek nem tagjai az Európa Tanácsnak (23. cikk), s ezt követően a kiegészítő jegyzőkönyvhöz (3. cikk 2. pont).
A 108. Egyezmény negyvenhárom tagállama közül huszonhét egyúttal tagja az Európai Uniónak is, ahol különösen a 95/46 és a 2002/58 irányelvek teremtik meg a személyes adatok kezelésére vonatkozó jogszabályok összhangját[135]. Ezekhez az államokhoz még hozzá kell adnunk Izlandot, Norvégiát és Liechtensteint, melyeket mint az Európai Gazdasági Térség tagjait ugyancsak kötnek ezek az irányelvek.
Egyébként az adatvédelmet kikényszerítő jogszabályok kizárólag a nemzeti eredetűek. Az OECD magánéletet és a személyes adatok határátlépő áramlását védő, nem kikényszeríthető iránymutatásai például ösztönző források lehetnek az idézett szövegeken felül. Végül megemlítjük a Világkereskedelmi Szervezet (WTO) adatvédelmi szabályait, amelyek a Szervezet szabályai között fontos helyet foglalnak el. Így a szolgáltatások nemzetközi kereskedelmét adatvédelmi megfontolások korlátozhatják: a General Agreement on Trade in Services Általános kivételek című XIV. cikk c) ii) pontja szerint „a Megállapodásban

[131] A közösségi jog meghatározása szerint: „az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás", az Európai Parlament és a Tanács 1998. július 20-i 98/48/EK irányelve a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás megállapításáról szóló 98/34/EK irányelv módosításáról, 1. cikk (2) bek. a) pont.
[132] E tekintetben főleg az alkalmazandó jog meghatározásának kérdésére koncentrálunk.
[133] Törökország és Oroszország aláírta, de nem ratifikálta, míg San Marino és Arménia nem írta alá a 108. Egyezményt.
[134] A jegyzőkönyvet még nem írta alá Arménia, Azerbajdzsán, Grúzia, Málta, San Marino és Szlovénia, és még nem ratifikálta Belgium, Dánia, Finnország, Görögország, Izland, Olaszország, Moldova, Norvégia, az Egyesült Királyság, Oroszország és Törökország.
[135] Lásd ugyancsak: Az Európai Unió alapjogi chartája.

foglaltakat semmiképpen nem lehet úgy értelmezni, hogy az a tagállamokat megakadályozza a szükséges intézkedések meghozatalában, melyek az egyén magánéletét védik személyes adatai feldolgozása és terjesztése, valamint egyéni iratai és számlái bizalmas jellege vonatkozásában". Adott esetben ennek a kivételnek a helytelen alkalmazását egy külön csoport állapítja meg a WTO által megfelelőnek tartott szankciókkal egyetemben.
A szakadás harmadik, a technikai fejlődés gyakran nemzetközi környezetéből (főleg az Internetből és szolgáltatásaiból) fakadó formája a jogrend és a jogi kultúra, amely ilyen vagy hasonló helyzetekben jogorvoslatokhoz vezet.
Egy ilyen környezetben a 108. Egyezmény és a hasonló nemzetközi szövegek rugalmassága garantálja a különféle szabályozási stratégiák koegzisztenciáját és lehetővé teszi az aktuális (és a jövőben megjelenő) technikákból adódó komplex és evolutív helyzetekben az igazságos és megfelelő jogorvoslatot. Az államok azok, melyek – adott esetben egy nemzetközi bíró felügyelete alatt – meghatározzák az érintett személy védelmét és biztosítják jogalkotásuk, bíróságaik és nemzeti adatvédelmi hatóságaik hatékonyságát. Érdemes lenne nyilvános konzultációt kezdeményezni az Interneten a nemzetközi magánjogi rendelkezések esetleges harmonizációjáról, és arról, mi legyen a szerepe e tekintetben az Európa Tanácsnak.

### 13.2 Az adatok határátlépő áramlása: az adatvédelemre alkalmazandó jogszabályok hiánya

Az Európa Tanács szintjén a határátlépő adatáramlás az Egyezmény 12. és a Jegyzőkönv 2. cikke szabályozza.
Így elvileg az Egyezményhez csatlakozott Felek egyike sem tilthatja vagy kötheti külön engedélyhez, a magánélet védelmének kizárólagos céljából, a személyes adatoknak az országhatárokat átlépő áramlását, ha az egy másik Fél területére irányul. Az Egyezmény ugyanakkor kivételeket is tartalmaz /12. cikk 3. a) és b) pont/: a imént említett rendelkezésektől bármelyik Fé eltérhet, ha „jogszabályai külön rendelkezéseket állapítanak meg meghatározott személyes adatokra vagy személyes adatok meghatározott automatizált állományaira, ezen adatok vagy adatállományok jellege miatt, kivéve, ha a másik Fél szabályozása azonos védelmet nyújt"; vagy ha „a továbbítás saját területéről egy másik Fél területén keresztül egy nem szerződő Fél területére irányul, annak érdekében, hogy megakadályozza, hogy az ilyen továbbítás a Fél e pont elején említett jogszabályainak kijátszását eredményezze". Az első esetben egy állam korlátozhatja egyes adatfajták határátlépő áramlását, ha az olyan államba irányul, amely nem nyújt „azonos" védelmet. A második esetben a jogszabályok kijátszása elkerüléséről van szó, a harmadik felek területére irányuló adatáramlást csak követve veszi figyelembe.
Az Unió Tagállamai a 95/46 irányelv rendelkezése szerint „nem korlátozhatják és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását" az irányelv „értelmében biztosított védelemmel kapcsolatos indokok miatt" /1. cikk (2) bek.). Ez a szabály az Európai Unió tagállamait tekintve tehát szigorúbb.
A 108. Egyezmény Kiegészítő Jegyzőkönyve rendelkezik az adatok határátlépő továbbításáról olyan címzett részére, aki vagy amely nem tartozik az Egyezményhez részes Fél joghatósága alá. A Jegyzőkönyv szerint a továbbítás csak akkor megengedhető, ha a címzett Fél (vagy szervezet) megfelelő szintű védelmet biztosít (2. cikk 1. pont). Egyrészt „ha ezt hazai joga lehetővé teszi: az adatalany meghatározott érdekére tekintettel, vagy jogszerű nyomós érdekre, különösen fontos közérdekre tekintettel /2. cikk 2. a) pont/. Az érintett hozzájárulása ugyancsak figyelembe vehető, ahogyan az a 95/46 irányelv kidolgozásának kezdete óta előirányozza. Mindazonáltal aggodalomra ad okot az a gyakorlatban jelentkező kockázat, hogy ez a hozzájárulás nem más, mint a jól ismert szerződéses kikötések egyike, amely a kínált szolgáltatás egyszerű igénybevételével válik érvényessé. Másrészt a megfelelő védelem

