

PhD DOLGOZAT

Mező István

Miskolc  
2009

**Miskolci Egyetem**  
**Állam- és Jogtudományi Kar**  
**Deák Ferenc Állam- és Jogtudományi**  
**Doktori Iskola**

**Mező István**

**SZEMÉLYES ADATOK VÉDELME**  
**AZ EURÓPAI UNIÓ JOGÁBAN ÉS MAGYARORSZÁGON**

(PhD értekezés)

**Deák Ferenc Állam-és Jogtudományi Doktori Iskola**

Doktori Iskola vezetője: Dr. Bragyova András DSc. egyetemi tanár

Doktori program címe: A magyar állam- és jogrendszer; jogtudomány továbbfejlesztése; különös tekintettel az európai fejlődési tendenciákra

Tudományos vezető: Dr. habil. Bragyova András egyetemi tanár

MISKOLC  
2009

## Tudományos vezető véleménye

Mező István doktori értekezése az adatvédelmi jog fontos kérdéseivel foglalkozik. Feldolgozza az adatvédelmi jog kialakulását, alkotmányos alapjait, ezen belül a magyar adatvédelmi jog kialakulását, különösen az Adatvédelmi törvény elfogadáshoz vezető utat; külön fejezet foglalkozik az adatvédelmi biztossal. Ugyancsak bemutatja az adatvédelem nemzetközi jogi szabályainak kialakulását Európában, illetve a gazdaságilag fejlettebb államokban.

A dolgozat részletesen bemutatja az Európai Unió adatvédelmi jogalkotását, az EU adatvédelmi irányelvét és az annak elfogadása utáni változásokat, egészen az Amszterdami Szerződésig. Erénye a dolgozatnak, hogy bemutatja a bírói gyakorlatot: az Európai Bíróság éppúgy, mint az Emberi Jogok Európai bírósága vagy magyar Alkotmánybíróság gyakorlatát. Emellett a külföldi jogok bemutatásakor is figyelembe veszi a bírói gyakorlatot. Ez mindenütt nagyon fontos, az adatvédelemben pedig, a benne használt fogalmak elkerülhetetlen általánossága és meghatározatalansága miatt külön jelentőséggel bír.

Az értekezés külön erénye, hogy jelentős része foglalkozik az adatvédelmi jog, amint nevezi szektorális kérdéseivel. Az adatvédelmi jog érvényesülésével kapcsolatos kérdések egész sorát mutatja be: foglalkozik a munkahelyi adatvédelemmel, a távközlés adatvédelmi kérdéseivel, az egészségügyi adatok védelmével. Kitér a sajtószabadság és az adatvédelem kapcsolatára, különös tekintettel a közszereplők személyes adatai és jogai védelmére. Nem kevésbé fontosak az értekezés fejtegetései a kereskedelmi adatvédelemről és az internettel kapcsolatos adatvédelmi kérdésekről. Külön fejezet szól az elektronikus térfigyelő és más hasonló biztonsági rendszerek adatvédelmi kérdéseiről.

A dolgozat, amint címe is ígéri, a magyar jog kimerítő bemutatása mellett feldolgozza az Európai Unió jogának a vizsgált kérdésekkel kapcsolatos szabályait és bírói gyakorlatát.

Miskolc-Budapest, 2008. február 21.

Dr. habil Bragyova András

## Tartalomjegyzék

Tudományos vezető véleménye

### I. RÉSZ: ALAPOK ÉS KERETEK

1. AZ ADATVÉDELEM PROBLEMATIKÁJA	5
1.1. Bevezető	5
1.2. Kutatás áttekintése és célja	9
1.3. Drittwirkung – az alapjogok horizontális hatásai	12
1.4. Drittwirkung hatás az adatvédelemben (hipotézis)	16
1.5. A kutatás módszertana	17
2. A SZEMÉLYES ADATOK VÉDELMÉNEK ALAPFOGALMAI	19
2.1. Adatvédelem, de miért?	19
2.2. A privacy fogalmáról	21
2.3. Adatvédelem fejlődésének történeti áttekintése	25
2.4. Az adatvédelem fogalmáról	33
2.5. A személyes adat fogalma	36
2.6. Különlegesen érzékeny adatok köre	39
2.7. Adat, információ, titok	42
2.8. Személyes adatok reindividualizálhatósága	45
2.9. Élő természetes személyek adatai	48
2.10. Jogi személyek jogvédelme és az adatvédelem	50
Az I. rész összegzése: Az adatvédelem fogalmi keretei	53

### II. RÉSZ: SZEMÉLYES ADATOK VÉDELME NEMZETKÖZI SZÍNTÉREN ÉS AZ EURÓPAI UNIÓBAN

3. SZEMÉLYES ADATOK VÉDELME NEMZETKÖZI SZÍNTÉREN	55
3.1. Az OECD Tanácsának adatvédelmi irányelvei	55
3.2. Az ENSZ adatvédelmi állásfoglalása	56
3.3. Az Európai Emberi Jogi Egyezmény 8. cikkelye	58
3.3.1. Leander-ügy	59
3.3.2. Klass és társai-ügye	60
3.3.3. Amman-ügy	61
3.3.4. Caroline Von Hannover-ügy	62
3.4. Az Európa Tanács Adatvédelmi Egyezménye	66
4. A SZEMÉLYES ADATOK VÉDELME AZ EURÓPAI UNIÓBAN	72
4.1. Személyes adatok védelmének alapjai az Európai Unióban	72
4.1.1 Alapjogok fejlődése az Európai Unióban	72
4.1.2 Európai Unió Alapjogi Chartája	73
4.2. Az Európai Unió adatvédelmi irányelve	74
4.2.1. A 95/46/EK irányelv előzményei	74

4.2.2. Az Európai Unió adatvédelmi irányelve céljai	76
4.2.3. Az irányelv hatálya és fogalmi rendszere	78
4.2.4. Adatvédelmi elvek az irányelvben és az adatkezelés jogcímei	83
4.2.5. Különleges adatok köre	85
4.2.6. Érintettek tiltakozási jogai	87
4.2.7. Automatizált egyedi döntések tilalma	88
4.2.8. Az „adatfeldolgozás” alapvető szabályai	90
4.2.9. A bejelentési kötelezettség	91
4.2.10. Személyes adatok továbbítása harmadik országokba	91
4.2.11. Bírói jogorvoslat, felelősség és a szankciók	94
4.2.12. A független adatvédelmi kontroll	94
4.2.13. A 29-es munkacsoport	97
5. ADATVÉDELEM AZ EU INTÉZMÉNYEIBEN	99
5.1. Személyes adatok védelme az Amszterdami Szerződésben	99
5.2. A 45/2001/EK rendelet	99
5.3. Az Európai Adatvédelmi Biztos	100
6. AZ EURÓPAI BÍRÓSÁG EGYES ADATVÉDELMI VONATKOZÁSÚ ÍTÉLETEI	103
6.1. A Rechnungshof-ügy	105
6.2. A Lindqvist-ügy	110
6.3. A légi utasok adatainak továbbítása az USA-ba	115
A III. rész összegzése: Az adatvédelem, európai alapjog	116

### **III. RÉSZ: MAGYAR ADATVÉDELEM KIALAKULÁSA**

7. AZ ADATVÉDELEM KIALAKULÁSÁNAK MAGYAR ÚTJA	118
7.1. A magyar nyilvántartási jog rövid története	118
7.2. Személyiségi jog és a személyes adatok védelme	125
7.3. Az informatikai törvénytervezetről	126
7.4. Személyes adatok védelme az (új 1989-es) Alkotmányban	128
7.5. Az Alkotmánybíróság a személyes adatok védelmezője	131
7.6. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII törvény parlamenti vitája	133
7.7. A magyar adatvédelmi törvény rendszere	136
7.8. Az adatvédelmi törvény célja és fogalmi rendszere	137
7.9. Az adatkezelés hazai szabályai (1992-es állapot)	139
7.10. Az érintettek adatvédelmi jogainak érvényesülése	143
7.11. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításai és közösségi jogharmonizációja	146
7.11.1. Az Avtv.. 1995-1999 közötti időszak változásai	146
7.11.2. A 2001-2002 közötti időszak	153
7.11.3. Az Avtv.. novellája 2003 és 2005 közötti időszak	155
7.11.4. Az Avtv.. 2005-es módosítása	162
8. A MAGYAR ADATVÉDELMI BIZTOSRÓL	164
8.1. Az Adatvédelmi Biztosok megválasztása	164
8.2. Az adatvédelmi biztos alapjogvédelmi funkciója	165
8.3. A magyar Adatvédelmi Biztos jogállása	168
8.4. Az Adatvédelmi Biztos hatáskörei, eljárása és eszközei	169

9.A MAGYAR ALKOTMÁNYBÍRÓSÁG EGYES ADATVÉDELMI VONATKOZÁSÚ ÍTÉLETEI	175
9.1. A személyi számról	175
9.2. A vagyonyilatkozatra kötelezésekről	183
9.3. Személyes adatok védelme a lelkiismereti szabadság biztosításáért	187
9.4. A személyes adatok védelme és a bírósági eljárások nyilvánossága	187
9.5. Személyes adatok védelme formai okból	188
9.6. Nemzetbiztonsági ellenőrzések adatvédelmi korlátairól	189
9.7. Közszereplők magánszférájáról	192
9.8. Titkos nyomozati eszközök alkalmazásának alkotmányos keretei	193
A III. rész összegzése: A magyar információs önrendelkezési jog alapjogi fejlődése és Drittwirkung hatása	199

## **IV. RÉSZ A SEKTORÁLIS ADATVÉDELEM KÖZÖSSÉGI JOGI ÉS MAGYAR RENDSZERE**

10. SEKTORÁLIS ADATVÉDELMI JOGALKOTÁS AZ EURÓPAI UNIÓBAN	201
10.1. Adatvédelem a belső piaci jogban	201
10.2. Távközlés adatvédelmi vonatkozásai	201
10.2.1. A távközlés adatvédelmi irányelv céljai	202
10.2.3. Forgalmi adatok kezelése és kötelező törlése	203
10.3. Az elektronikus kereskedelem adatvédelmi vonatkozásai	204
10.3.1. Elektronikus hírközlési adatvédelmi irányelv céljai	205
10.3.2. Tájékoztatási kötelezettség	206
10.3.3. Az internetre alkalmazandó szabályok	207
10.3.4. Helymeghatározási adatok	208
10.3.5. Nem-kívánt elektronikus levelek és hívások	209
10.3.6. Elektronikus adatvédelem közrendvédelmi korlátozása	210
10.3.7. Jobbiztonsági garanciák	210
11. SEKTORÁLIS ADATVÉDELEM A MAGYAR JOGBAN	211
11.1. Személyes adatok jogi védelme	211
11.1.1. Személyes adatok védelme és a személyiségvédelem	211
11.1.2. Személyes adatok védelme a képmás védelem	216
11.1.3. Közszereplők képmásvédelmi szabályai	221
11.1.4. A képmásvédelem egyéb adatvédelmi vonatkozású esetei	222
11.1.5. Személyes adatok büntetőjogi védelme	223
11.2. Személyes adatok védelme és a sajtószabadság	225
11.3. Egészségügyi adatok védelme	230
11.4. Személyes adatok védelme a munkahelyeken	239
11.4. 1 A munkahelyi privacyról az EU-ban	239
11.4.2. A magyar munkahelyi privacyról	240
11.4.3. Egyetemi hallgatók személyes adatainak kezelése	259
11.5. Személyes adatok védelme a magyar hírközlési jogban	259

11.6. Személyes adatok védelme és a direkt marketing	265
11.7. Hitelinformációs rendszerek és a személyes adatok védelme	274
11.7.1. Hitelinformációs rendszerekről általában	274
11.7.2. Központi hitelinformációs rendszer Magyarországon	275
11.7.3. A pozitív adólista bevezetésének adatvédelmi korlátai	278
11.8. Az adatvédelem és az internet	282
11.8.1. Véleménynyilvánítás az interneten	283
11.8.2. Internet-szolgáltatók adatvédelmi kötelezettségei	284
11.8.3. Hozzáférés az internet-szolgáltatók által tárolt személyes adatokhoz	287
11.8.4. Az e-mail cím adatvédelmi követelményei	288
11.8.5. Személyes adatok nyilvánosságra hozása az interneten	290
11.8.6. Regisztráció az elektronikus szolgáltatások esetében	291
11.8.7. Elektronikus kereskedelmi szolgáltatások adatvédelmi veszélyei	293
11.8.8. Outsourcing	295
11.9. Személyes adatok védelme és a biztonság	297
11.9.1. Biztonsági szolgáltatások, kamerás megfigyelések	297
11.9.2. Adatvédelmi jogi előírások az elektronikus megfigyelőrendszerekre vonatkozóan	298
11.9.3. Hálózati videó rendszerek alkalmazásának adatvédelmi kockázatai	299
11.9.4. Térfigyelő rendszereket telepítésének indokai és jogi keretei	300
 A IV. rész összegzése: Adatvédelem és technológiai fejlődés	 303
 EREDMÉNY: Adatvédelmi módszerváltás	 305
 Idegen nyelvű összefoglaló	 310
Felhasznált irodalom	311
Rövidítésjegyzék	326
Tárgymutató	327

A kézirat 2010. március 1-i időponttal került lezárásra.

# SZEMÉLYES ADATOK VÉDELME AZ EURÓPAI UNIÓ JOGÁBAN ÉS MAGYARORSZÁGON

*Dr. Mező István*

*„Mindenkinek joga van a  
rá vonatkozó személyes adatok védelméhez.”<sup>1</sup>”*

## I. RÉSZ: ALAPOK ÉS KERETEK

### 1. AZ ADATVÉDELEM PROBLEMATIKÁJA

#### 1.1. Bevezető

Az állam működését kezdetektől fogva a mai napig végig kíséri a hatalom birtokosainak igénye, hogy az állam céljainak elérése érdekében minél több információval rendelkezzenek polgáraik adatairól, vagyoni helyzetéről, a népesség összetételéről. A Bibliában Mózes IV. Könyve Izrael népének számbevételével kezdődik, amely egy kis túlzással korai "állampolgársági nyilvántartásnak" tekinthető. A Krónikák Első Könyvének 24. verse szerint a Dávid király által végrehajtott népszámlálás a sátán bűne és az Úr elleni véték, aki a fegyverforgatók összeírása miatt dögvésszel sújtotta Izraelt. Tudva levő, hogy az említett népszámlálásokról ránk maradt emlékek különböző korúak, de az megállapítható, hogy a népszámlálások és összeírások bibliai megítélése nem éppen pozitív. Az állami adatgyűjtések bibliai megítélése tükrözi azt az alapvető jellemvonásunkat, hogy tiltakozunk az ellen, hogy számunkra ellenőrizhetetlen nyilvántartásba vegyenek, és az adataink összekapcsolásából személyiség képeket, fogyasztói profilokat készítsenek, vagy vagyoni helyzetünket feltérképezzék. Ez az ősi tiltakozásunk párosul az állami

---

<sup>1</sup> Európai Unió Alapjogi Chartája II. 68. cikk  
<http://eurlex.europa.eu/hu/treaties/dat/12004V/htm/C2004310HU.01004101.htm> ; 2006.1.20.



hatalmat gyakorlók korszakokat átívelő igényével, hogy különböző nyilvántartásokkal polgárai vagyoni, adózási, honvédelmi képességeit vagy más tulajdonságait képzettség, vállalkozási potenciálját, vagy vallási meggyőződését, politikai véleményét több tekintetében feltérképezzék. A szakirodalom szerint "tulajdonképpen az állam története többek között a nyilvántartások történeteként is leírható<sup>2</sup>". Így ezt a helytálló megállapítást mindenképpen azzal kell egészíteni, hogy az állami nyilvántartások történetéhez hozzákapcsolódik a nyilvántartások elleni küzdelem is. A XX. században az állami működés mindennapjai nem nélkülözhetik a számtalan, szinte áttekinthetetlen nyilvántartási rendszerek létezését a közhatalmi jogosítványok gyakorlásához, illetve a közszolgáltatások lebonyolításához. A magánszféra megsemmisülésének veszélye ezzel arányosan növekedett, József Attila verssorai is tükrözik az állami hatalommal szembeni kiszolgáltatottság élményét:

„Számon tarthatják, mit telefonoztam  
s mikor, miért, kinek.  
Aktákba írják, miről álmodoztam  
s azt is, ki érti meg.  
És nem sejthetem, mikor lesz elég ok  
előkotorni azt a kartotékot,  
mely jogom sérti meg.”

(József Attila: Levegőt 1935)

A technológiai eredmények fejlődésével az állami adatkezelési és nyilvántartási rendszerek olyan mértékben fejlődtek, amelyek még a XX. század közepén is elképzelhetetlennek tűntek.

---

<sup>2</sup> LAKATOS Miklós, *A személyiség joga, az állam működőképességének joga (Egy alkotmánybíróági döntéshez)*, Valóság, 1993/36, 3.sz. 1.

Az állami adatkezelők és adatgyűjtők mellett - akiket, ha semmibe veszik a magánélet szentségét a szakirodalom Orwell után "Nagy Testvérnek" nevez - megjelentek a "Kis-Testvérek" is, vagyis az állami adatkezelők mellett a globális, regionális szinten szervezett mamutvállalkozások is kifejezetten aktív érdeklődést tanúsítanak személyes adataink megszerzése érdekében. Ezzel a tendenciával szemben a magánszféra védelme érdekében jogi szabályozókat alakítottak ki, hogy szabályozzák az elektronikus adattároló és feldolgozó rendszerek tömeges alkalmazását<sup>3</sup>. Sok esetben előfordul, hogy a magán adatkezelők, akik kereskedelmi, gazdasági megfontolásokból gyűjtik a fogyasztók adatait, a profit érdekében kevésbé törődnek a személyes adatok védelmével. A technológiai fejlődés mára olyan szintet ért el a megfigyelés (pl. az áruházi videokamerák, a munkahelyi hazugságvizsgálók) és az adatrögzítés terén, hogy a magánélet és a személyes adatok alkotmányos jogai megsértésének bármikor "áldozatai" lehetünk. „A biztonsági kamerák léte a folyamatos láthatóság érzetét kelti az emberben, ami a megfigyelőnek - az állami intézménynek, vagy a piaci élet szereplőjének - automatikusan hatalmi pozíciót biztosít. Nem tudhatjuk biztosan, hogy figyelnek-e bennünket, de abban biztosak lehetünk, hogy ez bármikor megtörténhet.”<sup>4</sup>

A XXI. század kihívása a személyes adatok védelme tekintetében az, hogy hogyan sikerül a sokszor ellentétes érdekek mentén a személyes adatok védelmének fenntartása a terrorizmus elleni harc, az egyre tökéletesedő titkosszolgálati lehallgatások, vagy a vagyonvédelmi célból felszerelt integrált kamerarendszerek rengetegében. Ma már nem tudhatjuk biztosan, hogy nem figyel-e minket éppen valaki, hiszen piackutatási szempontból figyelik internetezési szokásainkat, és rosszabb esetben kémprogramokkal kívánnak a banki adatainkhoz hozzáférni. Többször hallható, hogy bizonyos maffia csoportok új bűnözési terepe az internet, ahol először csak pénzmosásra

---

<sup>3</sup> JÓRI András, *Adatvédelmi kézikönyv: elmélet, történet, kommentár*, Budapest, Osiris Kiadó, 2005 (Osiris kézikönyvek), 21.

<sup>4</sup> 36/2005. (X. 5.) AB határozat

használják fel a gyanútlan szörfölőket, majd banki adatok lopására szakosodnak. Egyes szakértők éves szinten több milliárd dollárra teszik a fel nem derített bűncselekményeket, amelyeket számítógépek útján követnek el. Ebben a küzdelemben a széleskörű jogi, technikai, illetve oktatási eszközöket kell felhasználni az együttműködés keretei között, hogy az elveszni látszó magánszféránkat megóvjuk. Annak érdekében, hogy magánszféránk védelme érdekében fellépjünk, szükséges, hogy az adatvédelem jogi és intézményi rendszerét megismerjük.

Az adatvédelmi jog fejlődésének első szakaszát egyesek az állami információs-hatalom kiterjesztésének korszakaként határozzák meg. Norbert Wiener röviddel a második világháború után a *Cybernetics* című művében a magasan fejlett információs technológiák veszélyétől óvott. George Orwell valóságmű módon festette le a lakosság manipulálásának lehetőségeit, amelyekben az információs technológiák is szerepet kaptak egy diktatúra stabilizálásában és annak kiterjesztésében. A nyugati társadalmaknak az 1960-es években az adatfeldolgozási technológiák gyors fejlődése nem tűnt fel, e tendenciára a közvélemény figyelmét Kennedy választási győzelme irányította, amely során a Demokrata Párt egyes választókerületekben a választói viselkedéseket feltérképezte, majd a számítógépek segítségével kiértékelte.<sup>5</sup> A világ első adatvédelmi törvénye a Hesseni Adatvédelmi törvény 1970-ben az NSZK-ban került elfogadásra. A törvény célja az volt, hogy az elektronikus úton végzett adatkezelés, adatfeldolgozás kereteit meghatározza<sup>6</sup>. A törvény parlamenti vitája során alakult ki maga az adatvédelem (Datenschutz) fogalma is, amely később az információs önrendelkezési jog védelmére irányuló jogi normák összefoglaló elnevezésévé vált. Sólyom László megfogalmazása szerint >a számítógépek alkalmazásával az államigazgatás terjeszkedésének természetes korlátai is megdőltek, sőt az igazgatás növekedési spirálra tért: az állam szolgáltatásaiért cserébe a még

---

<sup>5</sup> Werner LIEDTKE, *Das Bundesdatenschutzgesetz: Eine Fallstudie zum Gesetzgebungsprozess*, Bamberg. Difo-Druck, 1980, 88

<sup>6</sup> SCHILD: Datenerhebung,- verarbeitung und nutzung in Handbuch Datenschutzes 502 old.

több „szükséges” információ, valamint ezáltal az igazgatottak még teljesebb függése egymást gerjesztve bővíthetett. Az igazgatás automatizálásának első szakasza a nagy gépek, a nagy nyilvántartások, a nagy hatalom kora. Minden országban nekiláttak, hogy megvalósítsák az egységes központi népességnyilvántartást, amelyről az uralkodók és klasszikus rendőrállamok csak álmodozhattak<sup>7</sup>. Ennek a rendszernek természetes velejárója az emberek adatbázisokban történő megszámozása, és az ebből következő veszélye, hogy a személyiség adatformában történő létezése jogalanyból jogtárggyá silányíthatja az embert. A dolgozatom célja, hogy a nemzetközi, közösségi, illetve a hazai adatvédelmi normák rendszerbe foglalásával egyrésztől áttekintést adjak, másrésztől a kutatásom hipotézisében megfogalmazottakat részleteiben kibontsam.

## 1.2. A kutatás áttekintése és célja

A dolgozatban azt kívánom bemutatni, hogy milyen folyamat vezetett addig, míg az európai országokban, közte hazánkban a világon szinte egyedülálló módon részletesen szabályozzák az adatkezelést, és védik a személyes adatokat. A dolgozatban arra is rá kívánok világítani, hogy a személyiség védelem jogi eszközrendszere az adatvédelem tükrében átalakult-e. A dolgozatom tárgyköre annak bemutatására irányul, hogy az információs önrendelkezési jog hogyan vált európai alapjoggá, illetve az adatvédelem alapjoggá válása milyen keretek között zajlott le Magyarországon. Az európai és a magyar jogszabályozás áttekintése során vizsgálom, hogy az adatvédelem tárgyköre miképpen válik alapvető jog által védett európai és nemzeti alkotmányos értéké.

A dolgozat első blokkját az adatvédelem fogalomkörének a tisztázása jelenti. A kutatás történeti kiindulásaként szemügyre veszem a privacy, illetve az

---

<sup>7</sup> SÓLYOM, *i.m.*, 54.

adatvédelem fogalmát, tárgykörét, illetve az adatvédelmi jogterület fejlődését. A dolgozat második részében az adatvédelem nemzetközi szabályozói, az Európa Tanács Adatvédelmi Egyezménye, valamint az Emberi Jogok Európai Bíróságának ítélezésében megjelenő, az adatvédelmet érintő fejlődés kerül bemutatásra. A személyhez fűződő adatok védelmére és kezelésére vonatkozó jogszabályok a 90-es évek végére európai alapjogi jelleget nyertek, amely jogfejlődés világos elismerésére az Európai Unió Alapjogi Chartájában az egyéni szabadságjogok körében került sor. Az európai adatvédelmi jog kialakulása szempontjából az Európai Unió másodlagos jogalkotását veszem szemügyre a személyes adatok védelme vonatkozásában. Az Európai Unió másodlagos jogalkotásának áttekintését egyrészt a természetes személyek jogainak, illetve a személyhez fűződő adatok feldolgozásakor nyújtandó védelemről és a szabad adatforgalomról szóló 1995. október 24-én az Európai Parlament és a Tanács által elfogadott 95/46/EK irányelv részletes elemzése, és bemutatása jelenti. A 95/46/EK irányelv egyes szakaszainak értelmezését, és áttekintését, továbbá a 29-es munkacsoport működésének bemutatását követően a szektorális adatvédelmi szabályozás részletes bemutatására kerül sor. A magánszféra és a személyes adatok védelmében a telekommunikációs szektorra vonatkozó speciális előírásokat rögzítő 97/66/EK irányelv<sup>8</sup> a személyes adatok feldolgozásának különös szabályait fektette le azzal a céllal, hogy a 95/46/EK irányelv alapvető jelleggel megfogalmazott szabályait a telekommunikációs szektorra is érvényesítsék részletes előírásokkal. Az elektronikus kereskedelem adatvédelmi szempontokat is figyelembe vevő megújítására<sup>9</sup> 2002-ben került sor, ekkor a távközlési-adatvédelmi irányelv

---

<sup>8</sup> Az Európai Parlament és Tanács 1997. december 15.-én elfogadott 97/66/EK irányelve a személyes adatok feldolgozásáról és a magánszféra védelméről a telekommunikációs szektorban EU O.J L. 24-30.01.1998 1-8. old.

<sup>9</sup> Az Európai Parlament és Tanács 2002/22/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról („Egyetemes szolgáltatási irányelv”) illetve a Az Európai Parlament és Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról („Keretirányelv”)

helyét átvette az elektronikus hírközlési adatvédelmi irányelv<sup>10</sup>, amely minden korábbi szabályozást megtartott, és kiegészítette az új speciális technikai előírásokkal, mint a forgalmi, illetve helymeghatározás adat fogalma és kezelése, továbbá a kommunikációhoz kapcsolódó értéknövelt szolgáltatásra, elektronikus levélre, valamint a cookie-kra, SMS-ekre vonatkozó szabályokkal.

A dolgozat harmadik részében a magyar személyiségi jog, és az adatvédelem kapcsolatát, valamint a magyar adatvédelmi törvény elfogadását tekintem át. A dolgozat ezen részében részletesen foglalkozom a magyar adatvédelmi törvénnyel, az adatvédelmi biztos gyakorlatával, valamint az alkotmánybíróságnak az adatvédelmet érintő ítélezési gyakorlatával. Áttekintem a személyes adatok védelmére vonatkozó alapjog lényeges tartalmát, kereteit, korlátozhatóságát, illetve értelmezési aspektusait. Az általános adatvédelmi normák áttekintésén túl részletesen foglalkozom a szektorális adatvédelem témakörével, így az adatvédelem, és a sajtó kapcsolatával, az egészségügyi adatkezeléssel, munkahelyi privacy témakörével, az adatvédelem és az internet kapcsolatával, valamint a biztonság és a személyes jellegű adatkezelés összefüggéseivel.

A dolgozat kutatási célja továbbá annak feltérképezése, hogy az alapjogi jelleget nyert személyes adatok védelmére vonatkozó jogszabályok horizontális jogviszonyokban, milyen keretek között érvényesülnek a mindennapi élet egyes területein. Így a személyiség védelem, a munkahelyi adatkezelés, az egészségügyi adatvédelem, a direktmarketing, a hitelintézeti adatkezelés, valamint az elektronikus hírközlés, és kereskedelem területén azaz a szektorális adatvédelem területein hogyan vált alapjoggá az adatvédelem.

---

<sup>10</sup> Az Európai Parlament és Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv”)

### 1.3. Drittwirkung - alapjogok horizontális hatásai

A klasszikus alapjogi felfogás szerint az egyéni szabadságjogok az egyén és állam közötti „vertikális” viszonyból fejlődtek ki. A végrehajtó hatalom önkényével szemben kialakult alapvető jogok az állami intézményeket kötik, és védik a magánszemélyek jogi pozícióját. De be kell ismerni, hogy az egyének szabadsága nemcsak az állam oldaláról veszélyeztetett, hanem a magánjogi viszonyokban is lehetnek egyenlőtlen jogi helyzetek, amelyek az egyén alávetésével járnak együtt. A II. világháború után bontakozott ki az a felfogás, hogy az alapvető jogokat a magánjog körébe tartozó személyek viszonyaiban is figyelembe kell venni, olyan mértékig, míg tényleges és jogi hatalmi pozíciója egy hatalmasságnak az egyén szabadságát korlátozni képes. A német jogi szakirodalomban ez a vita az alapvető jogok harmadik vagy horizontális hatása (Dritt- oder Horizontalwirkung) címen folyt. A horizontális hatású alapjogi viszonyok vitája egymással több tekintetben ellentétes álláspontok kialakulásához vezetett, míg egyesek kategorikusan elutasítják, addig mások vehemensen támogatják az elméletet.

A magyar alkotmányjogban a „Drittwirkung” fogalom kevésbé használatos, ezért szükséges a definíció részletesebb kifejtése. A „Drittwirkung” a német közjogban kialakult, kizárólag a jogi szaknyelvben használt fogalom. Egy alapjog Drittwirkung hatásáról akkor beszélünk, ha egy alapjog nem kizárólag állam és egyén viszonyában értelmezhető, hanem polgár és polgár közötti magánjogi jogviszonyra kiható védelmi hatással is bír. A polgár-polgár viszonylatban értelmezhető Drittwirkung hatást mindig kivételes esetként kell kezelni. Ennek érdekében a szakirodalom megkülönbözteti a közvetlen, direkt (unmittelbare) és a közvetett (mittelbare) Drittwirkung felfogást. Közvetlen Drittwirkung hatásról akkor beszélünk, ha az alapjogi norma tartalma maga határozza meg ezt a magánjogi jogviszonyokban is érvényesülő hatását. Így a német alaptörvény<sup>11</sup> szerint a polgárok közötti megegyezések vagy

---

<sup>11</sup> [\(Art. 9 Abs. 3 S. 2 GG\)](#)

intézkedések, amelyek célja, hogy szakszervezetek vagy munkavállalói szövetségek létrejöttét akadályozzák semmisnek tekintendők. A koalícióalkotási szabadság történelmi előzményeinek széleskörű garantálása fejeződik ki az alapjogi normatartalomban<sup>12</sup>. Az alkotmányozó a munkaadó és munkavállaló közötti eltérő hatalmi pozíciót kívánta kiegyensúlyozni. A közvetlen Drittwirkung érvényesítése a bíráskodásban alapvetően elutasított. Ezzel szemben egy alapjognak a közvetett Drittwirkung hatása általánosságban elismert. Példaként említhető értelmezési kiinduló pontként a személyiségi jog és emberi méltóság oldaláról a becsületet sértő kijelentések súlyának megítélése, vagy az egyenlő bánásmód megsértésének tilalma abból a szempontjából, hogy akár magánjogi, munkajogi kereset is indítható ezen alkotmányos tilalom megsértése miatt. Közvetett Drittwirkung hatásról akkor beszélünk, ha egy alapjog védelmi hatása (Schutzwirkung) csak közvetett módon egy általános elvből (Generalklausel) vezethető le. Egy alapjog védelmi hatásának megállapítására egy általános elv<sup>13</sup> elméleti kibontása során kerülhet sor, mivel a magánjogi jogviszonyok értelmezése során a bírónak az alaptörvényt, és ezzel együtt az alapvető jogokban rögzített objektív értékrendet kell figyelembe venni.

Az 1949-ben Herbert Krüger által kezdeményezett tudományos vita a „Verfassungen in der Zivilrechtssprechung<sup>14</sup>” című dolgozatával kezdődött. Krüger arra bátorította a polgári bíráskodást, „hogy a tiszta polgárjogi horizontális jogviszonyokból kitekintsenek, és argumentációjuk kialakítását gazdagítsák az alkotmányjogilag releváns álláspontokkal.” Az alapvető jogok horizontális jellegének megvilágítása érdekében szükséges áttekinteni a Német Alkotmánybíróságnak 1951-ben az alapjogok Drittwirkung hatásával

---

<sup>12</sup> Weimári Köztársaság Alkotmányának 118. szakasza szerint a munkajogviszonyokban tilos a véleménynyilvánítás korlátozása, illetve a 159. szakasz tiltott, és semmisnek nyilvánított minden olyan megegyezést vagy intézkedést, amely célja a egyesülési szabadság korlátozása.

<sup>13</sup> (pl: BGB 242. § Leistung nach Treu und Glauben Der Schuldner ist verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern, Jóhízemű teljesítés. A kötelezett a teljesítés során köteles a jóhízeműség alapján eljárni, úgy ahogy az a forgalmi szokásokra tekintettel szükséges. )

<sup>14</sup> Herbert KRÜGER: Verfassungen in der Zivilrechtssprechung, in Neue Juristische Wochenzeitschrift NJW 1949, S. 163 ff. [165]



kapcsolatosan hozott Lüth ítéletét<sup>15</sup>. Lüth úr egy sajtótársaság vezető tisztségviselőjeként nyílt levélével egy olyan film elleni bojkottra hívott fel, amelyet Veit Harland forgatott. A felhívás háttérében az állt, hogy Veit Harland a náci III. Birodalomban „Jud SüSS” címen antiszemita propaganda filmet készített. Hamburg Tartományi Bírósága Lüth urat a bojkott abbahagyására ítélte, amely ellen az Lüth úr alkotmányjogi panaszt nyújtott be a BVerfG részére.

Az Alkotmánybíróság döntését az alábbi irányelvekben foglalta össze:

- 1.) Az alapvető jogok elsősorban a polgárok védelmét szolgáló jogok az állammal szemben. Az alaptörvényben rögzített alapjogi előírások azonban megtestesítenek objektív értékrendet is, amely mint alkotmányjogi követelmény a jog minden területére irányadó.
- 2.) A polgárjogi jogviszonyokban az alapvető jogok tartalma megjelenik közvetett módon a magánjogi előírásokon keresztül. Ez minden jogi előírás kötelező karaktere, és ez a bírók számára különösen az általános elveken keresztül válik kézzelfoghatóvá.
- 3.) Egy magánjogi ügyben eljáró bíró ítéletével alapvető jogokat sérthet meg (§ 90.BVerGG<sup>16</sup>), ha a polgári jogi normának az alapvető jogra eső hatását félreismeri. A Német Alkotmánybíróság a polgári jogi ítéleteket az alapvető jogok ilyen jellegű megsértése esetén vizsgálja, és nem aszerint, hogy általános jellegű jogi hiba bekövetkezett-e.
- 4.) A polgári jogi normák az alaptörvény 5. cikke szerint „általános jellegű törvényeknek” minősülnek, így alkalmasak arra, hogy a véleménynyilvánítási szabadság alapvető jogát korlátozzák.
- 5.) Az „általános jellegű törvényeket” annak fényében kell értelmezni, hogy az megfeleljen a szabad véleménynyilvánítás jelentőségének egy demokratikus államrendezkedésben;

---

<sup>15</sup> Lüth-ítélet: BVerfGE 7, 198 I. BvR 400/51 1951.11.22

<sup>16</sup> (§ 90.BVerGG)

- 6.) Az alaptörvény 5. cikke nemcsak a vélemény kinyilvánításának formáját védi, hanem a véleménynyilvánításon keresztül annak lelki megnyilvánulásának hatásait is.
- 7.) Egy bojkottra történő felszólítást tartalmazó véleménynyilvánítás nem ütközik bele szükségszerűen a jó erkölcsbe a (BGB 826.§). A bojkottra történő felhívás az eset minden körülményének gondos mérlegelésével, az alkotmányjogilag értelmező véleménynyilvánítás szabadságával igazolhatóvá válhat.

A német Alkotmánybíróság a fenti mérlegelés alapján arra a meggyőződésre jutott, hogy a Hamburgi Tartományi Bíróság a panaszos viselkedésének megítélése során azt félreismerte, hogy ő akkor is jogosult a véleménynyilvánítási szabadság alapvető jogát gyakorolni, amikor az magánszemélyek közötti konfliktusokban jelenik meg. A Tartományi Bíróság ítélete alapjogi mértékű hibában szenved, és ezzel a panaszos alapvető jogát (Art 5.Abs.1.S.1.GG) megsértette, ezért a felsőbbíróság ítéletet hatályon kívül helyezésre került. Az alapvető jogok horizontális hatása az ítékezésben az 1990-es évekre teljesen mértékben elismerésre került olyan mértékben, amely a jogalkotó számára is megkerülhetetlenné vált. A német szövetségi új alkotmány előkészítése során az Alkotmányozó Bizottság<sup>17</sup> külön cikket fogadott el az alapvető jogok horizontális hatályáról:

*„ A hatóságok gondoskodnak arról, hogy az alapvető jogok, míg arra azok alkalmasak magánszemélyek között is hatékonyan érvényesüljenek. ”*

A német szakirodalom<sup>18</sup> szerint az alapjogok horizontális jellegének elfogadása olyan újdonság, amely elsősorban azokon a területeken jelenik

---

<sup>17</sup> Verfassungskommissionen des National- und Ständerates, BBl 1998 I 364 ff., 378, 446):

<sup>18</sup> Prof. Dr. Andreas Kley Der historische Weg zum Drittwirkungsartikel im Entwurf für eine neue Bundesverfassung; <http://www.unibe.ch/unipress/heft98/beitrag3.html>

meg, ahol a szociál-gazdasági hatalmi pozíciója az egyik partnernek a polgári jogi jogviszonyban jelentősen erőfölényt biztosít számára. Az álláspontom szerint a polgárok személyes adatainak kezelése terén az adatkezelőnek ez a szociál-gazdasági hatalmi pozíciója többnyire fennáll, mivel egyrészt a technológiai folyamatokat az adatkezelő belülről ismeri, másrésztől nem azonos gazdasági, jogi, pénzügyi helyzetben állnak az esetek többségében a természetesen személyek, és a személyes adataikat kezelő a magánjog körébe tartozó adatkezelő bankok, biztosítók, egészségügyi intézmények, távközlési társaságok, vagy éppen a munkáltatójuk.

#### 1.4. Drittwirkung hatás az adatvédelemben (hipotézis)

A dolgozatom elméleti célkitűzése az információs önrendelkezési jog horizontális jogviszonyokban történő részletes értelmezési módszertanának a kialakítása. A dolgozatomban azt kívánom bemutatni, hogy az adatvédelmi jellegű szektorális magánjogi jogviszonyokban a Drittwirkung hatás megragadható-e, és ha igen, akkor az alkotmányjogi értékek milyen jogelvek keretei között érvényesíthetőek. Az információs önrendelkezési jog megsértése, veszélyeztetése esetén a Drittwirkung elmélet alapján kibontható jogérvényesítés és jogvédelem eszközszerének tételes kibontás a dolgozatom tudományos újdonsága.

Elméleti álláspontom kiinduló tétele, hogy az adatvédelmi normákat közjogi és magánjogi adatvédelem körébe kell sorolni aszerint, hogy vertikális vagy horizontális jogviszonyban állnak-e a felek egymással. Az állami, önkormányzati, rendőrségi, vagy más hatósági adatkezelés a közjogi adatvédelem körébe tartozik, és az alapvető jogok korlátozására vonatkozó szükségességi és arányossági elvek szerint kell megítélni a közjogi adatkezelés alkotmányosságát. Ezzel szemben a magánjog körében működő adatkezelők esetében a magánjogi adatvédelem keretén belüli értelmezés során az

információs önrendelkezési jog hatékony, a XXI. századi technológiai fejlődéssel összhangban álló jogvédelmi, jogérvényesítési megoldását azzal lehet megtalálni, hogy ha a polgárjognak általános jogelveiből indulunk ki az adatvédelmi jellegű jogviszonyok értelmezésekor. Az általános jogelvek megfelelő alapot szolgáltatnak az alkotmányjogi értékeknek a magánjogi viszonyokba történő értelmezésére anélkül, hogy az alapjog korlátozás szigorú, lassú, körülményes követelményrendszerét alkalmazni kellene. Így a polgárjogban megjelenő elveket, mint a jóhiszeműség, tisztesség, kölcsönös együttműködés, joggal való visszaélés tilalma, általában elvárható magatartás követelménye által meghatározott normatartalmat kell alkotmányos értékekkel, mint az emberi méltóság, személyiség autonómiája, önrendelkezés szabadsága összhangban értelmezni a szektorális adatvédelem keretein belül.

#### 1.5. A kutatás módszertana

A dolgozat kutatás módszertana során az adatvédelem horizontális jellegű jogviszonyaira alkalmazandó elméleti tétel alátámasztása érdekében többféle módszertani irányt választottam. Egyrészt az információs önrendelkezési jog európai és nemzeti alapjoggá válásának történeti áttekintéséből kívánok következtetéseket levonni. Másrészt a magyar, illetve a német szakirodalomban fellelhető szakmai álláspontok ütköztetéséből kívánok elméleti következtetéseket levonni. A kutatás empirikus részeként a magyar Alkotmánybíróság esetjogát, az adatvédelmi biztos jelentős állásfoglalásait tekintetem át, és ezzel kívánom a jogeseteket az elméletem alátámasztása érdekében rendszerbe foglalni. A tudományos kutatás során – mint mintavételi helyen lehetőségem volt a Német Szövetségi Köztársaság Parlamentjének könyvtárában a témához kapcsolódó német nyelvű szakirodalom összegyűjtésére, illetve a Nemzeti Hírközlési Hatóság szakkönyvtára az angol és a magyar nyelvű szakirodalom összegyűjtésében és feldolgozásában volt segítségemre. A szakirodalom feldolgozása mellett az Adatvédelmi Biztosi

Hivatal munkatársaival vitattam meg adatvédelmi kérdéseket, és betekintést kaptam a Hivatalba benyújtott, a személyes adatok megsértése miatt benyújtott panaszok feldolgozásába. Az Adatvédelmi Biztos állásfoglalásaink gyűjteményét összeállítottam, majd témakörökhöz rendeltem.

## 2. FEJEZET: SZEMÉLYES ADATOK VÉDELMÉNEK ALAPFOGALMAI

### 2.1. Adatvédelem, de miért?

A személyes adatok védelme elsősorban az egyéni létnek, az egyéni önrendelkezésnek, a személyiség autonómiájának, végeredményben az emberi méltóságnak a XXI. századi technológiai hálózatok világában történő biztosításával áll összefüggésben. Az individualitás az emberi kultúránk alapvető értéke, mivel az egyéni kibontakozás, önmegvalósítás, külső zavarástól való mentes létezés életünk alapvető keretét adja. Az egyéni létezésünk, saját individualitásunk megélése nemcsak magányos tevékenység, hanem egyénként szűkebb és tágabb közösségeknek is a tagjai vagyunk. A kapcsolatainkban, közösséghez tartozásunk során folyamatosan kommunikálunk különböző technológiai csatornákon, valóságosan és virtuális közegben is kapcsolatokat teremtünk, ápolunk, és adott esetben zárunk le. Az adatvédelem által védett információs önrendelkezés kiterjed a másokkal folytatott kommunikációnk bizalmas jellegének megőrzésére, és ezzel együtt az adatvédelem egy szabad és demokratikus kommunikációs feltételrendszer alapja is egyben. Így az adatvédelem nem csak a személyiségünk védelmét biztosítja technológiai környezetben, továbbá nem csak a kommunikációs szabadságunk, kommunikációs önrendelkezésünk garanciális eszközszerete hanem alapja egy szabad és demokratikus közösségi lét fenntartásának. Az adatvédelem eszközszerete lehetővé teszi a polgárok cselekvési és együttműködési lehetőségét, és biztosítja, hogy külső kontroll nélküli információcsere valósuljon meg, és ez alapján szabad és demokratikus megvalósulása legyen akaratok kifejezésének.

Az adatvédelem azzal, hogy egyéni szabadságjogok védelmének jogi eszközszerete, és a demokratikus társadalmi berendezkedés garanciája is egyben, a XXI. század egyik legvitatottabb témakörévé kezd válni. Az elmúlt évtizedek tragikus és szenvedéssel teli történelmi tapasztalatai alapján, illetve

a XXI. században is fennálló autokratikus politikai berendezkedések működése alapján megalapozottan állítható, hogy az egyének és közösségeik közötti kommunikáció korlátozása a totalitárius és diktatórikus rendszerek sajátosságai. Annak érdekében, hogy a XXI. században egyre erőteljesebben megjelenő nemzetközi terrorizmusból fakadó biztonsági veszélyek elleni fellépés ne eredményezze a személyiségünk teljes lemeztelenítését, szabad kommunikációnk totális kontroll alá vonását, és végső soron egy rendőrállami „demokrácia” kialakulását, szükséges, hogy az „őrzők a strázsán” maradjanak, és az adatvédelem jogi, technológiai eszközrendszerét folyamatosan fejlesszék.

Az információs önrendelkezési jog védelmének garanciái tömören az alábbiakban foglalhatók össze:

- 1.) a személyes adatok kezelése abban az esetben megengedhető, ha ennek kereteit és célját a törvényhozó, vagy az érintett előzetesen meghatározta;
- 2.) az érintett az adatok kezeléséről informált, illetve a törvényi felhatalmazás keretei között ellenőrizheti az adatkezelő által végzett transzparens adatkezelést. Az érintettnek joga van a felvilágosításhoz, illetve személyes adatainak kijavításához.
- 3.) az adatkezelés kizárólag az előzetesen meghatározott cél érdekében végezhető, olyan mértékben, amely a cél elérése érdekében szükséges.

A vizsgálódásom arra irányul, hogy a magán adatkezelőkkel kapcsolatosan kialakított adatvédelmi jogviszonyokban az információs önrendelkezési jog garanciális elemei hogyan alakíthatók ki, illetve hogyan érvényesülhetnek a XXI. századi technológia világában.

## 2.2. A privacy fogalmáról

„Az életmódunk felgyorsulása, intenzitásának és bonyolultságának növekedése, mely velejárója a fejlett civilizációs rendszereknek szükségessé tették egy bizonyos fokú visszavonulást a világtól, és az egyén az őt körülvevő kultúra fejlettsége mellett éppen a nyilvánosságra vált érzékenyebbé, hogy az egyedüllét és magánélet lényegesebbé váljanak számára. A modern találmányok és szolgáltatások éppen a magánéletébe törtek be, olyan mentális (szellemi) fájdalomnak és gyötrelemnek téve ki az egyént, mely sokkal nagyobb, mint amit egy testi sérülés okozni tudna” - írta a privacy fogalmának meghatározásakor WARREN és BRANDEIS 1890-ben a Harvard Law Review<sup>19</sup>-ba megjelent tanulmányukban. Az amerikai privacy felfogás lényege, de legalábbis kiindulópontja sokak szerint a magánlakás szentsége<sup>20</sup>. Az európai és az amerikai jogi kultúra a privacy felfogások között abban ragadható meg, hogy míg az európai felfogásban az adatvédelem a piacra, az államra és a másik emberre koncentrál, és a korlátait a személyközi viszonyokra is kiterjeszti, addig az amerikai privacy-védelem az állammal szemben fogalmazódik meg<sup>21</sup>.

Az adatvédelem főbb fejlődési útjainak az áttekintéséhez nélkülözhetetlen az alapvető jogi fogalmak tisztázása. Az angolszász "privacy törvények" a magántitok védelméből kiindulva a személyiségvédelem eszközrendszerének használatára helyezik a hangsúlyt. A privacy megsértése miatt indított keresetek a magánjog keretében kerülnek elintézésre függetlenül attól, hogy a jogsértő közjogi vagy magánjogi személy volt. A privacy magyar fordításban a magánélet védelmét, a magántitok tiszteletét jeleneti, amely tartalmának megragadásához több fogalmat szükséges áttekinteni. Elsősorban a privacy a magánélet, magántitok és a személyes adatok védelméhez fűződő alapvető

---

<sup>19</sup> WARREN/BRANDEIS, Harvard Law Review 1890, 196.old.

<sup>20</sup> MAJTÉNYI László, *Az információs szabadságok : adatvédelem és a közérdekű adatok nyilvánossága*, Budapest, Complex, 2006, 214.

<sup>21</sup> MAJTÉNYI: U.A.



emberi jog, amely egyben több más értékünknek, így az emberi méltósághoz fűződő jognak vagy a gyülekezési és szólásszabadságnak is alapja. A privacy emberi méltósághoz való szoros kapcsolatából ered az a követelmény, hogy mindenki maga rendelkezzen személyes adatainak kezeléséről és azok feltárásáról.

Az irodalom<sup>22</sup> a privacy fogalmán belül négy "állapotot" különít el: ezek az egyedüllét (solitude), a bensőségesség (intimacy), a névtelenség (anonymity) és a tartózkodás (reserve). A bensőségesség és a névtelenség lehetővé teszi, hogy az emberek megfigyelés, azonosítás félelme nélkül vállalhassák a társadalmi, politikai érintkezést. Némi túlzással azt is mondhatnánk, hogy e kritériummal mérhető a szabadelvű-demokratikus, illetve az önkényuralmi rendszerek közötti különbség. Ezért a privacy védelme nemcsak azért fontos, mert lehetővé teszi az egyén számára a visszahúzódást a másokkal való érintkezéstől, hanem azért is, mert támogatja a demokráciákra jellemző társadalmi, és politikai közéletben való aktív szerepvállalást.<sup>23</sup>

A privacy fogalmát az egyén érdekei felől is meg lehet közelíteni. Az irodalom<sup>24</sup> az egyén privacyhoz fűződő érdekeit az alábbiakban határozta meg:

- Az egyéni függetlenséghez való jog;
- Az egyedülléthez való jog;
- A magánélethez való jog;
- A személyes adatok feletti rendelkezéshez való jog;
- Kizárólagos rendelkezési jog a magánszférához való hozzáférésről;
- A betolakodó magatartás elhárításához való jog;
- A titoktartás elvárásához való jog;
- A bensőségességhez való jog;

---

<sup>22</sup> Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1957, 31-32.

<sup>23</sup> Charles D. RAAB, *Gondolatok az információs jogok magyarországi tapasztalatairól = Oda átra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 33-55.

<sup>24</sup> David H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, 1989. = Magyar összefoglalás In: *Oda átra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 67.

- A névtelenséghez való jog;
- A tartózkodáshoz való jog;
- A titkossághoz való jog;

A privacy védelmének alapja a méltányos információs elvek érvényre juttatása, amelyek alapelvi szinten is megfogalmazhatók:

Felelősség: minden szervezet felelős a kezelésében levő személyes adatok sorsáért, és köteles kijelölni egy vagy több személyt, aki a szervezeteknél felel a következő elvek betartásáért.

Célmeghatározás: az adatfelvételkor vagy azt megelőzően a szervezet köteles tájékoztatást adni az adatgyűjtés céljáról;

Hozzájárulás: személyes adatot gyűjteni, felhasználni, illetve más számára hozzáférhetővé tenni csak az érintett tudomásával és hozzájárulásával szabad, kivéve, ha ennek megszerzésére nincsen mód.

A felhasználás, kiadás és tárolás korlátozása: személyes adatot az érintett hozzájárulása vagy törvényi rendelkezés hiányában csak az adatfelvételkor meghatározott célból lehet felhasználni, illetve más számára hozzáférhetővé tenni, tárolása pedig csak addig törvényszerű, ameddig az említett cél szempontjából elengedhetetlen.

Pontosság: a személyes adat a felhasználás céljának megfelelő mértékben legyen pontos, teljes és aktuális.

Garanciák: a személyes adat védelmére garanciákat kell nyújtani, mégpedig az adat érzékenységétől függő mértékben.

Nyitottság: a szervezet köteles konkrét tájékoztatást adni a személyes adatok kezelésében követett elvekről és gyakorlatról, illetve köteles az ilyen jellegű információt bárki számára hozzáférhetővé tenni.

Egyéni hozzáférés: az érintettet, ha kéri tájékoztatni kell személyes adatainak kezeléséről és továbbításáról. Biztosítani kell az érintett számára a saját adataihoz való hozzáférést, valamint annak lehetőségét, hogy azok pontosságát, teljességét vitassa, és a szükséges javításokat, kiegészítéseket kezdeményezze.

Szabályosság vitatása: az egyén számára biztosítani kell annak lehetőségét, hogy a szervezetnél felelős személyt vagy személyeket megkérdezhesse a fenti elvek betartásáról.<sup>25</sup>

Az irodalomban található egyes felfogások szerint az adatvédelem és a privacy az információs jogok körében negatív szabadságként "a valamitől való védelem szabadságaként" is értelmezhető. Ez a szabadság párosul az információszabadsággal, ami "a valamire való szabadságot jelenti". Berlin hangsúlyozza, hogy látszólag nincs különbség a szabadság eme két formája között, "egyik azt jelenti, hogy a magam ura vagyok, és a között, amelynek lényege, hogy mások sem szólnak bele a döntéseimbe". Berlin szerint a különbség pusztán annyi, hogy ugyanaz a dolog negatív és pozitív módon is megfogalmazható.<sup>26</sup>

Véleményem szerint a privacy fogalom és a Drittwirkung elmélet egymással párhuzamba állítható, és megfelelően kiegészítik egymást. A Drittwirkung elmélet lényege, hogy kiterjeszti az állam-egyén vertikális jogviszonyára irányadó elveket a magánszemély-magánszemély horizontális jogviszonyra, ha az alkotmányos érték jellegéből fakadóan ésszerűen és indokolható módon igazolható. A privacy fogalom nem a vertikális/horizontális jogviszonyok értelmezéséből indul ki, hanem az individuális lét biztosításának céljára helyezi a hangsúlyt. A privacy felfogás nem különbözteti meg az adatkezelő magánjogi vagy közjogi jellegét, hanem a jogsértés hatékony orvoslását segíti elő. Önmagában az angolszász jogrendszerekben elterjedt privacy elmélet alapján történő jogvédelem alátámasztja azt, hogy a kontinentális jogrendszernek is hasonló választ kell adnia.

---

<sup>25</sup> D. BANISAR, *A Privacy védelmének modelljei = Oda átra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 12.

<sup>26</sup> Isaiah BERLIN, *A szabadság két fogalma.* = I. B. , *Négy esszé a szabadságról*, Budapest, Európa, 1990. 342.

### 2.3. Adatvédelem fejlődésének történeti áttekintése

A privacy, illetve a magánszféra védelmére vonatkozó szabályok jóval megelőzték az adatvédelemre vonatkozó szabályrendszernek a kialakulását, de a magánszféra védelmére vonatkozó normák adták az adatvédelmi jog kiinduló lépéseit. Így 1890-es években a gyors fényképezéssel, mint technikai újítással kapcsolatosan fogalmazódott meg a képmásvédelem szabályrendszere, amely az egyént az általa nem kívánt képrögzítéstől kívánta védelmezni. A II. világháború utáni gyors technológiai fejlődés azzal a nyugat-európai felfogással párosult, hogy valójában ezek az országok az alapvető jogok védelmezői a Szovjetunió fenyegetettségében. Az adatvédelem, mint önálló jogterület kialakulását az NSZK-ban az segítette, hogy 1968-ban a II. világháború utáni politikai berendezkedés első jelentős átalakulására került sor, és egy reform-eufória, megújulási vágy széleskörű társadalmi igényként jelentkezett. A technológiai fejlődésre adott törvényhozási válaszként az első adatvédelmi törvény 1970-ben került bevezetése az NSZK-ban Hessen tartományban. Az új adatvédelmi törvény az elektronikus úton végzett adatfeldolgozások kereteit határozta meg >A németországi Hessen tartomány kormánya "Nagy Hessen Terv" címen az informatikai rendszerek kialakításával, összekapcsolásával a "funkcionálisan integrált igazgatási rendszert" kívánt létrehozni. A rendszer kiindulási pontja egy intergált rendszer kialakítása volt, melynek eredményként egy olyan hálózat létrejött, amelyben a statisztikai hivatal a rendőrséggel, az iskolával, az orvossal kommunikál. A rendszer középpontjában az adatfeldolgozási központ áll: ebben a hivatalban a személyi szám alapján közvetlenül hozzáférhető személyenként kb. 70 különböző fajtájú információ.<sup>27</sup>< Az NSZK-ban ugyan nem volt botrány vagy más egyéb olyan visszaélés az adatokkal, ami törvényhozói megoldásokat kívánt volna, hanem az adatvédelmi jogalkotás inkább egy orwelli világtól való félelmi reakciónak tekinthető. A technológia fejlődése az átlagos személy számára azt jelentette,

---

<sup>27</sup> SÓLYOM László, *Egy új szabadságjog: az információs szabadság*, Világosság, 1988. 1. sz. 25.

hogy minden háztartásban megjelent a televízió, így az orwelli tömegmanipuláció infrastruktúrája kialakult, sőt ismeretlen helyeken, ellenőrizhetetlen elektronikus adatbázisok léteznek, amelyekkel szemben a polgárok biztonságérzetükre hivatkozva védelmet követeltek. Az alapvető jogok védelmét zászlajára tűző politikának ezekre a társadalmi igényekre választ kellett adni a technológiai fejlődés jogi kereteinek meghatározásával. Az adatvédelmet érintő viták a technológiai fejlődés jövőbeni hatására irányultak, amelyek ekkor még csak körvonalaikban látszottak, sok esetben eltúlzott becslések formájában jelentek meg. A jogi szakirodalom<sup>28</sup> azt a véleményt képviselte, hogy a BGB tradicionális jogintézményei, és az általános személyiségi jogot védő Szövetségi Legfelsőbb bírósági ítélkezés elégséges lesz a problémák megoldására, és az USA jogfejlődésére voltak kitékintéssel. A gazdasági élet szereplői nagy ellenérzéssel és kezdetben radikális elutasítással reagáltak arra, hogy információs viszonyaikat az állam újraszabályozza, illetve nyitottá tegye az állami szervek felügyelete számára.<sup>29</sup> A politikai vita ellenére, és a gazdasági szereplő ellenállása ellenére 1970-ben Hessen tartományban hatályba lépett az első adatvédelmi törvény.

Az adatvédelem kérdése az USA-ban elsősorban a tudományos körökben jelentkezett, Norbert Wiener<sup>30</sup> hívta fel a figyelmet a magasan fejlett információtechnológiák veszélyeire. Azt hangsúlyozta, hogy a lakosság manipulálásának eszköze, amely a hatalmi technikák kiterjesztését, és a már hatalmi pozíciókban levők helyzetének a stabilitását szolgálja. Az adatvédelmi technológiák gyors fejlődését semmi sem zavarta kivéve, ha Science-Fiction történetek tárgyává váltak. Az információ technológia jelentősége először akkor tudatosodott, amikor a több évtizedes választási eredményeknek a számítástechnikára alapozott kiértékelését is figyelembe vevő kampány után megnyerte az elnökválasztást a demokrata párti Kennedy.

---

<sup>28</sup> SASSE: Sinn und Unsinn des Datenschutzes, 1976. Neue Juristische Wochenzeitschrift 1971. 673.

<sup>29</sup> ROSSNAGEL, *i.m.*, 195

<sup>30</sup> L. ABEL: Geschichte des Datenschutzes in Handbuch des Datenschutzes; München 2003, 198

Az USA-ban a „right to privacy” témája azzal kapcsolatosan vetődött fel, hogy 1964-ben be akarták vezetni a „National Data Center” elnevezésű rendszert, amely közös adatbázis rendszert hozott volna létre a szövetségi intézmények között. A gazdasági életben az adatvédelem témakörét azt hívta életre, hogy már az 1960-as években széleskörű informatikai rendszer alakult ki a vállalkozások és a polgárok hitelképességének megállapítása tekintetében. A gazdasági életben 1970-ben került bevezetésre a „Fair Credit Report Act”, míg a szövetségi közigazgatásra irányadó normaként 1974-ben a „Privacy Act” került elfogadásra. A két törvény elfogadásával a polgároknak leginkább veszélyeztetettnek tekintett életviszonya szabályozásra került, így az adatvédelem témaköre lekerült a társadalmi-politikai viták napirendjéről. Az USA adatvédelmi joga viszonylag kevés egyedi normatív előírást tartalmaz a hatóságok, vagy a magánjog meghatározott adatkezelői vonatkozásában. Hiányzik a tengerentúlon az olyan adatvédelmi szabályozás, amely széleskörűen, általános jelleggel rendezné az adatvédelem témakörére irányuló elveket, és előírásokat, ehelyett inkább szektor-specifikus reguláció alakult ki.

Az NSZK Szövetségi Parlamentjében a hesseni adatvédelmi törvény elfogadását követően már 1971 decemberében létrejött egy interparlamentális munkacsoport azzal a célkitűzéssel, hogy az adatkezelés feltételeit, adatbankok működtetését, illetve ezek hatósági felügyeletét kidolgozza. A belügyminiszter megbízást adott adatvédelmi tárgyú törvényjavaslat kidolgozására, amely 1973-ban a Bundestagban beterjesztésre is került, de a küszöbön álló parlamenti választások előtt a törvény elfogadására nem került sor. A törvény első olvasatára a választások után került sor a „Datenschutz” munkacsoportban, majd széleskörű szakmai vita következett a gazdasági szereplők, illetve a tartományi közigazgatás szereplőinek bevonásával. A többszöri nyilvános szakmai vitát követően a Bundestag 1976. 06. 10-én elfogadta a szövetségi adatvédelmi törvényt (BDSG), amely 1977 januárjában lépett hatályba. Az adatvédelmi törvényhozás első lépésében az informatikai

adatkezeléssel összefüggő személyes adatok kezelésére irányuló jogszabályokat fektették le:

- az adatfelvételhez és adatfeldolgozáshoz az érintett beleegyezésére vagy jogszabályi felhatalmazásra van szükség;
- az államigazgatás információ szempontjából nem lehet egyetlen egység; ezért a szervek közötti adat-továbbításhoz külön meghatározott törvényi jogalap kell;
- az adatáramlást az eredeti célja általában behatárolja;
- az érintettnek az adatkezelés folyamatában beleegyezési és bizonyos ellenőrzési joga van<sup>31</sup>;

A BDSG elfogadását követően viszonylag hamar megalkotásra kerültek tartományi szinten is az adatvédelmi törvények, illetve a Szövetségi Adatvédelmi Biztos is ellátja a tisztségét 1978-tól kezdve. Az adatvédelmi tárgyú bíráskodás viszonylag későn alakult ki, a BGH 1985-ben hozott elmarasztaló ítéletet Schufa-tag<sup>32</sup> ügyben, és meghatározta az érintettnek a forma követelmények szerinti megkövetelt hozzájáruló nyilatkozatával kapcsolatosan, hogy az adatkezelőt milyen tájékoztatási kötelezettség terheli. A bíróság egyedi ügyekben hozott határozatával egyre inkább tudatosította az adatvédelmi normákat az érintettek, és a jogalkalmazók körében.

Az adatvédelmi törvény megszületése hosszadalmas folyamat volt, és létrejöttét követően szinte minden oldalról kritika érte. Christoph Sasse a törvény rendelkezései között több butaságot talált, mint ésszerű rendelkezést. Némelyek a túlbürokratizálódás tényére hívták fel a figyelmet amellet, hogy a törvény jelentős jogbizonytalanságot hordoz magában. Mások a törvényi rendelkezéseket papírtigrisnek vélték, azt vetették fel kritikaként, hogy az érintettek rosszabb helyzetbe kerültek mint az adatvédelmi szabályozást megelőző időben voltak. A BDGS módosítása már 1981-ben felvetődött, mely

---

<sup>31</sup> SÓLYOM, *Egy új szabadságjog...*, i.m., 25.

<sup>32</sup> BGH NJW 1986, 49

rövidesen a belügyminiszter által beterjesztésre került a Bundestaghoz. Az adatvédelmi jog újabb jelentős változását a BVerfG által a népszámlálási törvénnyel kapcsolatos ítélete<sup>33</sup> hozta. Valójában a népszámlálási törvény parlamenti beterjesztését követően komoly kritika alakult ki a szabályozással szemben, amely gyorsan a határokat nem ismerő állami adatéhség szimbóluma lett. Széleskörű társadalmi tiltakozás alakult ki a törvénnyel szemben. A BVerfG talán meghallva az idők szavát az adatvédelmi normákat alkotmányos rangra emelte. A német Alkotmánybíróság a népszámlálási ítéletében kijelentette, hogy „az egyének védelme érdekében az Alaptörvény (GG) 2.1. bekezdésében meghatározott általános személyiségi jog védelme kiterjed a modern adatkezelés feltételei között zajló, a korlátokat nem ismerő személyes adatok gyűjtése, kezelése, tárolása, illetve továbbítása ellen. Az információs önrendelkezési jog korlátozása kizárólag jelentős közérdekből engedhető meg. De ebben az esetben is szükséges alkotmányos keretek között elfogadott törvényi alap, amely a jogállamiság elvéből fakadó normavilágosság követelményeknek megfelel. Az információs önrendelkezési jog szabályozása során a jogalkotónak az arányosság elvét figyelembe kell vennie, illetve olyan szervezeti és alkotmányjogi intézkedéseket kell tennie, amely a személyiségi jog megsértésének veszélye ellen hatnak. Az alkotmányjogilag indokolható korlátozások esetén meg kell különböztetni a személyre vonatkozó, individualizált adatokat, amelyek nem anonim módon kerülnek megszerzésre azoktól, amelyek kizárólag statisztikai cél szolgálnak...”.

Az BVerfG döntése alapján a szövetségi adatvédelmi törvény módosításra került már 1984-ben. A német adatvédelmi jog fejlődésében jelentős mozzanat az európai adatvédelemi irányelv elfogadása volt, amely az adatvédelmi jog új léptékének is tekinthető, mivel az irányelv olyan új koncepciót vezetett be, amely az NSZK-ban politikailag nem volt végrehajtható. Az EK irányelv német implementációjára 2001-ig várni kellett, és a törvény új rendelkezéseket vezetett be többek között az adattakarékosság elvét, adatvédelmi audit

---

<sup>33</sup> BVerfG 65.1.



szabályait, technológián keresztül adatvédelem rendszerét, lefekteti az adatkezelők önszabályozási jogát, valamint videofelvételekre vonatkozó szabályozást. A törvény alkalmazás köre a magángazdaságra is kiterjesztésre került.

A szakirodalom<sup>34</sup> az adatvédelmi jog fejlődését több egymástól érzékelhetően elkülöníthető fejlődési lépcsőfokra bontja. Az uralkodó nézet szerint az adatvédelem kezdetben a számítástechnikai úton előállított adatbázisokra terjed ki, majd minden nyilvántartásra kiterjed függetlenül annak technikai módszerétől. Majtényi László<sup>35</sup> szerint „az 1970-es évek jogalkotásában megjelent, úgynevezett első generációs adatvédelmi törvények és speciális nemzetközi jogi dokumentumok a számítógépes nyilvántartásoktól (vagy legalább részben automatizált nyilvántartásoktól) védték a polgárokat. Az államok normaalkotására jelentős hatást gyakorolt az OECD adatvédelmi irányelveiként ismert 1980-ban elfogadott „jog dokumentum”, ebbe a körbe tartozik az Európa Tanács 1981-es adatvédelmi egyezménye is. Az 1980-as és 1990-es évek fejleménye a második generációs adatvédelmi törvények megjelenése, amelyben az adatvédelem joga már nem függött az adatrögzítés technikájától. A harmadik generációs jogfejlődés legfontosabb része az 1995-ben elfogadott adatvédelmi irányelv<sup>36</sup>, amely már a fokozódó technikai fejlődésből következő szektorális kihívásokkal áll összefüggésben.” Súlyom László szerint az adatvédelmi törvények első lényegi fordulópontjának az tekinthető, amikor minden állami adatkezelésre kötelezően kiterjesztik az adatvédelmi előírások alkalmazását.<sup>37</sup> Ez a fordulópont a kelet-közép európai országokban akkor következett be, amikor a kommunista diktatúrák belső elhárításainak nyilvántartásait megnyitották, és az új demokráciák biztosítják az érintettek számára az információs kárpótlást azzal, hogy részben

---

<sup>34</sup> JÓRI, *i.m.* részletesen áttekinti a szakirodalomban meglévő nézeteket az adatvédelmi jog fejlődési generációira vonatkozóan

<sup>35</sup> MAJTÉNYI László, *Az információs jogok = Emberi jogok*, szerk. HALMAI Gábor, TÓTH Gábor Attila, Budapest, Osiris, 2003 (Osiris tankönyvek), 583.

<sup>36</sup> Az Európa Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról;

<sup>37</sup> SÓLYOM, *i.m.*, 54.

hozzáférhetnek a besugószervek által magánéletükről, mindennapjaikról készített jelentésekhez.

Rossnagel technológia felosztást követ az adatvédelem fejlődése szempontjából, szerinte az adatvédelem első generációja a számítástechnikai központokhoz köthető, amikor a személyes adatokat formanyomtatványokon gyűjtötték, kézzel került sor az adatrögzítésre, és az érintett életének viszonylag kis szeletére terjed ki az adatkezelő ellenőrzése. Az adatvédelem második fejlődési stációja, akkor következett be, amikor a szerverek hálózata épült ki, és ezen keresztül az internet virtuális világa alakult ki. Az érintett az adatnyomát otthagyja cybertérben, és számára ellenőrizhetetlen az adatok megszerzése, tárolása vagy továbbítása. A fejlődés harmadik lépcsőfokán az adatkezelés az élet minden területére kiterjed, és ezzel a valós és virtuális világ összeolvad<sup>38</sup>.

Az adatvédelem első korszakát egyesek a hesseni adatvédelmi törvényhez, illetve a BDSG megjelenéséhez kötik, míg az adatvédelem második fordulópontjaként mások, így például Baumler, vagy Abel is a BverG 1983-as népszámlálási ítéletéhez köti. A második generációban létrejött adatvédelmi szabályozások már tükrözik az önrendelkezési jog koncepcióját.<sup>39</sup> E felfogás szerint az adatvédelmi jog fejlődésének harmadik stációját az EK irányelvének megjelenése jelenti, és ebben az időszakban a szektorális szabályozások kialakulása jellemző, amelyben már nemcsak az általános hatályú adatvédelmi törvény előírásai követendők, hanem a jogalkotó az alkalmazandó technológia vonatkozásában is meghatároz előírásokat.

---

<sup>38</sup> ROSSNAGEL: Datenschutz im 21. Jahrhundert, Digitalisierung und Datenschutz, in: Aus Politik und Zeitgeschichte 5-6/2006 9.

<sup>39</sup> JÓRI, i.m., 23.

Abek szerint a német adatvédelmi törvények öt különböző fejlődési lépés mentén alakultak ki.<sup>40</sup> Az első csoportba a hesseni adatvédelmi törvény, a szövetségi adatvédelmi törvény, illetve azok a törvények tartoznak, amelyek a BVerG 1983-as népszámlálási ítélete előtt léptek hatályba. A második csoportba azok a törvények tartoznak, amelyek már megfelelnek az ítélet által meghatározott alapjogi követelményeknek, és az adatfeldolgozás folyamata meglehetősen precíz módon van a törvényekben meghatározva, ebbe a körbe tartozik BDSG 1984-es módosítása is. A jogalkotás harmadik lépését elsősorban az 1995-es EK adatvédelmi irányelvének való megfelelés, és másodsorban a PET (Privacy Enhancing Technologie) alkalmazásának jogi alapjainak megteremtése jellemzi. A negyedik fejlődési lépcső TDDSG<sup>41</sup> 1997-es elfogadásával kezdődik, korszak jellemzője, hogy a termékekre, adatfeldolgozási eljárásokra általános követelményeket meghatározzák az adattakarékosság alapelveinek gyakorlati megvalósítását, illetve a szabályozás arra irányul, hogy technikai megoldásokkal támogassák az adatvédelem megvalósítását. (Datenschutz durch Technik) Az ötödik fejlődési szintnek a BDSG 2001-es módosítása tekinthető, amely még egy lépést megtéve pontos meghatározását adja az adattakarékosság szabályrendszerének, illetve nagyobb hangsúlyt fektet az adatfeldolgozási eljárások áttekinthetőségére, és erősíti a felhasználók jogait.

Véleményem szerint az adatvédelem fejlődése szempontjából egyszerre van jelentősége a technológiai megközelítésnek, a nagyobb fejlődési „generációkat” felölelő elméleteknek, az állami információs egyeduralmat megtörő információ hatalommegosztásra épülő megközelítésnek, valamint az adatvédelmi jog szektorális kialakulására koncentráló elméletnek, mivel ezek az elméletek, és megközelítések együttesen tudják leírni az adatvédelem komplex fejlődéstörténetét.

---

<sup>40</sup> L. ABEK, *Geschichte des Datenschutzrechts* = Der neue Datenschutz, Datenschutz in der Informationsgesellschaft von morgen, Hrsg. BÄUMLER, H., Berlin, Luchterhand Verlag, 1998.

<sup>41</sup> Teledienstschutzgesetz

## 2.4. Az adatvédelem fogalmáról

Valójában az adatvédelem Rossnagel szerint egy félrevezető fogalom, mivel nem az adatbirtokos adatait kell valójában védeni, hanem az érintett információs önrendelkezését, mely a Német Alkotmánybíróság (BVerfG) felfogása szerint valójában egy válasz az automatizált adatkezelésből eredő kockázatokra, amely az egyén önmeghatározását veszélyeztetik.<sup>42</sup> Az adatvédelmi jogviszony tehát az adatkezelő és az érintett között létrejövő jogi kapcsolat, amely abból a kötelem keletkeztető tényállásból fakad, hogy az adatkezelő az érintett információs önrendelkezési jogát potenciálisan sértő vagy azt veszélyeztető tevékenységet folytat.

Az adatvédelmi jogalkotás már 1970-ben megkezdődött, de az adatvédelem alkotmányos alapjainak lerakása a BVerfG Mikrocenzus ítéletével<sup>43</sup> kezdődött, amelyben a BVerfG kijelentette, hogy az emberi méltóság része, hogy a polgárok magánéletükkel szabadon rendelkezessenek, és ennek érinthetetlennek kell lennie a közhatalom beavatkozásaitól, ezért a statisztikai célból végzett személyes adatgyűjtések törvényi feltételeit világosabban meg kell határozni. Az emberi méltósággal összeegyeztethetetlen, hogy az egyént úgy kezeljék, mint egy tárgyat, amely előfordulhat, ha az egyén egész személyiségét regisztrálják, katalogizálják. A BVerfG kimondta, hogy a személyről alkotott kép létrehozatalának lehetőségeit törvényi keretek között konkretizálni kell. Az adatvédelem fogalmának további tisztázását a BVerfG az 1983-ban elfogadott (Volkszählungsurteil) népszámlálási ítéletében<sup>44</sup> végezte el. A német Alkotmánybíróság az adatvédelem alkotmányos alapjának az általános személyiségi jogot határozta meg, amelyből levezette az információs önrendelkezési jogot<sup>45</sup>. A német alaptörvény<sup>46</sup> (GG) második

---

<sup>42</sup> Alexander ROSSNAGEL: Datenschutz im 21. Jahrhundert, Digitalisierung und Datenschutz; Das Parlament 5-6/2006; 2006.01.30.

<sup>43</sup> BVerfGE 27.1.(6)

<sup>44</sup> BVerfGE 65. 1. ff In.: *Entscheidungen des Bundesverfassungsgerichts. Studienauswahl*, hrsg. Jürgen SCHWABE, Hamburg, 2004, 45.

<sup>45</sup> Bern HOLZNAGEL, *Recht der IT-Sicherheit*, München, Beck C.H., 2003. 167

<sup>46</sup> Staatsrecht

cikkében van lefektetve az általános személyiségi jog. Ezen alapjog azon beavatkozások ellen nyújt védelmet, amelyek az egyén magánszféráját sértik. Így az általános személyiségi jog tartalmába beletartozik, hogy az egyén külső hatásoktól megvédhesse magát, megfigyelés nélkül visszavonuljon, és egyedül maradjon. Az általános személyiségi jog magába foglalja az önmeghatározás jogát, illetve az egyén azon jogát, hogy magát megvédhesse a lealacsonyító, a hamis vagy nem kívánt nyilvános ábrázolásoktól. Ugyanez az alapjog tartalmazza az egyén jogát, hogy maga határozhassa meg, hogy harmadik személyek felé milyen kép alakuljon ki róla, illetve az egyén kizárólagos joga az is, hogy megmondhassa, hogy mely személy rögzítheti szavait, és ő az, aki meghatározhatja, hogy milyen személyi kör számára lehet a felvett hangszalagot lejátszani. Az általános személyiségi jog biztosítja az egyén jogát az információs önmeghatározásra, amely azt jelenti, hogy alapvetően az egyén dönti el, hogy mikor és milyen határok között teszi nyilvánossá személyes életviszonyait.<sup>47</sup>

A német Alkotmánybíróság elé kerülő kérdés az volt, hogy gyűjtheti-e az állam a polgárok személyes adatait statisztikai célból a népszámlálást helyettesítve a már működő nyilvántartások felhasználásával. A népszavazási törvényben lefektetett adatfeldolgozó program a meglévő nyilvántartások összekapcsolása révén lehetővé tette volna, hogy a polgár élete teljes "átvilágítás" alá kerüljön. A német Alkotmánybíróság meghatározta azokat a követelményeket, amelyek az adatvédelem alkotmányos alapjának, az információs önrendelkezési jognak a tartalmát jelentik.<sup>48</sup> Kimondta, hogy általános személyiségi jogba ütközik a modern adatfeldolgozás viszonyai között a személyes adatok korlátlan megszerzése, feldolgozása, tárolása és továbbítása. A polgárok adatszolgáltatásra csak lényeges közérdekű cél érdekében kötelezhetők, ha azt világos törvényi előírás rendeli el. Az arányosság alapelveinek az adatvédelmi szabályozás körében is érvényesülnie

---

<sup>47</sup> Rolf SCHMIDT, *Grundrechte*, Bremen, Rolf Schmidt Verlag, 2003, 21.

<sup>48</sup> Brunhilde STECKLER, *Grundzüge des EDV-Rechts: das Recht der Datenverarbeitung und der online Daten*, München, Verlag Franz Vahlen, 1999, 21.

kell, ezért az egyén magánszférájába történő beavatkozást a lehető legkisebb mértékűre kell szorítani. A célhoz kötött adatkezelés elve alapján az állami adatgyűjtés során nem lehet több információt az egyénről gyűjteni, mint amennyi az adatkezelés céljának eléréséhez feltétlenül szükséges. Az adatgyűjtés eredeti céljától eltérően nem lehet a személyes adatokat felhasználni kivéve, ha ehhez az adatbirtokos előzetesen hozzájárult. Az adatvédelem vonatkozásában olyan szervezeti és eljárási intézkedéseket kell tenni, amelyek alkalmasak arra, hogy a személyiségi jog megsértésének veszélyét elhárítsák. A BVerfG döntése lefektette az információs hatalommegosztás elvét, így az adatkezelők korlátozva vannak a személyes adatok cseréje és átadása vonatkozásában. Az egyén magánszférája a modern info-kommunikációs technológiák feltételei között különösen veszélyeztetett, mert egy integrált adatfeldolgozó rendszerrel az egyénről személyiség képet lehet felállítani anélkül, hogy az érintett ennek helyességét vagy alkalmazását ellenőrizhetné. Az információs önrendelkezési joggal nem összeegyeztethető egy olyan szabályozás, amely lehetővé teszi, hogy a polgár ne tudhassa, hogy ki, mit, mikor és milyen alkalomból tud róla. Aki bizonytalan, hogy esetleg a viselkedési szabályoktól eltérő magatartását feljegyzik-e, és információként tartósan nem tárolják-e, arra fog törekedni, hogy viselkedése ne tűnjön fel. Aki azzal számol, hogy egy gyűlésen vagy állampolgári kezdeményezésben való részvétele a hatóságok által feljegyzésre kerül, annak érdekében, hogy az esetlegesen keletkező kellemetlenségeket elkerülje, inkább lemond alapjogai gyakorlásáról. Ez nemcsak az egyént korlátozná szabadságának és személyiségének szabad kibontakoztatásában, hanem a szabad cselekvésére és demokratikus részvételére épített közösségi jólétet is, amely a polgárok részvétele nélkül alapvető funkcióját veszítené el.

>Kétségtelen, hogy az adatvédelem a „magánszférához való jogból” ered, de mára kinőtt az intimszférából és legkülönbözőbb önrendelkezési, nemegyszer politikai jogok hordozója lett. Az adatvédelmet el kell szakítani a „személyiség” intimitásaként való értelmezéstől, hanem annak szubjektív és

objektív oldalát is figyelembe kell venni meghatározásakor. A „személyiséget” formálisan kell értelmezni, mint a személlyel kapcsolatba hozható információt: ugyanis bármely adat kerülhet olyan összefüggésbe, hogy annak következtében az érintett mintegy tárgyként mások rendelkezése alá kerül<sup>49</sup>.