biztosításának követelménye megszűnik, „ha a továbbításért felelős adatkezelő olyan, elsősorban szerződésben kikötött, biztonsági intézkedéseket tesz, amelyeket az illetékes felügyelő hatóságok a hazai jog szempontjából megfelelőnek találnak /2. cikk 2. b) pont/.
Az Európai Unió tagállamainak ugyancsak alkalmazniuk kell a 95/46 irányelvnek azokat rendelkezéseit, amelyek harmadik, nem EU tagállamba irányuló határátlépő áramlást szabályozzák, mely államok feltehetően egyúttal a 108. Egyezmény részes felei. A 95/46 irányelv 25. cikke ugyancsak előírja, hogy az adatok rendeltetési helyeként megnevezett harmadik államnak megfelelő védelmi szintet kell biztosítania, melytől a 26. cikk számos eltérést enged meg, köztük az érintett kétségbe vonhatatlan hozzájárulását és a szerződéses garanciákat. E vonatkozásban fontos hangsúlyozni, hogy azoknak a harmadik államoknak, amelyek az Európai Uniónak nem tagjai, de részesei a 108. Egyezménynek, hogy a Kiegészítő Jegyzőkönyvhöz csatlakozása elmaradása – hasonló belső jogszabályok hiányában – az ajánlott védelem súlyos hiányosságaihoz vezethet.[136] „Az alapelveket tényleges alkalmazását biztosító eljárási mechanizmusok" hiánya ugyancsak meghatározó jelentőségű lehet[137]. Röviden összefoglalva: az Európa Tanácsa 108. Egyezménye – és egyúttal Jegyzőkönyve – részes állama nem feltétlenül tekinthető úgy, mint amely megfelelő védelmet biztosít, még akkor sem, ha a gyakorlatban számos esetben minden valószínűség szerint ilyesmiről valamiféleképpen gondoskodik.
Mellesleg érdekes megjegyezni, hogy jelenlegi állapotában a 96/46 irányelv nem engedi meg a megfelelőség elemzésének figyelembe vételét a harmadik államokban mint rendeltetési helyeken olyan feldolgozások esetében, melyek „a közösségi jog hatályán kívül eső tevékenységek, mint például az Európai Unióról szóló szerződés V. és VI. címeiben megállapítottak, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási művelet nemzetbiztonsági ügyre vonatkozik), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek"[138]. Ez ellenben lehetséges a 108. Egyezmény Kiegészítő Jegyzőkönyve rendelkezései szerint[139].
Akárhogy áll is a dolog, a 108. Egyezmény határátlépő adatáramlást szabályozó célja, hogy „összeegyeztesse a hatékony adatvédelem követelményeit a határokra való tekintet nélküli a szabad információáramlás elvével, mely az Emberi Jogok Európai Egyezménye 10. cikkében van lefektetve" (Indokolás, 62. pont). Jelesül arról van szó, hogy el kell kerülni, hogy ezt az utóbbit „bármilyen protekcionizmus" veszélyeztesse (Indokolás, 20. pont). Ekképpen a tagállamok közötti határátlépő adatáramlás akadályozása nem megengedhető meg „*tiltások vagy külön felhatalmazások*" formájában (Indokolás, 67. pont) (a szerzők kiemelése). E rendelkezések azt mutatják, hogy az Egyezmény tilt egy bizonyos „adminisztratív ellenőrzést". Ez mindazonáltal egyrészt nem jelenti azt, hogy az államok „nem hozhatnak más rendelkezéseket arról, hogy információt szerezzen a saját és egy másik szerződő állam területén folyó adatáramlásról, például az adatkezelő kötelező nyilatkozata formájában"

[136] 29-es munkacsoport: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 1998. július 24. 9. oldal.
[137] Ugyanott.
[138] Az irányelv 3. cikk (2) bekezdés második fordulata ezt az irányelv hatályából kizárja.
[139] Az Európai Unió szintjén a 2008/977/JAI határozat a rendőrségek és bíróságok bűnügyi együttműködése keretében kezelt személyes adatok védelmével foglalkozik (lásd Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 1. cikk 2. bek.). Ez azonban nyilvánvalóan nem vonatkozik arra az esetre, amikor az illetékes külföldi hatóságok az Európia Unió polgárát érintő személyes adatokat megkaphatják a kérdéses harmadik államban telephellyel rendelkező, joghatósága alá tartozó szolgáltató által kezelt adatbázisokból. Márpedig ezt a kérdést érdemes lenne a megfelelőségre való tekintettel megvizsgálni. Ugyancsak ide tartozik az Egyesült Államok harmadik fél doktrínája. Ezt a doktrínát is fontolóra kellene venni az Európa Tanács Egyezménye szerint elvégzett megfelelőségi vizsgálat során.

(Indokolás, 67. pont). Másrészt, mint fentebb rámutattunk, az államok ezt az ellenőrzést személyes adatok vagy kezelések bizonyos fajtáira is alkalmazhatják[140].
A jelenleg hatályos szabályok rendszere, mindent összevéve, meglehetősen bonyolult. Mégis meg kell jegyezni, hogy a tárgyal rendelkezéseken túlmenően, A 108. Egyezmény és Jegyzőkönyve nem tartalmazza azt az esetet, amely egy szerződő állam jogának rögzítené a személyes adatok kezelésére vonatkozó alkalmazhatóságát. Ez a megállapítás mind a harmadik, mind pedig más szerződött államokba irányuló határátlépő adatáramlás tekintetében jelentős. Ez utóbbiakra nézve az Egyezmény Indokolása azt is elismeri, hogy „olykor nem könnyű megállapítani, melyik államnak van joghatósága és melyik nemzeti jog alkalmazandó" (10. pont), hangsúlyozva, hogy „a 'közös mag' [mármint az Egyezmény közös magja] a Felek törvényeinek összehangolását eredményezik, ami következésképpen csökkenti a jog és igazságszolgáltatás konfliktusainak lehetőségét" (20. pont). Így azonban **a 108. Egyezmény és Jegyzőkönyve nem küszöböli ki ezeket a konfliktusokat, nem határozza meg sem az adatvédelem esetében alkalmazandó jogot, sem az illetékes bíróságot, amely a vitás ügyeket eldöntheti**. Márpedig a technika környezet imént jellemzett szakadása e szabályok jelentőségét igazolja. Az alkalmazandó joggal és az illetékes joghatósággal kapcsolatos rendelkezések összhangjának kérdésében az Európai Unió jogrendszere a legfejlettebb.

### 13.3 A személyes adatok védelmére alkalmazandó jog: a 95/46 irányelv és a 864/2007 rendelet (Róma II)[141]

A személyes adatok védelmére alkalmazandó jog tekintetében a 95/46 irányelv 4. cikke az a rendelkezés, amelyik a legmesszebbre megy a személyes adatok kezelésére alkalmazandó jogot meghatározó szabályok összhangjának megteremtésében[142]. Ez a rendelkezés határozza meg azokat az eseteket, melyekben a tagállamoknak nemzeti jogszabályaikat kell alkalmazni. Meghatározza továbbá, a határátlépő adatáramlást szabályozó 25. és 26. cikkel összefüggésben az adatok európai védelmére vonatkozó jog alkalmazhatóságának területét[143].
Mindazonáltal először is *a priori* nem határozza meg, melyek azok az esetek, melyekben a tagállamoknak nemzeti jogszabályaikat kell alkalmazni. Másképp fogalmazva, ha egy tagállamnak nem kötelező saját nemzeti jogát alkalmazni, az irányelv nem határozza meg, melyik jogot kell alkalmaznia. Kivéve, ha ezt az alkalmazandó jogot meghatározó törvényi konfliktust eldöntő tényleges bilaterális szabályként értelmezzük, adott esetben az Európai Unió jogrendje szerint kell eljárni, hacsak nem egy unilateralista értelmezést alkalmazunk. E

[140] Ha ez az ellenőrzés az Egyezmény szerződő államai között megengedett, úgy véljük, *a fortiori* megengedett a harmadik államok tekintetében a Kiegészítő Jegyzőkönyv szerint is. A Jegyzőkönyv tiltja az adatáramlás engedélyezését, ha a címzett állam nem garantálja a megfelelő védelmet. Nem tiltja azonban egyes adatok áramlásának tiltását, még ha a címzett harmadik állam a megfelelő védelmet nem is garantálja.
[141] Az Európai parlament és a Tanács 2007. július 11-i 864/2007/EK Rendelete a szerződésen kívüli kötelmi viszonyokra alkalmazandó jogról (Róma II.).
[142] Az adatvédelemre alkalmazandó jog tárgyában, különös tekintettel a 95/46 irányelv 4. cikkeére lásd: C. KUNER, « Data Protection Law and International Jurisdiction on the Internet (Part 1) », *International Journal of Law and Information Technology*, 2010, n°18 (2), pp. 176-193 ; C. KUNER, « Data Protection Law and International Jurisdiction on the Internet (Part 2) », *International Journal of Law and Information Technology*, 2010, n°18 (3), pp. 227-247 ; J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *Revue Européenne de Droit de la Consommation*, 2010, n°2, pp. 255-270; F. RIGAUX, « Libre circulation des données et protection de la vie privée dans l'espace européen », in *La protection de la vie privée dans la société del'information, L'impact des systèmes électroniques*, P. Tabatoni (dir.), t. 2, P.U.F., Paris, 2000, pp. 25-40 .
[143] A közösségi jogból levezett területi alkalmazhatóság meghatározása tárgyában lásd: S. FRANCQ, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruylant, L.G.D.J., Bruxelles, Paris, 2005.