## 2.5. A személyes adat fogalma

Az adatvédelmi jogviszony lényegi eleme a személyhez köthető adat jelenléte. A jogrendünk a védendő érdekek, és érzékeny adatok zárt körben történő tartása érdekében titoktartási kötelezettségeket rögzít, így többek között az üzleti titok, a banktitok, a hivatásbeli titok megtartásának kötelezettségét, amelyek átfedhetik a személyes adatok fogalmát és párhuzamos védelmi kötelezettséget telepítenek az adatkezelőkre. A személyes adatok védelme és egyéb titok körök között hasonlóság az abszolút jogviszony fennállása, amely a titokgazdát kötelezi az adat zártan tartására, és kizárólag a titok, vagy az adatbirtokos felhatalmazása, illetve törvényi kifejezett felhatalmazás alapján ismerhetik meg más személyek a védendő adatot. Felmerül azonban az a jogértelmezési probléma, hogy mi tekinthető adatnak, illetve hogyan lehet elhatárolni egymástól az adat és az információ fogalmát. Szükséges-e az adatnak, illetve az információnak a valóságos tényhelyzettel kapcsolatban állni, vagy valótlan, illetve valótlaná vált adatok tekintetében is fennáll a védelmi kötelezettség?

Más tekintetben egyes szabadságjogok, így a véleménynyilvánítási szabadság, vagy a közérdekű adatok nyilvánossága érdekében némely adatfajták nyilvánosak. Egyes esetekben törvényi rendelkezések alapján a személyes adatoknak nemhogy zárt körben történő kezelésükre vagyunk kötelezettek, hanem éppen ezeknek az adatokhoz a nyilvánosság előtti hozzáférését kell

---

<sup>49</sup> SÓLYOM László, *Adatvédelem és személyiségi jog*, Világosság, 1988. 1. sz. 55.

biztosítani. Az Avtv.. alkalmazásában személyes adatnak minősül bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt közvetlenül vagy közvetve név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. A személyes adatok körén belül kiemelt jogi védelmet élveznek a különleges adatok, amelyek a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselési szervezeti tagságra, az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkoznak, illetve ebbe a kategóriába tartozik a bűnügyi személyes adat is.

A személyes adatok védelméről szóló Európa Tanácsi Adatvédelmi Egyezménye<sup>50</sup> szerint személyes adat: bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik (adatalany). Így személyes adatként kell kezelni olyan adatokat is, amelyek ugyan egy egyénre vonatkoznak, de nem feltétlenül hordoznak olyan érdemi információkat, amelyek jogi védelmet igényelnének, de ennek ellenére a jogi védelmet ki kell ezekre az információkra is terjeszteni. A szakirodalom<sup>51</sup> szerint „azonosíthatónak az a személy tekinthető, akinek különálló identitása felismerhető, de személye nem ismert.” A szerzők azt a meghatározást javasolják, amely szerint valaki akkor azonosítható, ha elég információ áll rendelkezésre, hogy elkülönült létezésének, egyénként való lényének tényét tükrözze, és akkor válik azonosítottá, ha elég információ áll rendelkezésre, a

---

<sup>50</sup> 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

<sup>51</sup> Rosemary JAY, Angus HAMILTON, *Data Protection Law and Practice*, London, Sweet and Maxwell, 1999, 108.



vele történő kapcsolatfelvételhez vagy másoktól való valamilyen módon történő megkülönböztetéséhez, felismeréséhez.

Az adatvédelmi biztos állásfoglalásai alapján a szakirodalomban<sup>52</sup> összeállítás készült, és személyes adatnak számítanak pl. a következők:

- név, születési adatok, lakcím, foglalkozás, beosztás, munkahely
- életrajzi adatok
- biometrikus azonosítók, testi jellemzők, ujjlenyomat, retina, írisz, kéz geometriája, hang és arc jellemzői
- vagyonra vonatkozó adatok
- kereset, havi jövedelem
- nyugdíj összege
- bankszámla egyenlege, magánszeméllyel kapcsolatba hozható banktitok
- érintett tulajdonában álló cégek neve, tevékenységi köre
- családi állapot, kiskorú eltartott gyermekek száma
- érintett azonosítására alkalmas kép- vagy hangfelvétel, tárolt felvételek
- beszélgetés során elhangzott vélemény vagy kijelentés
- természetes személy által bonyolított telefonhívások listája (mind a hívó és a hívott fél vonatkozásában)
- természetes személlyel kapcsolatba hozható e-mail cím, webcím, weboldal
- érintett internetezési szokásai, ha azzal azonosíthatóvá válik
- személyiség vizsgálatok eredményei
- adóminősítés során nyert megállapítások
- bizonyítvány tartalma
- fegyelmi vagy etika ügyekben hozott állásfoglalások, határozatok tartalma
- íráskép, vizsgatesztre adott válaszok

---

<sup>52</sup> JÓRI, *i.m.*, 111.

- orvos által kapott hálapénz összege

## 2.6. Különlegesen érzékeny adatok köre

Az Európa Tanácsi Adatvédelmi Egyezményrel összhangban Avtv.. is tartalmazza az alapvető katalógust, amely szerint szenzitív adatoknak számítanak:

- Faji és etnikai adatok, ebbe a csoportba a bőrszínnel kapcsolatos adatok is betartoznak
- Politikai véleményre vonatkozó adatok
- Vallási és világnézeti meggyőződés, amelybe az a tény is védelmet kell hogy kapjon, ha az adott személynek semmilyen vallásos meggyőződése sincsen
- Szakszervezeti tagság
- Egészségi adatok, úgymint korábbi, jelenlegi és jövőbeni fizikai, lelki egészséggel kapcsolatos információk, úgymint drog vagy alkohol használattal összefüggő szokások
- Szexuális szokásokkal kapcsolatos adatok

A különösen védendő személyes adatok kezelésével kapcsolatos korlátozások az EK irányelvvel összhangban a magyar jogban is fennállnak. A személyes adatok körén belül egyes adatoknak a szigorúbb feltételek mellett történő kezelésének megengedése az emberi méltóság, a lelkiismereti szabadság, vallásszabadság védelme miatt szükséges, mivel a törvényalkotó azt vélelmezi, hogy ezen adatoknak az indokolatlan kezelése az érintett információs önrendelkezési jogának közvetlen és súlyos sérelmét eredményezik. Alapvető szempont a különleges adatok kezelése során, hogy a korlátozások alóli kivételeket szűken kell értelmezni. Az adatkezelést lehetővé tevő az érintett részéről tett beleegyezésnek kifejezett nyilatkozatnak kell lennie. Az Avtv.. a kifejezett nyilatkozat adását pontosabban követeli meg,

mivel az érintett részéről tett írásbeli nyilatkozat adásához köti az adatkezelést. Tinnefeld<sup>53</sup> szerint az érzékeny adatok körébe tartozó genetikai adatok tekintetében nem lehet a kifejezett beleegyezés alapján az adatkezelést engedélyezni, hanem az érintett védelmében általános genetikai adatkezelési tilalmat kell a biztosítási szektor és a munkaviszony körében történő adatkezelésre hirdetni.

Az EK adatvédelmi irányelv az érzékeny adatoknak a munkaviszonnyal összefüggésben történő kezelésével kapcsolatosan tilalmat nem állít fel, hanem az adatkezelést az arányosság elve alapján teszi lehetővé. Míg az adatvédelem követelményeit a német jogban szakma specifikus szabályok a német munkajogban részletesen rendezik, addig a magyar jogban kizárólag a köztisztviselői jogállással összefüggésben léteznek részletes adatkezelési előírások, de a munkaviszony létesítésével, és a munkaviszony alatt a munkáltató által kezelhető pszichológiai alkalmassággal összefüggésben nincs olyan rendelkezés, amely a munkavállaló kiszolgáltatottságát az arányosság elve alapján korlátozná.

A magyar Avtv.. az EK irányelv rendelkezéseivel összhangban lehetővé teszi, hogy az érintett életét veszélyeztető helyzetben az ő és mások életének, egészségének megvédése érdekében az adatkezeléshez, ha az adott személy fizikai vagy jogi akadályok miatt nincs abban a helyzetben hozzájárulását adja. Az EK irányelv speciális adatkezelési felhatalmazást ad azon szervezetek számára, amelyek gazdasági tevékenységet nem végeznek, így pl. a vallási célú szerveződések, szakszervezetek, pártok részére, hogy a szervezetükön belül különlegesen védendő személyes adatok tekintetében belső adatkezelési tevékenységet folytassanak.

---

<sup>53</sup> Marie-Theres TINNEFELD, *Menschenwürde, Biomedizin und Datenschutz. Von der Zeit zu handeln* = Zeit und kommunikative Rechtskultur in Europa. Im Spiegel von Deutschen und Polen, hrsg. Siegfried LAMNEK, Marie-Theres TINNEFELD, Baden-Baden, 2000, 381

Az érintett által nyilvánosságra hozott személyes adatok tekintetében az adatkezelési korlátozások csak abban az esetben lépnek előtérbe, ha az adatok kezelése az érintett magánszféráját, alapvető szabadságjogait nem veszélyezteti. Példaként egy politikushoz kapcsolható politikai jellegű adatok kezelésének köre hozható fel, ha az érintett a védendő adatnak számító adatokat önkéntesen nyilvánosságra hozta, nem követelhet semmilyen védelmi igényt. De abban az esetben már korlátozott az adatkezelés, ha olyan adatokról van szó, amelyek jogi igények bíróság előtti érvényesítéséhez, gyakorlásához vagy védelméhez szükségesek. A jogi igények bíróság előtti érvényesítésének fogalma mindazokat a jogi pozíciókat magába foglalja, amelyek a közjog vagy a magánjog területén biztosítanak igényeket<sup>54</sup>. Az EK irányelv lehetővé teszi kezelését mindazon adatoknak, amelyek bűncselekmények, vagy büntetőjogi megítélést igénylő esetekhez vagy biztonsági intézkedések megtételéhez szükségesek, és alkotmányjogilag vagy nemzetközi jogban elfogadott szabályok szerint történik az adatok kezelése.

A személyes adatok fogalmi értelmezésének lényeges eleme, hogy a védendő adatnak egy konkrét élő és azonosítható személyre kell vonatkoznia, és az adat zárt körben történő kezelését, a személy és a rá vonatkozó adat közötti kapcsolat alapozza meg. Így ha az adat bizonyos átalakításra kerül és elveszti az adott személlyel a kapcsolatát úgy, hogy már egy konkrét személy általa később sem lesz azonosítható, akkor az adat zártan történő kezelésének kötelezettsége is megszűnik. A személyre vonatkozó adatok körén belül kizárólag tudományos szempontból személyek közötti, illetve dolgokra vonatkozó személyes adatokat különböztethetünk meg. Így személyek közötti személyes adatnak minősülnek a személy természetes azonosítói, a családi állapota, a foglalkozása, az egészségi állapota, vagy éppen a kommunikációs kapcsolatai, de ebbe a körbe vonható a világnézeti meggyőződése is. Egy személy vagyona, tulajdona, szerződéses vagy más kapcsolata harmadik

---

<sup>54</sup> Alexander ROSSNAGEL (hrsg.), *Handbuch Datenschutzrecht : Die neuen Grundlagen für Wirtschaft und Verwaltung*, München, Beck, 2003, 498.

személyekkel, a személyes adatok dologi aspektusaként értelmezhető, amely természetesen lehetőséget biztosít az érintettre vonatkozó következtetések levonására. Az adatvédelmi törvény alkalmazását az alapozza meg egy adatkör, adatbázis esetében, ha az adat személyes jellege felmerül, így ha az egyén tulajdonsága, jellemzője, vagy azonosítására alkalmas természetes adata, információja alapján egyértelműen meghatározható egyénre vonatkozó következtetés. A személyes adat értelmezése több tekintetben jogalkalmazási kérdéseket vet fel, ezért szükséges a személyes adat fogalmának értelmezési kérdéseit áttekinteni.

## 2.7. Adat, információ, titok

Az információelméletben kialakított definíciók szerint az adat egyik általános megközelítésű fogalma a következő: adatnak nevezünk minden olyan ismeretet, mely előzőleg már rögzítésre került. Míg az információ olyan jelsorozatokat által hordozott hírek minősül, mely egy rendszer számára új ismeretet jelent.<sup>55</sup> Az általános információelméletben a bit egy hír információtartalmának egyik mértékegysége.

Az adat a feljegyzett, rögzített szimbólumokkal is azonosítható. A rögzített szimbólum fogalmát a R. M. Hayes „primitív” fogalomként használja, mivel igazából nem bontja a definíciót. Az adat lehet betű, a mágneses szalag bitje, kimondott szavak, képek, DNS és RNS, pénzügyi számadatok, bármely értelmezhető jelsorozat. Az adat fogalmának értelmezése szinte korlátlan. A mindennapi életben az adat fogalmát gyakran csak a számadatokra redukálják, bár lehetséges sokkal szélesebb értelemben is használni az adat fogalmát. Az adat akár a tapasztalati tény lenyomataként is azonosítható. De valójában különbséget kell tenni a tény és az adat fogalma között, mivel az adatok rögzített jelek, amelyek reprezentálhatják a tényeket. Az adat tehát nem tény, s

---

<sup>55</sup>Claude Elwood SHANNON, Warren WEAVER, *A kommunikáció matematikai elmélete : az információelmélet születése s távlatai*, Budapest, Országos Műszaki Információs Központ és Könyvtár, 1986

ha ilyenként kezeljük, számos tévedést okozhat. Az adatnak, így értelmezve, nem biztos, hogy köze van a való világhoz vagy a tényekhez.<sup>56</sup>

A magyar Avtv.. megalkotása során az információelméleti definíciókat nem vették figyelembe, de az adat fogalmának meghatározása érdekében szükséges a személyes adat, illetve a közérdekű adat eltérő alkalmazásának fogalmi áttekintése. A közérdekű adat fogalom körébe tartozik az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől. A közérdekű adat megismerése iránt indított perekben az eljáró bíróságok a közérdekű adat fogalmának kézzelfoghatósága érdekében kizárólag akkor találják a kereseti kérelmet megalapozottnak, ha a felperes a közérdekű adatot tartalmazó dokumentumot egyértelműen megjelöli. Így a bírói jogfelfogás a közérdekű adat megismerését dokumentumhoz kötötten biztosítja. A bírói jogfelfogás oka, hogy egyértelműen körülhatárolható tények alapján lehet bírósági ítéletet hozni, így az adat fogalmát megragadható tárgyhoz, a dokumentumhoz kell kötni. A közérdekű adatok nyilvánosságra hozatalának másik korlátja a személyes adatok védelme mellett az államtitok és szolgálati titok védelme. Tekintettel arra, hogy a személyes adat a titokvédelmi szabályok alapján minősített adattá válhat, szükséges áttekinteni, hogy az adat és információ fogalmát miképpen kodifikálták ezen a jogterületen.

Az adat és az információ fogalmát az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény a minősített adat definíciójával kapcsolatosan használja. Minősített adatnak tekintendő a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló törvényben meghatározott köziratban szereplő, államtitkot vagy szolgálati titkot tartalmazó adat, illetve a szóban közölt államtitkot vagy szolgálati titkot képező információ, továbbá az

---

<sup>56</sup> Robert M. HAYES, *Az információ mérése*, Könyvtári Figyelő, 1994/40, 3. sz. 398.

államtitkot vagy szolgálati titkot képező információt hordozó objektum, technikai eszköz, végső soron a nem tárgyiasult formában megjelenő államtitkot vagy szolgálati titkot képező információ, eljárási mód vagy más ismeretanyag. A törvényi tényállás elemzéséből az a következtetés vonható le, hogy a titokvédelmi törvényben meghatározott definíció az adat és az információ fogalmát azonosítja, egymás szinonimájaként használja, a két definíciónak eltérő jogi tartalmat nem tulajdonít.

A minősített adat és a közérdekű adat között az a szoros összefüggés, hogy mindazon adat, amely nem kerül a minősített adatok kategóriájába automatikusan a közérdekű adat fogalom körébe kerül, így nyilvánosságra hozható, illetve az információszabadságról szóló törvény előírásai szerint nyilvánosságra hozandó.

A titok fogalmának meghatározása érdekében szükséges az ügyvédi törvény<sup>57</sup> előírásait is áttekinteni. A törvény szerint az ügyvédet titoktartási kötelezettség terheli minden olyan tény és adatot illetően, amelyről a hivatásának ellátása során szerzett tudomást. E kötelezettség független az ügyvédi megbízási jogviszony fennállásától, és az ügyvédi működés megszűnése után is fennmarad. A titoktartási kötelezettség kiterjed az ügyvéd által készített és a birtokában levő egyéb iratra is, ha ez a titoktartás körébe tartozó tény, adatot tartalmaz. Az ügyvédnél folytatott hatósági vizsgálat során az ügyvéd nem tárhatja fel a megbízójára vonatkozó iratokat és adatokat, de a hatóság eljárását nem akadályozhatja.

Az ügyvédi törvényben szereplő definíció lényeges különbsége a korábban értelmezett fogalmaktól, hogy használja a tény kifejezést. A tény fogalmának értelmezése további kibontást igényel. A tény a való világra vonatkozó megállapítás, amelynek igazságtartalma tapasztalati úton ellenőrizhetőnek kell lennie. A valós ténynek bizonyítási eszközökkel alátámasztottnak kell lennie. Az igazolhatóság a ténynek lényegi elemét képezi, mivel ez tükrözi a

---

<sup>57</sup> 1998. évi XI. törvény az ügyvédekről

bizonyosság fokát és ebből eredően a ténybe vetett bizalmat. A tény fogalmától elválaszthatatlan annak ellenőrzésének lehetősége. Az, hogy valami tény, nem jelenti azt, hogy igaz, pusztán annyit, hogy annak jelentéstartalma, más szóval igazsága, ellenőrizhető. Bár a tények a való világot tükrözik, sohasem teljeseek, szükségszerűen mindig hiányosak, mivel a valóságnak időben később rekonstruált valamely szempont szerint lényegesnek minősített részletei. A tény a való világ kivonata, így csak részben tükrözi a világ bonyolultságát. Legjobb esetben olyan eszköz, amely lehetővé teszi, hogy a világot bizonyos szempontból és bizonyos célból kezeljük.

Véleményem szerint a személyes és a közérdekű adatok elhatárolását jobban biztosítaná, ha a törvényi előírások az adat fogalmát kizárólag a személyes jellegű, míg az információ fogalmát a közérdekű, illetve a minősített körbe tartozó ismeretekre alkalmazná. A tény fogalmának mind a személyes adat, mind a közérdekű, illetve minősített információ definíciójában meg kellene jelennie, mivel a tény az adat és információ ellenőrizhetőségének lehetőségét, és a valósághoz történő kapcsolatát szolgálja. A személyes adatok, és a közérdekű, illetve a minősített információk további közös vonása, az adatok és az információk megjelenési formája. Ezért az adatvédelmi és a titokvédelmi törvényben a dokumentáció, és az irat fogalmát egységesen meg kellene határozni, amely felölelné az adatkezelés hagyományos, papír alapú, illetve annak digitális formáját a számítógépek merevlemezein, adatbázisokban, illetve bármilyen képi, hang vagy más jellegű adathordozón függetlenül annak fizikai megjelenési formájától.

## 2.8. Személyes adatok reindividualizálhatósága

Az adatoknak a személyre vonatkozó jellege relativizálható, bár vannak olyan természetes azonosítók, amelyek esetében nem is beszélhetünk arról, hogy



valaha ezen adatok elvesztenék személyes jellegüket, így a név, a születési idő, születési hely vagy az anyja neve egy adott személynek mindig személyes adatnak fognak minősülni. De a személyes adatok nagy többségénél a személyre vonatkozó jelleg relativizálható<sup>58</sup>. Sőt sok esetben egyes adatok, így például az IP-címek közvetlenül, önmagukban nem hordoznak olyan tulajdonságot, amely alapján személyes adatnak minősülnének, de más adatokkal történő összekapcsolás után elnyerik személyes jelleget is hordozó tulajdonságukat.

A személyes adatokra vonatkozó törvényi előírások alkalmazásának előfeltétele, hogy megállapítható-e egy személy érintettsége az adott adaton keresztül vagy nem. Ebben a kérdésben a nehézséget az okozza, hogy a személyre vonatkozó információ nem csak önmagából az adatból nyerhető, hanem még az adatokon kívül két egyéb faktor is meghatározza az adat személyes jellegét. Az egyik ilyen faktor az adatnak a re-individualizálhatósága, amely egy matematikai számsor mögé rejtett személy újbóli azonosíthatóságát jelenti. Tehát a matematikai számsor csak akkor nem kezelhető személyes adatként, ha maga a matematikai számsorhoz kapcsolódó adatkezelés rendszere zárja ki a reindividualizálhatóságot. Az adatvédelemi szakirodalom szerint a reindividualizálhatóság soha sem zárható ki teljesen, kizárólag annak valószínűsége térképezhető fel.

A reindividualizálhatóság kizárásához az anonim adatok kínálják a megfelelő megoldásokat, de valóságban az ügyviteli folyamatokban nem anonimizálják a személyes adatokat, hanem az egyes személyeket aggregált adatokkal azonosítják, emellett korlátozzák a hozzáférést, vagyis az adatkezelő különböző terjedelmű felhasználói jogosítványok alapján biztosít hozzáférést az aggregált adatokhoz, de a legfelső szintű felhasználói jogosítvány lehetővé

---

<sup>58</sup> Siegfried LAMNEK, Marie-Theres TINNEFELD, *Zeit und kommunikative Rechtskultur in Europa*, Baden-Baden, 2000, 185

teheti az aggregált adatok visszafejtését, és egy konkrét személyhez történő hozzárendelését.

Az aggregált adatokból történő visszafejtési lehetőségek, így a személyes jelleg megállapíthatósága nem magában az adat jellegéből erednek, hanem az adattól független külső tényezők határozzák meg. A reindividualizálhatóság valójában az adatkezelés metodikájától és módszertanától függ, amely matematikai módszereken alapul. Így például egy vizsgaeredménnyel összekapcsolt hallgatói azonosító szám a hallgatót mindazok számára azonosíthatóvá teszi, akik ismerik, hogy az adott hallgatónak mi az azonosító száma. Az azonosító számhoz hozzáférhet az oktató, a tanulmányi osztály, de a hallgató társak is ismerhetik egymás azonosító számát. Más esetben így például a dinamikus IP cím kiosztás esetén az adott felhasználó már sokkal nehezebben azonosítható, mivel az IP címek véletlenszerű kiosztása alapján az internet felhasználói címet kizárólag a tárhely szolgáltató legmagasabb szintű felhasználó jogosítvánnyal rendelkező vezetője képes visszafejteni a szerver működésébe történő beavatkozással. Az adat reindividualizálhatósága, azaz személyes jellegének megléte elég jelentősen relatív körülmény. Az adat reindividualizálhatósága, így az adat személyes jellegének megőrzése, nagymértékben attól függ, hogy milyen viszony áll fenn az adat és az adatkezelés között.

A személyes adatok reindividualizálhatóságával kapcsolatosan két eltérő álláspont alakult ki, ugyanazon normaszöveggel kapcsolatosan. Az Avtv.. szerint a személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg a kapcsolat az érintettel helyreállítható. Így az adatvédelmi biztos álláspontja szerint nem önmagában az adatkezelőnek kell a kapcsolatot helyreállítani az Avtv.. hatálya alá eső adatkezeléshez, hanem ha az adatok bárki által reindividualizálhatók, akkor az Avtv.. előírásait kell az adatgyűjtésre alkalmazni. A hatósági felfogás szerint például a gépjárművek hatósági jelzései, így a rendszámok nem minősülnek személyes adatnak,

ebből következően az autópályakezelő számítógépes rendszerének részét képező, gépjárművek rendszám-tábla adatait rögzítő kamerák sem végeznek adatgyűjtést. A német Autobahnmautgesetz<sup>59</sup> által gyűjtött adatok közvetlenül nem esnek a német adatvédelmi törvény hatálya alá, de az adatvédelmi szakértők és hatóságok kifogásolják, hogy túl széles körben történik az adatgyűjtés, és a rendőrség, illetve az ügyészségi hatóságok négy évig is hozzáférhetnek az adatokhoz<sup>60</sup>.

## 2.9. Élő természetes személyek adatai

Az Avtv.. indoklása szerint „az információs önrendelkezési jog szükségképpen az adattal érintett élő személyt illeti meg. A meghalt személy adatainak védelméről, illetőleg a velük való rendelkezésről – az adattal vagy az adatkezeléssel összefüggő külön jogszabályok szólnak (pl: Ptk., levéltári törvény, anyakönyvi jogszabályok”. A személyes adatok szektorális kezelésével foglalkozó Eüatv<sup>61</sup> 3.§ a) pontja szerint „egészségügyi személyes adat: az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátó hálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (pl. magatartás, környezet, foglalkozás).” Az egészségügyi személyes adatok védelmére vonatkozóan egyrészt az orvosi titok, másrészt az egészségügyi dokumentáció fogalma adja meg a jogi keretet, amely alapján a védendő adatok kötelezettje, a védett adatok tárgyiasult megjelenése meghatározható,

---

<sup>59</sup> Gesetz über die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen (Autobahnmautgesetz für schwere Nutzfahrzeuge - ABMG)

<sup>60</sup> Peter SCHAAR, Regeln und Grenzen für Erfassung, Speicherung und Verwendung von Daten. [http://www.bfdi.bund.de/nr\\_531026/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2006/GlaesernerAutofahrerUnterGeneralverdacht.html](http://www.bfdi.bund.de/nr_531026/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2006/GlaesernerAutofahrerUnterGeneralverdacht.html) ; 2006.11.20.

<sup>61</sup>1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

és a védelem az iratkezelési szabályokkal biztosítható. Az orvosi titok körébe tartozik a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat. Mivel az orvosi szakmai szabályok szerint a gyógykezelésre vonatkozó minden adatot és információt rögzíteni kell, így az egészségügyi dokumentáció fogalmát is meghatározza a törvény. Egészségügyi dokumentáció az, ami a gyógykezelés során a betegellátó tudomására jutott, egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától.

Azon alapelv alól, hogy az adatvédelem kizárólag élő természetes személyekre vonatkozik, kivételt tesz az átvilágítási törvény<sup>62</sup>. Anonimizált formában bárki megismerheti és nyilvánosságra hozhatja az Állambiztonsági Szolgálatok Levéltárában kezelt iratokat. De azon személyek esetében, akik érintettnek minősülnek, így minden olyan természetes személy, akinek személyes adata az Állambiztonsági Szolgálatok Történeti Levéltára (a továbbiakban: Levéltár) kezelésében levő iratokban bármilyen jogcímen szerepel, legyen az hálózati személy, megfigyelt, vagy hivatásos alkalmazott, az adatai a halálozási évét követő harminc év után anonimizálás nélkül megismerhetők. Ha a halálozás éve nem ismert, a védelmi idő az érintett születésétől számított kilencven év, ha pedig a születés és a halálozás időpontja sem ismert, az irat keletkezésétől számított hatvan év. Az érintett halálozási évét követő hatvan évig anonimizáltan sem ismerhetők meg a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a vallásos vagy más világnézeti meggyőződésre, az egészségi állapotra, kóros szenvedélyre és szexuális életre vonatkozó adatok. Ha a halálozás éve nem ismert, a védelmi idő az érintett születésétől számított százhusz év, ha pedig a születés és a halálozás időpontja sem ismert, az irat keletkezésétől számított kilencven év.

---

<sup>62</sup> 2003. évi III. törvény az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról

Az adatvédelmi biztos álláspontja szerint ugyan a halál időpontjában megszűnik az adatvédelmi jog hatálya, de egy esetben azért marasztalt el egy bulvár újságot, mert egy a futballpályán szívelégtelenségben eszméletlen sportoló újraélesztését címlapon közölte, és ezzel álláspontja szerint megsértette a haldokló emberi méltóságát. Abban az állapotban a sportoló még élt, egészségi állapotáról a kép alapján következtetést lehetett levonni, és ebben az esetben az egészségügyi személyes adat nyilvánosságra hozásához az érintett beleegyezésére lett volna szükség.

## 2.10. Jogi személyek jogvédelme és az adatvédelem

Az adatvédelem érintettjei tekintetében az Európai Unió tagállamaiban kétféle markáns felfogás létezik. Az uralkodó megközelítés szerint az adatvédelem centrumában a természetes személyekre vonatkozó adatok védelme áll, a másik szabályozási gyakorlat alapján így pl. Svájcban, Ausztriában és Norvégiában minden, a jogi személyek adatai is védelmet élveznek.

Az adatvédelem uralkodó felfogása szerint az információs önrendelkezési jog védelme minden élő természetes személyre kiterjed. A német BDSG védelemben részesíti a személyek csoportjait összekapcsoló szervezeteket is, de csak abban a vonatkozásban, hogy a természetes személyeknek milyen a kapcsolati hálója van a szervezeten belül más természetes személyekkel, illetve milyen vonatkozásban kapcsolódik a természetes személy a jogi személyhez. A német telekommunikációs jogban megfogalmazott adatvédelem kiterjed minden személyre, így a természetes személyek mellett azon jogi személyekre, akik képesek jogokat megszerezni, és kötelezettségeket vállalni. A német TKG<sup>63</sup> szerint a távközlési titok minden egyedi üzenetre kiterjed függetlenül attól, hogy az természetes személytől származik, vagy jogi

---

<sup>63</sup> Telekommunikationsgesetz

személy törvényes képviselőjén belül eljárva adta ki valamely természetes személy.

Ha a magyar elektronikus hírközlésről szóló 2003. évi C törvényben keressük a távközlési vagy a hírközlési titok fogalmát nem találjuk, helyette a személyes adatok körén belül védendő adatokra vonatkozó rendelkezéseket találunk. Az elektronikus hírközléssel kapcsolatos adatvédelem biztosítására tekintettel érdemes a személyes adatok reindividualizálhatóságának a kérdéskörét áttekinteni.

Az Alkotmánybíróság a 34/1994. (VI.24.) AB határozatában úgy foglalt állást, hogy a természetes személyekkel kapcsolatba hozható adatok védelmére irányadó rendelkezéseket alkalmazni kell szervezetekre is. Ez az álláspont arra vezethető vissza, hogy általában az alapjogok nyújtotta általános védelmet jogi személyek is érvényesíthetik, mint pl. a Ptk.-ban meghatározott személyiségi jogok körén belül az üzleti titok védelmére vonatkozó szabályokat, de az Avtv.-ben rögzített szabályokat kizárólag természetes személyekkel összefüggésbe hozható adatkezelések esetén kell figyelembe venni<sup>64</sup>.

Álláspontom szerint szükséges lenne egységes elvi keretekbe történő foglalása annak, hogy jogi személyen belül a természetes személyek közötti kapcsolati hálózatra is kiterjedjen az információs önrendelkezési jog által biztosított védelem. Ha a jogi személyek és tagjaikra vonatkozó adatvédelmi szabályokat áttekintjük, az információs önrendelkezési jog különböző szintű korlátozásai figyelhetőek meg. A védelem legmagasabb fokán azok a jogi személyekkel kapcsolatba hozható személyes adatok állnak, amelyekből a jogi személy jellegéből adódóan egyértelmű és világos következtetés vonható le az adott személynek a lelkiismereti szabadság körébe tartozó meggyőződésre. Így egy párttagság, szakszervezeti tagság, vagy egy felekezethez történő tartozásból az egyén lelkiismereti meggyőződésére, kapcsolatrendszerére lehet következtetéseket levonni. A védelem legfelső szintjén álló adatok a

---

<sup>64</sup> JÓRI, *i.m.*, 117.

különleges adatok körébe sorolandók, mivel ezen adatok tekintetében a törvényalkotónak jelentősen korlátozottak azok a legitim indokai, hogy az egyénnek az adatok feletti rendelkezési jogát korlátozza, és az adatok kötelező kiadását rendelje el.

Az egyén és a jogi személyek közötti második védelmi szinten a törvényalkotó önmagában a jogi személyhez történő tartozás jogcímén egyes személyes adatoknak a kötelező megosztását rendeli el. Így a gazdasági élet hatósági ellenőrizhetősége érdekében a gazdasági társaságok ügyvezetőinek, tagjainak az adatait a cégjegyzékbe, adóhatósági nyilvántartásokba kell bejelenteni, és adatváltozásokat folyamatosan szigorú kötelezettségek mellett a hatóságok részére történő bejelentéssel vezetni. A jogi személy és az egyén közötti kapcsolat vonatkozásában a törvényalkotó nemcsak adatszolgáltatást, hanem az adatok kötelező nyilvánosságra hozását is elrendelheti a gazdasági verseny tisztasága és tisztességessége, valamint a hitelezők biztonsága érdekében. A magyar cégjegyzékben szereplő cégszemélyes adatok nyilvánosságát az állam viszonylag széles körben garantálta. A cégtörvény (Ctv) 2009-es módosítása adatvédelmi szempontból korlátozta a vezető tisztségviselők, valamint a társaság tagjainak egyes személyes adatainak megismerhetőségét, mivel a korábban teljesen nyilvános lakcím adatok kiadására akkor kerülhet sor, ha az érdeklődő igazolja jogos érdekét a személyes adat megismerése tekintetében.

Álláspontom szerint a jogalkotó adatvédelmi szempontból indokolt módon korlátozta a társaságoknak a nyilvánosság általi teljes átláthatóságát, mivel a vezető tisztségviselők, tagok lakcím adatainak nyilvánossága közvetlen módon nincs összefüggésben a gazdasági életben megkövetelt tisztességességgel, valamint a hitelezők jogos érdekeinek védelmével. A jogi személyek és egyének kapcsolatainak adatvédelmi szempontú rendszerének második lépcsőfokán az információs önrendelkezési jog korlátozása akkor indokolható az alapjog korlátozás arányossági és szükségességi elvei között, ha az

alkotmányos érték, vagy alapjog közvetlenül sürgető érvényre juttatása szükséges.

A jogi személyek és a természetes személyek kapcsolatrendszerének adatvédelmi jellegű szabályozásának a harmadik szintjen a jogalkotó széleskörű felhatalmazással rendelkezik az információs önrendelkezési jog korlátozására, így egyes személyes adatnak közérdekű adattá, vagy közérdekből nyilvános adattá történő minősítésében. Az információs önrendelkezési jog korlátozásának oka lehet a közhatalmi jogosítvány gyakorlása, közmegbízatus betöltése, közügyek átlátható működésének biztosítása, vagy éppen az állami, önkormányzati vagyonnal történő gazdálkodás, illetve központi, önkormányzati költségvetésből, illetve Európai Unió forrásaiból jutott támogatások felhasználása. Az információs önrendelkezési jog korlátozásának indoka közvetlen és széleskörűen megalapozott.

#### I. rész összegzése: Az adatvédelem fogalmi keretei

Az adatvédelem alapfogalmainak és a fejlődésének áttekintése alapján véleményem szerint két markáns, eltérő fejlődési tendencia különíthető el. Nyugat-Európában az információs önrendelkezési jog elsősorban technológia szabályozási céllal jött létre, de a megszületését követő másfél évtizeden belül alkotmányos elismertséget és ezzel együtt alapvető jogi jelleget nyert az állam által végzett adatkezelések vonatkozásában. Az adatvédelem, mint technológia szabályozás elterjesztése a magánjog körébe tartozó adatkezelőkre korántsem ment olyan gyorsan, mint ahogy az adatvédelmi jog első fejlődési szakaszában a vertikális jogviszonyokra vonatkozóan megvalósult. Míg az állami adatkezelés tekintetében 1970-ben az első német szabályozás megvalósult, addig a magán adatkezelőkre az állami adatvédelem szabályrendszerét kizárólag az EK irányelvből fakadó belső jogalkotási kényszer miatt sikerült olyan módon kiterjeszteni, ahogy a vertikális jellegű állami adatkezelésekre



vonatkozóan korábban már megvalósult. A német nemzeti szabályozás sokáig ellenállt annak, hogy a vertikális jogviszonyokra kialakított információs önrendelkezési szabályokat magánjog körébe tartozó horizontális jogviszonyokra is alkalmazzák.

Az adatvédelem fejlődésének közép-kelet európai útját leginkább a magyar adatvédelem fejlődésével lehet szimbolizálni. A magyar fejlődés sajátossága, hogy a diktatórikus rendszer lebomlása, és új demokratikus kormányzati rendszer kialakulása egy időben zajlott le az adatvédelem nemzeti jogba történő recepciójával együtt. Ezért kelet-közép európai szemmel nézve az adatvédelem valójában lényeges garancia a megfigyelés, és titkolózásra épülő diktatórikus kormányzat ellen. A magyar adatvédelem kezdettől fogva összekapcsolódott az információ szabadsággal, ezért a magyar információs jogi fejlődés kezdettől fogva átpolitizálódott, mivel eszközzé vált a demokratikus kormányzati rendszerbe történő átmenethez, és az adatvédelem technológiai szempontú megközelítése másodlagos maradt. Másrészt ezekben az országokban az adatvédelmi jogalkotás haladó gondolkodói az Európa Tanács Adatvédelmi Egyezménye alapján olyan adatvédelmi jogi recepciót készítettek elő, amely kezdettől fogva egyenlőséget tett az állami adatkezelés, és a magán adatkezelés között. Ezáltal a magyar jogban az adatvédelem egyszerre alakult ki a horizontális és vertikális viszonyokban, így a magyar szabályozás már az uniós csatlakozásunk előtt nagyjából megfelelt az információs önrendelkezési jog széleskörű érvényesítését célzó EK irányelv követelményeinek.

## II. RÉSZ A SZEMÉLYES ADATOK VÉDELME NEMZETKÖZI SZÍNTÉREN ÉS AZ EURÓPAI UNIÓBAN

### 3. FEJEZET: A SZEMÉLYES ADATOK VÉDELME A NEMZETKÖZI SZÍNTÉREN

Az adatvédelem nemzeti szabályozásával párhuzamosan a nemzetközi szervezetek keretei között is szabályozási elvek alakultak ki, hogy az informatika, a számítástechnika egyre szélesebb körben való elterjedését a megfelelő keretek között tartsa. Az informatikai fejlődés magával hozta a határokat bármilyen kontroll nélkül átlépő adatáramlást, amelynek kezelése az adatvédelem nemzetközi szabályozása nélkül nem vezethet eredményre<sup>65</sup>. 1973-ban az Európa Tanács Miniszteri Bizottsága adott ki ajánlásokat az egyének magánéletének védelméről a magán, illetve állami szektorban tárolt elektronikus adatbankokra vonatkozóan. 1980-ban az OECD a magánélet védelméről, és a személyes adatok határon átnyúló továbbításáról bocsátott ki irányelveket, ezt 1981-ben az Európa Tanács keretében elfogadott Adatvédelmi Egyezmény követte. A nemzeti és nemzetközi szintén párhuzamosan futó jogfejlődés az európai közösségeket is elérte az 1990-es évek elejére, és elindította az uniós adatvédelmi jog kialakítását.

#### 3.1. Az OECD tanácsának adatvédelmi irányelvei<sup>66</sup>

Az informatikai ipar növekedésével párhuzamosan felmerült annak a kérdése, hogy alapvető jelleggel, nem kötelező módon, határokon átívelő szolgáltatásokhoz kapcsolódóan az adatvédelem minimális normáit le kell fektetni az informatikai ágazatot érintő jogi szabályozás kialakításához. Az

---

<sup>65</sup> F. HATÓ Katalin, *Adatbiztonság, adatvédelem* [önálló tanulásra], Budapest, SZÁMALK, 2000, 12

<sup>66</sup> I [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html); 2006.05.10. Az irányelvek kivonatos közlése Infófilia 1992. Az OECD irányelvekről ír még JÓRI, *i.m.*,28.

OECD által 1980-ban elfogadott globalizált adatvédelem ajánlásai között fogalmazódik meg a korlátozott adatgyűjtés elve, amely az adatgyűjtések törvényes alapját kívánja meg azzal, hogy lehetőség szerint az adatalany hozzájárulását az adatgyűjtéshez biztosítani kell. Az adatvédelem célhoz kötöttségének az elve az OECD ajánlásban is megjelenik azzal, hogy az adatgyűjtést megelőzően ki kell tűzni annak célját, és az adatgyűjtést csak a törvényileg meghatározott célra kell korlátozni. Az irányelvben megjelenik az adatok minőségével szemben támasztott követelmény, hogy az adatok pontosak, teljesek, időszerűek legyenek. Az adatbiztonság elve is lefektetésre került az irányelvben, amely előírja, hogy az adatokat védeni kell az illetéktelen hozzáféréstől, azok jogosulatlan megváltoztatásától, és azok megsemmisülésétől. Az OECD részes tagjainak ajánlja, hogy az érintettek számára jogokat kellene biztosítani, hogy tájékoztatást kapjon adatairól, az adatkezelőről, az adatkezelés feltételeiről, illetve számára lehetővé kellene tenni, hogy sérelem esetén jogorvoslati út álljon számára nyitva. Az irányelv javasolja, hogy jogsérelem esetén az érintett adatait töröljék, helyesbítsék, illetve kiegészítsék, továbbá az irányelv lefekteti az adatkezelők elszámoltathatóságának elvét. Az OECD ajánlását követően 1981-ben az Európa Tanács keretén belül is elfogadásra került a számítógépes adatfeldolgozás során a magánszféra és a személyes adatok védelméről szóló nemzetközi egyezmény.

### 3.2. Az ENSZ adatvédelmi állásfoglalása

Az 1960-as évek óta foglalkozott az ENSZ azzal a kérdéssel, hogy az elektronikus adatfeldolgozás milyen hatást gyakorol az emberi jogokra. Az ENSZ Emberi Jogi Bizottsága<sup>67</sup> és a Főtitkárság<sup>68</sup> több jelentés keretében

---

<sup>67</sup> Commission on Human Rights: Human Rights and Scientific and Technological Developments, Report of the Secretary General – UN Dok. E/CH. 4/1028;

<sup>68</sup> Report of the Secretary General, UN Economic and Social Council, Human Rights and Scientific and Technological Developments, Uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in democratic society – UN Doc. E/CN. 4/1192

vizsgálta a kérdéskört. Az előkészítő munka eredményeképpen 1990-re egy irányelv tervezet készült el a személyes adatokat tartalmazó akták számítógépes feldolgozása vonatkozásában,<sup>69</sup> amely mind a magán és mind a közjog körébe tartozó adatkezelőkre, illetve az automatizált és a manuális adatfeldolgozásra egyaránt irányadónak tekintettek. Az irányelv négy strukturális elemet határozott meg, így az adatok minőségének biztosítását, a célhoz kötöttség meghatározását, az érintettek betekintési jogainak biztosítását, illetve az adatbiztonság követelményeinek teljesítését. Az irányelv új alapelvként határozza meg a hátrányos megkülönböztetés tilalmát, amelyet az érzékeny adatok vonatkozásában bír fontos jelentőséggel. Az irányelv meghatározza azokat a különös okokat is, amely esetekben el lehet térni ezektől az alapelvektől. Törvényekben vagy más jogszabályokban kell a kivételeket szabályozni, amelyek alkalmazására csak a szükséges esetben kerülhet sor, ha a nemzetbiztonság, a közbiztonság, a közegészségügy, vagy az erkölcs, illetve mások jogainak vagy szabadságának a megóvása érdekében van erre szükség. Az ENSZ ajánlja, hogy megfelelő felügyelő hatóságot kell létrehozni az adatvédelem követelményeinek teljesítése érdekében. A határon átnyúló adatforgalom vonatkozásában az ENSZ irányelve alapján mind a küldő, mind a fogadó oldalán az azonos mértékű védelmet kell biztosítani. Az irányelv 10. pontjában tekintve a humanitárius tevékenység speciális vonatkozásait megengedi, hogy az adatvédelem alapelveinek alkalmazásától humanitárius okból eltekintsenek, ha az adatgyűjtés célja az alapszabadságok biztosítása, illetve humanitárius intézkedések végrehajtása. Az ENSZ az adatvédelmi irányelvvel saját szervezetére vonatkozóan jogi előírásokat határozott meg, és a tagállamok számára nem kötelező jellegű ajánlásokat adott.

---

<sup>69</sup> Guidelines Concerning Computerized Personal Data Files; Resolution 44/132; elfogadva 1990.12.14 UN. Doc. E/CN.4/Sub. 2/1988/22

### 3.3. Az Európai Emberi Jogi Egyezmény 8. cikkelye

Az Európai Adatvédelmi Biztos<sup>70</sup> szerint az adatvédelem érdekében az első lépéseket az Európa Tanács keretében tették azzal, hogy az alapvető szabadságokról és az emberi jogokról szóló európai egyezmény<sup>71</sup> 8. cikkelyében lefektették a magán és a családi élet védelmének alapvető szabályait.

A 8. cikk az alábbiak szerint szabályozza a magán- és családi élet tiszteletben tartásához való jogot:

1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.

2. E jog gyakorlásába a hatóság csak a törvényben meghatározott esetekben avatkozhat be, amikor az a demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

A 8. cikk az egyezmény egyik nyitott végű rendelkezése, amely tükröződik abban, hogy milyen szerteágazó esetjog alakult ki. Az adatvédelem alapjogi alapjainak meghatározása szempontjából lényeges az adatokhoz való hozzáférés kérdése, a lakás és levelezés tiszteletben tartása, a távközlési titok követelményeinek kialakítása, illetve a titkos megfigyelés szabályozásának összeegyeztetése a nemzetközi emberi jogi követelményekkel. A 8. cikk alapján az egyéneket megillető védelem kiterjed a fizikai vagy mentális integritásuk vagy morális, illetve intellektuális szabadságuk ellen intézett támadásokra. Azokkal a támadásokkal szemben is védelmet nyújt a 8 cikk,

---

<sup>70</sup> Peter J. Hustinx: Data Protection in the European Union.  
[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2005/05-04-21\\_Data\\_Protection\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2005/05-04-21_Data_Protection_EN.pdf); 2007.01.10

<sup>71</sup> 1993. évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről

amelyek az egyén becsülete, jó hírneve ellen irányul, vagy más sérelmet okoznak, mint a megfigyelések, kikémlelések, zaklatások, illetve olyan információk nyilvánosságra hozatala, amelyek hivatali titoknak minősülnek<sup>72</sup> Az Emberi Jogok Európai Bírósága az egyezmény alkalmazás során az angolszász irodalomban kialakított privacy fogalom alapján határozta meg a 8. cikk tartalmát, amely a magánélet tiszteletben tartására alapulva arra terjed ki, hogy az egyén védve legyen a nyilvánosságtól, arra azonban nem, hogy a személyes adataihoz hozzáférjen.

### 3.3.1. Leander-ügy

A Leander contra Svédország ügyben<sup>73</sup> a panaszos ácsként jelentkezett a svéd haditengerészet múzeumába. Mivel a múzeum részben a közeli haditengerészeti bázison található a panaszosnak biztonsági vizsgálaton kellett átesnie. Az átvilágítás során biztonsági szempontból veszélyesnek minősítették, ezért alkalmazására nem került sor. A panaszos a bíróság előtt azt kifogásolta, hogy nem ismerhette meg azokat a biztonsági kifogásokat, amelyeket vele szemben felhoztak, és ezekkel szemben megfelelően nem tudott védekezni. A bíróság előtt az nem volt kétséges, hogy a rendőrségi nyilvántartás a panaszos magánéletére vonatkozó adatokat tartalmazott, és az a tény, hogy ezeket az adatokat közölték és továbbították, illetve, hogy elutasították kérelmét, ez érintette a panaszos magánélet tiszteletben tartásához való jogát. A bíróság nem állapította meg az egyezmény sérelmét, mert a hivatkozott cikk nem biztosít jogot az egyéneknek arra, hogy hozzáférjenek a saját helyzetét, személyes adatait tartalmazó nyilvántartásokhoz, és a kormányokat sem kötelezi ezek közlésére.

---

<sup>72</sup> Francis G. JACOBS, Robin C.A. WHITE, *The European Convention on Human Rights*, Oxford, Clarendon Press, 2002, 218.

<sup>73</sup> Vincent BERGER, *Az Emberi Jogok Európai Bíróságának joggyakorlata*, Budapest, HVG, 1999, 387.

A Leander-ügy tekinthető az első esetnek, amikor a strasbourgi bíróság az adatvédelmet, mint önállóan meghatározható jogi problematikát elismerte, bár ez a bíróság döntését egyáltalán nem befolyásolta. Bár az ítélet meghozatalát követően pár hónappal lépett hatályba az Európai Adatvédelmi Egyezmény, a bírók az adatvédelmi probléma kapcsán az egyezmény elveit meg sem említették<sup>74</sup>.

### 3.3.2. Klass és társai ügye

Klass ügyvéd<sup>75</sup> és öt jogász kollégája azért fordult az Emberi Jogok Európai Bíróságához 1968-ban, mert az elfogadott új német törvények a levelezés, a postai küldemények, és a telekommunikáció területén szélesebb körben engedélyezik a titkos ellenőrzést, mint korábban. Lehetővé teszik az újonnan elfogadott jogszabályok azt is, hogy az érintettet tájékoztatására ne kerüljön sor akkor sem, ha ez nem veszélyezteti a bűnüldözést. A bíróság két időtálló megállapítást tett, egyik szerint a demokratikus társadalmat a kémkedés és a terrorizmus összetett formái fenyegetik, hogy e veszélyek elleni küzdelem céljából meg kell adni az államoknak a jogot, hogy a területükön működő felforgató elemeket titokban megfigyelhessék. Ezért el kell ismerni, hogy egy demokratikus társadalomban is szükség van a levelezés, a postai küldemények és a telefonbeszélgetések titkos ellenőrzését lehetővé tevő rendelkezésekre a nemzetbiztonság, a közbiztonság valamint a bűncselekmények megelőzése céljából. Másodsorban az egyezmény az ellenőrzési rendszerek tekintetében széleskörű diszkrecionális jogkört biztosít a tagállamoknak, de ez nem jelenti azt, hogy az államok korlátlan szabadsággal bírnának abban, hogy a főhatalmuk alá tartozó személyeket titkos ellenőrzésüknek alá vessék. Számba véve az ilyen törvényekben rejlő veszélyt, mely alááshatja, sőt rombolóan hathat a demokráciára, annak védelmére hivatkozva, a Bíróság

---

<sup>74</sup> SIEMEN 90.

<sup>75</sup> JÓRI u.o., 442.

megállapítja, hogy az államok a kémkedés és a terrorizmus elleni harc címén nem tehetnek bármilyen, általuk megfelelőnek tartott intézkedést. Bármilyen legyen is a titkos megfigyelési rendszer, a bíróságnak meg kell győződnie arról, hogy a visszaélésekkel szemben megfelelő és elégséges biztosíték létezik.

### 3.3.3. Amman-ügy

Amman<sup>76</sup> úr Svájc ellen indított ügyében az Emberi Jogok Európai Bírósága megállapította, hogy a svájci hatóságok megsértették az egyezmény 8. cikkét, az érintett telefonbeszélgetésének lehallgatásával és a magánélet körébe eső személyes adatai titkosszolgálati nyilvántartásával. A jogsértés okaként a Bíróság megállapította, hogy a titkosszolgálati eszközök használatáról és a titkosszolgálati nyilvántartásról szóló svájci jogszabályok jelen ügyre vonatkozóan nem tartalmaznak pontos és részletes szabályokat az információszerzés, az adatrögzítés, és az adatkezelés tekintetében, így az "előre kiszámíthatóság" követelménye nem érvényesült a fenti korlátozásoknál. Az EJEB kimondta, hogy az egyénre vonatkozó információk tárolása a magánéletbe való beavatkozásnak minősül, még akkor is, ha nem tartalmaz szenzitív adatokat. A strasbourgi ítékezés szempontjából mivel ebben a döntésben utal a bíróság az Európai Adatvédelmi Egyezmény elveire, mint amelyek nagyjából egybe esnek a magánélet védelméből levezethető elvekkel. Más ügyben<sup>77</sup> a magánülethez való jog megsértését állapította meg az EJEB, a telefonbeszélgetések adatainak olyan rögzítése során, amikor olyan eszközöket alkalmaznak, amelyek automatikusan rögzítik a telefonon tárcsázott számokat és a hívások időtartamát.

---

<sup>76</sup> Eur. Court H. R., Case of Amann v. Switzerland, judgment of 16 February 2000; 2000-II.; 27798/95. sz. kérelem

<sup>77</sup> Malone v Egyesült Királyság; Eur Court H. R. Case of Malone v the United Kingdom, judgement of 2 August 1984, Series A no. 82 (Hasonló ügyek Huvig Kruslin A v Franciaország; Lüdi v. Svájc)



Az Emberi Jogok Európai Bíróság által kialakított szempontrendszer a személyes adatok védelmének Európai Unió általi szabályozásához több tekintetben kapcsolódik, így a személyes adatnak is minősülő távközlési adatok kötelező megőrzése, illetve a légi utasok adatainak harmadik országba történő továbbítása tekintetében is, amely szabályozások az EU-n belül igen kritikusan vannak megítélve.

#### 3.3.4. Caroline von Hannover ügy<sup>78</sup>

Caroline von Hannover, a monacói herceg idősebb lánya számos közszereplést vállalt a kultúra fejlesztése és segélyezési szervezetek működtetése terén. A bulvár sajtó előszeretettel foglalkozott a hercegnő közszerepléseivel, és rendszeresen készített fényképeket a magánéletéről lovaglás vagy éppen vacsorázás közben. A hercegnő a személyiségi jogainak megsértése miatt Európa több országában pert indított a bulvár sajtóban megjelenő képeinek nyilvánosságra hozása ellen, illetve a róla készült fotóknak a jövőbeni nyilvánosságra hozatalát is meg kívánta tiltatni. A hamburgi városi bíróság 1993 novemberében úgy foglalt állást, hogy a panaszos a jelenlegi történelem egyik „par excellence” személyisége, akinek tűrnie kell a jogos érdekként az őt érő közérdeklődést. A bíróság álláspontja szerint a közszereplőknek a magánlakásuk ajtajától kezdődik a magánélethez való jog, és így arra tekintettel, hogy a róla készült felvételek mind közterületen készültek, nem állapította meg a magánélethez való jog sérelmét. A hamburgi fellebbviteli bíróság helyben hagyta az I. fokú bíróság álláspontját, melyet kiegészített azzal, hogy ugyan megállapítható, hogy a panaszos mindennapi életét megnehezítik a fotósok, de ezt tűrnie kell a közvélemény tájékoztatása érdekében. A német Szövetségi Legfelsőbb Bíróság is egyetértett az alsóbb bíróságokkal, és kifejtette, hogy a panaszosnak tolerálnia kell azon fotók

---

<sup>78</sup>

<http://www.echr.coe.int/ger/Chamber%20judgment%20von%20Hannover%20German%20version.htm>; 2006.11.20

közzétételét, amelyeken ő közterületen tűnik fel, függetlenül attól, hogy a magánéletéből fakadóan vagy éppen hivatali teendői elvégzése okán tartózkodik a közterületen. A legfelsőbb bíróság megtiltotta azoknak a fotóknak a közzétételét, amelyeken a panaszos a gyermekeivel, illetve egy színésszel látható. A legfelsőbb bíróság a fotók közzétételének megtiltását a kiskorúak és családi élet védelmében a sajtószabadság arányos korlátozásaként fogadta el. A közvéleménynek törvényes érdeke tudni, hogy a panaszos miként viselkedik és tartózkodik közterületen. A panaszos a német Szövetségi Alkotmánybírósághoz is fordult, de az a személyiségi jog védelmére vonatkozó német szabályok tekintetében nem állapított meg alapjog sérelmet.

Az kétség kívüli, hogy a német újságokban közzétett fotók, amelyeken a panaszos egyedül vagy más személyekkel a mindennapi élet körülményei között látható, a magánéletet érinti. Az Emberi Jogi Konvenció 8. cikkelye ezért ebben az esetben alkalmazandó. Bár a panaszos által a 8. cikk által hivatkozott védelem nem lehet abszolút, mivel a 10. cikkelyben biztosított szabad véleménynyilvánítás tekintetében korlátozott.

A szabad véleménynyilvánítás esetén is érvényesülni kell a jó hírnév védelmének, illetve figyelembe kell venni, hogy ez esetben nem érvek és vélemények szabad, akár határokon átnyúló terjesztéséről van szó, hanem képekről, amelyek személyes vagy akár intim információkat tartalmaznak egyes emberekről. Másrészt a bulvársajtóban közzétett fotók gyakran olyan körülményeket eredményeznek, amelyek egy állandósult terhet jelentenek az érintett személy számára. Ez a teher a panaszos magánéletét korlátozza, és nem ritkán akár üldözés érzetét kelti.

Az Emberi Jogok Európai Bíróság álláspontja szerint a magánélet védelme és véleménynyilvánítás szabadsága közötti összeütközés esetén azon szempont alapján kell döntenet, hogy a nyilvánosságra hozott fotók hozzájárulnak-e egy olyan vitához, amelyet a közösség, vagy a közérdek tekintetében érvényesíteni lehet. A jelen esetben olyan fotókról van szó, amelyek Caroline von Hannover

magánéletéről készültek, és amelyek kizárólag a magánélet tevékenységeit mutatják. A bíróság figyelembe veszi a panaszos azon kifogását is, amelyek a fotók elkészítésével kapcsolatosak, azaz, hogy a fotókat a panaszos tudta nélkül, az ő beleegyezése nélkül készítették. A bíróság álláspontja szerint a szóban forgó fotókat nem lehet olyan véleménynek tekinteni, amely az általános közérdek tekintetében kialakult vitához való hozzájárulás lenne.

Ugyan a nyilvánosságnak joga van arra, hogy tájékozott legyen, és ez a jog meghatározott körülmények esetén a közélet egyes személyiségeinek a magánéletére is kiterjedhet. A jelen esetben a bíróság szerint ez a jog nem áll fent. A bíróság felfogása szerint a nyilvánosság nem bír jogos érdeklődéssel, hogy megtudja, hogy Caroline von Hannover hol található, és hogy ő általában a magánéletben hogyan viselkedik, még akkor se, ha egy ismert személyiségről van szó. Ugyan fennáll a közvélemény ilyen fajta érdeklődése, és emellett szintén létezik az újságnak egy kereskedelmi érdeke is, hogy a fotókat, és a cikkeket nyilvánosságra hozza, de a Bíróság meglátása szerint a jelen esetben ezen érdekeknek a magánélet védelmére vonatkozó hatékony jogvédelem tekintetében meg kell hajolni.

A bíróság utalt arra, hogy a magánélet védelmének joga kiterjed az egyének személyiségének szabad kibontakoztatására, és megállapította, hogy minden személyről, akiről mint a közélet személyiségéről lehet beszélni, törvényes várakozásokkal rendelkezik, hogy a magánélete tisztelete és védettsége megvalósuljon. A bíróság meglátása szerint a tagállami bíróság által megállapított kritérium, mely szerint a jelenkor személyisége között az alapján tetett különbséget, hogy „abszolút”, illetve „relatív” személynek tekintendő-e, nem biztosít hatékony védelmet a panaszos magánéletének védelme tekintetében.

Mindezek alapján a bíróság meglátása az a tagállamokat ezen a területen megillető mérlegelési kör ellenére, hogy a német bíróság az egymással szembenálló érdekeket nem a konvenció szellemében szerint mérlegelte, és

ezzel a konvenció 8. cikkében a magán, és családi élet tiszteletben tartására vonatkozó jogot megsértette.

Az adatvédelem alapjogi fejlődésének áttekintése csak akkor lehet teljes, ha az adatvédelemnek, mint európai alapjognak<sup>79</sup> az Európai Emberi Jogi Bíróság általi jogfejlesztő tevékenységét is áttekintjük. A strasbourgi ítélkezési gyakorlat kiteljesedése alapján a magánélet védelme körében jogvédelmet kell biztosítani elsősorban a testi, lelki, erkölcsi, és lelki szabadságnak, valamint fel kell lépni a családi élet ellen irányuló beavatkozások ellen. A 8. cikkben rögzített védelem kiterjed a jó hírnév elleni támadások ellen, név,- identitás lopás, vagy más hasonló visszaélések ellen, valamint a megfigyelés, a lehallgatás, vagy a zaklatás ellen. A strasbourgi emberi jogi ítélkezés alapján a magánélet védelme kiterjed továbbá az üzleti titok által védett információk jogosulatlan továbbítása ellen is<sup>80</sup>. Az adatkezelésre vonatkozó strasbourgi standardok elsősorban a büntetőeljárás körében a titkos lehallgatásokkal kapcsolatosan fogalmazódtak meg, első megközelítésre nem kapcsolódnak az adatvédelem európai alapjogi kialakulásához. Kezdetben a strasbourgi ítélkezési gyakorlat alapján a tagállamoknak érvényre kell juttatniuk a nemzeti büntetőeljárások során alkalmazott kényszerintézkedések vonatkozásában az adatvédelmi szabályokat. Az esetválogatás alapján összefoglalható, hogy az európai emberi jogi egyezmény rendszerében az adatvédelem csak egy aspektusa a magán-, és családi élet védelmének. Az EEJB szerint a személyes adatok és a magánélet védelme között egyedi esetekben fennálló, világosan felismerhető vonatkozásnak kell fennállnia. A strasbourgi bíróság ezen viszonyoknak a felismerésében kezdetben igen visszafogott volt, és az adott információ tartalma alapján állapította meg csak a személyes adat visszaélésszerű kezelése esetén a 8. cikkely sérelmét. Ennek következtében az Európai Emberi Jogi Bíróság felfogása szerint csupán a magánszféra körébe tartozó adatokra, de nem az összes személyes adatra terjed ki az EEJ 8.

---

<sup>79</sup> Birte SIEMEN: Datenschutz als europäisches Grundrecht; Duncker und Humblot, Berlin 2005

25.old

<sup>80</sup> SIEMEN 62. old

cikkelyének hatálya. Az utóbbi időkben adta fel az Emberi Jogok Európai Bírósága azt az álláspontját, hogy nem szükséges az adatnak a magánéletre vonatkozó jelleggel (tartalommal) rendelkeznie, hanem önmagában az adatok felhasználásának a módja, vagy az adatok tárolása is megvalósíthatja a magánélet sérelmét. Az utóbbi évek ítélkezési gyakorlatában az Emberi Jogok Európai Bírósága már alkalmazza azt az adatvédelmi terminológiát, amelyet korábban igen konzekvensen elkerülni igyekezett<sup>81</sup>.

Az európai emberi jogi egyezményben lefektetett magánélet védelme cikkely alapján képezte a személyes adatok védelmére irányuló szabályozás kialakításának. A konvencióban rögzített magánélet védelméhez való jog a strasbourgi bíróság ítélkezésében is megjelent többféle megközelítésben. A konvencióban rögzített alapjogokat érintő bírósági ítélkezés során az adatvédelem egy részterületként került megfogalmazásra. Az Emberi Jogok Európai Bírósága az ítélkezése során kerülte az Európai Adatvédelmi Egyezményre történő hivatkozást, mivel azt a felfogást követte, hogy a magánélet védelme körébe sorolható tényállásban szereplő adatnak a magánszférához köthetőnek kell lennie. Így az strasbourgi bíróság a személyes adat fogalmát nem azonosította a magánszféra körébe tartozó adattal, mivel az utóbbi jóval szűkebb kört ölel fel a személyes adatok körén belül.

#### 3.4. Az Európa Tanács Adatvédelmi Egyezménye

Az Emberi Jogok Európai Egyezménye a védendő szabadságok között határozta meg a magánszférához való jogot. E jog mindennapi érvényesülése érdekében az Európa Tanács Parlamenti Bizottsága a hatvanas évek végén vizsgálódni kezdett, hogy a tagállamokban létezik-e a magánszféra védelmének megfelelő szabályrendszere. Az Európa Tanács keretében

---

<sup>81</sup> SIEMEN 329.

ajánlásokat<sup>82</sup> dolgoztak ki arra vonatkozóan, hogy az elektronikus adatbázisok működtetése során hogyan kell védeni a magánszférát<sup>83</sup>. Az Európa Tanács Adatvédelmi Egyezménye<sup>84</sup> az adatvédelem jogi dokumentumok korai generációját képviseli. Az első generációs fejlődése során kimunkált elvek alapján készítették el a korábbi ajánlások figyelembe vételével 1981-re. Az egyezmény<sup>85</sup> a gépi automatizált adatkezelésekre terjed ki, a manuális nyilvántartásokra az alkalmazása nem irányadó. Az egyezményt a magyar kormány képviselői már 1993. május 13-án aláírták, a parlamenti ratifikációjára négy évet kellett várni, majd 1998. február 1-jén a magyar jogban is kihirdették<sup>86</sup>. E késlekedés nem tekinthető kirívónak az egyezmény ratifikációja vonatkozásában. Az Olaszország az elsők között 1983-ban aláírta az egyezményt, de 1995-ig kellett várni annak olasz kihirdetéséig. A magyar késlekedésnek valószínű oka az lehetett, hogy a jogalkotó a szektorális adatvédelmi szabályozást összhangba kívánta hozni az egyezmény szellemével.<sup>87</sup> Az egyezmény magyar aláírásakor a magyar adatvédelmi törvény (Avtv..) már kihirdetésre került, ezért magyar részről az egyezményhez azt a kiegészítő nyilatkozatot tették az ott meghatározott opciók alapján, hogy a magyar jogba nemcsak az elektronikus, illetve automatizált adatfeldolgozási eljárásokban, hanem az minden adatfeldolgozási eljárásban alkalmazandó. A magyar adatvédelmi törvény előkészítése során a jogalkotó már szem előtt tarthatta az egyezmény normáit. Erre vezethető vissza az, hogy az Avtv.. mind szerkezete, belső arányai, mind fogalomalkotása tekintetében rendkívül sok hasonlóságot mutat az

---

<sup>82</sup> . R (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector. <http://tinyurl.com/3fsz9> ; 2006.11.18. és Resolution (74) 29 on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector. <http://tinyurl.com/36olj> ; 2006.06.20.

<sup>83</sup> OROS Paulina, SZURDAY Kinga, *Adatvédelem az Európai Unióban*, Budapest, Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ, Külügyminisztérium, 2003 (Európai füzetek, 35.), 3.

<sup>84</sup> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.:108. Az egyezmény hatályba lépéséhez szükséges volt, hogy legalább öt tagállam kihirdessék. Az Egyezmény 1985. október 01-én lépett hatályba.

<sup>85</sup> Az Egyezmény áttekintését lásd még: DÓSA Imre, POLYÁK Gábor, *Informatikai jogi kézikönyv*, Budapest, KJK-Kerszöv, 2003, 45.

<sup>86</sup> 1998: VI. tv.

<sup>87</sup> MAJTÉNYI László, *Az információs..., i.m.,* 56.

egyezménnyel,<sup>88</sup> amelyet Majtényi László is a magyar adatvédelmi törvény mintájának tart.<sup>89</sup>

Az Európa Tanács Adatvédelmi Egyezménye fogalom meghatározásokkal kezdődik, számba veszi a legfontosabb jogi definíciókat, ezek közül legfontosabb a személyes adatok fogalmának meghatározása. Az egyezmény szerint személyes adat bármely információ, amely egy azonosított vagy azonosítható egyénre, azaz az adatalanya vonatkozik. Az egyezmény alkalmazása szempontjából fontos az adatkezelő meghatározása. 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 egyezmény megnyitja a lehetőséget az előtt, hogy a személyes adatok védelmének garanciáit a részes tagállamok egyesületek, alapítványok vagy gazdasági társaságokra vonatkozóan is alkalmazzák.

Az egyezmény a soron következő 3. cikkében meghatározza az egyezmény tárgyi hatályát, így a személyes adatok automatizált állományaira és a személyes adatok gépi feldolgozása során a köz- és a magánszektorban egyaránt alkalmazni kell az egyezményt. A nemzetközi dokumentum II. fejezete részletezi az adatvédelem alapelveit. Így az egyezmény 5. cikkében előírja az adatok minőségére vonatkozóan, hogy az adatokat csak tisztességesen és törvényesen szabad megszerezni, illetve feldolgozni. Az egyezmény lefekteti az adatok célhoz kötött kezelésének elvét, amely abban a tilalomban is megfogalmazódik, hogy az adatokat az előírt törvényes céltól eltérően módon nem lehet felhasználni. Az egyezményben az arányosság elve is megjelenik, mely szerint az adattárolásnak az adatkezelés céljával arányban

---

<sup>88</sup> BALOGH Zsolt György, *Az adatvédelmi törvény fejlesztésének kérdései*, Jogtudományi Közlöny, 1997/52, 6. sz. 271.

<sup>89</sup> MAJTÉNYI László, *Az adatvédelem Magyarországon és az Európai Unióban*, Budapest, Magyar Posta Részvénytársaság, 1999 (A postai ágazat és az Európai Unió : integrációs füzetek) (Európai Unió füzetek)

kell állniuk, azon nem terjeszkedhetnek túl. Az adatok minőségi követelményéhez szükségszerűen hozzátárazik, hogy azok pontosaknak, időszerűeknek legyenek. A személyiség védelmében az egyezmény előírja, hogy az adatok tárolási módjának olyannak kell lennie, amely az adatalany azonosítását csak a tárolás céljához szükséges ideig teszi lehetővé.

Az egyezmény a 6. cikkben a személyes adatok definícióján belül meghatározza a különleges adatok körét is. E körbe a faji eredetre, a politikai véleményre, a vallásos vagy más meggyőződésre, valamint az egészségre, a szexuális életre vonatkozó személyes adatokat sorolja az egyezmény, hozzátéve a büntető ítéletekkel kapcsolatos személyes adatok körét is. Ezen adatok kezelésének előfeltételeként az egyezmény a nemzeti jogtól különleges biztosítékok létét követeli meg, amelyek hiányában tiltja az adatkezelést.

Az adatkezelés alapvető követelményeként előírja az egyezmény, hogy a tagállamoknak megfelelő biztonsági intézkedéseket kell tenni az automatizált adatállományokban tárolt személyes adatok védelme érdekében a véletlen vagy jogtalan megsemmisítés, illetve véletlen elvesztés, valamint a jogtalan hozzáférés, megváltoztatás továbbá terjesztés megakadályozása érdekében. Az egyezmény 8. cikkelye szabályozza az adatalanyt védő további garanciákat. Alanyi jogként érvényesítendő kötelezettségként írja elő az egyezmény, hogy minden adatalany joga van arra, hogy tudomást szerezzen a személyes adatok automatizált állományáról, annak fő céljairól, valamint az adatállományt kezelő személyéről és szokásos lakhelyéről vagy székhelyéről. Az érintetteknek joga van arra, hogy ésszerű időközönként és túlzott késedelem vagy költség nélkül értesüljenek arról, hogy valamely automatizált adatállományban személyes adatait tárolják-e, és ezekről az adatokról számára érthető formában tájékoztassák. Az egyezmény előírja, hogy mindenki helyesbítheti, vagy töröltheti adatait, ha ezen adatok feldolgozása ellentétes az egyezmény rendelkezéseivel. Az érintettek jogainak érdemi védelme érdekében az egyezmény lefekteti azt a nemzeti jogalkotói kötelezettséget,



hogy jogorvoslatot kell biztosítani az érintettnek, ha tájékoztatási vagy indokolt esetben közlési, helyesbítési, illetve törlési kérelmét nem teljesítik. Az egyezményben a tagállamok vállalták, hogy az Egyezménybe foglalt adatvédelmi előírások megsértésének esetére szankciókat fogadnak el, illetve jogorvoslati lehetőségeket biztosítanak a nemzeti jogrendjükben az Egyezményben foglalt jogok érvényesítése érdekében.

Az egyezmény meghatározza azokat a tárgyköröket, amelyek szükség esetén egy demokratikus társadalomban elfogadható módon törvények által előzetesen szabályozott keretek között lehetővé teszik a személyes adatokhoz való jog korlátozását. A tagállamok eltérhetnek az egyezményben lefektetett célhoz kötött adatkezelését elvétől, az arányosság elvétől, illetve korlátozhatják az érintett jogait a róla nyilvántartott személyes adatainak megismerése, helyesbítése, vagy törlötése vonatkozásában, ha az állam biztonsága, a közbiztonság, az állam pénzügyi érdekének a védelme vagy a bűncselekmények megelőzése érdekében erre szükség van. Az egyezmény az érintett jogainak korlátozása vonatkozásában megengedi, hogy a tagállam törvényes úton zárja ki az érintettnek jogorvoslati jogait. Az egyezmény statisztikai célból vagy a tudományos kutatások elvégezhetőségének érdekében megengedi, hogy az érintettek tájékoztatási, helyesbítési jogának korlátozását nemzeti törvény elrendelheti, ha ezzel az adatalany magánélete nyilvánvalóan nem kerül veszélybe. Az Európa Tanács Adatvédelmi Egyezménye az országhatárokat átlépő adatáramlás vonatkozásában lefekteti az adatok szabad határátlépésének az elvét. Így a tagállamok nem tilthatják meg, illetve nem köthetik külön engedélyhez a magánélet védelmének kizárólagos céljából a személyes adatoknak az országhatárokat átlépő áramlását, ha az egy másik az egyezményben részes állam területére irányul. A tagállamok a személyes adatok szabad határátlépésének elvét korlátozhatják, ha olyan állam területére irányul, amely nem nyújt az egyezményben részes tagállamok által biztosított védelmet. Az Európai Tanács keretében folyó jogharmonizáció sok esetben összekapcsolódik az

Európai Közösségen belüli jogfejlődéssel, így van ez az adatvédelem esetében is. Az egyezmény második kiegészítése lehetővé tette 1999-ben az Európai Közösség számára, hogy részese legyen az Európai Adatvédelmi Egyezménynek, azzal a szándékkal, hogy az adatvédelem nemzetközi eszközrendszere bővüljön, és az adatvédelmi követelményeket egységesítsék a különféle intézmények.

Az Európai Unió adatvédelmi keretjogszabálya, az 95/46/EK irányelv indoklása hivatkozik a magánélet tiszteletben tartására vonatkozó alapelvek vonatkozásában az Emberi Jogok Európai Egyezményének 8. cikkére, valamint a strasbourgi bíróságnak az magánélet-, és a család védelme tárgykerében hozott ítéletekre. Így az állíthatjuk, hogy nemcsak a 95/46/EK irányelv létrejöttében játszott jelentős szerepet az emberi jogok európai egyezményben rögzített magán- és családi élet tiszteletben tartására vonatkozó alapjog, hanem az adatvédelem európai alapjoggá válásának egyik nélkülözhetetlen lépcsője volt az Európa Tanács Adatvédelmi Egyezménye, és az Emberi Jogok Európai Bíróság alapjog fejlesztő ítélkezése.

## 4. FEJEZET: A SZEMÉLYES ADATOK VÉDELME AZ EURÓPAI UNIÓBAN

### 4.1. Személyes adatok védelmének alapjai az Európai Unióban

#### 4.1.1. Alapjogok fejlődése az Európai Unióban

Az Európai Közösségeket létrehozó alapszerződések nem tartalmaztak saját alapjogi katalógust, mivel a tagállamok elsősorban gazdasági célú szupranacionális együttműködés érdekében hozták létre az Európai Gazdasági Közösséget. De már 1969-ben konfliktusba került a közösségi jog és a tagállamokban lefektetett alapjogok, így az EKB kimondta<sup>90</sup>, hogy az alapvető jogok védelme a közösségi jog általános alapelvei közé tartozik. Az Európai Közösségek Bírósága fektette le a Hauer-ügyben<sup>91</sup> hozott ítéletében, hogy az alapvető jogokkal szemben is elsőbbséget élveznek a közösségi jogi normák, mivel a tagállamokban a közösségi jog anyagi jogi egységességét, és hatékonyságát biztosítani kell. Annak érdekében, hogy a közösségi jogi aktusok alapvető jogi konformitása vizsgálható legyen, szükséges, a közösségek szintjén egy önálló alapjogvédelmet kialakítani.

Az európai alapjogi rendszer létrejöttének első lépcsőjének a Nold-eset tekinthető, amikor az EKB kimondta, hogy a tagállamok alkotmányos hagyományát mint jogforrást elfogadja. E fogalom nem jelentett konkrét alapjogi normatartalmak érvényesítését a közösségi jogban, hanem inkább tagállamok alkotmányaiban fellelhető alapjogi jogelvek, alkotmányos joggyakorlat recipálását a közösségi jogba. A Nold-ügy<sup>92</sup> hozott ítéletében az EKB kimondta, hogy az alapvető jogok védelme a közösségben azokból az alapjogok védelmére irányuló a nemzetközi szerződésekből is levezethető,

---

<sup>90</sup> EKB 26/69 Stauder

<sup>91</sup> EKB 44/79 Hauer

<sup>92</sup> EKB 4/73 Nold

amelyekhez a tagállamok korábban már csatlakoztak. Az Európai Emberi Jogi Egyezmény a legfontosabb forrássá vált a közösségi alapjogi fejlődés során, mivel ez volt az egyetlen alapjogi katalógus, amelyet a tagállamok egységesen saját magukra nézve kötelezőnek elismertek. A Maastrichti Szerződésben már a közösségi jog alapelveként megjelenik az alapvető jogok tisztelete, és ezzel együtt párhuzamosan megnőtt a jogi igény arra, hogy az Unió saját alapjogi katalógussal rendelkezzen.

#### 4.1.2 Az Európai Unió Alapjogi Chartája

Az Európai Unión belüli emberi jogok fejlődése tekintetében mérföldkőnek tekinthető a 2001-ben elfogadott Alapjogi Charta.<sup>93</sup> Az ünnepélyesen proklamált charta az általános hatályú nemzetközi dokumentumok között elsőként ugyan, de mégsem kötelező jelleggel rögzíti a személyes adatok védelméhez való jogot. Az első Konvent az egyéni szabadságjogok körében, kitüntetett helyen (II.-68.) rögzítette a személyes adatok védelméhez való jogot alkotmányos alapjogként. Ez a közösségi alapjog megillet minden személyt, legyen magánszemély, vagy jogi személy. A Charta a személyes adatok védelmére vonatkozó legfontosabb alapelveket is lefekteti, így a személyes 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. A Charta előírja, hogy a személyes adatok védelmének érvényesülését egy független hatóságnak kell ellenőriznie. Ugyan kronológiailag az Alapjogi Charta jóval később került megfogalmazásra, mint az EU adatvédelmi irányelv, de valójában az Alapjogi Charta csak összegzi az adatvédelem alapjogi fejlődésének jelenlegi stációját, és európai alapjogként definiálja az információs önrendelkezési jogot.

---

<sup>93</sup> [http://europa.eu.int/constitution/hu/part16\\_hu.htm#a88](http://europa.eu.int/constitution/hu/part16_hu.htm#a88)

## 4.2. Az Európai Unió adatvédelmi irányelve

### 4.2.1. A 95/46/EK irányelv előzményei

A különböző nemzetközi szervezetek felől érkező hatások, de különösen az, hogy az Európai Tanács keretében a 1980-as évek végére kialakított adatvédelmi jogalkotás generálta az Európai Közösség ezirányú jogfejlődését. Az Európai Parlament 1976 óta több olyan határozatot hozott, amelyben sürgette a Bizottságot a személyes adatok hatékony védelmének kialakítására. Az Európai Bizottság közleményben<sup>94</sup> sürgette a személyes adatok védelméről szóló közösségi jogalkotást. A jogalkotás szükségességét azzal indokolta, hogy a személyes adatok kezelése egyre gyakoribbá vált a gazdasági élet és a társadalmi élet minden területén, valamint az adatszerésre irányuló új igények megkövetelik, hogy a közösség intézkedéseket hozzon a személyek adatainak kezelésével kapcsolatosan, különös tekintettel a nyílt távközlő hálózatok fejlődésére. A tagállamok többsége a 1970-es években ugyan hozzákezdett a személyes adatok kezelésének szabályozásához, és ilyen adatok felhasználását korlátok közé szorították. De amellett, hogy a szabályozások célja többnyire hasonló, még jelentős különbségek vannak abban, hogy a szabályozás kiterjed-e a manuális adatkezelésekre, a jogi személyek alanyai-e a szabályozásnak. Eltérőek a nemzeti szabályok az adatkezeléshez kapcsolódó értesítési kötelezettség értelmezésében, a tájékoztatás, és a különleges adatok kezelésének megengedhetősége tárgyában. A bizottság álláspontja szerint a nemzeti megközelítések változatossága és a közösségi szintű védelmi rendszer hiánya akadályozza a belső piac kiteljesedését. A közösségen belüli azonos védelmi szint lehetővé teszi a határon átvélő adatáramlást, amely lényeges

---

<sup>94</sup> *Communication de la Commission relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté et à la sécurité des systèmes d'information*, SYS 287. , Commission de Communautés Européennes COM (90) 314 final SYN 287 et 288 Bruxelles le 13 septembre 1990

feltétele az informatikai ipar, és távközlési szolgáltatások fejlődésének. Az összehangolt szabályok bevezetése a személyes adatok és a magánélet védelmére és a digitális távközlő hálózatokra tekintettel, nélkülözhetetlen a távközlési szolgáltatások és eszközök belső piacának kiteljesedéséhez. A közösségi szabályozás további célja a magas szintű informatikai biztonság fenntartása, és hatalmas mennyiségű elektronikusan tárolt személyes adat sérthetlenségének biztosítása. A megközelítés keretei között a Bizottság lefektette, hogy szükséges a személyiségi jogok közel azonos és magas szintű védelmének megteremtése mellett az információrendszerek biztonságára vonatkozó politika kialakítása. A bizottság javasolja, hogy az Európai Közösségek csatlakozzon az Európa Tanács 108. számú adatvédelmi egyezményéhez, és másrészt az általános hatállyal rendelkező irányelv kerüljön elfogadásra, amely garantálja a személyes adatok kezelésének törvényi feltételeit, az érintett jogait a felvilágosításra, tájékoztatásra, helyesbítésre. Az irányelvben követelményeket kell meghatározni az adatok minőségére vonatkozóan, hogy az adatok felvétele tisztességes, és az adatok helyesek legyenek, illetve kezelésükre csak törvényes cél alapján kerülhessen sor. A bizottság javasolja, hogy egy adatvédelmi tanácsadó csoportot állítson fel az irányelv. A bizottság szándéka az irányelv hatályával kapcsolatosan arra irányult, hogy annak alkalmazása a magánszféra mellett, azokra a területekre is terjedjen ki, ahol a közszeaktor tevékenysége során köteles a közösségi jogot alkalmazni. A bizottság az irányelv alapelveit akarta kiterjeszteni azokra a területekre is, ahol a közigazgatási szervek tevékenységét nem a közösségi jog szabályozza. Az irányelv elfogadását sokáig hátráltatta a tagállamokkal folytatott viták, amelyek középpontjában az állt, hogy az információs önrendelkezési jogra épített - a német adatvédelmi szabályokhoz hasonló közösségi előírásokat - egyes tagállamok nem akarták átvenni.