két esetben tehát nem kellene csak az alkalmazandó jogot meghatározni 95/46 irányelv területi hatályával lefedett esetekben[144].
*Melyik* tehát az az esetlegesen alkalmazandó nemzeti jog azokban az esetekben, melyet az 95/46 irányelv hatálya kizár. A 29-es Munkacsoport rámutat, hogy: „vannak helyzetek, melyek az irányelv hatályán kívül esnek. Ez az az eset, amikor a nem az EU-ban telephellyel rendelkező kezelők személyes adatok gyűjtésére és további feldolgozására irányuló tevékenységükkel az EU területén lakó személyeket céloznak meg. Erről van szó például akkor, ha online kereskedők és effélék „helyi ízléshez" igazított hirdetéseket vagy web helyeket használnak, *közvetlenül megcélozva* (méghozzá saját nyelvükön) az EU polgárokat. Ha ezt anélkül teszik, hogy az EU-ban elhelyezett eszközöket használnának, a 95/46 irányelv nem alkalmazható"[145] (a szerzők kiemelése). *Mi* a szerepe ebben az esetben a nemzeti jognak.
Másodszoris az adatok kezelése szerint és a felelős kezelő telephelye szerint ugyanazt a felelős kezelőt több, különféle nemzeti jog köthetné. Ezek alkalmazása bonyolult lehet. Ezenkívül a tekintetbe vett elemeknek az alkalmazandó jogra való visszavezetése, tudniillik az Unió területén az adott kezelés céljára használt eszközök kritériuma és az adott kezelési tevékenység végzésére szolgáló telephely tekintetében, komolyan megnehezíti annak értelmezését és alkalmazását a bevezetőben jellemzett három részre szakadt környezetben. Az Európai Bizottság által nem régiben megrendelt tanulmányban például az olvasható, hogy: „a 4. cikk (1) bek. (a) pontjában rögzített szabályok felettébb zavarosak, alkalmazásuk az új globális és technikai környezetben lehetetlen" [146]. Másrészt a kezelés céljaira használt eszközök helyének tekintetbe vétele a technika fejlődése következtében nem feltétlenül alkalmazható[147]. A tanulmány szerint továbbá „az irányelv alkalmazandó jogra vonatkozó rendelkezései ténylegesen lehetetlen alkalmazni azokra a nem EU/EGT területen működő vállalkozásokra és szervezetekre, amely tevékenysége Európára is kiterjed, különösen ha tevékenységüket az Interneten folytatják (mint azt szinte valamennyi teszi napjainkban és tenni fogja a jövőben is"[148].
Végül harmadszor: az előbb mondottakkal összefüggésben a 95/46 irányelv 4. cikkének érvényesítése végül is attól függ, hogyan ültették át a tagállamok. A 95/46 irányelv 4. cikke tehát nem ad teljes választ az Európai Unió jogrendszerében az adatok védelmére alkalmazandó jog kérdésére.

---

[144] Ebben az esetben a 95/46 irányelv területi hatályával kapcsolatos helyzetekben az irányelv *in fine* meghatározza az alkalmazandó jogot. Ha ezt a rendelkezést a tagállamok, természetesen *mutatis mutandis*, betű szerint átültetnék, elvileg minden, területi hatállyal kapcsolatos kezelést egyetlen egy tagállam jogának kellene alávetni (pl. azon állam jogának, melynek területén az a felelős kezelő telephelyet létesített, melynek tevékenységi köre a személyes adatok kezelését is felöleli. Logikus lenne, hogy a tagállamok, a 95/46 irányelvvel való összhang következtében, kölcsönösen elismerik e tárgyról rendelkező jogszabályaikat. Mindazonáltal meg kell jegyezni, hogy ez az összhang az irányelv által a tagállamokra hagyott mozgástérre való tekintettel nem küszöböli ki a nemzeti jogszabályok között mutatkozó eltéréseket. Ez még inkább igaz a 108. Egyezmény részes államaira nézve.

[145] Article 29 Working Party and Working Party on Police and Justice, WP 168, The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data, adopted on 1 December 2009, pp. 10-11.

[146] Lásd LRDP Kantor Ltd, in association with Centre for Public Reform, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final report.
Forrás: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 2010. január, 37. pont.

[147] A *cloud computing* (számítási felhő) esetében például a kezelés eszközeinek (különösen a tárolóknak és a programoknak) a helyét valós időben szolgáltatásai optimális hatékonysága és informatikai erőforrásai legjobb helyének megválasztása érdekében a szolgáltató határozza meg.

[148] Fentebb idézve: LRDP Kantor Ltd, in association with Centre for Public Reform, 39. pont.

Érdemes rámutatni, hogy az adatvédelem itt nem követi ugyanazokat a szabályokat, mint a magánélet esetében alkalmazandó jog meghatározása, melyet az EEJE 8. cikke rögzít[149]. A szerződésen kívüli kötelmi viszonyokra alkalmazandó jog a magánélethez való alapvető jog sérelme esetében egyébként nem határozottabb a szerződésen kívüli kötelmi viszonyokra alkalmazandó jogról szóló „Róma II" rendeletben sem[150]. Másképpen fogalmazva erre a kérdésre a tagállamok nemzeti jogszabályai adnak választ. Belgiumban például, az irányelvben elfogadott unilateralista logika jegyében, a magánéletről szóló törvény unilaterálisan határozza meg területi hatályát, míg Belgiumnak a nemzetközi magánjogról szóló törvénye egy multilaterális – a minden esetben alkalmazandó (külföldi vagy belga) jogot meghatározó – szabályban rendelkezik arról, mely jog szabályoz egy olyan kötelezettséget, amelyet a magánéletet sérelméből adódóan kell érvényesíteni[151]. Másképpen fogalmazva: a magánélet sérelmének megállapítása elvileg az EEJH 8. cikkének horizontális (minden esetben indirekt) hatályán alapszik, a jogorvoslatra pedig az Európai Unió tagállamának a jogszabályait lehet alkalmazni, míg az adatvédelemre az EU-n kívüli harmadik állam jogszabályait. Éppígy egy fogyasztó – érintett személy – és egy vállalkozó – felelős kezelő – között fennálló szerződéses viszonyokra a fogyasztó szokásos tartózkodási helyéül szolgáló állam jogát lehet alkalmazni[152], míg az adatvédelem esetében az EU-n kívüli harmadik állam joga az irányadó.
Végül még egy olyan területen, ahol a jogszabályokat *a priori* harmonizálták és ahol az államoknak kölcsönösen el kell ismerniük jogszabályaikat, az adatvédelemre alkalmazandó jog kérdése bonyolult marad és nem szükségképpen garantálja a jogbiztonságot az érintett személyt és a felelős kezelőt ért sérelem esetén. Ez még inkább igaz a 108. Egyezmény, sőt mi több, az EEJE részes államai közötti viszonyokra is. A jövőben tehát még nagyobb hangsúlyt kell adni annak a potenciális szerepnek, amelyet az EEJE 8. cikke játszhat az adatok és a magánélet védelme esetében alkalmazandó jogmeghatározásában.