#### 4.2.2 Az Európai Unió adatvédelmi irányelv céljai

Az irányelv<sup>95</sup> bemutatása során az irányadó szabályozás áttekintése mellett azokat a vitás kérdéseket is érintem, amelyeket az európai bizottság az adatvédelmi irányelv végrehajtásával kapcsolatos 2003. évben lefolytatott vizsgálata során tárt fel. A vizsgálat eredményeit egy jelentésben<sup>96</sup> foglalták össze. A vizsgálat több tekintetben késedelmet szenvedett, mert a tagállamok az irányelvben megállapított határidőig, 1998-ig nem implementálták a szükséges közösségi előírásokat a nemzeti jogba, ezért a bizottság 1999-ben eljárást indított az európai bíróság előtt Franciaország, Németország, Írország, Luxemburg és Hollandia ellen. A bizottság határozott fellépését követően 2001-ben Németország és Hollandia notifikáltatta a vonatkozó adatvédelmi előírásokat, így a bizottság felfüggesztette az eljárást. Franciaország az 1978-ból származó adatvédelmi törvényét jelentette be, és jelezte, hogy új törvényt fog a tárgyban kibocsátani, ezért a bizottság ebben az esetben is a bírósági eljárás megszüntetését kérte a bíróságtól. Luxemburg esetében a bizottság az eljárásban bebizonyította, hogy a luxemburgi jogalkotó megsértette az EK szerződésből eredő kötelezettségeit, és az európai bíróság ítéletével zárult a szerződésszegési eljárás. Ezt követően Luxemburgban új adatvédelmi törvényt fogadtak el, ami 2002-ben hatályba is lépett. Írország 2001-ben az irányelv egyes részeinek nemzeti jogba történő átültetését jelentette be, majd ezt követően az ír parlament rövid időn belül az adatvédelmi irányelvvel teljesen összhangban álló szabályozást fogadott el.

Az Európai Parlament és a Tanács 1995. október 24-én fogadta el a személyes adatok feldolgozása vonatkozásában az egyének védelmére vonatkozó irányelvet, amely e célkitűzés mellett biztosítja a személyes adatok szabad

---

<sup>95</sup> Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a természetes személyek jogainak a személyhez fűződő adatok feldolgozásakor nyújtandó védelemről és a szabad adatforgalomról, HL L 281, 1995. november 23.

<sup>96</sup> Bericht über den Ersten Bericht über die Durchführung der Datenschutzrichtlinie 95/46/EG KOM(2003)265 - C5-0375/2003 - 2003/2153(INI)).

áramlását az Európai Közösségen belül.<sup>97</sup> Az irányelv preambuluma felvázolja a jogalkotást kiváltó körülményeket. A személyes adatok kezelésére vonatkozó nemzeti szabályokat azért kellett harmonizálni egymással, mert a közösségen belül az áruk, a szolgáltatások és a tőke szabad áramlásával párhuzamosan nőtt a vállalkozások közötti személyes adatok cseréje is. A belső piac nemcsak azt követeli meg, hogy az adatok szabad áramlásával megfelelően biztosítva legyen az áruk, a személyek, a szolgáltatások és a tőke szabad mozgása, hanem azt is, hogy az egyének alapvető jogai is megfelelően biztosítva legyenek. A közösségi szintű szabályozást indokolja az is, hogy a gazdasági és a társadalmi élet számos területén egyre többször folyamodnak a személyes adatok informatikai eszközökkel történő feldolgozásához. Mivel a tagállamok a személyes adatkezelés terén eltérő nemzeti jogszabályokkal rendelkeznek, ezért az informatikai és a távközlési szolgáltatások kiegyensúlyozott fejlődéséhez, illetve a közösségen belül a telekommunikációs hálózatok összehangolt bevezetéséhez szükséges, hogy a gazdasági élet területén folyó személyes adatok kezelésére vonatkozóan közel egységes nemzeti szabályozások alakuljanak ki. Az irányelv célként tűzi ki, hogy a nemzeti jogszabályok közelítése nem vezethet a már kialakult védelmi szint csökkentéséhez, hanem a közösségen belül magas védelmi szintet kell biztosítani a magánszféra védelmének a személyes adatok feldolgozása során.

A bizottság jelentésében természetesen vizsgálta, hogy az irányelv elérte-e a kitűzött célokat. Azt állapította meg, hogy az irányelv szabályainak késedelmes implementálása és egyes jogfogalmak értelmezési nehézségei ellenére a kitűzött célját az adatvédelmi irányelv elérte, mivel a közösségen belül sikerült a személyes adatok szabad forgalmát korlátozó előírásokat lebontani. A nehézségek okát a bizottság oda vezette vissza, hogy 1995-ben a tagállamok többsége már rendelkezett adatvédelmi törvénnyel, azonban

---

<sup>97</sup>Az irányelv részletes feldolgozásához lásd még HAJDÚ József, *A munkavállalók személyes adatainak védelme az EU és a tagállamok jogában, különös tekintettel az elektronikus kommunikációra*, Szeged, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 2003 (Acta Universitatis Szegediensis), (Acta Juridica et Politica), 7.



néhányuk, mint Olaszország vagy Görögország nem, az irányelv egységes implementálásával ez az akadály megszűnt. A bizottság személyes adatok szabad áramlásának kialakulásaként fogadja el, hogy az irányelv elfogadása óta a bizottság nem találkozott olyan esettel, amelyben az EK tagállamok közötti személyes adatok cseréjét adatvédelmi okból felfüggesztették, vagy elutasították volna. Természetesen ez nem jelenti azt, hogy egyes tagállamokban szükségtelenül szigorú jogszabályok ne korlátozzák a személyes adatok tagállamon belüli cseréjét, amely ennek következtében korlátozó hatást fejt a személyes adatoknak egy másik tagállamba irányuló exportjára is.

A bizottság az adatvédelmi irányelv másik céljával is elégedett, mely szerint a belső piacot akadályozó korlátok lebontásával egyidejűleg sikerült egy olyan magas adatvédelmi szintet elérni az Európai Unión belül, amely talán a világon egyedülálló, bár az on-line kérdőívet<sup>98</sup> kitöltő polgárok nem így érezték.

#### 4.2.3 Az irányelv<sup>99</sup> hatálya, fogalmi rendszere

Az irányelv hatálya kiterjed a személyes adatok részben vagy egészben automatizált módon való „feldolgozására”, illetve azokra az adatkezelésekre, amelyekben a személyes adatokat manuális nyilvántartás keretében kezelik, vagy arra a célra szánják a személyes adatokat, hogy azok nyilvántartás részei legyenek. A személyes adatok védelmét szolgáló jogszabályok a manuális adatkezelés esetében kizárólag a nyilvántartásokra terjednek ki, a strukturálatlan adatállományokra azonban nem. Az irányelv meghatározza azokat a területeket, amelyekre nem terjed ki a személyes adatok

---

<sup>98</sup> A Európai Bizottság az irányelv végrehajtása tekintetében egy széleskörű online kampányt indított, amelyben a vállalkozóktól, a fogyasztói érdekképviseletektől, és maguktól az érintettektől érdeklődött, hogy mennyire váltotta be az adatvédelmi irányelv a hozzáfűzött reményeket.

<sup>99</sup> Az irányelv hatályos szövegét a [www.europa.eu](http://www.europa.eu) oldalon megtalálható eu-lex adatbázisból merítettem 2010. február 9-én

vonatkozásában a nemzeti jogszabályok harmonizálási kötelezettsége, így a közbiztonsággal, a védelemmel, a nemzetbiztonsággal kapcsolatos tevékenységek, vagy a tagállamok bűnüldözési tevékenysége során kezelendő személyes adatokra érvényben levő előírások nem tartoznak az Európai Közösségekről szóló szerződés hatálya alá. Az irányelv hatályát kiterjeszti a természetes személyek hang- és képadatainak felvételére, továbbítására, „feldolgozására”, rögzítésére, tárolására és ezen adatok közlésére szánt módszerekre, ha ezeknek az adatoknak a „feldolgozása” automatizált módon történik, vagy ha a feldolgozott adatokat egyénekhez kapcsolják valamilyen speciális szempontok szerint, és ezeket az adatokat egy könnyen kezelhető nyilvántartásban rendszerezetten tárolják. A hang- és képrögzítésre alkalmas videokamerás megfigyelő rendszerek alapján kezelt személyes adatok nem tartoznak az irányelv hatálya alá, ha a megfigyelés és adatkezelés közbiztonsági, honvédelmi, nemzetbiztonsági célból történik. Az irányelvet nem kell alkalmazni a természetes személyek által végzett házi használatra készített címjegyzék vonatkozásában. A sajtó által végzett személyes adat kezeléseket esetén az irányelv a tagállamokra bízta, hogy a saját a nemzeti jogukban a magánélet tiszteletben tartását, a személyes adatok védelmét biztosító nemzeti jogszabályaikat, az újságírás céljából, vagy művészeti, illetve irodalmi tevékenység során gyűjtött személyes adatok kezelését összehangolják. Szükséges a személyes adatok védelmének összeegyeztetése Az emberi jogok és alapvető szabadságok védelméről szóló egyezmény 11. cikkében biztosított az egyéneket megillető tájékozódáshoz való joggal, illetve az információszerzéshez és annak közléséhez fűződő joggal, ezért az adatvédelmi kötelezettségek teljesítése tekintetében a tagállamok az adatbiztonságra vonatkozó előírások kivételével bizonyos mentességeket állapíthatnak meg. Az adatvédelmi tájékoztatási kötelezettség alól a tagállamok felmentést adhatnak a statisztikai vagy tudományos célból történő adatkezelések esetén, ha a tájékoztatás lehetetlen vagy aránytalanul nagy erőfeszítéseket igényelne.

Az irányelv 2. cikke részletezi az adatvédelmi előírások alkalmazása szempontjából alapvető fogalmakat. A szabályozás központi kérdése a személyes adatok fogalma: az azonosított vagy azonosítható természetes személyre ("érintettre") vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén. Így e fogalom alá kell érteni a személyről készített képeket, videó- és hangfelvételeket, telefonbeszélgetések részleteit.<sup>100</sup>

Az irányelv alapján azonosítható személynek tekinthető, aki közvetlenül vagy közvetetten azonosíthatóvá válik függetlenül az azonosítás módjától. A definíció meghatározza a személy azonosításának legfőbb szempontjait is, így ez az adott személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén történik. A 2. cikk nem határozza meg a személyes adatok körén belül a különleges érzékenységgel rendelkező adatok körét. Az irányelv 8. cikkében írja elő a tagállamok részére, hogy megtilthatják azon „személyes adatok feldolgozását”, amelyek az érintett faji vagy etnikai hovatartozására, a politikai véleményére, a vallási vagy világnézeti meggyőződésére, a szakszervezeti tagságára, az egészségi állapotára vagy a szexuális életére vonatkoznak. A 8. cikk (1) bekezdés által meghatározott adatkezelési tilalom alól számos kivételt enged meg a jogszabály.

Az irányelv meghatározza "személyes adatok feldolgozása" ("feldolgozás"<sup>101</sup>) definícióját is. Megjegyzem, hogy az Avtv.. által meghatározott adatkezelés

---

<sup>100</sup> JÓRI, *i.m.*, 111. A magyar adatvédelmi biztos szerint személyes adatnak számít a név, születési adatok, a foglalkozás, életrajzi adatok, biometrikus azonosítók azaz a testi jellemzők, a képmás, a vagyona vonatkozó adatok, kereset, a nyugdíj összege, a bankszámla adatok, családi állapot, adóminősítési eljárás eredménye, egy beszélgetés során elhangzó kijelentés, a tanúvallomás, peres ügyben tett kijelentések, cégtulajdonosi adatok, számítógépes keresés során látogatott IP címek, vizsgaeredmények, írásképek, oktatói minősítés eredménye;

<sup>101</sup> Tekintettel arra, hogy a „személyes adatok feldolgozása”, „feldolgozás” definíciót az EK irányelv, és az Avtv. is ismeri, de a magyar jogszabály az adatkezelést érti a fogalom alatt, ezért az EK irányelv által használt „feldolgozás” fogalmat „---”, megkülönböztetéssel használom.

fogalma azonosítható az EK irányelv által meghatározott „személyes adatok feldolgozása” definícióval. A magyar Avtv.. adatkezelés fogalma, és az EK irányelv által használt „feldolgozás” definíciója közös abban, hogy technikai közegtől függetlenül igen széles körben jelölik ki a fogalom alá vonható adatkezelői magatartások körét. Az EK irányelv által használatos „feldolgozás” átfogja az információk kezelésének minden mozzanatát. Így „feldolgozásnak” minősül az adatok gyűjtése, rögzítése, rendszerezése, tárolása, átalakítása, vagy megváltoztatása. „Feldolgozásnak” minősül a betekintés, a felhasználás, közlés és továbbítása, a terjesztés, vagy a hozzáférhetővé tétel, az összekapcsolás, összehangolás, zárolás, törlés és a megsemmisítés. A két legfontosabb fogalom mellett az irányelv 2. cikke definiálja a személyes adat-nyilvántartó rendszer, az adatkezelő, a feldolgozó, a harmadik személy, a címzett fogalmát. Feldolgozónak az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv tekinthető, amely személyes adatokat dolgoz fel az adatkezelő nevében. A feldolgozótól meg kell különböztetni a harmadik személy fogalmát, legyen az természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely nem azonos az érintettel, az adatkezelővel, a feldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy a feldolgozó közvetlen felügyelete alatt felhatalmazást kaptak az adatok feldolgozására. Az EK irányelv eltérően az Avtv..-től ismeri a címzett fogalmát, aki az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, akinek vagy amelynek a részére az adatot továbbítják, függetlenül attól, hogy harmadik személy-e vagy sem; mindazonáltal azok a hatóságok, amelyek egyedi megkeresés alapján kapnak adatokat, nem tekinthetők címzettnek.

Az irányelv az egyének megfelelő védelmének biztosítása érdekében előírja a tagállamok számára azt a kötelezettséget, hogy a közösség területén végzett minden „személyes adat feldolgozási” tevékenységet folytató vállalkozás a jogi formájától függetlenül valamely tagállam nemzeti jogszabályai alapján tegye. Tehát az adatvédelmi tevékenységekre az alkalmazandó jogot a

letelepedett vállalkozás székhelyének joga határozza meg. A tagállamok számára a közösségi jogalkotó az is előírja, hogy törekedni kell arra, hogy a „személyes adatok feldolgozást” végző vállalkozók ne bújhassanak ki a közösségi adatvédelmi előírások kötelezettségei alól. Ha egy vállalkozás több tagállamban telepedett le, akkor a vállalkozónak egyes részvállalkozásainak székhelye szerinti tagállami jog által megkövetelt adatvédelmi kötelezettségeknek meg kell felelnie. Az irányelvnek előírja az adatvédelmi irányelv alkalmazásának kötelezettségét olyan vállalkozások számára is, amelyek nem az EK-ban telepedtek le, de székhelyük az EK belül található, rájuk a nemzetközi jogi kötelezettség alkalmazandó. A 4. cikk c) pontja kiterjeszti az irányelv alkalmazásának kötelezettségét a közösségen belül székhellyel nem rendelkező vállalkozásokra extra-territoriális hatállyal, ha „személyes adatfeldolgozásra” alkalmas eszközük valamely tagállam területén található.

Az irányelv 2003-as felülvizsgálata során a 4. cikkben lefektetett elvet az „adatfeldolgozásra” alkalmazandó jog vonatkozásában több hozzászólaló kritizálta, szerintük a „székhely elve” helyet az alapján kellene az alkalmazandó jogot meghatározni, hogy mely országból származik az adott vállalkozás. Ez megkönnyítené az EU-ban nemzetközi szinten tevékenykedő vállalatok, és szervezetek számára, hogy egységes jogi szabályozási renddel dolgozhassanak. Másodsorban a hozzászólók szerint a 4. cikk c) pontjában meghatározott eszköz kifejezés annyira pontatlan, hogy az alapján nem lehet eldönteni, hogy az EU jogot az EU-n kívüli adatkezelő vonatkozásában milyen esetekben kell alkalmazni. A Bizottság a származási ország elve alapján nem tartja az adatvédelmi jog alkalmazását kivitelezhetőnek, másrészt a 4. cikk c.) pontja vonatkozásában szükséges a jogértelmezés és a fogalom további tisztázása, és nem zárta ki annak a lehetőségét sem, hogy más lényeges elemmel kellene az alkalmazandó jogot meghatározni.

#### 4.2.4. Adatvédelmi elvek az irányelvben és az adatkezelés jogcímei

Az irányelv 6. cikke a tagállamok számára előírja, hogy rendelkezzenek arról, hogy:

- a.) a „személyes adatok feldolgozását” tisztességesen és törvényesen kell végezni;
- b.) személyes adatok gyűjtése csak világosan meghatározott, egyértelmű, törvényes célból történhet. Az adatkezelések a céltól eltérő módon nem végezhetők. A személyes adatoknak az eredeti céltól eltérő „feldolgozása” történelmi, tudományos kutatási vagy statisztikai célból megengedett, ha a tagállamok előírják a megfelelő garanciákat;
- c.) Az adatgyűjtéseknek a kitűzött célból megfelelőnek, relevánsnak kell lennie, és nem lehet túlzott mértékű.
- d.) Az adatkezeléseknek pontosnak, és ha szükséges, időszerűnek kell lennie. Az adatkezelőknek minden ésszerű intézkedést meg kell tenniük annak érdekében, hogy a hibás vagy hiányos adatok törlésre vagy helyesbítésre kerüljenek.
- e.) A személyes adatok tárolásának olyan formában kell történnie, amely az érintett azonosítását csak addig teszi lehetővé, ameddig az adatkezelés céljának teljesítéséig feltétlenül szükséges.

Az irányelv 7. cikke meghatározza azokat a feltételeket, amelyek az adatkezelések törvényi alapjaiként számba vehetők. Az irányelv elsősorban az érintett egyértelmű hozzájárulását tekinti megfelelő alapnak az adatkezelésre. Az érintett hozzájárulásának fogalmát az irányelv 2. cikk h.) pontjában határozta meg, mely szerint az érintett hozzájárulásának az a nyilatkozat tekinthető, amely az érintett kívánsága alapján, önkéntesen, egyértelműen kifejezve és az adatkezelésről történő tájékoztatást követően lett kinyilvánítva. Az érintett hozzájárulása beleegyezésnek tekinthető az őt érintő személyes adatok „feldolgozásába”. Az irányelv 7. a.) pontja alapján a beleegyezés akkor

történik meg, ha „minden kétséget kizáróan<sup>102</sup>” megtörtént az érintett hozzájárulása. Ennek a fogalomnak az érdemi értelmezése akkor nyer jelentőséget, amikor egy jogvita esetén a nyilatkozat megadásának bizonyítási terhét kell szemügyre venni. Abban az esetben, ha a nyilatkozat értelmezése kétséges, az irányelv nyitva hagyja a megoldást. A magyar adatvédelmi törvény (Avtv..) 4.§ (4) bekezdésének utolsó mondata az érintett személyiségi jogainak és magánszférájának védelmében azt a megdönthető vélelmet állítja fel, hogy az érintett beleegyezését kétség esetén nem adta meg.

Az érintett beleegyezése mellett az „adatfeldolgozást” további indokok is legitimálhatják, így

- az érintett és az „adatfeldolgozó” között fennálló szerződéses kötelezettség teljesítése;
- az adatfeldolgozót terhelő jogi kötelezettséghez szükséges az érintett személyes adatainak kezelése;
- az érintett létfontosságú érdeke teszi szükségessé;
- hatósági jogkör gyakorlása vagy közérdekű feladat teljesítése indokolja az adatkezelést;
- az „adatfeldolgozó” vagy az adatokat birtokában tartó harmadik fél, aki valamely jogos érdeke érvényesítése érdekében kezeli a személyes adatokat feltéve, hogy az adatfeldolgozónak, más harmadik személynek a jogos érdeke a magánszférához és a személyes adatok védelméhez fűződő jogot nem haladják meg túlzottan. Az irányelv a tagállamok jogalkotása számára ebben a vonatkozásában előírja, hogy az egymással szemben álló jogi érdekek konfliktusára vonatkozóan mérlegelési kötelezettséget írjanak elő nemzeti jogukban.

A bizottság a tagállami jogszabályok részletes vizsgálatát követően megállapította, hogy a tagállamok több esetben is elmulasztották a 6. cikk b) pontja esetén, hogy megfelelő garanciákat írjanak elő akkor, ha személyes

---

<sup>102</sup> ROSSNAGEL, *i.m.*, 683.

adatokat történelmi, tudományos kutatási vagy statisztikai célból az eredeti adatgyűjtési céltól eltérően dolgoznak fel. Az érintett beleegyezésével kapcsolatosan a bizottság megállapította, hogy „a minden kétséget kizáró módon” kifejezést az érintettek beleegyezése vonatkozásában pontosabban kellene meghatározni, és egységes értelmezésre lenne szükség. A bizottság szerint az érintetteknek fontos tudniuk, különösen az on-line ügyletek esetében, hogy mely magatartás minősül egy érvényes adatkezelési hozzájárulásnak. Másrészt a Bizottság kifogásolta, hogy némely tagállam a 7. cikkben rögzített listát a nemzeti jogban megrövidítette, vagy több olyan felhatalmazást is meghatároztak, amelyet a 7. cikk nem sorolt fel.

#### 4.2.5. Különleges adatok köre

A személyes adatok fajtái között különböző érzékenyséű adatok kerülhetnek „feldolgozásra”. Általánosan elfogadott gyakorlat, hogyha bizonyos adatok illetéktelen kezekbe, vagy még rosszabb esetben nyilvánosságra kerülnek, ez a társadalmi következmények miatt az érintett személyiségi jogait sérti, vagy veszélyezteti. Az érintett személyiségi jogainak sérelmét a stigmatizálás jelenti, amely az érintett viselkedésétől függetlenül valamilyen körülmény alapján alkotott ítélet. Az alaptalan értékítélet létrejötte önmagában veszélyeztetési tényező, a személyiségi jog konkrét sérelmét pedig az jelenti, hogyha a stigmatizálás alapján létrejött ítélet ténylegesen korlátozza az egyén személyiségének kibontakoztatását, önazonosságának megvallását, vagy társadalmi kapcsolatai megromlása révén személyes fejlődését. Ezért a jogalkotónak már a veszélyhelyzet kialakulásával szemben reagálnia kell. A különleges adatok köre nem szűkíthető le kizárólag egy rövid felsorolásra, amely kiterjed a faji, etnikai, származási adatokra, az egészségi állapotra, a szexuális szokásokra, a káros szenvedélyekre vonatkozó információkra, illetve a büntetett előélet törvényi következményeinek fennálltára vonatkozó



adatokra. A szféra elmélet<sup>103</sup> szerint az adatok védelmét aszerint kell megszabni, hogy az adott adat kezelése, nyilvánosságra hozatala, milyen társadalmi következményekkel jár az érintettre. De az irányelv nem a szféra elmélet alapján határozza meg a különleges adatok körét, hanem egy felsorolásban határozza meg a szenzitív adatokat.

Az irányelv 8. cikke alapján a tagállamok megtilthatják, illetve az adatkezelés tekintetében szigorúbb feltételeket állapíthatnak meg, ha az adatok faji vagy etnikai hovatartozásra, politikai véleményre, vallási illetve világnézeti meggyőződésre utalnak. A különleges adatok körébe tartozik az érintett egészségi állapotára, szexuális életére illetve szakszervezeti tagságára vonatkozó adatok. Az adatkezelő csak akkor gyűjtheti, tarthatja nyilván ezeket az adatokat, ha az érintett kifejezett hozzájárulását adta az adatkezeléshez. A kifejezett hozzájárulás fogalma a jognyilatkozat megtétele szempontjából több kötelezettséget telepít az adatkezelőre, mivel ha az adatkezelő mentesülni kíván a jogellenes adatkezelés miatt bekövetkezett kár megtérítése alól, akkor bizonyítania kell, hogy a kárt okozó eseményért nem felelős. Az adatkezelőnek ebben az esetben bizonyítania kell, hogy az érintett kifejezett beleegyezésével történt az adatkezelés. A magyar Avtv.. a különleges adatok kezelése esetében, ha nem törvény rendelte el az „adatfeldolgozást”, akkor az érintett írásbeli beleegyezését követeli meg. Az irányelv nem határozza meg ennyire egyértelműen, hogy mi minősül kifejezett beleegyezésnek.

Az irányelv 8. cikke meghatározza a különleges adatok kezelésének további jogalapjait is. Így nemzeti jogszabályok lehetővé tehetik, hogy az adatkezelő kötelezettségei vagy meghatározott jogai gyakorlása érdekében a foglalkoztatás területén az érintettre vonatkozó különleges adatokat kezeljen, ha megfelelő jogi garanciákat rögzítenek a foglalkoztatási jogszabályok. Az

---

<sup>103</sup> Matthias LEIST, *Verfassungsrechtliche Schranken des steuerlichen Auskunfts- und Informationsverkehrs*, Frankfurt, 2000 (Mannheimer Beiträge zum Öffentlichen Recht und Steuerrecht, 22), 10.

irányelv a világnézeti, vallási, szakszervezeti illetve politikai alapon szerveződő alapítvány, egyesület vagy bármely más nonprofit szervezet tekintetében a különleges adatok kezelését akkor engedi meg, ha az adatgyűjtés megfelelő törvényes biztosítékok mellett történik, így ha az adatgyűjtés szoros kapcsolatban áll a szervezet céljaival, az érintettek beleegyezése nélkül az adatokat harmadik személy részére nem adhatják ki. Az irányelv megengedi a különleges adatok kezelését, ha olyan adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott, illetve az adatkezelés jogi követelések megállapításához, ezek gyakorlásához, védelméhez szükségesek.

Az érintett beleegyezése nélkül kezelhetők különleges személyes adatok az egészségügy területén, ha az érintett vagy más személy létfontosságú érdekei védelmében szükséges, vagy ha az érintett fizikailag vagy jogilag képtelen hozzájárulását adni az adatkezeléshez. A tagállamoknak az érintett egészségére vonatkozó különleges adatok kezelését nem tilthatják meg, ha orvosi titoktartási kötelezettséggel alá eső személy dolgozza fel az adatokat. A tagállamok nemzeti rendelkezéseikben, illetve a felügyelő hatóság határozatában különleges adatok kezelése tekintetében alapvető közérdekből, megfelelő garanciák mellett további mentességeket állapíthatnak meg arra, hogy az érintett kifejezett beleegyezése nélkül is lehessen szenzitív adatokat kezelni. A bűncselekményekre, a büntető ítéletekre vagy más biztonsági intézkedésre vonatkozó adatok „feldolgozása” kizárólag hatósági ellenőrzés mellett történhet. A tagállamok dönthetnek úgy, hogy kizárólag a történelmi kutatás céljából folyó adatkezelések esetében nem írják elő a személyes adatoknak az irányelvvel összhangban történő kezelését.

#### 4.2.6. Az érintettek tiltakozási jogai (14. cikk)

Az adatvédelmi jog alapvető eleme az érintett tájékoztatása, amely minden tagállami adatvédelmi szabályozásban megtalálható, és amelyet a nemzetközi

normák is megkövetelnek. Abban a vonatkozásban viszont, hogy milyen formában kell a tájékoztatásnak megtörténnie, illetve a tájékoztatási kötelezettség alól milyen kivételeket lehet megengedni, már jóval tarkább a kép. A tájékoztatási kötelezettség lényege, hogy az érintett ismeretet szerezzen az „adatfeldolgozás” tényéről, illetve az „adatfeldolgozás” körébe eső személyes adatairól. Az irányelv előírja, hogy az érintettnek korlátozás nélkül, ésszerű időközönként, túlzott késedelem vagy költség nélkül érhető tájékoztatást kell kapnia a rá vonatkozó adatok „feldolgozásáról”, annak céljáról, az „adatfeldolgozó” személyéről, és arról, hogy kik felé továbbítják adatait. Az irányelv külön kiemeli, hogy az érintettnek tájékoztatást kell kapnia az „adatfeldolgozás” logikájáról, és annak rendszeréről.

A nemzeti jognak biztosítania kell, hogy az érintett adatbirtokos kérhesse az „adatfeldolgozótól”, hogy személyes adatait helyesbítsék, töröljék, illetve zárolják, ha az adatkezelés nem felel meg az irányelv szabályainak. Az érintett helyesbítési, törlési, vagy zárolási joga nem csak az adatkezelővel szemben áll fent, hanem kérheti, hogy az adatokról tudomást szerző harmadik fél is tájékoztassák adatvédelmi jogainak gyakorlásáról, kivéve akkor, ha ez lehetetlen, vagy aránytalanul nagy erőfeszítést igényelne az adatkezelőtől.

#### 4.2.7. Automatizált egyedi döntések tilalma (15.cikk)

Az adatvédelem alkotmányos alapjainak kialakításakor a BVerfG lefektette, hogy az automatizált módon és a külső személyek által összeállított személyiség kép alkalmazásának lehetőségeit konkretizálni kell. A BVerfG által megállapított veszélyforrás abban rejlik, hogy az automatikus „adatfeldolgozás” során az egyént tárgyként kezelik, a különböző életviszonyait tükröző adatait sematizálják, és ez korlátozza az egyéneket abban, hogy meghatározzák személyiségükről alkotott képeket. Az automatizált egyedi döntés alapján létrejövő személyiség profil azt a veszélyt is magában hordozza, hogy az érintett nem kap tájékoztatást az értékelés

adatairól, és szempontjairól.<sup>104</sup> Az irányelv 15. cikkében lefektetett tilalom az automatizált adatok alkalmazására vonatkozóan arra reagál, hogy a köz- és magángazdaság területén működő „adatfeldolgozók” egyre növekedő érdeklődést tanúsítanak aziránt, hogy szoftverekkel különböző szempontok alapján profilokba sorolják a polgárokat. Az adatgyűjtés szempontjai irányulhatnak a polgárok érdeklődési körére, fogyasztói szokásaikra, megbízhatóságra, hitelképességre. Az automatizált döntés tilalma azt jelenti, hogy az egyén csoportokba sorolása nem lehet gépi döntés következménye, hanem emberi döntéshozónak kell felelősséget vállalnia döntései következményeiért, és embernek kell vizsgálnia nemcsak formailag, hanem érdemben az ügy egyediségeit is figyelembe véve, az adatokat. Az automatizált döntések tilalma csak azon döntésekre vonatkozik, amelyek az érintettre valamilyen jogi következménnyel járnak. Az irányelv felsorol eseteket, amelyekben ha jogi következménnyel jár az érintettre a döntés, így különösen, ha egyes személyes tulajdonságai, képességei kerülnek kiértékelésre, mint például a munkahelyi teljesítménye, hitelképessége, megbízhatósága, életvitele, akkor tilos az automatizált gépi döntés.<sup>105</sup> Az irányelv e szabálya túlmutat az Európa Tanács 108-as egyezményében rögzített jogain, és a tagállamok többsége még ennek a jognak az elfogadásáig sem jutott el<sup>106</sup>.

A 15. cikk (2) bekezdése meghatározza azokat a kivételeket, amelyek a tiltás ellenére lehetővé teszik a személyt érintő automatizált döntéseket, így ha a döntést valamely szerződés megkötése során hozzák, illetve valamely szerződés teljesítéséhez kapcsolódik, továbbá ha jogszabály írja elő az automatizált döntéshozatalt. Az irányelv előírja, hogy a jogos érdekek biztosítására garanciákat kell a nemzeti jogban lefektetni, például elő kell írni

---

<sup>104</sup> Philip SCHOLZ, *Datenschutz bei Data Warehousing und Data Mining* = Handbuch Datenschutzrecht : die neuen Grundlagen für Wirtschaft und Verwaltung, hrsg. von Alexander ROSSNAGEL, München, Beck, 2003

<sup>105</sup> Lásd még automatizált egyedi döntés tilalmához: JÓRI, *i.m.*, 250-255.

<sup>106</sup> BRÜHANN, *Grundlagen des Datenschutzes* = Handbuch Datenschutzrecht ... hrsg. ROSSNAGEL, *i.m.*, 144.

az érintett véleményének kinyilvánítását lehetővé tevő intézkedéseket. Kifogásolható, hogy az adatkezelőnek az érintett véleménye alapján nem kell felülvizsgálnia a szerződéskötésre vonatkozó álláspontját.

#### 4.2.8. Az „adatfeldolgozás” alapvető szabályai

Az „adatfeldolgozás” egész folyamata során biztosítani kell a személyes adatok védelmére vonatkozó alapelvek és más részletszabályok érvényesülését. E követelmény teljesítése érdekében az „adatfeldolgozás” titkosságát és biztonságosságát biztosítani kell, ezért a tagállamok számára az irányelv előírja, hogy megfelelő technikai előírásokat kell az „adatfeldolgozótól” megkövetelniük, hogy az adatokat védjék a véletlen vagy jogellenes megsemmisülés, elvesztés, a jogellenes megváltoztatás, illetve a jogosulatlan nyilvánosságra hozatal vagy hozzáférés ellen, különösen, ha az adatok továbbítására hálózaton keresztül kerül sor. Az irányelv nem határozza meg egyértelműen, hogy mekkora technikai biztonsági szintet követel meg az „adatfeldolgozás” tekintetében, hanem a technikai biztonsági szintet az elért technikai vívmányokra, azok alkalmazási költségeire, illetve a felmerülő kockázatok és a védendő adatok körére vonatkozóan kell meghatározni. Az adatvédelmi követelmények teljesítése nemcsak az adatkezelőket terheli, hanem az „adatfeldolgozót” is, akik az adatkezelő nevében dolgozzák fel a személyes adatokat, mert csak olyan adatfeldolgozót választhat az adatkezelő, aki a technikai biztonsági intézkedések, illetve a szervezeti működése oldaláról megfelelő garanciákat nyújt az adatvédelmi előírások teljesítésére. Az adatkezelő és az adatfeldolgozó között kötött írásbeli szerződésnek kell létrejönnie, vagy a megállapodást bizonyítás szempontjából más hasonló formában kell rögzíteni. A megállapodásnak kötelező tartalmaznia, hogy az adatfeldolgozó az adatkezelő utasítása alapján jár el, és az adatfeldolgozóra annak a tagállamnak a szabályait kell alkalmazni, ahol az letelepedett.

#### 4.2.9. A bejelentési kötelezettség

A tagállamoknak a nemzeti jogszabályaikban rendelkezniük kell arról, hogy az adatkezelőket bejelentési kötelezettség terheli a nemzeti adatvédelmi szervezet számára, ha „személyes adatok feldolgozását” tervezik. Az értesítésnek tartalmaznia kell az adatkezelő nevét, címét, az „adatifeldolgozás” célját, az érintettek körét, a kezelt adatok kategóriáit, azoknak a címzetteknek a leírását, ahova az adatokat továbbították, a harmadik országba irányuló tervezett adattovábbításokat, illetve az „adatifeldolgozás” biztonságosságát szolgáló intézkedések leírását. Az irányelv felülvizsgálata során többen kifogásolták, hogy a bejelentésre vonatkozó tagállami követelményeket egyszerűsíteni, és uniformizálni kellene. A bizottság osztotta többek véleményét, de emlékeztetett rá, hogy az irányelv a tagállamok számára sokféle lehetőséget kínál a bejelentési kötelezettség alóli kivételek alkalmazása tekintetében. A bejelentési kötelezettség alóli kivételt jelent, ha nem állnak fent az érintettek jogait sértő adatkezelési kockázatok, illetve ha az adatkezelő belső adatvédelmi felelőst nevez ki. Az irányelvben meghatározott kivételek elegendő flexibilitást adnak, és egyúttal nem csökkentik az adatvédelem színvonalát. A bizottság álláspontja szerint a tagállamok ezeket a kivételeket nem használták ki kellőképpen.

#### 4.2.10. Személyes adatok továbbítása harmadik országba

A tagállamoknak rendelkezniük kell arról, hogy a „feldolgozásra” kerülő vagy „feldolgozásra” szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha az adott ország megfelelő védelmi szintet tud biztosítani. A harmadik ország által a személyes adatok védelme vonatkozásában nyújtott védelmet az adattovábbítás feltételeinek figyelembevételével kell értékelni, így az adatok jellege, az „adatifeldolgozás” célja, időtartama, a kiindulási és a célországban hatályos általános és ágazati jogrend, valamint az ott érvényesülő

szakmai, illetve biztonsági intézkedés alapján kell megítélni. A megfelelő védelmi szint nem jelenti azt, hogy az azonos védelem szintje lenne megkövetelhető, amely globális nézőpontból szemlélve nem lenne reális<sup>107</sup>.

A bizottság harmadik országba irányuló adattovábbítás kérdéskörben áttekintve a nemzeti szabályozásokat azt állapította meg, hogy a tagállamok jogszabályai közötti hatalmas az eltérés. Az egyik tagállam által követett szabályozás az adatkezelő feladatává teszi annak megítélését, hogy a címzett a fogadó országban megfelel-e az uniós jog által garantált védelmi szintnek, és emellett a nemzeti adatvédelmi hatóságnak az adatforgalom ellenőrzése tekintetében jelentősen korlátozott hatáskört biztosít. Az ilyen jellegű szabályozás a Bizottság álláspontja szerint nyilvánvalóan nem felel meg az irányelv által elvárt követelményeknek. Másrésztől némely tagállam szabályozása a harmadik országba irányuló adatforgalom tekintésében minden továbbítást hivatalos engedélytől tesz függővé, ez sem tekinthető olyan megoldásnak, amely összhangban lenne az irányelvvel, mert az elvárt magas szintű védelem fenntartása mellett lehetőség szerint akadálymentes adatforgalmat kell biztosítani a tagállamokban. A bizottság felfogása szerint harmadik országba irányuló adattovábbítás vonatkozásában a nemzeti adatvédelmi szervezetnek történő bejelentés megkövetelendő, de nem lehet az adattovábbítást engedélyezési eljáráshoz kötni, különösen akkor nem, ha a továbbítás harmadik országba egyértelműen megengedhető, mivel az ott letelepedett címzett a Bizottság kötelező döntése alapján megfelelő védelmet biztosít a személyes adatok „feldolgozása” során. A harmadik országba irányuló adattovábbítások jogalapjának egységes tagállami értelmezése érdekében a 29-es munkacsoport ajánlást<sup>108</sup> fogadott el.

---

<sup>107</sup> HUSTINX, *Megfelelő...*, i.m., 80.

<sup>108</sup> Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24. October 1995. [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp114\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf); 2006.11.05.

Abban a kérdésben, hogy mely ország biztosít megfelelő védelmi szintet, a bizottság állást foglalhat. Ha a bizottság megállapítja, hogy valamely ország nem biztosít megfelelő védelmi szintet a személyes adatok „feldolgozása” során, akkor a tagállamok kötelesek megakadályozni a szóban forgó harmadik országba irányuló adattovábbításokat. A bizottság azt is megállapíthatja, hogy melyek azok a Non-EU tagállamok, amelyek megfelelnek az uniós adatvédelmi normáknak, és ezekbe az országokba a személyes adatok továbbítása nem jelent veszélyt. A bizottság több országról, így még a 2004-es EU csatlakozás előtt Magyarországról is megállapította,<sup>109</sup> hogy korlátozás nélkül fogadhat személyes adatokat az EU tagállamaiból. A bizottság többek közt „fehér listára” vette a Svájcba, Kanadába irányuló, illetve az USA Kereskedelmi Minisztériumával kötött ún. Safe Harbor megállapodás<sup>110</sup> keretén belül történő adatcseréket, és ezeket ismerte el az EU-normákkal összeegyeztethetőnek, ha a partnerek az előírt szerződéses feltételeket teljesítik. A személyes adatok „feldolgozására” vonatkozó „Safe Harbor” elvet az amerikai Kereskedelmi Minisztérium dolgozta ki, amelyet az EK Bizottsága is elfogadott, mint alkalmas eszközt arra, hogy megfelelő védelmet hozzon létre az USA-ba irányuló kereskedelmi célú személyes adattovábbítások vonatkozásában. A rendszer az önszabályozásra épül, mivel az amerikai vállalatok szabadon eldönthetik, hogy önként alávetik-e magukat a szabályoknak, azonban számolniuk kell azzal, hogyha a szabályokat megszegik hatósági szankcióval és polgári jogi felelősséggel kell számolniuk. Jelenleg 614 vállalkozás jelentette ki az előírt nyilvános közzététel mellett, hogy alkalmazza<sup>111</sup> a Safe Harbor szabályokat, és „adattfeldolgozását” hozzáigazítja az előírásokhoz.

A harmadik országokba irányuló személyes adatok továbbításának rendezése érdekében a bizottság felhatalmazást<sup>112</sup> kapott, hogy ún. általános szerződési

---

<sup>109</sup> 2000/519/EC

<sup>110</sup> 2000/520/EC

<sup>111</sup> Richard CUMBLEY, *European Union: Report on the Implementation of Safe Harbor*, World Data Protection Report, 2004/11, 11.

<sup>112</sup> 2000/497/EC



feltételeket (Standard Contractual Causes) határozzon meg, amelyek egy szabványszerződési mintának is tekinthetők, és ezek használata a tagállamok számára kötelező. A bizottság két ilyen tartalmú határozatot hozott, egyet a harmadik országba történő személyes adattovábbításokra, és egy másikat a harmadik országban alapított adatfeldolgozók részére történő adatátadásokra.<sup>113</sup>

#### 4.2.11 Bírósági jogorvoslat, felelősség és szankciók

Az irányelv harmadik fejezete a címben megjelölt három témakört egy-egy rövid cikk keretében szabályozza. A jogorvoslat cikkben az irányelv tagállami kötelezettségként előírja, hogy a közigazgatási eljárási jogszabályok által biztosított jogorvoslat mellett az érintett adatbirtokosok számára lehetővé kell tenni, hogy az adatvédelmi felügyelő szervezetéhez fordulhassanak a bírósági felülvizsgálatot megelőzően. A felelősség kérdésére vonatkozóan a tagállamoknak nemzeti jogszabályaik keretén belül ki kell mondaniuk, hogy kártérítési felelősség terheli azt az adatkezelőt, aki a jogellenes személyes adat kezelésével kárt okozott. Az adatkezelő felelőssége alól részben vagy egészben akkor mentesülhet, hogyha ő bizonyítja, hogy a kárért nem felelős. Az irányelv a szankciók vonatkozásában annyit ír elő a tagállamok számára, hogy azokat a nemzeti jogban szabályozniuk kell, hogy azok biztosítsák az irányelv maradéktalan végrehajtását.

#### 4.2.13. A független adatvédelmi kontroll

A személyek magánszférája védelme érdekében az adatvédelmi irányelv 28. cikke előírja, hogy minden tagállam köteles egy vagy több közjogi ellenőrző szervezetet létrehozni, és azt megfelelő személyezettel, anyagiakkal ellátni,

---

<sup>113</sup> OROS Paulina, SZURDAY Kinga, *i.m.*, 13.

hogy a magánszféra védelme érdekében megfelelő intézkedéseket fogadhatson el. Az irányelv kimondja, hogy ezek a szervezetek a rábízott hatásköröket minden más szervezettől teljesen függetlenül lássák el. A teljes függetlenség követelménye akkor teljesül, hogy ha az ellenőrző testület vezetőjét, vagy a vezető testületét nem kizárólag a végrehajtó hatalom nevezi ki, továbbá ha az ellenőrző szervezet vezetője nem mozdítható el, illetve csak akkor, ha valamilyen külön meghatározott eset következik be (pl.: bűncselekmény elkövetése, vagy meghatározott életkor elérése). A teljes függetlenség garanciája, hogy az ellenőrző szervezet nem lehet utasításokhoz kötve, illetve ha a szervezet az általa ellátott feladatokra vonatkozóan megfelelő személyzettel, és anyagiakkal van ellátva. A szervezeti függetlenséget biztosító követelményeket az irányelv nem írja elő, így a tagállamok széles mérlegelési körrel rendelkeznek, hogy a teljes függetlenséget szervezeti jellemzőként értékelik, vagy csak a tevékenység ellátásával szemben támasztott minőségi követelményként. Ezért a nemzeti adatvédelmi biztosok jogállása tekintetében jelentős különbségek vannak. Így egyes országok adatvédelmi vagy információs biztosait a nemzeti parlamentek választják, míg más esetekben az adatvédelmi biztosok kormánytisztviselők, akik egyes kritikusok szerint sokkal megértőbbek a kormányzati cselekvések vonatkozásában, és elnézőbbek a jogalkotási mulasztások esetén. A teljesség igénye nélkül nézzünk néhány tagállami példát: Dániában az adatvédelmi tanács 6 tagját az Igazságügy Minisztérium nevezi ki 4 évre, elnökének bírói tapasztalattal kell rendelkeznie<sup>114</sup>. Észtországban a belügyminiszter javaslatára a kormány nevezi ki az adatvédelmi biztost<sup>115</sup>. Finnországban adatvédelmi tanács és adatvédelmi ombudsman is működik, a biztost, és a tagokat az Államtanács nevezi ki.<sup>116</sup> A görög adatvédelmi hivatal az igazságügy miniszter felügyelete alá tartozik. Az adatvédelmi ügyekben egy egyetemi tanárokból álló „Board” foglal állást, az adatvédelmi hivatalt elnökévé bírót neveznek ki. Más tagállamokban a nemzeti parlament is bekapcsolódik az

---

<sup>114</sup> [www.datatilsynet.dk](http://www.datatilsynet.dk)

<sup>115</sup> [www.dp.gov.ee](http://www.dp.gov.ee)

<sup>116</sup> [www.tietosuoja.fi](http://www.tietosuoja.fi)

adatvédelmi biztos megválasztásának folyamatába, így a német szövetségi adatvédelmi biztost a kormány javaslatára a Bundestag tagjainak abszolút többségével választja, és a köztársasági elnök nevezi ki. Csehországban a szenátus jelöltjét a köztársasági elnök nevezi ki<sup>117</sup>. 2003-ban Olaszországban elfogadott adatvédelmi törvény alapján a parlament mindkét háza részt vesz az eljárásban, a képviselők és a szenátorok is választanak 2-2 főt, akik az adatvédelmi tanácsot alkotják, akik maguk közül elnököt választanak. Ausztriában<sup>118</sup> az adatvédelmi bizottságnak 6 tagja van, akiket a kormány javaslatára az elnök nevez ki. A jelölés eléggé összetett, mert a Szövetségi Legfelsőbb Bíróság által javasolt három jelöltből egyet, a tartományok által ajánlott mindkét jelöltet, a Munkaügyi Minisztérium által javasolt három fő közül egyet, a Gazdasági Kamara által ajánlott három jelölt közül egyet, és egy szövetségi kormánytisztviselőt kell az adatvédelmi bizottságba kinevezni. Az egyes nemzeti szabályozások az adatvédelmi biztosok vonatkozásában további különbségeket mutatnak, mert különböző ellenőrzési szervezetek vannak a magánjogi, illetve a közjogi területen működő adatkezelők vonatkozásában. Az EU adatvédelmi irányelvéből folyó kötelezettség, hogy egységes ellenőrzési szervezetrendszerek alakuljanak ki<sup>119</sup> mind a köz, mind a magánjog területén.

Az irányelv előírja, hogy az ellenőrző szervezeteket az adatvédelemhez kapcsolódó jogszabályok kidolgozása során meg kell hallgatni. Az irányelv részletesen szabályozza azokat a hatásköröket, amelyekkel az adatvédelmet ellátó szervezeteket a tagállami jog szerint fel kell ruházni, így többek között, hogy az adatkezelés ellenőrzése és az érintettek jogainak védelme érdekében vizsgálatokat folytathasson le, illetve az adatkezelést megelőzően állásfoglalást adjon ki, vagy jogellenes adatkezelés vonatkozásában az adatok törlését, zárolását, megsemmisítését rendelhesse el, továbbá az adatkezelést

---

<sup>117</sup> [www.uouu.cz](http://www.uouu.cz)

<sup>118</sup> [www.dsk.gv.at](http://www.dsk.gv.at)

<sup>119</sup> GARSTKA, *Datenschutzbeauftragte der Laende* = Handbuch Datenschutzrecht..., hrsg. ROSSNAGEL, *i.m.*, 801.

ideiglenesen vagy véglegesen megtilthassa. Az adatvédelmi szervezet számára biztosítani kell továbbá, hogy figyelmeztetést vagy bírságot szabhasson ki jogellenes adatkezelés esetén az adatkezelőre, illetve a parlamenthez vagy politikai testülethez fordulhasson adatkezelési visszásság esetén. A nemzeti adatvédelemi jogszabályok megsértése esetére az adatvédelmi szervezet számára keresetindítási jog biztosítandó, illetve más hatóság felé bejelentési kötelezettség is előírandó. Az adatvédelmi szervezet döntései ellen bíróság előtt indított felülvizsgálati eljárásnak nem lehet törvényi akadály. Az irányelv előírja, hogy minden természetes személy, illetve valamely jogi személy képviselőjében eljáró személy beadvánnyal fordulhat az adatvédelmi szervezethez, amely köteles őt arról tájékoztatni, hogy a beadványa alapján miképpen járt el az adatvédelemi tisztviselő. A 28. cikk 4. bekezdése alapján az érintett panasszal fordulhat az adatvédelmi szervezethez, ha vitatja, hogy a közbiztonság, honvédelem, nemzetbiztonság vagy bűncselekmények felderítése, nyomozás eredményessége érdekében lefektetett jogszabályokat az eljáró hatóságok az előírtaknak megfelelően betartották-e.

Az irányelv kijelöli az adatvédelmi kontroll szervezetek területi hatáskörét is azzal, hogy kizárólag a saját tagállamuk felségterületén folytathatják vizsgálatukat, függetlenül attól, hogy a kérdéses „adatfeldolgozásra” mely tagállam joga irányadó. Az adatvédelmi szervezeteket felkérhetik egy másik tagállamból, hogy adatvédelmi vizsgálatot folytasson le a tagállami adatvédelemi szervezetek között fennálló együttműködési kötelezettség alapján.

#### 4.2.13. A 29-es munkacsoport

Az adatvédelmi irányelv 29. cikkében kapott felhatalmazás alapján az egyének személyes adatainak és személyiségi jogaik védelme érdekében létrehozásra került egy tanácsadó szerepkörrel rendelkező munkacsoportot, amely tagállamok adatvédelmi szervezeteinek és a felügyelő hatóságainak

képviselőiből áll. A munkacsoport tanácsadói feladata arra terjed ki, hogy az irányelv egységes alkalmazása érdekében, jogértelmezési kérdésekben kidolgozza a követendő értelmezési megoldásokat. A munkacsoport véleményt nyilvánít az Európai Közösség és harmadik ország által biztosított adatvédelmi szabályozásokról. A munkacsoport az adatvédelmi irányelv módosításával kapcsolatosan véleményt nyilvánít, illetve a 29. munkacsoport a személyes adatok védelmével kapcsolatos bármely kérdésben ajánlást tehet. Az 97/66/EK<sup>120</sup> irányelv 14. cikke a telekommunikáció területén történő személyes „adatfeldolgozások” vonatkozásában is vélemény-nyilvánítási jogot adott a munkacsoportnak. Az elfogadott ajánlásokat, véleményeket és éves jelentetéseket a bizottság a parlament irányába megküldi, illetve nyilvánosságra hozza. A munkacsoport 2005. év folyamán<sup>121</sup> foglalkozott ágazati kérdésként az egészségügyi beteglapok kezelésével, és a munkavállalók adatai védelmének kérdéseivel, illetve a vállalkozásokon belüli kötelező szabályok alkalmazását tekintette át. Az adatvédelmi irányelv alkalmazásával kapcsolatosan a munkacsoport áttekintette a harmadik országba irányuló adattovábbítások egységes értelmezését. A munkacsoport véleményt nyilvánított Kanada, Ausztrália, illetve Új-Zéland adatvédelmi szintjének megállapításáról. A munkacsoport többek között foglalkozott a biometrikus azonosítókkal,<sup>122</sup> a szellemi tulajdonjogokkal<sup>123</sup>, geolokalizációs szolgáltatásokkal, a PET technológiák fejlesztésével, légi utasok személyes adatainak továbbításának kérdéseivel, az új VISA, illetve SIS II rendszer adatvédelmi problémáival.

---

<sup>120</sup> A személyes adatok feldolgozásáról és a magánszféra védelméről a telekommunikációs szektor területén

<sup>121</sup> A 29-es munkacsoport 2005. évi munkaprogram 00862/05/HU WP 109.

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp109\\_hu.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp109_hu.pdf)

<sup>122</sup> 2252/2004 EC. Official Journal L 385 , 29/12/2004 , 1 – 6.

<sup>123</sup> Arbeitspapier, Datenschutzfragen im Zusammenhang mit Immaterialgüterrechten  
[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp104\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_de.pdf)

## 5. FEJEZET: ADATVÉDELEM AZ EU INTÉZMÉNYEIBEN

### 5.1. Személyes adatok védelme az Amszterdami Szerződésben

Az Amszterdami Szerződéssel lett az Unió alapszerződésébe rögzítve a 286. cikk mely szerint:

„(1) 1999. január 1-jétől a személyes adatok kezelése tekintetében a természetes személyek védelmére és az ilyen adatok szabad áramlására vonatkozó közösségi jogi aktusokat alkalmazni kell az e szerződés által vagy az e szerződés alapján felállított intézményekre és szervekre.

(2) Az (1) bekezdésben említett időpontot megelőzően a Tanács a 251. cikkben megállapított eljárásnak megfelelően független ellenőrző szervet hoz létre, amely figyelemmel kíséri az ilyen közösségi jogi aktusok közösségi intézményekre és szervekre történő alkalmazását, és szükség szerint egyéb megfelelő rendelkezéseket fogad el.”

Az adatvédelem alapjogi elismerésére - közösségi elsődleges jogában - ezzel az aktussal került sor, amely valójában megnyitotta annak elismerését, hogy a személyes adatok védelmének mint európai alapjognak a kinyilvánítására az Európai Alapjogi Chartában is sor kerüljön.

### 5.2. A 45/2001/EK rendelet

Az adatvédelmi követelményeknek az EU intézményeire vonatkozó alkalmazását szabályozza az Európa Parlament és a Tanács 45/2001/EK rendelete, amely preambuluma hivatkozik a 95/46/EK és 97/66/EK irányelvekre, és átveszi az általános adatvédelmi irányelv fogalmait, struktúráját. A rendelet meghatározza az „adatfeldolgozás” alapelveit,

alapvető szabályait, a célhoz kötöttség módosításának rendjét. Emellett részletesen szabályozza az egyes szervezeteken belüli, illetve az Európai Közösség szervezetei közötti adattovábbítás szabályait. IV. fejezetében az adatkezelőnek az érintettekkel szembeni információs kötelezettségeit részletesen szabályozza, felsorolja, hogy mely adatokról kell az érintettet tájékoztatni. Az V. fejezet meghatározza az érintettek által gyakorolható jogokat, az adatok törlésének, zárolásának rendjét, illetve az adatbirtokos kifogásolási jogát. A rendelet VI. fejezetében az „adatfeldolgozás” titkosságát, és biztonságosságát szabályozza. A 45/2001/EK rendelet két szintű adatvédelmi intézményrendszert hozott létre egyrészt azzal, hogy hivatali adatvédelmi megbízottakat kell kinevezni, másrészt felállította az európai adatvédelmi biztosi tisztséget. A belső adatvédelmi megbízottak feladatkörébe tartozik, hogy biztosítsák az érintettek adatvédelmi jogait, megtegyék a szükséges tájékoztatást, és független módon járjanak el a rendeletben foglalt betartatása érdekében. A megbízottak feladata, hogy az európai adatvédelmi biztos kérésére tájékoztatásokat adjanak, illetve vezetik a hivatali adatkezelési nyilvántartást. A rendelet 25. cikke alapján az egyes hivatalok által végzett személyes „adatfeldolgozásokat” be kell jelenteni a hivatali adatkezelési nyilvántartásba, melynek részletes adattartamát is szabályozza a jogszabály. A rendelet kitér arra, hogy a belső telekommunikációs hálózatokban milyen rend szerint kezelhetők a személyes adatok, és biztosítani kell a távközlési hálózatok bizalmas voltát. A rendelet szabályozza, hogy milyen jogorvoslati lehetőségek állnak nyitva, ha valamely személynek a személyes adatainak védelméhez fűződő jogát megsértenék.

### 5.3. Az európai adatvédelmi biztos

A 45/2001/EK rendelet létrehozta független adatvédelmi hatóságként az európai adatvédelmi biztosi tisztséget, akinek alapvető feladataként az alapjogok és alapszabadságok garantálását, különös tekintettel a magánszféra védelméhez fűződő jog védelmét szabta meg. Az európai adatvédelmi biztos a

rendelet alkalmazásának és végrehajtásának felügyelete tekintetében az Európai Közösség bármely szerve által folytatott személyes „adatfeldolgozások” esetén eljárhat. Az EU adatvédelmi biztosát az Európai Parlament és a Tanács együttesen választja, egy a bizottság által nyilvános jelölések útján összeállított listáról. A biztost öt éves időtartamra választják, és egyúttal megbízzák a helyettesét is. A rendelet az újraválasztást is lehetővé teszi. A biztost olyan személyi körből választják, amely garantálja, hogy feladatát megfelelő tapasztalattal és hozzáértéssel fogja végezni. A rendelet példaként meghatározza a 95/46/EK irányelv alapján létrehozott nemzeti adatvédelmi hatóságok korábbi vagy jelenlegi vezetőit. A rendelet a biztos jogállása tekintetében szabályozza azokat a különleges okokat, amelyek a megbízatás idő előtti megszűnését okozhatják.

A rendelet a biztos kötelezettségévé teszi, hogy tevékenysége során függetlenül járjon el, így nem fogadhat el utasításokat más személyektől. A függetlenség biztosítása érdekében a biztos nem fogadhat el semmilyen más, akár fizetett, akár nem fizetett tisztséget. A biztos számára a rendelet előírja, hogy megbízatását követően is hivatalához méltóan, visszafogottan cselekedjen. Az európai adatvédelmi biztos feladataként határozza meg a rendelet, hogy a hozzá benyújtott panaszok alapján vizsgálódjon, és tájékoztassa az érintettet egy meghatározott időn belül vizsgálatának eredményeiről. A biztos ellenőrzi a 45/2001/EK rendelet alkalmazásának szabályait az EK intézményeinek belső szabályozásai tekintetében, ez alól kivétel az Európai Bíróság. A biztos felügyeli azon információ- és kommunikációs technológiai fejlesztéseket az EK intézményein belül, ami a személyes adatok védelmére kihatással van. A biztos közösségi intézmények számára konzultációs eljárás keretében minden olyan kérdésben tanácsot adhat, amely a személyes adatok „feldolgozására” vonatkozhat. A biztos hatáskörrel rendelkezik az Eurodac<sup>124</sup>, illetve a VIS (visa információ rendszer)

---

<sup>124</sup> Az eurodac rendszerben tárolják az EU valamely tagállamában menekültügyi kérelmet benyújtott személy azonosító adatait, és ujjlenyomatát. Azzal a céllal, hogy a kiszűrjék azon kérelmezőket, akik több országban is benyújtanak menekültügyi kérelmet.



adattvédelmi felügyelete tekintetében. A biztos részt vesz a 29-es munkacsoport munkájában. A biztos az érintett számára jogairól tájékoztatást ad. A biztos a személyes adatok „feldolgozását” előzetesen vizsgálhatja, és jogellenes adatkezelés esetén figyelmeztetést adhat ki, továbbá az adatkezelést ideiglenesen vagy véglegesen megtilthatja. A biztos szükséges esetben a Parlamentet, a Tanácsot, és a Bizottságot az ügyről tájékoztatja, illetve az Európai Bíróság előtt folyamatban lévő perbe beavatkozhat. A tevékenységének eredményes végrehajtása érdekében minden olyan információhoz, hivatali helyiséghez hozzáférését kell biztosítani, amelyek személyes adatok „feldolgozásával” kapcsolatosak.

## 6. FEJEZET:

### AZ EURÓPAI BÍRÓSÁG EGYES ADATVÉDELMI VONATKOZÁSÚ ÍTÉLETEI

A közösségi jogban az adatvédelmet érintő első lényegi megfogalmazásnak a Stauder-ítélet<sup>125</sup> tekinthető. A bizottság jóváhagyta a tagállamoknak, hogy szociálisan rászorult személyek számára a túltermelésből származó vajtermékeket átadják. A visszaélések megakadályozása érdekében a bizottság előírta, hogy a vajhoz kizárólag névre szóló utalvány alapján lehet hozzáférni. A stuttgarti közigazgatási bíróság álláspontja szerint a közösség ezen szabályozással megsértette azon alapvető jogokat, amelyek tiszteletben tartására a közösség részben köteles. Az EK Bíróság arra a megállapításra jutott, hogy az érintett nevének feltüntetése nem feltétlenül szükséges, ha más módon is megoldható az ellenőrzés. Ugyan ez a döntés adatvédelmi terminológiát nem használ, de ez a megközelítés a mai felfogás szerint az adattakarékosság elvének gyakorlati megvalósulását jelentette<sup>126</sup>. Az EK Bíróságnak az adatvédelmet érintő döntése a versenyjogi esetekhez kapcsolódóan kerültek megfogalmazásra. Az egyik esetben<sup>127</sup> a bizottság olyan információt adott ki, amely miatt egy versenyjogi kartell összefonódást bejelentő belső munkatárs személye a kartellező társaság számára azonosítható vált, aki ezen információ alapján büntetőfeljelentést tett a volt alkalmazottja ellen üzleti titok kiadása miatt. A volt alkalmazott kártérítési pert indított a EK ellen, mivel egy svájci bíróság büncselekmény miatt elítélte. A Hoechst-ügyben<sup>128</sup> a Bíróság azt vizsgálta, hogy a versenyjogi eljárás alá vont társaságot irodai székhelyeinek hatósági átkutatása során, milyen alapvető jogok illetik meg, és arra a megállapításra jutott, hogy a jogi személyek nem hivatkozhatnak az emberi jogok európai egyezményének 8. cikkelyében biztosított magánélet védelme alapvető jogra.

---

<sup>125</sup> EKB 29/69; 1969. 419.

<sup>126</sup> SIEMEN i.m. 214.

<sup>127</sup> Stanley Adams-ügy; EKB 145/83 1985. 3556

<sup>128</sup> EKB 46/87 és 227/88 1989. 2859

Az EKB kezdeti adatvédelmi tárgyú ítélkezési gyakorlatáról az mondható, hogy a magánélet védelme szempontjából az ítélkezés világos normára nem támaszkodhatott, mivel a közösségi jogban a magánélet védelme, vagy az adatvédelem nem került az alapszerződések szintjén lefektetésre. Ezért volt szükség arra, hogy az EKB elismerje a magánélet védelmét a tagállamok közös alkotmányos hagyományaként, így jogforrási szinten támaszkodni tudott az Európai Emberi Jogi Egyezményben megfogalmazottakra. Az EKB az egészségügyi adatok kezelésével kapcsolatosan fejtette ki, hogy az EEJ 8. cikke kiterjed arra, hogy az érintett egészségi állapotára vonatkozó adatokat titokban tartsák<sup>129</sup>. Az EKB gyakorlatában hamar teret nyert, hogy az érzékeny adatok, és egyes személyes adatok a magánélet védelme körébe sorolandók, de az üzleti adatokkal kapcsolatosan már más álláspontra helyezkedett, mint a strasbourgi bíróság. Az EKB szerint a jogi személyek üzleti célú helyiségei nem esnek a magánélet védelme körébe.

Az Európai Közösségek Bíróságának ítélkezési gyakorlata szempontjából meghatározó, hogy az alapszerződésben az adatvédelem lefektetésére sor került, illetve az 95/46/EK irányelv elfogadása megtörtént. Az irányelv implementációval kapcsolatosan a Bizottság részéről Luxemburg ellen indítottak eljárást,<sup>130</sup> amely eljutott az ítélethozatalig, más, korábban már ismertetett<sup>131</sup> eljárások bírósági döntést megelőzően megszüntetésre kerültek. Az adatvédelmi szakértők vártak a „Data Privacy” irányelv EKB általi értelmezésére, de eddig viszonylag kevés eljárás zárult le az Európai Közösségi Bíróság előtt, amelyekben az adatvédelem szempontjából lényeges értelmezési kérdésekre világítottak rá.

---

<sup>129</sup> EKB C404/92 X v. Commission 1994. I-4737

<sup>130</sup> C-450/00 Commission v. Luxemburg, April.10.2001.

<sup>131</sup> Lásd: a 95/46/EK irányelv és előzményei cím alatt

Az EKB első adatvédelmi vonatkozású ítélete az irányelv elfogadását követően a TR és P Fischer-ügyben<sup>132</sup> született. Ugyan az irányelv még nem lépett hatályba, de az EKB ítélethozatala során támaszkodott az abban a személyes adatoknak harmadik személyek részére történő átadásra vonatkozóan megfogalmazottakra, és arra a megállapításra jutott, hogy hatósági adatbázisokban felhalmozott személyes adatnak harmadik személy részére történő kiadása lehetséges, ha ez a harmadik személy jogos érdekeinek védelme szempontjából szükséges, de ebben az esetben a hatóságnak érdemi mérlegelést kell lefolytatni az egymással szembenálló érdekek tekintetében.

## 6.2. A Österreichische Rundfunk versus Rechnungshof-ügy<sup>133</sup>

Az adatvédelmi irányelv jelentősége a közösségi alapjogvédelem szempontjából ebben az ügyben vált jelentőssé. Az osztrák Alkotmánybíróság és a Legfelsőbb Bíróság is előzetes döntéshozatali kérelemmel fordult a luxemburgi bírósághoz, két kérdés megválaszolása iránt érdeklődve. Az osztrák számvevőszék jogvitába keveredett számos, a felügyelete alatt álló, a központi költségvetésből részben vagy egészben finanszírozott intézménnyel, így az ORF-fel, az Austrian Airlines-sal, Niederösterreich tartománnyal, és még két magánszeméllyel. A jogvita lényege abban állt, hogy az intézmények megtagadták a számvevőszék részére azon adatok átadását, amelyek magánszemélyek fizetéseinek, tiszteletdíjának összegeire vonatkoztak, arra való hivatkozással, hogy ez sérti az EU adatvédelmi irányelvében foglaltakat. A vonatkozó osztrák szabályozás szerint a számvevőszék azoknak a személyeknek a nevét és fizetését teszi közzé, akik az adott évben egy meghatározott összeg felett részesülnek állami díjazásban. Ez az adott évben 82.414 euro volt (kb. 20 millió Ft). Az Alkotmánybíróság rámutatott a törvényhozó azon szándékára, mely a széleskörű nyilvánosság biztosításával

---

<sup>132</sup> EKB C-369/98

<sup>133</sup> C-465/00, a C-138/01 és a C-139/01 Bíróság ítélete 2003. május 20-ról

az érintett intézményekre nyomást kívánt gyakorolni, hogy a fizetéseket alacsonyan tartsák, és így a közpénzekkel takarékosan bánjanak, azokat gazdaságosan, és hatékonyan használják fel. Az Alkotmánybíróság kétségét fejezte ki, hogy a számvevőszékre vonatkozó előírás összhangban lenne a közösségi előírásokkal, mert aránytalan mértékben korlátozza a személyes adatok védelméhez fűződő jogot.

Az eljárás során az érintett intézmények és magánszemélyek arra hivatkoztak, hogy a fizetési adataik nyilvánosságra hozatala sérti az európai emberi jogi konvenciót, illetve megnehezíti a munkavállalók tárgyalási pozícióját, ha más EU tagállamban kívánnának állást vállalni, mivel fizetési igényeiket a munkaadók előzetesen már megismerhetik.

Az eljárás során előkérdésként felmerült, hogy alkalmazható-e egyáltalán a közösségi jog a jogvitában. Az olasz és osztrák kormány által is támogatott számvevőszéki álláspont szerint a számvevőszék által végzett ellenőrzési tevékenység, amely célja az általános közérdek alapján az osztrák államháztartás területén végzett ellenőrzési tevékenység nem esik a közösségi jog hatálya alá. Másrészt a peres fél által állított joghatóság megállapítását szolgáló indok, hogy az osztrák szabályozás sérti a munkavállalók szabad mozgását hipotetikus és indirekt. A bizottság is hasonló álláspontot képviselt, azaz ennek az ügynek nincs közösségi jogi relevanciája.

A bíróság ezzel szemben arra a megállapításra jutott, hogy a 95/46/EK irányelv alkalmazását nem lehet attól függővé tenni, hogy az alapeljárásban egy megfelelően kielégítő ok áll-e összefüggésben az EK alapszerződésében garantált alapszabadságokkal, így a munkavállalók szabad mozgásával. Egy ellentétes értelmezés arra vezetne, hogy az irányelv alkalmazási körének lehatárolását bizonytalanná tenné, és így véletlenszerű eseményektől válna függővé annak alkalmazása, amely a jogharmonizáció legfőbb célját sértené. Az, hogy az irányelv azon tényállásokra alkalmazandó, amelyek esetében nem

áll fent a közvetlen összefüggés az EK alapszerződésekben garantált alapszabadságokkal, levezethető az irányelv 3. cikkének (1) bekezdésében rögzítettekben, melyben a jogalkotó az irányelv széles alkalmazási körét határozza. Az irányelv tárgyi hatályát a 3. cikk (2) bekezdés korlátozza azzal, hogy nem alkalmazandó az irányelv az Európai Unió Alapszerződésében V. és VI. címeiben meghatározott területeken, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal, továbbá büntetőjog területén, továbbá természetes személy által végzett kizárólag személyes vagy családi tevékenysége vonatkozásában.

A Bíróság előzetesen megállapította, hogy az érintettek adatai - úgymint a részükre fizetendő fizetés nagysága - az irányelv szerint személyes adatnak tekinthetők. A tagállamoknak az „adattfeldolgozás” során teljesíteni kell 6. cikkben az adatok minőségével szemben támasztott követelményeket, így az „adattfeldolgozásnak” tisztességesnek, a célhoz kötöttnek kell lennie, figyelembe kell venni a készletező adatgyűjtés tilalmát, továbbá az adatok tárolására csak annyi ideig kerülhet sor, mint amennyit az „adattfeldolgozás” célja szükségessé tesz. A bíróság álláspontja szerint a 6. cikk alóli kivételeket a 13. cikk szabályozza, amelynek e) és f) pontja megengedi szükséges esetben a korlátozásokat. Egy tagállam fontos gazdasági vagy pénzügyi érdekéből kifolyólag, vagy devizaügyi, államháztartási, illetve adózási ügyekben, továbbá állami felügyeleti, ellenőrzési és igazgatási funkciók esetén, ha azok tartósan vagy időlegesen összekapcsolódnak közhatalom gyakorlásával, akkor a személyes adatok kezelése tekintetében a 6. cikk alól kivételeket állapíthat meg. A bíróság megállapította, hogy a kérdéses ügyben a magánéletbe történő beavatkozás megállapítható, de továbbiakban azt vizsgálta, hogy igazolható-e a beavatkozás szükségessége és arányossága.

A beavatkozás igazolásának áttekintését a bíróság az Emberi Jogok Európai Egyezményének 8. cikkének értelmezésével kezdi, mely megengedi, hogy a 8. cikkben rögzített magánélethez való jog védelmének korlátozását, ha

törvényileg szabályozott, és ez a 8. cikk (2) bekezdésében lefektetett célok elérése érdekében egy demokratikus társadalomban is szükséges korlátozásnak tekinthető. A Bíróság e kiinduló pont alapján azt vizsgálta, hogy a beavatkozást, korlátozást megengedő szabályok a címzettek számára kellőképpen világosan vannak-e megfogalmazva. Az EKB az előzetes döntést kérő bíróságra bízta e kérdés alapján annak eldöntését, hogy a törvényi előírások megfelelnek-e a jogbiztonság követelményeinek. A beavatkozás igazolásának második kérdése, hogy a kérdéses beavatkozás szükséges-e a demokratikus társadalomban a kitűzött cél elérése érdekében.

A bíróság szerint egyik oldalról a számvevőszéknek és a parlamenti szerveknek kétségtelenül ismerniük kell a különböző közjogi szervezetekben a személyzeti kiadások nagyságát azért, hogy a közpénzek szabályszerű felhasználását ellenőrizhessék. Ezen kívül a demokratikus társadalomban az adófizetőknek és a nyilvánosságnak is igénye van arra, hogy a közpénzek elköltéséről, különösen a személyzeti kiadásokról tájékozottassák. Ilyen jellegű információknak a közreadása hozzájárul a közügyek érdemi megvitatásához. Másrésztől adódik a kérdés, hogy az érintettek nevének a számukra fizetendő összeggel történő összekapcsolása és közreadása arányos mértékben áll-e az elérendő céllal. Ennek a kérdésnek a vizsgálata az előzetes döntéshozatal előterjesztő bíróság feladata.

A Bíróság az előzetes döntést kérő bíróság második kérdésével is foglalkozott. A kérdés arra irányult, hogy ha a nemzeti jogszabályok az irányelvben meghatározottakkal ellentétesek, akkor az adatok közzétételére kötelezett személyek hivatkozhatnak-e közvetlenül alkalmazandóan az irányelvre? A kérdés megválaszolásakor a bíróság emlékeztetett arra, hogy az egyének az irányelvre akkor hivatkozhatnak, ha azok az előírt határidőn belül nem kerültek implementálásra, ha az irányelv meghatározásai tartalmilag feltételhez nem kötöttek, és megfelelően pontosak. Ha ezen feltételek fennállnak, akkor minden az irányelvbe ütköző tagállami szabályozással

szemben hivatkozni lehet az irányelv rendelkezéseire. A bíróság a 95/46/EK irányelv 6. cikk (1) bekezdés c.) pontja, illetve a 7. cikk c.) és e.) pontjai esetében megállapította, hogy ezek kellő világosan vannak meghatározva, és az egyének számára biztosítanak jogokat. A Bíróság kimondta, hogy az irányelv ezen részei közvetlenül alkalmazandók, az egyének a nemzeti bíróságok előtt e cikkekre hivatkozhatnak, azért hogy a közösségi szabályokkal ellentétes nemzeti előírások alkalmazását megakadályozhassák.

Az Österreichische Rundfunk-ügyben olyan döntés született, amely a közösségi jogban az adatvédelem fejlődését markánsan kijelölte. Az Európai Közösségek Bírósága meghatározta az irányelv hatályát, és alkalmazhatóságát, valamint azt a követelményt, hogy a nemzeti előírásoknak a közösségi jogban elfogadott adatvédelemi elvekkel összhangban kell állniuk. Az EKB ítélete alapján az adatvédelmi irányelvnek széleskörű alkalmazása áll fenn, azaz olyan tényállások esetén is alkalmazandó, amelyben kizárólag nemzeti elemek vannak határon átnyúló relevancia nélkül. Az EKB az irányelv közvetlen alkalmazhatóságát (direkte Anwendung) állapította meg, ha a tényállásban közösségi elem merülne fel.

Az EKB a jogeset vizsgálatakor visszanyúlt az Emberi Jogok Európai Bírósága esetjogához és vizsgálati módszeréhez. A Bíróság megállapította, hogy a jelen esetben a jövedelmi adatok nyilvánosságra hozatala a magánszférába történő beavatkozását jelent, így a konvenció 8. cikkelyének sérelme fennáll. A bíróság ezt követően azt vizsgálta, hogy az alapvető jog korlátozása indokolható-e valamely egy a demokratikus államban elfogadott okból, így mások alapvető jogának érvényre juttatása, vagy más alkotmányosan indokolt közérdek védelmében. Azt a bíróság megállapította, hogy a jövedelmi adatok nyilvánosságra hozatala egy jelentős beavatkozás a magánélet védelmébe, de a nemzeti bíróság hatáskörébe utalta annak eldöntését, hogy az alapjog korlátozás szükségessége indokolható-e.



Az EKB a magánélet védelmével kapcsolatos ítélkezésében szorosan igazodik az Emberi Jogok Európai Bírósága joggyakorlatához, de egy jelentős különbség mégis fellelhető a két bíróság jogértelmezése között. Az EKB felfogása szerint egy személyes adat akkor is a konvencióban rögzített 8. cikkely hatálya alá esik, ha a személyes adat nem közvetlenül a magánszféra körébe sorolható<sup>134</sup>. Az EKB ítélete megalapozta az irányelv alkalmazásának kiterjesztését, valamint azt, hogy a magánszemélyek kizárólag nemzeti jogban felmerülő jogsérelem esetén is hivatkozhatnak közvetlenül az irányelv alkalmazhatóságára. A személyes adatok védelmének sérelme esetén nemcsak az adatvédelmi irányelvre lehet közvetlenül hivatkozni, hanem a közösségi jog általános jogelvei is felhívhatók a hatékony alapjogvédelem megvalósítása érdekében.

Az adatvédelem alapjogi fejlődésének áttekintése szempontjából megjegyezendő, hogy a jogeset lényege annak vizsgálata volt, hogy egy állami szabályozás összeegyeztethető az alapvető jogokkal, alapszabadságokkal, elsősorban a természetes személyeknek a magánszféra védelméhez fűződő jogával, ha a természetes személynek a személyére vonatkozó adatoknak a kezelésére kerül sor. A jelen esetben az adatvédelemnek a vertikális jogviszonyokban alkalmazható elméleti módszere került kibontásra, a következőkben horizontális jogviszony esetén tekintem át az adatvédelem érvényesülését.

## 6.2. A Lindqvist-ügy<sup>135</sup>

Bodil Lindqvist nevű hölgy, aki a svéd protestáns egyház egyik helyi szervezetében önkéntesként dolgozott, elhatározta, hogy számítógépes tanfolyamot szervez, és oktatást tart arról, hogyan lehet otthon egyszerűen

---

<sup>134</sup> SIEMEN i.m. 266

<sup>135</sup> C-101/01 6.11.2003)

saját szerkesztésben weblapokat létrehozni. Az asszony létre is hozta a saját weblapját és elhatározta, hogy információkat használ fel a saját egyházaról, és emellett egy linkkel összekapcsolta a saját és a svéd protestáns egyház weblapját. A probléma abban állt, hogy Mrs. Lindqvist által közzétett weblap az egyháznál dolgozó más személyekről is tartalmazott információkat, például a teljes nevüket, vagy csak a keresztnévüket, illetve Mrs. Lindqvist kissé humoros formában leírta a kollégái által ellátott munkaköröket, és a szabadidős szokásaikról is tett közzé információkat, emellett megemlítette személyes, családi körülményeket, továbbá telefonszámokat is közzétett. Természetesen Lindqvist asszony nem kapott felhatalmazást ezen adatok publikálására, amit kifogásoltak az érintettek, és hamarosan követelték tőle a weblap törlését, amelynek ő eleget is tett. Az ügy nem zárult le ezzel, mert a svéd ügyészség az asszonyt 4.000 SEK pénzbírság fizetésére kötelezte, mert előzetesen nem jelentette be a személyes adatok kezelését, és azoknak harmadik országba való továbbítását a svéd adatvédelmi hatóságnak, illetve mert az érintettek engedélye nélkül kezelt érzékeny adatokat.

Az Európai Bíróság a jogesetet több vizsgálandó kérdésre bontotta<sup>136</sup>. Így először azt értelmezte, hogy mely adatok tekinthetők olyan személyes adatnak, amelyek az irányelv hatálya alá esnek. Így az irányelv 2 cikke szerint személyes adatnak mindazon információ tekinthető, amely egy természetes személy azonosításával vagy azonosíthatóságával kapcsolatban áll. Az irányelv nem határozza meg, hogy azok az adatok, amelyek a nyilvánosság számára korábban már hozzáférhetőek voltak, minősíthetők-e személyes adatnak. Az érintettek telefonszámai korábban a nyilvánosság számára már hozzáférhetőek voltak, a bíróság megerősítette, hogy ezen személyes adatok kezelése is az irányelv hatálya alá esnek.