### 13.4 Az EEJE 8. cikke hatása a magánéletre és az adatvédelemre alkalmazandó jog meghatározására.

Mindenek előtt érdemes felidézni az adatvédelem és a magánélet védelme között fentebb jellemzett jogi kapcsolatot (lásd 1.1.1 pont). Az Európai Emberi Jogi Bíróság több alkalommal elismerte az EEJE 8. cikkének alkalmazását a személyes adatok kezelésére[153], és egyebek mellett hivatkozott a 108. Egyezményre is. Ez két szempontból is érdekes. Egyrészt elvileg ebből az következik, hogy az EEJ Bíróság szankcionálhatja az EEJE-hez csatlakozott állam eljárását a személyes adatok kezelésének szabályozására vonatkozó indokok alapján. Ebben az esetben a 108. Egyezmény és Jegyzőkönyve alkalmazása nem tartozik a Bíróság hatáskörébe. Ugyanígy megjegyzendő, hogy a Lisszaboni Szerződés előirányozza, hogy az

[149] Rámutathatunk arra, hogy bizonyos mértékben – mert az adatvédelem nem korlátozódik a magánélet védelmére – az egyént a személyes adatok kezelése tekintetében védő szabályozás az EEJE 8. cikke horizontális kiterjesztéséhez vezet. Lásd lentebb az EEJE 8. cikke esetleges hatását a nemzetközi magánjogi szabályokra.
[150] Lásd:"Róma II" rendelet, 1. cikk (2) g) pont.
[151] Lásd: article 99 de la loi du 16 juillet 2004, portant le Code de droit international privé, *Monit.B.* du 27 juillet 2004, et l'article 3 bis de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Monit.B.* du 18 mars 1993.
[152] Lásd az Európai Parlament és a Tanács 2008. június 17-i 593/2008/EK rendelete a szerződéses kötelezettségekre alkalmazandó jogról (Róma I.) 6. cikk; J.-P. Moiny et B. De Groote, „'Cyberconsommation' et droit international privé", *Revue du Droit des Technologies de l'Information*, 2009, n°37, pp. 5-37.
[153] Lásd Cour eur. D.H., 16 février 2000, *Amann c. Suisse*, no 27798/95, 16 février 2000 ; Cour eur. D.H., 4 mai 2000, *Rotaru c. Roumanie*, no 28341/95 ; Cour eur. D.H., 31 mai 2005, *Antunes Rocha c. Portugal*, n°64330/01 ; Cour eur. D.H., 10 octobre 2006, *LL c. France*, n°7508/02 ; Cour eur. D.H., 4 décembre 2008, *Marper v. Royaume-Uni*, n°30562/04 et 30566/04 ; Cour eur. D.H., 2 septembre 2010, *Uzun c. Allemagne*, n°35623/05.

Európai Unió csatlakozzon az EEJE-hez[154], ami növeli az EEJ Bíróság szerepét az Európai Unióval szemben[155], melynek a jogszabályai ezentúl a Bíróság előtt vitathatók. Másrészt ez azzal jár, hogy azokat az államokat, amelyek még nem írták alá vagy nem ratifikálták ezeket az eszközöket, mégis kötelezik a személyes adatok kezelésére vonatkozó szabályok az EEJE 8. cikke alapján.
Így az EEJ Bíróság az EEJE 8. cikke alapján ellenőrizhet[156] és – adott esetben szankcionálhat – egy államot, ha az valamely ítéletében, adott esetben, külföldi jogot alkalmaz, aminek okából nem ismeri el az EEJE 8. cikkét az érintett peres egyén sérelmére[157], aki az EEJE 1. cikke szerinti állam joghatósága alá tartozik [158]. „Ha egyszer az állam gyakorolja kompetenciáját, [ ] az Egyezménnyel összhangban kell eljárnia"[159]. Ilyen típusú esetben a külföldi jogot egy közrend alóli kivételt megengedő típusú mechanizmus révén el kell vetni. Logikus, hogy ha ez a „külföldi jog" az Európa Tanács egy másik államának a joga, akkkor ennek a kivételnek a szerepét korlátozni kell (*a fortiori* ha a kérdéses állam ugyancsak a 108. Egyezményhez részes fél, és még inkább, ha az államok az Európai Unió tagjai). Ez a helyzet elvileg akkor, ha a 108. Egyezményhez nem csatlakozott harmadik állam nem garantál megfelelő védelmet, ami viszont egy ilyen kivétel esetében elengedhetetlen. Ezekben az esetekben meggondolandó, hogy a kérdéses peres ügyben a 108. Egyezmény „kemény magját" kellene alkalmazni, adott esetben szembenézve az Európai Emberi Jogi Bíróság szankciójával, amely valószínűleg úgy ítél, hogy a 108. Egyezmény kemény magját az EEJE 8. cikke garantálja. Ugyanez várható az adatvédelem valamennyi szabálya tekintetében, melyek alól a 8. cikk alapján a Bíróság felmentést adott.

### 13.5 Következtetés: a 108. Egyezménynek az alkalmazandó jogot meghatározó szabálya

A 108. Egyezmény célja, hogy „minden egyes Fél területén minden egyén számára, tekintet nélkül nemzetiségére vagy lakóhelyére, biztosítva legyen, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák a személyes adatainak gépi feldolgozása során" (1. cikk). Az Egyezmény így az adatvédelem anyagi jogának minimális közös keretét garantálja, amely, adott esetben, mint fentebb kifejtettük, bizonyos hiányosságokat mutat. Fejtegetéseink minden kétséget kizárva bemutatták a nemzetközi magánjog tekintetében felmerült kérdések komplexitását, különösen az alkalmazandó jog vonatkozásában.

---

[154] „Az Unió csatlakozik az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményhez. Ez a csatlakozás nem érinti az Uniónak a Szerződésekben meghatározott hatásköreit." /Az Európai Unióról szóló szerződés, 6. cikk. (2) bek./. A csatlakozási tárgyalások 2010. július 7-én kezdődtek, lásd: http://www.coe.int/t/dc/files/themes/eu_and_coe/default_EN.asp?

[155] Lásd: Parliamentary Assembly, Committee on Legal Affairs and Human Rights M.-L. Bemelmans-Videc, (rapporteur), „The accession of the European Union/European Community to the European Convention on Human Rights", 18 March 2008., letölthető: http://assembly.coe.int/ASP/Doc/DocListingDetails_E.asp?DocID=12321, 8. oldal, 12. pont.

[156] Az ellenőrzésről lásd P. MAYER, "La Convention européenne des droits de l'homme et l'application des normes étrangères", *Rev. crit. dr. internat. privé*, 1991, p. 664.

[157] Az EEJB hatása a jogszabályi rendelkezések konfliktusának rendezése tárgyában lásd: L. GANNAGÉ, "A propos de l' "absolutisme" des droits fondamentaux", in *Vers de nouveaux équilibres entre ordres juridiques – Liber amicorum Hélène Gaudemet-Tallon*, Paris, Dalloz, 2008, pp. 265-284.

[158] Lásd S. KARAGIANNIS, « Le territoire d'application de la convention européenne des droits de l'homme, *Vaetera et nova* », *Rev. trim. dr. h.*, n°61, 2005, pp. 33-120. Voy. not. Cour eur. D.H., 23 mars 1995, *Loizidou c.Turquie* [GC], n°15318/89 ; Cour eur. D.H., 12 décembre 2001, *Bankovic et al. c. Belgique et al.* [décision GC], n°52207/99 ; plus récemment, Cour eur. D.H., 29 mars 2010, *Medvedyev et al. c. France* [GC], n°3394/03.

[159] G. COHEN-JONATHAN et J.-F. FLAUSS, « Cour européenne des droits de l'homme et droit international général », *Annuaire français de droit international*, n°47, 2001, p. 438.