---

<sup>136</sup> Andre FIEBIG, Some Judicial Guidance in the Interpretation of European Data Privacy Directive, World Data Protection Report, 2003/12, 6.

A bíróság másodsorban az értelmezte, hogy az irányelv alkalmazásának kizárását a személyes adatok nem gazdasági jellegű használata tekintetében milyen keretek között lehet megengedni, illetve milyen adatkezelés minősül „magáncélú adatkezelésnek”. Mrs Lindqvist arra hivatkozott, hogy tulajdonképpen az általa végzett adatkezelés ezen kivétel alá esik<sup>137</sup>. A főtanácsnok azzal érvelt, hogy „az adatkezelések olyan fajtája, amely során adatokat egy homepage-re feltelepítik a gazdasági nyereségszerzés szándéka nélkül, kizárólag egyházi szervezet részére végzett önkéntes kisegítő tevékenységként, amelyben a munkavállalói jogviszony nem merül fel, nem esik az irányelv hatálya alá”. Az EKB most is, mint a legtöbb esetben, követte a Főtanácsnok álláspontját, bár sokkal nyersebben fogalmazott, mint a Főtanácsnok. Az EKB szerint azon tevékenységek, amelyek a magán vagy családi élettel kapcsolatosak, nem minősülnek olyan adatkezelésnek, mint amikor az interneten közelebbről meg nem határozható számú ember számára hozzáférhető publikáció kerül közreadásra.

A Bíróság által vizsgált második kérdés az adatvédelmi irányelv a személyes adatoknak harmadik országba történő továbbításával kapcsolatos rendelkezésekre irányult. Az adatvédelmi irányelv megtiltja személyes adatok továbbítását az EU-n kívüli országba, ahol a személyes adatok védelme nem felel meg az EU által meghatározott védelmi szintnek. Például a Bizottság az USA-t olyan országgént határozta meg, amely az elvárt védelmi szintet nem garantálja, így oda főszabály szerint nem lehet adatokat továbbítani. Sajnálatosan az irányelv nem határozza meg, hogy mi az adattovábbítás fogalma. Tisztázatlan, hogy adattovábbításnak minősül-e, ha valaki az EU-n belül feltölti az adatokat az internetre, és egy másik személy kapcsolatba lép az interneten keresztül ezzel a weblappal. Az EKB vizsgálata alapján az interneten történő adattovábbítás két különböző folyamatból áll. Az első

---

<sup>137</sup> Ulf BRÜHANN, *Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem*, Datenschutz und Datensicherheit, 2004/28, 201.

lépcsőben az adattovábbító feltölti az adatokat a fogadó „provider”-re (szerverre), a második lépcsőben a kereső a számítógépének infrastruktúráját használva hozzájut az adatokhoz a szerverről. Az EKB leszögezte döntésében, hogy az adatok feltöltése a szerverre önmagában nem valósítja meg az adattovábbítást, hanem az nem jár az idegen szerverrel való kapcsolatba lépéssel. A bíróság megállapította, hogy más országokba történő adattovábbítás lehetne az is, hogy ha személyes adatokat weblapra feltöltenek, és lényegében sokkal több országot jelent, mint amelyekre vonatkozóan a bizottság a védelem megfelelő szintjét kimondta. A bíróság a jogalkotó helyett nem mondhatja ki, hogy adatok idegen szerverre történő postázása egyben adatok továbbításaként lehetne felfogni. A bíróság arra az eredményre jutott, hogy különbséget kell tenni aktív adattovábbítás, és adatoknak egy idegen szerverre történő postázása között. A bíróság felfogása szerint a 25. cikk kizárólag az aktív adattovábbításra vonatkozik.

A bíróságnak harmadik kérdésként a véleménynyilvánítás szabadsága és a személyes adatok védelmének összeütközése tekintetében is vizsgálódnia kellett. Mrs. Lindqvist hivatkozott arra, hogy a véleménynyilvánítás szabadsága a közösségi jog alkotmányos alapelve közé számít. Az ő meglátása szerint természetes személyek nevének említése, telefonelérhetőségük közreadása, illetve munkakörülményeik, egészségi állapotuk egyes részleteinek nyilvánosságra hozatala nem érinti lényegesen a magánélet tiszteletéhez fűződő jogot. Az EKB megállapította, hogy bizonyos speciális esetekben konfliktus keletkezhet a véleménynyilvánítás és a személyes adatok védelme között, amelyek közötti egyensúlyt a tagállamoknak kell létrehozni. A bíróság hangsúlyozta, hogy mivel Mrs. Lindqvist tevékenysége nem gazdasági jellegű volt, ezért ebben a kérdésben a tagállami jogalkotásnak kell az alapvető jogok megfelelően arányos korlátozása mellett az egyensúlyt megtalálni.

A Lindqvist-ügy jelentősége abban határozható meg, hogy áttekintette a véleménynyilvánítási szabadság és a magánszféra védelmének összeütközését, és meghatározta azokat a mérlegelési szempontokat, amelyeket alapvető jogok összeütközése tekintetében követnie kell a hatóságoknak. A bíróság kimondta, hogy a önmagában nem áll fenn ellentmondás a véleménynyilvánítási szabadság, és a személyes adatok védelme között. De a személyes adatok kezelésével kapcsolatos esetekben a nemzeti hatóságoknak a nemzeti jogszabályaikat nemcsak az EK adatvédelmi irányelvvel összhangban kell értelmezni, hanem tekintettel kell lenni a közösségi jog általános jogelveire. A bíróság megerősítette, hogy a magánszféra védelmében szükség van hatékony szankciók alkalmazására, és tekintettel kell lennie az arányosság elvére, így figyelembe kell venni a jogsértés súlyát, tartamát, illetve az érintett személyekről közreadott adatok körét.

A Lindqvist-ügy magánszemélyek személyiségi jogainak megsértése miatt indult büntetőeljáráshoz kapcsolódik. Véleményem szerint közvetetten következtethetünk magánszemélyek közötti horizontális jogviszonyokban alkalmazandó elvekre is a jelen ügyből kifolyólag. Így személyiségi jogi sérelem miatti polgári ügyekben is alkalmazandó alkotmányos elvként az arányosság elve.

Véleményem szerint a horizontális jogviszonyokban is alkalmazható az arányosság elvéből levezethető adattakarékosság elve, mely szerint kizárólag az adott cél elérése érdekében szükséges adatkezelésre kerülhet sor magánszemélyek közötti szerződéses jogviszonyokban. Az állami hatóságok az adatgyűjtési hatáskörüket kötelezettségként magánszemélyekre kivételes esetben ruházhatják át, és igen szűk körben lehet magánszemélyek közötti jogviszonyokban az adatkezelőt az állam meghosszabbított adatgyűjtőjeként meghatározni.

### 6.3. Légi utasok adatainak továbbítása az USA-ba<sup>138</sup>

2001. szeptember 11-ét követően az USA újraszabályozta a légi közlekedésre irányadó szabályokat. Ez alapján minden az USA-ban leszálló légi járatnak meg kell előzetesen küldenie utasainak személyes adatait az illetékes amerikai hatóságnak. Az Európából az USA-ba tartó légi járatok vonatkozásában a bizottság 2004/535/EK döntésével tette kötelező a légi utasok adatainak USA-beli továbbítását. Az Európa Parlament a bizottság ellen keresetet<sup>139</sup> nyújtott be, hogy a bizottság 2004/535/EK döntését semmisítse meg a bíróság. Az Európa Parlament négy okkal támasztotta alá keresetét, amelyekkel azt kívánja igazolni, hogy a bizottság túllépte hatáskörét, megsértette a 95/46/EK irányelv lényeges szabályait, továbbá alapjogokat sértett, valamint megsértette az arányosság követelményét is. A hatáskör túllépés tekintetében a bizottság olyan döntést bocsátott ki, a 95/46/EK irányelv figyelembe vétele nélkül, amely olyan területre vonatkozik, ami nem esik a közösségi jog hatálya alá. Az Európai Parlament érvelése szerint az amerikai Vám-és Határőrség (CBP) nem minősül harmadik országnak az irányelv 25. cikke alapján. A megfelelő védelmi szintről szóló döntés lehetővé tesz adattovábbításokat minden amerikai hivatal és harmadik ország számára, amely az irányelv nyilvánvaló sérelmét jelenti. A bizottság döntése alapján a CBP közvetlenül hozzáférhet minden légi utas adatához, amely az irányelv megalkotóinak nem volt szándéka. Az Európai Parlament arra is hivatkozott, hogy a CBP megfelelő adatvédelmi szintjének kinyilvánításával megsértette az irányelv lényeges alapelveit. A jogsértés abban áll, hogy a lefektetett céltól eltérő célokra használják fel az adatokat, nincsen jogi előírás az „adatfeldolgozás” rendjére vonatkozóan, az érzékeny adatok kezelésére nincs megfelelő eljárás, nincsen

---

<sup>138</sup> Heather ROWE, *The Transfer of Personal Data Regarding Airline Passengers from the EU to the U.S.*, World Data Protection Report, 2004/03, 13.

<sup>139</sup> C-318/04 2004. 09.11 32.old

biztosítva a bírói jogvédelem az „adattfeldolgozás” kifogásolására, illetve az adattovábbítás bizottsági engedélyezése más amerikai hivatalok számára és más országok számára összeegyeztethetetlen az irányelv által megkövetelt tényleges és hatékony védelemmel. Az Európa Parlament szerint a bizottság döntése aránytalan mértékben megsértette az Európai Emberi Jogi Egyezmény 8. cikkében lefektetett magánélet védelméhez való jogot azzal, hogy a légi utasok túlzottan sok adatát továbbítják az amerikai hatóságoknak, és ezek az adatok ott túl hosszú ideig, 15 évig kerülnek tárolásra. Az Európa Parlament oldalán beavatkozott az európai adatvédelmi biztos is, illetve még az Egyesült Királyság, és Írország avatkozott be a perbe, amely 2004 őszén indult. A főtanácsnok véleménye alapján az EKB ítélete megszületett, amely nem tartalmi, hanem formai szerződés sértésre hivatkozással semmisítette meg az USA és az EU között létrejött megállapodást, mivel annak megkötésére a bizottságnak a tagállamoktól nem volt felhatalmazása. A jogvita lezárulása előtt már elkezdődtek a tárgyalások a légi utasok személyes adatkezelésére vonatkozó feltételrendszer átalakításáról. Az egyeztetések ahhoz vezettek, hogy a bizottság már a tagállamok jóváhagyása alapján köthette meg a légi utasok adatainak továbbítására vonatkozó egyezményt, illetve a személyes jellegű adatkezelés tekintetében az európai adatkezelési elveket alkalmazzák az amerikai hatóságok.

A II. rész összegzése: Az adatvédelem, európai alapjog

Az adatvédelem európai alapjoggá vált, ehhez nem férhet kétség. Az európai adatvédelmi jog fejlődése szorosan köthető az Európai Közösségek Bíróságának jogfejlesztő ítélkezéséhez azzal, hogy az Európai Emberi Jogi Egyezményben lefektetett magánélet védelmének alapjogát elismerte a közösségi jogban úgymint a tagállamok közös alkotmányos hagyományát. Ugyan az Európai Közösségek Bírósága sok tekintetben támaszkodott az Európai Emberi Jogi Bíróságnak a magánszféra védelmével kapcsolatosan

kialakított jogfelfogására, de egy lényeges tekintetben eltért tőle, mely szerint az EKB a magánélet sérelmét megállapíthatónak tartja akkor is, ha a személyes adat nem közvetlenül a magánszférával függ össze.

Az európai adatvédelmi jog kialakulásának nélkülözhetetlen lépcsője volt az Európa Tanács Adatvédelmi Egyezménye, amely az EK tagállamaiban az adatvédelem önkéntes recepció útján előkészítette. Az Európa Tanács Adatvédelmi Egyezményében megfogalmazott információs önrendelkezési jog alapjogi jelleggel került a tagállamok által elfogadásra a vertikális jogviszonyokban. Az adatvédelem elveinek, szabályainak a nemzeti jogalkotás útján horizontális jogviszonyokban történő elismerésére véglegesen valójában az EK adatvédelmi irányelve alapján került sor. Az NSZK, mint az adatvédelmi jogalkotás úttörője sokáig késlekedett az adatvédelmi irányelvnek a hazai jogába történő átültetéssel. Az európai információs önrendelkezési jog gyakorlati érvényesüléséhez nélkülözhetetlen volt az Európai Közösségek Bíróságának döntése az Österreichische Rundfunk ügyben, amely lehetővé tette a nemzeti jogban közösségi jogi relevancia nélkül az irányelvre történő hivatkozást, illetve közösségi relevanciával bíró esetekben kimondta az irányelv közvetlen alkalmazhatóságát.

Azzal, hogy az adatvédelem európai alapjog benne rejlik annak „területi hatálya” is, így Európát elhagyva annak alapjogi jellege megszűnik. A mai globalizált világban, amikor adataink már másodperc alatt megkerülik a földet, és személyesen pár óra alatt más kontinensen lehetünk az európai adatvédelem által nyújtott kényelem könnyen kiszolgáltatottá tehet minket.



### III. RÉSZ A MAGYAR ADATVÉDELEM ALAPJAI ÉS KERETEI

#### 7. AZ ADATVÉDELEM KIALAKULÁSÁNAK MAGYAR ÚTJA

##### 7.1. A magyar nyilvántartási jog rövid története

A személyes adatok védelméről csak a XX. század közepétől beszélhetünk, de adatvédelem gyökerei mindenekelőtt az adatgyűjtésekhez kapcsolódnak. Állami adatgyűjtéseket a központi hatalmi rendszerek kialakulásától kezdve végeztek, ezért adatgyűjtésekre vonatkozó szabályokban érhető tetten az adatvédelmi garanciák „ős elveinek” a megjelenése is. Minden központi hatalom működésének alapja a rendszeres adókiadás és beszedése, ezért magától értetődik, hogy az első adatgyűjtések is az adózás terén kezdődtek. E téren a magyar jogalkotási források a XVI. században jelentek meg, mert a központi hatalom megerősödését az adóbevételek növelését megalapozó adóösszeírásoktól várta. Az adófizetés módjáról szól a 1537. évi III. törvénycikk, amely az adóösszeírásra vonatkozó szabályokat rendezi. A törvénycikk előírja, hogy "minden egyes vármegyében választandó az előkelőbbek közül két nemes (a kiknek hűsége és becsületessége tudniillik mindenki előtt ismeretes), a kik hitük és becsületük elvesztésének és összes javaik elkobzásának büntetése alatt úgy az uraknak, mint a nemeseknek és szabad városoknak meg bármely más birtokosoknak minden jobbágyát kapunként hűségesen írják össze. És azok az adólajstromokat mindjárt az összeírás után láttassák el mindenütt híven az alispánok és szolgabírák pecsétjeivel." A központi hatalom törekvései a teljes vagyoni állapotok felmérésére a középkorban sem jártak sikerrel. A polgárok a vagyoni védelme érdekében nem jogi eszközöket vettek igénybe, hanem olyan ötleteket eszeltek ki, amelyekkel az adófizetés alapjául szolgáló tényeket megváltoztassák, illetve az adófizetési kötelezettségüket csökkentsék. Az állami adatgyűjtés fő módszertanaként alakult ki, hogy az adóösszeírások

során felmérték a lakosságot lélekszám és vagyoni állapot szerint. Ha a mai fogalmakat akarnánk használni, akkor az adófizetési képesség felmérése során két adatbázist alakítottak ki, egyet a népesség nyilvántartásra és egyet a vagyoni állapot felmérésére, és ezeket az adatbázisokat összekapcsolva kezelték.

A kora középkortól kezdődően a személyekre vonatkozó adatgyűjtő és nyilvántartó szervezet nem a központi hatalom, hanem az egyházi intézményrendszer volt. Az egyházak felekezetenként vezették a születésekről, házasságkötésekről, és a halálozásokról az anyakönyveket. Az egyháznak voltak olyan "helyi szervei", amelyek a legfontosabb személyi adatokat, mint a név, születés, házasság, halálozás ideje rögzítették. A másik, az ingatlanok tulajdoni állapotokra vonatkozó nyilvántartási rendszert, a hites helyek hálózata vezette. Az 1764/65. évi XI. törvénycikk rendelkezik a hites helyekről és kötelezettségeiről. "Igazságosnak és illendőnek ismeri ő szent felsége, hogy a hites helyek a levéltárakban létező irományok pontos lajstromozására szoríttassanak, s az a végett szükséges intézkedések a helytartó tanács útján tétessenek meg." A pontos adatgyűjtés és nyilvántartás követelményeit nemcsak a hites helyek rendszerével kapcsolatosan követelte meg a központi kormányzat, hanem a nemesi vármegyéknek a levéltárakra vonatkozóan is teljesíteni kellett ezeket az előírásokat.

A XVIII. században a hadi igények megkövetelték a tömeghadseregek létrehozását. A napóleoni háborúk utáni időben terjedőben volt Európaszerte az általános hadkötelezettség bevezetése, amely az egész népességre kiterjedő egységes nyilvántartási rendszer működtetését követelte meg. Ez a folyamat Magyar Királyságot sem kerülhette el, ezt a történelmi folyamatot tükrözi az 1790/91. évi XXXIII. törvénycikk "a népesség közigazgatási és katonai célból való összeírásáról." Az Országgyűlés a korábbi közigazgatási és katonai összeírás rendszerét eltörölte, és a hatékonyabb adatgyűjtés kidolgozásának érdekében felállított egy bizottságot, és előírta, hogy ennek a

bizottságnak az új népszámlálási rendszer tervét a legközelebb tartandó országgyűlésre be kell terjesztenie.

A XIX. századra a népesség-nyilvántartásnak két módszere alakult ki. Egyrészt a születésekről és a halálozásokról vezetett egyházi nyilvántartás, másrészt a központi állam által lefolytatott népszámlálás. Az állami népesség-nyilvántartási rendszer az egyházi nyilvántartási rendszerekből fejlődött ki. Ezt a folyamatot tükrözi a 1827. évi XXIII. törvénycikk, amely "az egyházi anyakönyveknek másod példányban a törvényhatóságok levéltárába helyezésétől s ott leendő őrzésétől" szól. Az Országgyűlés meghatározta azt is, hogy mi ezen törvényalkotás oka: "azon zavar megelőzése végett, mely a honlakosokat nemzetiségi leszármazásuk megállapításában, az egyházi anyakönyveknek valami véletlen eset miatt történő megsemmisülése vagy megromlása által fenyegethetné, határozatuk, hogy az illető lelképásztorok, minden valláskülönbség nélkül, a kereszteltek, házasulók és elhalálozottak anyakönyveit ezentúl két példányban szerkesszék; minden év végével pedig az illetékes törvényhatóság törvényes bizonyossága az egyik példányt vegye át, írja alá, s ilyenképpen az illető a törvényhatóság levéltárába vigye be. Az anyakönyvek ezen példányai azonban a törvényhatóságok levéltáraiban zár alatt tartassék, és ne legyen egyébként használható, csak akkor, midőn az egyházak birtokában levő anyakönyvi példányt valamely baleset következtében elveszne vagy megromlanék". E törvényi rendelkezéseket követően még több mint 60 évnek kellett még eltelnie ahhoz, hogy az állami anyakönyvezési rendszert felállítsák.

Az állami adatgyűjtés jogi szabályozására alkotta meg az Országgyűlés 1869-ben a népszámlálásról szóló törvénycikket. A népszámlálás során minden személy köteles volt adatokat szolgáltatni saját magáról, családtagjairól, hozzátartozóiról. A szolgáltatandó adatok köre nem volt egyértelműen és pontosan meghatározva a törvényben, csak az derül ki a jogszabályból, hogy a személyek mellett a lakhelyek és a hasznos állatok összeírására is sor került. A

törvénycikk az adatszolgáltatást kötelezővé tette, és a hatóságok számára bírság kiszabására adott lehetőséget, ha valaki kivonta magát a népszámlálás alól, vagy hamisan vallotta be adatait. A törvénycikk az adatvédelem kialakulása szempontjából két fontos elemet tartalmaz. Előírja, hogy a bírság kiszabása és behajtása közigazgatási úton történik, tehát a büntető hatalom eszközei nem alkalmazhatók a jogszabályt megsértő személlyel szemben. Ez az alapelv az állami adatgyűjtés és az adatvédelem összeütközésének fontos garanciális szabálya, vagyis az állami adatgyűjtést akadályozó személlyel szemben büntetőjogi eszközök és szankciók nem voltak alkalmazhatók. A másik fontos lépés az adatvédelem kialakulásának feltárása szempontjából, hogy a törvénycikk bírósági jogorvoslati lehetőséget<sup>140</sup> engedett meg a népszámlálás során hozott határozatok ellen, hogyha az vagy annak végrehajtása a polgárt jogaiban sértené. A döntés elleni jogorvoslati lehetőség abból a szempontból úttörő jellegű, hogy elsőként engedi meg a közigazgatási hatóságok döntéseinek bírósági felülvizsgálatát. A törvénycikk a népszámlálás részletszabályinak a kidolgozására belügyi, a földművelésügyi, az ipari és kereskedelmi minisztereket hatalmazta fel. A miniszterek közös rendeletükben<sup>141</sup> szabályozták a népszámlálás rendjét, és szükségesnek tartották lerögzíteni, hogy "ha olyan balítéletek merülnének fel, hogy a népszámlálás olyan célzatú puhatolás akarna lenni, mely új terhek kiszabására, adó felemelésére fogna vezetni, ezeket el kell oszlatni".

A népszámlálási rendszer nyugat-európai szintre történő fejlődése az 1890-es évben következett be. Ebben az időszakban végezték a magyar korona Országában egyedülállóként Európában az első jelentős nagyságrendű cigány összeírást. A közigazgatás fejlődése és az állami adatgyűjtés fontos lépésének tekinthető az állami anyakönyvezés 1895-ben történő bevezetése. A statisztikai rendszer fejlődése szempontjából alapvető jelentőségű volt a Magyar Királyi Központi Statisztikai Hivatalról szóló 1897. évi XXXV. törvény megalkotása. A törvénycikk továbbra is fenntartotta a kötelező

---

<sup>140</sup> 1869.évi. III. tc. 4§ A népszámlálás

<sup>141</sup> A belügyi és földművelés-, ipar- és kereskedelmi ügyi és honvédelmi miniszter 12876. sz. rendelete. Felhívás

adatszolgáltatást, és büntetni rendelte kihágásként, azt ha valaki "tudva hamis vagy valótlan statisztikai adatot vallott be, vagy a jelen törvény szerint beszolgáltatandó statisztikai adatok beszolgáltatását a szabályszerű felszólítás jogerőre emelkedése után megtagadta"<sup>142</sup>. A bírósági út a kihágások tekintetében jogorvoslati fórumként a polgárok számára elérhető volt. A törvénycikk fellépett az állami statisztikai célú adatgyűjtés akadályozása ellen is. "Aki a jelen törvény szerint beszolgáltatandó statisztikai adatok gyűjtését hamis hírek terjesztésével megnehezíti, avagy ez által a felvételnek az előszabott időben való végrehajtását megakadályozza; az ebből származó károkat, úgymint az esetleg szükségessé vált újabb felvételi vagy egyéb intézkedések költségeit viselni tartozik. " A bíróság volt jogosult a károkozási felelősség és az okozott károk mértékének megállapítására. A törvénycikk 15.§-a már a jövőbeni adatvédelem egyik legfontosabb alapelvét fektette le, amely a statisztikai adatszolgáltatás lelkét képezte<sup>143</sup>. A rendelkezés tiltja, hogy üzleti titkot képező információk a statisztikai rendszerből kiáramoljanak. "15.§ A központi statisztikai hivatal alkalmazottja vagy a jelen törvény értelmében szolgáltatandó statisztikai adatok gyűjtésével vagy feldolgozásával megbízott más egyén, ki ily minőségben tudomására jutott egyéni természetű statisztikai vagy egyéb adatoknak, akár alkalmazásának vagy megbízásának idejében, akár annak megszűnte után magánosoknak vagy oly hatóságoknak, melyek azok átvételére jogosítva nincsenek, elbeszél, kiszolgáltat, felmutat, megtekinteni enged vagy a jelen törvény ellenére köztudomásra juttat ... kihágást követ el"<sup>144</sup>. A törvényben nagyon korszerű módon fogalmazták meg, hogy az "egyéni természetű statisztikai bevallások és adatgyűjtés vagy ellenőrzés alkalmával a központi statisztikai hivatal tudomására jutott egyéb adatok az adók kivételénél alapul nem vehetők". A személyes adatok védelme érdekében a jogszabály kimondta, hogy "a központi statisztikai hivatal a statisztikai adatokat - címterek körébe tartozó közlemények és azon adatok

---

<sup>142</sup> 1897.évi XXXV 13§ A m. kir. központi statisztikai hivatalról

<sup>143</sup> LAKATOS Miklós, *Az adatvédelem jogi szabályozása a magyar népszámlálások tükrében* = Népszámlálások az ezredfordulón, szerk: KEPECS József, Budapest, KSH, 1998.

<sup>144</sup> 1897: XXXV. tv. 13 §

kivételével, amelyek törvény alapján vagy máskülönben úgyis nyilvánosságra hozatnak - nem egyenkint, hanem mindenkor csak területi vagy tárgy szerinti összefoglalásban teheti közzé". Ezzel főszabályként a jogszabály a személyes adatok önkényes nyilvánosságra hozatalát tiltotta meg. A személyes adatok nyilvánosságra hozatalára kivételesen törvény alapján volt lehetősége a hivatalnak. A mai napig fennálló joggyakorlat, hogy a népszámlálás szempontjából fontos adatvédelmi garanciákat a statisztikáról szóló törvény tartalmazza, a népszámlálást elrendelő törvény csak utal a statisztikai törvényben lefektetett garanciákra.

A statisztikáról szóló törvény megújítására az 1930-as években került sor, de az adatvédelmi szabályokat szinte érintetlenül átvették az új jogszabályba is. A hivatalos statisztikai szolgálatról szóló 1929. évi XIX. törvénycikk és a 4341/1930. ME sz. végrehajtási rendelet alapján tartották az 1930-as és az 1941-es népszámlálásokat. "Sajnos hiába volt az 1941.évi népszámlálás szokásosnak megfelelő jogi szabályozása és az adatvédelmi előírásoknak a miniszterelnöki rendeletben történő pontos megfogalmazása. A második világháború után nem a jogállamiság talaján álló politikai-társadalmi folyamatok nagy csapást mértek a statisztikai adatszolgáltatás hitelességére. .... Az elmúlt 130 éves időszakra visszatekintve csupán az 1941. évi népszámlálás esetében fordulhatott elő, hogy a Hivatal illetékességét messze meghaladó okok miatt nem tudott érvényt szerezni az adatvédelem garanciáinak és az információk bizalmas kezelésének elveinek. Az 1941. évi népszámlálás adatállományának nemzetiségekre és anyanyelvre vonatkozó információit felhasználták a magyarországi németek ellen 1945-ben, aminek következtében a német lakosság jelentős részét kitelepítették az ország területéről, a következő években hozott jogfosztó intézkedések végrehajtásával.<sup>145</sup>"

---

<sup>145</sup> LAKATOS Miklós, *Az adatvédelem jogi szabályozása a magyar népszámlálások tükrében* = Népszámlálások az ezredfordulón, szerk: KEPECS József, Budapest, KSH, 1998, 799.

A kommunista hatalomátvételt követően a kor szellemében született az 1952. évi VI. törvény, amely nem tartalmazta a korábbi népszámlálásokra vonatkozó adatvédelmi garanciákat. Az 1960-as népszámlálás szabályait a 1959. évi 30. törvényerejű rendelet állapította meg. Az adatgyűjtés érdekei miatt a jogszabály előírta, hogy a népszámlálás adatai hivatali titkot képeznek, amelyeket csak a Központi Statisztikai Hivatal használhat fel. Ez a megoldás a személyes adatok védelmét nem oldotta meg, mert az állami szektoron belül az adatáramlást nem korlátozta semmilyen jogi előírás, de a közérdekű információszerzés lehetőségeit teljesen kizárta. A 1952. évi VI. törvénynek a centralizációt szolgáló kötöttségeit lazította a 1973. évi V. törvény, amelybe visszaemeltek néhány az 1897. évi XXV. törvényből származó a magánszemélyeket védő biztosítékot, mint pl: a statisztikai adatszolgáltatást a magánszemélyre vonatkozóan csak törvény, törvényerejű rendelet, vagy minisztertanácsi rendelet állapíthatott meg. Az új jogszabály alapján korlátozták a magánszemélyek személyes adatainak közlését.

Az 1970-es években a közigazgatásért felelős szervek számára vonzónak tűnt az a megoldás, amely segítségével a különböző nyilvántartásokban tárolt adatokat össze lehet kapcsolni, és az egyedi adatokat különböző szempontok szerint lehet csoportosítani, ami technikai szempontból az állampolgárok, és állam illetve az állam szervei közötti adatáramlást jelentősen megkönnyíti. Az egységes központi népesség-nyilvántartási rendszer célból került bevezetésre a személyi szám az 1970-es években. A statisztikai rendszerből kifejlődött a népesség-nyilvántartás új rendszere, mivel a Központi Statisztikai Hivatal felügyelete alá tartozott az 1980-as évek végéig a Népesség-nyilvántartó Hivatal. A személyi szám bevezetését nem a privát szférába történő beavatkozás szándéka, hanem praktikus okok vezették<sup>146</sup>. A szocialista állam politikai elitje az uralmának fenntartása és a szocialista típusú "jóléti állam" megvalósítása érdekében, az összlakosságra kiterjedő adatbázisokkal kívánta a

---

<sup>146</sup> LAKATOS Miklós, *A személyiség joga, az állam működőképességének a joga*, Valóság, 1993/36, 3. sz. 5.

társadalmi transzferek szétesztását megoldani. A nagy adatbázisok összekapcsolása egyszerűbbé tette a közigazgatási szervek között folyó adatáramlást. Az az elképzelés, hogy az adatbázisok összekapcsolásával az adatkezelő a polgárra vonatkozó adatokból olyan következtetéseket vonhat le, amelyek a magánszférába való túlzott beavatkozáshoz vezetnek, a magyar jogi irodalomban csak a nyugat-európai politikai viták hatására jelentek meg.

## 7.2. A személyiségi jog és személyes adatok védelme

A magyar jogban 1978-ban a Ptk.. 83.§-ban került először kodifikálásra a személyiség jogi védelme körében a személyes adatok védelme: „a számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat”. Az állami adatkezelést a statisztikáról szóló 1973. évi V. törvény, az állami néesség-nyilvántartásról szóló 1986. évi 10 tvr. és a kapcsolódó végrehajtási jogszabályok rendezték azzal a céllal, hogy minden polgár könnyen azonosítható legyen, és az állampolgárról minél több információ álljon rendelkezésre az állami szervek számára, amely adatok akadálytalanul áramolhatnak az államigazgatási alrendszerei között. A fenti előírások nem biztosítottak hathatós garanciákat, amely alapján a Ptk.. személyiségvédelmi előírásai alkalmazhatók lettek volna.

Az információs önrendelkezés nem került rögzítésre az akkori Alkotmányban, így csak deklaráció szintjén maradt a Ptk.. előírása. Bár a magyar adatvédelmi törvény elfogadása előtt is léteztek számítógépes adatfeldolgozásra vonatkozó előírások, amelyek a szektorális szabályozás körében voltak fellelhetők, úgy mint a bűnügyi nyilvántartás, cégnyilvántartás, ingatlan-nyilvántartás, gépjármű-nyilvántartás, és a néesség nyilvántartás működtetésére vonatkozóan, amelyekre érvényesíteni lehetett volna a Ptk.. személyiség védelmi előírásait, de nincsen bizonyíték arra nézve, hogy a gyakorlatban a Ptk.. ezen személyiség védelmi előírása alkalmazásra került volna. A magyar



jogfelfogásban egyes szakírók az adatvédelmet a személyiségi jogok részének tekintették, amely az Európai Emberi Jogok Egyezményének 8. cikkében lefektetett magánélet tiszteletben tartásához való jogból ered<sup>147</sup>. A Ptk.. 83.§ (1) és (3) bekezdéseit a személyiség védelmi előírásai között találjuk azt a kötelezettséget, amely kimondja, hogy a számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat. A nyilvántartott adatról tájékoztatást az érintett személyen kívül csak az arra jogosult szervnek, vagy személynek lehet adni. Az érintett személy tájékoztatását csak abban az esetben lehet megtagadni, ha ennek teljesítése állami vagy közbiztonsági érdeket sértene. A Ptk.. lefektette az érintett adathelyesbítési jogát arra az esetre, ha valamely nyilvántartásban szereplő adat nem lenne valódi. A személyes adatok és a személyiségvédelmi jog kapcsolatának részletesebb bemutatására a szektorális adatvédelemi kérdések között kerül sor.

### 7.3. Az információs törvény tervezetéről

Magyarországon az informatikai fejlődéssel párhuzamosan elkezdődött az 1980-as évektől az informatikai törvény előkészítése, amelyhez lendületet az Európa Tanács 1981-es adatvédelmi egyezménye adott. Az 1980-as évek végén a Központi Statisztikai Hivatal számítástechnika alkalmazási főosztálya dolgozta ki az "információs" törvény tervezetét. A törvény szükségességét felvázoló tanulmány szerint a "XX. század utolsó évtizedeinek egyik általános érvényű jelensége, hogy az állam és gazdaság működéséhez, a társadalmi tevékenységek tervezéséhez és szervezéséhez egyre több információra van szükség. A nagytömegű információt viszont mind kevésbé lehetséges hagyományos módszerekkel kezelni, ezért növekszik az informatikai jelentősége, ami azonban bizonyos potenciális veszélyeket is hordoz magában."<sup>148</sup> A törvény megalkotásának indokként a műszaki fejlődés

---

<sup>147</sup> PETRIK Ferenc, *A személyiség jogi védelme*, Budapest, Közgazdasági és Jogi Könyvkiadó, 1992, 167

<sup>148</sup> *Az információs törvényről*, Statisztikai Közlemények, 1990, 348.

kihívása szerepelt. Az indoklás meghatározza az alapkonfliktust is, amely feloldása az adatvédelem feladata. "Az államoknak általánosságban és egyes állami szerveknek különösen is fontos érdeke fűződik ahhoz, hogy ha már igen nagy költségek árán kialakítanak és naprakész állapotban tartanak információ-rendszereket, akkor azok tartalma minél szélesebb körben felhasználható legyen a legkülönbözőbb célokra. Ezzel ellentétben áll az adatalányok nem csupán a természetes személyeknek, hanem a jogi személyeknek is azaz érdeke, hogy a magánélet szűkebb szférájába, vagy az üzleti titok fogalmi körébe tartozó adataik ne kerülhessenek külső szervek nyilvántartásába, vagy ha ez mindenképpen elkerülhetetlen, hatékony garanciák előzzék meg az adatoknak illetékteleneknek kezébe jutását. Ugyancsak alapvető érdeke az adatalányoknak, hogy a rájuk vonatkozó információkat csak az általuk ismert célra használhassák fel<sup>149</sup>. A törvénytervezet tárgyi hatályát is meghatározták, mely szerint az információs törvénynek a kézi és a gépi adatfeldolgozási eljárásokra is ki kell terjednie. A tervezet meghatározta a törvény elveit is:

**Társadalmi indokoltság:** adatot felvenni csak akkor szabad, ha arra a társadalom kisebb nagyobb csoportjainak tevékenységének szabályozásához elengedhetetlenül szükség van;

**Személyes részvétel:** Az érintettek így tudják, hogy ki, milyen célra, milyen okból és milyen felhatalmazás alapján veszi fel adataikat, és azokat mire-meddig használja.

**Adatok helyessége:** az adatoknak a valóságos helyzetet kell tükrözniük.

**Célhoz kötöttség:** a következőket érvényesítése szavatolja, hogy adatokat csak akkor lehessen kezelni, ha azt egy vagy több társadalmilag indokolható cél szükségessé teszi.

**Adatfelvétel korlátozottsága:** az érintettek és adataik körének pontos, célhoz illő meghatározását jelenti, vagyis csak azon személyektől és csak olyan adatokat szabad felvenni, akiket, és amelyeket a meghatározott cél elérése érdekében a felvételbe be kell vonni.

---

<sup>149</sup> A 1990-es törvénytervezet indoklása alapul szolgált az 1992.évi.LXIII tv. általános indoklásához

**Adatátadás korlátozottsága:** ha az adatátadó a személyes részvételt nem tudja érvényesíteni, akkor az adatátadás csak akkor történhet, ha az adatátvevő adatkezelése is a korábbi célhoz igazodik.

**Időbeli korlát:** az adatokat, ha csak más érdek, mint tudományos, közbiztonsági, nemzetbiztonsági érdek nem indokolja, csak addig szabad megőrizni, ameddig erre a meghatározott cél elérése érdekében feltétlenül szükség van.

**Nyíltság:** az adatkezelőnek az érintett számára biztosítani kell, hogy kontroll jogait gyakorolhassa, ha azok felvételére a személyes részvétele nélkül került sor.

**Adatkezelő felelőssége:** az adatkezelő polgári és büntetőjogi felelősséget is visel azért, hogy az adatokkal kapcsolatos előírásokat betartsa.

**Adatbiztonság:** az adatkezelőnek gondoskodnia kell, hogy az adatok illetéktelenek kezébe ne kerüljenek. Minden technikai és műszaki megoldást meg kell tennie az adatok védelme érdekében.

#### 7.4. Személyes adatok védelme az (új 1989-es) Alkotmányban

Az Alkotmány rendelkezéseinek kimunkálása, és a békés politikai rendszerváltást elősegítő törvények kidolgozása a Nemzeti Kerekasztal többszintű tárgyalás sorozatain alakult ki. A háromszintű egyeztető fórumokon a demokratikus államrend működése szempontjából lényeges kérdések kerültek megvitatásra. Az érdemi döntéseket a középszintű tárgyalásokon vitatták meg. A tárgyalók munkáját munkabizottságok segítették elő. Az I/5. sz. munkabizottság foglalkozott a tájékoztatás, az információk kérdésével, illetve az új tájékoztatási törvény megalkotásának ügyével. Az I/5. bizottságra hárult az MSZMP tájékoztatási monopóliuma áttörésének szakmai előkészítése, a tájékoztatási fórumokhoz történő hozzáférés és a tárgyalások nyilvánosságának előkészítése, illetve az új sajtótörvény alapelveinek a meghatározása. A munkabizottság foglalkozott azzal a kérdéssel is, hogy

miképpen lehet a tárgyalások eredményét az országos és a megyei lapokban közreadni. A napi politikai kérdések mellett - amelyek azonnali cselekvést igényeltek - a munkabizottság foglalkozott azzal a kérdéssel is, hogy hogyan lehetne az elkobzott sajtótermékeket visszaszereznie az ellenzéknek. Az I/5. munkabizottság ellenzéki képviselőjeként Sólyom László szorgalmazta, hogy a bizottságnak elsősorban hosszútávra szóló demokratikus törvényhozást kellene szem előtt tartania, ezért a bizottságnak az információszolgáltatásról és az adatvédelmi szabályozásról szóló törvény mielőbbi megalkotásával kellene foglalkoznia.<sup>150</sup> Sólyom László az Ellenzéki Kerekasztal résztvevői számára készített jelentésében már a tárgyalások közepén jelezte, hogy az informatikáról szóló törvény előkészítéséhez szükséges egyeztetések hiánya miatt nem lesz mód egy informatikai törvény elfogadására.

A Nemzeti Kerekasztal tárgyalásokat lezáró megállapodás harmadik részében a felek rögzítették, hogy a tárgyalások eddig elért eredményére alapozva folytatni kell a munkát a békés átmenetet érintő, még nyitott kérdések rendezése érdekében. Az aláírók abban megállapodtak, hogy a köztársasági elnök választásának rendje, a választási etikai kódex, a választások nyilvánosságának szabályozása, az új tájékoztatási törvény, az informatikai törvény, a közszolgálati törvény, a munkásőrség feloszlata, és a politikai kérdések erőszakos megakadályozása érdekében a munkabizottságok az egyeztetéseket tovább folytatják.<sup>151</sup> A megállapodás ezen része hamar értelmét veszítette, mert az ellenzék részéről 1989. szeptember 18. után már nem vettek részt szakértők a tárgyalásokon, mivel maga az Ellenzéki Kerekasztal is felbomlott. A megállapodásban rögzített témakörök törvényi szintű szabályozása az 1990-ben demokratikusan megválasztott Országgyűlésre maradt.

---

<sup>150</sup> *A rendszerváltás forгатókönyve* : kerekasztal-tárgyalások 1989-ben : dokumentumok, szerk. ELBERT Márta, [et al.], VI, Budapest, Új Mandátum Kiadó, 2000, 474.

<sup>151</sup> U.O. 518.

A Nemzeti Kerekasztal tárgyalásokon az Alkotmány módosításának leglényegesebb kérdéseivel az I/1-es munkabizottság foglalkozott. Az alapjogokkal kapcsolatos Alkotmány módosítás munkaanyagát<sup>152</sup> az Igazságügyi Minisztérium dolgozta ki, figyelembe véve a Polgári és Politikai Jogok Nemzetközi Egyezségokmányát, illetve az emberi jogok és alapvető szabadságok védelméről szóló európai egyezségokmány rendelkezéseit. Az új Alkotmány VII. fejezetét, közöttük a személyes adatok védelméhez való jogot a Nemzeti Kerekasztal tárgyalások utolsó munkabizottsági fordulóján fogadták el. A szocialista Alkotmányt módosító 1989. évi XXXI. törvényben a személyes adatok védelmére vonatkozó szakasz az Igazságügy Minisztérium által előterjesztett, és a Nemzeti Kerekasztal bizottságai által jóváhagyott formában került megalkotásra. A 1989. évi XXXI. törvény parlamenti vitája során az eredeti javaslatból hiányzó joggal, a közérdekű adatokhoz való hozzáférés jogával az alapjogi fejezetet kiegészítették a törvényalkotók. Az 1990. májusában megválasztott Országgyűlés Antall-Tölgyessy paktum alapján az 1990. évi XL. törvény 39. §-ával beiktatta a (2) bekezdést, mivel az alkotmányerejű törvény fogalma törlésre került az Alkotmányból:

**59. § (1)** A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.

(2) A személyes adatok védelméről szóló törvény elfogadásához a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges.

Majtényi László szerint a személyes adatok védelmére vonatkozó törvénycikk fejezetten szerencsétlen megfogalmazására sikeredett. ... „Téves az Alkotmány 59. §-ának megfogalmazása, mert az adatvédelemre irányuló jogot egy némileg ötletszerűen nevesített személyiségi jogi felsorolás végére biggyeszti. Ennél nagyobb hiba, hogy protektív jogként, az állam által a

---

<sup>152</sup> *Egy alkotmány-előkészítés dokumentumai: kísérlet Magyarország új Alkotmányának megalkotására, 1988-1990*, szerk. KILÉNYI Géza, Budapest, Magyar Tudományos Akadémia Államtudományi Kutatóközpont, 1991.

polgároknak nyújtott védelemként fogalmazza meg, nem pedig információs önrendelkezési jogként<sup>153</sup>. A személyes adatok védelmének első hazai jogtudományi<sup>154</sup> megfogalmazására a 80-as évek közepén személyiségi jogok védelmének témakörében került sor, amely jognak a jogtudományi besorolását megerősítette a 90-es évek elején a személyiségi jogok védelméről kiadott kézikönyv.<sup>155</sup> E jogtudományi rendszerezés is befolyásolta a személyes adatok védelméhez fűződő jog alkotmányos megfogalmazását, amely értelmezést maga a személyes adatok védelméről szóló törvényjavaslatot beterjesztő igazságügyi miniszter is élt, mikor a privacyt biztosító magyar törvény zárószavazására<sup>156</sup> került sor. A személyes adatok védelme és a személyiségi jogok közötti kapcsolatot erősíti, hogy az Avtv.. megalkotásakor a Ptk.. 83.§-a is módosításra került, mely szerint a számítógéppel vagy más módon történő adatkezelés és adatfeldolgozás a személyhez fűződő jogokat nem sértheti.

#### 7.5. Az Alkotmánybíróság a személyes adatok védelmezője

Az információs törvény megalkotása késett, de az információs szabadságjogok alkotmányos védelme már 1991-ben nem tűrhetett halasztást. A demokratikus jogállami követelményeknek megfelelő új Alkotmánnyal ellentétesnek minősítette az Alkotmánybíróság az állami adatkezelés számos előírását, mert azok szükségtelenül és aránytalanul korlátozták a polgárok információs önrendelkezési jogát, illetve egyáltalán nem szolgálták a személyes adatok védelmét. A korszerű magyar adatvédelem alapjainak a lerakása és dogmatikai rendszerének kialakítása a 15/1991. (IV.13) határozatban történt meg. „... A személyi szám határozat közvetlen jelentésében az adatvédelemnek kissé

---

<sup>153</sup> MAJTÉNYI László, *Az adatvédelem és az információs szabadság az Alkotmányban*, Acta Humana 1995, 18/19, 96.

<sup>154</sup> SÓLYOM László, *A személyiségi jogok elmélete*, Budapest, Közgazd. és Jogi Kvk., 1983

<sup>155</sup> PETRIK, i.m.,

<sup>156</sup> Országgyűlés Jegyzőkönyve Az Országgyűlés 1992. évi őszi ülészaka október 26-27-28-i ülésének jegyzőkönyve 20634. old

ismétlés, ódivatú felfogását képviselte talán már létrejöttkor is, az újabb fejlemények mégsem teszik a határozatot múzeumi darabbá. Maradéktalanul időszerűek lesznek mindig a célhoz kötöttségről, a készletező adatgyűjtésről, az információs hatalommegosztásról, az adattovábbításról, a nyilvánosságra hozatalról, az adatbiztonságról, és főként a polgárok önrendelkezési jogáról mondtak.<sup>157</sup>»

A magyar adatvédelem kialakulása során a kontinentális fejlődés útját követte, amelynek mozgató rugója az állami hatalommal szemben fennálló bizalmatlanság, amely a hatványozottan jelent meg egy olyan politikai rendszerben, amely a politikai jogok korlátozására, a titkolózásra építve és a társadalom manipulálásának sokrétű eszköztársát felhasználva működtette az államhatalmat.

Az Alkotmánybíróság 15/1991. (IV.13.) AB határozata az adatkezelés addigi rendjét gyökeresen felforgatta, mert az Európa Tanács Adatvédelmi Egyezménye és a német BVerfG népszámlálási ítéletében megfogalmazottakra építve a magyar jogi gondolkodásba bevezette az információs önrendelkezési jogot, és az információs hatalommegosztás elvét. Az Országgyűlés az 1980-as évek végén megindult informatikai törvény előkészítő munkáinak alapján 1992-ben október 27-én elfogadta a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt, amelynek a közérdekű adatok nyilvánosságáról szóló fejezete 1992 decemberében, a személyes adatok védelmére vonatkozó fejezete 1993. májusában lépett hatályba.

Az Európa Tanács Adatvédelmi Egyezményével összhangban álló magyar adatvédelmi törvény<sup>158</sup> (Avtv.) kellő garanciát biztosít a személyes adatok

---

<sup>157</sup> MAJTÉNYI László, *Az "első" Alkotmánybíróság és az információs szabadságjogok = Alkotmánybírósoklás tíz éve*, Budapest, 2000

<sup>158</sup> 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

védelmére. A törvény újdonsága, hogy Európában elsőként együtt szabályozza az információs önrendelkezést, és a közérdekű adatok megismerésének jogaként az információs szabadságot. Az alapjogok érvényesülése érdekében az információs szabadságjogok felügyeletére külön parlamenti biztosi intézményt állított fel az Országgyűlés. "A magyar megoldás komoly intellektuális izgalmat visz a személyes adatok védelmének gyakorlatába, mert a jogalkalmazót - az adatvédelmi biztost - ez a kettős szerepe folyton arra kényszeríti, hogy keresse az egyensúlyt vagy talán még pontosabban a gyakran keskeny ösvényt a két gyakorta ellentétesnek látszó és egymás kölcsönösen korlátozó szabadságjog között. Ez mind a sajtószabadság érvényesítése, mind pedig a közhatalmat gyakorlók és egyéb közszereplők korlátozott magánélete körének meghatározása során különleges feladatot jelent. Továbbá az adatvédelmi biztos és a sajtó kapcsolatában távolról sem mindegy, hogy a biztos a magánélet védelmezőjeként csak, mint a sajtószabadság korlátozója lép-e fel, vagy információs szabadság-biztosként az állam titkolózási hajlandóságával szemben a sajtószabadság védelmezőjének a szerepét is betölti."<sup>159</sup>

#### 7.6. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény parlamenti vitája

Az Avtv.. megalkotásának indokaként<sup>160</sup> az az érdek összeütközés szolgált, ami a XX. század utolsó évtizedeitől kezdve általános jelenség, vagyis az állam és a gazdaság működéséhez, társadalmi tevékenységek tervezéséhez és szervezéséhez egyre több információra van szüksége. Az államnak és az egyes állami szervezeteknek különösen fontos érdeke fűződik ahhoz, hogy ha már nagy költségek árán kialakítanak és naprakész állapotban tartanak információrendszereket, akkor azok adattartama minél szélesebb körben

---

<sup>159</sup> MAJTÉNY, *Az adatvédelem Magyarországon, ...i.m.,*

<sup>160</sup> 1992: LXIII. tv



felhasználható legyen a legkülönbözőbb célokra. Ezzel ellentétben áll az adatalanyoknak és nem csupán az állampolgároknak az érdeke, hogy bizonyos, a magánélet szűkebb szférájába vagy az üzleti titok fogalmi körébe tartozó adataik egyáltalán ne kerülhessenek külső szervek nyilvántartásaiba, vagy ha ez elkerülhetetlen, hatékony garanciák előzzék meg az említett adatoknak illetéktelen kezekbe kerülését. A különböző érdekek összeütközése számos jogi problémát vett fel, gyakori a jogbizonytalanság, főleg annak megítélésében, hogy meglevő adatállományokhoz, kik, mely szervek, milyen terjedelemben férhetnek hozzá. A jogbizonytalanság megszüntetése érdekében terjesztett be az igazságügy miniszter a törvényjavaslatot, amely igazodik a nemzetközi mércékhez, többek között az Európa Tanács Adatvédelmi Egyezményében foglaltakhoz.

Az Országgyűlés több ülészakon keresztül tárgyalta a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvényjavaslatot (továbbiakban: javaslat). A korabeli országgyűlési jegyzőkönyvek alapján kitűnik, hogy ebben az időszakban az adatvédelem törvényi szabályozása másodlagos problémának tűnt ahhoz viszonyítva, hogy az országnak gazdasági válsággal kellett megküzdenie. A kormány parlamenti támogatottsága a sorozatos MDF képviselő kilépések és az FKGP frakció kettészakadása miatt bizonytalanná vált. Tisztázatlanok voltak a médiaviszonyok, folyt az „első médiaháború”. A kommunista-szocialista korszak áldozatai érdekében a kormány igazságtételt kívánt végrehajtani, és célként tűzte ki a büntetőjog eszközeivel történő állami fellépést. A mezőgazdaság talpon tartása érdekében rendezni kellett a földtulajdonlás, és a szövetkezetek további sorsát. A személyes adatok védelméről szóló törvényjavaslat tárgyalását követően az Országgyűlés napirendjére tűzte az állampolgári jogok biztosának jogállásáról szóló törvényt, és betervezte a kormány a nemzeti és etnikai kisebbségek jogait védő törvényjavaslatot is. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvényjavaslatot és a benyújtott módosító indítványokat az alkotmányügyi, az emberi jogi, és a

nemzetbiztonsági bizottság tárgyalta meg. Az alkotmányügyi bizottság állásfoglalása szerint a javaslat 31.§ és 32.§-a kivételével, amelyek egyszerű többséggel is elfogadhatók, a jelen lévő képviselők kétharmadának többségi szavazatát igénylik.

A törvényjavaslat alapelveiként az előterjesztő a személyes részvétel, az érintettek és adatfajták korlátozottságának elvét, a célhoz kötött adatkezelés elvét, a továbbadás korlátozását, az adathelyesség követelményét, az időbeni korlátozást, a biztonsági óvintézkedések alkalmazását és a felelősség elvét határozta meg. A javaslat megtárgyalása során az ellenzéki képviselők több módosító indítványt nyújtottak be, amelyek közül a kormány támogatta azokat, amelyek a javaslatban megfogalmazott alapelveket erősítik, illetve a fogalmakat pontosítják. A KDNP javaslatára került a különleges adatok fogalma kettéválasztva, így a fajra, eredetre, nemzeti vagy nemzetiségi hovatartozásra, a politikai véleményre, a pártállásra, a vallásos vagy más meggyőződésre vonatkozó adatok kiemeltbb védelmet kaptak. Az SZDSZ javaslatát az adatkezelés minőségére és feltételeinek meghatározására vonatkozóan elfogadta a kormány, de javaslatát a vitatott adat fogalmára vonatkozóan nem támogatta, mivel szerinte a bírósági út kellő garanciát biztosít akkor, ha az érintett személy megkérdőjelezné a rá vonatkozó adat helyességét. A kormány a közérdekű adatok nyilvánosságára vonatkozó indítványokat, amelyek a gyakorlati megvalósulást segítik, és pontosítják a törvényjavaslat rendelkezéseit támogatta, de elvetette azokat az indítványokat, amelyek a kormányzati szervek munkáját, vagy a közigazgatási feladatok ellátását akadályozzák. „A közérdekű adatokhoz való hozzáférés nagyon lényeges jog, ennek szabályozása komoly feladat. Meg kell találni a megfelelő egyensúlyt az információkhoz való szabad hozzájutás és az állami, valamint az önkormányzati szervek zavartalan munkájának biztosítása között.<sup>161</sup>” A javaslat elfogadásához az Alkotmány 59.§ (2) bekezdése szerint a jelen lévő

---

<sup>161</sup> *Országgyűlés Jegyzőkönyve*, Az Országgyűlés 1992. évi őszi ülészsaka október 26-27-28-i ülésének jegyzőkönyve, 20636.

országgyűlési képviselők kétharmadának igen szavazata szükséges, ezért a Kormány széleskörű konszenzus létrehozására volt kötelezett a törvényjavaslat elfogadása érdekében.

#### 7.7. A magyar adatvédelmi törvény rendszere

A korábbiakban említésre került, hogy az adatvédelmi törvény címen emlegetett törvény két alkotmányos jog gyakorlati érvényesítését biztosítja, egyrészt az Alkotmány 59.§-ában lefektetett személyes adatok védelméhez fűződő jogot, másrészt a 61.§-ban rögzített információszabadság jogát, másféle elnevezés szerint a közérdekű adatok megismeréséhez való jogot. A két alkotmányos jog több esetben egymás korlátjaként jelent meg a joggyakorlatban, ezért újdonságnak számított a 90-es évek elején e két jognak egy törvényben történő szabályozása, és az unikum jelleg, hogy a két alkotmányos jog védelmére egy biztost állít a törvényhozó hatalom. A dolgozat témáját tekintve elsősorban a személyes adatok védelmére vonatkozó jog hazai szabályozásának a fejlődését mutatom be, de figyelembe kell venni e jog információszabadsággal való kapcsolatát is.

Az Avtv.. rendszerét tekintve általános és különös részből áll. Az általános rész négy fejezetből áll, amelynek első része a törvény célját és a személyes adatokkal kapcsolatos értelmező rendelkezéseket foglalja össze. A második fejezet a személyes adatok védelmére vonatkozó adatkezelési szabályokat, az adatkezelés célhoz kötöttségére, az adatok minőségére irányadó szabályokat foglalja össze amellet, hogy rendelkezik az adattovábbítás és adatkezelés összekapcsolására, illetve a külföldre irányuló adattovábbításra vonatkozó szabályokról. Az általános rész második fejezetében kerültek szabályozásra az adatbirtokosok jogainak érvényesítésére, és védelmére vonatkozó szabályok, továbbá itt került lefektetésre a bírósági jogvédelem lehetősége amellet, hogy a jogsértő adatkezelés miatt bekövetett károkozás felelősségi szabályai is

törvényi szabályozást nyertek. Az általános rész harmadik fejezete foglalkozik a közérdekű adatok nyilvánosságának kérdésével, míg a negyedik fejezetben az adatvédelmi biztosra és az adatvédelmi nyilvántartásra vonatkozó szabályok kerültek elfogadásra.

A törvény a különleges rendelkezések cím alatt az V. fejezet keretében a személyes adatok kezelésének egyes szektorális eljárási és anyagi kérdéseit kellene rendeznie, de sajnos csak a tudományos kutatás céljára felvett adatkezelésre vonatkozóan ad törvényi eligazodást a jogszabály. Az Avtv.. egyik nagy hiányossága, hogy a megalkotását követő 15 évben a szektorális adatkezelésekre vonatkozó szabályait nem fejlesztették tovább. Ugyan születtek a szektorális adatkezelést szabályozó jogszabályok, így mint a kutatást és közvetlen üzletszerzés célját szolgáló 1995. évi CXIX. tv. más néven direkt marketing törvény, vagy az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről szóló 1997. évi XLVII. törvény, vagy az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, de ezen jogszabályok összhangja az Avtv.. előírásával nem teljes mértékben lett megoldva.

#### 7.8. Az adatvédelmi törvény célja és fogalmi rendszere

A jogalkotó a törvény 1.§-ában az Avtv.. céljaként azt határozta meg, hogy a személyes adatával mindenki maga rendelkezzen kivéve, ha az Avtv..-ben meghatározott jogszabály e jog alól kivételt nem enged. A zárószavazáson Vastagh Pál azt javasolta, hogy az adatvédelmi törvény által meghatározott jogviszonyokat kizárólag törvény szabályozhassa, de ezt a többség elvetette. Így az Avtv.. 1§.(1) bekezdése alapján a törvényben meghatározott témában bármely szintű jogszabály kivételt biztosíthat az információs önrendelkezési jog lényege alól. A törvény 1.§ (2) bekezdés a törvény kogens jellegét mondja

ki, amely szerint az Avtv..-től eltérni csak akkor lehet, ha azt e törvény kifejezetten megengedi. A törvény 1.§ (3) bekezdését, mely szerint az Avtv. szerint megengedett kivételt csak meghatározott adatfajtákra és adatkezelőre együttesen lehessen megállapítani Tirts Tamás ellenzéki képviselő indítványozta, amelyet a kormány támogatott és az Országgyűlés elfogadott.

A törvény 2.§-a az értelmező rendelkezéseket tartalmazza, meghatározva a személyes adat, a különleges adat, az adatkezelés, az adattovábbítás, a nyilvánosságra hozatal, az adatkezelő, és az adattörlés fogalmát. A 2.§ 1. pontja szerint személyes adatnak minősül egy meghatározott természetes személlyel kapcsolatba hozható adat, az adatból az érintettre levonható következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolat az érintettel helyreállítható. Az országgyűlési tárgyalás során vita alakult ki a képviselők között a különleges adat fogalmának meghatározása körül, a 2. pont b) bekezdésre vonatkozóan több szövegváltozat készült, de a kormány a KDNP javaslatát fogadta el, mely két kategóriára bontotta a különleges adatok körét. Mészáros István László képviselő indítványozta, hogy egyes tudományos kutatások céljait szolgáló betekintések is a különleges adatok fogalma alá tartozzanak, de az Országgyűlés nem fogadta el a módosítást. Az Avtv.. 2.§ 2. a) pontja szerint különleges adatnak minősül a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre vonatkozó adat. A 2.§ 2.b) pont szerint minősül különleges adatnak az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett életre vonatkozó adatok.

Az Avtv.. meghatározza az adatkezelés fogalmát, mely szerint az alkalmazott eljárástól függetlenül személyes adatok felvétele, tárolása, feldolgozása, hasznosítása, (ideértve a továbbítást, és a nyilvánosságra hozatalt) továbbá adatkezelésnek számít az adatok megváltoztatása, és további felhasználásuknak a megakadályozása is. Az adatkezelőnek az a személy minősül, aki ezen

tevékenységeket maga végzi, vagy mással végezteti. Az adattovábbítás és a nyilvánosságra hozatal fogalmai közötti különbséget a jogalkotó abban határozta el, hogy az adattovábbításnak számít, ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszi, míg nyilvánosságra hozatalnak minősül az, ha az adatot bárki számára hozzáférhetővé teszik. Mészáros István László javaslatára került a törvényszövegbe az adattörlesztés fogalma, amely az adatok felismerhetetlenné tétele olyan módon, hogy a helyreállításuk nem lehetséges.

#### 7.9. Az adatkezelés hazai szabályai (1992-es állapot)

A Avtv.. 3.§ (1) bekezdése alapján személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárult, vagy azt a törvény vagy törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzati rendelet elrendeli. Különleges adat akkor kezelhető, ha ahhoz az érintett írásban hozzájárul, vagy a 2.§ 2. a.) pontban foglalt adatok esetén az adatkezelés nemzetközi egyezményen alapul, vagy az Alkotmányban biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében törvény elrendeli. A 2.§ 2.a) pontban nem meghatározott különleges adat egyéb esetekben akkor kezelhető, ha azt törvény elrendeli. Az SZDSZ több javaslata az adatgyűjtés kezelésre irányult, így az SZDSZ ki akarta egészíteni a 3.§ (2) bekezdés b) pontját azzal, hogy a személyes adat akkor kezelhető, ha a felhatalmazott az adatgyűjtés céljának, és az adatok körének pontos meghatározásával elrendeli, de a kormány ezt nem támogatta. A különleges adatok kezelésére vonatkozóan javasolta az SZDSZ a cél és a gyűjtendő adatok körének előzetes meghatározását, a kormány elvetette, de garanciális szabályként lefektette, hogy különleges adat akkor kezelhető, ha az érintett ahhoz írásban hozzájárul, vagy ha azt törvény elrendeli. A különleges adatok kezelésére vonatkozóan Szelényi Zsuzsa javasolta, hogy a különleges adatok közül a faji eredetre, a politikai véleményre vagy pártállásra, vallásos meggyőződésre és a szexuális életre vonatkozó adatok statisztikai célból

gyűjthetők és névtelenül kezelhetők legyenek, de ezt az indítványt sem a bizottságok, és sem a kormány nem támogatta.

Az Avtv.. 3.§ (3) bekezdése szerint törvény közérdekből – az adatok körének kifejezett megjelölésével- elrendelheti a személyes adat nyilvánosságra hozatalát. Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett hozzájárulása, különleges adat esetén írásbeli hozzájárulása szükséges. Az Alkotmányügyi Bizottság indítványozta, hogy az Avtv.. 3.§ (3) bekezdésébe kerüljön bele, hogy kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg. Az Országgyűlés a 3.§ (3) bekezdését az Alkotmányjogi Bizottság javaslatára kiegészítette.

Az érintett hozzájárulásával kapcsolatosan a törvény előírja, hogy azt megadottnak kell tekinteni az érintett közszereplése során általa közölt vagy nyilvánosságra hozatal céljából átadott adatok tekintetében. A hozzájárulás tekintetében további eligazodást ad a 3.§ (5) bekezdése, mely szerint az érintett kérelmére indult eljárásban a szükséges adatainak kezelésére való hozzájárulást vélelmezni kell. A jogszabály ezen előírására az érintettet fel kell hívni. A személyes adatok nyilvánosságra hozatalának korlátjaként Vastagh Pál azt javasolta, hogy a törvény a bűnmegelőzés, a bűnüldözés, valamint az állami pénzügyek érdekeire nézve korlátozza a személyes adat nyilvánosságra hozatalát, az indítványt azonban a kormánytöbbség nem támogatta. Az Igazságügyi Minisztérium eredeti előterjesztésében a személyes adatok védelme a jogi személyekre, és a jogi személyiség nélküli szervezetekre is kiterjedt volna, de ezt a kiterjesztést biztosító 4.§ (2) bekezdést végül kihagyták a jogalkotók a törvényből.

Az ellenzéki képviselők a célhoz kötöttség elvét mindenképp le kívánták horgonyozni a törvényjavaslatban, ezért azt javasolta Tirts Tamás, hogy a személyes adatot csak pontosan meghatározott és jogszerű, az adatvédelmi nyilvántartásba bejegyzett célból szabad kezelni. Az Alkotmányügyi bizottság

a szövegjavaslatból csak azt támogatta, hogy az adatkezelésnek minden szakaszában meg kell felelnie a bejelentett célnak. Az Avtv.. 5.§ (1) bekezdésének végső szövege szerint személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Az SZDSZ javaslatára került az 5.§ (2) bekezdés elfogadásra, mely szerint csak olyan személyes adat kezelhető, amely az adatkezelés céljainak megvalósulásához elengedhetetlen, a cél elérésére alkalmas a cél megvalósulásához szükséges mértékben és ideig. Az adatalany tájékoztatása kérdésében Mészáros István László azt javasolta, hogy amellet, hogy az érintettel előzetesen közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező, illetve tájékoztatni kell az adatkezelés céljáról, és az adatkezelő személyéről, arról is tájékoztatni kellene az érintettet, hogy az adatot kinek továbbítják, és az adatkezelés milyen várható hatással lesz a jogalanyra. A 6.§ (2) bekezdését kiegészítő javaslatot sem a bizottságok, sem az igazságügy miniszter nem támogatta. Az érintettek tájékoztatására vonatkozóan az Országgyűlés a 6.§ (2) bekezdésében elfogadta, hogy az érintettek tájékoztatni kell az adatkezelés céljáról, és arról, hogy ki az adatkezelő. A tájékoztatás megtörténik azzal is, hogyha jogszabály rendelkezik a már létező adatkezelésből származó adat továbbításáról vagy összekapcsolásáról.

Az adatok minőségére vonatkozó 7.§ (1) szakasz szinte szóról szóra megegyezik az egyének védelméről a személyes adatok gépi feldolgozása során elfogadott 1981-es Európa tanácsi egyezmény 5. cikkével. Az Avtv.. 7.§ (1) bekezdése szerint személyes adatok kezelésének meg kell felelniük a tisztességesség és törvényesség követelményének. Az adatoknak pontosaknak, teljeseeknek, időszerűnek kell lenniük. Az adatok tárolásának módjának alkalmasnak kell lennie arra, hogy az érintettek csak a tárolás céljához szükséges ideig lehessen azonosítani. Az Avtv.. 7.§ (2) bekezdése kimondja, hogy korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos.



Az adattovábbítás és az adatkezelések összekapcsolására vonatkozóan az Avtv.. a 8.§-ban kimondja, hogy az adatok akkor továbbíthatók, valamint különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy a törvény megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Az ellenzéki képviselők javaslatára az Avtv.. kiegészítése elfogadásra került, mely szerint az (1) bekezdést kell alkalmazni ugyanazon adatkezelő, valamint az állami és az önkormányzati szervek által kezelt adatok összekapcsolására is.

A külföldre történő adattovábbítással kapcsolatosan az Avtv. 9.§-a szerint a személyes adat az országból az adathordozótól vagy az adatátvitel módjától függetlenül külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve, hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek. Az Avtv.. ezen szakasza az informatikai fejlődéssel, különösen az internet elterjedésével, az integrálódó gazdasági viszonyok közepette hamar gátló tényező vált.

Az Avtv.. 10.§-ában az adatbiztonság követelményeit határozta meg a jogalkotó, mely szerint az adatkezelő köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az Avtv.. valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatbiztonság fokozottabb védelme érdekében Vastagh Pál azt javasolta, hogy törvény sem biztosíthatson kivételt az adatkezelőnek azon kötelezettsége alól, hogy ő gondoskodni köteles az általa kezelt adatok biztonságosságáról és védelméről. A 10.§ (2) bekezdése előírja az adatkezelő részére, hogy védeni kell a személyes adatokat a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, törlés, illetőleg megsemmisülés vagy sérülés ellen.

## 7.10. Az érintettek adatvédelmi jogainak érvényesülése

Az Avtv.. 11.§-a sorolja fel az érintett adatbirtokosok jogait, mely szerint az adatbirtokos kérhet tájékoztatást a személyes adatai kezeléséről, kérheti személyes adatainak helyesbítését, illetve kérhetik személyes adataik törlését kivéve, ha az adatkezelést nem jogszabály rendelte el. Az érintettek jogaik gyakorlásának részletes szabályait a 12.§-16.§ terjedő előírások rögzítik. Ha az érintett kérelmezi, az adatkezelőnek tájékoztatást kell adnia az általa kezelt adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. Az adatkezelőnek a tájékoztatást a kérelem benyújtásától számított legrövidebb idő alatt, de legfeljebb 30 napon belül írásban, közérthető formában kell megtennie. Ezen tájékoztatás évente egy alkalommal ingyenes, ha az érintett azonos kérdésben már nyújtott be tájékoztatási kérelmet, akkor az adatkezelő költségtérítést állapíthat meg.

Mészáros István László a 12.§ (1) és (2) bekezdésekhez kapcsolódón azt javasolta, hogy az érintett tájékozódási jogának korlátozására időbeli határt szabjon a törvény, így ha adattovábbításra vonatkozó nyilvántartás és ennek alapján fennálló tájékoztatási kötelezettség időtartamát az adatkezelést szabályozó jogszabály korlátozhatja, de a személyes adatok esetén öt évnél, különleges adatok esetén húsz évnél a korlátozás időtartama hosszabb nem lehet. Az adatszolgáltatás költségeit rendező 12.§ (3) bekezdés is az SZDSZ frakciójának képviselője terjesztette elő, amelyet az Országgyűlés támogatott. Vastagh Pál az adatszolgáltatás megtagadására vonatkozó 13.§ (1) és (2) bekezdésére vonatkozóan a megtagadás okainak felsorolását és a kérelem elutasításának indoklási kötelezettségét javasolta, amelyet a minősített többség elfogadott. Így az adatkezelő a tájékoztatást csak akkor tagadhatja meg, ha az állam külső vagy belső biztonsága, bűnmegelőzés, vagy bűnüldözés érdekében,

továbbá állami vagy helyi önkormányzati pénzügyi érdekből, esetleg mások jogainak védelme érdekében törvény lehetővé teszi.

A személyes adatok törlése tekintetében az Avtv.. 14.§-a előírja, hogy a valóságnak nem megfelelő adatot az adatkezelő helyesbíteni köteles, továbbá köteles törölnie, ha kezelése jogellenes, érintett kéri adatai törlését, továbbá ha az adatkezelés célja megszűnt. Az ellenzéki padosorokból javasolták az Avtv. 14.§ (3) bekezdését, amelyet a minősített többség támogatott. E cikk alapján a törlési kötelezettség – a jogellenes adatkezelés kivételével - nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyagok védelmére vonatkozó jogszabályok értelmében levéltári őrizetbe kell adni. Az Avtv.. 15.§-ról a képviselők között jelentős véleménykülönbség keletkezett, és több módosító indítvány is benyújtásra került. Tirts Tamás szerint a személyes adatok törlése vagy helyesbítése esetén nem mellőzhető az értesítés. Az adatkezelésről szóló értesítést csak akkor lehetne mellőzni, ha az érintett a helyesbítésről vagy törlésről más forrásból már tudomást szerzett. E javaslatot egyik bizottság sem támogatta, és az igazságügyi miniszter is ellene szavazott és végül az Országgyűlés az igazságügyi miniszter eredeti előterjesztését fogadta el. Az Avtv.. 15.§-a alapján a helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára tekintettel az érintett jogos érdekét nem sérti. A képviselők az érintett jogainak korlátozhatóságával kapcsolatosan is terjesztettek be módosító javaslatot. A 16.§ szerint az érintett jogainak korlátozását megengedő törvény az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűnmegelőzés, vagy a bűnüldözés érdekében, továbbá állami vagy helyi önkormányzati érdekből, valamint az érintett vagy mások jogainak védelme érdekében engedhet meg korlátozást. A módosító javaslatot, mely szerint a különleges adatok vonatkozásában az érintett jogai csak kivételesen legyenek korlátozhatók, az Országgyűlés nem fogadta el.

Az adatvédelmi igények bíróság előtti érvényesítésére vonatkozóan az Európai Adatvédelmi Egyezményrel összhangban lefektetésre került, hogy az érintett jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. Az Avtv.. az adatkezelőre helyezi át a bizonyítás terhét, mivel neki kell bizonyítania, hogy az adatkezelése jogszerű volt. A 17.§ (3) bekezdése meghatározza az eljáró bíróság illetékességét, továbbá kiterjeszti a perképeséget az érintettek vonatkozásában. Fekete Gyula betervezte azon indítványát, amely megsabta volna az adatvédelmi igény elévülési idejét. Ugyan az Emberi Jogi Bizottság támogatta, de az Alkotmányügyi Bizottság nem, és az igazságügyi-miniszter is ellene szavazott, így az elévülésre vonatkozó rövidebb három éves határidő nem került az Avtv..-ben lefektetésre. Tirts Tamás azt javasolta, hogy a 17. § (4) bekezdése a bíróság számára ideiglenes intézkedésként tegye lehetővé, hogy a bíróság az adat helyességének megállapításáig elrendelhesse a vitatott adat zárolását. Az Országgyűlés a módosító javaslatot 94 igen szavazattal, 105 ellenszavazattal, 3 tartózkodás mellett elvetette. Az Országgyűlés az eredeti javaslatot fogadta el a 17.§ (4) bekezdése vonatkozásában. Így ha a bíróság a kérelemnek helyt ad, az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, törlésére kötelezi. A 17.§ (5) bekezdését az Országgyűlés Mészáros István László javaslatára fogadta el, mely szerint a bíróság elrendelheti ítéletének adatvédelmi nyilvántartásba történő bejegyzését, ha azt az adatvédelem érdekei és nagyobb számú érintett e törvényben védett jogai megkövetelik.

Az Avtv.. 18.§-a szabályozza a jogellenes adatkezeléssel okozott kártérítés szabályait. Az adatkezelő köteles azon kárt megtéríteni, amelyet az érintett adatainak jogellenes kezelésével vagy technikai adatvédelem követelményeinek megszegésével másnak okozott. Az adatkezelésből eredő károkért az adatkezelő objektív felelősséggel tartozik, ami az érintetthez viszonyított túlereje, az érintett által gyakorolható befolyásolási lehetőség hiánya és a bizonyítási nehézségek miatt indokolt. Ezért az Avtv.. 18.§ (1) bekezdése szerint az adatkezelő akkor mentesül a felelősség alól, ha bizonyítja,

hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Az adatkezelő jogellenes adatkezelésével okozott kártérítés vonatkozásában az eredeti javaslat három éves elévülési időt állapított meg, Mészáros István László javaslatára a 18.§ (3) bekezdését az Országgyűlés elvetette.

Az adatvédelmi biztosról szóló fejezet címet Mészáros István László módosítani kívánta, mivel nemcsak a személyes adatok védelmét, hanem a közérdekű adatok nyilvánosságát is szolgálja az új tisztség, ezért az információs biztos kifejezést indítványozta, de az Országgyűlés a javaslatot elvetette. Az adatvédelmi biztosra vonatkozó eredeti törvényi előterjesztéshez a képviselők csak szövegpontosítást fűztek a 28.§ és a 30.§-hoz. A személyes adatok kutatóintézetekben történő felhasználására vonatkozóan Mészáros István László új fejezetet terjesztett be a törvényjavaslat kiegészítésére. A bizottságok támogatták ezt, az igazságügy miniszter is, így az Országgyűlés elfogadta a különleges rendelkezések cím alatti V. fejezetet. A törvény hatályba lépésével kapcsolatosan a képviselők között vita alakult ki, hogy az Avtv.-nek a folyamatban levő adatkezelésekre milyen időponttal kellene hatályba lépnie. Az Országgyűlés végül az eredeti törvényjavaslatban szereplő időponttal, a kihirdetést követő 6. hónap első napjával lépteti hatályba a törvényt. Az Avtv.-vel párhuzamosan a Ptk.. 83.§(1) bekezdését is módosította az Országgyűlés, mely szerint a számítógéppel vagy más módon történő adatkezelés és adatfeldolgozás a személyhez fűződő jogokat nem sértheti.

7.11. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításai és közösségi jogharmonizációja

7.11.1. Az Avtv. 1995-1999 közötti időszak változásai

Az adatvédelmi törvény első módosítására 1995-ben került sor, párhuzamosan a titokvédelmi<sup>162</sup>, illetve a levéltári<sup>163</sup> törvény megalkotásával. A titokvédelmi

---

<sup>162</sup> 1995. évi LXV. törvény az államtitokról és a szolgálati titokról

törvény kiegészítő rendelkezései között került elfogadásra az Avtv. 25.§-ának azon módosítása, hogy az adatvédelmi biztos „kezdeményezheti az államtitokkörben, valamint a szolgálati titokkörben meghatározott adatfajták szűkítését vagy bővítését.” A titokminősítéssel kapcsolatos eljárásra vonatkozóan az Avtv.. 26.§-a kiegészült azzal, hogy „ha az adatvédelmi biztos eljárása során az adat minősítését indokolatlannak tartja, a minősítőt annak megváltoztatására vagy a minősítés megszüntetésére szólítja fel. A felszólítás megalapozatlanságának megállapítása iránt a minősítő 30 napon belül a Fővárosi Bírósághoz fordulhat. A bíróság az ügyben zárt tárgyaláson soron kívül jár el.”

Az levéltári törvény záró és vegyes rendelkezései között kapott helyet az Avtv..-t módosító rendelkezések, amelyek elsősorban a közérdekű adatok nyilvánosságával voltak kapcsolatosak. Az Avtv.. 19. §-ának (1) bekezdésében rögzített „az állami vagy helyi önkormányzati feladatot ellátó szerv és személy” szövegrész helyébe „az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy” szövegrész lépett. A módosítás során megváltozott a közérdekű adat fogalma, így a törvényi definícióként „*közérdekű adat*: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat”. A személyes adatok védelme és a közérdekű adatok nyilvánosságának egyik lényeges konfrontációjának számító kérdést a törvénymódosítás egyértelműen rendezte, mely szerint az állami vagy helyi önkormányzati feladatot, illetve jogszabályban meghatározott egyéb közfeladatot ellátó szerv hatáskörben eljáró személy neve és beosztása – ha törvény másként nem rendelkezik - bárki számára hozzáférhető, nyilvános adat. A törvény módosítás során az is lefektetésre került, hogy az említett szervek hatáskörében eljáró személynek a feladatkörével összefüggő

---

<sup>163</sup>1995. évi LXVI. Törvény a közokiratokról, közlevéltárakról és magánlevéltári anyag védelméről (továbbiakban: Ltv)

személyes adata a közérdekű adat megismerését nem korlátozza. A közérdekű adatok nyilvánosságának korlátozására tekintettel került elfogadásra az Avtv.. 19. §-ban az a rendelkezés, amellyel kapcsolatban az Alkotmánybíróság később ugyan mulasztásban megnyilvánuló alkotmányellenességet állapított meg<sup>164</sup> - ha törvény másként nem rendelkezik, a belső használatra készült, valamint a döntés előkészítéssel összefüggő adat a keletkezését követő harminc éven belül nem nyilvános. Kérelemre az adatok megismerését a szerv vezetője e határidőn belül is engedélyezheti."

A polgárok személyes adatainak kezelésével összefüggő egyes törvények módosításáról szóló 1999. évi LXXII. törvény első részében az Avtv.. rendelkezéseinek a módosítására került sor, de módosításra került a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény, A külföldre utazásról szóló 1998. évi XII. törvény, A büntetések és intézkedések végrehajtásáról szóló 1979. évi 11. törvényerejű rendelet, Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, a Büntető Törvénykönyvről szóló 1978. évi IV. törvény is.

Az Avtv.. módosítása során megváltozott az adatkezelés, illetve az adatkezelő fogalma, a törvénybe beiktatásra került az adatfeldolgozás és az adatfeldolgozó meghatározása is. Adatkezelésnek tekintendő „az alkalmazott eljárástól függetlenül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is. Az Avtv. 7. a) pontjában kerül sor az adatkezelő fogalmának új meghatározására, mely szerint az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy

---

<sup>164</sup> 12/2004. (IV.7) AB határozat

amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg. Kötelező adatkezelés esetén az adatkezelés célját és feltételeit, valamint az adatkezelőt az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg. Az adatfeldolgozásnak minősül az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Az adatfeldolgozónak pedig az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet tekintendő, aki vagy amely az adatkezelő megbízásából személyes adatok feldolgozását végzi.

Az Avtv.. kiegészült az adatfeldolgozás szabályainak pontosabb meghatározásával, így a 4/A.§ szerint „az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Avtv., valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel. Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért. Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe.”

Az adatfeldolgozás szabályainak meghatározása érintette az adatbiztonság, az érintett tájékoztatási jogait, illetve az adatkezeléssel okozott kárfelelősség kérdést továbbá az adatkezelési nyilvántartásba történő bejelentés tartalmát is. Az Avtv.. 10. §-a helyébe lépett az új szöveg, mely szerint „az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat – kiemelten az államtitokká és a szolgálati titokká minősített személyes adatot – védeni kell, különösen a



jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen."