A nemzetközi magánjog közös szabályai természetesen jól szolgálhatnák az idézett célt. Egyrészt növelnék a jogbiztonságot, és ezáltal természetesen az anyagi jogi rendelkezések alkalmazásának fokozott hatékonyságához is[160] Egyértelmű, hogy az alkalmazandó jogi rendelkezések szabatos voltának hiánya feltehetően rontja az anyagi jogi rendelkezések hatékony alkalmazását, mivel jelentősen – talán túlságosan is – komplikálja a vállalkozások működését. Így az Európai Unió területén, ahol a szabályozás célja az egységes piac megteremtése, egy még inkább szükség van egy közös szabályra.
Másrészt egy nemzeti bíróságnak hiányosnak mutatkozhat az egyén védelme, ha a bíró egy kevesebb (nem megfelelő) védelmet nyújtó külföldi jogszabályt alkalmazna. Ilyen esetben egy közrend alóli kivételt megengedő típusú mechanizmus lehetővé tenné *in casu*, hogy a nemzeti bíróság egy külföldi jogszabályi rendelkezés alapján ne fossza meg az egyént a 108. Egyezmény „kemény magjának" teljes vagy részleges alkalmazásától vagy az EEJE 8. cikkében garantált jogoktól.
Mindemellett két főbb nehézség mutatkozik az alkalmazandó jogot meghatározó szabályok esetleges definiálása tekintetében a 108. Egyezmény kontextusában. Egyrészt politikailag várható-e, hogy az Európa Tanács tagállamai megegyeznek egy ilyen szabály elfogadásában? Gondoljunk csak arra, hogy a Madridi Nyilatkozat elfogadása alkalmával nem volt egyetértés a nemzetközi magánjog kérdésében, és hogy minden ilyen esetben egy ilyen szabály elfogadása szükségessé teszi az Európai Unióval való koordinációt. Az Egyezményhez csatlakozott államok eltérő anyagi jog szabályai e tekintetben minden bizonnyal nehézségeket okoznak.
Másrészt a helyzetek, a szereplők és a jogi ügyek sokfélesége egy adatvédelmi perben komplikálják a nemzetközi magánjogi kérdéseket szabályozó rendelkezések megállapítását. Az alkalmazandó jog megállapítását valószínűleg segítheti egy olyan szabály, amely előirányozza a szubszidiaritás elvének alkalmazását. Ez a szabály nevezetesen tekintettel lehet az jogrendben mutatkozó eltérésekre (európai, Európa Tanács – EEJE –, Európa Tanács – 108. Egyezmény és Kiegészítő Jegyzőkönyve –, „széles értelemben" nemzetközi –, a harmadik államokhoz való viszony). Egy olyan eszköznek, mint a 108. Egyezmény, megfelelő rugalmassággal lehetővé kellene tennie az államoknak (és szervezeteiknek), hogy tekintetbe vegyék a fentebb már jellemzett három részre szakadt környezetet, és józanul döntsenek a jogok, szabadságok és az egyének érdekei tekintetében, figyelembe véve a társadalom széles értelemben vett érdekeit is. A nemzeti bíróságnak minden esetben rendelkeznie kell a helyzet értékeléséhez szükséges eszközökkel, ami elvileg a szabályok értelmezése tekintetében *in casu* megilleti, bármi is legyen az eredetük (adott esetben egy nemzetközi bíró ellenőrzése– az Európai Unió Bírósága vagy az EEJ Bíróság az EEJE 8. cikke alkalmazása tekintetében – mellett). Még szabatosabban kifejezve tehát arról van szó, elérhető-e – *elméletileg és gyakorlatilag* – egy, az adatok védelmére alkalmazandó jogot meghatározó közös szabály megfogalmazása.
Figyelembe véve valamennyi előbbi megfontolást, feltehetjük a kérdést, hogy **az adatvédelem tárgyában alkalmazandó jogot meghatározó szabály hiánya valóban hiányossága-e a 108. Egyezménynek, hiszen a tagállamok nemzetközi magánjoga szabályozza ezt a kérdést**. Az államok legtöbb jogszabálya hasonló, legalábbis e szabályokkal kapcsolatos következmények jelentősége tekintetében. Itt újra emlékeztetünk arra, hogy az Európa Tanácshoz nem tartózó államok csatlakozhatnak a 108. Egyezményhez (23. cikk) és ezt követően a Kiegészítő Jegyzőkönyvhöz (3. cikk 2. pont). Végül is minden

[160] Az Európai Unió szintjén a 95/46 irányelv 4. cikkével kapcsolatban nem régiben rámutattak arra, hogy „mindezek a problémák súlyosak és akadályozzák a nemzetközi tevékenységet folytató vállalkozásokat és szervezeteket abban, hogy megfeleljenek az adatvédelmi szabályoknak és elveknek. Ezek a problémák még súlyosabban az új, általában internacionalizált szocio-technikai környezetben, különösen (de nem csak) az Internet tekintetében". LRDP Kantor Ltd, in association with Centre for Public Reform, 42. pont.

esetben a peres ügyben alkalmazandó jogról a bíró dönt. Mindazonáltal az adatvédelemre alkalmazandó jogot meghatározó szabályokról folyó vita nemcsak hasznos, hanem elengedhetetlen is: először is azért, mert az egyénnek hatékonyabb védelmet biztosít, másrészt mert növeli a jogbiztonságot a felelős kezelő szempontjából. Mindezért az Európa Tanács **Miniszteri Tanácsának az ajánlása** legalábbis gazdagítaná a vitát és hasznos lenne az alkalmazandó jogi rendelkezések harmonizálására irányuló kutatások számára is.

### 13.6 A határátlépő adatáramlásra vonatkozó kiegészítő elemek

Mindazon túl, amit a határátlépő adatáramlósról fentebb már elmondtunk,
Az új technikai környezetben **elengedhetetlen tisztázni, mit értünk határátlépő adatáramláson**. Különösen azt kell megvizsgálni, hogy a Kiegészítő Jegyzőkönyv 2. cikke[161] „továbbítás" fogalma kiterjed-e az adattal való rendelkezésre bocsátásra, terjesztésre és közzétételére is. Ez a pontosítás kulcsfontosságú az adatoknak egy Internet-oldalon való rendelkezésre bocsátása tekintetében[162].
A Kiegészítő Jegyzőkönyv 2. cikke[163] tartalmazza a határátlépő áramlás kritériumaként a „megfelelő védelem" elvét. Kétség kívül érdemes lenne hozzáfűzni, hogy **a megfelelőség meghatározása változóban van**, mert a megfelelőséget nem lehet egyszer s mindenkorra meghatározni, hanem csak az Egyezményt értelmező, a strasbourgi bíróság által hozott ítéleteknek és az újabban elfogadott jogszabályoknak (ajánlások, kiegészítő jegyzőkönyvek) a tükrében.
A Kiegészítő Jegyzőkönyv indokolása a megfelelőség értékelésének pontosításáról így szól: „27. A védelem szintjét minden egyes továbbításra vagy továbbítási kategóriára nézve esetről esetre értékelni kell. [ ] 28. A megfelelőség értékelése hasonló módon egy egész államra vagy szervezetre nézve is elvégezhető, aminek alapján e rendeltetési helyekre irányuló valamennyi adattovábbítás megengedhető. Ebben az esetben a védelem megfelelő szintjét minden fél illetékes hatóságai állapítják meg." **Ez helytállónak tekinthető akkor is, ha a megfelelőség értékelése** egy harmadik állam által nyújtott védelemre vonatkozik. Ez az „illetékes hatóság" teljes körű értékelésére vonatkozik, de nem szól arról, mit jelent az esetről esetre végzett értékelés.

## 14. Az ellenőrző hatóságok

Nemrégiben egy minőségi mérleg készült az adatvédelmi hatóságokról:
„Az AVH-k kiválóan ismerik a jogszabályokat, és hasznos tanácsokat adnak alkalmazásukra, de végrehajtásukat tekintve nem túl hatékonyak: az adatvédelmi jogszabályoknak való megfelelés „ellenőrzése" általában gyenge és hatástalan."[164] „Ez az összehasonlító jelentés az EU 27 tagállamának aktuális, személyes adatokat védő rendszerében mutatkozó hibákat veszi

[161] „Minden egyes Fél csak akkor engedélyezheti a személyes adatok továbbítását olyan címzett részére, aki vagy amely olyan állam vagy szervezet joghatósága alá tartozik, amely nem részese az Egyezménynek, ha az az állam vagy szervezet megfelelő szintű védelmet biztosít a célzott adattovábbítás során."
[162] Lásd az EEJB Lindqvist ügyben hozott ítéletét, amely az Internet környezetben végrehajtott továbbítás fogalmának vitáját váltotta ki, melyre a Bíróság ügyetlenül válaszolt: C.J.C.E., 6 novembre 2003, (Lindqvist), C-101-01, *Rec*. p. I-12971. Az ítélet kritikáját lásd: v. C. de TERWANGNE, « Arrêt Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I*., 2004, n° 19, pp. 67 et s.
[163] „Minden egyes Fél csak akkor engedélyezheti a személyes adatok továbbítását olyan címzett részére, aki vagy amely olyan állam vagy szervezet joghatósága alá tartozik, amely nem részese az Egyezménynek, ha az az állam vagy szervezet megfelelő szintű védelmet biztosít a célzott adattovábbítás során."
[164] LRDP Kantor Ltd, in association with Centre for Public Reform, op. Cit. 104. pont.

számba. A hiányosságokat az adatvédelmi hatóságok függetlensége, erőforrásokkal való ellátottsága és hatásköre tekintetében figyeltük meg."[165]

**E megállapításokból** kétség kívül **le kellene vonni a tanulságokat, melyek alapján fontolóra kellene venni a jogszabályok módosítását, különösen a hatóságok függetlenségét garantáló kritériumok tekintetében**. Indokolt lenne e hatóságok hatáskörét **kibővíteni**, például azzal, hogy **véleményt formálhassanak a magánélettel kapcsolatos jogszabályi rendelkezések tervezetéről, melynek figyelembe vétele akár kötelező, akár nem**.

A Madridi Nyilatkozat a maga részéről hangsúlyozza, hogy szükség van „független adatvédelmi hatóságokra, amelyek a jogszabályi keretek között átlátható módon és bármiféle kereskedelmi érdek vagy politikai befolyásolás nélkül hozzák meg döntéseiket".

Az európai adatvédelmi biztos is levonta az aktuális helyzetből adódó következtetéseket: „Az adatvédelemmel szemben jelentkező új kihívások egységesebb és hatékonyabb felügyeletet igényelnek. Az új keretnek ezért egységes szabályokkal kell garantálnia a függetlenséget, a reális hatáskört, konzultációs szerepet a jogszabályalkotásban és annak lehetőségét, hogy munkaprogramját maga alakítsa ki, különösen a panaszok kezelését illető prioritások megállapítása tekintetében. Erősíteni kell továbbá az adatvédelmi hatóságok nemzetközi együttműködését."[166]

Megfontolandó továbbá, hogy **a jogszabályok az ellenőrző hatóságokon túlmenően „adatvédelmi tisztviselők" kinevezéséről is rendelkezzenek**, akik szervezeteken, intézményeken, vállalkozásokon belül a hatósági ellenőrzést egészítenék ki. E tisztviselők esetleg az adatvédelem elvei és szabályai fokozottabb betartását garantálnák szervezetükön belül.

Végül valamennyi érdekelt fél úgy véli, hogy **erősíteni kell a párbeszédet és a nemzetközi együttműködést, különösen a felügyelő hatóságok között**.

Az OECD Ajánlása a magánélet védelmét szolgáló jogszabályok alkalmazásáról a határon túlnyúló együttműködésben (2007. június 12.) javasolja, hogy „A határon túlnyúló együttműködést folytató tagországok a magánéletet védő jogszabályok alkalmazása érdekében megfelelő intézkedéseket tegyenek, többek között

- fejlesszék a magánéletet védelmére vonatkozó jogszabályok alkalmazásának nemzeti kereteit;
- dolgozzanak ki hatékony nemzetközi mechanizmusokat a magánéletet védelmére vonatkozó jogszabályok alkalmazását támogató határon átnyúló együttműködés elősegítésére;
- kölcsönösen támogassák egymást a magánéletet védő jogszabályok alkalmazásában, különös tekintettel a tájékoztatásra, a panaszok továbbítására, a vizsgálatok lefolytatására és az információcserére, s mindezt megfelelő garanciák mellett;
- szervezzék meg azoknak a feleknek a kapcsolatát, akik a magánéletet védő jogszabályok alkalmazása fejlesztését célzó megbeszélések és tevékenységek iránt érdeklődnek.

[165] Comparative Legal Study on assessment of data protection measures and relevant institutions, rapport commandé par l'Agence des droits fondamentaux (FRA) de l'Union européenne, Synthèse, 2009, para. 8.

[166] P. Hustinx: „30 years after: the impact of the OECD Privacy Guidelines", Joint ICCP-WPISP Roundtable, Paris, 10 March 2010, Session 3: The Privacy Guidelines in the Current Environment "Recent developments in the European Union". Letölthető: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-03-10_Privacy_guidelines_EN.pdf