Az érintett részére adott tájékoztatásának ki kell terjedni arra is, hogy a személyes adatokat kik fogják feldolgozni, ezért az Avtv.. 6. §-ának (2) bekezdése akképpen módosult, hogy „az érintettet tájékoztatni kell az adatkezelés céljáról és arról, hogy az adatokat kik fogják kezelni, illetve feldolgozni. Az adatkezelésről a tájékoztatás megtörténik azzal is, hogy jogszabály rendelkezik a már létező adatkezelésből továbbítással vagy összekapcsolással az adat felvételéről. Az érintett kérelmére történő tájékoztatás során az adatkezelőnek az Avtv. módosított 12.§-a alapján tájékoztatást kell adnia az általa kezelt, illetőleg az általa megbízott feldolgozó által feldolgozott adatairól, az adatkezelés céljáról, jogalapjáról időtartamáról, az adatfeldolgozó nevééről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. Az adattovábbításra vonatkozó nyilvántartás – és ennek alapján a tájékoztatási kötelezettség - időtartamát az adatkezelést szabályozó jogszabály korlátozhatja. A korlátozás időtartama személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb nem lehet."

Az adatkezeléssel kapcsolatosan fennálló kárfelelőség tekintetében az adatkezelő felelősségét kiterjesztették az adatfeldolgozó által okozott károkra is, így az Avtv.. 18. §-ának (1) bekezdése helyébe lépett a módosított törvényszöveg, mely szerint „az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt köteles megtéríteni. Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért is. Az adatkezelő mentesül a felelősség alól, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő." Az adatfeldolgozással kapcsolatosan ki kellett egészíteni az adatkezelési nyilvántartásba történő bejelentés adattartalmát, így

az adatkezelő tevékenysége megkezdése előtt köteles az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét is bejelenteni"

A titokvédelmi törvénnyel való összhang megteremtése érdekében kiegészült az Avtv.. azzal az előírással, hogy „az államtitok és szolgálati titok az adatvédelmi biztost az Avtv.-ban szabályozott jogainak gyakorlásában nem akadályozhatja, de a titok megtartására vonatkozó rendelkezések rá nézve is kötelezőek. Az államtitkot vagy a szolgálati titkot érintő adatkezelés esetén az adatvédelmi biztos jogait csak személyesen, vagy az általa kezdeményezett nemzetbiztonsági ellenőrzésen átesett munkatársai útján gyakorolhatja."

Az 1999-es év abból a szempontból is lényegesnek tekinthető, mivel az Európai Unió Adatvédelmi Munkabizottsága ekkor véleményezte a magyarországi adatvédelmi rendelkezéseket, a törvény által biztosított adatvédelmi szintet<sup>165</sup>. A munkacsoport több alkalommal is megkereste az adatvédelmi biztost a magyar adatvédelmi szabályozásra és a biztos tevékenységére, gyakorlatára irányuló kérdéseivel 1999 tavaszán. A biztos válaszai nyomán a munkacsoport olyan ajánlást készített a bizottságnak és a tanácsnak, amelyben javasolta: állapítsák meg azt, hogy Magyarország az irányelv értelmében megfelelő védelmi szintet biztosít. A munkacsoport kedvező ajánlása azért is jelentős, mert az adatvédelem terén kedvező megítélést biztosít Magyarországnak az uniós jogharmonizáció, majd a belépési folyamatban<sup>166</sup>. A scrining vizsgálat<sup>167</sup> során a munkacsoport elnöke több alkalommal is megkereste az adatvédelmi biztost, hogy egyes kérdések egyértelműen tisztázásra kerüljenek. Az ombudsman válaszában kifejtette,

---

<sup>165</sup> PÉTERFALVI Attila, *A személyes adatok védelméről és közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításai* = Tízéves az Adatvédelmi Biztos Irodája, Budapest, Adatvédelmi Biztos Irodája, 2006. 24. old

<sup>166</sup> ABI 1999

<sup>167</sup> A 2004-ben csatlakozó 10 tagállam közül csak Magyarországon folyt le részletes vizsgálat az adatvédelem tekintetében.

hogy a szakszervezeti tagság bár nem szerepel a különleges adatok között, de gyakorlatilag mégis különleges adatnak tekinthető, mivel politikai véleményt tükröz. Az ombudsman kifejezte, hogy a személyes adatok védelmét kizárólag törvényi előírások korlátozhatják ennek alátámasztására megküldte a rendőrségi törvény, a nemzetbiztonsági törvény, illetve a hitelintézeti törvény vonatkozó rendelkezéseit. A 29-es munkacsoport véleménye<sup>168</sup> kiemelte, hogy az Avtv.. alkalmazás köre szélesebb, mint a személyes adatok köre, mivel ez szabályozza a közigazgatási dokumentumokhoz való nyilvános hozzáférés kérdéseit is, és az parlament által választott ombudsman jogosult mindkét terület ellenőrzésére. A vélemény a személyes adatok védelme tekintetében kiemeli Magyarország nemzetközi kötelezettség vállalását az Európa Tanácsnak az egyének védelméről személyes adatok gépi feldolgozása során egyezménynek a ratifikációja tekintetében. A véleményben kiemelésre került, hogy az alkotmányos rangon védi a magyar jog a magánéletet és a személyes adatok kezelését. A 29-es munkacsoport kitért a személyes adatok kezelésével kapcsolatos egyes szektorális törvényekre, így a nemzetbiztonsági szolgálatokról, a statisztikáról, a kutatásról és közvetlen üzletszerzésről szóló törvényre, de különösen az egészségügyi adatok kezelésére vonatkozó szabályozás megfelelő védelmet biztosít a személyes adatok kezelése tekintetében. A Bizottság 2000. július 26-án kelt határozatában állapította meg, hogy a magyar adatvédelem szintje megfelel az EK jogának. Az 1999-es módosításban egyébként az EK Bizottság 29-es Munkacsoportjának hatására dolgozták ki az adatkezelő és az adatfeldolgozó közötti megkülönböztetést<sup>169</sup>.

---

<sup>168</sup>Opinion 6/99 Working Party on the protection of individuals with regard to the processing of personal data; *Concerning the level of personal data protection in Hungary*. Adopted on 7 September 1999; A vélemény megtalálható magyar nyelven az Adatvédelmi Biztos 1999 évi beszámolójában

<sup>169</sup>Peter J. HUSTINX, *Megfelelő védelem - A 29. cikk Adatvédelmi Munkacsoport 6/99. sz. véleménye = Tízéves az Adatvédelmi Biztos Irodája*, szerk. PÉTERFALVI Attila, Budapest, Adatvédelmi Biztos Irodája, 2006, 86.

### 7.11.2. A 2001-2002 közötti időszak

Az Adatvédelmi Biztos a 2001-évi beszámolójában kifejtette, hogy „a majd tíz éve hatályos Avtv.. a jelen viszonyok közt időtálló, és más országok törvényalkotói számára is példamutató törvénytűnek mondható, mindazonáltal a személyes adatok védelme és a közérdekű adatok nyilvánossága szempontjából kedvező, hogy az összegyűlt jogalkalmazói tapasztalatok alapján és az EU-csatlakozás követelményeire tekintettel megindult az Avtv.. újrászabályozásának előkészítése, melynek során az Igazságügyi Minisztérium az adatvédelmi biztost is felkérte észrevételei és javaslatai megtételére<sup>170</sup>”. Az Avtv.. felülvizsgálatát célzó kodifikációs munka a kormány jogalkotási terve szerint 2001-ben kezdődött. Az előterjesztés egy teljesen új törvény elfogadására irányult volna, pontosabban két törvény megalkotását foglalta volna magába a módosítás, mivel az előterjesztés alapvető koncepcióváltást tartalmazott. Egyrészt a személyes adatok védelme és az közérdekű adatok és információk nyilvánossága két különböző törvényben került volna szabályozásra, másrészt az adatvédelmi biztos számára kötelező jellegű hatásköröket biztosított volna, a hozzá tartozó szankciórendszerrel (jogosulatlanul kezelt adatok zárolása, törlése, megsemmisítése), harmadrészt az adatvédelmi biztos jogosítványokat kapott volna bírósági eljárásokban is.

Az adatvédelmi biztos közel hat éves tapasztalatait összegezve állapította meg, hogy a személyes adatok védelméhez való jog, valamint az információszabadság büntetőjogi védelme a szabályozás hiányosságaiból következően nem érvényesül a kívánt mértékben. A büntető törvénykönyv ezen két alapjoggal összefüggő rendelkezései ugyanis egyrészt túlságosan tágan húzzák meg a büntethetőség határát, vagyis olyan cselekményeket is büntetni rendelnek, amelyek elleni fellépés nem igényli a büntetőjog eszközeit, másrészt olyan fogalmakat használnak, amelyek nem pontosan

---

<sup>170</sup> Adatvédelmi biztos beszámolója 2001. <http://abiweb.obh.hu/abi/index.php?menu=165> ; 2006.07.06.

felelnek meg az adatvédelmi jog dogmatikai rendszerének, ezért a két érintett alkotmányos jog valóságos és hatékony büntetőjogi védelme érdekében a Btk.. módosításnak előkészítésére kérte fel az igazságügy-minisztert<sup>171</sup>.

A 2001-es évben szükségessé vált ajánlás kiadása az internet használat és személyes adatok védelme tekintetében. Az ajánlás javasolja a jogalkotó, jogszabály-előkészítő számára, hogy az Avtv.. módosításával hozza összhangba a külföldre történő adattovábbítás szabályozását a 95/46/EK Irányelv rendelkezéseivel. Az elektronikus információszabadság megteremtése érdekében írja elő, hogy a közérdekű adatok meghatározott körét kötelező közzé- vagy elérhetővé tenni elektronikus formában is, továbbá a kapcsolódó szektorális törvények módosításával gondoskodjon: a kéréstlen üzleti célú üzenetekre vonatkozó szabályozás kialakításáról, a forgalmi adatok kezelésének jogszerűvé tételéről, a hackerek elleni védekezés jogi lehetőségeiről, továbbá az internetre vonatkozó szabályozások kialakítása előtt minden esetben folytasson konzultációkat az internet-felhasználók és szolgáltatók képviselőivel<sup>172</sup>.

A kormány 2002. második félévi munkatervében is szerepelt még az Avtv. felülvizsgálata, és az irányelvvel történő összhang kialakítása. A törvényjavaslatból kikerültek az Alkotmánybíróság gyakorlatával, illetve a magyar alapjogi korlátozás arányossági és szükségességi követelményeivel ellentétes szabályok, de megmaradt az a koncepció, mely szerint két külön törvényben kellene szabályozni az információs önrendelkezési jogot, illetve az információs szabadságot. A kodifikációs munkára az EU csatlakozás előtt nem került sor, mivel a személyes adatok megfelelő védelmére vonatkozó megállapodások újra napirendre kerültek volna. De az Avtv.. 2003. évi módosításainak alapját a 2001-ben elkezdett jogalkotói munka és lefolytatott egyeztetések nyújtották<sup>173</sup>.

---

<sup>171</sup> 272/H/2001

<sup>172</sup> 406/K/2000

<sup>173</sup> PÉTERFALVI, *i.m.*, 27.

### 7.11.3. Az Avtv.. novellája 2003 és 2005 közötti időszak

A 2003-ban az információs jogok évének tekinthető, az Országgyűlés elfogadta az üvegzebtörvényt, elkészült a titokvédelmi törvény módosítása, és a 2003. évi XLVIII. törvény a közösségi jogharmonizációs célból módosította az Avtv.. jelentős részét. Az új törvényi előírások elsősorban a személyes adatok kezelését, illetve a fogalmi rendszerét rögzítették az Avtv.. személyi, tárgyi hatályát. A személyes adatok körén belül a törvénymódosítás bevezette az egyedi automatizált döntésre vonatkozó adatvédelmi követelményeket, adatkezelések esetében kötelezővé tette az írásbeli szerződések megkötését, továbbá egyes szolgáltatók tekintetében kötelezővé tette a belső adatvédelmi felelős kinevezését, és adatvédelmi szabályzat megalkotását. A jogharmonizációs módosítás másik iránya az adatvédelmi biztos hatásköreit, és eszköztárszerét érintette. A módosítások áttekintése során elsősorban azokat a változásokat veszem számba, amelyek a személyes adatok védelmét érintették. Az adatvédelmi biztos hatáskörei tekintetében a következő fejezet ad áttekintést.

Az Avtv. kiegészült a tárgyi és személyi hatály világos körülírásával, mely szerint az Avtv. irányadó minden olyan adatkezelésre és adatfeldolgozásra, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz. A törvényt mind a teljesen vagy részben, illetve automatizált vagy manuálisan végzett adatkezelésekre kiterjed. A törvényt nem kell alkalmazni, ha valamely magánszemély kizárólag saját céljaira vonatkozóan bonyolít le adatkezelést. A törvény hatálya függetlenné vált az adatkezelő székhelyétől, kizárólag a tevékenység végzésének adatkezelés, illetve adatfeldolgozás esetén is a helye határozza meg az irányadó jog alkalmazását.

A módosítások kiegészítették és átalakították az Avtv. fogalmi rendszerét is. A személyes adatok fogalma kiegészült az azonosítás módjára vonatkozó

rendelkezésekkel, így egy személy akkor tekinthető azonosítottnak, ha őt – közvetve vagy közvetlenül – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. A különleges adatok körén belül a törvényszövegbe beemelésre került a nemzetiségi, illetve szakszervezeti tagságra vonatkozó adat, mint szenzitív adat. Míg korábban a büntetett előéletre vonatkozó adatot tekintette a törvény különleges adatnak, addig a módosítás ezt a fogalmat megszüntette, és helyette a bűnügyi személyes adat fogalmát definiálja önálló adatsportként a különleges adatok körén belül. Az Avtv. 2.§ 3. pontja szerint bűnügyi személyes adatnak minősül a büntetőeljárás vagy azt megelőzően a bűncselekménnyel vagy büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtásra jogosult szervezeteknél keletkezett az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

A törvény fogalmi struktúrája kiegészült a közérdekből nyilvános adat fogalmával, illetve egyértelműen meghatározásra került az érintett részéről az adatkezelésekhez történő hozzájárulás törvényi feltétele. Az érintett hozzájárulása az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Az módosítás érintette az adatkezelés eddigi törvényi definícióját is, így adatkezelésnek minősül az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy

tenyényomat, DNS-minta, íriszkép) rögzítése is. A módosítás során újra definiálták az adatfeldolgozó és az adatfeldolgozás fogalmát. Az Avtv. értelmező rendelkezései között újonnan meghatározásra került a tiltakozás, az adattovábbítás, a nyilvánosságra hozatal, az adattörlés, az adatszárolás, az adatmegsemmisítés, a személyesadat-nyilvántartó rendszer, az adatállomány, a harmadik személy, illetve a harmadik ország fogalma is.

Az adatkezelés új törvényi keretként került 2003-ben meghatározásra az Avtv. 3.§ (3) bekezdésében, hogy kötelező adatkezelés esetén az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvénynek vagy a felhatalmazása alapján önkormányzati rendeletnek kell meghatároznia. A szerződési kötelezettségen alapuló adatkezelésekre vonatkozóan az Avtv. módosítása során lefektetésre került, hogy az érintett az adatkezelés tekintetében a hozzájárulását az adatkezelővel kötött szerződésben írásos formában is megadhatja a szerződésben foglalt jogok és kötelezettségek teljesítése céljából. Ebben az esetben a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az Avtv. előírásai alapján az érintettnek ismernie kell, így különösen a kezelendő adatok körének meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának, és adatfeldolgozó igénybevételének a tényét. A törvény meghatározta egyes kivételes esetekre vonatkozóan a személyes adatok, beleértve a különleges adatok kezelésének jogalapját, így ha az érintett fizikai okból, vagy cselekvőképtelensége folytán nem képes hozzájárulását adni adatai kezeléséhez, akkor a saját vagy más személy létfontosságú érdekeinek védelme érdekében, illetve katasztrófa vagy sürgősségi helyzet elhárításához, megelőzéséhez szükséges mértékben sor kerülhet személyes adatainak kezelésére.

Az Avtv.. adatfeldolgozásra vonatkozó előírásai között került elfogadásra, hogy az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni,



illetve adatfeldolgozásra nem adható megbízás olyan vállalkozásnak, amelynek üzleti célból érdeke a személyes adatok feldolgozása. Az Avtv. 4/A.§ (6) bekezdésében került sor az Avtv.- hatálya alá tartozó adatkezelések tekintetében annak meghatározására, hogy ha személyes adatok feldolgozására az Európai Unió területén kívüli székhellyel rendelkező személy olyan a Magyar Köztársaság területén székhellyel, telephellyel, vagy lakóhellyel rendelkező adatfeldolgozót bíz meg, vagy itt található eszközt használ fel, akkor az adatkezelőnek egy képviselőt kell a Magyar Köztársaság területén kijelölni. Az adatkezelőt nem terheli ez a kötelezettség, ha az adott eszköz csak az Európai Unió területén átmenő adatforgalom lebonyolítását szolgálja.

Az adatkezelés célhoz kötöttsége körében az EK irányelv rendelkezéseivel összhangban az Avtv. 5.§ (4) bekezdése került beiktatásra, amely lefekteti az adatkezelés jogalapjaként, hogy személyes adatot az érintett, vagy jogszabály alapján akkor lehet kezelni, hogy ha ez közérdekű feladat, vagy az adatkezelő törvényi kötelezettségének tesz eleget, illetve hivatalos feladat teljesítéséhez, továbbá az érintett létfontosságú érdekeinek a védelméhez szükségesek. Az adatbirtokos és az adatkezelő közötti szerződés teljesítése is megalapozza a személyes adatok kezelését, illetve társadalmi szervezetek is jogosultak a működésükhöz szükséges mértékben személyes adatok kezelésére. Azon személyes adatok kezelésére, amelyek bűnüldözési, bűnmegelőzési, bünyügyi valamint közigazgatási, polgári peres vagy igazságszolgáltatási feladatok teljesítése érdekében kerülnek gyűjtésre, feldolgozásra, illetve tárolásra, kizárólag állami vagy önkormányzati szervek keretein belül kerülhet sor.

Változtak az Avtv.-ben az érintett tájékoztatására vonatkozó előírások is. Így azon alapvető követelmény mellett, hogy az érintettet az adatfelvételt megelőzően tájékoztatni kell az adatgyűjtésnek az önkéntes vagy kötelező voltáról, kiegészült a törvény azzal, hogy az érintettet egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatosan minden

tényről, így különösen az adatkezelés céljáról, annak jogalapjáról, továbbá az adatkezelésre és adatfeldolgozásra jogosult személyről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatás során ki kell térni az érintett jogaira, illetve jogorvoslati lehetőségeire. A tájékoztatások sajátos esetét kell alkalmazni különösen a statisztikai, illetve tudományos, elsősorban történelmi kutatások esetén, ha az egyénre szóló tájékoztatás lehetetlen vagy aránytalan költséggel járna, ebben az esetben az érintettek körének, az adatgyűjtés céljának, az adatkezelés időtartamának és az adatoknak mindenki számára történő hozzáférés nyilvánosságra hozatalával mellőzhető az egyéni tájékoztatás.

A 95/46/ EK irányelvvel való összhang kialakítása érdekében a magyar jogban is átvételre kerültek az automatizált egyedi döntésre vonatkozó szabályok. Automatizált személyes adatfeldolgozáson kizárólag számítógép által végrehajtott automatizált adatfeldolgozást ért a törvényalkotó, amelyre csak akkor kerülhet sor, ha ahhoz az érintett kifejezetten hozzájárult, vagy ha azt a törvény lehetővé teszi. A törvény előírja, hogy az automatizált egyedi döntés tekintetében az érintett számára lehetőséget kell adni álláspontja kifejtésére. Az automatizált adatfeldolgozás esetén az érintett részére tájékoztatást kell adni az alkalmazott matematikai módszerről és annak lényegéről.

A törvényben változtak a személyes adatok kötelező törlésére vonatkozó előírások, így ha a jogszerű állapot nem állítható helyre a téves vagy hiányos adatot törölni kell. A személyes adatokat törölni kell, ha az adatkezelés célja megszűnt, illetve a személyes adatok tárolására határozott határidő letelt. Az adatvédelmi biztos megváltozott szerepkörével összefüggésben került sor annak lefektetésére, hogy a személyes adatokat törölni kell, ha azt a bíróság vagy az adatvédelmi biztos elrendelte. A törvény módosítása során kiegészítésre kerültek azok az okok, amelyek megalapozhatják a személyes adatok törvényi korlátozását. Az érintett jogai a személyes adatok védelme tekintetében törvényben korlátozhatók akár az érintett, vagy mások jogainak

védelme érdekében, de az Avtv.. 16.§-a korábban is felsorolt okok, mint a honvédelmi, nemzetbiztonsági érdek, a bűnmegelőzés vagy a bűnüldözés céljából, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdek mellett lefektetésre került, hogy a foglalkozások gyakorlásával összefüggő fegyelmi, etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása érdekében, beleértve ez esetekben az ellenőrzést és a felügyeletet is lehet a személyes adatokat korlátozni. Ez a felsorolás kiegészült továbbá azzal is, hogy az érintett információs önrendelkezési joga korlátozható az Európai Unió pénzügyi, és gazdasági érdekeire hivatkozással is.

Az Avtv.-ban a tiltakozási jog önállóan nem került meghatározásra, de ezt a hiányt pótolta a 2003-évi módosítás. Az érintett tiltakozhat személyes adatának kezelése ellen, ha a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el. Az érintett tiltakozhat abban az esetben is, ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik. A törvényi előírások egyéb esetekben is lehetővé tehetik a tiltakozást a személyes adatok kezelése ellen.

A tiltakozási jog gyakorlása során az adatkezelő – az adatkezelés egyidejű felfüggesztésével – a tiltakozást köteles a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 nap alatt megvizsgálni, és annak eredményéről a kérelmezőt írásban tájékoztatni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszüntetni és az adatokat zárolni, valamint a tiltakozásról, illetőleg az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében. Ha az érintett az adatkezelőnek a döntésével nem ért egyet, az ellen – annak közlésétől számított 30 napon belül – az Avtv. szerinti bírósághoz fordulhat.

Az érintettet az adatok harmadik személy részére történő átadással kapcsolatosan is megilleti a tiltakozási jog. Ebben az esetben, ha az adatátvevő törvényes jogának érvényesítéséhez szükséges adatokat az érintett tiltakozása miatt nem kapja meg, akkor az adatkezelőnek az érintett részére kiküldött értesítés közlésétől számított 15 napon belül, az adatokhoz való hozzájutás érdekében bírósághoz fordulhat az adatkezelő ellen. Az adatkezelő az érintettet is perbe hívhatja. Ha a bíróság az adatátvevő kérelmét elutasítja, az adatkezelő köteles az érintett személyes adatát az ítélet közlésétől számított 3 napon belül törölni. Az adatkezelő köteles az adatokat akkor is törölni, ha az adatátvevő az igen rövid 15 napos határidőn belül nem fordult bírósághoz. Az adatkezelő az érintett adatát nem törölheti, ha az adatkezelést törvény rendelte el. Az adat azonban nem továbbítható az adatátvevő részére, ha az adatkezelő egyetértett a tiltakozással, illetőleg a bíróság a tiltakozás jogosságát megállapította.

Az Avtv.. egyik jelentős újításának tekinthető német mintára, hogy az adatkezelőknek belső adatvédelmi felelőst kell kineveznie, aki közvetlenül a szerv vezetőjének felügyelete alá tartozik. Az Avtv. szerint belső adatvédelmi felelőst az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőnél és adatfeldolgozónál, a pénzügyi szervezetnél, a távközlési és közüzemi szolgáltatónál kell kötelezően kinevezni. A belső adatvédelmi felelősnek jogi, közigazgatási, számítástechnikai képzettséggel kell rendelkeznie feladatai ellátásához, aki közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában. Ellenőrzi továbbá az adatkezelésre vonatkozó jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását. A belső adatvédelmi felelős kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az

adattfeldolgozót. A belső adatvédelmi felelős feladatkörébe tartozik, hogy elkészítse a belső adatvédelmi és adatbiztonsági szabályzatot, illetve ő vezeti a belső adatvédelmi nyilvántartást, illetve gondoskodik az adatvédelmi ismeretek oktatásáról.

#### 7.11.4. Az Avtv. 2005-es módosítása

Az Avtv. a 2003-as jelentős novelláris módosítását követően a 2005. év folyamán ismét az Országgyűlés elé került, amelynek elsődleges oka a törvényjavaslat általános indoklása szerint is az Alkotmánybíróság 12/2004. (IV.7.) határozata, amely a belső használatra készült dokumentumokkal kapcsolatosan mulasztásban megnyilvánuló alkotmányellenességet állapított meg. A törvényalkotás során a közérdekű adatok megismeréséhez fűződő joggaranciának jobb kiépítése érdekében került sor módosításokra. A törvényjavaslat másik célja az adatvédelmi biztos jogkörének és jogállásának újraszabályozása, mivel 2003 óta ügydöntő hatáskörrel is rendelkezik. A módosítás harmadik irányát az általános indoklás az internet elterjedésével magyarázta, amely szükségessé tette külföldre irányuló adattovábbítás szabályainak harmonizálását az EK joggal, hogy a megfelelő védelem a harmadik országba történő adattovábbítás esetén is biztosítva legyen. Egyébként a magyar adatvédelmi szabályok szigorúbb feltételeket támasztottak, mint az EK joga, így a külföldre történő adattovábbítás esetén a magyar adatvédelem szintjét le kellett szállítani<sup>174</sup>.

Az Avtv.. 9.§ (1) bekezdése alapján a személyes adat akkor továbbítható harmadik országban található adatkezelő vagy adattfeldolgozó részére, ha ahhoz az érintett kifejezetten hozzájárult, vagy ha azt törvény elrendeli és a harmadik országban az átadott adatok kezelése és feldolgozása során biztosított a személyes adatok megfelelő szintű védelme. A személyes adatok megfelelő

---

<sup>174</sup> HUSTINX, *Megfelelő...,i.m.*, 87.

szintű védelmének kialakítására az Avtv. három esetkört szabályoz. A harmadik országokba irányuló adattovábbítások tekintetében az EK a megfelelő védelmi szintet követeli meg, amely elvárja, hogy az EK jogában kikristályosodott adatvédelemhez hasonló, de szükségképpen nem azonos védelmet biztosítson. A harmadik országba történő adattovábbítás során figyelembe kell venni, hogy a belső piaci témakört érintő adatkezelésekre a harmadik országba történő adattovábbítás tekintetében érvényesül a közösségi jog elsőbbsége. A közösségi jog hatálya alá eső témakörökben a magyar jogalkotóra, illetve jogalkalmazóra is kötelező 95/46/EK irányelv alapján a Tanács határozatban állapítja meg azon harmadik országok körét, amelyek az EK jogával azonos szintű védelmet biztosítanak az adatkezelés során. A belső piac körébe tartozó kereskedelmi célzatú adatkezelések esetén a megfelelő védelmi követelmények tekintetében is az EK által előírt<sup>175</sup> általános szerződési feltételeket kell alkalmazni a jogügylet során. Az úgynevezett Safe Harbour megállapodásokkal a harmadik országban székhellyel rendelkező egyes üzleti partnerek önkéntesen az EK jogához hasonló szerződési kötelezettségeket vállalnak az adatkezelések során. A harmadik országba irányuló nem kereskedelmi célzatú személyes adatkezelések tekintetében az EK jog, így ezen keresztül a magyar Avtv. is megköveteli, hogy a harmadik ország és a Magyar Köztársaság között olyan nemzetközi szerződés létezzen, amely az EK jog által meghatározott személyes adatok védelmi szintjét biztosítja, és megfelelő garanciákkal, így független ellenőrzéssel is kikényszeríti. Ezen nemzetközi szerződések általában jogsegély egyezmények, így az Avtv.. le is fekteti, hogy személyes adatokat kizárólag jogsegély egyezmények alapján lehet harmadik országba továbbítani.

---

<sup>175</sup> 106. Személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbításra vonatkozó általános szerződés feltételekről szóló 2001. december 27-i 2002/16 EK bizottsági határozat. <http://abiweb.obh.hu/abi/index.php?menu=137&nyomtat=1> ; 2006.10.25.

## 8. A MAGYAR ADATVÉDELMI BIZTOS

### 8.1. A magyar adatvédelmi biztosi intézmény kialakulása

Mielőtt az adatvédelmi biztos jogállásának a részletes elemzésébe kezdenék, vissza kell utalnom ennek a közjogi intézménynek a keletkezésére, mégpedig a névválasztással kapcsolatos vitára. Az Országgyűlésben elhangzott az a vélemény, hogy ha az információs önrendelkezési jog és az információ szabadság védelmét egy törvényen belül oldja meg a törvényalkotó, akkor információs jogok biztosának kellene ezt a közjogi intézményt elnevezni. Valószínűleg ez az elnevezés jobban kifejezte volna e közjogi intézmény alkotmányos funkcióját, de az Országgyűlés többsége maradt az előterjesztő által javasolt adatvédelmi biztosi elnevezésnél. E rövid visszatekintés is tükrözi az adatvédelmi biztosi intézmény újszerűségét nemcsak a rendszerváltás időszakában, hanem az 1990-es évek Nyugat-Európájában is. A magyar modell, mely szerint egy ombudsman egyszerre védi az információs önrendelkezési jog érvényesülését és az információszabadság alkotmányos alapját nemzetközi értelemben is példaértékű, úttörő vállalkozásnak számított. Az adatvédelmi biztos elmúlt több mint 10 éves működésére visszatekintve egyértelműen állítható, hogy a személyes adatok védelme tekintetében a törvényi előírásokat sikerült élő joggá, ténylegesen alkalmazott védelemmé fejleszteni. Az adatvédelmi biztosi intézmény keletkezés története során lényeges körülmény, hogy az Alkotmánybíróság a magyar adatvédelmet megalapozó határozatában<sup>176</sup> tulajdonképpen kijelölte ennek az intézménynek a keretét, addig az általános biztosra vonatkozó elképzelések már az 1989-es Nemzeti Kerekasztal tárgyalások során kialakultak.

Az adatvédelem garanciális intézményei tekintetében többféle lehetőség kínálkozott. A nemzetközi minták alapján lehetett volna az adatvédelem

---

<sup>176</sup> 15/1991 (IV.13) AB határozat

érdekében független szakértő testületet is létrehozni, vagy a belügyminiszter illetve az igazságügy miniszter által kinevezett független vezetőt a feladattal megbízni, de mindkét esetben olyan hatóság jött volna létre, amely apparátusa némely minisztériumhoz szorosan kötődik. Az 1990-es évek elején választott megoldás, mely szerint az adatvédelmi biztos az Országgyűlésnek alárendelt szakombudsman, az állampolgári jogok országgyűlési biztosával megegyező jogállással, függetlenséggel és összeférhetetlenséggel, a magyar demokratikus fejlődés egyik fontos előre lépése volt. Talán ezért is tartott olyan sokáig, míg végül sikerült az első adatvédelmi biztos Majtényi Lászlót az Avtv.. hatályba lépését követő harmadik évben megválasztani.

## 8.2. Az adatvédelmi biztos alapjogvédelmi funkciója

Az Országgyűlés az ombudsmanokat, így az adatvédelmi biztost is neki felelős szervként választja meg. Így értelmezhető az ombudsmanok funkciója akképpen is, hogy ők a népszuverenitás közvetett megbízottjaiként járnak el a parlament által átadott hatáskörben, hogy az alkotmányos jogokkal kapcsolatban tudomásukra jutott visszasságokat kivizsgálják, vagy kivizsgáltassák, és orvoslásuk érdekében általános vagy egyedi intézkedéseket tegyenek. Sem az Alkotmány, sem az ombudsmani törvény nem határozza meg, hogy miképpen kell az alkotmányos visszasság fogalmát értelmezni, ezért annak kitöltése az ombudsman feladata. Az általános biztos bizonytalan terepen haladva az Alkotmányban rögzített alapelvekre, illetve az Alkotmánybíróság esetjogára támaszkodhat, ha az egyes alapjog megsértésére vonatkozó kereteket meg kívánja határozni.<sup>177</sup> Az adatvédelmi biztos feladatköre az általános országgyűlési biztoshoz képest az Avtv. rendelkezései alapján sokkal inkább körülhatárolhatóbb, mivel a tevékenysége során a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való

---

<sup>177</sup> SÓLYOM László, *Az ombudsman „alapjog értelmezése” és „normakontrollja”*, Fundamentum, 2001/5, 2. sz. 14.



alkotmányos jog védelme érdekében működik. Az adatvédelmi biztos tevékenysége során vizsgálja e két alapjog érvényesülésének az Avtv.-ben meghatározott feltételeinek teljesítését, illetve az adatkezelésre vonatkozó más jogszabályok megtartását, ami természetesen kiterjed az információs alapjogok érvényesülését biztosító más törvényben, illetve rendeletben megfogalmazott jogszabályi környezet vizsgálatára is. Ezért az adatvédelmi biztos nemcsak az Avtv. rendelkezéseinek a megsértése esetén, hanem minden olyan más jogszabály sérelme esetén vizsgálódik, amelyek közvetve vagy közvetlenül a személyes adatok védelmét, illetve a közérdekű adatok nyilvánosságát biztosítják. Az adatvédelmi biztos a személyes adatok védelmének hiányzó garanciái során hivatkozhat az Avtv. általános rendelkezései a célhoz kötöttségre, a készletező adatgyűjtés tilalmára, vagy az adatkezelés jogalapjának meghatározásának kötelezettségére anélkül, hogy az alkotmányos sértés „közjogi vádját” fogalmazná meg.

Sólyom László az adatvédelmi biztos tevékenységével kapcsolatosan kifejtette<sup>178</sup>, hogy az ombudsmani vizsgálat során sok esetben elkerülhetetlen alapjog értelmezése az alkotmánybírói határozatokban keletkező alapjogi kazuisztikához hasonlít, illetve olyan mint, amelyet a rendes bíróságok által végzett alapjogi bíráskodás fejleszthet ki, ha ezt a bíróságok felvállalják. Szem előtt tartva azt az alapvető különbséget, ami egy kötelező bírósági határozat és egy ombudsmani ajánlás között fennáll, mégis azt állíthatjuk, hogy legalábbis egyes alapjogok tekintetében az ombudsmani jogértelmezés képes a hiányzó alapjogi bíráskodás jogértelmező funkcióját részben pótolni. A személyes adatok védelmét érintő alapjogi bíráskodás esetjogát az adatvédelmi biztos által közreadott ajánlások, nyilatkozatok és éves beszámolóit pótolhatják, és szokásjogi erővel érnek el hatást a joggyakorlat terén. Az adatvédelmi biztos ajánlásai igen gyakran tartalmazzak olyan megállapításokat, amelyek a vizsgált ügyek tanúságait általánosítva, követendő irányelveket fogalmaznak meg. A címzettek számára úgy jelennek meg, mintha önálló normák lennének, és az

---

<sup>178</sup> U.A., 16.

ember érzése az lehet, hogy a megállapításokat valamely végrehajtási rendelet vagy az annak alapján kiadott utasítás is tartalmazhatná<sup>179</sup>.

Az általános biztos és az adatvédelmi biztos közötti további lényeges különbség, hogy míg az állampolgári jogok általános biztosa a közigazgatási szervek működése tekintetében határozza meg az alkotmányossági visszasságok körét, addig az adatvédelmi biztos hatásköre az adatkezelőkre terjed ki, akik lehetnek az állami szférában, de egyre nagyobb mértékben a privát gazdaság területén is sor kerülhet személyes adatok feldolgozására. Ebből fakadóan az általános biztos szerepköre az államigazgatással szemben megfogalmazott ellensúlyként értelmezhető, és így nélküli is a hatósági eszközöket, ezzel szemben az adatvédelmi biztos funkciója a 2003-as novelláris módosítást követően a hatósági szerepkör felé mozdult el, ugyan érdemi eszközök nélkül, de jogosult személyes adatok törlését elrendelni. Így az adatvédelmi biztos az alapjogvédelem területén hatékonyabb eszközökkel van felszerelve, mint az általános biztos a maga területén.

Álláspontom szerint az adatvédelmi biztos a személyes adatok védelmére vonatkozó joggyakorlata alapján az alapjogvédelmi funkciójából indult ki, és ehhez kapcsolódó vizsgálati módszereket alkalmazott. Az adatvédelmi biztosok állásfoglalásaik során az adatkezelés tisztességességének kérdését nem, vagy csak alig bontották ki, bár ez a fogalom széleskörű interpretációra adna lehetőséget. A fogyasztóvédelmi jogban tisztességtelen szerződési feltételek alkalmazása ellen részletes normarendszer alakult ki, amely elvi, módszertani alapot adhatna az adatvédelmi biztosnak, hogy magánjog körében írásban, szóban, vagy ráutaló magatartással megkötött szerződésekben adott adatkezelési felhatalmazások tekintetében az adatkezelő és az érintett között adatvédelmi jogviszony magatartási normáit meghatározza. Ha az adatvédelmi biztos általános polgári jogelvként is létező tisztességesség követelményén keresztül értelmezné a felek közötti adatvédelmi jogviszonyokat azzal, hogy az

---

<sup>179</sup> U.A., 18.

alapjogvédelmi funkcióját betölti, sokkal rugalmasabb, gyakorlatban alkalmazhatóbb magatartási normákat határozhatna meg ajánlás formájában. Véleményem szerint a magánjog körébe tartozó adatkezelők számára a tisztesség fogalma köré felépített jogvédelmi érvelés érthetőbb, és így befogadhatóbb lenne, mint kizárólag az alapjogi érvrendszerre támaszkodó jogvédelem.

### 8.3. A magyar adatvédelmi biztos jogállása

Az adatvédelmi biztos jogállására irányadó az állampolgári jogok országgyűlési biztosáról szóló többször módosított 1993. évi LIX. törvény, így ahol az ombudsmani törvény országgyűlési biztost említ, azon a külön biztosokat is érteni kell. Arra az esetre, ha az adatvédelmi biztosi tisztség nem lenne betöltve, helyette az országgyűlési biztos jár el. Az ombudsmani törvény meghatározza, hogy országgyűlési biztosnak, így szakombudsmannak választható minden olyan egyetemi jogi végzettségű, büntetlen előéletű magyar állampolgár, aki kiemelkedő tudású elméleti vagy legalább tízévi szakmai gyakorlattal rendelkezik, olyan jogász, aki az alkotmányos jogokat érintő eljárások lefolytatásában, felügyeletében vagy tudományos elméletében jelentős tapasztalatokkal rendelkezik, és köztisztletnek örvend. Emellett az adatvédelmi biztosnak meg kell felelnie az Avtv. által támasztott követelményeknek is, így neki a fenti követelmény mellett az adatvédelmet érintő eljárások lefolytatásában, felügyeletében vagy tudományos elméletében is jelentős tapasztalatokkal kell rendelkeznie. Országgyűlési biztos nem lehet az, aki a választásra irányuló javaslat megtételének időpontját megelőző négy évben országgyűlési képviselő, köztársasági elnök, az Alkotmánybíróság tagja, a kormány tagja, államtitkár, helyettes államtitkár, a helyi önkormányzati képviselő-testület tagja, jegyző, ügyész, a fegyveres erők, a rendvédelmi szervek hivatásos állományú tagja, valamint pártnak az alkalmazottja volt.

Az adatvédelmi biztos személyére a köztársasági elnök tesz javaslatot, akit az Országgyűlés illetékes bizottságai, így az Alkotmányügyi, az Emberi Jogi és más szaktanácsadói meghallgatja. Ahhoz, hogy az adatvédelmi biztosnak jelölt személy elnyerje a tisztséget az országgyűlési képviselők kétharmadának igen szavazata szükséges. Ha a javasolt személyt az Országgyűlés nem választja meg, a köztársasági elnök legkésőbb harminc napon belül tehet új javaslatot. Az adatvédelmi biztost, úgymint az országgyűlési biztost az Országgyűlés hat évre választja meg, de ezt követően még egyszer újraválaszthatja.

Az adatvédelmi biztosra szigorú összeférhetlenségi szabályok vonatkoznak, mivel megbízatása összeegyeztethetetlen más állami, önkormányzati, politikai vagy társadalmi szerepvállalással, sőt a feladatkörén túlmenően politikai tevékenységet nem végezhet, politikai tárgyú véleményét sem adhatja közre. Az adatvédelmi biztos más kereső foglalkozást nem tölthet be, díjazást nem fogadhat el, kivéve a tudományos, az oktatói, a művészeti, a szerzői jogi védelem alá eső, továbbá lektori és a szerkesztői tevékenységet. Az adatvédelmi biztosi tisztségre a szigorú, még a gazdasági tevékenységre is kiterjedő összeférhetlenség mellett az országgyűlési képviselőkre irányadó vagyonnyilatkozat tételi kötelezettség is kiterjed. Az adatvédelmi biztost megilleti a mentelmi jog is, amelynek indokolt megszüntetéséről az országgyűlés elnökének javaslatára a Ház minősített többséggel dönt.

#### 8.4. Az adatvédelmi biztos hatáskörei, eljárása és eszközei

Az adatvédelmi biztos hatásköre kiterjed az Avtv. rendelkezéseinek megtartásának, illetve az adatkezelésre vonatkozó más jogszabályok betartásának ellenőrzésére, továbbá az adatvédelmi biztos vezeti az adatvédelmi nyilvántartást. Az adatvédelmi biztosi intézményhez kezdettől

fogva kapcsolódott az a hatáskör, amely szerint az adatvédelmi biztos javaslatot tehet az adatkezelés és a közérdekű adatok nyilvánosságát érintő jogszabályok megalkotására, módosítására, továbbá véleményezi ezen jogszabályok tervezeteit. Az Avtv. rendelkezései közül kimaradt az az előírás, hogy a jogalkotási hatáskörrel rendelkező szervezeteknek kötelező megküldeni jogalkotási tervezeteiket az adatvédelmi biztosnak, illetve az is tisztázatlan, hogy a jogalkotás mely szakaszában kell az adatvédelmi biztos számára a tervezetekhez kapcsolódóan a véleményezési jogot biztosítani. Az adatvédelmi biztosnak a hatásköreit és eszközeit a 2003-as novelláris módosítás alapvetően újraformálta, és az adatvédelmi biztosi intézményt a hatósági szerepkör irányába tolta el. Az adatvédelmi biztos új feladataként lett definiálva, hogy elősegíti a személyes adatok kezelésére és a közérdekű adatok nyilvánosságára vonatkozó törvényi rendelkezések egységes alkalmazását. Ehhez kapcsolódóan került lefektetésre, hogyha az adatvédelmi biztos az adatkezelést elrendelő jogszabályt kifogásolja, ajánlást tehet a jogszabály módosítására.

A törvényalkotó az adatvédelmi biztos számára az állami és szolgálati titokról szóló törvény 1998-as módosítása<sup>180</sup> során a titokfelügyelettel kapcsolatosan is határozott meg kompetenciát, amely szerint az adatvédelmi biztos, ha valamely adatnak a minősítését indokolatlannak tartja, akkor annak megváltoztatására vagy a minősítés feloldására szólítja fel a titokgazdát. A minősítő a felszólítás megalapozatlansága miatt 30 napon belül a Fővárosi Bírósághoz fordulhat. A jogszabály ezen a helyen egy lényeges jogkövetkezményt nem szabályoz, így ha a Fővárosi Bíróság helyben hagyja az adatvédelmi biztos megállapításait, akkor a minősítőnek eleget kell tennie az adatvédelmi biztos és a bíróság döntésének. Így az adatvédelmi biztos titokfelügyeleti szerepköre inkább szimbolikusnak tekinthető, mint érdemi funkcionak.

---

<sup>180</sup> 1998. évi LXXX. törvény az államtitokról és a szolgálati titokról szóló

Az adatvédelmi biztos nemcsak jogállása, hanem az általa alkalmazott eszközök tekintetében is, a létrejöttekor a klasszikus közjogi ombudsmani intézményhez állt közelebb. Az adatvédelmi biztos a hozzá beérkezett beadványokat, bejelentéseket kivizsgálja, a beadványtevőt tájékoztatja az indítványának a nyilvántartásba vételéről, és arról, hogy az adatvédelmi biztos nincs a közigazgatási törvény (korábban Áe, jelenleg Ket.) szabályaihoz kötve, így az ügy elintézésére a 30 napos határidő nem irányadó. Az adatvédelmi biztos megteheti, hogy a beadványozót a szóban forgó ügyben már kialakított korábbi levelének, állásfoglalásának a megküldésével tájékoztatja. Abban az esetben, ha az adatvédelmi biztos érdemi vizsgálatot kezdeményez, mert az ügy jelentősége, az érintettek viszonylag nagy száma azt indokolja, akkor a vizsgálat eredményéről a beadványtevőt a biztos értesíti. Az adatvédelmi biztos vizsgálati módszereit tekintve tematikus, illetve területi vizsgálatokat végez. A tematikus vizsgálatok során a vizsgálat adott adatkezelői körre, mint a bankok, a biztosítók, vagy az egészségügyi szolgáltatók egyes adatkezelési folyamataira terjed ki. Az adatvédelmi biztos az eljárása során az adatkezelőtől minden olyan kérdésben felvilágosítást kérhet, amely a vizsgálat szempontjából releváns lehet. Az adatvédelmi biztos az általa vizsgált ügyben eljáró munkavállalót, illetve az adott szervezet bármely alkalmazottját meghallgathatja. Az érintett személy a meghallgatás során a nyilatkozattételt akkor tagadhatja meg, ha magát vagy közeli hozzátartozóját a beadvány érinti, illetve, ha magát vagy közeli hozzátartozóját bűncselekmény elkövetésével vádolná. Az adatvédelmi biztost az eljárása során az államtitok és a szolgálati titok nem akadályozhatja, de a betekintési jogát csak személyesen gyakorolhatja.

Az adatkezelési vizsgálatok megállapításait, esetleges kifogásait az adatvédelmi biztos az érintett adatkezelő tudomására hozza. Abban az esetben, ha jogellenes adatkezelést állapít meg, akkor felszólítja az adatkezelőt az adatkezelés megszüntetésére. Ha az adatkezelő a kérdésben megfogalmazott

határidőn belül nem tenne eleget a felszólításnak, akkor az adatvédelmi biztos tájékoztatja a nyilvánosságot az adatkezelés tényéről, a kezelő személyről és a kezelt adatok köréről. Az adatvédelmi biztos élhet az ombudsmani törvényben rögzített eszközökkel, így ha jelentősebb visszaélés megállapítására került sor, akkor a biztos a nyilvánosság számára is közzétett ajánlásban fogalmazza meg érdemi álláspontját. Az érintett adatkezelőnek kötelessége, hogy az ajánlásban foglaltaknak a teljesítéséről 30 napon belül tájékoztatást adjon az adatvédelmi biztos számára. Ha államigazgatási szervet érint az adatkezelés kifogásolása, akkor az adott szervezetnek kötelessége, hogy az adatvédelmi biztos ajánlását az ellenvéleményével együtt a felettes szervéhez megküldje.

Ahogy a korábbiakban már jeleztem az Avtv.. 2003. évi módosítása az adatvédelmi biztosi intézményt a klasszikus ombudsmani szerepkörből kimozdította, és azt hatósági jellegű eszközrendszerrel hatalmazta fel. Az intézmény jellegének a megváltozása egyrészt jogharmonizáció szempontjából, másrészt alapjog védelmi okból vált kívánatossá. Az adatvédelmi biztos vizsgálata kiterjed a piacgazdaság magántulajdonban álló gazdasági, kereskedelmi célú adatkezeléseket végző vállalkozásaira, de anélkül, hogy a vizsgálatának eljárási rendjét, illetve a megállapításai jogszerűségét bírósági eljárásban jogvita tárgyává lehetett volna tenni. A jogbiztonság követelményeinek teljesítése érdekében szabályozni kellett, hogy az adatkezelés jogellenességének megállapítása esetén az adatvédelmi biztosnak milyen eszközei, illetve az adatkezelőnek milyen jogai vannak. Az Avtv. 2003-as módosítása során lefektetésre került, hogyha az adatkezelő vagy az adatfeldolgozó a személyes adatok jogellenes kezelését nem szünteti meg, akkor az adatvédelmi biztos elrendelheti a jogosulatlanul kezelt adatok zárolását, törlését vagy megsemmisítését, valamint felfüggesztheti az adatok külföldre történő továbbítását is. Az adatvédelmi biztos határozata ellen közigazgatási úton további jogorvoslatnak helye nincs. Abban az esetben, ha az adatkezelő vitatja a biztos határozatának megalapozottságát, akkor a határozat kézhezvételét követő 30 napon belül kérheti annak felülvizsgálatát

jogszabálysértésre hivatkozással az illetékes bíróságtól. Az Avtv. 2005. évi módosításakor került a törvényszövegbe beillesztésre, hogy a közigazgatási perekre irányadó szabályok szerint kell a felülvizsgálat során eljárni.

Az adatvédelmi biztosnak az átalakult szerepköre több törvényi hiányosságot tükröz még, mivel egyrészt a vizsgálatának részletes szabályai, illetve a határozatának kötelező tartalma nem került megállapításra. Az adatvédelmi biztos által alkalmazható szankciók köre meglehetősen szegényes, mivel abban az esetben, ha az adatkezelő nem fordul bírósághoz, és továbbra sem szünteti meg a jogellenes adatkezelését, akkor az adatvédelmi biztos nem szabhat ki pénzbírságot. Az adatvédelmi biztosnak nincs jogköre arra, hogy az adatkezelési jogszabályokat rendszeresen és súlyosan megsértő vállalkozásokat gazdasági tevékenységükben korlátozza.

Az adatvédelmi törvénybe a 2003-as módosítása során kerültek beiktatásra az előzetes ellenőrzésre vonatkozó szabályok. Az adatvédelmi biztos egyes adatkezelések esetén azoknak az adatvédelmi nyilvántartásba vételét megelőzően előzetes ellenőrzést végezhet. Új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően az adatvédelmi biztos előzetes ellenőrzést végezhet az országos hatósági, munkaügyi és bűnügyi adatállományok kezelése tekintetében, a pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelései, illetve a távközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezelései vonatkozásában. Az adatvédelmi biztos előzetes ellenőrzési eljárást folytathat le a külön törvényben meghatározott egyedi statisztikai adatokat tartalmazó adatállományok kezelése esetében is. Az adatkezelőnek az új adatállomány feldolgozására vagy az új adatfeldolgozási technológia alkalmazására irányuló szándékát a tevékenység megkezdését megelőzően 30 nappal be kell jelentenie az adatvédelmi biztosnak. Az adatvédelmi biztos az előzetes ellenőrzésre vonatkozó igényét a bejelentéstől számított 8 napon belül köteles jelezni az adatkezelőnek, és az adatvédelmi biztos az ellenőrzést 30 napon belül köteles



elvégezni. Az adatkezelő a feldolgozást csak az adatvédelmi biztos előzetes ellenőrzésének befejezése után kezdheti meg. Az ellenőrzés alapján az adatvédelmi biztos a kezelendő adatok körének, illetőleg az adatfeldolgozás módszerének megváltoztatására hívhatja fel az adatkezelőt.

Az adatvédelmi biztos feladatkörébe tartozik az adatvédelmi nyilvántartás vezetése, amely valójában az adatkezelők nyilvántartásának tekinthető. Az adatvédelmi nyilvántartás jogintézménye már az Avtv.. eredeti törvényszövegében is megtalálható volt. A módosítások több tekintetben az adatvédelmi nyilvántartásba történő bejelentendő adatok körét érintették. Az Avtv.. 28.§ (1) rendelkezése szerint a személyes adatokat kezelő adatkezelő köteles e tevékenysége megkezdése előtt az adatvédelmi biztosnak nyilvántartásba vétel végett bejelenteni az adatkezelés célját, az adatok fajtáját és kezelésük jogalapját, az érintettek körét, az adatok forrását, a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, az egyes adatfajták törlési határidejét. Abban az esetben, ha van adatkezelő adatfeldolgozót bíz meg, akkor az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét is be kell jelenteni. Ha az adatkezelőnek kötelező a belső adatvédelmi felelős kinevezni, akkor az ő nevét és elérhetőségi adatait is be kell jelenteni. Ha jogszabály rendeli el az adatkezelést a szabályozás tárgya szerint illetékes miniszter, országos hatáskörű szerv vezetője, illetőleg a polgármester, főpolgármester, a megyei közgyűlés elnöke köteles azt bejelenteni a jogszabály hatálybalépését követő 15 napon belül. Az adatkezelő az első nyilvántartásba vételkor nyilvántartási számot kap, amelyet az adatok minden továbbításánál, nyilvánosságra hozásánál és az érintettel történő levelezés során, illetve az adatok kiadásakor fel kell tüntetni.

## 9. FEJEZET: A MAGYAR ALKOTMÁNYBÍRÓSÁG ADATVÉDELMI VONATKOZÁSÚ ÍTÉLETEI

A hazai adatvédelmi jog kialakulásában az Alkotmánybíróságnak meghatározó szerepkör jutott. Valójában az Alkotmánybíróság 15/1991. (IV.13) határozatában az Országgyűlés számára előírta a magyar adatvédelmi törvény rendelkezéseit. Az Alkotmánybíróság által meghatározott elméleti modellben került megfogalmazásra az információs önrendelkezési jog tartalma, az információs szabadsággal fennálló kapcsolata, illetve a két alapjog együttes védelmére rendelt ombudsmani koncepció.

### 9.1. A személyi számról

A személyes adatok védelmével kapcsolatosan az Alkotmánybíróságnak már a működése kezdetén<sup>181</sup> állást kellett foglalnia. Az indítványozók az országgyűlési képviselők választásáról szóló 1989. évi XXXIV. törvénynek az ajánlószevevények tartalmára vonatkozó rendelkezései miatt kérték alkotmányellenesség megállapítását. Álláspontjuk szerint a támadott rendelkezések sértik a magántitok és személyes adatok védelmének alapjogát, illetve a választások titkosságát. Az Alkotmánybíróság a kérelmet azon indok alapján utasította el, mert ugyan mindenkit megillet a magántitok és a személyes adatok védelméhez való jog, de ez a jog nem abszolút érvényű, és indokolt esetben ezek az alapjogok arányosan korlátozhatók. A személyes adatok védelme nem arra vonatkozik, hogy az érintetten kívül soha, senki semmiféle okból és semmilyen körülmények között nem ismerheti meg a személyes adatokat. Az Alkotmánybíróság szerint a korlátozás akkor alkotmányos, ha a személyes adatok védelme alapjogának korlátozása más alapvető jog érvényesülése miatt szükséges<sup>182</sup>. A választáshoz való alapjog

---

<sup>181</sup> 2/1990. (II.18.) AB határozat

<sup>182</sup> Az alapjog korlátozás okai: Alk. 8§ (3) állam biztonsága, a belső rend, közbiztonság, a közegészség, a közérkölc, vagy mások alapvető jogainak és szabadságának a védelme. Az Alk. ezen rendelkezését azóta felváltotta a lényeges tartalom korlátozhatatlanságának tilalma. (1990: tv. 3§)

érvényesülése indokolja a személyes adatok korlátozását, mivel az ajánlószelvényen szereplő személyes adatok ellenőrzésével a választási visszaélések megakadályozhatók. Az alkotmánybírók többsége szerint az egyéni választókerületi rendszerben a választópolgároknak az ajánlószelvényen fel kell tüntetniük személyes adataikat, hogy az ajánlás hitelessége ellenőrizhető legyen. Az ajánlószelvény léte szükséges ahhoz, hogy mind a választópolgár mind a jelölt politikai jogait gyakorolhassa, és továbbá a jelölt jogosultságait igazolhassa. Mivel nem kötelező a választópolgároknak az ajánlószelvény átadása a jelöltek számára, így nem sérül az információs önrendelkezés alapelve, mivel a polgár saját maga rendelkezik arról, hogy a személyes adatait rögzítő ajánlószelvényt odaadja-e valamely jelöltnek.

Sólyom László a határozat különvéleményében megfogalmazta a személyes adatok védelmének a tartalmát: "Az Alkotmány 59.§-a szerint a Magyar Köztársaságban mindenkit megillet a személyes adatok védelméhez való jog. Ennek a jognak a tartalma, hogy mindenki maga rendelkezik személyes adatainak a feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csak az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát". Sólyom László szerint a korlátozásnak nemcsak az Alkotmányban meghatározott okokon kell nyugodnia, hanem az állam akkor nyúlhat egy alapvető jog korlátozásához, ha más alapjog érvényesülésének csak ez az útja, továbbá a korlátozás a végső eszköz az alapjog érvényesítéséhez. A korlátozás mértékének a cél eléréséhez szükséges és arányos mértékűnek kell lennie." Sólyom László azért nem támogatta a határozatot, mert szerinte az ajánlószelvényen feltüntetett személyes adatok köre túlságosan széles körben lett meghatározva, és ezzel az alapjog korlátozásának az egyik feltétele az arányosság követelménye sérült, mert az ajánlószelvény ellenőrzéséhez nem elengedhetetlenül szükséges a személyi szám, a lakcím, és a választói nyilvántartási sorszám adatai. Sólyom szerint az

ellenőrzés alapjául szolgáló adatok eltúlzott mértékben történő meghatározása „a túlbiztosítás” kétélű fegyver, mert a nyilvánosságra került személyes adatokkal kapcsolatosan a visszaélés veszélye is megnőtt.

A személyes adatok védelmével kapcsolatosan az Alkotmánybíróság a 11/1990 (V.1.) határozatában hozott újra döntést. Az indítványozó kérelmére az Alkotmánybíróság a cégbejegyzésről és cégnyilvántartásról szóló 13/1987 (XII.16.) IM rendeletnek a személyi szám feltüntetésére vonatkozó rendelkezéseit megsemmisítette. Az indítványozó sérelmezte, hogy a gazdasági társaságot alapító tagok személyi számát is fel kell tüntetni a cégbejegyzési kérelmeken. Mivel a cégbejegyzés alapjául szolgáló adatok nyilvánosak, így az iratokon szereplő adatok, és ezzel együtt a személyi számok is nyilvánossá válnak. Az Alkotmánybíróság szerint a személyi szám közlésének és nyilvánosságra kerülésének rendelettel való előírására az igazságügy miniszternek nem volt törvényes felhatalmazása. A személyi szám nyilvános használatának kötelező elrendelése a személyes adat védelméhez fűződő alapvető jog (Alkotmány 59. §) gyakorlásának korlátozása. Ilyen tartalmú rendelkezést miniszteri rendelet nem írhat elő. Ezen formai okok miatt a támadott rendelkezések alkotmányellenességét állapította meg az Alkotmánybíróság. Az indítvány először vetette fel a személyi szám alkotmányossági kérdését is. Az Alkotmánybíróság úgy nyilatkozott, hogy „a személyi szám az állampolgár személyazonosítására szolgáló adat. E jogszabályi rendelkezésből azonban nem következik az, hogy a személyi szám a személyek azonosításának egyedüli eszköze. Csupán az azonosításra, az adott követelményekhez képest, más adatok is megfelelőek és elégségesek lehetnek. A személyi szám önmagában is adatokat tartalmaz az állampolgár személyére, általa más, ugyancsak a személyi számot tartalmazó nyilvántartási rendszerhez kapcsolódva pedig az elérhető személyi információk köre különösen kitágulhat. Mindezekre tekintettel a személyi számot is olyan személyes adatnak kell tekinteni, amelynek védelméhez való

jog, a Magyar Köztársaság Alkotmányának 59. §-a szerint, mindenkit megillet<sup>183</sup>”.

A 18/1990. (VIII.1.) AB határozatban az Alkotmánybíróság megsemmisítette a cégbejegyzésről és cégnyilvántartásról szóló 13/1987. (XII.16.) IM rendeletnek azon szabályait, amelyek előírták, hogy a cégjegyzést ellátó személyek tekintetében is fel kell tüntetni a személyi számot. A jogszabály támadott rendelkezéseinek a megsemmisítését azon okok indokolták, amelyek a 11/1990 (V.1.) AB határozat alapjaként szerepeltek.

A magyar adatvédelem alapjainak a lerakása és a dogmatikai rendszer kialakítása a 15/1991. (IV.13.) határozatban történt meg „... a személyi szám határozat közvetlen jelentésében az adatvédelemnek kissé ismétlős, ódivatú felfogását képviselte talán már létrejöttekor is, az újabb fejlemények mégsem teszik a határozatot múzeumi darabbá. Maradéktalanul időszerűek lesznek a célhoz kötöttségről, a készletező adatgyűjtésről, az információs hatalommegosztásról, az adattovábbításról, a nyilvánosságra hozatalról, az adatbiztonságról, és főként a polgárok önrendelkezési jogáról mondtak.”<sup>184</sup>

Az Alkotmánybíróság a 15/1991. (IV.13.) határozatában a személyes adatok védelméhez való jog új fogalmát használta, e jog lényegét: az érintett beleegyezését az adatkezelésbe, azaz az adatai feletti rendelkezést megragadva információs önrendelkezési jogként definiálta. E alapjognak szoros kapcsolata van az emberi méltósághoz való joggal, mert a személyes adatok hiányos védelme és az adatok jogi garanciák nélküli továbbítása sérti az érintett önrendelkezést, és ezzel együtt az emberi méltóságát is. Az egyének információs önrendelkezési jogának védelmét az államnak biztosítania kell, és az Alkotmány alapján a magán illetve az állami adatkezelésekbe törvényi erővel jogi garanciákat kell beépíteni. Az információs önrendelkezés alapjogát

---

<sup>183</sup> 11/1990 (V.1) AB határozat

<sup>184</sup> 15/1991. (IV.13.) AB határozat

garancia rendszernek kell biztosítania, azon alapelv szerint, hogy mindenki önkéntesen rendelkezhesse saját adatainak a felhasználásáról, illetve azok feltárásáról. Ha kivételesen mégis az érintett beleegyezése nélkül kerül sor az adatkezelésre, akkor az alapjog korlátozása nem sértheti e jog lényeges tartalmát. Az érintett számára biztosítani kell, hogy megismerhesse azt, hogy ki, milyen célból, hogyan kezeli a személyes adatait. Az információs önrendelkezési jog korlátozása csak akkor alkotmányos, ha arra más alapjog érvényesülése céljából van szükség. „Az államigazgatás hatékonysága nem lehet ilyen érdek, mert nem bizonyítható, hogy az információs önrendelkezési jog súlyos sérelmével járó adatfeldolgozás az egyetlen lehetséges útja a hatékony államigazgatásnak<sup>185</sup>”.

Az információs önrendelkezési jog lényeges tartalmi eleme, hogy az érintettnek olyan információkkal kell rendelkeznie a személyes adatai kezeléséről, amelyek alapján megítélheti, hogy az adatkezelés hogyan hat jogaira, illetve az adatkezelés teljes folyamata során biztosítani kell, hogy az adatközlő megismerhesse, hogy ki, hol, mikor, milyen célra használja el az adatait. Az információs önrendelkezési jog egyik legfőbb garanciája, mondhatni pillére függetlenül attól, hogy az adatközlés önkéntes volt, vagy kényszerű a „célhoz kötöttség” alapelve. Az információs önrendelkezési jog e legfőbb biztosítékának az adatkezelés teljes folyamatában fent kell állnia. Az adatkezelés célját előre pontosan meg kell határozni, és ha e cél megváltozik, arról az érintett értesíteni kell. Az adatkezelés céljának meghatározása csak törvényi formában történhet, és e jogforrási szinten kell biztosítani, hogy az adatkezelés körébe tartozó adatok mennyisége és minősége a célok elérésére alkalmasak legyenek, mert a meghatározott cél nélkül „készletre” történő adatgyűjtés illetve tárolás az alapjog sérelmét okozza. Az információs önrendelkezési jog akkor valósul meg, ha az érintett valóságban is rendelkezhet az adatról, e jog magába foglalja azt, hogy betekinthesse a róla készült nyilvántartásokba, kérheti adatainak a helyesbítését, illetve törlését, ha

---

<sup>185</sup> 15/1991. (IV.13.) AB határozat

az adatkezelés célja megszűnt. Az érintett jogának ki kell terjednie arra, hogy megtilthassa az adatainak nyilvánosságra hozatalát persze a törvényekben meghatározott egyes kivételektől eltekintve.

Az információs önrendelkezési jog további biztosítéka az adattovábbítás és adatok nyilvánosságra hozásának korlátozottsága. Az adattovábbítás körében az adatkezelő meghatározott harmadik személy számára az adatot hozzáférhetővé teszi. Az adattovábbítás fogalmának két értelmezését adja az Alkotmánybíróság. A szűkebb értelmezés szerint az adattovábbítás azt jelenti, hogy az adatkezelő számára a meghatározott személy hivatali vagy üzleti viszony alapján rendszeresen végzi az adatfeldolgozást, míg a tágabb értelmezés szerint az adattovábbítás adatbázisok közötti adatáramlást jelent. A második esetben az adattovábbítás csak akkor lehet alkotmányos, ha a célhoz kötöttség biztosítéka az adatkezelés további folyamatában is fennáll, illetve az adatbázisok összekapcsolását az adatkezelők törvényi felhatalmazás alapján vagy az érintett beleegyezésével tették. Az adattovábbítás alanyai között különbséget kell tenni aszerint, hogy az adatkérő az igazságszolgáltatás, az államigazgatás körébe vagy azon kívülre tartozik. Ha az igazságszolgáltatás vagy a közigazgatás körébe tartozó adatkérő az adatot a feladatának teljesítéséhez igényli, akkor nem sérül a célhoz kötöttség elve, mert az adott szervezet működési célja behatárolja, hogy milyen jellegű adatot kérhet, de teljesülnie kell annak a követelménynek, hogy az adat útja nyomon követhető legyen. E szélesen felfogott adattovábbítás már közel áll az adatok nyilvánosságra hozatalához, amely azt jelenti hogy bármely harmadik személy az adatot megismerheti. Az adatok nyilvánosságra hozatala során is érvényesülnie kell a célhoz kötöttség elvének. A személyes adatok nyilvánosságra hozatalára vonatkozó általános felhatalmazás tilos, mert ilyen adatokat csak akkor lehet nyilvánosságra hozni, ha a cél anonimizált adatokkal nem érhető el. Az Alkotmánybíróság további követelményként rögzíti, hogy szükséges az adatvédelem független ellenőrzése.

A személyes adatok védelmének második pillére az állami osztott információs hatalom elve. Az állami szférában igen sok célból gyűjtenek és tárolnak adatokat a polgárokról. Egységes személyi számmal az adatbázisok összekapcsolhatók, és egyenlőtlen kommunikációs helyzetet teremtenek, mert az érintettől származó nagy mennyiségű adat kiszolgáltatottá teszi az egyént az állami adatkezelő apparátussal szemben. Ebben a helyzetben az államigazgatás hatalma mértéktelenül megnő. Az információs hatalmat korlátozni kell azzal az eszközzel, hogy univerzális személyi szám nem használható az állami szférán belül.

Az adatfeldolgozással szembeni további alkotmányos követelmény, hogy az ne legyen parttalan, ellenőrizhetetlen, és határozatlan ideig tartó. A parttalan adatkezelés azzal küszöbölhető ki, hogy ha az adatkezelés körébe tartozó érintettek személyi köre és adatok egyértelműen fel vannak sorolva. Mivel az érintettek joga, hogy az adatainak feldolgozását ellenőrizhesse ezért az adatkezelés teljes folyamatában dokumentálni kell az adatforgalmat. Az alkotmánybírósági határozat azokat az adatkezelési formákat is felsorolta, amelyek egyértelműen sértik az információs önrendelkezési jogot. Ilyen eset, ha az adatkezelő több a vagyoni vagy az egészségi állapotra vonatkozó adatbázis összekapcsolásával, kiragadott adatok alapján „személyiség profilt” alkot, és tesz döntésének alapjául. Az emberi méltóságot súlyosan sérti „a családfa program” is, ha a személyi számok összekapcsolásával olyan távoli rokoni szálakat fednek fel, amely az ismert rokoni kapcsolatoktól teljesen független összefüggéseket mutat ki. Az alkotmányos követelmények szerint az sem megengedhető, hogy olyan speciális nyilvántartások jöjjenek létre, amelyben az az adatgyűjtés szempontja, hogy egy adott helyen kik tartózkodnak.

Az Alkotmánybíróság 29/1994. (V.20.) AB határozatban a személyi adatok védelmével kapcsolatosan több indítványt együttesen bírált el. A határozat megismétli a 11/1990. döntésben foglaltakat, azaz a személyi számra is



érvényesül a személyes adatok védelmére vonatkozó védelem. A szabálysértési törvény elrendelte az elkövető személyi adatainak a feltüntetését az iratokon, de a törvény részletesen nem sorolta fel a személyes adatok körét. Az Alkotmánybíróság alkotmányellenessé nyilvánította ezt a gyakorlatot, hogy a hatóságok a szabálysértési határozatokon feltüntetik az elkövető személyi számát. A megbiztosítási kártyán szereplő adatok rendeleti szinten történő meghatározása miatt formai alkotmányellenességet állapított meg az Alkotmánybíróság. A formai okon kívül az Alkotmánybíróság azt is megállapította, hogy a megbiztosítási igazolványon szereplő személyi szám feltüntetése olyan helyzetet teremt, amelyben lehetetlen annak a követelménynek a teljesítése, hogy az érintett nyomon tudja követni, hogy a személyi száma hol és ki által kerül megismerésre, ezzel az információs önrendelkezési jog lényege sérül. Az Alkotmánybíróság szerint az is Alkotmányba ütközik, ha egy célra több személyazonosító jelet alkalmaznak.

Az Alkotmánybíróság a 46/1995. (VI.30.) AB határozatával a személyazonosító jel (személyi szám) alkalmazásának időbeli meghosszabbítását tiltotta meg. Az indítványozó sérelmezte, hogy a jogalkotó 1999. december 31-éig meghosszabbította a személyi szám alkalmazását, és az adatkezelés körében feljogosította a közigazgatási szerveket, bíróságokat, ügyészségeket, hogy az egymás szerveivel történő kapcsolattartás és adattovábbítás során is használhatják a személyi számot. Az Alkotmánybíróság szerint a támadott jogszabályok olyan helyzetet eredményeznek az adatkezelés, és adatáramlás területén, amelyet az Alkotmánybíróság már 1991-ben alkotmányellenesnek ítélt. Az indítványozó által sérelmezett jogszabályok az információs önrendelkezés garanciális elemeit: az adatkezelés célhoz kötöttségét, az osztott információs rendszerek alkotmányos követelményét, és az adattovábbítás meghatározott feltételekhez kötését tette teljesen semmissé. Az Alkotmánybíróság azt is megállapította, hogy a támadott előírások figyelmen kívül hagyják a korszerű adatvédelmi törvény rendelkezéseit is. Az információs önrendelkezés jog lényeges

tartalmát az adatkezelés ellenőrizhetőségét üresíti ki a személyi szám közigazgatási szervek között folyó parttalan adattovábbítása, mivel az érintett ellenőrzési jogát, az őt érintő adattovábbításokról, nem tudja gyakorolni. Ha a közigazgatási szervek az egymással folyó kapcsolattartásra, és adatátadásra a személyi számot használhatnák, akkor az adatok útja követhetlenné válna. A személyi szám használatának meghosszabbítása azért is alkotmányellenes, mert már kiépültek az ágazat specifikus azonosító számok, a személyi szám használata már egy meglévő azonosító szám alkalmazásával együtt történne, amely az Alkotmánybíróság szerint alkotmányellenes. Az Alkotmánybíróság döntésében vizsgálta az információs önrendelkezési jog korlátozhatóságát. A határozat kijelentette, hogy "kivételesen a törvény elrendelheti a személyes adat kötelező kiszolgáltatását, és előírhatja felhasználásának módját is. Az ilyen törvény azonban korlátozza az információs önrendelkezés alapvető jogát, ezért csak akkor alkotmányos, ha megfelel az Alkotmány 8.§-ában megkövetelt feltételeknek<sup>186</sup>". Az Alkotmánybíróság megállapította, hogy a külső-, belső pénzügyi egyensúlyi helyhez javítása, a tartós gazdasági növekedés feltételeinek a kibontakoztatása, azaz a célzott vagy ígért gazdasági növekedés ugyan a közérdek fogalma alá sorolható be, de nem olyan indok, amely egy alapvető jog korlátozásának hivatkozási alapja lehet.

## 9.2. A vagyonynyilatkozatra kötelezésről

A 20/1990 (X.4.) határozatában az Alkotmánybíróságnak arra kellett választ adnia, hogy alkotmányos-e az egyes állami és pártvezetők vagyonynyilatkozattételre kötelezése. Az indítványozó szerint alkotmányellenes, hogy a törvényhozó a vagyonynyilatkozattételi kötelezettséget kiterjeszti a társadalmi szervezetek és a pártok országos vezetőire is. Az Alkotmánybíróság visszamenőleges hatállyal a sérelmezett jogszabályt megsemmisítette. Az alkotmányellenesség megállapításának az indokai között szerepelt, hogy az

---

<sup>186</sup> 46/1995. (VI.30.) Ab határozat

állami tisztviselők a közérdek tisztasága és a korrupció megelőzése érdekében vagyonyilatkozat-tételre kötelezhetők, de állami tisztséget nem viselő párt és társadalmi szervezetek országos vezetői tekintetében a magántitok és a személyes adatok védelméhez való jog korlátozása aránytalan mértékben történik a vagyonyilatkozat-tételi kötelezettség előírásával, és az alapjog korlátozás indoka sem felel meg az Alkotmány követelményeinek. Ugyan kivételesen törvény elrendelheti a magántitok körébe tartozó adatok kötelező kiszolgáltatását vagy a személyes adatok körébe tartozó adat feltárását, de az alapjogok korlátozásának a törvényhozó által elérni kívánt cél fontosságával, és az okozott alapjogi sérelem súlyával összhangban kell állni. Azon személyek tekintetében, akik nem töltenek be állami tisztséget a vagyonyilatkozat-tételre kötelezés alkalmatlan és szükségtelen eszköz, amely ebben az esetben nem elégíti ki az arányosság kritériumát. Egy hobby egyesület vezetője tekintetében nem indokolható az állami korrupció elleni harc a vagyonyilatkozat-tételre kötelezéssel, mert van olyan állami eszköz (ügyészségi jogkörök, Állami Számvevőszék), amelyek ellátják a társadalmi egyesület és a pártok felügyeletét. Az Alkotmánybíróság e korai felfogása szerint a magántitok és személyes adatok védelméhez való jog tartalma az, ha mindenki maga rendelkezik a magántitkainak és személyes adatainak a feltárásáról és felhasználásáról. Az Alkotmánybíróság közös nevezőre helyezte e két jogot, mert álláspontja szerint az ember magántitkai, például a vagyoni állapota, egyben személyes adatnak is minősül. Az Alkotmánybíróság e döntésében a magántitok és személyes adatok védelméhez való jog fogalom használatához tért vissza, amelyet már a 2/1990 (II.18.) határozatában is alkalmazott. A két jog összeolvasztásának alapja tulajdonképpen maga az Alkotmány volt, mivel az alaptörvény egy normaszövegben rögzíti a két alapjogot. „A Magyar Köztársaságban mindenkit megillet a jó hírnévhez, a magánlakás sérthetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.”<sup>187</sup> A szakirodalom<sup>188</sup> szerint hiba, hogy az Alkotmány a

---

<sup>187</sup> Alkotmány 59§ (1)

<sup>188</sup> MAJTÉNYI László, *Az adatvédelem és az információs szabadság az Alkotmányban*, Acta Humana 1995.18/19, 96.

személyes adatok védelméhez fűződő alapjogot protektív jogként, azaz a polgárnak az állam által nyújtott védelemként fogalmazza meg. Valójában az államnak a polgárok információs önrendelkezési jogának megsértésétől tartózkodnia kell. Az államnak ezt a be nem avatkozási kötelezettségét az Alkotmány szövegének is tükröznie kellene. Valószínűleg Sólyom László a határozathoz csatolt különvéleményében nem véletlenül használta a "mindenkit megillető személyes adatok védelméhez való jog" fogalmát. Majtényi László álláspontja szerint<sup>189</sup> ekkor még az Alkotmánybíróság fogalom használata és dogmatikai rendszere még nem forrt ki. Az Alkotmánybíróság gyakorlatát 1992 őszétől az is befolyásolta, hogy október 27-i ülésnapján az Országgyűlés elfogadta a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi. LXIII törvényt. A megalkotott törvény sok tekintetben követte az Alkotmánybíróság elvi irányvonalát. Ez nem is lehetett volna másképpen, mert Sólyom László még 1988-ban kidolgozta a később elfogadott adatvédelmi törvény alapelveit és annak rendszerét. Így magától értetődő, hogy az Alkotmánybíróság döntéseiben alkalmazza a törvényben meghatározott fogalmakat, de arra is volt példa, hogy kifejezetten eltért az Alkotmánybíróság a törvényi definícióktól<sup>190</sup>.

A 21/1993.(IV.2.) alkotmánybírósági határozat az adóellenőrzés eszközeként bevezetendő vagyonyilatkozat alkotmányossági kérdéseiről nyilvánított véleményt. A törvény a vagyonyilatkozat-tételi kötelezettséget minden jövedelemmel rendelkező személyre kiterjesztette anélkül, hogy valamilyen egyéb feltétel bekövetkeztétől vagy adófizetési kötelezettség mulasztástól függővé vált volna a vagyonyilatkozat- tételi kötelezettség keletkezése. Az adóhatóság a jogszabály alapján jogosítványt kapott volna arra, hogy megállapítsa azon személyek körét, akiknek vagyonyilatkozatot kell tenniük. A vagyonyilatkozat-tételi kötelezettségeket a támadott jogszabályok

---

<sup>189</sup> MAJTÉNYI László, „A megtalált alkotmány? Az alapjogi bíráskodás első kilenc éve, Az első alkotmánybíróság és az információs szabadságok”, Budapest, INDOK, 2000, 312.

<sup>190</sup> 60/1994. (XII.24.) AB a közérdekű adat fogalmát nem a törvényi fogalomként használta

kiterjesztették a kötelezett személy házastársára, az élettársára és a gyerekére is. Az Alkotmánybíróság megállapította, hogy ugyan a személyes adatok védelméhez fűződő jog lényeges tartalma nem sérül, és a korlátozást az arányos közteher viselése indokolhatja. De a szabályozás nincs tekintettel arra, hogy vagyonyilatkozat-tételre az a személy is kötelezhető, akinél nem merült fel az „adófizetési kötelezettség” gyanúja, így kényszerítő ok nélkül történik a személyes adatok védelméhez való jog korlátozása. Másrészt az általános vagyonyilatkozatra kötelezés, mint eszköz, alkalmatlan a törvényhozó által kitűzött cél elérésére, mivel ez a nyilatkozat is önbevalláson alapul, mint az adó bevallások megtétele az ellenőrzés korábbi szakaszában. Az Alkotmánybíróság megállapította, hogy a vagyonyilatkozat-tételre kötelezés nem olyan eszköz, amely az alapjog korlátozásának legkíméletesebb formája lenne. Az Alkotmánybíróság szerint alkotmányellenesség áll fent, mert az elérni kívánt cél fontossága, és az ennek érdekében okozott alapjogsérelem arányossága nem teljesül. Az Alkotmánybíróság kijelentette továbbá, hogy „a vagyoni helyzetre vonatkozó személyes adatok feltárására irányuló általános kötelezettség alkotmányos indokokkal nem támasztható alá”. Az Alkotmánybíróság megállapította továbbá, hogy az Alkotmány 2§(1) bekezdésében deklarált jogállamiság eszméjével is ellentétes a támadott szabályozás, mert „az adózó állampolgárokat az állammal szemben teljesen kiszolgáltatottá teszi.”<sup>191</sup> A határozat további érdekessége a köztisztviselőkre és a velük közös háztartásba élő hozzátartozókra vonatkozó vagyonyilatkozat-tételi kötelezettség 2001. évi hatályba lépése után az, hogy az Alkotmánybíróság a jogbiztonság sérelmét állapította meg azért, mert a vagyonyilatkozat-tételi kötelezettséget nem a házastársi vagyonközösség fennállásához, hanem a házastársi életközösség létezéséhez kötötte a jogszabály. Alkotmányossági aggályra adhat okot, ha a köztisztviselői jogállásáról szóló törvény 2001. évi módosítása a köztisztviselői vagyonyilatkozat-tétellel kapcsolatban, mert a köztisztviselő ezen

---

<sup>191</sup> 21/1993 (IV.2.) AB határozat

kötelezettsége kiterjed a vele közös háztartásban élő élettársára is, bár a Csjt főszabálya szerint köztük nem áll fent vagyonközösség.

### 9.3. A személyes adatok védelme a lelkiismereti szabadság biztosításáért

A művelődési és közoktatási miniszter alkotmányértelmezési kérelmére vonatkozóan az Alkotmánybíróság kifejtette: a vallás vagy más lelkiismereti szabadság kommunikációs alapjogi jellegéből következik, hogy mindenki szabadon nyilatkozhat vallási vagy lelkiismereti adatairól, de ezen felmérések során az önkéntességet és az anonimitást biztosítani kell. Az Alkotmánybíróság az információs önrendelkezési jognak a vallás és lelkiismereti szabadsághoz való kapcsolatáról kifejtette: „a vallás és más lelkiismereti meggyőződés az emberi méltóság és önrendelkezés egyik legbensőbb ügye, az információs önrendelkezési jog különösen érzékeny tárgya. Ezért az egyház saját híveire vonatkozó vallási tárgyú adatgyűjtésén kívül, más szervezett adatgyűjtés számára a vallási hovatartozás, illetve egyéb lelkiismereti meggyőződés az adatalany írásba foglalt hozzájárulása nélkül nem lehet személyes adat. Személyes adattá az egyént érintő információt a személyi azonosítás, illetve azonosíthatóság teszi.<sup>192</sup>” Majtényi László szerint az utolsó mondatnak téves az értelme, és helyesen úgy próbálja értelmezni, hogy a „jogellenes adatgyűjtés nem létező adatgyűjtés, a jogszerű nyilvántartásban meg talán a személyes adat megszűnik személyes adat lenni.<sup>193</sup>”

### 9.4. A személyes adatok védelme és a bírósági eljárások nyilvánossága

Az 58/1995. (IX.15.) AB határozatban az Alkotmánybíróság a magántitok és személyes adatok védelméhez fűződő jog viszonyát vizsgálta a büntetőeljárás

---

<sup>192</sup> 74/1992. (XII.28) AB határozat

<sup>193</sup> lásd 7. jegyzet 320. old.

elveinek érvényesülése tükrében. Az indítványozó sérelmezte, hogy a bíróságnak a terhelt elmeállapotáról beszerzett szakvéleményeket fel kell olvasnia. Az Alkotmánybíróság megállapította, hogy az indítvány alaptalan. A büntetőeljárás elvei: a közvetlenséget, és a tárgyalás nyilvánosságát kifejtő szabályok olyan előírások, amelyek az alapjog korlátozásának arányos és szükséges kritériumai. A bíróságok büntető ügyben ítéleteiket csak azon tények alapján hozhatják meg, amelyeket a tárgyalás anyagává tettek, azaz a bíró közvetlenül megvizsgált. A közvetlenség alapelvéből eredően a bizonyítás eszközéül szolgáló iratot fel kell olvasni a tárgyaláson. Mivel a beszámítási képesség megállapítása a bűnösség kimondásának egyik főkérdése, nem lehet eltekinteni az eljárás során a garanciális szabályok alkalmazásától. A bizonyítékok tárgyaláson történő ismertetése, egyrészt eszköz a büntető hatalom érvényesítésére, másrészt információt szolgáltat az eljárásban résztvevő magánfeleknek, hogy jogaikat gyakorolhassák, harmadrésben az igazságszolgáltatás működésének ellenőrzését szolgálja. A büntető eljárási szabályok ennek ellenére mégis lehetővé teszik, hogy konkrétan meghatározott okok esetén erkölcsi okból, az eljárásban részt vevő kiskorú védelme érdekében, az eljárásban részt vevő személyek vagy a tanú magánéletének védelme érdekében, az államtitok vagy szolgálati titok megőrzése végett a nyilvánosság kizárását a bíróság elrendelje, de ebben az esetben is nyilvánosan kell az ítéletet kihirdetni. Nincs akadálya annak, hogy bíróság döntse el, akár a nemzetközi egyezményekben<sup>194</sup> meghatározott okok figyelembevételével is, hogy a nyilvánosságot kizárja a tárgyalásról a felek magántitkainak a védelme érdekében.

## 9.5. Személyes adatok védelme formai okból

---

<sup>194</sup>Az emberi jogokról és alapvető szabadságokról szóló 1950 november 4.-én Rómában aláírt egyezményt Magyarországon az 1993:XXXI tv. hirdette ki.

A személyes adatok védelmével kapcsolatos következő ügyben az indítványozó azt sérelmezte, hogy a Művelődési Minisztérium 25/1988. (XII.22.) rendelete erkölcsi bizonyítvány benyújtását kívánja meg a felsőoktatási intézményekbe való felvételhez, és ez az előírás sérti a személyes adatok védelméhez fűződő jogát. Az Alkotmánybíróság megállapította az 1992. évi. LXIII. a személyes adatok védelméről szóló törvény (Avtv.) előírásainak a figyelembe vételével, hogy a büntetett előélet ténye különleges személyes adatnak minősül, mely akkor kezelhető, ha az érintett ahhoz írásban hozzájárult, vagy az adatkezelésre okot adó körülmény nemzetközi egyezményen alapul, vagy az Alkotmányban biztosított alapvető jog érvényesítéséhez szükséges okból, továbbá ha nemzetbiztonsági, bűnmegelőzési vagy bűnüldözési okból a törvény elrendeli. Az Alkotmánybíróság megállapította az Avtv. előírásainak a figyelembe vételével, hogy kormányrendelet sem kifejezetten, sem közvetve nem írhatja elő a büntetett életre vonatkozó adatok közlését, illetve kezelésének kötelezettségét. Ezért az Alkotmánybíróság formai okból a rendelet alkotmányellenességét állapította meg.

#### 9.6. Nemzetbiztonsági ellenőrzések adatvédelmi korlátairól

Az Alkotmánybíróság 16/2001. (V.25.) AB határozata abból a szempontból érdekes, hogy a jogállami keretek között működő titkosszolgálatok tevékenységét és a különlegesen érzékeny adatok gyűjtését vizsgálta. Az indítványozó a C típusú nemzetbiztonsági ellenőrzéshez kapcsolódó házastársi nyilatkozattal kapcsolatosan fejtette ki alkotmányossági aggályait, mert az indítványozó szerint a jogszabályi előírások a jogbiztonságot sértik, ha a Nemzetbiztonsági Szolgálat időbeli korlátozás nélkül gyűjthet az ellenőrzés alá vont személyről adatokat a házastársi nyilatkozat alapján. Az Alkotmánybíróság részletesen megvizsgálta a nemzetbiztonsági szolgálatokról szóló törvényt, továbbá a fontos és bizalmas munkaköröket betöltő személyek



biztonsági vizsgálatára vonatkozó előírásokat. Az Alkotmánybíróság a vizsgálat során megállapította, hogy a házastársi nyilatkozat járulékos jellegű, mert a kinevezni kívánt személy ellenőrzési nyilatkozatához kapcsolódik. Az alapintézmény vizsgálata során az Alkotmánybíróság azt is megállapította, hogy a politikai biztonság, a gazdasági és a honvédelmi érdekek védelme szempontjából indokolt a kockázati tényezők feltárása biztonsági ellenőrzéssel, mely során a személyes adatok védelméhez, és a magántitokhoz fűződő jogokat sért a Nemzetbiztonsági Szolgálat, de törvényi követelmény, hogy a biztonsági ellenőrzés során a körülményekhez képest mindig a lehető legenyhébb eszközöket kell alkalmazni. Az arányossági követelmények vizsgálata során az Alkotmánybíróság kijelentette, hogy az alapjog korlátozásának arányossági követelménye azzal teljesül, hogy különböző típusú adatlapok önkéntes kitöltésével a szolgáltatott adatok köre a munkakör bizalmas jellegéhez viszonyul, másrészt az ellenőrzés során különböző mértékben kerül sor a személyiségi jogok korlátozására. A törvényi előírások az Alkotmánybíróság szerint teljesítik az alapjog korlátozás arányossági követelményeit. A "célszemély" biztonsági vizsgálata során természetesen a közeli hozzátartozóinak a kapcsolatait is vizsgálják, hiszen ők vannak a "célszemélyhez" legközelebb. Az indítványozó által sérelmezett házastársi nyilatkozatot az Alkotmánybíróság tájékoztatásnak tekintette, amelyben a "célszemély" házastársa értesítve van arról, hogy a Nemzetbiztonsági Szolgálatok ellenőrzése ő rá is ki fog terjedni. Az a körülmény, hogy a célszemély biztonsági ellenőrzése kiterjed a házastársára az Alkotmánybíróság szerint "az állam méltánylást érdemlő érdeke, hogy a jelöltek ne csak személyükben, hanem közvetlen környezetükben se legyenek kitéve olyan kapcsolatoknak, amelyek által tevékenységük jogellenes céllal befolyásolhatóvá, illetve támadhatóvá teszi őket, és ezáltal a nemzetbiztonságot sértő vagy veszélyeztető helyzet keletkezzen"<sup>195</sup>

---

<sup>195</sup> 16/2001. (V.25.) AB határozat

Az Alkotmánybíróság ez évben hozott érdemi döntést<sup>196</sup>a magánszemélyek megfigyelhetőségének alkotmányossági feltételeiről. A sportról szóló 2000. évi CXLV. törvénynek a sport huliganizmusra vonatkozó részeit támadták az indítványozók, mivel ezen előírások sértik a személyes adatok védelméhez fűződő alkotmányos jogot. Az alapjog sérelmét abban látták az indítványozók, hogy a törvény lehetővé teszi a sportmérkőzések alatt a nézőközönség totális megfigyelését, függetlenül attól, hogy szabálysértés vagy bűncselekmény történt-e. A törvény lehetővé teszi a személyes adatoknak 30 napos tárolását, és megengedi, hogy ezek a felvételek szabadon átadásra kerüljenek a sportszervező társaságok között. Az Alkotmánybíróság megállapította az információs önrendelkezési jog korlátozhatóságát az emberi méltóság védelme érdekében, illetve, hogy a kamerás megfigyelés a bűnüldözés szempontjai miatt nem minősülnek az információs alapjog korlátozása szempontjából szükségtelennek és aránytalannak. A nézőközönségről készített felvételek esetében az Alkotmánybíróság többsége szerint maradéktalanul teljesül a célhoz kötöttség elve is, és a 30 napos adattárolási időhatár kielégíti a készletre történő adatgyűjtés tilalmát is. Az Alkotmánybíróság megsemmisítette azokat a szövegrészeket, amelyek a személyes adatok korlátozás nélküli áramlását tették volna lehetővé több felhasználói kör között. A döntéshez Kiss László és Kukorelli István különvéleményt fűztek, mivel álláspontjuk szerint a megsemmisítés hatályát szélesebb körben kellett volna meghatározni, mivel a mérkőzések alatti „totális megfigyelés” sérti az információs önrendelkezési jogot. A kamerás megfigyelés az információs hatalom kiterjesztését eredményezi, mivel nyilvános, de magánjellegű rendezvények helyszínén bűnüldözési célból felvételek készíthetők. A rendőrség kényszerintézkedésként készíthetett ilyen jellegű felvételt, de a sporttörvény alapján már részletes és teljes körű felvételekhez juthat. Az alkotmánybírók szerint alaposabb vizsgálatot igényelt volna, hogy a felvételek rögzítéséről rendelkező szabályok mennyiben korlátoznak alapvető jogokat, és az információs hatalomgyakorlás eszközeként a megfigyelés milyen hatásokat

---

<sup>196</sup> 35/2002. (VII.19.) AB határozat

válthat ki az alapjogokra. A különvéleményként az alkotmánybírák azt hangoztatták, hogy a kamerás megfigyelés már önmagában is alapjog korlátozást jelent, és ez a korlátozás fokozottabbá válik, ha a felvételeket rögzítik, tárolják, és továbbítják. A különvéleményt megfogalmazó alkotmánybírók szerint, bár a mérkőzések "veszélyes üzemnek" tekinthetők, de vannak más eszközök is, amelyekkel a személy- és vagyonbiztonság megóvható, így a kamerás megfigyelés az információs önrendelkezési jog szükségtelen korlátozásának minősül. Remélhetőleg a különvéleményben foglaltakat az Alkotmánybíróság többsége is álláspontjaként fogja elfogadni a későbbiekben.

#### 9.7. Közszerplők magánszférájáról

A 30/1997 (IV.29.) AB határozat érintőlegesen foglalkozik a személyes adatok védelmével, mert az indítvány az országgyűlési képviselők összeférhetetlenségi szabályait támadta, és csak mellékesen az országgyűlési képviselők vagyonyilatkozatainak az adatkezelési szabályait. Az indítványozók szerint az országgyűlési képviselők információs önrendelkezési jogát korlátozó törvény nem felel meg az alapjogok korlátozhatóságára vonatkozó követelményeknek, mert az információs önrendelkezési jogot a jogalkotó nem elkerülhetetlenül szükséges esetben és módon korlátozza, továbbá az alapjog korlátozása nem alkalmas a kívánt cél elérésére. Az Alkotmánybíróság a korábbi gyakorlatára támaszkodva kijelentette, hogy a személyes adatok védelméhez való jog nem abszolút jog, így a korlátozása megengedett ugyan, de az információs önrendelkezési jog korlátozásának meg kell felelnie az alapjogok korlátozására vonatkozó alkalmassági, arányossági és szükségességi követelményeknek. A korlátozás alkotmányosságának a megállapításához az Alkotmánybíróság a korlátozás terjedelmét és formáját vizsgálta. A képviselőket a vagyoni, érdekeltségi és személyes adataik tekintetében kötelezte a jogalkotó adatszolgáltatásra. Az érintetteket egyrészt a személyes adataik és magántitkaik vonatkozásában bejelentési, és

nyilatkozattételi kötelezettség terheli, másrészt ezen személyes adatok közül többet nyilvánosságra is kell hozni. A képviselők személyes adatainak a nyilvánosságra hozatalát az indokolja, hogy mivel az országgyűlési képviselők a politikai közéletben résztvevő személyek, ezért a választópolgároknak a közérdekű adatok megismeréséhez fűződő joga elsőbbséget élvez ezen személyek személyes adatainak a védelméhez fűződő jogához viszonyítva. Az országgyűlési képviselők személyes adatainak a feltárása addig indokolt, míg az adatok nyilvánossága a közszereplők tevékenységének megítélése szempontjából jelentőséggel bír. A képviselői vagyonynyilatkozatok adatkezelési szabályait vizsgálva az Alkotmánybíróság megállapította, hogy az indítványozók érvelése nem megalapozott, mivel a személyes adatok védelméhez fűződő jog nem sérül, mert az érintettek bármikor ellenőrizhetik, hogy milyen körben forognak a személyes adataik, mert a vagyonynyilatkozatok tartalmát csak az összeférhetetlenség ellenőrzése céljából a Mandátum Vizsgáló Bizottság keretein belül kezelik.

#### 9.8. Titkos nyomozati eszközök alkalmazásának alkotmányos keretei

Az Alkotmánybíróság 2007 januárjában a rendőrségi törvény, illetve a büntetőeljárásról szóló törvény több rendelkezését megsemmisítette<sup>197</sup>, mivel a titkos nyomozati eszközök alkalmazhatóságára vonatkozó szabályok sértik a jogállamiság követelményeit, másrészt aránytalanul és szükségtelenül korlátozzák a magánlakás sérthetlenségéhez, a magántitok és a személyes adatok védelméhez való jogot. Az Alkotmány a magánszférához való jogot az emberi méltósághoz való jog az 54.§ (1) bekezdésén keresztül az általános személyiségi jog részeként, annak egyes elemeit: a magánlakás sérthetlenségét, a magántitok és a személyes adatok védelméhez való jogot pedig az 59.§ (1) bekezdésében nevesített alapjogi védelem alá helyezi. A titkos módszerek és eszközök alkalmazása közvetlenül és szükségképpen a magánszféra legszorosabban vett tartományát, az egyéni autonómia

---

<sup>197</sup> 940/B/2003. AB határozat

kiteljesedésének terepet biztosító magánlakást, az ott folyó individuális tevékenységet és a magánlakás védelmével szorosan összefüggő magántitkot korlátozzák. A magánlakás sérthetlensége az emberi méltósághoz való jog konkretizálása, és kapcsolatban áll az emberi méltóság jogából levezett más kommunikációs jogokkal. Az információs önrendelkezési jognak lényeges eleme, hogy az érintett tudja, hogy a személyes adatait ki kezeli illetve, hogy kérelmére tájékoztatást kaphasson a kezelt adatok köréről, az adatkezelés céljáról és jogalapjáról, annak időtartamáról, továbbá az adattovábbítások köréről.

Az Alkotmánybíróság kijelentette, hogy az állam mint a közhatalom gyakorlója, és mint az igazságszolgáltatási monopólium birtokosa köteles a büntető igény érvényesítésére, és ennek érdekében a bűnüldözéshez hatékony eszközöknek kell rendelkezésre állnia. De a jogállamban a büntető közhatalom is korlátozott, ezért a bűnüldözés is csak szigorú anyagi és eljárási szabályok által meghatározott rendben folyhat. Az alkalmazott eszközök lehetnek súlyosan jogkorlátozóak, és a bűncselekmény elkövetőjén túl érinthetnek más személyeket is, de az alkalmazott alapjog korlátozásnak meg kell felelnie az arányosság és szükségesség követelményeinek.

Az Alkotmánybíróság áttekintette a titkosszolgálati eszközök alkalmazására vonatkozó jogszabályokat, amelyek jelenleg a büntetőeljárásról<sup>198</sup>, a rendőrségi törvényben<sup>199</sup>, a Vám- és Pénzügyőrségről szóló törvényben<sup>200</sup>, a Határőrségről<sup>201</sup>, az ügyészségről<sup>202</sup>, továbbá a nemzetbiztonsági szolgálatokról<sup>203</sup> szóló törvényekben találhatók. A felsorolt törvények rendelkezéseit több kormányrendelet szabálya egészíti ki. Bírói — illetve a nemzetbiztonságot érintő egyes kérdések esetén igazságügy-miniszteri — engedélyhez kötött eszközök: titkos kutatás és az észlelt technikai eszközzel történő rögzítése, magánlakásban történtek technikai eszközökkel történő

---

<sup>198</sup> 1998. évi XIX. törvény a büntetőeljárásról

<sup>199</sup> 1994. évi XXXIV. törvény a Rendőrségről

<sup>200</sup> 2004. évi XIX. törvény a Vám- és Pénzügyőrségről

<sup>201</sup> 1997. évi XXXII. törvény a határőrizetről és a Határőrségről

<sup>202</sup> 1972. évi V. törvény a Magyar Köztársaság ügyészségéről

<sup>203</sup> 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

megfigyelése és rögzítése, levél, postai küldemény, telefonvezeték vagy azt helyettesítő távközlési rendszer útján továbbított közlés tartalmának megismerése és technikai eszközzel történő rögzítése, internet vagy más számítástechnikai eszköz alkalmazásával történő levelezés útján továbbított adatok, információk megismerése és felhasználása. A technikai jellegű infiltrációra ebben az esetben nincsenek tilalmak. A Be. alapján alkalmazható eszközök közé tartoznak: a magánlakásban történtek technikai eszközökkel történő megfigyelése és rögzítése, levél, postai küldemény, telefonvezeték vagy azt helyettesítő távközlési rendszer útján továbbított közlés tartalmának megismerése, számítástechnikai rendszer útján továbbított és tárolt adatok megismerése és felhasználása.

A jogszabályok a titkosszolgálati eszközök alkalmazása szempontjából különbséget tesznek titkos információgyűjtés és titkos adatszerzés között. Az előbbire a nyomozás elrendelése előtt kerülhet sor, míg a büntetőeljárás szabályok szerint a nyomozás elrendelését követően kerülhet sor a titkos adatszerzési eljárás lefolytatására. Ha a nyomozás elrendelése előtt titkos információgyűjtés volt folyamatban, akkor azt a nyomozás elrendelését követően titkos adatszerzéssé kell átalakítani. A titkos információgyűjtés külső engedélyhez kötött eseteit a törvény meghatározza, amely jelenthet igazságügy miniszteri, illetve bírói engedélyezést. A Be kizárási szabályai szerint a titkos információgyűjtést engedélyező bíró nem lehet azonos az ítélező bíróval, illetve nem lehet azonos az egyes külön törvények alapján engedélyeket kiadó bírókkal. A kizárási szabályok ilyen alkalmazása azt eredményezte, hogy a titkos információgyűjtést követően a titkos adatszerzés engedélyezése során eljáró bíró nem ismerheti meg az ügy előzményeit, és így blankettaszerű felhatalmazást ad a titkos adatszerzés lefolytatására. Másrészt a titkos információgyűjtést lefolytató szervezet a titkos adatgyűjtés indítványozása során maga dönt arról, hogy a titkos információgyűjtés során keletkezett iratok közül, melyeket mutatja be a döntéshozónak.

Az Alkotmánybíróság arra való tekintettel, hogy a határozatai során eddig a nyílt eljárásokkal foglalkozott, megvizsgálta az Emberi Jogok Európai Bíróságának a rejtett nyomozásokhoz kapcsolódó ítélkezési gyakorlatát, többek között az általam is tárgyalt Klass ügyvéd és társai Németország<sup>204</sup> ellen lefolytatott ügyét. Az Emberi Jogi Bíróság határozataiban rámutatott azokra a minimális követelményekre, amelyeket a titkos nyomozati eszközök alkalmazása során minimálisan be kell tartani a nemzeti hatóságoknak. Arra tekintettel, hogy ezen eszközök alkalmazása a végrehajtó hatalomnak „beláthatatlan” lehetőségeket ad, elengedhetetlen, hogy maguk a precíz és részletes eljárási garanciák nyújtsanak biztosítékot az egyéni jogok védelmére. A normavilágosság követelményeinek megfelelő előírásoknak biztosítani kell, hogy a döntéshozó bíróság hatásköre, az intézkedések lényege, és azok gyakorlásának módja egyértelműen meghatározásra kerüljön. A minimális biztosítékok között határozta meg a Bíróság, hogy a titkos eszközök alkalmazásának az eseteit és feltételeit világosan meg kell határozni, továbbá az érintett személyi körnek előre meghatározottnak kell lennie. A minimális garanciáknak biztosítani kell a keletkezett dokumentációk megőrzését, és azoknak megóvását. A Bíróság álláspontja szerint a hatóságok nem kaphatnak széles mérlegelési jogot a titkos eszközök alkalmazása során. Az egyezményhez kapcsolódó bírósági gyakorlat megköveteli, hogy a titkos eszközök alkalmazására csak minősítetten súlyos esetben kerüljön sor akkor, ha a hagyományos nyomozati eszközök az ügy körülményei miatt hatástalanok. Az Alkotmánybíróság az Európai Emberi Jogi Bíróság álláspontját követve megerősítette, hogy a zárt eljárások esetén a szükségességi és arányossági követelmények teljesítését szigorúbb mércével vizsgálja, mint a nyílt eljárások esetén, mert ezen titkos eszközök alkalmazása rendkívüli hatalmat biztosít a hatóságok számára, és fokozottan kiszolgáltatottá teszi az érintetteket. Az Alkotmánybíróság a 16/2001. (V.25.) határozatában rámutatott arra, hogy a titkos és sajátos eszközöket alkalmazó nemzetbiztonsági szolgálatok azért igényelnek megfelelő szabályozást, hogy

---

<sup>204</sup> Case of Klass and Others v. Germany

semmilyen körülmények között ne jelenthessenek veszélyforrást a demokratikus jogrendre.

Az Alkotmánybíróság áttekintette több európai országban elfogadott szabályokat a titkos nyomozati eszközök alkalmazására, és az eltérő megoldási módok ellenére megállapítható, hogy a titkos eszközök alkalmazását általános és speciális feltételek egyaránt meghatározzák, de ezen feltételek teljesítése esetén is csak akkor lehet ezen eszközöket alkalmazni, ha a nyomozás hagyományos eszközeit várhatóan nem kielégítő eredménnyel lehetne alkalmazni. Az Alkotmánybíróság a kifogásolt szakasz vonatkozásában alkotmányellenességet állapított meg, mivel a titkos eszközök alkalmazásának Rtv. 69.§ (1)-(3) bekezdésében meghatározott különös feltételei nem értelmezhetők, mert maga a bűncselekmény, mint viszonyítási alap hiányzik, azért mert a titkos eszközök alkalmazását még el nem követett bűncselekményhez kapcsolja a törvény. A megelőzés pedig önmagában egy olyan általános felhatalmazás, amely alapján a titkos információszerzés határai tetszés szerint kiszélesíthetőek. A Rtv. 69§ (3) bekezdésében meghatározott fogalmak, mint „nemzetközi bűnözés, bűnös kapcsolat, szervezett elkövetéssel, fegyveres elkövetéssel” olyan fogalmak, amelyek tartalma nehezen tisztázható és bizonytalan, ezért azok nem tartoznak a normavilágosság követelményébe. A törvény hiányossága, hogy a bűncselekmény súlyosságát nem objektíve a szabadságvesztés tartamához, vagy konkrét bűncselekmény típushoz kapcsolódóan határozza meg, hanem ezen bizonytalan tartalmú fogalmakkal, így a titkos eszközök alkalmazása az indítványozók és az engedélyezők szubjektív megítélésétől válik függővé.

Az indítványban kifogásolt Be. 206. §-át az Országgyűlés 2006 júniusában módosította. Így az Alkotmánybíróság hatályon kívül helyezett jogszabályok alkotmányosságát csak olyan esetben vizsgálja, amikor bírói indítvány alapján felfüggesztett eljárásra tekintettel lehetőség van a konkrét ügyben való alkalmazási tilalom kimondására. Erre nézve az Alkotmánybíróság vizsgálta a



kifogásolt szakaszt és megállapította, hogy a titkos információszerzés és a titkos adatgyűjtés anyaga nem része a büntető iratoknak, ahhoz sem az ügyben dönteni jogosult bíró, sem a védelem nem fér hozzá. A vizsgált rendelkezés hatálya idején a bírósági irathoz a titkos információszerzés és a titkos adatgyűjtés anyagából az ügyész csupán néhány okirati bizonyítékot csatolt: a titkos adatszerzés engedélyezése iránti indítványt, a bíróság engedélyezéséről szóló határozatát és az adatszerzés végrehajtásáról szóló, de nem annak a végrehajtója által jegyzett jelentést. Ezek alapján a titkos adatgyűjtés lefolytatásának törvényessége rendkívül szűk körben, az alapjogok korlátozásának tényleges szükségessége és arányossága pedig egyáltalán nem volt ellenőrizhető. A jelentésből nem derült ki sem a résztvevőkre, sem az eszköz alkalmazásának időtartamára, helyszínére, illetve az engedéllyel érintett és a harmadik személy közötti kapcsolatfelvétel és kapcsolattartás terepére vonatkozó semmilyen adat. Az alkalmazás folyamatáról ez az okirat eltérő törvényi rendelkezés híján csupán a jelentés készítője által „szükségesnek ítélt mértékig” tartalmazott tájékoztatást. A titkos adatszerzéssé alakított titkos információgyűjtés anyagáról pedig az ügyben dönteni jogosult, s ennek során a bizonyítás törvényességének vizsgálatára is köteles bíróság számára semmilyen adatot nem kellett bemutatni, a törvény még tényleges megtörténtének igazolását sem kívánta meg. Az ügyben (a tárgyalási szakaszban) eljáró bírónak a vizsgált szabályozás idején nem volt módja annak ellenőrzésére, hogy a titkos adatszerzést megelőzően a titkos információgyűjtés a törvénynek megfelelően folyt-e, s arra is csak részlegesen, hogy a titkos adatgyűjtésnél az engedély kereteit nem lépték-e át. Az okirat, mint bizonyítási eszköz hiteltérdemlőségét sem ellenőrizhette, minthogy a titkos eljárás részleteire (az engedélyen, illetve az arról szóló jelentésen kívül) más adat nem állt rendelkezésére. Mindez különösen aggályossá vált akkor, amikor a titkos adatszerzés eredményét olyan személlyel szemben vagy olyan ügyben használták fel, akikre, illetve amelyekre az engedély eredetileg nem vonatkozott. Az eredetileg korlátozó értelmű szabály így a titkos eszközök büntetőeljárás felhasználásának újabb jogbiztonságot sértő elemévé vált.

A III. rész összefoglalása: a magyar információs önrendelkezési jog alapjogi fejlődése és Drittwirkung hatása

A magyar adatvédelmi jog kialakítása során az Alkotmánybíróság az adatvédelem területén meghatározó jogfejlesztői szerepkörben járt el. Míg az NSZK-ban a tartományi, és a szövetségi parlament által elfogadott adatvédelmi törvényhozásra reagált a német Bundesverfassungsgericht, addig a magyar Alkotmánybíróság határozataiban megalapozta az Európai Adatvédelmi Egyezményben rögzített, és a német alapjogvédelemben kialakított tartalommal az információs önrendelkezési jog hazai alkalmazását, mielőtt az Országgyűlés ezzel a jogalkotási kérdéskörrel foglalkozhatott volna. A magyar jogban az információs önrendelkezési jog fogalmi létrejöttétől, szakirodalmi megjelenésétől, valamint alkotmánybírósági értelmezésétől kezdve alapjogként került elfogadásra. Így az információs önrendelkezési jognak a jogállami keretek között érvényesülő információs hatalom megosztásban betöltött szerepe miatt az Országgyűlés is alapjogként definiálta, és emiatt az adatvédelem polgári jogi oldalának kibontására nem került sor. Az Alkotmánybíróságnak célkitűzése volt, hogy a 90-es években a magyar „jogállami forradalmat” megvalósítsa, és ebben az információs önrendelkezési jog kibontása, és kialakítása meghatározó lépés volt.

Véleményem szerint az információs önrendelkezési joghoz kapcsolódó alkotmánybírósági felfogás alapján az adatvédelmi normákkal kapcsolatosan nem is vetődhetett fel annak világos elkülönítése, hogy az állammal szembeni vertikális jogviszonyokban kell az információs önrendelkezési jog alapjogvédelmét kialakítani, míg a magánjog körén belül működő magánadatkezelőkre vonatkozó horizontális jogviszonyokban az adatvédelmi jog polgári jogi elvek alapján működő rendszerét kell megteremteni. A magyar jogban az Alkotmánybíróság döntései alapján az információs önrendelkezési

jog alapjoga a közjogi és a magánjogi viszonyokra is azonos tartalommal érvényesül. Így az információs önrendelkezési jognak, mint alapjog drittwirkung hatása egyformán érvényesül az adatkezelőkre, függetlenül attól, hogy az adatkezelők az érintettel vertikális (azaz alapjogi jogviszonyban) vagy horizontális (polgári jogi jogviszonyban) állnak. Az információs önrendelkezési jog közvetett drittwirkung hatása nem az Alkotmány által, hanem az adatvédelmi törvény, valamint az Alkotmánybíróság határozatai által került kialakításra anélkül, hogy felismerésre került volna annak alapjogi dogmatikai jellege. Az adatvédelmi biztos 1995-96-os beszámolójában a tisztességesség fogalmával kapcsolatosan kijelentette, hogy ugyan az „Avtv..-ben megtalálhatjuk a tisztességes és törvényes adatkezelésre vonatkozó követelményeket, amelyek szinte szó szerint megegyeznek az EU-irányelv és az ET-egyezmény rendelkezéseivel. A tisztesség fogalma azonban a magyar jogban kevésbé meghonosodott, szubjektív jellegű, meglehetősen képlékeny, számos értékelemet hordozó kifejezés, amelyet csak gondos mérlegeléssel vizsgálhatunk. Sem az Avtv., sem a többi vizsgált dokumentum nem tartalmaz eligazítást ennek mibenlétével, jogilag releváns definíciójával kapcsolatban. A jobb értelmezhetőség érdekében *etikai szabályzatokat* kellene alkotni egyes adatkezelési ágazatok számára. Az Irányelv is tartalmaz etikai kódexek kiadásával kapcsolatos rendelkezéseket”.<sup>205</sup> Az adatvédelmi biztosok a későbbi állásfoglalásaikban<sup>206</sup> a tisztesség fogalmára kizárólag, mint polgári jogelvként hivatkoztak, és tartózkodtak annak akár részbeni kibontásától is. Ha a tisztességesség elvének értelmezése során az információs önrendelkezési jog közvetett drittwirkung hatását felismerjük, akkor a normatartalom szubjektív jellege, és meglehetősen képlékenysége megszűnik, és a tisztességesség elvének szélesebb körű megfogalmazását és alkalmazását lehet elérni.

---

<sup>205</sup> Adatvédelmi Biztos 1995. évi beszámolója

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1995-96/I/1&dok=beszamolok\\_1996\\_3](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1995-96/I/1&dok=beszamolok_1996_3)  
(2010.02.21)

<sup>206</sup> Adatvédelmi Biztos 2001. évi beszámolója Tájékoztató a kép- és hangfelvételt rögzítő berendezések működtetésével összefüggő eddigi adatvédelmi gyakorlatról; [http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=636\\_H\\_2001](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=636_H_2001) (2010.02.21)

## IV. RÉSZ: A SEKTORÁLIS ADATVÉDELEM KÖZÖSSÉGI JOGI ÉS MAGYAR RENDSZERE

### 10. SEKTORÁLIS ADATVÉDELMI JOGALKOTÁS AZ EURÓPAI UNIÓBAN

#### 10.1. Adatvédelem a belső piac jogában

A technológiai fejlődésre válaszul már 1997 decemberében újabb adatvédelmi tárgyú irányelvet fogadott el az Európai Parlament és a Miniszterek Tanácsa. A 97/66/EK irányelv<sup>207</sup> személyes adatok feldolgozásának szabályait fektette le a magánszféra védelmében a telekommunikációs szektorra vonatkozóan, azzal a céllal, hogy a 95/46/EK irányelv alapvető jelleggel megfogalmazott szabályait konkrét előírásokkal a telekommunikációs szektorra is érvényesítsék. A szektorális adatvédelmi jogalkotás második lépcsőjére sem kellett sokáig várakozni, mert az on-line információs rendszerekben elkövetett személyes adatokkal való visszaélések növekvő társadalmi félelmeket okoztak, és az adatvédelem alapvető szabályainak a tagállamok nemzeti jogába történő beépítése nehezen alkalmazható az információs technológiák újonnan keletkező területeire.<sup>208</sup> Az Európa Parlament és a Miniszterek Tanácsa 2002. július 12-én fogadta el a személyes adatok feldolgozásának szabályairól és az elektronikus kommunikációban a magánszféra védelméről szóló 2002/58/EK irányelvet<sup>209</sup>, amely a korábbi szektorális irányelvet aktualizálta, és kiterjesztette hatályát minden elektronikai kommunikációs szolgáltatóra, ebbe beleértve az internet szolgáltatókat is. Az irányelv célja, hogy függetlenül az alkalmazott technológiától a tagállamokban azonos és magas szintű védelem legyen biztosítva a személyes adatok vonatkozásában.

---

<sup>207</sup> Az Európa Parlament és a Tanács 1997. december 15.-én elfogadott 97/66/EK irányelve a személyes adatok feldolgozásáról és a magánszféra védelméről a telekommunikációs szektorban EU O.J.L. 24-30.01.1998 1-8. old.

<sup>208</sup> Future Bottlenecks in the Information Society. <http://www.jrc.es/FutureBottlenecksStudy.pdf>; 2006.05.12.

<sup>209</sup> EU O.J. L. 31.07.2002 37-47 old. A tagállamok 2003. október 31-ig kaptak határidőt az irányelv nemzeti jogba történő átültetésére.

A belső piac jogában az elektronikus aláírás adatvédelmi vonatkozásai is szabályozásra kerültek, amelyek szorosan kapcsolódnak az aláírás hitelesítés egységes technológiai és jogi szabályaihoz. A szerzői jog védelméről az adatbankok vonatkozásában már 1996-ban fogadtak el irányelvet<sup>210</sup>. A 29-es munkacsoport javaslatot<sup>211</sup> fogadott el az adatvédelem és a szellemi termékek jogvédelmével kapcsolatban, ami az internet gazdasági használhatósága tekintetében készíti elő a jövőbeli jogalkotás alapjait. A belső piac joga mellett az Európai Közösség a munkavállalók védelmében tervezi<sup>212</sup>, hogy egységesen szabályozza a privacy kérdéseit a munkahelyen. A szociális kérdések tekintetében pedig elkészült az egységes európai betegbiztosítási kártya, amely az érintettek kór- és kezeléstörténete vonatkozásában teremti meg az egységes egészségügyi személyi számrendszert.

## 10.2. Távközlés adatvédelmi vonatkozásai

A távközlés területén számos irányelv született az 1997. év folyamán. A távközlési szektorra specifikus adatvédelmi irányelv indoklása az általános adatvédelmi irányelvre történő hivatkozással kezdődik, utalva arra, hogy a távközlési szektorban további speciális adatvédelmi rendelkezések szükségesek. A két irányelv több vonatkozásban is összekapcsolódik, egyrészt egybeesik a két irányelv tárgyi hatálya, az irányelv alapfogalmai is azonosak, így például a személyes adatok definíciója is azonos. Másrészt az adatbiztonság tekintetében a 95/46/EK irányelv szabályait a távközlési irányelvben is alkalmazni kell, továbbá az adatvédelmi irányelv III. fejezetében lefektetett jogok a kifogásolásra, a felelősségre és a szankciókra a távközlési irányelv által meghatározott egyéni jogokra is alkalmazandók. A

---

<sup>210</sup> Európai Parlament és a Tanács 1996. március 11-i 96/9/EK irányelve az adatbankok jogi védelméről, EK Hivatalos Közlöny L. 077, 1996. március 27. 20 old

<sup>211</sup> Arbeitspapier: Datenschutz im Zusammenhang mit Immaterialgüterrechten  
[www.europa.eu.int/omm/privacy](http://www.europa.eu.int/omm/privacy) Dok 10092/05/DE WP 104

<sup>212</sup> *Commission proposes new framework for Data Protection at work*, World Data Protection Report, 2003/01, 24.

két irányelv intézményi szinten is összekapcsolódik, mivel az adatvédelmi irányelv által felállított 29-es munkacsoportot a távközlés területén is figyelemmel kíséri az alapszabadságok és alapjogok érvényesülését. A távközlési irányelv újdonsága, hogy nemcsak a természetes személyek adatvédelmére vonatkozik, hanem a tagállamok számára felkínálja azt a lehetőséget, hogy a jogi személyek jogos érdekében álló adatok védelmére is kiterjessék a nemzeti szabályozást.

#### 10.2.1. A távközlési adatvédelmi irányelv céljai

A távközlési-adatvédelmi irányelv megalkotására a jogalapot az EK szerződés korábbi 100. cikke, jelenlegi 95. cikke szolgáltatta, mivel szükséges volt a tagállamok eltérő nemzeti szabályainak a harmonizálása a telekommunikációs piac tekintetében, hogy eltérő nemzeti előírások ne korlátozzák a belső határon átnyúló szolgáltatások kialakítását. Az irányelv célja a távközlési szektoron belül a természetes személyek személyes adatainak, és magánszférájának a védelme, a telekommunikációs szolgáltatások elterjedéséhez szükséges bizalom megerősítése. A nyilvánosság számára nyitva álló telekommunikációs szolgáltatásokat használó személyek igénylik, hogy speciális jogi, szervezeti, és technikai előírásokkal szabályozzák a személyes adataik védelmét. A Bizottság meglátása szerint a határon átnyúló technológiák, így az ISDN, a videotelefon, digitális mobiltelefon szolgáltatások elterjedése részben attól függ, hogy a használók mennyire bíznak abban, hogy magánszférájukat nem érinti hátrányosan ezen technológiák alkalmazása. Az irányelv meghatározza azokat a területeket párhuzamosan a 95/46/EK irányelvvvel, amelyek nem esnek a hatálya alá. Így a tagállamok hatáskörébe tartozik az alapjogok korlátozásának kérdése, ha arra közbiztonság, a honvédelem, a nemzetbiztonság, az állam vitális gazdasági érdekei okán kerül sor. Az irányelv nem terjed ki a tagállamok azon hatáskörére, hogy törvényes okból megfelelő eljárási rendben a telekommunikációs forgalmat megfigyeljék. A szolgáltatóknak olyan technikai intézkedéseket kell tenni, amelyek kizárják a

jogosulatlan hozzáféréseket a kommunikációs csatornához, továbbá a szolgáltatást igénybevevőket minden rizikóról, és a hálózati biztonság sérüléséről tájékoztatni kell.

## 10.2. Forgalmi adatok kezelése és kötelező törlése

Az irányelv 6. cikke alapján a távközlési szolgáltatás során keletkező személyes adatokat, mint a hívó fél azonosítási adatai, a hívott fél, a tárcsázott szám, a két fél közötti kommunikáció minősége, kezdete, tartama, és a fizetési információk a létrejött kapcsolat után a szolgáltatónak a rendszerből törölni kell. A szolgáltatónak az adatok megsemmisítésére irányuló kötelezettsége azután áll be, ha már az adatokat a számlázási rendszerben feldolgozták, a szolgáltató a számláját a fogyasztónak megküldte, és lejárt a számla kifogásolására nyitva álló határidő. Az adatok kötelező törlése alóli kivételt a 6. cikk (2) bekezdése szabályozza, így ha a szolgáltató beszerezte a fogyasztójának előzetes beleegyezését, akkor saját piackutatási céljaira is felhasználhatja a megszerzett adatokat.

A távközlési szolgáltatóknak a fogyasztók részletes tájékoztatása érdekében a távközlési adatokról részletes számlát kell kiállítani, amelyen a hívott számot, a hívás idejét, tartamát kell feltüntetni. A részletes számla világos tükre a kommunikációs szokásoknak, ezért a fogyasztónak adatvédelmi okból azt is biztosítani kell, hogy ha igényli, a számlát részletes hívásjegyzék nélkül kapja meg. A távközlési irányelv alapján a szolgáltatóknak biztosítani kell, hogy ha a hívók igénylik, akkor megakadályozhassák, hogy telefonszámukat a hívott készülék kijelezze. A távközlési szolgáltató kötelességévé teszi az irányelv, hogy a rosszindulatú, vagy a zaklató hívások felderítése érdekében természetesen a nemzeti jogszabályok alapján a hívó felet a szolgáltató azonosítsa, ezeket az adatokat tárolja, illetve az érintett személy kérésére kiadja. Az irányelv szabályozza a telefonkönyvekben közreadásra kerülő

személyes adatok kezelését is. A szolgáltató által összeállított adatbázisok, így a telefonkönyvek adatai is a vonatkozó szerzői jog előírások alapján a szolgáltató tulajdonát képezik<sup>213</sup>. Ezt a jogot korlátozza az irányelv adatvédelmi jogok érvényesítésével, így személyes adatokat ilyen nyilvános regiszterekben csak akkor lehet közreadni, ha a fél kétségtelenül hozzájárulását adta az adatok nyilvánosságra hozatalához. Az irányelv szabályozza a 12. cikkében a direkt marketing célból eszközölt automata hívásokat és telefaxokat is, amelyek megküldéséhez megköveteli a hívott fél előzetes beleegyezését. Az irányelvet a tagállamoknak 1998. október 24-ig kellett a nemzeti jogokba implementálni, de ekkora már folytak az előkészületek az informatika új technológiai eredményei jogi szabályozásának előkészítéséhez.<sup>214</sup>

### 10.3. Elektronikus kereskedelem adatvédelmi vonatkozásai

Annak érdekében, hogy a technikai fejlődéssel lépést tartson a belső piaci jogalkotás, és reagáljon a gazdasági kapcsolatok új formáira, már 1997-ben irányelvet<sup>215</sup> fogadtak el a távollevő felek között kötött szerződések érvényes létrejöttének szabályozása érdekében azért, hogy fogyasztóvédelmi szempontból a gyengébb fél jogi helyzetét erősítsék<sup>216</sup>. Az irányelv a fogyasztót megillető tájékoztatási és elállási jogokat építette ki a közösségen belül egységes módon, és ezzel az elektronikus kereskedelem szabályozásának alapjait is lefektette. Az elektronikus kereskedelem megújítására<sup>217</sup> 2002-ben

---

<sup>213</sup> KOPPÁNYI Szabolcs, *A hírközlés szabályozása az Európai Közösségben és Magyarországon*, Budapest, Osiris, 2003 (Osiris tankönyvek), 94.

<sup>214</sup> 3/97. ajánlás a névtelenségről az interneten ; 1/99. ajánlás a személyes adatoknak szoftver és hardver által végzett, rejtett és automatikus kezelésről az interneten ; 2/2000. vélemény a telekommunikáció jogi kereteinek felülvizsgálata kapcsán ; 7/2000 vélemény a Bizottság 2000. július 12.- javaslatáról a személyes adatok kezeléséről és a magánélet védelméről az elektronikus kommunikációs szektorban ; 2/2002 vélemény az egyéni azonosítók használatáról a telekommunikációs terminál eszközökben

<sup>215</sup> Az Európai Parlament és a Tanács 1997. május 20-i 97/7/EK IRÁNYELVE a távollevők között kötött szerződések esetén a fogyasztók védelméről, Az irányelvet a 17/1999 (II.5) Korm. Rendelet implementálta

<sup>216</sup> DÓSA Imre, POLYÁK Gábor, *i.m.*,226.

<sup>217</sup> Az Európai Parlament és Tanács 2002/22/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és



került sor, ekkor a távközlési-adatvédelmi irányelv helyét átvette az elektronikus hírközlési adatvédelmi irányelv<sup>218</sup>, amely minden korábbi szabályozást megtartott, és kiegészítette az új speciális technikai előírásokkal, mint a forgalmi, illetve helymeghatározási adat fogalma és kezelése, továbbá a kommunikációhoz kapcsolódó értéknövelt szolgáltatásra, elektronikus levélre, valamint a cookie-kra, SMS-ekre vonatkozó szabályokkal.

### 10.3.1. Az elektronikus hírközlési adatvédelmi irányelv céljai

Az elektronikus hírközlési adatvédelmi irányelv a 95/46/EK irányelvnek speciálisan a hírközlés szektorában történő érvényre juttatása azzal, hogy a vonatkozó 97/66/EK irányelvet az elektronikus hírközlési szolgáltatások piacának és technológiájának alakulásához hozzá kellett igazítani. A szabályozás célja, hogy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások felhasználói számára a személyes adatok és a magánélet tiszteletben tartásához való jog – az alkalmazott technológiától függetlenül – azonos szintű védelmet élvezzen. Az új korszerű digitális technológiák, amelyek a lakosság széles körei számára hozzáférhetőek, különleges követelményeket támasztanak a felhasználóknak személyes adataik és a magánélet tiszteletben tartásához fűződő jogukkal kapcsolatban. Az internet felborítja a hagyományos piaci struktúrát azzal, hogy világméretű infrastruktúrát biztosít az elektronikus hírközlési szolgáltatások széles körének biztosításához, amely a fogyasztók számára új lehetőségeket teremt, de egyben új veszélyeket is rejt a személyes adatok és a magánélet tiszteletben tartásához való joguk vonatkozásában. Az irányelvben megjelenik a modern adatvédelem egyik elve, mégpedig az, hogy olyan technológiákat kell alkalmazni, amelyek

---

elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról („Egyetemes szolgáltatási irányelv”) illetve az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról („Keretirányelv”)

<sup>218</sup> Az Európai Parlament és Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv”)

nem járnak személyes adatok felhasználásával, illetve követelmény az adattakarékosság elve, mely szerint lehető legminimálisabb mértékben kell személyes adatot feldolgozni a szolgáltatás során.

Az irányelv célja, hogy jogi védelmet adjon a felhasználóknak a rejtett kémszoftverek, web-poloskák, és más rejtett azonosítók alkalmazása ellen, amelyek a felhasználó tudta nélkül bejuthatnak annak számítógépébe, mobiltelefonjába, a felhasználó tevékenységének nyomon követése vagy rosszabb esetben adatlopás érdekében. A számítógépekre az egyes weblapok látogatása során automatikusan feltöltődnek ún. cookie-k, amelyek lehetőséget adnak a weblap megnézéséhez. A cookie-k a látogatott weblap tulajdonosával kapcsolatban maradhatnak például az on-line belépés esetén a felhasználó azonosítás érdekében. Ha ilyen jellegű program kerül feltelepítésre, akkor ezek használata csak akkor engedélyezhető, ha a felhasználó megfelelően részletes tájékoztatást kap, hogy tudomása legyen a végberendezésén elhelyezett adatokról. A tájékoztatási kötelezettség kiterjed a helymeghatározási adatok felhasználására az értéknövelt szolgáltatások igénybe vétele esetén.

### 10.3.2. Tájékoztatási kötelezettség

Az irányelv a szolgáltatók számára kötelezettségként előírja, hogy az előfizetőket, felhasználókat a szolgáltatónak tájékoztatnia kell az általa feldolgozott adatok típusáról, adatfeldolgozás céljáról, és időtartamáról. A szolgáltatónak tájékoztatnia kell előfizetőit a hálózati biztonság megsértésének minden különös kockázatáról. A szolgáltatónak kiemelten fontos kötelezettsége, hogy az előfizetőit teljes mértékben tájékoztassa olyan meglevő biztonsági kockázatokról, amelyek ellen a szolgáltatónak nincs módja fellépni. A szolgáltatók gyakran nem tesznek eleget tájékoztatási

kötelezettségüknek, a telekommunikációs szolgáltatások terén a bizalom kérdése ezért nyitott<sup>219</sup>.

### 10.3.3 Az internetre alkalmazandó szabályok

A távközlés során a közlés forgalmi adatait a számlázás és az összekapcsolás díjának megállapítását követő számlakifogásolási időszak után törölni kell, illetve anonimá tenni. Az interneten történő forgalom vonatkozásában az IP címek elraktározására a domain név rendszerben, vagy az egyes számítógépekhez kapcsolódó IP címek tárolására nem vonatkozik a kötelező adattörlési kötelezettség. Ez azt jelenti, hogy az interneten történő barangolás elviekben technikai úton visszafejthető, ezért fontos az Adatvédelmi Munkacsoport megállapítása, amely az IP címeket személyes adatoknak tekinti. Az interneten történő meghatározatlan számú személy részére történő műsorszórásra az irányelv nem alkalmazható, kivéve akkor, hogyha az egyéni előfizető személyre szóló szolgáltatást kap megrendelt videó-szolgáltatások formájában.

### 10.3.4. Helymeghatározási adatok

Az irányelv szabályozza a helymeghatározási adatok kezelésének alapvető szabályait, amelyek a magánéletre vonatkozó alapvető információkat tartalmazznak. A jelenlegi digitális mobil távközlési rendszer cella rendszerbe állított adó-vevő berendezések alapján működik, amely lehetővé teszi a mobil telefont, vagy GPRS-t használó személy pontos földrajzi helyének a definiálását egy meghatározott időpontban. A közlés idejére vonatkozó forgalmi adatok mellett, a közlés útvonalára, hosszára vagy mennyiségére valamint a küldő és a fogadó fél végberendezésének elhelyezkedésére vonatkozó adatok csak akkor kezelhetők, ha valamilyen értéknövelt

---

<sup>219</sup> Marie-Theres TINNEFELD, Heidi SCHUSTER, *Mangel an Vertrauen in die Telekommunikation*, *Datenschutz und Datensicherheit*, 2005/29, 79

szolgáltatáshoz kapcsolódnak. Ilyen értéknövelt szolgáltatást lehet például a tanácsadás a legolcsóbb tarifacsomaggal kapcsolatban, útvonal-információ, vagy közlekedési információ.

#### 10.3.5. Nem-kívánt elektronikus levelek és hívások

Elektronikus levélnek az a nyilvános hírközlő hálózaton küldött szöveges, hangalapú vagy képi üzenet tekinthető, amely a hálózatban vagy a címzett végberendezésén addig tárolható, amíg a címzett át nem veszi<sup>220</sup>. A közösségi jogalkotó védeni kívánja az előfizetőket a közvetlen üzletszerzés céljából, különösen automatizált végberendezéseken, telefaxon, e-mailben, SMS-üzenetekben küldött nem kívánt tájékoztatásokról, amelyek az előfizető magánéletét zavarják. Ezért az irányelv 13. cikke előírja, hogy személyes adatoknak emberi beavatkozás nélküli automatizált hívóberendezésekkel, telefax berendezésekkel, elektronikus levelek közvetlen üzletszerzési célból történő használata kizárólag akkor lehetséges, hogy ha előzetesen ahhoz az előfizető hozzájárult. Az előfizető hozzájárulása tekintetében a 95/46/EK irányelv szabályai alkalmazandók, mely szerint a beleegyezésnek önkéntesnek, konkrétan, és a megfelelő információk birtokában történő kifejezésnek kell lennie, amely lehet egy internetes honlap látogatása során egy rovat bejelölése is. A szolgáltató elektronikus levelezés céljából megszerezheti ügyfeleitől elektronikus elérhetőségi adataikat saját közvetlen üzletszerzési érdekében, feltéve ha az ügyfelei számára egyértelmű és kifejezett lehetőséget biztosít, hogy elektronikus elérhetőségük ilyen célú felhasználása ellen díjmentes és egyértelmű módon kifogással élhessenek. Az irányelv tiltja a SPAM-ek küldésének tilalmát azaz, minden esetben tilos olyan közvetlen üzletszerzési célú elektronikus levelezés folytatása, amely elrejtí annak a feladónak személyazonosságát, akinek nevében a tájékoztatás történik, illetve amely nem tartalmaz olyan érvényes címet, amelyre a címzett

---

<sup>220</sup> 2002/58/EK irányelv fogalom-meghatározások 2. cikk. h) pont

elküldhetné az ilyen tájékoztatás további küldésének tilalmára vonatkozó kérését.

#### 10.3.6. Elektronikus adatvédelem közrendvédelmi korlátozása

Az irányelv 5. cikke előírja a szolgáltatók számára, hogy biztosítsák a nyilvános hírközlő hálózatokban a szolgáltatások titkosságát. Az irányelv különösen tiltja, hogy a felhasználón kívül más személyek az érintett felhasználó hozzájárulása nélkül a közlést lehallgassa, meghallgassa, tárolja, vagy más módon elfogja kivéve, ha erre egy olyan tagállami jogszabály alapján kerül sor, amely egy demokratikus társadalomban szükséges, megfelelő és arányos intézkedésnek minősül. Továbbá a közlés titkosságának korlátozása a nemzetbiztonság, a közbiztonság, a honvédelem, vagy bűncselekmények megakadályozása szempontjából, illetve elektronikus hírközlési rendszer jogosulatlan használatának megelőzése, felderítése vagy üldözése érdekében szükséges. A közlés titkossága alóli kivételek vannak a feldolgozott forgalmi adatok törlésének kötelezettsége, illetve a hívóvonal és a hívott vonal azonosító kijelzésének és korlátozásának szabályai alól.

#### 10.3.7. Jogbiztonsági garanciák

Az elektronikus adatvédelemről szóló irányelv 15. cikk (2) bekezdése előírja, hogy az irányelvből eredő egyedi jogokra vonatkozóan a 95/46/EK irányelvben meghatározott jogorvoslati garanciákat, felelősségi szabályokat és szankciókat kell alkalmazni. A 29-es munkacsoport feladata kiegészül azzal, hogy ezen irányelv hatálya alá tartozó területeken is ellátja az alapvető jogoknak és szabadságoknak, valamint a jogos érdekeknek elektronikus hírközlési ágazaton belüli védelmét.

## 11. SEKTORÁLIS ADATVÉDELEM A MAGYAR JOGBAN

### 11.1. Személyes adatok jogi védelme

#### 11.1.1. Személyes adatok védelme és a személyiségvédelem

A modern adatvédelmi jog első amerikai<sup>221</sup> megfogalmazásával szinte egyidőben Zlinszky Imre 1897-ben megjelent Magyar magánjog művében az eszmei javakon való jogok körében utal arra, hogy modern jog nemcsak a testi javakra terjeszti ki oltalmát, hanem az eszmei javak is a jog tárgyává válnak. E jogok körében jelenik meg a névhez, védjegyhez, valamint a saját képmáshoz való jog „miután pedig a képmás a személyre mutat vissza, s egyenesen arra utal, azért a képmás szabad utánképzésnek lehetősége a legnagyobb jogsérelemeknek lehet az eszköze; e mellett közvetlenül is gazdasági, vagyoni érdeket is érinthet s közvetlen és tényleges kárt okozhat.”<sup>222</sup> A személyiségvédelmi jog dogmatikai rendszerének megfogalmazására<sup>223</sup> Szladits Károly szerkesztésében megjelent Magyar magánjog című gyűjteményben került sor. „A személyiség, a maga alkotó szabadságával a társadalom szempontjából értékes javakat – kultúrértékeket – tud létrehozni, amelyre a társadalomnak szükséges van. Minthogy minden embernek lehet képessége ilyen érték létrehozására és senkitől sem lehet az ellenkezőjét – legalább pro futuro – kimutatni, ezért a jognak vélelmeznie kell minden ember személyiségét, egyúttal pedig minden ember értékalkotásra való képességét. Ebben az irányban a jognak a feladata, hogy megóvja a személyiséget minden olyan háborítástól, amely a társadalom szempontjából nem szükséges”<sup>224</sup>. E tétellel került a magánjogi törvényjavaslatba az a megfogalmazás, hogy mindenkinek joga van arra, hogy törvények és mások jogainak korlátai között

---

<sup>221</sup> WARREN/BRANDEIS, Harvard Law Review 1890, 196.old.

<sup>222</sup> ZLINSZKY Imre: A magyar magánjog mai érvényében különös tekintettel a gyakorlat igényeire, Franklin Társulat Budapest, 1897. 465. old

<sup>223</sup> SZLADITS Károly (szerk): Magyar Magánjog Általános rész IV. füzet, Grill Károly Könyvkiadóvállalata Budapest, 1941.625. old.

<sup>224</sup> SZLADITS im. 626.lld

személyiségét szabadon érvényesítse, és ebben őt senki ne háborgassa. A személyiségi jog oltalmát kiterjeszti az élet, a testi épség, az egészség, személyes szabadság, névvédelem, a becsület, képmással kapcsolatos oltalomra, illetve a titokszférára. Balás P. Elemér<sup>225</sup> szerző szerint a titokszféra lényege, hogy „bizonyos tények tekintetében a személyiségnek annyira túlnyomó jelentősége, hogy ezek a tények már nem is számítanak a külső világ tényei közé jogi szempontból, hanem a személyiség függvényének tekinthető. A titok fogalma, azaz, hogy valami nem közismert, természetesen csak relatív fogalom, csak annyit jelent, hogy az élet rendes folyása szerint nem lehet számítani arra, hogy a titkot azoktól, akik ismerik, bárki megtudja”. A titokszféra megsértésének egyik formájaként határozza meg a szerző, a titok megtestesülésének jogosulatlan továbbadását, vagyis azé a dologét, amelyen a titok megfelelő jelek alakjában rögzítve vannak, így az lehet levél, lejegyzett szöveg, irat másolata, fénykép, hanglemez, vagy film. A titkot megtestesítő tárgyat nem is szabad továbbadni a titokra jogosult beleegyezése nélkül, kivéve ha azt jogszabály egyedi esetekben lehetővé teszi. A szerző ezt követően részletesen foglalkozik a titokszférába történő behatolás jogszerű eseteivel, amelyek kivételes esetekben lehetővé teszik a titok felfedését egyrészt magánjogi okból pl: öröklési igényhez, vagy perbeli védekezéshez kapcsolódóan, vagy közjogi okból a végrehajtás eredményessége, vagy rendőri intézkedés céljából. A szerző foglalkozik továbbá a megismert titok továbbadásának korlátozásával. Véleményem szerint a személyiségi jog elméleti megfogalmazásában már a XX. század közepén megjelent a titkot megtestesítő tárgyak védelme, amely későbbiekben alapvető kapcsolódási pont a személyiségvédelem és az adatvédelem között.

A magyar jogban 1978-ban a Ptk. 83.§-ban került először kodifikálásra a személyiség jogi védelme körében a személyes adatok védelme: „a számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő

---

<sup>225</sup> SZLADITS Károly (szerk): Magyar Magánjog Általános rész IV. füzet, Grill Károly Könyvkiadóvállalata Budapest, 1941.629. old

jogokat”. Az állami adatkezelést a statisztikáról szóló 1973. évi V. törvény, az állami népesség-nyilvántartásról szóló 1986. évi 10. tvr. és a kapcsolódó végrehajtási jogszabályok rendezték azzal a céllal, hogy minden polgár könnyen azonosítható legyen, és az állampolgárról minél több információ álljon rendelkezésre az állami szervek számára, amely adatok akadálytalanul áramolhatnak az államigazgatási alrendszerei között. A fenti előírások nem biztosítottak hathatós garanciákat, amely alapján a Ptk.. személyiségvédelmi előírásai alkalmazhatók lettek volna. Az információs önrendelkezés nem került rögzítésre az akkori Alkotmányban, így csak deklaráció szintjén maradt a Ptk.. előírása. Bár a magyar adatvédelmi törvény elfogadása előtt is léteztek számítógépes adatfeldolgozásra vonatkozó előírások, amelyek a szektorális szabályozás körében voltak fellelhetők, úgy mint a bűnügyi nyilvántartás, cégnyilvántartás, ingatlan-nyilvántartás, gépjármű-nyilvántartás, és a népesség nyilvántartás működtetésére vonatkozóan, amelyekre érvényesíteni lehetett volna a Ptk.. személyiség védelemi előírásait, de nincsen bizonyíték arra nézve, hogy a gyakorlatban a Ptk.. ezen személyiség védelmi előírása alkalmazásra került volna.

A magyar jogfelfogásban egyes szakírók az adatvédelmet a személyiségi jogok részének tekintették, amely az Európai Emberi Jogok Egyezményének 8. cikkében lefektetett magánélet tiszteletben tartásához való jogból ered<sup>226</sup>, ezért az adatvédelem jogdogmatikai besorolása a 90-es évek elején a személyiségvédelem tárgykörébe került. A Ptk..83.§ (1)<sup>227</sup> és (3) bekezdéseiben találjuk azt a kötelezettséget, amely kimondja, hogy a számítógéppel vagy más módon történő adatkezelés és adatfeldolgozás nem sértheti a személyhez fűződő jogokat. A nyilvántartott adatról tájékoztatást az érintett személyen kívül csak az arra jogosult szervnek, vagy személynek lehet

---

<sup>226</sup> PETRIK Ferenc, *A személyiség jogi védelme*, Budapest, Közgazdasági és Jogi Könyvkiadó, 1992, 167

<sup>227</sup> A Ptk 83.§ (1) bekezdését az 1992. évi LXIII törvény (Avtv) 33.§-ával megállapított szövege.



adni<sup>228</sup>. A Ptk.. lefektette az érintett adathelyesbítési jogát arra az esetre, ha valamely nyilvántartásban szereplő adat nem lenne valódi. Így ha a nyilvántartásban szereplő valamely tény vagy adat nem felel meg a valóságnak, az érintett személy a valótlan tény vagy adat helyesbítését külön jogszabályban meghatározott módon követelheti.

Egy Ptk. kommentár<sup>229</sup> szerint a „nyilvántartások bármilyen technológiával készülnek is végső soron hatalmat adnak a velük rendelkezni jogosultak kezébe. Az informatika fejlődése ezért az egész világon nyugtalanságot keltett. Különösen azért, mert az informatika az embereket egyszerű tárgyként, adatokként kezeli, s mert az emberek félnek az informatikával való visszaélésektől. Szükségessé vált ezért az adatok bizalmas kezelésének biztosítása, hatékony védelmükről való gondoskodás, az adatokkal – s általában a nyilvántartásokkal – való visszaélések meggátlása”.

Véleményem szerint a kommentár szűkítő álláspontja, hogy kizárólag az informatikához kapcsolódó jogellenes adatkezelés ellen ad védelmet a 83.§ (1) bekezdés alapján nem tartható. A törvényi megfogalmazásban szerepel a ”más módon” történő adatkezelés is, így az személyiségvédelem kiterjed minden a személyhez kapcsolódó digitális vagy nem digitális formában rögzített, a személyiség lenyomatát visszaadni képes adatra, tényre. Álláspontom szerint Ptk.. megfogalmazásából hiányzik a személyes adat fogalma, ami jelentősen megnehezíti a személyiségvédelmi igény és az adatvédelem elhatárolását.

Az új Ptk. 2:83<sup>230</sup>. § szakaszában már megfogalmazásra kerül a személyes adatok védelméhez való jog. Az (1) bekezdés szerint „A személyhez fűződő jogok védelme kiterjed a személyes adatok védelmére”. A további (2)

---

<sup>228</sup> A Ptk 83.§ (2) bek. második fordulatát: „Az érintett személy tájékoztatását csak abban az esetben lehet megtagadni, ha ennek teljesítése állami vagy közbiztonsági érdeket sértene.” A 1993. évi XCVII törvény 40.§ (4) bek. a) pontja hatályon kívül helyezte

<sup>229</sup> A Polgári Törvénykönyv Magyarázata, KJK-KERSZÖV Jogi és Üzleti Kiadó Budapest, 2001, 290. old.

<sup>230</sup> Magyar Közlöny 165. szám 2009.11.20 2009. évi CXX. törvény

bekezdés szerint: „A személyes adatokhoz fűződő jog megsértését jelenti különösen a személyes adat jogosulatlan megszerzése, kezelése, illetéktelen személlyel való közlése vagy nyilvánosságra hozatala.” Véleményem szerint utalni kellett volna az új Ptk.-nak arra, hogy a személyes adat fogalmát külön jogszabály határozza meg. Így világos kapcsolat alakulhatott volna ki a személyiségvédelem és az adatvédelem eszközrendszere között. A bírói gyakorlatnak kellene kimondania, hogy a Ptk. 83.§-ban lefektetett személyes adatok fogalmán az Avtv.-ben rögzített definíciót érti.

Álláspontom szerint azon személyiségi jogi sérelmek esetén, amikor az informatikai adatrögzítés, illetve a digitális jelleg megjelenik, mint tényállási elem, akkor a jogsérelmet szenvedett félnek választási lehetősége van, hogy a Ptk.-ban rögzített személyiségi jogi pert indít, vagy az Avtv. alapján adatvédelmi keresetet nyújt be. A személyiségi jogi kereset benyújtása esetén a Ptk. 84.§ (1)-(2) bekezdésében meghatározott kereseti kérelmeket határozhatja meg, de azzal kell szemben néznie, hogy a sérelmet szenvedett félnek kell bizonyítani a jogsértés tényét, a jogsértő személyét, és a személyiségi jogában bekövetkezett sérelem tényét, és annak mértékét. Ezzel szemben egy adatvédelmi perben a bizonyítási teher megfordul, így a törvény az adatkezelőt kötelezi arra, hogy bizonyítsa eljárása jogszerűségét. A adatvédelmi pernek létezik néhány egyéb vonása is, amely az érintett számára kedvező perbeli pozíciót biztosít, így a bíróság soron kívül jár el, illetve perképesége van annak is, akinek egyébként nincs perbeli jogképesége. A kártérítési igényvel kapcsolatban is eltérő a személyiségi jogi per, illetve az adatvédelmi per, mivel az adatkezelő köteles a jogellenes adatkezeléssel, vagy technikai követelmények megsértésével másnak okozott kárt megtéríteni, és egyetlen egy esetben mentesülhet a kárfelelősség alól az adatkezelő, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Véleményem szerint a személyiségi jogi, illetve az adatvédelmi kereset párhuzamosan is indítható, ha a képmással való visszaélés a jogsértés tárgya.

### 11.1.2. Személyes adatok védelme a képmásvédelem

A személyes adatok védelme és a magántitok védelmére vonatkozó jogszabályok áttekintése során már kitértem az információs önrendelkezési jog és a személyiségi jogok védelme között fennálló kapcsolatra. A kapcsolatot lényegesen meghatározza a személyek képmásának védelme, illetve a személyekről készített képeknek személyes adatként történő védelméhez fűződő jog. A képmásvédelem lényege, az ember külső megjelenésének a védelme, amely jogelméletileg az emberi méltóság jogából levezethető önazonosság, és önrendelkezési szabadságból is levezethető, mivel az embert megilleti az a jog, hogy a külvilágban, a társadalmi viszonyaiban róla kialakuló képet alapvetően meghatározhassa. Az adatvédelmi biztos álláspontja<sup>231</sup> szerint az Avtv. személyes adat és az adatkezelés fogalmának alapulvételével egyértelműen meghatározható, hogy a képfelvevő, -rögzítő berendezések által felvett és tárolt felvételek – amennyiben azon személyek felismerhetőek és azonosíthatóak - személyes adatot tartalmaznak, ezért az ilyen berendezések működtetése adatkezelésnek minősül.

A képmásvédelem és a személyes adatok védelmének egymásra tekintettel történő meghatározásához és elhatárolásához szükséges a képmásvédelem jogi szabályozásának az áttekintése. A Polgári Törvénykönyv tiltja más képmásával vagy hangfelvételével kapcsolatos bármiféle visszaélést<sup>232</sup>. A képmásvédelemmel kapcsolatos jogviták tárgya, hogy a kifogásolt magatartás azonosítható-e bármiféle visszaéléssel, mint a személyiségi jogot sértő cselekménnyel. A visszaélésszerű magatartást a személyiségvédelemmel kapcsolatos bírói gyakorlat annak alapján határozta meg, hogy a képmás, illetve a hangfelvétel készítése visszaélésszerűen történt-e, ennek megítélése során azt kell eldönteni, hogy a kifogásolt jogsértéssel érintett személy

---

<sup>231</sup> Adatvédelmi biztosi ajánlás 2001, *A megfigyelés, adatgyűjtés céljából üzemeltetett képfelvevő,- rögzítő berendezésekkel kapcsolatba.*

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=636\\_H\\_2001](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=636_H_2001) ; 206.12.15.

<sup>232</sup> 1959. évi IV. törvény a Polgári Törvénykönyvről

magánszférája megsértésre került-e. „A személyhez fűződő jogok megsértése megvalósulhat a képmás vagy hangfelvétel visszaéléssel történő elkészítésével is. Ha a lakó a falon áthallatszó hangos kijelentéseket tesz a szomszédos lakás lakójának személyével kapcsolatban, és ez utóbbi erről a saját lakásában elhelyezett hangfelvevő berendezéssel felvételt készít, ez a magatartás nem jelent más jogvédett érdekkörébe történő illetéktelen behatolást (jogsértést).<sup>233</sup>” A bírói gyakorlat szerint a birtokháborító magatartásról készült videofelvétel bizonyítékként való felhasználása nem minősül visszaélésnek, és nem sérti a személyhez fűződő jogokat<sup>234</sup>.

A képmásvédelem és a személyes adatok védelme között lényeges elhatárolási szempont, hogy míg a személyiségi jogvédelem nem tiltja a képmásról felvétel készítését, ha annak nem célja visszaélésszerű magatartás keretében adott személy képmásának eszközként történő felhasználása. Azonban a személyes adatok védelme körében a képmásnak, mint személyes adatnak a gyűjtéséhez az érintett hozzájárulása szükséges, amelyet az érintett csak akkor tud megadni, ha tudomása van arról, hogy fényképezik, vagy filmezik. Ebből kifolyólag a képmásnak személyes adatként történő védelme már a fénykép-, és filmkészítés folyamatára is irányadó, addig a személyiségvédelem a képmás felhasználásának tiltott eseteit szankcionálja.

A személyes adatok védelmével kapcsolatos további párhuzamok és emellett eltérő jellegzetességek az érintett jognyilatkozatával kapcsolatosan fogalmazhatók meg. A képmásvédelmi bírói joggyakorlat szerint az érintett hozzájárulásának értelmezése során a személyhez fűződő jogok megsértését kizáró hozzájárulásnak kifejezettnek kell lennie, azt a jogosult terhére kiterjesztően nem lehet értelmezni.<sup>235</sup> A személyes adatok körében a személyes adatok gyűjtéséhez az érintett önkéntes, előzetes és tudatos hozzájárulása szükséges, amely különleges adatok gyűjtése során további garanciális

---

<sup>233</sup> PK BH 1985/57

<sup>234</sup> PK BH 2000/485

<sup>235</sup> Legf. Bír. Pfv.IV.22.415/1999. sz. Bírói Határozatok Közleménye 1999

elemmel, azaz az írásbeli nyilatkozatban történő hozzájárulással van kiegészítve. Ha kétség áll fent a beleegyezés, illetve a hozzájárulás tekintetében, akkor az Avtv. szerint azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

A visszaélészerű magatartások közül a személyiségvédelmi szabályok a képmás, és hangfelvétel jogosulatlan nyilvánosságra hozatalát is tiltják. A bírói gyakorlat szerint nem minősül visszaélészerű magatartásnak a jogszerűen készített hangfelvétel vagy képfelvétel bírósági vagy szabálysértési eljárásban bizonyítékként való előterjesztése. „A bíróság vagy más hatóság előtt folyó eljárásban az igazság érvényesülésének biztosítása közérdek, és a bizonyítás ezt a célt szolgálja. Nem lehet ezért - az egyébként is jogsértés nélkül készült - hangfelvétel felhasználását visszaélésnek tekinteni, ha ez a hangfelvétel felhasználójával szemben elkövetett jogsértéssel kapcsolatos bizonyítás érdekében történik”<sup>236</sup>. A bíróság álláspontja szerint a képmás vagy hangfelvétel bírósági eljárásban történő felhasználása nyilvánosságra hozatalnak minősül, és a felhasználás tényének megállapítása szempontjából közömbös az, hogy a hangfelvétel készítése a személyiségi jogok megsértésével vagy ilyen jogsértés nélkül történt.

A Ptk. 80.§ (2) bekezdése felmentést ad a felvételt készítő számára, hogy az érintett beleegyezését megszerezze képmásának nyilvánosságra hozatalához, ha az érintett nyilvános közszereplésen vesz részt<sup>237</sup>. Tehát a nyilvános közszereplés esetén nincs szükség az érintett hozzájárulására. „A képmás nyilvánosságra hozatalának tilalma nem vonatkozik a nyilvános eseményekről, rendezvényekről, táj- és utcarészletekről készült felvételekre, amikor az ábrázolás módja nem egyéni, amikor a felvétel összehatásában örökíti meg a nyilvánosság előtt lezajlott eseményeket. A nyilvános eseményen készült képnek a nyilvános közléséhez a felvételen ábrázolt személy hozzájárulására

---

<sup>236</sup> PK BH 1985/57

<sup>237</sup> Ptk. 80.§ (2) Képmás vagy hangfelvétel nyilvánosságra hozatalához – a nyilvános közszereplés kivételével – az érintett személy hozzájárulása szükséges.

van viszont szükség, ha – az összes körülményre tekintettel – megállapítható a felvétel egyedisége, egyéni képmás jellege<sup>238</sup>. Az érintett beleegyezése nem szükséges azonban akkor, ha a felvétel olyan nyilvános közéleti eseményről készül, melyen képfelvétel készítése szokásos, amelyre tehát arra minden résztvevő alappal számíthatott. Egy rendezvényről készült, egyes személyeket kiemelve ábrázoló képfelvételek nyilvánosságra hozatala – az eseményről való tudósítás céljából, az ahhoz szükséges mértékben és formában – csak a média számára megengedett.

A nyilvánosságra hozatallal kapcsolatosan vitára adhat okot, hogy mit kell valójában nyilvános közszereplésnek tekinteni. Egy nyilvános összejövetelen, gyűlésen felszólaló szónok, vagy előadóművész esetében nem kétséges a nyilvános közszereplés ténye, így a felszólaló engedélye nélkül is az előadást feljegyezhetik, rögzíthetik. De a nyilvános közszerepléseken csupán hallgatóként résztvevő személyre vonatkozóan a nyilvános közszereplés fogalmát tágan vagy szűken kell értelmezni? Azaz értelmezés fogadható el talán a modern tömegkommunikációs eszközök működésére is tekintettel, amely szerint nemcsak a nyilvános közszereplés alkalmával aktívan résztvevő felszólaló, szónok vagy előadó személytől nem kell megkövetelni a beleegyezést, hanem a nyilvános közszereplésen passzívan résztvevő személytől sem kell megkövetelni a fénykép-, illetve filmkészítésbe a beleegyezését. Továbbá a bírói gyakorlatból az is megállapítható, hogy ha valakit egy nyilvános eseményről készített felvételen felismerhetően mutatnak be, akkor ehhez csak abban az esetben nem kell az érintett beleegyezése, ha az a média valamelyik formáján keresztül történik. Ugyanis ezekben az esetekben az ésszerűség szabályával, a mindennapi élet és a modern technika követelményével ellentétes lenne, ha minden egyes résztvevőtől hozzájárulást kellene kérni, ha a képfelvételt be kívánják mutatni a televízióban vagy a

---

<sup>238</sup> *Polgári Törvénykönyv magyarázata*, szerk. GELLÉRT György, Budapest, KJK-Kerszöv, 200, 283. ; BH 1985/17

sajtóban. De az adatvédelmi biztos szerint<sup>239</sup> az érintett beleegyezésének megszerzése alóli mentesség kizárólag a sajtó vagy a média törvény alapján működő személyeket és szervezeteket illeti meg.

Egy politikai rendezvényen (demonstráción, tüntetésen) való részvétel esetében azt kell megvizsgálni, hogy az azon jelenlévő személy valamely közfeladat ellátása érdekében van-e jelen vagy csak mint „magánember”. Amennyiben a részvétel célja nem az, hogy nyilvános tevékenységgel valamilyen értéket továbbítson mások számára, akkor a nyilvános közszereplés feltételei nem állnak fenn, vagyis az ilyen esetben történő egyéniesített bemutatáshoz az érintett hozzájárulására van szükség.

Ha a személyes adatok védelme felől közelítünk a nyilvános magántereken, illetve köztereken készített képfelvételek adatgyűjtéséhez, akkor a nyilvános közszereplésen való passzív részvétel tekinthető az érintett önkéntes beleegyezésének a fényképfelvételbe. Ellenben, ha az érintett egyértelműen tiltakozik a fényképfelvétel ellen, - mert az politikai rendezvényen történik, és így a részvétele óhatatlanul politikai véleményének gyűjtésére is irányul - akkor már nem lehet a rendezvényen való részvételt önmagában ráutaló magatartásként alapul venni az adatkezelés jogszerűségéhez, mert az érintett részéről ezzel ellentétes kifejezett jognyilatkozatot kapott az adatkezelő.

A nyilvános közszereplések alkalmával jogszerűen készített képfelvételek, amelyeken magánszemélyek politikai véleményüket hangoztatják, személyes adatkezelésnek minősül. Álláspontom szerint a nyilvános közszereplések alkalmával készített tömegfelvételeken szereplő és politikai véleményüket kifejező személyek egyedi azonosítása már ütközik a különleges adatok kezelésére vonatkozó Avtv.. előírásokkal, mert az adott személy és a politikai véleményének kezelésére vonatkozó adat csak akkor kezelhető, ha ahhoz az

---

<sup>239</sup> Az MSZP honlapján nyilvánosságra hozott, különböző rendezvényeken résztvevő személyekről készített fényképekkel kapcsolatos adatkezelésről.  
<http://abiweb.obh.hu/abi/index.php?menu=30002&docid=11722&key=k%E9pm%E1s> ; 2006. 10. 13.

érintett hozzájárult. A tömegfelvételeken szereplő személyek politikai véleményének azonosításán túl, a szabad véleménynyilvánításra is különösen veszélyes, ha adatkezelésekre vonatkozóan adatbázis összekapcsolási tilalmat az adatkezelő megsérti. E tilalom szerint „a személyes adatok akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek”. A tömegrendezvények alkalmával politikai véleményüket kifejező személyekről készített képfelvételekhez kapcsolódóan az adott személy közéleti, magánéleti viszonyait hozzákapcsolják, és azt nagy nyilvánosság előtt közzéteszik, ez a személyes adatok sérelmét jelenti, de képmással való visszaélés törvényi előírásaiba a bírói joggyakorlat figyelembe vétele alapján álláspontom szerint nem ütközik, ha kizárólag személyiségi jogi kereset alapján jár el a bíróság.

### 11.1.3. Közszerplők képmásvédelmi szabályai

A politikusi közszerplőknek az alkotmányosan meghatározható magánszférájuk szűkebb, és ezzel párhuzamosan jobban kell tűrniük a közvélemény, és a sajtó kritikai megjegyzéseit. „A közszerplőről készült, karikatúrának minősülő fényképfelvétel nyilvánosságra hozatala nem sérti a képmáshoz való jogot, és az ezáltal kifejezett vélemény sem sért becsületet vagy emberi méltóságot, ha a véleménynyilvánítás nem indokolatlanul bántó, sértő vagy lealacsonyító.”<sup>240</sup> A Legfelsőbb Bíróságnak egy olyan perben kellett állást foglalnia, hogy megengedhető a közszerplő képmásával való „játszadozás”, amikor a felperes közéleti politikus arcképét hozzámontírozták, egy hiányos öltözetű idegen női testhez. A képhez a szerzők megjegyzéseket is fűztek, amelyek a felperes politikus jellemvonásaira is utaltak. (Mármint ő, mint markos menyecske képes saját testi épségének is a megvédésére, ha arra kerül sor.) A Legfelsőbb Bíróság szerint a felperes arcképe a lapban

---

<sup>240</sup> PK BH 2000/293



jogosulatlanul lett felhasználva, mert nem a felperes közszerepléséről készült, és annak közléséhez a felperes nem járult hozzá, emellett pedig az ábrázolás módja - a ruhátlanság – a felperest női mivoltában, és így emberi méltóságában is sértette.<sup>241</sup> A Bíróság egyik eseti döntésében<sup>242</sup> kijelentette, hogy „a közszereplő képmása csak közszerepléseivel összefüggésben, a közéleti megnyilvánulásai által meghatározott keretben, annak bemutatására használható fel az érintett hozzájárulása nélkül”.

#### 11.1.4. A képmásvédelem egyéb adatvédelmi vonatkozású esetei

Az adatvédelmi biztosok a személyi és egyéb képmást tartalmazó igazolványok másolásával kapcsolatosan többször adtak ki állásfoglalásokat. Az adatgyűjtés speciális formája valósul meg, amikor a hitelintézet fénymásolatot készít ügyfelének személyi okmányairól, leggyakrabban a személyazonosító igazolványról. Bár az adatvédelmi biztos évről-évre felhívja a hitelintézetek figyelmét az adatvédelmi szempontból kívánatos eljárástól való eltérésre, a gyakorlat ezzel kapcsolatban nem változott. Az igazolványban szereplő képmás is személyes adat, mely törvényi felhatalmazás hiányában csak az érintett beleegyezésével kezelhető. Az adatvédelmi biztos álláspontja szerint a tanárról tanóra közben, munkaideje alatt a hozzájárulása nélkül nem készíthető sem kép, és sem hangfelvétel, mert mindkettő személyes adatnak minősül. A tanárról készített hang,- és filmfelvétel adatkezelésnek minősül, amely nem nélkülözheti az érintett előzetes beleegyezését az adatkezelésbe<sup>243</sup>. Egy beadványozó azzal a panasszal<sup>244</sup> fordult az Adatvédelmi Biztosi Hivatalhoz, hogy a képmását, egy kartontáblán, az életnagyságnál nagyobbak ábrázolva, a bejáratnál nyilvánosan közzétették. A beadványozó állítása

---

<sup>241</sup> LB Pfv. IV.21327/1993 BH 1994/27 Bírósági Határozatok Közleménye 1994

<sup>242</sup> PÜ BH 2006/282

<sup>243</sup> A tanórán történtek kép- és hangfelvételi rögzítéséről és felhasználhatóságáról 2005. október 25. 1590/K/2005-3. sz. ügyirat

<sup>244</sup> <http://abiweb.obh.hu/abi/index.php?menu=30002&docid=10689&key=k%E9pm%E1s> ; 2006.02.15.

szerint a fényképfelvétel idegenvezetőként, munkája közben ábrázolta, a felvétel elkészítéséhez és nyilvánosságra hozatalához nem járult hozzá, az ábrázolás csúnya és sértő volt, ám a kiállítás rendezője nem kívánt foglalkozni az esettel. A képmásvédelem megsértése esetén az adatvédelmi biztos válaszában felhívja az érintett figyelmét az Avtv. és a személyiségi jogok megsértésének esetére, és részletesen tájékoztatja a jogszabályok előírásait idézve, hogy bíróság előtt indíthat pert személyiségi jogai megsértése miatt.

#### 11.1.5. Személyes adatok büntetőjogi védelme

A személyes adatok védelme tekintetében a Büntető Törvénykönyvben több bűncselekmény törvényi tényállása sorolható fel. Így a privacyt és az információs önrendelkezési jogot védi a Btk. 177 §-a, amely a magántitok megsértése miatt bünteti azokat, aki a foglalkozásuknál, vagy köz megbízatásuknál fogva tudomásukra jutott magántitkot alapos ok nélkül felfedik. A magántitok megsértésének minősített esete, ha a bűncselekmény jelentős érdeksérelmet okoz. A bűncselekmény jogi tárgya a sértettnek a magántitkai megőrzéséhez fűződő személyiségi joga. A Btk. nem határozza meg, hogy miképpen kell értelmezni a magántitok fogalmát, de a közfelfogásban kialakult gyakorlatra tekintettel magántitok minden olyan az érintett személyre vagy annak viszonyaira, környezetére vonatkozó adat, amely csak szűk körben, a beavatottak által ismert tény, és amely megőrzéséhez a jogosultnak méltányolható érdeke fűződik. A magántitok lehet eszmei titok, amely a beavatottak tudatában rögződött, de lehet valamilyen materiális titok is, amely tárgyasult formában létezik, így leírt, lefényképezett, kép vagy hangfelvételen rögzített tény vagy adat. A magántitok tartalmát tekintve lehet személyi, erkölcsi jellegű, mint például a betegsége, rejtett szellemi vagy testi fogyatékossága, de utalhat a magántitok az adott személy vagyoni viszonyaira, amelyből következtetni lehet adósságára, hitelképességére, vagyonának mértékére. Magántitok minden

olyan bizalmas, – csak szűk körben, illetve beavatottak előtt ismert – személyi, családi, vagyoni helyzetre, egészségi állapotra, szokásokra vonatkozó tény vagy adat, amelynek nyilvánosságra hozatala a sértettre érdeksérelemmel jár.<sup>245</sup> Az elkövetési magatartás szempontjából lényeges körülmény, hogy az elkövetőnek speciális kvalifikáltsággal kell rendelkeznie, így tettes csak az lehet, aki foglalkozásánál vagy közmegebízásánál fogva jutott a magántitok birtokába. A magántitok felfedése akkor minősül bűncselekménynek, ha annak megőrzésére kötelezett személy azt alapos indok nélkül felfedi.

A Btk. 177/A. bekezdése szabályozza<sup>246</sup> a személyes adattal való visszaélés bűncselekményét. Korábban A Btk. e szakaszában a jogosulatlan adatkezelés, illetve a 177/B §-ban a különleges személyes adatokkal való visszaélés törvényi tényállása volt lefektetve. A személyes adatokkal való visszaélés bűncselekménye keret-diszpozíciós tényállás, mivel az Avtv. rendelkezéseinek egyes megszegését, így jogosulatlan vagy a céltól eltérő személyes adatkezelést, az érintett tájékoztatásának vonatkozó kötelezettség elmulasztása, illetve az adatbiztonságot szolgáló intézkedések elmulasztása tekinthetők elkövetési magatartásnak. A bűncselekmény akkor valósul meg, ha az elkövetési magatartás más vagy mások érdekeinek jelentős sérelmét eredményezi. A bűncselekmény egyik minősített esete, ha a jelentős érdeksérelem jogtalan haszonszerzés érdekében követik el, a másik minősített eset, ha a személyes adattal való visszaélést különleges személyes adatra követik el.

A személyes adatok védelmét szolgálja még a levéltitok védelme, illetve a magántitok jogosulatlan megismerése elleni büntető tényállások. A privacy védelmét szolgálja a jogosulatlan titkos információgyűjtés tilalma, illetve közvetve a gazdasági titok megsértése. A számítástechnikai rendszer és adatok elleni bűncselekmény elkövetése során cél lehet személyes adatok

---

<sup>245</sup> BÜ BH 2004/170

<sup>246</sup> A 177/A. §-t és az előtte lévő alcímet az 1993: XVII. törvény 39. §-ának (1) bekezdése iktatta be, szövegüket újonnan a 2003: II. törvény 11. § (1) bekezdése állapította meg.

megszerzésre, amelyekkel jogtalan haszonszerzésre irányuló magatartásokat lehet elkövetni.

## 11.2. A személyes adatok védelme és a sajtószabadság

A magyar adatvédelmi szabályok a sajtó és média területén működő adatkezelőkre nem határoznak meg kivételeket, bár időről időre felmerül a kérdés, hogy a sajtó adatkezelőnek minősül-e. A sajtó munkatársai csupán a személyes adatkezelők egy meghatározott csoportját alkotják, és ebbéli minőségében nem élvezhet különleges kedvezményeket, törvényi előírások alóli mentességeket. Így a sajtó is elköveti a személyes adatok védelmére vonatkozó előírások megsértését, ha indokolatlanul teszi közzé valamely személy nevét, lakcímét, telefonszámát, arcképét, vallásos világnézetét vagy más személyes adatát. A sajtó nem számít ugyan a legnagyobb adatkezelők közé, de arra tekintettel, hogy a sajtótermékek igen széles közvéleményhez juthatnak el, ezért a személyes adatok védelmére vonatkozó előírások kisebb megsértése is jelentős, akár helyrehozhatatlan<sup>247</sup> jogsérelmet okozhat. A sajtó működése a személyes adatokra, illetve a személyiségi jogokra nézve veszélyes üzemnek tekinthető, mivel az egyes érintettre ható jogsértések nagysága nem becsülhető, és nem határozható meg, mivel a sajtó közreműködésekképpen a közvéleményben újabb hatások alakulhatnak ki. A sajtó veszélyes üzemi működése korlátok közé szorítható a sajtó munkatársainak adatvédelmi kulturáltságának fejlesztésével.

A személyes adatok és a sajtószabadság kapcsolatának értékelése során figyelemmel kell lenni arra, hogy két alapjog összeütközésének a kérdéséről van szó, így nem lehet általánossággal kimondani, hogy az egyik vagy a másik alapvető jog mindig elsőbbséget élvez, mert az egyik oldalon a személyes adatok és a személyiségi jogok védelmére, míg a másik oldalon a

---

<sup>247</sup> *Adatvédelmi biztos beszámolója, 1998, 319/A/1996 sz. ügyirat*

sajtószabadság, és a közérdekű adatok nyilvánossága tekintendő védendő érdekeknek. A két alapjog összeütközése során az arányosság és a szükségesség mércéjével mérve lehet egyedi élethelyzetekben mérlegelve az alkotmányos megoldást megtalálni. A két különböző alkotmányos érdek világos elhatárolásának a mércéje a magánélet, és a közélet határvonalának a megtalálása, amely cseppet sem könnyű feladat. A személyes adatok védelmét és a sajtószabadságot nem lehet kizárólag egymással konfrontáló alapjogként értelmezni, mivel a sajtószabadság csorbulását eredményezné, ha egyes személyek, akik a törvényi korlátokba nem ütköző, de a közvélemény érdeklődésére számot tartó információkat tudnak, azt úgy adnák közre a sajtónak, hogy közben az adatvédelmi kötelezettség alapján a sajtó köteles lenne ezeket a személyes adatokat védett, zárt körben tartani.

A magánélet és a közélet elhatárolásának kérdéskörével, a közszereplők személyiségi jogainak, a közszereplők múltjának és jelenének megismerhetőségével kapcsolatban az Alkotmánybíróság által lefektetett és az adatvédelmi biztos által is képviselt elvet idézem, mely szerint politikai közszereplést vagy közhatalmat gyakorló személynek a magánszféra határa szűkebben van meghúzva, így a közvéleménynek jogában áll megismerni az egyéb személyek esetében védendőnek minősülő személyes adatokat<sup>248</sup> is. Másfelől az alapelv kiegészítésre szorul az adatvédelem és a jogbiztonság oldaláról, mert a személyes adatoknak sajtó általi nyilvánosságra hozatalához a jelenlegi előírások szerint vagy az érintett önkéntes és tudatos beleegyezése, vagy törvényi felhatalmazás szükséges. Ezért a törvényalkotónak meg kellene határoznia a közszereplők esetén igen részletekbe menő alapossággal, hogy mely személyes adataikat ismerheti meg a közvélemény.

Bűnügyi tárgyú bulvár újságírás esetén a közszereplő magánszemély megkülönböztetés nem érvényesíthető, mivel minden személyt az ügy jogerős befejezéséig megillet az ártatlanság vétele. A nyilvános tudósításban az

---

<sup>248</sup> *Adatvédelmi biztos beszámolója, 1996, 319/A/1996. sz. ügyirat*

ítélelhirdetésről is be lehet számolni, mert ebben az esetben elsőbbséget élvez a közösség tájékoztatása, de ebben az esetben sem lehet az áldozatok személyiségi vagy éppen adatvédelmi jogait figyelmen kívül hagyni. A személyes adatokat és a személyiségi jogokat súlyosan sértő cselekmény, ha az elektronikus médiában katasztrófák, családi tragédiák áldozatai, azok hozzátartozói bemutatására úgy kerül sor, hogy az érintettek teljes mértékben azonosíthatók<sup>249</sup>.

A sértettekkel történő kapcsolatfelvétel érdekében a rendőrségi törvény lehetővé teszi, hogy a sértetti kör megállapítására, a tanú, az elkövető felkutatására, illetve a bűncselekmény tényállásának tisztázása érdekében a sajtóban, rádióban, televízióban – díjmentesen – felhívást tegyen közzé. Egy esetben család elkövetésével vádolt férfi azzal a kéréssel fordult az Adatvédelmi Biztos Irodához, hogy a rendőrség felhívása sértette az információs önrendelkezési jogait, mivel a közérdekű tájékoztatásban a rendőrség hírt adott korábbi büntetett előéletéről. A panaszosnak az igaza bebizonyosodott, mivel a büntetett előéletre vonatkozó különleges adatok közzétételének a rendőrség részéről nem volt meg a jogalapja.

A személyes adatok megsértésének az esetkörébe tartozik az is, ha törvényi felhatalmazás hiányában a nyilvánosság számára közzétesznek büntetőeljárásban keletkezett vagy felhasznált iratot, vádiratot. Mivel a Be. lehetővé teszi a nyilvános tárgyalást, így a kialakult adatvédelmi gyakorlat szerint a nyilvános tárgyaláson elhangzottak, vagy az ott felhasznált iratanyagok nyilvánosságra hozhatók, ha az a jogerős ítélet meghozataláig nem jár együtt az érintett személy személyiségi jogainak, és az ártatlanság vélelmének sérelmével. Ha a Bíróság kiskorúak védelme érdekében a tárgyalás zárt megtartása mellett dönt, akkor a sajtó munkatársai nem jelentethetnek meg a kiskorú személyéhez kapcsolható adatokat<sup>250</sup>.

---

<sup>249</sup> *Adatvédelmi biztos beszámolója, 1999, 593/H/1999. sz. ügyirat*

<sup>250</sup> *Adatvédelmi Biztos közleménye, 273/A/2001. sz. ügyirat*

A sajtó illetve a televízió műsorok készítői részére adott személyes adatkezelési hozzájárulás visszavonásának érdekes kérdésére világított rá egy jogeset<sup>251</sup>. Egy televíziós társaság riportműsort készített az érintett beleegyezésével, majd azt az érintett visszavonta. Felmerül a kérdés, hogy ebben az esetben az egész elkészült műsort le kell-e törölni, mert megszűnt az adatkezelés jogalapja. Az adatkezelő nem hivatkozhat arra, hogy az érintett személy joggal való visszaélést valósított meg, mivel a személyes adatok védelmének rendszere nem ismeri el ezt a polgári jogi fogalmat. A köztes megoldás az lehet, hogy az érintett magánszemély hangját nem lehet közreadni, illetve ha nem közterületen készült a felvétel, akkor az érintett személy arcképét sem lehet közreadni, de a riportban az érintett részéről elhangzott személyes adatokat nem tartalmazó közlésről lehet tájékoztatást adni.

A 100 leggazdagabb magyar jogeset kapcsán újra felmerült a sajtó adatvédelmi kötelezettségeinek betartása. A panaszos a közzététel előtt kifejezetten tiltakozott az ellen, hogy a személyére, vagyonára vonatkozó becsült adatok, a hobbijára, foglalkozására, munkahelyére utaló információk nyilvánosságra kerüljenek. A sajtó tájékoztatásra irányuló feladatát nem lehet olyan kiterjesztően értelmezni, amely jogalapot adna arra, hogy az érintett hozzájárulása ellenére adatait közzé lehetne tenni. Az ingatlan-nyilvántartás nyilvánossága sem értelmezhető úgy, hogy adatkezelésre törvényi felhatalmazást adna arra, hogy az érintett által tulajdonolt összes ingatlanának az adatát összegyűjtsék, és azokat közzétegyék.

A valóságshow műsorok 2003-ben érkeztek el Magyarországra, és a bemutatott műsorok a magánszférát és a személyes adatok védelmét illetően számos kérdést vetnek fel. Az Alkotmánybíróság 35/2002. (VII.19.) AB határozata és az Avtv. későbbi módosítását követően nem lehet vitás, hogy

---

<sup>251</sup> *Adatvédelmi biztos beszámolója*, 1999, 302/A/1999. sz. ügyirat

kamerával történő megfigyelés és annak eredményének a rögzítése adatkezelésnek minősül. Az Avtv. előírásai alapján az adatkezelésnek nemcsak a törvényesség, hanem a tisztességesség követelményének is meg kell felelnie. Az adatvédelmi biztos a tisztesség követelményét tulajdonképpen az Alkotmánybíróságnak az emberi méltóság jogából levezetett információs önrendelkezési jog lényeges tartalmával azonosította, így az adatkezelés során az érintett nem válhat kiszolgáltatottá sem az adatkezelővel, és sem más személlyel szemben.

A magyar adatvédelmi szabályozás a sajtó tekintetében nem tartalmaz speciális adatkezelési előírásokat, bár meglátásom szerint erre szükség lenne. Az, hogy szükséges lenne a sajtó adatkezelési kötelezettségeit szabályozni a 29-es munkacsoport által elfogadott ajánlásból is kiderült. A 29-es munkacsoport állásfoglalást fogadott el a sajtó és a média viszonyáról<sup>252</sup>, amelynek az oka arra vezethető vissza, hogy az Egyesült Királyságban, illetve a Németországban eltérően egyeztetik össze a személyes adatok védelmét és a sajtószabadságot. A személyes adatok és a sajtó adatkezelése tekintetében a tagállamokban létező szabályozást három csoportba lehet sorolni. Néhány esetben, így Nagy-Britanniában, Belgiumban, Spanyolországban az adatvédelmi rendelkezések semmilyen kifejezett kivételt nem rögzítenek a sajtó vonatkozásában. Az Németországban, Franciaországban, Ausztriában, Finnországban a sajtó adatkezelésére vonatkozóan speciális rendelkezések kerültek törvényi szinten elfogadásra. Más országokban a média az adatvédelmi szabályokon kívülesik, és speciális szabályozás alá vonták a tagállamok ezt a területet. A szabályozás abban is különbözik, hogy míg Dániában a teljes média szektor speciális szabályok alá tartozik, addig az Németországban a közösségileg finanszírozott rádió és televízió szolgáltatók nem a szövetségi, illetve a tartományi adatvédelmi szabályok hatálya alatt állnak, hanem speciális, a tartományok által megkötött államszerződések

---

<sup>252</sup> EMPFEHLUNG 1/97 Datenschutzrecht und Medien angenommen von der Datenschutzgruppe am 25. Februar 1997. [http://ec.europa.eu/justice\\_home/fsj/privacy/](http://ec.europa.eu/justice_home/fsj/privacy/); 2003.11.12.



rögzítik ezeket a szabályokat. A tagállamokban meglevő eltérő szabályozások közötti különbséget nem szabad eltúlozni, mivel mindegyik tagállami adatvédelmi szabályozás az Alkotmányokban rögzített sajtó és véleménynyilvánítási szabadság érvényesülése érdekében korlátozott keretek között érvényesül a média tekintetében.

### 11.3. Egészségügyi személyes adatok védelme

Az egészségi állapotra vonatkozó adataink az Avtv. előírása alapján különleges adatnak számítanak. Az egészségügyi adatok körébe beletartozik a testi és lelki egészségi állapotunkra, annak változására vonatkozó adatok, így az esetleges betegségekre, fertőzöttségre, kórtörténetre utaló adat. Védett információnak minősül foglalkozás egészségügyi szempontból az arra vonatkozó információ is, hogy bizonyos munkakörök betöltésére alkalmas-e az adott személy, illetve, hogy várandós állapotba került-e a női munkavállaló. Az egészségügyi adatok körébe tartozik az is, hogy igénybe vette valaki rosszullete, vagy éppen a szerencséjére megghiúsult öngyilkossági kísérlete miatt a mentőszolgálat segítségét. Az egészségügyi adatok körébe tartoznak természetesen a szenvedélybetegsége, drogfogyasztásra, illetve a pszichiátria betegsége utaló adatok is. Egészségügyi adatnak tekintendők a véradók, a donorok adatai, elérhetősége, illetve a saját genetikai adataink<sup>253</sup> is. Egészségügyi adatnak tekinthető a kórházi gyógykezelés igénybe vétele, és az, hogy ezen időszak alatt, mely kórterem mely ágya, kihez tartozik.

Az egészségügyi adataink kezelésére számtalan helyen kerül sor, így a házi orvos saját számítógépes rendszerében rögzíti évekre visszamenőlegesen egészségi állapotunk alakulását, de a gyógyszertárakban is leellenőrzése kerül, hogy rendelkezünk-e társadalombiztosítási jogviszonnyal. A munkaügyi

---

<sup>253</sup> Stellungnahme 6/2000 Zur Genomproblematik Angenommen am 13. Juli 2000; [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2000/wp34de.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp34de.pdf); 2006.11.15.

jogvitában, vagy gondnokság alá helyezési jogvitában, de akár házassági vagyoni jogi perben alkalmazott igazságügyi szakértők megállapításai tartalmaznak egészségügyi személyes adatokat. De egészségügyi adatok kezelésére sor kerülhet szociális juttatások megállapítása során is. Az egészségügyi intézmények a hozzájuk forduló beteg adatait, kezelésük eredményét szintén saját irattári rendszerükben dokumentálják, és a törvényi kötelezettségek esetén egyes fertőző betegségekre vonatkozóan eleget tesznek jelentési kötelezettségüknek. Az egészségügyi adatok védelmét nem csak a személyes adatok védelmére vonatkozó Avtv., illetve az orvosi titoktartásra vonatkozó kötelezettségek biztosítják, hanem 1997-ben az Országgyűlés elfogadta az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvényt.

A törvényi szabályozás alapján a betegeknek információs önrendelkezési joguk van a gyógyításukkal kapcsolatos teljes körű tájékoztatásra, dönthetnek a javasolt kezelések, beavatkozások tekintetében, továbbá megismerhetik az egészségi állapotunkra vonatkozó dokumentációt<sup>254</sup>. Az egészségügyi adatok védelméről szóló törvény (továbbiakban Eüat) a személyes adatok védelmének szektorális szabályozását biztosítja. A törvény meghatározza a szükséges törvényi definíciókat, mint pl. az adatkezelő, az adatfeldolgozó, az orvosi titok, az egészségügyi dokumentáció. Nem utolsósorban az egészségügyi adat fogalmát is rögzíti a törvény, mely szerint az „az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátó hálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat, továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (pl. magatartás, környezet, foglalkozás)”.

---

<sup>254</sup> *Adatvédelmi biztos beszámolója 1998*

A törvény meghatározza az egészségügyi adatok kezelésének céljait, így az egészség megőrzésének, fejlesztésének, javításának, egészségi állapotának nyomon követése céljából kerül sor adatkezelésre, de a népegészségügyi, és a járványügyi szempontból történő adatkezelés is legális. Az egészségügyi adatok kezelését más törvények egészségügyi szakemberképzés, tudományos vizsgálat, az egészségügyi szerv hatósági ellenőrzése, az egészségügyi ellátás finanszírozása, társadalombiztosítási ellátások megállapítása, bűnüldözés, közigazgatási eljárás, szabálysértési eljárás, ügyészségi és bírósági eljárás lefolytatása érdekében lehetővé teheti. Így külön törvényi rendelkezés alapján egészségügyi adatok kezelésére sor kerülhet az oktatási rendszerben, a katonai szolgálatra, a munkavégzésre vonatkozó alkalmasság megállapítása érdekében. E adatkezelési céloktól eltérő adatkezelés esetében az érintett beleegyezését írásbeli hozzájárulás formájában kell megadnia az adatkezelő részére. A törvény részletesen szabályozza a gyógykezelés céljából, a közegészségügyi, népegészségügyi, a statisztikai és a tudományos célú adatkezelések rendjét. A törvény előírja, hogy a társadalombiztosítási szervek és az ellátásszervező adatkezelő milyen keretek között kezelheti a személyes adatokat. Az Eatv. szabályozza, hogy a bűnüldözési, közigazgatási, szabálysértési, ügyészségi és bírósági eljárások lefolytatásához szükséges adatok az egészségügyi ellátóhálózaton kívüli szervezet részére annak megkeresése alapján továbbításra kerüljenek.

A törvényi előírások nem változtatták meg egycsapásra az orvosok hozzáállását, mivel az orvosok gyakran nem vonják be a beteget az őt érintő döntések meghozatalába. Az állampolgárokat a gyógykezelés során tájékoztatni kellene az őket megillető jogokról, hogy az egyenrangú orvos beteg kapcsolat kialakuljon. A törvény alkalmazásáról az adatvédelmi biztos később pozitív hangvétellel számolt be, mivel álláspontja szerint a törvény hatályba lépését követő két évvel sokkal nyitottabb az egészségügyi rendszer a jogait érvényesíteni kívánó beteg felé.

Az adatvédelmi biztoshoz érkező panaszok az egészségügyi intézmények iratkezelésével és az egészségügyi adatokat tartalmazó iratok továbbításával, azok megsemmisítésével, illetve a dokumentációk indokolatlan másolásával foglalkozott. Így például 1998 májusában Gyöngyösön a MÉH telepen több konténernyi egészségügyi dokumentációt találtak<sup>255</sup>, amelyek boncolási jegyzőkönyvek, illetve terhesség megszakításokkal kapcsolatos iratok voltak. Az egészségügyi intézmény vezetője az iratokat visszazállította, és gondoskodott azok törvényes megsemmisítéséről, de ez az eset is rávilágított arra, hogy szükséges adat- és iratkezelési szabályzat, amelynek betartását külön adatvédelmi felelősnek kell ellenőriznie. Egy másik esetben az adatbiztonságra hivatkozva Kecskeméten a város egészségügyi alapellátási intézményének vezetője arról döntött, hogy bekéri az összes házi orvosnak az általuk kezelt betegek egészségügyi dokumentációját, hogy azokat lefénymásolva egy pánccsaszekrénybe elzárja. A jogvita során az adatvédelmi biztos úgy foglalt állást, hogy ugyan az adatbiztonság alapvető követelmény a vállalkozó háziiorvossal szemben, de e követelményről történő gondoskodás nem alapozza meg, hogy minden egyéb ok és cél nélkül kerüljön sor az indokolatlan adatkoncentrációra. Az egészségügyi dokumentációk megőrzésére vonatkozó adatbiztonsági követelmény megsértésére került sor abban a jogesetben, amikor a panaszos azt sérelmezte, hogy az egészségügyi intézmény az irattározás rendjének megsértésével megsemmisítette azokat a laborvizsgálati eredményeket, amelyek alátámaszthatták volna a munkáltatója ellen indított perben az egészségkárosodásának a mértékét. Az egészségügyi ellátónak a kötelezettsége lett volna az iratok őrzése, amely az egészségügyi dokumentációk esetén 30 év, míg a zárójelentést legalább 50 évig kell megőrizni.

Az egészségügyi adatkezelésekkel kapcsolatos szabálytalanságok, és az ilyen jellegű adatokkal kapcsolatos visszaélések minden esetben súlyosnak minősülnek, de az egészségügyi adatok között is vannak olyan adatok,

---

<sup>255</sup> *Adatvédelmi biztos beszámolója, 1998, 368/A/1998. számú ügyirat*

amelyek minden vitán felül a legsérülékenyebb adatok közé tartoznak. Minden bizonnyal ebbe a körbe tartoznak a pszichiátriai betegségekre, az AIDS fertőzöttségre, vagy drogfogyasztásra vonatkozó adatok, mert a társadalmi előítéletek miatt az érintettek személyiségi jogai különösen nagy mértékben sérülnek, a társas kapcsolatrendszerük, elismertségük beszűkül ezen sérülékeny adatok nyilvánosságra kerülésével.

Az adatvédelmi biztos tematikus vizsgálata során megállapította, hogy több vidéki intézetben az Eakt. és az adatvédelmi törvény rendelkezéseibe ütköző gyakorlatot folytatnak a HIV betegek szűrése során. Annak ellenére, hogy az Eakt. 15.§ (6) bekezdése előírja, hogy amennyiben az érintett annak megállapítása érdekében, hogy HIV vírusával fertőződött-e – személyazonosságának előzetes felfedése nélkül – szűrővizsgálaton kíván részt venni, személyazonosító adatait a betegellátó részére nem köteles átadni. Előfordult, hogy az anonim-szűrés lehetőségére vonatkozó tájékoztatás hiányzott, sok helyen a vizsgálathoz TAJ-azonosítót és személyazonosító igazolványt kértek, megsértve ezzel az anonimitás elvét. Az adatvédelmi biztos kifogásolta, hogy nem megfelelő az azonosítók alkalmazása, így pl. az anonim teszteredmény visszakereshetőségéhez a vérmintát a tesztre jelentkező születési dátumával látták el, vagy TAJ-számot alkalmaztak. Az adatvédelmi biztos megállapította a vizsgálat lezárását követően, hogy az anonim HIV-szűrés törvényben deklarált szabályai a gyakorlatban nem érvényesülnek kellőképpen. Ezért felhívta a figyelmet arra, hogy az anonim szűrés esetén az ÁNTSZ városi intézetei nem kérhetik be az érintett személyazonosító adatait „közegészségügyi vagy járványügyi érdekre” hivatkozva, mert ez sérti az önként szűrésre jelentkező személyek információs önrendelkezési jogát. Az adatvédelmi biztos felhívta a figyelmet arra, hogy az egészségügyről szóló 1997. évi CLIV. törvény tájékoztatásra vonatkozó alapelvét (13. §) és a 62. § (4) bekezdésében leírt széles körű tájékoztatást a HIV ellenanyag vizsgálat során is alkalmazni kell, az egészségügyi dolgozónak előzetesen tájékoztatnia kell az érintettet az anonim szűrés lehetőségéről is. Az adatvédelmi biztos a

téma jelentőségére tekintettel tovább folytatta a kérdéskör vizsgálatát, és 2005. évben újabb ajánlást adott ki a szexuális úton terjedő fertőző betegségben szenvedő betegek adatainak kezelésével összefüggésben folytatott adatvédelmi biztosi vizsgálat eredményéről<sup>256</sup>. Az adatvédelmi biztos kifejtette, hogy elő kell segíteni a szabad orvosválasztás jogának gyakorlását a lakóhelytől távoli kezelés érdekében, illetve biztosítani kell, hogy privát adatfeldolgozók a rendszerbe ne kerülhessenek be. Ezen különleges érzékenységgel bíró a egészségügyi adatok laboratóriumi vizsgálatait, lehetőleg az ellátónál működő laboratóriumokban történjen, vagy mellőzzék személyes adatok használatát a labor eredmények küldése során. Szükséges annak körütekintő megteremtése is, hogy a kontaktusszemélyek adatainak kezelését is csak az erre törvényben felhatalmazott és megfelelő gyakorlattal, valamint megfelelő emberi hozzáállással rendelkező egészségügyi dolgozók végezhessék.

A drogfogyasztók egészségügyi adataihoz kapcsolódó jogesetben az adatvédelmi biztos ajánlásában lefektette, hogy a mentőszolgálat munkatársainak nem lehet értesítenie a rendőrséget, ha kábítószer befolyásoltság hatása alatt álló személyhez hívják segítségnyújtás céljából, és ha mentősöknek a helyszínen nem kell fenyegetettséggel számolniuk. Az Országos Mentőszolgálat a rosszullétük miatt gyógykezelésre szoruló drogfogyasztókról nem tehet bejelentést a rendőrségnek, illetve a mentőállomásokon az orvosokra és az egészségügyi dolgozókra vonatkozó titoktartási kötelezettség, valamint az adatvédelmi törvény előírásainak betartásával, fokozott körültekintéssel kell kezelni és óvni a betegek személyes adatait.<sup>257</sup> Az adatvédelmi biztos álláspontja szerint az, hogy a mentőszolgálat riaszthatja a rendőrséget, ha a helyszínre érkező mentősök élete vagy testi épsége veszélybe kerül, az nem tekinthető olyan felhatalmazásnak, hogy a mentők mérlegelés nélkül minden drogfogyasztóról érkező riasztás esetén a rendőrség segítségét kérje. Egy másik esetben a rendőrség egy nevet tartalmazó listát küldött a Nyíró Gyula Kórháznak adatkérés végett, mivel az

---

<sup>256</sup> *Adatvédelmi biztos beszámolója*, 2005. 260/K/2005. számú ügyirat

<sup>257</sup> *Adatvédelmi biztos beszámolója*, 1998, 522/A/1997. számú ügyirat

egészségügyi adatokat büntetőeljárásban hivatalosan kívánják felhasználni. Az adatvédelmi biztos álláspontja szerint a rendőrség anélkül, hogy konkrét bűncselekmény elkövetésével valamely személy nem lenne meggyanúsítva, nem kérheti a bűncselekményhez kapcsolódóan az egészségügyi adatszolgáltatást. A rendőrség az adatkérései során gyakran elmulasztja megjelölni az adatkérés pontos célját, illetve a vádlotton kívül a vele kapcsolatban levő személyekről is felvilágosítás megszerzésére törekszik<sup>258</sup>. A bűncselekmény gyanúsítottjáról történő adatszolgáltatás csak akkor jogszerű, ha a kérelemben megnevezik a kért adatok pontos körét, de ebben az esetben sem adható ki a betegről a teljes egészségügyi dokumentációja<sup>259</sup>.

A rendőrségi adatkérések adatvédelmi követelményeiről az adatvédelmi biztos 2006. október 23-i összecsapásokat követően adott ki újabb ajánlást, mely szerint a rendőrségnek meg kell nevezni azt a bűncselekményt, melyben a nyomozást folytatják, meg kell jelölnie az adatszolgáltatás jogalapját. A rendőrségi adatkérés jogalapjaként Be.71.§ (3) bekezdésére kell hivatkozni, amely előírja, hogyha a megkeresés személyes adatok közlésére vonatkozik, az csak annyi és olyan személyes adatra vonatkozhat, amely a megkeresés céljának megvalósításához elengedhetetlenül szükséges. A megkeresésben az adatkezelés pontos célját és a kért adatok körét meg kell jelölni. Az adatvédelmi biztos szerint a rendőrségi megkeresésben azt is meg kell jelölni, hogy az elkövető, tanú felderítése, sértett felkutatása miatt kell-e az adatszolgáltatást teljesíteni. Az adatvédelmi biztos szerint nem felel meg a rendőrségi adatkérési kérelem időbeli terjedelme sem (2006. október 23-án 00.00 óra és 2006. október 24-én 08.00 óra közötti időben ellátásra jelentkezett személyek neve, születési helye és ideje, anyja neve, lakcíme), mivel nem felel meg az adattakarékosság követelményének, mely szerint csak az elengedhetetlenül szükséges személyes adatok gyűjthetők. Az adatkérés teljesítése esetén a Rendőrség megkapná még az összecsapások előtt az

---

<sup>258</sup> *Adatvédelmi biztos beszámolója, 1999, 499/K/1999. sz. ügyirat*

<sup>259</sup> *Adatvédelmi biztos beszámolója, 2001, 25/K/2001. sz. ügyirat*

otthoni sérüléssel, egyéb megbetegedéssel kezelt beteg adatait éppúgy, mint a gumilövedék okozta sérüléssel kezelt beteg adatait is; de az érintetti kör kiterjedne a pár hónapos csecsemőre és a nyolcvan éves mozgáskorlátozott állampolgárra is. Tehát az adatkérés nemcsak az időintervallum miatt, hanem a személyi kör tekintetében is túlzó, ezért nem felel meg a törvényi feltételeknek. Az adatvédelmi biztos felhívta a figyelmet arra, hogy a túl általános jellegű, gyakorlatilag készletező jellegű adatkérésre és adatgyűjtésre irányuló megkeresések nem felelnek meg sem a Be., sem az Eüak., sem az Avtv.. szabályainak, ezért jogszerűen nem is teljesíthetők<sup>260</sup>.

Ahogy az Eakt. is lehetővé teszi, sor kerülhet egészségügyi adatoknak tudományos célú kezelésére is. A tudományos célú egészségügyi adatkezelések igen fontosak a népesség egészségügyi helyzetének feltérképezése céljából, de az adatok szenzitív jellegére a közvélemény kutatási jellegű tudományos kutatásoknál szükséges, mind az Avtv., a direktmarketing törvény, és a Eüat. előírásait betartani. A gyermekek egészségi állapotát érintő felmérések esetén az adatvédelmi biztos megfelelőnek találta azt a megoldást, hogy az érintett gyermekek szüleit az intézményben kitett visszaküldendő adatközlésre kérte fel a kutató. Más esetben az adatvédelmi biztos kijelentette, hogy méltányossági alapon egyedi esetben sem ő, sem más nem adhat felmentést a törvényi kötelezettségek alól.<sup>261</sup> Az iskolákban végzett drogfogyasztási szokásokat feltérképező kutatások esetében az adatvédelmi biztos kizárólag azt a megoldást tartotta elfogadhatónak, ha az iskola nem kötelezi tanulóit arra, hogy alávéssék magukat kábítószer-fogyasztási ellenőrzésnek, mert erre sem az iskolának, sem a tanároknak törvényi felhatalmazása nincsen. Az adatvédelmi biztos szerint akkor várható el a drogfogyasztási szokásokról reális adatgyűjtés, ha a válaszadás önkéntes, ha az érintett diákok személyes adatait nem kezelik, és ha a diákok nincsenek fenyegetett helyzetben.

---

<sup>260</sup> *Adatvédelmi Biztos Állásfoglalása, 2006, 1734/K/2006-2. sz. ügyirat*

<sup>261</sup> *Adatvédelmi biztos beszámolója, 2002*



A házi orvosok körében 2003 folyamán nagy visszhangot váltott ki az Egészségügyi, Szociális és Családügyi Minisztérium megbízásából lefolytatott vizsgálat, amelyben az adatgyűjtők a roma lakosságtól olyan adatok közlését is várták, amelyek a világnézetükre, politikai hovatartozásukra, vallásosságukra vonatkoztak. A kérdőívben a roma lakosságot pejoratívan beállító feltételezések voltak, amelyen negatív értékítéletek közül kellett választaniuk. Az adatvédelmi biztos az állampolgári jogok általános biztosával együtt lefolytatott vizsgálat során kiadott ajánlásban<sup>262</sup> megállapította, hogy a kérdőív sérti mind az egyes megkérdezettek, mind az egyes roma és más halmozottan hátrányos helyzetű polgárok személyiségi jogait, (emberi méltóságát, becsületét, jó hírnevét) ugyanúgy mindkét (foglalkozási, illetve etnikai) csoport közösségének alapvető jogait is veszélyezteti. Az adatvédelmi biztos felkért mindenkit, hogy tartózkodjon a kérdőív kitöltésétől, és felhívta a kérdőívet összeállító figyelmét, hogy a jövőben tartózkodjon hasonló kérdéssor összeállításától.

Az egészségügyi adatok és a sajtószabadság kérdéskörében az adatvédelmi biztos még 1999-ben foglalt állást, hogy amikor egy szerző művében is leírta, hogy mely orvos, mely munkakörben, mely egészségügyi intézményben, milyen műhibákat vétett, és idézte a bírósági eljárások anyagait és újságcikkeket. A szerző a legtöbb információt a betegektől, az elhunytak hozzátartozóitól szerezte meg a források megjelölésével. Az adatvédelmi biztos vizsgálta, hogy az egészségügyi adatok kezelésének jogalapja megfelelő-e, illetve az adatkezelésbe az önkéntes beleegyezés megtörtént-e. Arra tekintettel, hogy az egészségügyről szóló törvény 112.§ (8) bekezdése alapján az egészségügyi dolgozó neve, munkahelye közérdekű adatnak minősül, az adatvédelmi biztos nem állapította meg az Avtv.. sérelmét.

---

<sup>262</sup> *Állásfoglalás a roma lakosság egészségügyi állapotával kapcsolatos felmérésről*, 2003. december 13. *Adatvédelmi biztos beszámolója*, 2003

## 11.4. Személyes adatok védelme a munkahelyen

### 11.4. 1. Munkahelyi privacyról az EU-ban

A munkaviszonnal kapcsolatos adatvédelmi szabályok és jogvitára okot adó körülmények számba vétele előtt, lényeges leszögezni, hogy az EU egyes tagállamaiban így Finnországban, vagy az új olasz adatvédelmi törvényben<sup>263</sup> speciális rendelkezések kerültek elfogadásra a munkahelyi privacy védelmében. A munkahelyi adatvédelem az EU egyes tagállamiban, mint például az Németországban a személyes adatok védelmének klasszikus területét jelenti. Az Európa Tanács Miniszteri Bizottsága 1989-ben ajánlást<sup>264</sup> adott ki a munkahelyi privacy védelmében, de ezt a törekvést nem követte további előrelépés a tagállamok részéről. Az EU intézményeiben többször kísérelték meg, hogy a munkahelyi privacy védelmében irányelv kerüljön elfogadásra, de eddig nem sikerült megegyezésre jutni a jogharmonizációs kötelezettségekről.

A 29-es munkacsoport a munkahelyi adatvédelem vonatkozásában több ajánlást<sup>265</sup> fogadott el, a legfontosabbnak a 8/2001. sz. állásfoglalás tekinthető, de emellett a munkavállalók teljesítmény értékelésére vonatkozóan is közös álláspontra<sup>266</sup> jutott a testület. A munkavállalók elektronikus kommunikációjának kérdéséről is fogadott el állásfoglalást<sup>267</sup> a 29-es munkacsoport.

---

<sup>263</sup> Personal Data Protection, Legislative Decree no. 196 of 30 June 2003 Titel VII.

<sup>264</sup> [Recommendation No.R\(89\) 2](#) on the protection of personal data used for employment purposes (18 January 1989) and [Explanatory Memorandum](#).

[http://www.coe.int/t/e/legal\\_affairs/legal\\_co%2Doperation/data\\_protection/documents/international\\_legal\\_instruments](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international_legal_instruments); 2006.12.14.

<sup>265</sup> Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten; [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2001/wp48de.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48de.pdf); 5062/01/DE/engd. WP 48

<sup>266</sup> Empfehlung 1/2001 Beurteilungsdaten von Beschäftigten angenommen am 22.3.2001; [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2001/wp42de.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp42de.pdf)

<sup>267</sup> Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten Angenommen am 29. Mai 2002; [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2002/wp55\\_de.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_de.pdf); 2006.12.01.

#### 11.4.2. A magyar munkahelyi privacyról

A munkahelyi privacy kérdését az Mt. a Ktv. és a Kjt. is eltérően szabályozza. Az Mt. 77. § (1) szerint „a munkavállalótól csak olyan nyilatkozat megtétele vagy adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely személyiségi jogait nem sérti és a munkaviszony létesítése szempontjából lényeges tájékoztatást nyújthat”. A munkáltató a munkavállalóról a munkaszerződés megkötéséhez, az általa elvégzendő munkakör betöltésére vonatkozó képességekről széleskörűen akar informálódni, hogy a számára leginkább megfelelő munkavállalót választhassa ki. A munkáltatók megismerik a munkavállaló természetes azonosítóit, iskolai végzettségét, családi állapotát, gyermekeik számát és életkorát. Az Mt. 77.§ (1) bekezdése kevés eligazodást nyújt arra, hogy melyek azok a személyes adatok, amelyek a munkáltató számára tabunak számítanak. Az Mt. 77.§ (2) bekezdése kizárólag a terhesség megállapításra vonatkozó egészségügyi adat megszerzését tiltja a munkáltató számára.

*„A munkakör betöltéséhez szükséges alkalmassági vizsgálatok elvégzése sem sértheti a munkavállaló személyiségi jogait, azok elvégzéséhez a munkavállaló beleegyezése szükséges – A munkavállaló beleegyezésével (orvosi titoktartás alóli felmentés) – amely a munkaköri alkalmasságát érintő kétely esetén az együttműködési kötelezettsége teljesítését jelenti – az alkalmassági vizsgálat céljához kötötten az orvos a háziorvostól információkat kérhet<sup>268</sup>”*

A közszerződési jogviszonyokra a köztisztviselők jogállásáról szóló 1992. évi XXIII. törvény szabályai mellett az Mt. 77.§-t kell alkalmazni. Az államigazgatási szféra munkáltatói számára a Ktv. sokkal szélesebb mértékben kinyitja a munkavállalók magánszféráját, mivel a munkáltatónak biztosítani kell az összeférhetetlenség követelményét, továbbá a Ktv. előírja munkavállalók kötelező minősítését, illetve a közszerződési munkakörök egyes

---

<sup>268</sup> MÜ BH 2005/367

betöltőit vagyonyilatkozat tételre kötelezheti a munkáltató. A Ktv. 4. melléklete sorolja fel azokat a munkavállalói adatokat, amelyeket a köztisztviselőnek a központi közszolgálati nyilvántartás<sup>269</sup> számára meg kell adnia. A közalkalmazottak jogviszonyára vonatkozó 1992. évi XXXIII. törvény melléklete szintén felsorolja azokat az adatokat, amelyeket a közalkalmazotti nyilvántartás körében a munkáltató kezelhet. A Kjt-nek egyes ágazatokban történő végrehajtásáról kormányrendeletek rendelkeznek, amelyek közül például a 257/2000. (XII.26.) Korm. rendelet a Kjt-nek a szociális és gyermekjóléti ágazatban történő részletes alkalmazását rendezi, és meghatározza az alkalmazandó minősítési lap kötelező tartalmát.

A munkavállalók magánszférájának védelme szempontjából az Mt. 3.§ (4) bekezdése is jelentősséggel bír, amely előírja, hogy a „A munkáltató a munkavállalóra vonatkozó tény, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet. A munkavállalóra vonatkozó adatok statisztikai célra felhasználhatók és statisztikai célú felhasználásra - személyazonosításra alkalmatlan módon - átadhatók.”

Az adatvédelmi biztos gyakorlatát áttekintve a munkahelyi privacyval kapcsolatban megállapítható, hogy a panaszok száma viszonylag csekélynek mondható, amelynek több oka is lehet. Egyrészt a munkavállalók relatíve kiszolgáltatott helyzete, amelyben az őket ért jogsértéseket egzisztenciájuk védelmében inkább eltűrik. Az adatvédelmi biztos a panaszok alacsony számát >a rendszerváltozás utáni időszak nagyobb munkavállalói függőségének, kiszolgáltatottságának, korábban kivívott – noha gyakran kiüresedett – munkavállalói jogok erodálódásával, rosszabb érvényesíthetőségével, a munkahelyi érdekképviselők visszaszorulásával, a „klasszikus kapitalista” munkaviszonyok elterjedésével<sup>270</sup> magyarázza.

---

<sup>269</sup> 233/2001. (XII. 10.) Korm. rendelet

<sup>270</sup> *Adatvédelmi Beszámoló, 1997*, munkáltatókról szóló fejezete

A munkahelyi privacy védelmének speciális szabályait a munkáltató és a munkavállaló között létrehozott munkaviszonyra tekintettel kell kialakítani. A felek között megkötött munkaszerződés (közszolgálati jogviszonyban kinevezés) alapján a munkavállaló arra vállal kötelezettséget, hogy a munkáltató széles körű utasítási jogát elfogadja, és a munkáltató által meghatározott rendszerességgel, személyesen, a munkáltató ellenőrzése mellett, a munkahelyi fegyelmi rendet és a jogszabályokat betartva munkát végez, a munkáltató számára hasznot hajt, ezért cserébe a dolgozónak ellenszolgáltatást fizet. A munkahelyi privacy korlátozását megengedi, a munkáltató legitim érdekei, amelyek közé sorolható a munkáltatónak a munkavállaló kiválasztására, a munkavégzés rendjére, a munkaviszony fenntartásához, vagy éppen a gazdasági, üzleti érdekei védelmében végzett ellenőrzési tevékenységéhez kapcsolódó személyes adatkezelés.

A felek között kialakított munkajogviszonyra nem csak az irányadó foglalkoztatási törvény előírásai vonatkoznak, hanem a magyar jog alkotmányos jogelvei is, amelyek közvetetten, a Ptk. személyiség védelmi előírásain vagy az Avtv. szabályain keresztül érvényesülnek a felek közötti jogviszonyban. A munkavállaló magánszférájának a korlátozása során nem lehet az általános jogelveket, mint az arányosság és a szükségesség, továbbá az adatvédelem alapelveit, mint a célhoz kötöttség elvét, a törvényes és tisztességes adatkezelés elvét, a lehető legkevesebb személyes adatgyűjtésre való törekvés elvét, és a korlátlan adatgyűjtés tilalmát figyelmen kívül hagyni. A munkahelyi privacy első alapkérdése, hogy a munkáltató a munkaviszonnyal kapcsolatosan milyen jellegű személyes adatokat kezelhet, és melyek kezelésére nincsen törvényes felhatalmazása. Személyes adatként kell kezelni a munkavállaló természetes azonosítóit, de ebbe a körbe sorolhatók, a béradatok, a közalkalmazotti vagy a közszolgálati nyilvántartás keretében kezelt adatok, a családi állapot vagy a nyugdíjjogviszony fennállására vonatkozó adat, továbbá a büntetett előélet alóli mentesülés ténye, de személyes adatként kell kezelni a video készülékekkel készített felvételeket

is. Ha a felek a munkaszerződésben eltérően nem rendelkeztek, akkor személyes adatként kezelendők a munkavállaló által folytatott elektronikus levelezés adatai és a munkavállaló által látogatott weboldalak is, bár erre a kérdésre az e-privacy témakörben részletesebben kitérek. A munkaviszonnyal kapcsolatosan személyes adatként kell kezelni a munkavállaló teljesítményére, személyiségére vagy a minőségbiztosítás keretében az ügyfelektől és munkatársaitól róla gyűjtött adatokat.

A munkahelyi privacy sérelmével kapcsolatos jogeseteket három csoportba lehet sorolni. Az első kategóriába azok az esetek tartoznak, amelyekben a munkáltató legitim cél nélkül, túlzott vagy készletező módon gyűjt személyes vagy különleges adatot munkavállalójáról. A második csoportba azok a jogsértések sorolhatók, amelyekben az érintett adatbirtokos az őt megillető jogokat nem gyakorolhatja. A jogesetek harmadik kategóriáját képezik azok a jogkérdések, hogy a munkáltató milyen feltételek mellett továbbíthatja vagy hozhatja nyilvánosságra munkavállalójának személyes adatait.

Az adatkezelésekkel kapcsolatos felhatalmazások alapulhatnak egyrészt jogszabály általi jogcímen, illetve az adatbirtokos által adott előzetes, önkéntes és tudatos felhatalmazáson. A munkaviszonyban az adatbirtokos alárendelt félnek tekinthető, ezért az önkéntesség megléte a felhatalmazás törvényességének kulcskérdése, és az önkéntességet minden körülmények között biztosítani kell. A munkáltató részére adott személyes adatok kezelésére vonatkozó felhatalmazás adatvédelmi szempontból akkor támadható, ha a felhatalmazás megadása nem önkéntesen történik a munkavállaló részéről. Az utasításra történő hozzájárulás nem önkéntes, így nem is tekinthető adatkezelésre alapot adó hozzájárulásnak. A már munkaviszonyban álló dolgozók egzisztenciális kényszere, illetőleg a saját döntése körülményeiben való tájékozatlansága – valódi akarat hiányában - kétségessé teszik hozzájárulásuk érvényességét. Önkéntességről ugyanis csak akkor beszélhetünk, ha a dolgozók biztosan tudják, hogy a részvétel megtagadása esetén nem érheti őket hátrányos megkülönböztetés. Ha ez

számukra kétséges, tehát alappal tarthatnak a munkáltató rájuk nézve hátrányos intézkedésétől, akkor a hozzájárulás nem lehet önkéntes. Nem beszélhetünk valódi önkéntességről akkor sem, ha a hozzájárulás megtagadása esetén az érintetteknek munkájuk elvesztésével kell számolniuk.<sup>271</sup>

Adatvédelmi szempontból azok az esetek a legaggályosabbak, amikor a munkáltatók meg sem kísérlik a munkavállaló beleegyezését beszerezni egyes adatkezelésekhez, amelyekre a jogszabályok nem adnak számunkra lehetőséget. Így előfordult, hogy a munkáltató meg kívánta ismerni, hogy a munkavállaló a személyi jövedelem adójának 1%-t milyen célra kívánja fordítani, és előfordult a nyomásgyakorlás megengedhetetlen formája is<sup>272</sup>. Az adóeljárásról szóló törvényi előírások részletesen meghatározzák, hogy minden az adózást érintő tény, adat, határozat, igazolás adótitoknak minősül. Ebben az esetben a megszerzeni kívánt adatok kettős jogi védelem alatt álltak.

A munkáltatók számára nehézséget okoz, hogy egyes állami nyilvántartásokhoz használt azonosítókat milyen keretek között használhatják fel a munkavállalóval kapcsolatban. Az adatvédelmi biztos az egyik konzultációs eljárás során kifejtette, hogy a munkáltató a személyi azonosító kezelésére nem jogosult, mivel erre törvényileg nincsen felhatalmazva, illetve olyan törvényben meghatározott feladata sincsen, amelyhez ezen azonosító használata szükséges volna.<sup>273</sup> Az adatvédelem célhoz kötöttségének elvét sértené, hogyha a munkáltatók az adóazonosító jelet az adóhatóság felé történő adatszolgáltatáson túl más célokra, így mint például cégen belüli azonosításra használnák fel<sup>274</sup>. Adatvédelmi szempontból nem csak annak van jelentősége, hogy a munkáltató olyan adatokat kezeljen, amelyre törvényi felhatalmazással bír, hanem annak is, hogy azokat törvényes módon tárolja. A munkáltató jogosult az adóazonosító jel, a TAJ szám, és a személyazonosító használatára az utolsó négy számjegy nélkül, ám ezeknek elkülönített vezetéséről

---

<sup>271</sup> Adatvédelmi biztos beszámolója, 2003, 874/A/2003. sz. ügyirat

<sup>272</sup> Adatvédelmi biztos beszámolója, 1998, 510/K/1998. sz. ügyirat

<sup>273</sup> Adatvédelmi biztos beszámolója, 2001, 722/A/2001. sz. ügyirat

<sup>274</sup> Adatvédelmi biztos beszámolója, 2001, 691/A/2001. sz. ügyirat

gondoskodnia kell. Mindhárom azonosító együttes feltüntetése a bérkartonon, az adatvédelmi biztos szerint,<sup>275</sup> jogszabályt sért.

A munkavállalóknak joguk van arra, hogy az egyes munkakörökre olyan személyeket alkalmazzanak, akik egyrészt rendelkeznek a szükséges képzettségekkel, másrészt – ha bizalmas, nagy felelősséggel járó munkakörökről van szó – olyan háttérrel bírnak, amely a lehetséges kockázati tényezőket kizárja, vagy legalábbis csökkenti azokat. A munkavállalók kiválasztásához a munkáltatóknak számos személyes adatra szükségük lehet. A törvény nem rögzíti pontosan azon adatok körét, amelyet a munkáltatók kezelhetnek, az adatkezelésnek összhangban kell állnia a célhoz kötöttség elvével, amely ebben az esetben a munkaviszony rendeltetésszerű kialakítása és fenntartása. A munkahelyi privacyt sértő munkáltatói magatartás, hogyha a munkavállalót a munkaviszonnyal összefüggésben nem álló adatok megadására szorítják rá, vagy a munkáltató az arányosság követelményét megsértve túlzó módon vagy készletező cézzal gyűjt adatokat a munkavállalóktól.

A munkáltatók célja a minél nagyobb hatékonyság elérésére, ezért meghatározó számára, hogy a céljainak elérésére legalkalmasabb jelöltet vegye fel. A hatékonyság érdekében a kialakított munkaviszony során a humán erőforrás fejlesztésének, és a munkavállalók személyiségének, motiválhatóságának feltérképezése a munkaszervezés meghatározó elemévé vált. A személyiség feltérképezésének egyik eszköze a grafológiai vizsgálat. A munkaviszonyban a grafológiai vizsgálatot, a munkáltató törvényi felhatalmazás hiányában csak akkor alkalmazhatja, ha ahhoz a munkavállaló előzetesen hozzájárult. A személyiség vizsgálatára irányuló elemzések elvégzéséhez a már munkaviszonyban állók esetén az önkéntes hozzájárulás kétséges, ezért a munkaviszonyban álló személyekkel főszabály szerint a tesztek úgy kell kitöltetni, hogy azok később az egyes személyekkel ne legyenek kapcsolatba hozhatók. A pszichológusi személyiség vizsgálatokon

---

<sup>275</sup> *Adatvédelmi biztos beszámolója*, 1998, 272/A/1998. sz. ügyirat



alkalmazott adatlapok kitöltése előtt a kitöltővel közölni kell, hogy milyen kérdésekre vár választ az adatlapok elemzésével az elemzést elvégzett személy, illetve arról is tájékoztatást kell adni, hogy az adatoknak a kezelése milyen célból történik. A tájékoztatásban meg kell nevezni azt a személyt is, aki az elemzéseket el fogja végezni, és közölni kell, hogy kizárólag ez a személy fogja az érintett személy által adott válaszokat megismerni. Ha a pszichológiai tesztek nem tudja az elemzést elvégző személy azonnal átvenni, akkor a válaszlapok biztonságos őrzéséről a munkáltatónak kell gondoskodnia. Miután a pszichológus szakember az elemzést elvégezte, azt az érintett személynek meg kell mutatnia, aki dönthet arról, hogy az elemzés a munkáltatónak továbbítható-e.<sup>276</sup> A pszichológusi, vagy grafológusi szakvélemény tartalmazhat különleges adatokat is, (mint egészségi állapot, kóros szenvedély, szexuális szokások), amelyek megismeréséhez a munkáltatónak szükséges az érintett írásbeli hozzájárulása. A vizsgálat eredményének az összefoglalását, arra vonatkozóan, hogy a munkavállaló alkalmas vagy nem alkalmas a munkavégzésre, az érintett írásbeli hozzájárulása nélkül is megismerheti.<sup>277</sup> Az egészségügyi alkalmasság kérdése vonatkozásában számos panasz érkezett az adatvédelmi biztoshoz. A munkavédelmi törvénynek<sup>278</sup> az egészséget nem veszélyeztető és biztonságos munkavégzést előíró rendelkezései alapján a munkáltató csak munkára alkalmas személyt alkalmazhat. A munkáltatónak a munkavállaló az egészségügyi alkalmasságról előzetes, illetve időszakonkénti orvosi vizsgálat alapján kell döntenie. A szellemi dolgozók esetében, ahol általában nem jár együtt a munkavégzésük káros fizikai vagy vegyi hatásokkal, nem indokolt széleskörű adatgyűjtést és orvosi vizsgálatot végezni. Az egészségügyi alkalmassági vizsgálat részletes szabályait a 33/1998. (VI.24.) NM rendelet határozza meg, amely szerint a vizsgálatot végző orvos a munkáltatót csak összegző megállapításairól tájékoztathatja. Az adatvédelmi biztos a rendelettel kapcsolatosan az egészségügyi miniszterhez fordult, mivel meglátása szerint a

---

<sup>276</sup> *Adatvédelmi biztos beszámolója, 2004, 814/A/2004. sz. ügyirat*

<sup>277</sup> *Adatvédelmi biztos beszámolója, 1999, 227/A/1999. sz. ügyirat*

<sup>278</sup> 1993. évi XCIII. törvény a munkavédelemről 49.§-53.§

rendelet a célhoz kötöttség elvével összefüggésben nem álló módon rendkívül széles adatszolgáltatási kötelezettséget ró a munkavállalóra, másrészt az adatkezelést elrendelő jogszabály jogforrási szintje nem megfelelő. A miniszter nem tartotta szükségesnek a változtatást.

A munkavisztonnyal összefüggésben nem álló adatgyűjtésre példa, mikor egy kft főkönyvelője a dolgozókat egymás közötti, illetve céggel szerződéses viszonyban állókkal rokoni és baráti viszonyaikat feltáró írásbeli nyilatkozat megtételére hívta fel. A felhívásban a dolgozókat megfenyegették, hogy valótlán adatok közlése elbocsátást von maga után<sup>279</sup>. Az adatvédelmi biztos jogellenesnek állapította meg az adatkezelést. Egy másik esetben szintén a munkavisztonnyal össze nem függő adatkezelést állapított meg az adatvédelmi biztos, amikor a munkáltató az érintett munkavisztonyának létesítésekor anyagi helyzetére, és lakáskörülményeire vonatkozóan gyűjtött adatot<sup>280</sup>. Álláspontom szerint indokolatlan munkáltatói adatgyűjtésnek minősül, ha a munkáltató az érintett munkavállaló családi állapotára iránt érdeklődik, illetve a gyermekeinek számára és életkorára kíváncsi, mivel ezen adatok a munkavisztonnyal nem függenek össze szorosán, így sértik a célhoz kötött adatgyűjtés elvét. Az indokolatlan adatgyűjtés valósult meg szintén, mikor egyes közigazgatási szervek a náluk dolgozó köztisztviselőiket arra kötelezték, hogy nyilatkozzanak arról, hogy közszolgálati jogviszonyukon kívül milyen jövedelemforrással rendelkeznek, és milyen gazdasági társaságban érdekeltek. A köztisztviselők jogállásáról szóló 1992. évi XXIII. törvény 21.§ (2) szerint „köztisztviselő munkavégzésre irányuló egyéb és további jogviszonyt – tudományos, oktatói, művészeti, lektori, szerkesztői, valamint jogi oltalom alá eső szellemi tevékenység, továbbá a közérdekű önkéntes tevékenység kivételével – csak a munkáltatói jogkör gyakorlójának engedélyével létesíthet”. A Ktv. előírja, hogy köztisztviselő bizonyos kivételektől eltekintve nem lehet gazdasági társaság vezető tisztségviselője, vagy felügyelő bizottsági tagja. A törvényi előírások alapján nem kifogásolható, hogy közszolgálati

<sup>279</sup> *Adatvédelmi biztos beszámolója, 2001 184/A/2001. sz. ügyirat*

<sup>280</sup> *Adatvédelmi biztos beszámolója, 1999 828/A/1999. sz. ügyirat*

jogviszony létesítésekor a köztisztviselő nyilatkozzon, hogy az összeférhetlenségi követelményeknek megfelel. A későbbiekben azonban nem a munkáltató vagy munkahelyi vezető feladata az összeférhetlenség vizsgálata, hanem a köztisztviselő kötelessége az összeférhetlenség jelzése, amely elmulasztása fegyelmi vétség. A munkavégzésre irányuló egyéb jogviszonyt törvényben meghatározott kivételekkel be kell jelenteni, és azok létesítése a munkáltatói jogkör gyakorlójának engedélyével lehetséges. A kivételeket ugyanakkor - amelyekhez nem szükséges engedély – a köztisztviselőnek nem kell bejelentenie, amennyiben az a közszolgálati jogviszonyának ellátását nem akadályozza<sup>281</sup>.

A munkáltató számára különösen fontos, hogy az üzleti titkaik védelmére, és a társaság biztonságos működése érdekében a bizalmas munkaköröket számukra megbízható és feddhetetlen személyekkel töltsék fel. A bizalom kialakításához a munkáltató e munkakörök betöltőitől indokolt módon több személyes adatot kérhet, de csak ebben az esetben lépheti át az arányosság korlátját. Előfordul, hogy egyes munkáltatók a bizalmas munkakörök betöltőit adatlapok kitöltésére kötelezik. Az adatvédelmi biztos szerint az ilyen adatkezelés csak akkor lehet jogszerű, ha előre meghatározzák az egyes munkakörök betöltéséhez szükséges követelményeket, és ennek megfelelően azt az adatkört, amelynek ismerete alapján eldönthető, hogy a jelentkező alkalmas-e a munkakör betöltésére. Ha az adatlap más személyekre, így családtagokra vonatkozóan is kérdéseket tartalmaz, akkor előzetesen be kell szerezni az érintett személy hozzájárulását az adatkezeléshez. A munkáltató bocsáthat ki fontos és bizalmas munkakörök betöltésének szabályairól utasítást, de annak rendelkezései nem lehetnek ellentétesek az Avtv.-ben foglalt szabályokkal, mivel az Avtv. 1. § (2) bekezdése szerint az adatvédelmi törvényben foglaltaktól csak akkor lehet eltérni, ha azt a törvény kifejezetten megengedi.<sup>282</sup> A munkáltatók az üzleti titkaik és bizalmas információk védelmére vonatkozóan csak a megelőző, a munkajog viszonyban elfogadott,

---

<sup>281</sup> *Adatvédelmi biztos beszámolója, 2001, 178/A/2001, 406/K/2001, 200/A/2001.sz. ügyiratok*

<sup>282</sup> *Adatvédelmi biztos beszámolója, 2000, 234/K/2000. sz. ügyirat*

szabályozó jellegű intézkedéseket tehetnek. Az adatvédelmi biztos álláspontja szerint az üzleti titok megsértése esetén a munkáltatónak nincsen nyomozati joga, ha gyanúja merül fel, hogy az üzleti titkaival visszaélnék, akkor büntető feljelentést kell tennie.

Az adatvédelmi jogszabályok korlátozzák a munkáltatókat bizonyos intézkedések megtételétől, még akkor is, ha a munkáltató lényeges érdeke indokolná is az eszköz alkalmazását. Egy beadvány alapján 2000.-ben az adatvédelmi biztos első alkalommal nyilvánított véleményt a hazugságvizsgáló eszközöknek a büntetőeljárásen kívüli alkalmazásáról. Egy részvénytársaság vezetője – feltételezve, hogy a cégnél a munkavállalók lopnak – négyszáznyolcvan kérdésből álló személyiség tesztet, és egy poligráfos vizsgálatot is magába foglaló biztonsági kockázati ellenőrzést rendelt el. Az adatvédelmi biztos állásfoglalásában<sup>283</sup> rámutatott, hogy a hatályos jog kifejezetten meghatározza azokat a szervezeteket, amelyek jogosultak büntetőfelderítő eszközként definiált poligráffal vizsgálatot végezni. A büntetőeljárásen kívül, az ott érvényesülő eljárási garanciák mellőzésével, nyomozási céllal, „rendkívüli események felderítése” céljából, a már munkaviszonyban álló dolgozók „humán kockázati vizsgálata” céljából végzett hazugságvizsgálat nem jogszerű, mert ebben az esetben tényleges, önkéntes hozzájárulás az adatok kezeléséhez nem várható az érintettektől. A biztos a betöltetlen munkakörre jelentkezők esetében megengedhetőnek tartja a kockázati vizsgálat elvégzését, mivel ők még szabadon dönthetnek arról, hogy alávetik magukat a vizsgálatnak vagy sem<sup>284</sup>.

A munkahelyi privacy részét képezi, hogy az érintett munkavállaló a róla tárolt adatokat megismerheti, a köztisztviselő a közszolgálati nyilvántartás adataiba betekinthez, illetve a munkavállaló követelheti, hogy róla kizárólag a jogszabályokban előírt mennyiségű adatot tároljanak. Az érintett számára az adatvédelmi törvény alapján, ha más speciálisabb jogszabály a kérdést nem

---

<sup>283</sup> *Állásfoglalás a poligráf használatáról*, 2000. év

<sup>284</sup> *Adatvédelmi biztos beszámolója*, 2000, 354/A/2000.sz. ügyirat

rendezi a kérelem benyújtásától számított legrövidebb idő alatt, de legfeljebb 30 napon belül írásban, közérthető formában tájékoztatást kell adnia a munkáltatónak az általa kezelt adatokról. A munkáltató nem kötelezheti a munkavállalókat, hogy kérelmeiket írásban nyújtsák be, bár célszerű, ha a munkavállaló ezt megteszi, illetve az adatszolgáltatás nem függhet a felettes jóváhagyásától<sup>285</sup>. A tájékoztatásnak ingyenesnek kell lennie, kivéve akkor, ha az adott évben már hasonló jellegű kérelmet a munkáltató már teljesített.

Az adatvédelem általános kérdéseire tartozik a személyes adatok nyilvánosságra hozatalának megengedhetősége, és annak feltételeinek meghatározása. A panaszok tanúsága szerint gyakran előforduló eseteknek számítanak, hogy a munkáltatók jogosulatlanul hoznak nyilvánosságra személyes adatoknak minősülő adatokat. Munkajogi előírás, hogy a munkáltató a munkavállalóra vonatkozó adatot, tény, véleményt harmadik személlyel csak a törvényben meghatározott esetben, vagy a munkavállaló hozzájárulásával közölhet. Ennek ellenére egy esetben a munkáltató a vele jogviszonyban álló gazdálkodó szervezetek felé hirdetményben közzétette, hogy kinek, mikor, miért és milyen módon szüntette meg munkaviszonyát.<sup>286</sup> De olyan eset is előfordult, hogy a munkáltató egy érintett buszvezető munkavállaló munkaviszonyának megszüntetéséről szóló megállapodását a buszpályaudvar hirdető tábláján nyilvánosságra hozta<sup>287</sup>. Más esetben előfordult, hogy a munkavállalók bérjegyzékét olyan listán küldte ki a munkáltató, amelyhez az arra jogosulatlanok is hozzáférhettek<sup>288</sup>, ezekben az ügyekben az adatvédelmi előírások durva megsértését állapította meg az adatvédelmi biztos.

A nyilvánosságra hozatal mellett összetettebb adatvédelmi probléma, hogy a munkavállalók adatait lehet-e, és milyen körülmények között lehet harmadik személynek átadni. A szakszervezeteket megilleti a jog a munkaviszonnyal

---

<sup>285</sup> *Adatvédelmi biztos beszámolója*, 1998, 477/A/1998. sz. ügyirat

<sup>286</sup> *Adatvédelmi biztos beszámolója*, 1998, 559/K/1998. sz. ügyirat

<sup>287</sup> *Adatvédelmi biztos beszámolója*, 1997, 305/A/1997. sz. ügyirat

<sup>288</sup> *Adatvédelmi biztos beszámolója*, 1999, 132/A/1999. sz. ügyirat

összefüggő tájékoztatás kérésére, de ebből a jogosultságból nem következik, hogy a szakszervezet megismerhetné az egyes dolgozók béradatait. A szakszervezet a munkavisztonnyal kapcsolatos adatokat anonimizált, és statisztikai feldolgozásra alkalmas módon kaphatja meg<sup>289</sup>. Az Avtv.. 2004. január 1-je óta hatályos rendelkezései szerint különleges adat az „érdekképviseleti szerv tagságára” vonatkozó adat, mely csak az érintett írásbeli hozzájárulása vagy törvényi felhatalmazás alapján kezelhető. Miután olyan törvényi rendelkezés nincs, amely az érdekképviseleti szervezeti tagságra vonatkozó adatok kezelését elrendelné, azaz például a munkáltató számára lehetővé tenné ezen adatok nyilvántartását, egyértelmű, hogy csak az érintettek írásos hozzájárulása alapján lehet jogszerűnek tekinteni a szóban forgó adatok kezelését. Az érintett munkavállaló hozzájáruló nyilatkozatát magának a szakszervezetnek kell beszereznie. Az érdekképviseleti szervezeti tagságra vonatkozó adat megváltozott minősége a tagdíjak munkabérből történő levonásával összefüggésben is nehézséget okoz. Általános gyakorlat ugyanis, hogy a munkáltatók kezelik a munkavállalók tagságára vonatkozó adatot, és a tagdíjat meghatározott időnként levonják a munkabérből, és átutalják a szakszervezetnek. Az adatvédelmi biztos állásfoglalásában leszögezte, hogy a munkavállaló akkor kezelheti az érdekképviseleti tagságra vonatkozó adatokat, ha ahhoz az érintett munkavállaló írásban hozzájárult, és az adatkezelés célja meghatározásra került. A munkáltató szervezetrendszerén belül az adatokhoz kizárólag azok a személyek férhetnek hozzá, akiknek a feladataik ellátása érdekében szükségük van rá<sup>290</sup>. A munka világát érzékenyen érintő kérdés a fizetésre vonatkozó információ. A fizetés és prémiumok mértéke személyes adatnak tekintendő, amelyek nyilvánosságra hozatala kizárólag törvényi előírás alapján lehetséges. A munkajogi viszonyok esetén kizárólag az érintetten múlik, hogy hozzájárul-e a fizetésére vonatkozó adatok nyilvánosságra hozatalához, míg a közhatalom gyakorlásával szorosan

---

<sup>289</sup> Adatvédelmi biztos beszámolója, 1999, 678/K/1999. sz. ügyirat

<sup>290</sup> Adatvédelmi biztos beszámolója, 2005, 358/K/2004 és 314/H/2004. sz. ügyiratok

összefüggő jogviszonyok esetében a törvény<sup>291</sup> vagyonyilatkozat tétel keretében elrendeli a jövedelmek, és a fizetés összegének a nyilvánosságra hozatalát.

A munkavállalók adatai mellett egy gazdasági társaság az üzleti partnerei, és a vele kapcsolatban levő fogyasztók adatait is kezeli. Az üzleti életben előforduló stratégia, hogy egyes üzleti folyamatokat kiszerveznek a társaságból, és egy külső cégnek adják át a tevékenység folytatását. A tevékenység átadását követi a működéshez szükséges információk, és adatok átadása is, amely az adatfeldolgozásra alkalmas módon tömeges jelleggel fordul elő. Ez az outsourcing tevékenység kizárólag az adatvédelmi törvény keretei között történhet, azaz a külső társaság az adatkezelés eredeti céljától nem térhet el, és adatfeldolgozói tevékenységére vonatkozóan az adatkezelővel szerződéses keretben kell a garanciális szabályok betartását vállalnia. Az üzleti tevékenységük során egyes cégek a fogyasztóik személyes adataiból adatbázisokat készítenek, amelyeknek gazdasági értéke meghatározható, és akár jelentős értéket is képviselhet. Ha az adott társaság az adatbázisát egy általa alapított gazdasági társaságnak nem vagyoni jogosultságként át kívánja adni, akkor az apportálás szintén személyes adatok továbbításának minősül, amelynek meg kell felelnie az adatvédelmi előírásoknak. Az adattovábbítások speciális esete a gazdasági társaságokról szóló 1997. évi CXLIV. törvény 27.§ (2) bekezdésében rögzített előírás<sup>292</sup>, mely szerint „A vezető tisztségviselők kötelesek a tagok (részvényesek) kérésére a társaság ügyeiről felvilágosítást adni, a társaság üzleti könyveibe és irataiba való betekintést lehetővé tenni.” E jogszabályhely alapján egy gazdasági társaság vezető tisztségviselője úgy vélte, hogy két munkavállalóval kötött szerződés nem szolgálja a társaság üzleti érdekeit, ezért a

---

<sup>291</sup> Az országgyűlési képviselők jogállásáról szóló 1990. évi LV törvény 19.§-a, a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2006. évi LVII. törvény 10.§-a

<sup>292</sup> Az új Gt 27.§ (2) bekezdése: *A vezető tisztségviselők – ha e törvény másként nem rendelkezik – kötelesek a tagok (részvényesek) kérésére a társaság ügyeiről felvilágosítást adni, a társaság üzleti könyveibe és irataiba való betekintést lehetővé tenni.*

munkavállalók személyes adatainak továbbítása mellett, tájékoztatta erről fő részvényesét. Az adatvédelmi biztos megállapította, hogy az adattovábbítás jogszerűtlen volt, mert a részvényes nem kérte a felvilágosítás megadását, így a vezető tisztségviselő az adattovábbításra való törvényi felhatalmazás hiányában továbbította a munkavállalók személyes adatait.<sup>293</sup> Az adatvédelmi biztos felfogása szerint a munkáltató tulajdonosa (fenntartója, irányítója, vagy felügyeleti szerve) harmadik személynek minősül, így az adatokat csak akkor ismerheti meg, ha arra törvény felhatalmazást ad, vagy az érintett ahhoz megfelelő tájékoztatás után hozzájárult<sup>294</sup>. A munkáltató jogutódlása esetén a jogutód munkáltatóra szállnak át a munkaviszonyból származó jogok és kötelezettségek a jogutódlás időpontjától. A jogutódlással a jogutód adatkezelőként is a jogelőd helyébe lép<sup>295</sup>.

A munkahelyi privacy védelmével kapcsolatosan a panaszok számának növekedése 2001 után azzal magyarázható, hogy a munkavállalók érzékenysége nőtt, mivel a munkáltatók erőfölényüket kihasználva az új információ technológiák elterjedésével (e-mail, internet, videokamerák) visszaélnek, illetve a magyar jogban még nem léteznek kellően világos szabályok ezen új problémák rendezésére.

A telefonhívásokkal kapcsolatosan az adatvédelmi biztos kijelentette, hogy mind a hívó, mind a hívott fél személyes adatának minősül az, hogy az adott időpontban beszélgetettek, és hogy azt egymással tették. Az is személyes adatnak minősül, hogy a hívó és a hívott fél között valamilyen kapcsolat van. Tekintettel arra, hogy a hívott fél hozzájárulásának a beszerzése gyakorlatilag nem lehetséges, a híváslisták készítése még a munkavállaló hozzájárulása esetén sem jogszerű<sup>296</sup>. A telefonköltségek csökkentése elérhető a magán célú telefonálás megtiltásával, illetve nyilvános hozzáférésű telefonkészülék felszerelésével. A munkáltatók által közkedvelt megoldás, hogy egy bizonyos

---

<sup>293</sup> *Adatvédelmi biztosi beszámoló*, 2000, 191/A/2000.sz. ügyirat

<sup>294</sup> *Adatvédelmi biztosi beszámoló*, 2003, 692/A/2003 sz. ügyirat

<sup>295</sup> *Adatvédelmi biztosi beszámoló*, 2003, 819/A/2003 sz. ügyirat

<sup>296</sup> *Adatvédelmi biztosi beszámoló*, 2000, 764/K/2000.sz. ügyirat



összeghatárig engedélyezi a magáncélú használatot, illetve a külföldre vagy bizonyos számokra irányuló hívásokat engedélyhez köt. Az is bevett gyakorlat, hogy a munkáltatók kódot vezetnek be, amely azonosítja a hívást kezdeményező felet. E megoldás esetében elegendő a munkavállaló hozzájárulását beszerezni, ha a hívott felet vagy annak telefonszámát nem azonosítja a rendszer. Az adatvédelmi biztosnál panaszt tett egy munkavállaló, hogy a saját telefonszáma mellett, az általa kezdeményezett hívások listáját is át kellett adnia a munkáltatója részére. Bizonyos készenléti munkakörök esetében elfogadható, hogy a munkáltató elérhesse a munkavállalót, ha ő az adatkezeléshez önként hozzájárult. Ezzel szemben az adatvédelmi biztos a munkáltatónak a munkavállalójának saját telefonjáról kezdeményezett hívások vonatkozásában tett intézkedését az adatkezelés célhoz kötöttségének elvével nyilvánvalóan ellentétesnek találta.

Az egyik panaszos a levéltitok sérelme miatt fordult az adatvédelmi biztoshoz. A levéltitok védelmének alkotmányos jogát a Ptk., és a Btk. is védi. A levéltitok védelmét olyan szabályokkal kell biztosítani, amelyek a levél tartalmát, adatait védik attól, hogy azt jogosulatlanok megismerhessék. A levéltitok védelmével kapcsolatos panaszok többnyire az iratkezelési szabályzatok hiányosságait kifogásolják. A levelek iratkezelése során törekedni kell arra, hogy minden beérkező hivatalos irat iktatása kerüljön, annak nyomon követése biztosítva legyen, másrészt a magánlevelek címzettjei számára biztosítani kell a levéltitok védelméhez fűződő jogot. Korábban a 40/1998. (III.6.) Korm.rendelet szabályozta a kormány, a minisztériumok és az országos hatáskörű államigazgatási szervek iratkezelési mintaszabályzatát. A levéltári törvényt módosította 2005. évi CXLIX törvény, amely alapján a beiktatott új 10.§-a előírja, hogy a közfeladatot ellátó szervezet egyedi iratkezelési szabályzatot ad ki. Mivel a levelek magánjellege nem minden esetben állapítható meg egyértelműen, az adatvédelmi biztos azt javasolta,

hogy a névre szóló, megállapíthatóan magánjellegű levelek felbontása során kétségek elkerülése érdekében a címzettel bontassák fel a levelet<sup>297</sup>.

Az elektronikus levelezés munkahelyeken történő elterjedésével a munkavállalók egyre több panasszal fordultak az adatvédelmi biztoshoz, hogy tájékozódjanak, konzultáljanak, illetve a munkáltatók jogellenes adatkezelési tevékenységét bejelentsék. Az egyik beadványozó aziránt érdeklődött, hogy a munkáltató jogosult-e megismerni a munkahelyi számítógépén folytatott elektronikus levelezést. Az adatvédelmi biztos válaszában kifejtette, különbséget kell tenni a munkavállaló személyes használatára adott, esetleg nevét, vagy nevének töredékét is tartalmazó, valamint az olyan e-mail címek között, amelyek a cég ügyeinek intézését szolgálják, és nem egy-egy munkavállalóhoz kötöttek. Ez utóbbiakon folytatott levelezésbe a munkáltató betekinthet, még akkor is, ha e címek valamelyikén a munkavállaló magánjellegű levelezést folytatott. A személyes e-mail címen folytatott levelezést a hagyományos magánjellegű levelezéshez hasonlóan kell megítélni, így a munkáltató nem ismerheti meg, azokat nem semmisítheti meg a munkavállalójának a hozzájárulása nélkül.<sup>298</sup>

A munkáltató a munkavégzés ellenőrzése céljából a munkavállaló tudta nélkül annak számítógépén tárolt összes adatát lemásolta. Az adatvédelmi biztos a munkáltatói ellenőrzéssel kapcsolatban azt kifogásolta, hogy az ellenőrzésről, és annak körülményeiről a munkavállalókat előzetes nem tájékoztatták. Az adatvédelmi biztosnak e tárgyban kiadott állásfoglalása<sup>299</sup> szerint különbséget kell tenni a beérkező magánlevelek - amelyek tartalmát a munkavállaló nem tudja kontrollálni – és a kimenő levelek között. A beérkező leveleket a munkáltató nem ismerheti meg, kizárólag arra van jogosultsága, hogy a munkavállalót utasíthatja, hogy az elektronikus postafiókról ne folytasson magánlevelezést. A munkáltató e levelezést kizárólag a munkavállaló hozzájárulásával ismerheti meg. Ha a munkáltató az ellenőrzés során az

---

<sup>297</sup> *Adatvédelmi biztosi beszámoló, 1998, 791/K/1998. sz. ügyirat*

<sup>298</sup> *Adatvédelmi biztosi beszámoló, 2000, 772/A/2000. sz. ügyirat*

<sup>299</sup> *E-mail küldésekkel kapcsolatos adatkezelés, 2005*

érintett hozzájárulása nélkül mégis betekintene a beérkező levelek tartalmába, akkor azokat az adatokat nem kezelheti, nem használhatja fel. A munkavállaló által írt levelek esetén a munkáltató jogosítványai már jóval szélesebbek, mivel a munkavállaló a levél elküldésével hozzájárulását adta a saját személyes adatainak a megismeréséhez és kezeléséhez,<sup>300</sup> mivel a munkáltató tulajdonában álló szerverre továbbította a küldeményt postázás céljából. Ha a munkavállaló által használt számítógép merev lemezének ellenőrzése során – a munkáltató korábbi utasítása ellenére személyes adatokra bukkan, akkor azokat saját maga, a munkavállaló tudta nélkül nem törölheti. A munkáltató az ellenőrzése során tudomására jutott személyes adatokat nem kezelheti, azokat nem használhatják fel.

A munkavállalók nemcsak az elektronikus levelezéssel kapcsolatban szokták ellenőrizni a munkavállalókat, hanem arra is kíváncsiak, hogy a munkaidejüket ténylegesen munkavégzésre fordítják, vagy éppen szórakozásból szörfölgetnek a világhálón a munkavisztonnyal összefüggésben nem álló oldalakat nézegetve. A munkáltatók tevékenysége nem kifogásolható, ha a munkavállaló eszközeinek használatát ellenőrzi, de az ellenőrzés nem lehet korlátlan, mivel a munkáltatónak e jogkörében eljárva is be kell tartani az adatvédelmi előírásokat. Az a tény, hogy ki milyen oldalakat és milyen gyakorisággal tekint meg személyes adatnak minősül. A munkáltatónak az internetezési szokásokra kiterjedő ellenőrzési joga azon alapul, hogy a munkáltató kizárólag munkavégzés céljából engedélyezi, vagy magáncélból is engedélyezi a használatát. Ha a munkáltató kizárólag munkavégzési célból engedélyezi a világháló használatát, az ellenőrzése csak akkor jogszerű, ha e szándékáról a munkavállalók figyelmét előzetesen felhívta. Ha a munkáltató elmulasztja a tájékoztatást a munkahelyi internet használat korlátairól, illetve az ellenőrzésről és mégis kimutatásokat készít

---

<sup>300</sup> *Adatvédelmi biztosi beszámolója*, 2004, 120/A/2004. sz. ügyirat

dolgozók által látogatott oldalak IP címeiről, akkor ugyanolyan jogellenes adatkezelést végez, mintha a dolgozók telefonbeszélgetését hallgatná le<sup>301</sup>.

A munkáltató a vagyoni védelmi érdekei védelmében vagy az élet és testi épség megőrzése érdekében nem vitatható el azon joga, hogy megfigyelő kamerákat telepítsen. A vagyoni védelmi megfigyelő rendszer kiépítése során figyelembe kell venni a dolgozók személyiségi jogait, és az adatvédelem követelményeit. Egy telephelyen raktározott termékek őrzése céljából lehet megfigyelő rendszert felállítani, amely nem szolgálhatja a munkavállalók megfigyelését. A megfigyelő rendszert felhasználni a munkahelyi jelentét, vagy a munkavégzés intenzitásának ellenőrzésére csak a munkavállalók hozzájárulása esetén lehet, de ebben az esetben az önkéntesség igencsak kétséges lehet. Ezért a kamerák nem irányulhatnak olyan területre, amelyek megfigyelését vagyoni védelmi érdek nem támasztja alá, így például nem lehet megfigyelni a munkavállalók öltözőjét, vagy pihenőhelyét. A munkáltatók gyakran jelölik meg az adatkezelés céljaként a munkavállalók ellenőrzését. Kétségtelen, hogy a kamerák felszerelése és működtetése a munkáltató számára egyszerű megoldás, azonban a munkavégzés vagy a munkavállaló munkahelyi viselkedésének a megfigyelése, ellenőrzése azonban nem szolgáltat megfelelő jogalapot az adatkezeléshez. Ennek elsősorban azaz oka, hogy az elérni kívánt cél megvalósításához más eszközök is rendelkezésre állnak, amelyek kevésbé sértik és korlátozzák a munkavállaló alapjogait. A megfigyelő rendszer felállítása előtt tájékoztatni kell a munkavállalókat a rendszer legfontosabb jellemzőiről, így például, hogy a felvételek rögzítésre kerülnek, vagy nem. Ha a felvételek rögzítésre kerülnek, akkor tájékoztatást kell adni, hogy mennyi ideig tárolják a képeket. A képek tárolásának céljáról is tájékoztatást kell adni. Az adatvédelmi biztos szerint a kamerák által rögzített képeket, amelyeken a dolgozók képmása szerepel csak akkor lehet tárolni, ha fegyelmi vétség, szabálysértés, vagy bűncselekmény elkövetése azt

---

<sup>301</sup> *Adatvédelmi biztos beszámolója*, 2001, 570/A/2001. sz. ügyirat

indokoltá teszi<sup>302</sup>. Nem egyeztethető össze a törvénnyel, ha a felvételeket korlátozás nélkül rögzítik. Az érintetteknek joguk van tudni, hogy az adatkezelő mely személyes adataikat kezeli, és joga van megtekinteni a róla készült felvételeket is<sup>303</sup>. Egyre elterjedtebb megoldás a webkamerák interneten történő felhelyezése, és a kamera által felvett képek megtekintése. Ha egy beruházás vagy építkezés megvalósulásáról ad hírt a webkamera, akkor a képeket csak olyan módon közvetítheti, hogy azokon a munkavállalókat ne lehessen azonosítani. Ha a kamera látómezőjébe azonosítható személyek kerülnek, akkor az ő hozzájárulásukat be kell szerezni.

A munkáltatók a vagyonvédelem, a belső biztonság fokozása érdekében kiépítenek olyan beléptető és videokamerákra épülő megfigyelő rendszereket, amelyek tárolják az egyes munkatársak adatait, és alkalmasak személyazonosításra is, illetve a felvételeket automatikusan akár korlátlan időtartamra is képesek rögzíteni. Az adatvédelmi biztos szerint az adatgyűjtés indokolatlanul széles körre terjedhet ki, amely sérti az arányosság elvét, illetve garanciális szabályokat szükséges a működtetés során betartani. A munkahelyi belső biztonság fokozása érdekében a biztonságtechnikai cégek már kínálnak biometrikus azonosítási képességgel rendelkező összetett védelmi-megfigyelő rendszereket. A biometrikus azonosítók (ujjlenyomat, retina, írisz képe, a kéz geometriája, a hang és az arc jellemzői) személyes adatok. Ezen adatok kezelését a munkáltatónak nem írja elő semmilyen jogszabály, ezért ezen adatok kezelése előtt az érintettek, azaz minden jövőbeni felhasználó előzetes hozzájárulását be kell szereznie. Az adatvédelmi biztos a biometrikus azonosító rendszerek elvi bevezethetőségét nem vitatta, azonban felhívta a figyelmet, hogy a rendszer specialitásai vonatkozásában a video megfigyelési rendszerekre vonatkozó előírásoknál is több biztosítékot szükséges kiépíteni.

---

<sup>302</sup> Adatvédelmi biztos beszámolója, 1998, 461/A/1998. sz. ügyirat

<sup>303</sup> Adatvédelmi biztos beszámolója, 1999, 388/K/1998. sz. ügyirat

### 11.4.3. Egyetemi hallgatók személyes adatainak kezelése

Az adatvédelmi biztos a felsőoktatási adatkezelések vonatkozásában közleményt adott ki, így a felsőoktatási intézmények a felsőoktatási törvények alapján kizárólag a hallgatói jogviszonnal összefüggő adatokat kezelhetik. Más törvényi előírások előírják, hogy a felsőoktatási intézménynek nyilván kell tartani a hallgatók adószámát, és társadalombiztosítási azonosító számát, illetve az érintett beleegyezése alapján a szociális juttatások nyújtásához szükséges adatokat kezelhetik az intézmények. Minden más adatkezelés vonatkozásában az intézménynek be kell szereznie a hallgatók önkéntes és tájékozott beleegyezését az adatkezelésbe. Az adatvédelem biztos állásfoglalása szerint felsőoktatási intézmények összetett szervezete tekintetében felelős adatkezelőnek a tanulmányi osztályok minősülnek. A felsőoktatási intézményen belüli adattovábbításhoz be kell szerezni az adatbirtokos hozzájárulását.

### 11.5. Személyes adatok védelme a magyar hírközlési jogban

Az elektronikus hír- és távközlési eszközök robbanásszerű elterjedése természetszerűleg magával vonzotta azt a körülményt, hogy a magánéletünkben jelentős szerepet játszik a különböző elektronikus és mobil kommunikációs eszközök használata. A szolgáltatókra így különösen nagy felelősség hárul, hogy a közléseink bizalmasságát megőrizze, és a személyes adataink törvényi védelmének maradéktalanul eleget tegyen. A távközlés területén a személyes adatok védelme különösen fontos, mert nagyon könnyen személyiségprofil<sup>304</sup> készíthető a felhasználói adatokból. Így például a telefonos híváslisták alapján egyes személyek kapcsolatrendszerére és a személyek között meglévő kapcsolatok jellemzőire lehet a híváslistákból

---

<sup>304</sup> Marie-Theres TINNEFELD, H. TUBIES, *Datenschutzrecht*, München, Oldenburg Verlag, 1989, 2.

következtetni. Ezért az Avtv. előírásai mellett az elektronikus hírközlésről szóló 2003. évi C. törvény (továbbiakban: Eht.) XVII. fejezete szabályozza a személyes adatok kezelésének jogalapját, illetve az adatkezelés részletes szabályait. A szektorális adatvédelmi előírások kiegészítik az adatvédelem általános előírásait, ezért az elektronikus távközlési szolgáltatóknak is be kell jelentkezniük az adatvédelmi biztos által vezetett adatvédelmi nyilvántartásba<sup>305</sup>. Az elektronikus hírközlési szolgáltatások kapcsán a szolgáltatók nemcsak az érintett természetes azonosítóit kezelik, hanem tárolják az előfizetői állomás számát vagy egyéb azonosítóját, az előfizető címét és az állomása típusát, az elszámolási időszakban elszámolható összes egység számát, a hívó és a hívott előfizetői számokat, a hívás vagy egyéb szolgáltatás típusát, irányát, kezdő időpontját és a lefolytatott beszélgetések időtartamát, illetőleg a továbbított adat terjedelmét, mobil rádiótelefon szolgáltatásnál a szolgáltatást nyújtó hálózat és cella, valamint a szolgáltatás igénybevételekor használt készülék egyedi azonosítója (IMEI), IP hálózatok esetén az alkalmazott azonosítókat. A szolgáltatók kezelik a hívás vagy egyéb szolgáltatás dátumát, a díjfizetéssel és a díjtartozással összefüggő adatokat, tartozás hátrahagyása esetén az előfizetői szerződés felmondásának eseményeit, illetve a távbeszélő szolgáltatás esetén az előfizetők és felhasználók részéről igénybe vehető egyéb, nem elektronikus hírközlési szolgáltatásra, különösen annak számlázására vonatkozó adatokat.

Az Eht. előírja, hogy a szolgáltató személyes adatokat kizárólag az elektronikus hírközlési szolgáltatásra irányuló szerződés megkötése, a megállapodás tartalmának meghatározása, módosítása, illetve a szerződési kötelezettségek teljesítésének figyelemmel kísérése céljából kezelhet. A szolgáltató adatkezelését megalapozza a hírközlési szolgáltatások díjának számlázására, valamint az azzal kapcsolatos követelések érvényesítése is. A szolgáltató kezelheti a felhasználó, illetve előfizető azonosításához szükséges,

---

<sup>305</sup> KOPPÁNYI, *i.m.*, 334. old

illetve arra elégséges személyes adatot. Arra vonatkozóan, hogy mi tekinthető elégséges adatkezelésnek, a törvény teljes körű meghatározást nem rögzít, csak a legfontosabb adatok körét határozza meg, úgymint a szolgáltatás igénybevételének időpontjára, időtartamára és helyére vonatkozó adatot. A szolgáltató azon személyes adatok körét kezelheti még, amelyek a szolgáltatás nyújtásához műszakilag elengedhetetlenül szükségesek. Az adatvédelemben elfogadott adatminimalizálás alapelve az Eht. előírásai között is megjelenik, mivel a szolgáltató kötelezett arra, hogy az elektronikus hírközlési szolgáltatás üzemeltetése során olyan hírközlő eszközöket használjon, amelyek biztosítani tudják, hogy személyes adat kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez elengedhetetlenül szükséges. Az adatkezelés célhoz kötöttségének biztosítása érdekében az Eht. előírja, hogyha a szolgáltató az általa kezelt személyes adatot az arról való tudomásszerzését követően haladéktalanul törli, ha megállapítást nyer, hogy a szolgáltatónál nem a törvényben meghatározott célból került sor adatkezelésre.

Az érintettek megfelelő tájékoztatása érdekében az Eht. előírja, hogy a személyes adatok védelméről szóló törvényben meghatározott tájékoztatáson kívül a szolgáltatónak biztosítani kell, hogy a felhasználó az elektronikus hírközlési szolgáltatás igénybevétele előtt, illetve az igénybevétel során bármikor megismerhesse, hogy a szolgáltató, mely adatkezelési célokból milyen személyes adatokat kezel. A szolgáltatónak tájékoztatnia kell az előfizetőt a szolgáltatás biztonságát veszélyeztető, illetve a szolgáltató által megtett műszaki és szervezési intézkedések ellenére fennmaradó, ismert kockázatokról, továbbá a védelem érdekében az előfizető által tehető intézkedésekről. A tájékoztatásnak ki kell terjednie a felhasználó, illetve előfizető által, a továbbított közlések bizalmosságának védelme érdekében használható szoftver és titkosítási megoldás alkalmazásának lehetőségeire. Ha a szolgáltatás biztonságát érintő vagy veszélyeztető esemény következtében korábban nem ismert, új biztonsági kockázat jelentkezik, a szolgáltató



haladéktalanul tájékoztatja az előfizetőt a korábban nem ismert, új biztonsági kockázatról, a védelem érdekében az előfizető által tehető intézkedésekről, és azok várható költségeiről. A szolgáltató által nyújtott tájékoztatás nem mentesíti a szolgáltatót a védelem érdekében teendő, a szolgáltatás megszokott biztonsági szintjének visszaállítása érdekében szükséges intézkedések megtétele alól.

Az Eht. rendelkezései mellett az elektronikus hírközlési szolgáltatót kötelezik a személyes adatok védelmére, a szolgáltatás nyújtása során továbbított közlések bizalmas kezelésére, valamint a szolgáltatás biztonságával kapcsolatosan érvénybe lépnek egyéb részletszabályok<sup>306</sup> is, amelyek az azonosító kijelzés és hívásátirányítás feltételeit részletezik. Az elektronikus hírközlési szolgáltatóknak a személyes adatok kezelése során biztosítani kell, hogy az érintett a saját adataihoz hozzáférjen, továbbá biztosítani kell az adatkezelés hitelességét, a szolgáltatónak igazolnia kell az adatintegritást azaz, hogy az adatokat nem változtatták meg, illetve védenie kell a személyes adatokat a jogosulatlan hozzáférés ellen.

A távközlési szolgáltatónak az Avtv. 31/A.§ (1) c.) pontja szerint belső adatvédelmi felelőst kell megbízni, illetve szabályzatot kell alkotnia a személyes adatok kezelése tekintetében. A szabályzatban meg kell határozni a kezelhető adatok körét, ezen adatok tárolásának időtartamát és módját, illetve a személyes adatok továbbításának eseteit is. Az előfizetői szerződésben rögzíteni kell, hogy ha az előfizető a díj kiszámításához, illetve a díjvita eldöntéséhez a számlához csatolt hívásrészletezõn túl, a hívott felek telefonszámait tartalmazó részletes kimutatást kér. Ilyenkor fel kell hívni a figyelmét, hogy a kimutatással együtt az szolgáltatás igénybe vevő előfizető más természetes személyek előfizetői adataihoz juthat, amelynek megismerésére csak akkor jogosult, ha ahhoz a felhasználók hozzájárultak. A

---

<sup>306</sup> 226/2003. (XII. 13.) Korm. rendelet az elektronikus hírközlési szolgáltató adatkezelésének különös feltételeiről, az elektronikus hírközlési szolgáltatások adatbiztonságáról, valamint az azonosítókijelzés és hívásátirányítás szabályairól

rendelet előírása szerint a szolgáltató a hozzájárulás meglétét vagy annak tartalmát nem köteles vizsgálni, a hozzájárulásért kizárólag az előfizető tartozik felelősséggel. Ezen előírás nincs összhangban az Avtv. előírásaival, amely megköveteli, hogy az érintett személyes adatainak harmadik személy részére történő adattovábbításához történő hozzájárulása előzetes, önkéntes és tudatos legyen.

Az elektronikus hírközlési szolgáltató a közlés bizalmassága érdekében köteles megfelelő műszaki és szervezési intézkedésekkel gondoskodni arról, hogy a továbbított közlés és a közléshez kapcsolódó forgalmi adatok jogosulatlan lehallgatására, tárolására vagy megfigyelésére nem kerülhet sor, illetve a szolgáltató köteles arra, hogy a közléshez és az ahhoz közléshez kapcsolódó forgalmi adatokhoz történő jogosulatlan vagy véletlen hozzáférést megakadályozza. A szolgáltató csak olyan technikai eszközöket választhat, amelyek minden esetben alkalmasak arra, hogy biztosítani tudja a közlés bizalmasságát. Az Eht. azt is korlátozza, hogy a szolgáltató az általa továbbított közleményeket teljes körűen megismerhesse, így a szolgáltató a továbbított közlések tartalmát csak olyan mértékben ismerheti meg és tárolhatja, amely a szolgáltatás nyújtásához műszakilag elengedhetetlenül szükséges. Az adatbiztonság követelményének teljesítése érdekében a szolgáltató műszaki és szervezési intézkedésekkel köteles gondoskodni a nyújtott szolgáltatás biztonságának védelméről. Abban a tekintetben, hogy milyen műszaki és szervezési intézkedéseket kell a szolgáltatónak alkalmaznia, az Eht. csak annyi kötelezettséget rögzít, hogy a szolgáltatás nyújtásával általában jelentkező kockázatoknak megfelelő biztonsági szintet kell nyújtania a szolgáltatónak.

Az elektronikus hírközlési szolgáltatóknak nemcsak a közlések bizalmasságát kell biztosítaniuk, hanem azt is, hogy a nemzetbiztonsági szolgálatok és a

nyomozó hatóságok - külön törvényben foglaltak<sup>307</sup> szerint - közléseket megfigyelhessenek, lehallgathassanak, tárolhassák vagy a küldeménybe, közlésbe azok megfigyelése érdekében más módokon beavatkozhatnak. Az elektronikus hírközlő szolgáltatókat a titkos információgyűjtés és titkos adatgyűjtés során a hatóságokkal együttműködési kötelezettség terheli<sup>308</sup>. Az Eht. elég homályosan fogalmazza meg, hogy a nyomozó hatóság mely bűncselekmények esetén élhet titkos információgyűjtés eszközével. Az Eht. a védendő jogi tárgyakat így az életet, a testi épséget, a vagyont veszélyeztető fenyegetést, és a zsarolás alapos gyanúját határozza meg, amikor a nyomozóhatóság az előfizető vagy a felhasználó írásbeli kérelmére az előfizető vagy a felhasználó használatában lévő végberendezésen folytatott beszélgetés, üzenetküldés, e-mail levelezés útján vagy más módon továbbított közlést lebonyolítók személyes adatait megismerheti és rögzítheti.

A jogalkotó az Eht. keretei között felhatalmazta az elektronikus hírközlési szolgáltatókat, ahogy a hitelintézetek számára korábban a bankközi adós lista megalkotását is lehetővé tette, hogy a díjfizetési, illetőleg a szerződésből eredő egyéb kötelezettségek kijátszásának megelőzése, illetve a díjfizetési visszaélések megakadályozása céljából jogosultak egymásnak tájékoztatást adni, illetve másik elektronikus hírközlési szolgáltatónak a „fizetésképtelen előfizetők” személyes adatait átadni vagy attól átvenni, illetőleg ezen személyes adatokból közös adatállományt létrehozni. Az előfizető adatait a szolgáltató abban az esetben adhatja át, illetve az adatok akkor kerülhetnek be a közös adatállományba, ha számlatartozás miatt a szolgáltató a szerződést felmondta, vagy a szolgáltatás igénybevételét az előfizető számára korlátozta. A feketelistára kerülhet az érintett akkor is, ha számlatartozása miatt a szolgáltató bírósági vagy hatósági eljárást kezdeményezett az előfizető ellen, illetve az előfizető tartózkodási helye ismeretlen. A szolgáltató köteles az

---

<sup>307</sup> Lehallgatásokat biztosító törvények felsorolása

<sup>308</sup> 180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről

előfizetőt haladéktalanul tájékoztatni az adatátadás tényéről. Ha a feketelistára tétel oka megszűnt, akkor a szolgáltató köteles haladéktalanul intézkedni aziránt, hogy az érintett személyes adatai az adatbázisból törlésre kerüljenek.

A távközlési szolgáltatások igénybevételét az előfizetők számára megkönnyíti a telefonkönyvek, előfizetői címlisták összeállítása és nyilvános közreadása. A telefonkönyvek összeállítása a szolgáltató törvényi kötelezettsége, de felmerül ezen adatnyilvántartások rendeltetésszerű használatára vonatkozó szabályok betartásának kérdése. Ezen okból a nyilvános telefonkönyvek esetén az érintett személyekről a lehető legkevesebb adatot lehet közzétenni, és az előfizetők számára lehetővé kell tenni, hogy kívánságuk szerint a névjegyzékből kimaradjanak. Az Eht. előírja, hogy tilos a telefonkönyvben, az elektronikus előfizetői névjegyzékben és címtárakban levő személyes adatok összekapcsolása más adattal vagy nyilvántartással, kivéve, ha erre az elektronikus hírközlési szolgáltató működtetésének érdekében kerül sor. A direkt marketing eszközeinek törvényességi követelményeivel kapcsolatban már említettem, hogy az emberi beavatkozás nélküli, automatizált hívórendszer az előfizetők felhívása, és a velük való közvetlen kapcsolat teremtése tekintetében csak akkor alkalmazható közvetlen üzletszerzési vagy tájékoztatási célra, ha ehhez az előfizető előzetesen hozzájárult. A politikai célú direkt marketing tekintetében is hasonló korlátozó szabályt kellene elfogadni.

#### 11.6. A személyes adatok védelme és a direkt marketing

A direkt marketing üzleti eszközei elválaszthatatlanok a modern fogyasztói társadalomban nyújtott szolgáltatások reklámozásától. Az üzleti megrendelések elérése érdekében csomagküldő, illetve áruküldő cég alkalmaz direkt marketing nyújtotta módszereket, amelynek a lényege, hogy a fogyasztó névre szóló leveleket, csomagokat, termékmintákat kap, hogy az felkeltse az

érdeklődését az áru, illetve a szolgáltatás megrendelése iránt. A direkt marketing eszközei között találjuk a telefonos vagy a közvetlen személyes megkereséseket, hogy az ajánlataikkal rávegyék a címzetteket a megrendelésre, szolgáltatás igénybe vételére.

A direkt marketing az 1990-es évek kezdete óta alkalmazott kereskedelmi módszer Magyarországon, 1993 májusa előtt törvényi szabályozás nem rendezte ezt a kérdést, majd az adatvédelmi törvény előírásait tekintették irányadónak ezen a területén is. De szükség volt arra, hogy az adatvédelmi törvény egyes általánosnak tekinthető rendelkezése konkretizálásra kerüljön. Ezért az Országgyűlés az első szektorális adatvédelmi szabályozásként 1995 végen elfogadta a kutatás és közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvényt. A törvény hatályba lépését követően a még létező fekete- és szürkelisták legalizálására 1997 januárjáig adott haladékokot.

A direkt marketing tevékenységet végző cégeket több csoportra lehet osztani, így egyik körbe azok a társaságok tartoznak, akik saját termékeiket és szolgáltatásaikat igyekeznek a fogyasztók részére közvetlenül, névre szóló módon eljuttatni. A másik csoportba azok a társaságok tartoznak, akik más kereskedő, szolgáltató termékeit vagy információit juttatják el a megcélzott vevőkörhöz. Ezen üzleti szektorban tevékenykedők a tisztességes piaci magatartás megvalósítása érdekében létrehozták a Magyar Áruküldők Egyesületét<sup>309</sup>, amely saját etikai kódex alkalmazásával kíván az adatkezelés törvényes kereteinek betartásához hozzájárulni, kiegészítve a törvényi rendelkezéseket a piaci önszabályozás ezen eszközével is. A harmadik körbe azon társaságok tartoznak, akik névleges áruküldő tevékenység álcája mögé bújva, a fogyasztóknak az általuk megszerzett név és lakcímadataival kereskednek. A Kűtv. elfogadását követően folyamatosan felmerülő probléma, hogy azon cégek amelyek ugyan törvényes forrásból szerzik be a személyes

---

<sup>309</sup> <http://www.arukuldok.hu/>

adatokat, az érintetteket nem tájékoztatják az adatok forrásáról, az adatkezelés jellemzőiről, illetve az érintettek jogairól nem adnak tájékoztatás holott a Kükt alapján a kapcsolatfelvétellel egyidejűleg ez is kötelező lenne.

A direkt marketing törvény előírásai alapján a tudományos kutató, közvélemény-kutató és a piackutató, valamint a közvetlen üzletszerző szerv kapcsolatfelvétel céljából személyes adatot gyűjthet több forrásból is, elsősorban az érintett hozzájárulásával, de ezt nem teheti úgy, hogy az érintettet megtéveszti és a személyes adatait olyan cél érdekében gyűjti, amelyet egy másik céllal eközben leplezni próbál. Ilyen leplezett adatgyűjtések lehetnek az egyes nyereményjátékok, beküldendő részvény-feladványok szervezése, vagy utcai „közvélemény” kutatások.

A direkt marketing törvény alapján a személyes adatok megszerzhetőek olyan szervezettől is, akivel korábban az adatkezelő szerv, mint ügyfél, vagy támogató kapcsolatban állt. Személyes adatok gyűjtésére felhasználhatók a jogszerűen nyilvánosságra hozott név- és címjegyzékek, telefonkönyv, szaknévsor, statisztikai jegyzék. A gazdasági társaságok közötti ügyféllisták átadására csak akkor kerülhetne sor, ha az adatgyűjtéskor az érintettet tájékoztatták az eredeti céltől eltérő adat-felhasználási célról, illetve arról, hogy adatait átadását letilthatja. A személyes adatokat tartalmazó lista adásvételei esetén legtöbbször elmaradt az érintettek előzetes tájékoztatója. A közvetlen üzletszerzési tevékenységet végző cégeknek törvényi felhatalmazásuk van arra, hogy a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény hatálya alá tartozó nyilvántartásokból egyes szempontok szerint meghatározott, és csoportosított adatlekérdezéseket tegyen, feltéve, ha az érintett polgár korábban nem tiltotta meg a személyes adatainak üzleti célú kiadását. A törvény az adatvédelem követelményeinek teljesítése érdekében előírja, hogy az érintettel a kapcsolatfelvétellel egyidejűleg írásban közölni kell, hogy a megkereső az adatokat milyen forrásból szerezte be. A tájékoztatásnak ki kell terjednie az

adatfelhasználás céljára, módjára, időtartamára, illetve arra, hogy az adatkezelő igénybe vett-e közreműködőt. A tájékoztatás során meg kell adni az adatkezelő nevét és címét, továbbá hogy az adatszolgáltatás önkéntes. Az érintettet tájékoztatni kell, hogy jogában áll adatainak a megjelölt célra vagy annak egy részére történő kezelésének a megszüntetését kérni. Az adatok megfelelő minősége érdekében az adatkezelőnek az érintett személlyel a cím adatok pontosságát, és időszerűségét közvetlen kapcsolatfelvétellel le kell ellenőriznie, vagy a személyi adat és lakcímnnyilvántartótól kell adatigénylést kérnie. A személyes adatok megfelelő minőségét és időszerűségét a törvény hat hónapos időtartamban szabja meg, azaz a személyes adatokat felhasználni annak leellenőrzésétől számított hat hónapon belül lehet.

Az adatátadást a törvény korlátok közé szorítja, de lehetőség van arra, hogy más ugyanazon tevékenységet végző személytől vagy szervtől hasonló tevékenységet végző szervezet, üzleti vállalkozás a személyes adatokat átvegye, ha az érintett ezt az adatátadást előzetes tájékoztatás után kifogásolta. Az adatátadásról mind az átadónak mind az átvevő szervezetnek nyilvántartást kell vezetnie, amelyet öt évig meg kell őriznie.

A törvényben elkülönítetten szabályozzák a tudományos célú adatkezelést, a közvélemény-kutatási és piackutatási célú adatkezelést, illetve a közvetlen üzletszerzésre irányuló adatkezelések részletes szabályait. A tudományos, illetve a közvélemény kutatási adatkezelések közös szabályának tekinthető, hogy mind a két tevékenységre vonatkozóan kutatási tervet kell készíteni, amelyben meg kell határozni a kutatási jogosultságot, a kutatás célját, a kezelendő adatok körét, és forrását, az adatkezelés folyamatát, továbbá azt, hogy az érintettek a jogukat milyen biztosítékok megléte mellett gyakorolhatják. A tudományos célú adatkezelések vonatkozásában is szükséges beszerezni az érintett hozzájárulását a személyes adatainak kezeléséhez, ez alól akkor van kivétel, ha az érintett személy az adatok felvételét, vagy átvételét megelőző harminc évvel meghalt, ha korábban hunyt

el az a személy, akinek a személyes adatainak a felhasználására sor kerül, akkor helyette az örököse, vagy közeli hozzátartozója adhatja meg a felhasználási engedélyt. Ha a személyes adatokat érintő tájékoztatási kötelezettség teljesítése a kutatás célját veszélyeztetné, akkor az adatgyűjtés befejezését követően kell az érintett személyt személyes adatainak a felhasználásáról tájékoztatni.

Az adatkezelési hozzájárulás beszerzésétől, illetve a tájékoztatási kötelezettség teljesítésétől akkor lehet eltekinteni, ha a kutatás célja szociális, népegészségügyi, közoktatási vagy környezetvédelmi célokkal van összefüggésben, illetve az érintettek nagy száma miatt a tájékoztatás, illetve a hozzájárulás beszerzése aránytalanul sok időt, költséget és emberi munkát igényelne.

A közvélemény kutatási céllal gyűjtött adatkezelések esetén egyik leglényegesebb előírás, hogy a kapcsolatfelvétel után az érintett név és lakcímét a válaszaitól elkülönítetten kell tárolni, hogy személye ne legyen azonosítható. A név és lakcím adatok újbóli felhasználására, illetve adatainak közös feldolgozására akkor kerülhet sor, ha ahhoz írásban, külön, és kifejezetten hozzájárult. Az adatkezelés során olyan technika módszert kell alkalmazni, amely lehetetlenné teszi a válaszadó személy adatainak és válaszáinak összekapcsolását. A közvélemény-kutatás során annak minden szakaszában biztosítani kell a megkérdezett személy teljes anonimitását, valamint a véleményadás önkéntességét. A közvélemény-kutatás eredményéből nem lehet olyan következtetésre jutni, amely az adatot személyre vonatkoztatja, vagy őt érinti.

A közvetlen üzletszerzési célú adatkezelések tekintetében a személyes adatok átvétele kizárólag a törvényben meghatározott forrásokból lehetségesek. A nem kereskedelmi célú versenyek és rejtvénypályázatok szervezése esetén, az abban résztvevő személyek személyes adatai csak akkor használhatók fel, ha



az érintettek figyelmét felhívták arra, hogy az adataikat közvetlen üzletszerzés céljára kívánják felhasználni, és ehhez ők írásban hozzájárultak. A személyes adatokat tartalmazó üzletszerzési listára vonatkozó jogügyletet írásos szerződésbe kell foglalni, amelyben a személyes adatok felhasználásának a feltételeit a törvény előírások alapján meg kell határozni. Az a szerződés, amely nem tartalmazza a személyes adatok kezelésének feltételeit és korlátait semmisnek tekintendő.

Az érintettnek joga van arra, hogy megtagadja, vagy letiltsa a név – és lakcím adatainak közvetlen üzletszerzésre irányuló kezelését, illetve harmadik személynek történő átadását. Az érintett ezen irányú kéréséről az adatkezelőnek mindazon harmadik személyeket tájékoztatnia kell, akik számára az adott személyes adat továbbításra került.

A direkt marketing üzleti tevékenység keretében az adatvédelmi biztoshoz számos olyan panasz érkezik, amely kifogásolja a személyes adatok kezelését. A megalapozott panaszok általában a társaságok közötti követhetetlen adatmozgásra, hiányos, nem megfelelő tájékoztatások miatt kerülnek megfogalmazásra. Egy 1997-ben indult vizsgálat a cég és a hozzá kapcsolódó társaságok közötti adatmozgásokat, és ezek adatkezelését kívánta felderíteni. Az egyik panaszos nevét és lakóhelyét, fényképét egy reklám anyagon úgy tüntették fel, mint egy korábbi nyereményjáték nyertesét, közben ő nem vett részt játéksorsoláson. A vizsgálat során kiderült, hogy a kft nem teljesítette a letiltási kérelmeket, többször nevet változtatott, miközben ugyanazt az adatbázist használta. Az adatvédelmi biztos az ajánlásában<sup>310</sup> leszögezte, hogy „egy adatkezelésnek csak egy adatkezelője lehet. Nem használhat közös direkt marketing adatbázist több önállóan bejegyzett cég. Amennyiben több cég közös direkt marketing célú akciót szervez, az érintett személyeket tájékoztatniuk kell arról, hogy ki a felelős adatkezelő, akivel vagy amellyel az

---

<sup>310</sup> *Közvetlen üzletszerzési adatkezelésekre irányuló panaszokra indított vizsgálat eredményeit összegző adatvédelmi biztosi ajánlás, Adatvédelmi biztos beszámolója, 1998, 398/A/1998. sz. üggyirat*

érintett kapcsolatban áll, valamint tájékoztatni kell az érintetteket az adatátadás tényéről, céljáról. Átadni (közös akcióban felhasználni) csak akkor lehet a név- és címlistán szereplő adatokat, ha az érintettek előzetes tájékoztatása megtörtént és az adatátadást (közös felhasználást) az érintettek nem tiltották meg. Ha egy közvetlen üzletszerzési módszereket alkalmazó cég megváltoztatja elnevezését, erről egyértelműen tájékoztatnia kell mind korábbi – még aktív – ügyfeleit, mind pedig az üzletszerző tevékenysége során megkeresett személyeket. A direkt marketing tevékenységet végző cégek adatkezelését és ügyiratkezelését oly módon kell kialakítani, hogy az mind az érintettek, mind a külső ellenőrzés számára átlátható legyen, a személyes adatok felhasználásának teljes folyamata követhetővé váljon. A nyilvántartásnak tartalmaznia kell a személyes adatok forrására és továbbítására vonatkozó adatokat (naplózás); az ügyiratokon, leveleken és más postai küldeményeken – beleértve azok borítékjait is – fel kell tüntetni a dátumot. A direkt marketing adatkezelőnek gondoskodnia kell arról, hogy az adataikat letiltók rendelkezését késedelem nélkül teljesítse és nyilvántartásba (tilalmi listára) vegye, és erről az érintett személy írásbeli visszaigazolást kapjon. Az adatkezelőnek az érintettekhez eljuttatott direkt marketing célú nyomtatványain egyértelműen és a magyar nyelv szabályainak megfelelően kell közölnie az adat forrását, az adat esetleges későbbi továbbítására vonatkozó információkat, valamint az adatletiltás érvényesítési lehetőségeit”.

A direkt marketing tevékenységet végző társaságoknak nemcsak az egyes kereskedelmi tevékenységek végzésének feltételeiről szóló előírások<sup>311</sup> szerint kell nyilvántartásba venni tevékenységüket, hanem az adatvédelmi biztos által vezetett adatkezelési nyilvántartásba is be kell jelentkezniük.

A direkt marketing tevékenység egyik módszere, hogy a cégek ügyfélkörüket úgy kívánják bővíteni, hogy a velük üzleti kapcsolatban lévő ügyfelektől

---

<sup>311</sup> Egyes kereskedelmi tevékenységek gyakorlásáról szóló többször módosított 15/1989. (X.7) KeM rendelet

ellenszolgáltatás érdekében azt kéri, hogy az ismerőseik név és lakcím adatait adják át a számukra. Abban az esetben, ha magánszemélyek által magáncélra tárolt adatokat a társaság üzleti céljai érdekében felveszi és tárolja, akkor beleütközik a Kútv előírásaiban, mivel a törvény taxatívén határozta meg a személyes adatok forrásának esetköreit, és ilyen jellegű adatgyűjtéseket a törvény nem nevesít.

A direkt marketing tevékenységgel kapcsolatosan az adatvédelmi biztos ajánlásban fogalmazta meg, hogy ha név és lakcím adatok mellett más személyes adatok, mint például egészségi állapotra utaló adatok is szerepelnek a küldeményben, akkor azt csak zárt borítékban lehet postára adni, a visszaküldendő nyílt levelező lapokon megadott személyes adatok kezelése nem felel meg az adatvédelem követelményeinek. Ha a direkt marketing cég személyes adatok gyűjtését postai úton folytatja, akkor az adatok zártan történő kezeléséhez szükséges borítékot neki kell a küldeményhez mellékelnie.

Az üzleti tevékenységek fejlődésével párhuzamosan a telemarketing területére 2002-ig nem sikerült speciális szabályokat alkotni, mivel a telefonon történő megkeresések esetében lehetetlen a Kútv szerinti írásbeli tájékoztatás megadása. Ennek a hiánynak a pótlására a hírközlésről szóló 2001. évi. XL törvény<sup>312</sup> 65.§-ában kerül sor. A személyes adatok közvetlen üzletszerzési célra történő felhasználása az emberi beavatkozás nélküli, automatizált hívórendszer az előfizető tekintetében csak akkor alkalmazható, ha ehhez az előfizető előzetesen hozzájárult. Közvetlen üzletszerzés célját szolgáló közlemény telefonon vagy egyéb távközlési úton nem továbbítható annak az előfizetőnek, aki úgy nyilatkozott, hogy nem kíván semmilyen reklámanyagot. Az elektronikus hírközlésről szóló 2003. évi C. törvény a korábbi szabályozást teljes mértékben átveszi és kiegészíti azzal, hogy az előfizető kifejezett hozzájárulása ellenére sem lehetséges olyan közvetlen üzletszerzési célú

---

<sup>312</sup> A hírközlésről szóló 2001. évi. XL törvény 2002.10.21-től 2003.12.31-ig volt hatályban.

küldemény továbbítása, amelyből nem ismerhetők fel a feladó azonosító adatai. A beszédcélú elektronikus hírközlési szolgáltatást nyújtó szolgáltatók kötelesek az egyetemes szolgáltatóknak átadni – az előfizető hozzájárulásától függően – az előfizetőkre vonatkozó azon adatokat, amelyek az országos belföldi tudakozó nyújtása, illetve előfizetői névjegyzék készítéséhez szükségesek. Az így átadott előfizetői adatok ettől eltérő célra nem használhatók fel.

A név és lakcím adatok egyik legnagyobb üzleti adatkezelőjének a Magyar Posta Zrt. tekinthető, amely rendszeresen végez olyan direkt marketing típusú megkereséseket, amelyek a lakosság igen széles körét érintik, és a magánélet, illetve a személyes adatok széleskörű feltérképezését célozza. Némely esetben az adatkezelő a részére történő adatok visszaküldését azzal fokozza, hogy az adatgyűjtést nyereménysorsoláshoz köti. Ugyan a Magyar Posta Zrt. adatkezelései megfelelnek a törvényi előírásoknak, de az adatvédelemi biztos azt tanácsolja akár nyilvános formában<sup>313</sup> is, hogy az állampolgárok legyenek körültekintőek, és ne adják ki a személyes adataikat olyan mértékben, amely személyiség profil létrehozását is lehetővé teszi.

Az Európai Unió döntéshozatali mechanizmusának befolyásolása érdekében a belső piacon érdekelt direkt marketing cégek létrehozták az ágazati szövetségüket FEDMA<sup>314</sup> névvel, amely egyrészt a kötelező szabályozást kiegészítve önszabályozás eszközével kívánja a direkt marketing piacot hatékonyabbá tenni, másrészt az információ technológia területén kialakításra kerülő új szabályozások vonatkozásában, így például a kereskedelmi célú e-mail küldések témakörében a direkt marketing üzleti tevékenységet végző vállalkozások érdekeit képviseli.

---

<sup>313</sup> Adatvédelmi biztosi beszámoló 2000, illetve *Adatvédelmi biztosi beszámoló, 2006*

<sup>314</sup> Europäischer Ehrenkodex für die Verwendung personenbezogener Daten in der Direktwerbung  
[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2003/2003-06-13-code-conduct-fedma\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/2003-06-13-code-conduct-fedma_en.pdf)

## 11.7. Hitelinformációs rendszerek és a személyes adatok védelme

### 11.7.1. Hitelinformációs rendszerekről általában

A magyar pénzügyi világban többször felvetődött a kérdés, hogy szükséges lenne olyan központi hitel-nyilvántartási rendszer kialakítása, amely hitelreferencia szolgáltatással támogatná a hitelezés biztonságát. A hitelreferencia-szolgáltatás az ügyfelek hiteleiről, illetve kölcsönfelvételéről szóló adatok begyűjtésével, feldolgozásával és nyilvántartásával biztosítaná azt, hogy ellenőrzött keretek szerint a hitelnyújtók a kölcsönnyújtási kérelem elbírálása során a leendő adós hitelezési és a kölcsönök visszafizetési szokásait megismerje. A hitel-referencia szolgáltatás biztosítaná, és támogatná a hitelezés biztonságát.

A Pénzügyi Szervezetek Állami Felügyelete átfogó tanulmányban<sup>315</sup> vizsgálta a pozitív adóslista bevezetésének jogi kérdései, és adatvédelmi korlátait. A közösségi jogban nem létezik speciális szabályozás a lakossági hitelinformációs rendszerekre vonatkozóan, bár felmerült egy egységes európai hitelnyilvántartó rendszer kialakításának igénye, de ezen a területen az együttműködés jogalkotási eredményeket nem produkált. A 95/46/EK adatvédelmi irányelv rendelkezései ezen a szolgáltatási területen is irányadóak, speciális rendelkezések nélkül. Az EU több tagállamában létezik valamilyen központi hitelnyilvántartó rendszer, ezek lehetnek kormányzati háttérű, kötelező nyilvántartási rendszerek<sup>316</sup>, illetve piaci alapon szerveződő credit bírók (CB). A hitelnyilvántartó rendszerek nem minden hitelügyletről gyűjtenek adatokat, általában valamilyen küszöbérték feletti ügyletekre vonatkozóan kerül sor adatkezelésre. Az adósnilvántartó rendszerek különböznek abban, hogy milyen típusú adatokat tárolnak, vannak olyan

---

<sup>315</sup> Háttéranyag a lakossági hitelinformációs rendszerekről 2006. augusztus [www.pszaf.hu](http://www.pszaf.hu) 2007.11.04

<sup>316</sup> Public Credit Registers PCRs

rendszerek, ahol már az elutasított hitelkérelem is rögzítésre kerül, nemcsak az adott hiteladósok a hátraléka vagy késedelme. A Németországban, és Ausztriában a jól fizető adókat is nyilvántartják. Az adatbázishoz történő hozzáférés eltérő jellegű, mivel általában a hitelnyújtók a régi illetve az új adósaikról kérhetnek le adatokat, máshol így Ausztriában a tagok bárkiről kérhetnek le adatokat.

#### 11.7.2. Központi hitelinformációs rendszer Magyarországon

A hitelintézetekről és a pénzügyi vállalkozásokról szóló többször módosított 1996. évi CXII. törvény XX/A. fejezete szabályozza Magyarországon a központi hitelinformációs rendszer (KHR) működését, amelyet a törvény zárt rendszerű adatbázisként definiál azzal a céllal, hogy a hitelképesség differenciáltabb megítélését és ezáltal a hitelezésnek szélesebb körű lehetővé tételét, valamint a referenciaadat-szolgáltatók biztonságosabb működése érdekében a hitelezési kockázat csökkentését elősegítse. A hitelinformációs rendszerben kizárólag a Hpt.-ben meghatározott, a szerződésre utaló referenciaadatok, illetve az adós azonosítását lehetővé tevő személyes adatok kezelhetők. A magyar hitelinformációs rendszer credit büro jellegű, azaz pénzügyi vállalkozás működteti a referenciaadatok teljes körű és naprakész nyilvántartását. A hitelnyújtó pénzügyi intézetek referenciaadat-szolgáltatóként kötelesek az általuk kezelt referenciaadatokat a hitelinformációs rendszer részére átadni. A pénzügyi intézetek a KHR-t kezelő pénzügyi vállalkozás részére átadják annak a természetes személynek, vagy jogi személynek az azonosítását biztosító adatait, aki hitelszerződésben, vagy más pénzügyi szolgáltatás nyújtására irányuló szerződésbe foglalt kötelezettségének oly módon nem tett eleget, hogy a lejárt és meg nem fizetett tartozásának összege meghaladja a késedelembe esés időpontjában érvényes legkisebb összegű havi minimálbért, és ezen minimálbérösszeget meghaladó késedelem folyamatosan, több mint kilencven napon keresztül fennállt. A KHR-t kezelő pénzügyi vállalkozás a referenciaadatokat öt évig kezeli. Az öt év letelte után a KHR-t kezelő

pénzügyi vállalkozás a referenciaadatokat véglegesen és vissza nem állítható módon törli.

Az ügyfelek jogainak védelme érdekében a Hpt. 130/J §-a előírja, hogy az érintett természetes személyek részére, a hitelt nyújtó pénzügyi vállalkozás a szerződés megkötését megelőzően, írásbeli tájékoztatást kell nyújtania, hogy az érintett adatai bekerülhetnek a KHR rendszerbe, azzal, hogy meg kell jelölnie az adatátadás célját, az átadható adatok körét, illetve a jogorvoslati lehetőségeket. Az érintettet továbbiakban a szerződés megkötését követően tájékoztatni kell, ismertetve a konkrét okokat arról, hogy személyes adatai bekerülhetnek a KHR-be. Abban az esetben, ha az adós szerződéses kötelezettségeit megsértené, akkor a referencia adatoknak a tervezett átadását megelőzően harminc nappal tájékoztatni kell arról, hogy az ügyfél személyes adatai bekerülnek a KHR-be, ha nem tesz eleget a szerződésben foglalt kötelezettségének. Az adóst a referencia adatok átadást követően legfeljebb nyolc napon belül tájékoztatni kell, annak megtörténtéről.

Bárki jogosult a Hpt. szerint meghatározott referenciaadat-szolgáltatónál tájékoztatást kérni arról, hogy milyen adatai szerepelnek a KHR-ben, és ezen adatait mely referenciaadat-szolgáltató adta át. Ebben az esetben a tájékoztatás iránti kérelmet a KHR-t kezelő pénzügyi vállalkozásnak kell haladéktalanul megküldeni, aki legkésőbb két munkanapon belül zárt módon megküldi a referenciaadat-szolgáltatónak az adatokat, aki a kézhezvételt követően ugyancsak zárt módon, kézbesítési bizonyítvánnyal feladott irat formájában haladéktalanul, de legkésőbb két munkanapon belül eljuttatja a kérelmezőnek. A tájékoztatás a kérelmező számára évente egy alkalommal díjtalan. További tájékoztatás kérése esetén a kérelmezőnek költségtérítést kell fizetnie, amely legfeljebb a kapcsolódó közvetlen költségek ellenértékét tartalmazhatja.

Az érintett személy a pénzügyi vállalkozás által nyilvántartott adatai vonatkozásában kifogást emelhet referenciaadatainak a KHR-t kezelő

pénzügyi vállalkozás részére történt átadása, illetve azoknak a KHR-t kezelő pénzügyi vállalkozás által történő kezelése ellen, és kérheti a referenciaadat helyesbítését, illetve törlését. A KHR-t kezelő pénzügyi vállalkozás a kifogást a nyilvántartott egyidejű értesítése mellett haladéktalanul, de legkésőbb két munkanapon belül köteles ahhoz a referenciaadat-szolgáltatóhoz megküldeni, amely a kifogásolt referenciaadatot a KHR-t kezelő pénzügyi vállalkozásnak átadta.

A referenciaadat-szolgáltató, illetőleg a KHR-t kezelő pénzügyi vállalkozás köteles a kifogást annak kézhezvételét követő tizenöt napon belül kivizsgálni, és a vizsgálat eredményéről a nyilvántartott érintett személyt írásban, kézbesítési bizonyítvánnyal feladott irat formájában haladéktalanul, de legkésőbb két munkanapon belül tájékoztatni. Ha a referenciaadat-szolgáltató a kifogásnak helyt ad, haladéktalanul, de legkésőbb két munkanapon belül köteles a helyesbített vagy törlendő referenciaadatot a nyilvántartott egyidejű értesítése mellett a KHR-t kezelő pénzügyi vállalkozás részére átadni, amely a változást haladéktalanul, de legkésőbb két munkanapon belül köteles átvezetni. Az érintett személy a nyilvántartott referenciaadatainak átadása és kezelése miatt, illetőleg azok helyesbítése vagy törlése céljából a referenciaadat-szolgáltató és a KHR-t kezelő pénzügyi vállalkozás ellen keresetet indíthat. A keresetlevelet a KHR-t kezelő pénzügyi vállalkozás által a kifogás elbírálására irányuló tájékoztató kézhezvételét követő harminc napon belül a nyilvántartott lakóhelye szerint illetékes helyi bírósághoz kell benyújtani vagy ajánlott küldeményként postára adni. Ha a KHR-t kezelő vállalkozás nem ad tájékoztatást, akkor a perindítási határidő attól számítandó, amikor a vállalkozásnak a tájékoztatást meg kellett volna adnia.

A bíróság végzésével már a tárgyalás előkészítése során elrendelheti a referenciaadatok kezelésének felfüggesztését, ha a rendelkezésre álló adatok alapján a kereseti kérelem megalapozottsága valószínűnek mutatkozik. A bíróság végzése a fellebbezésre tekintet nélkül előzetesen végrehajtható. A



referenciaadat-szolgáltatót, illetőleg a KHR-t kezelő pénzügyi vállalkozást terheli annak bizonyítása, hogy a referenciaadat átadásának, illetve KHR-ben történő kezelésének e törvényben meghatározott feltételei fennálltak. E körben a bizonyítás elmaradása vagy eredménytelensége a referenciaadat-szolgáltatót, illetőleg a KHR-t kezelő pénzügyi vállalkozást terheli.

### 11.7.3. A pozitív adólista magyarországi alkalmazásának kérdései

A pozitív adósnnyilvántartás bevezetése érdekében először 2002-ben a Bankszövetség az MNB-vel együttműködve tett javaslatot, majd 2006-ban a téma újra a szaksajtó érdeklődésébe került. A 2008 őszén kibontakozó hitelválság valószínűleg felgyorsítja a pozitív adólista bevezetését, annak érdekében, hogy jogi eszközökkel erősítsék meg a bankrendszer hitelezési oldalának stabilitását. A pozitív adólista bevezetésének többféle indokát jelölték meg a hitelezési piac szakértői. A lakossági hitelpiacon a hitelkereslet növekedését prognosztizálják amellet, hogy a negatív adólistán szereplők köre kb 500.000 fő nagyon magas a magyar háztartások létszámához viszonyítva. Ez a körülmény előrevetíti a hitelezési piac bővülése mellett annak egyre nagyobb kockázatát a hitelező oldalán, hogy nem ismeri teljes körűen a hitelkérelmező pontos adóssághelyzetét. A pénzpiaci szakértők számos okkal támasztották alá a pozitív adólista létrehozásának indokait, egyrészt a bankrendszer stabilitásával, mint nemzetgazdasági érdekekkel, ingatlanárak stabilitásának szükségességével, hitelköltségek csökkentésének lehetőségével, hitelkérelmező egyértelmű eladósodottsági visszajelzésével. A piaci tapasztalatok alapján a pozitív adólistát működtető piaci vállalkozás jogszabályi felhatalmazás nélkül nem tudta létrehozni a pozitív adólistát, mivel maguk a pénzintézetek önkéntesen a piaci alapon működő credit bürohoz nem szívesen csatlakoztak. A pozitív adósnnyilvántartó rendszer kötelező csatlakozáson kell alapuljon, központilag koordinált rendszerrel oldható meg, amely kizárólag a célhoz kötöttség elve alapján a hitelképesség

megállapítására vonatkozóan szolgáltatna adatokat tagja részére azzal, hogy az adatszolgáltatás biztonsági, és jogi garanciáit jogszabályban rögzítenék.

A pozitív adólista megítélése tekintetében az országgyűlési biztosok között ellentétes álláspont alakult ki. Lenkovics Barnabás az állampolgári jogok országgyűlési biztosa szerint a bankoknak és a hitelt felvevő ügyfeleknek is előnyös lenne a rendszeren fizető adósokról készített lista. A „jó adósok nyilvántartása” csökkenthetné a bankok hitelnyújtási kockázatát, miközben a rajta szereplő, megbízhatónak minősített adósok könnyebben juthatnának más hitelekhez. Az általános biztos álláspontját a lista bevezetését szorgalmazó szervezeteknek, köztük a Bankszövetségnek és a pénzügyi felügyeletnek eljuttatott ajánlásában fejtette ki. Lenkovics Barnabás ombudsman szerint a pozitív adólista összeállításának nincsenek alkotmányos vagy személyiségi jogi akadályai.

Az adatvédelmi biztos kiadott állásfoglalásában<sup>317</sup> kifejtette, hogy a Bankközi Adós- és Hitelinformációs Rendszer (BAR), illetve a helyébe lépő Központi Hitelnyilvántartó Rendszer (KHR) nem tekinthető önkéntes hozzájáruláson alapuló adatkezelésnek, ugyanis az állampolgároknak nincs valós választási lehetőségük abban a tekintetben, hogy kapcsolatba lépnek-e a BAR, majd a helyébe lépő KHR rendszerrel, mivel a Hpt hatálya alatt álló pénzügyi vállalkozással megkötött szerződési kötelezettségének megsértése adja a jogalapot az adatkezelésre. A hitelinformációs rendszerben szereplő természetes személyek esetén az adatok (azonosító adatok, hitelre vonatkozó adatok) személyes adatok, kötelezően előírt kezelésük tehát a személyes adatokkal való rendelkezés – mely a személyes adatok védelméhez való jog része – korlátozását jelenti.

Az adatvédelmi biztos álláspontja szerint bármely alapvető jog, így a személyes adatok védelmére vonatkozó alapjog korlátozása csak akkor felel

---

<sup>317</sup> Állásfoglalás a pozitív adólistával kapcsolatban; dr. Péterfalvi Attila; Budapest, 2006. január 30.

meg az alkotmányosság követelményének, ha az más alapvető jog, vagy kötelezettség érvényesítése érdekében történik, illetve e jog vagy kötelezettség oly mértékű közérdeket jelenít meg, amely indokolttá teszi a jog korlátozását, továbbá az előbbi két feltétel alapján meghatározott cél más módon nem érhető el, valamint a korlátozás a cél elérésére alkalmas. Az adatvédelmi biztos álláspontja szerint a 2006 decemberében működő „negatív” adólista e feltételeknek alapvetően megfelel: a hitelintézetek, illetve ügyfelek tulajdonhoz való joga (gazdasági érdeke) indokolttá teszi, hogy azon személyek, akiknek felhalmozott, és szerződésszegően nem rendezett adósságállományuk van, szerepeljenek egy központi nyilvántartásban, megakadályozva a további adósság-felhalmozást. A rendszer azonban részben a hibás törvényi szabályok, részben a jogellenes gyakorlat miatt évekig úgy működött, hogy súlyosan sértette az érintettek személyes adataik védelméhez való jogát. E hiányosságokat – előzetes értesítés, jogorvoslati rendszer hiánya, díjfizetéshez kötött tájékoztatás, stb. – csak a 2006-ban hatályba lépett törvénymódosítás orvosolja.

A piaci szereplők által a pozitív adólista melletti legfőbb érv az volt, hogy a bankok így hatékonyabban tudják értékelni a hitelezés kockázatát, amely az ügyfelek irányában úgy jelentkezne, hogy a kockázat csökkenésével a hitelek kamata is csökkenhet. Az adatvédelmi biztos álláspontja szerint a vázolt cél valójában egy több milliós adatbázist jelentene, melynek meghatározó része – itt a szerződészerűen teljesítő adósokra köréről van szó – cél nélküli, készletező adatgyűjtés lenne. Vagyis az elérni kívánt cél az adatvédelmi biztos álláspontja szerint nem indokolja az alapvető jog korlátozását. Az adatvédelmi biztos felhívta arra a figyelmet, hogy a pozitív adólista kedvező hatásait külföldi példákkal a piaci szereplők igazolják. Ez azonban nem történt meg, így nem támasztható alá, hogy a pozitív adólista bevezetése csökkentené a behajthatatlan követelések számát, vagy csökkentené a hitelek kamatait a

pozitív adólista bevezetése<sup>318</sup>. Vagyis egyelőre semmilyen bizonyítékot az adatvédelmi biztos nem talált, hogy a pozitív lista az állampolgárok számára járhatna oly előnyökkel, hogy indokolt legyen a személyes adatok védelméhez való jog korlátozása.

A bankok számára valóban kétségtelen előnyökkel járna a pozitív lista, de a bankok már most számos adatot ismernek az érintettekről, hiszen a hitelezés során a polgárokat meglehetősen alaposan kikérdezik jövedelmi, vagyoni, munkahelyi, sok esetben családi háttéréről. Az adatvédelmi biztoshoz érkező panaszok számos banki túlkapásra, jogellenes adatkezelésre világítottak rá, így az adatvédelmi biztos a legkevesbé sem tartaná örvendetesnek, hogy a bankok még a jelenleginél is „*árnyaltabb képet*” kapjanak a hitelt felvevő magánszemélyekről. Az adatvédelmi biztos állásfoglalásában hangsúlyozza, hogy az előnyök megfelelő mértékét és bizonyítottságát, azok pusztán lehetősége ugyanis nem indokolja az alapvető jog korlátozását. A bankok, hitelintézetek érdekeinek védelme, a számukra jelentkező előnyök olyan kategóriák, melyeket országgyűlési biztосként nem értékelhet, adatvédelmi biztосként a kérdést csak az állampolgárok alapvető jogainak szemszögéből vizsgálhatja. Az alapjogi megközelítés pedig nem vezethet a bankokat védő „veszélyközösségi” szemlélethez.

---

<sup>318</sup> Egyébként a PSZÁF tanulmány sem tudott összefüggést felmutatni a pozitív adólista létezése és a hitelezés költségeinek csökkenése között

## 11.8. Az adatvédelem az interneten

Az internet számos olyan jellemzővel bír, amelyet az adatvédelmi kérdések vizsgálatakor figyelembe kell venni, olyan számítógépes világhálózat, amely személyes és közérdekű adatok millióit gyűjti, tárolja, továbbítja, és azokat nyilvánosságra hozza. Olyan rendszer, amely nyilvános, elvileg bárki számára hozzáférhető, nincs tekintettel az országhatárokra, adatvédelmi, adatbiztonsági szempontból igen sérülékeny, megkönnyíti a közvéleményt érdeklő az állami és önkormányzati szervek működésével összefüggő közérdekű információk megismerhetőségét. Olyan információk, adatok érhetők el általa, amelyek egy része nem valós, vagy nem pontos, továbbá a jogsértő cselekmények elkövetésére is teret enged<sup>319</sup>. Az internet nem jog mentes terület, mivel számos jogszabály irányadó erre a területre, de ezen jogszabályok többször nem adnak megfelelő eligazítást a felmerülő jogvitákra. Az internettel kapcsolatos adatvédelmi követelmények teljesítése érdekében az adatvédelmi biztos 2001-ben ajánlást<sup>320</sup> adott ki.

Az internet elterjedése olyan új adatvédelmi problémákat vetett fel, amelyek gyakran a felhasználók részére nem is tudatosulnak. Az internet használatának lényeges jellemzője, hogy az interneten részvevő szolgáltatók, és felhasználók közötti kapcsolatokban számos személyes adatnak a közlésére kerül sor, mivel a felhasználó minden mozdulatával nyomot hagy maga után. Így a személyes adatként gazdát cserél a felek e-mail címe, esetlegesen a felhasználó internetes azonosítója, az IP címe. Az internet-szolgáltatók levelezőszervereiken tárolják az elektronikus levelezések tartalmát, mielőtt ahhoz a felhasználó hozzáférne, mások azt ellenőrizhetik, elolvashatják. A tárhely szervereken jegyzik, hogy milyen IP címről érkező felhasználó az egyes honlapok nézegetésével mennyi időt töltött, milyen rendszerben lapozgatott, tehát végső soron a

---

<sup>319</sup> *Adatvédelmi Biztos Beszámoló*, 2001. Mellékletek 1. pont

<sup>320</sup> Az internettel összefüggő adatkezelések egyes kérdéseiről szóló adatvédelmi biztosi ajánlás 2001. év <http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001>

felhasználónak az összes internetes aktivitása technikailag feltérképezhető. Az egyedi személyes és a sokszínű felhasználói profilk kialakítása elé igazából csak a költségek állítanak akadályokat. Ezért a személyes adatok védelme érdekében jogi szabályozókkal a technikai eszközök működtetését szabályozni kell. Szükséges azt is meghatározni, hogy milyen feltételek mellett, milyen adatokhoz juthatnak hozzá egyes közigazgatási, vagy büntető eljárásban résztvevő hatóságok. Az internettel kapcsolatosan több esetben fordultak az adatvédelmi biztoshoz, így amikor magyar gyermekeket ajánlottak fel örökbefogadásra fényképpel, személyes adatokkal,<sup>321</sup> több beadvány érintette a rendőrség internet-szolgáltatóktól történő adatkérésének jogszerűségét,<sup>322</sup> az interneten folytatott direkt marketing tevékenységgel kapcsolatban is érkeztek megkeresések<sup>323</sup>; egy magánszemély kifogásolta, hogy a domain-név regisztráció során a szolgáltató nyilvánosságra hozta adatait.<sup>324</sup> Az elmúlt években a halapenz.hu honlapon folytatott szabad véleménynyilvánítással kapcsolatos probléma irányította rá a figyelmet az interneten történő közlések adatvédelmi korlátaira.

#### 11.8.1. Véleménynyilvánítás az interneten

Az interneten bárki közzéteheti a véleményét, ennek során azonban ügyelni kell az egyén személyiségi jogainak, így becsületének, magántitkainak és személyes adatainak a védelmére. E jogok megsértése esetén az érintett bírósághoz fordulhat<sup>325</sup>. A halapenz.hu esettel kapcsolatosan Péterfalvi Attila adatvédelmi biztos kifejtette a véleményét, mely szerint a honlapon nem egyszerű véleményfórumról volt szó, hanem az üzemeltető létrehozott egy olyan adatbázist, amelyben az orvosok neve, mobiltelefon-száma és a vélelmezett halapenz mértéke egyaránt szerepelt. Az adatvédelmi törvény szerint ezeknek az adatoknak az érintett hozzájárulása nélküli nyilvánosságra

---

<sup>321</sup> Adatvédelmi biztos beszámolója, 1996 256/A/1996

<sup>322</sup> Adatvédelmi biztos beszámolója, 1998 394/K/1996, 802/A/1998

<sup>323</sup> Adatvédelmi biztos beszámolója, 1999 577/A/1998, 627/K/1998

<sup>324</sup> Adatvédelmi biztosi beszámoló, 2000 295/A/2000)

<sup>325</sup> Adatvédelmi biztosi beszámoló, 2004 1370/A/2004

hozatala jogellenes. Mint ahogy az is, ha valaki hozzászólásával ezt az adatbázist tovább bővíti. Péterfalvi Attila adatvédelmi biztos véleménye: „nagyon félrevezetőnek tartom, hogy egyesek azt képzelik, a világhálóra feltett fórumokra különleges szabályok vonatkoznak. Világos, hogy aki egy fórumban valakit bűncselekménnyel vádol, személyes adatokat hoz róla nyilvánosságra, ellenőrizetlen dolgokat állít, jogellenes tevékenységet folytat, mert megsérti az érintett, jelen esetben az orvos személyiségi jogát. Ebben az esetben persze nem a fórum üzemeltetőjének kell a felelősséget viselni, hanem a fórumba beíróknak”. Egyébként a nyilvános fórumon regisztráló felhasználó jogosult arra, hogy hozzászólását töröltesse. Az adatvédelmi biztos állásfoglalása szerint nemcsak a regisztrációkor átadott személyes adatokat, hanem az érintett személy hozzászólását<sup>326</sup> is törölnie kell a moderátornak, ha az érintett élni kíván adatvédelmi jogaival az adatkezelő nem tagadhatja meg ennek teljesítését.

#### 11.8.2. Internet-szolgáltatók adatvédelmi kötelezettségei

Az internetes szolgáltatók kötelezettsége hogy a felhasználók részére adatvédelmi tevékenységükről a tájékoztatást adjanak. A széles körben és folyamatosan hozzáférhető tájékoztatásban információkat kell adni a az adatkezelés egyes körülményeiről, így az adatkezelés céljáról, önkéntes vagy kötelező jellegéről, az adatkezelő illetve adatfeldolgozó személyéről. Az adat felvétele előtt kötelezően, illetve egyes további körülményekről az adatalany kérelmére tájékoztatást kell adni. Azoknak a szolgáltatóknak, amelyek a természetes személy felhasználóval szerződéses kapcsolatba lépnek, törvényi kötelezettsége, hogy az adatkezelésre vonatkozó kötelező tájékoztatást az adatkezelés megkezdése előtt célszerűen a felhasználóval kötött szerződés megkötésekor megadják, s eleget tegyenek a felhasználók további adatokra vonatkozó kérelmének. Azoknak a szerver-üzemeltetőknek, illetve szerveren

---

<sup>326</sup> *Adatvédelmi biztosi beszámoló, 2001 351/A/2001*

szolgáltatást nyújtóknak, amelyek birtokába a szolgáltatás nyújtása során személyes adat kerül, a felhasználónak a tájékoztatást az Avtv. szerint az adat felvétele előtt kell megadniuk. Az Európa Tanács R 99. (5) számú, a magánszféra interneten történő védelméről szóló ajánlása szerint a nyitó weboldalon egyértelmű adatvédelmi nyilatkozatnak kell szerepelnie, amelyhez linkelve a kezelt adatok körére, az adatkezelés céljára, módjára, időtartamára vonatkozó tájékoztatást kell elhelyezni. A felelős szolgáltatóknak tájékoztatniuk kell a felhasználókat az internet használatával együttjáró, a magánszférát fenyegető veszélyekről, illetve fel kell hívni figyelmüket a bizalmas kommunikáció lehetőségét biztosító technológiákra. Az internet szolgáltatóknak az érintett vonatkozásában egyfajta kitanítási kötelezettsége van, amelynek ki kell arra térnie, hogy felhívja az érintett figyelmét, hogy a személyes adatainak megadásával ő maga is takarékosan bánjon.

A személyes adatok védelmével és az elektronikus kereskedelmi szolgáltatásokkal kapcsolatos adatvédelmi kérdéseket a 2001. évi CVIII. törvény<sup>327</sup> szabályozza (továbbiakban: Ektv). Az információs társadalommal összefüggő szolgáltatás nyújtásáról szóló törvény megengedi, hogy az Ektv. hatálya alá tartozó szerződések esetében a megállapodás létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése céljából kezelheti az igénybe vevő azonosításához szükséges és elégséges azonosító adatokat. A szolgáltató az információs társadalommal összefüggő szolgáltatás nyújtására irányuló szerződésből származó díjak számlázása céljából kezelheti az információs társadalommal összefüggő szolgáltatás igénybevételével kapcsolatos olyan személyes adatokat, amelyek a díj meghatározása és a számlázás céljából elengedhetetlenek, így különösen a szolgáltatás igénybevételének időpontjára, időtartamára és helyére vonatkozó adatokat. A szolgáltató az igénybevett

---

<sup>327</sup> 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről



szolgáltatás nyújtásához kezelheti azon személyes adatokat, amelyek technikailag elengedhetetlenül szükségesek. Az adattakarékosság elve az elektronikus szolgáltatók esetében azt a kötelezettséget tartalmazza, hogy úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig.

A szolgáltató a szolgáltatás igénybevételével kapcsolatos adatokat bármely, az előzőekben ismertetett céltól eltérően – így különösen szolgáltatása hatékonyságának növelése, az igénybe vevőnek címzett elektronikus hirdetés vagy egyéb címzett tartalom eljuttatása, piackutatás céljából – csak az adatkezelési cél előzetes meghatározása mellett és az igénybe vevő hozzájárulása alapján kezelhet. A szolgáltatást igénybe vevő felhasználó részére az információs társadalommal összefüggő szolgáltatás igénybevételét megelőzően és a szolgáltatás igénybevétele során is folyamatosan biztosítani kell, hogy a piackutatási vagy a szolgáltatáshoz nem kapcsolódó célból történő adatkezelést megtilthassa.

Az elektronikus kereskedelmi szolgáltatás nyújtása céljából kezelt személyes adatokat törölni kell a szerződés létrejöttének elmaradását, a szerződés megszűnését, valamint a számlázást követően. A piackutatási vagy egyéb kereskedelmi célból kezelt adatokat törölni kell, ha az adatkezelési cél megszűnt, vagy az igénybe vevő így rendelkezik. A számvitelről szóló törvény vagy más törvény eltérő rendelkezése hiányában az adattörlést haladéktalanul el kell végezni. Az adatvédelmi törvényben meghatározott tájékoztatáson kívül a szolgáltatónak biztosítani kell, hogy az igénybe vevő az információs társadalommal összefüggő szolgáltatás igénybevétele előtt és az igénybevétel során bármikor megismerhesse, hogy a szolgáltató mely adatkezelési célokból

mely adatfajtákat kezel, ideértve az igénybe vevővel közvetlenül kapcsolatba nem hozható adatok kezelését is.

### 11.8.3. Hozzáférés az internetszolgáltatók által tárolt személyes adatokhoz

A büntetőeljárás törvényben rögzített kényszerintézkedés alapján kötelezést lehet kiadni a számítástechnikai rendszer útján rögzített adatok megőrzésére. A megőrzésre kötelezés a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének a számítástechnikai rendszer útján rögzített meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása. A bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli annak a számítástechnikai rendszer útján rögzített adatnak a megőrzését, amely bizonyítási eszköz, vagy bizonyítási eszköz felderítéséhez, a gyanúsított kilétének, tartózkodási helyének a megállapításához szükséges. A megőrzésre kötelezett a határozat vele történő közlésének időpontjától köteles a határozatban megjelölt számítástechnikai rendszer útján rögzített adatot változatlanul megőrizni, és szükség esetén más adatállománytól elkülönítve biztosítani annak biztonságos tárolását. A megőrzésre kötelezett köteles a számítástechnikai rendszer útján rögzített adat megváltoztatását, törlését, megsemmisülését, valamint annak továbbítását, másolat jogosulatlan készítését, illetőleg az adathoz való jogosulatlan hozzáférést megakadályozni. Ahhoz az adathoz, amelyet a megőrzésre kötelezés érint, az intézkedés tartama alatt kizárólag az elrendelő bíróság, ügyész, illetőleg nyomozó hatóság, valamint az elrendelő engedélyével az adat birtokosa vagy kezelője jogosult hozzáférni. Arról az adatról, amelyet a megőrzésre kötelezés érint, az adat birtokosa vagy kezelője az intézkedés tartama alatt csak az elrendelő kifejezett engedélyével adhat más részére tájékoztatást. A megőrzésre kötelezett köteles haladéktalanul tájékoztatni az elrendelőt, ha a megőrzésre kötelezéssel érintett adatot jogosulatlanul megváltoztatták, törölték, átmásolták, továbbították,

megismerték, vagy hogy ezek megkísérlésére utaló jelet észlelt. A megőrzésre kötelezést követően az elrendelő haladéktalanul megkezdi az érintett adatok átvizsgálását, és ennek eredményéhez képest az adatnak a számítástechnikai rendszerbe vagy más adathordozóra történő átmásolásával az adat lefoglalását kell elrendelni, vagy a megőrzésre kötelezést meg kell szüntetni. A megőrzésre kötelezés az adat lefoglalásáig, de legfeljebb három hónapig tart. A megőrzésre kötelezés megszűnik, ha a büntetőeljárást befejezték. A büntetőeljárás befejezéséről a megőrzésre kötelezettet értesíteni kell. Az adatvédelmi biztos állásfoglalása szerint az e-mailek tartalmát a nyomozó hatóság bírói engedély alapján, csak súlyos bűncselekmények esetén ismerheti meg és használhatja fel.

#### 11.8.4. Az e-mail cím adatvédelmi követelményei

A panaszos azt tudakolta az adatvédelemi biztostól, hogy a honlapján közzétett e-mail címe személyes adatnak minősül-e, és annak direkt marketing célú nyilvántartásba vételét megtilthatja-e. Az adatvédelmi biztos állásfoglalása szerint az e-mail cím akkor személyes adat, ha a kapcsolat a cím és birtokosa között helyreállítható. Így például személyes adat az e-mail cím, ha megegyezik a birtokosa nevével. Személyes adat az e-mail cím akkor is, ha az egy web-oldal üzemeltetőjének a címe, mert az ő adatait az interneten keresztül elérhető nyilvános adatbázisból a domain név alapján bárki megismerheti. A kéretlen üzleti levélküldés esetén az adatkezelési céltól eltérő adatkezelésre kerül sor, akkor az e-mail adatainak a törlése kérhető. Az elektronikus kereskedelmi szolgáltatásokra vonatkozó törvényi előírások megkövetelik, hogy az elektronikus levelezés vagy azzal egyenértékű egyéni kommunikációs eszköz útján kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető elektronikus hirdetés. Hozzájáruló nyilatkozat bármely olyan módon tehető, amely lehetővé teszi a hozzájáruló nyilatkozatot tevő személy azonosítását, valamint a hozzájárulás önkéntes és a megfelelő tájékoztatás birtokában történő kifejezését.

A munkahelyi levelezéssel kapcsolatban az adatvédelmi biztos kifejtette, hogy különbséget kell tenni azon e-mail-ek esetében, amelyeket a munkáltató a munkavégzéshez átadott a cég ügyeinek az intézése érdekében, és ha ezen e-maileket címek nem egy-egy munkavállalóhoz kötöttek. Ezen levelezésbe a munkáltató betekinthez, mivel az e-mailek is úgy kell tekinteni, mint a hagyományos levélforgalmat. A munkáltató jogosult egyébként a munkahelyen a magáncélú levelezésnek az előzetes megtiltására. A személyes e-mail postafiókon keresztül folytatott kommunikációt a hagyományos levelezéshez és telefonáláshoz hasonlóan kell megítélni, mivel jogszabályi felhatalmazás hiányában a munkáltató nem hallgathatja le a munkavállalók beszélgetését, és nem bonthatja fel a munkavállalói magánlevelezését sem. A munkavállaló által látogatott weboldalak felderítésére ugyanazokat a követelményeket kell alkalmazni, mint az e-mailekre.

Az elektronikus kereskedelem területén a Nemzeti Hírközlési Hatóság ellátja a kéretlen elektronikus hirdetésekkel (spam) kapcsolatos hatósági feladatokat, amelyeket az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény határoz meg<sup>328</sup>. A felügyelet lefolytatja azon jogsértőkkel szembeni hatósági eljárást, akik magyar IP címről, illetve magyar domain név felhasználásával küldött kéretlen elektronikus üzenet feladójaként lehet azonosítani. A fogyasztók tájékoztatását szolgáló anyagok készítésével és közzétételével a hatóság a spam elleni fellépés komplex kezelését célozza. A hatóság valójában az interneten megjelenő fogyasztó magánszféráját védi azzal, hogy az érintett engedélye nélkül, a részére küldött elektronikus üzenetek feladóit bírságolja meg hatósági eljárása keretében<sup>329</sup>. A legfontosabb jogszabályi változás, hogy a fogyasztók védelmének érdekében

---

<sup>328</sup> [www.nhh.hu](http://www.nhh.hu)

<sup>329</sup> *Az elektronikus hirdetésekre vonatkozó szabályokat tartalmazó az elektronikus kereskedelmi szolgáltatások, valamint információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.) 2008. szeptember 1-jétől jelentősen módosul.*

ezután más megítélés alá esik, ha a címzett természetes személy illetve, ha jogi személy részére küldték a kéretlen levelet. 2008. szeptember elsejétől a kifejezett és előzetes hozzájárulással küldhető reklámokra vonatkozó korlátozások ebben az esetben alkalmazhatóak, ha a címzett természetes személy.

#### 11.8.5. Személyes adatok nyilvánosságra hozása az interneten

Az adatvédelmi biztoshoz több kéressel fordultak a nyilvános és széleskörű hozzáférést biztosító szolgáltatások tekintetében, amelyek lényege személyes adatok nyilvánosságra hozatala. Így a gazdasági társaságok cégadatainak nyilvánosságra hozatalával, adósok listáját illetve hitelezői követelések közzétételével kapcsolatos ügyekben kérték az adatvédelmi biztos állásfoglalását. Az adatvédelmi biztos álláspontja szerint a gazdasági társaságok cégnyilvántartásában szereplő adatok nem személyes adatok, arra nem terjed ki a kompetenciája, de az adósok, illetve hitelezői követelések nyilvánosságra hozatalával kapcsolatosan leszögezte, hogy törvényi előírás hiányában kizárólag az érintett előzetes bejegyzése alapján lehet a személyes adatokat nyilvánosságra hozni.

Az internet elterjedésével párhuzamosan az elmúlt években többször előfordult, hogy a tartalom szolgáltatók, legyenek akár állami vagy önkormányzati intézmények indokolatlanul nyilvánosságra hoztak személyes adatokat. A közérdeklődésre szánt adatokat úgy kell a nyilvánosság számára hozzáférhetővé tenni, hogy a személyes adatok védelméhez való jog ne sérüljön. A köztisztviselők neve és beosztása közérdekű adat, de arcképüket már nem lehet nyilvánosságra hozni<sup>330</sup>, és szakmai pályafutásuk közreadására csak akkor kerülhet sor, ha a nyilvánosságra hozatalhoz az érintettek önkéntesen, tudatosan hozzájárultak. Az elektronikus információszabadságról szóló 2005. évi XC. törvényben meghatározott követelmények, illetve

---

<sup>330</sup> *Adatvédelmi biztosi beszámoló*, 2003. 162/K/2003, 181/A/2003, 440/A/2003

meghatározott adatkörök eligazítás adnak a közérdekű adatok közzététele tekintetében. A Eitv. a bírósági határozatok nyilvánosságra hozatala tekintetében is részletes eligazítást ad, így elkerülhetők azok a korábban elfordult esetek<sup>331</sup>, amikor bírósági honlapon személyes adatok indokolatlanul kerültek nyilvánosságra.

#### 11.8.6. Regisztráció az elektronikus szolgáltatások esetében

Az internetes szolgáltatások igénybevétele sok esetben regisztrációhoz kötött, amely magában rejti azt az adatvédelmi veszélyt, hogy hibás honlap működés következtében a személyes adatok tömege válik megismerhetővé. Ez fordult elő a BME egyik könyvtára esetében, amikor a regisztráló felhasználó számára az összes korábbi olvasó neve, címe, és egyéb azonosító adatai hozzáférhetővé váltak<sup>332</sup>. A honlap üzemeltetők által legtöbbször figyelmen kívül hagyják az Avtv.. adattakarékossági előírásait, így túlzottan sok személyes adatot követelnek meg a regisztráció során. Egyébként a nyilvános fórumon regisztráló felhasználó jogosult arra, hogy hozzászólását töröltesse. Az adatvédelmi biztos állásfoglalása szerint nemcsak a regisztrációkor átadott személyes adatokat, hanem az érintett személy hozzászólását<sup>333</sup> is törölnie kell a moderátornak, ha az érintett élni kíván adatvédelmi jogaival, az adatkezelő nem tagadhatja meg ennek teljesítését. Ha az érintett elfogadja a honlaphoz kapcsolt egyértelmű regisztrációs feltételeket, amelyben hozzájárulását adja adatai kezeléséhez, és az e-mail címének a honlapon történő nyilvánosságra hozatalához, akkor később már nem hivatkozhat adatvédelmi követelmények megsértésére. Az adatvédelmi biztos állásfoglalása szerint nem felel meg a tisztességesség követelményének, ha a regisztráció esetén az érintettet a szerződésben lemondadják az adatvédelmi igényeinek érvényesíthetőségéről.

---

<sup>331</sup> *Adatvédelmi biztos beszámoló*, 2003. 79/A/2002; 642/A/2002

<sup>332</sup> *Adatvédelmi biztos beszámoló*, 2003. 789/A/2003

<sup>333</sup> *Adatvédelmi biztos beszámoló*, 2003. 351/A/2001

A személyes adatok védelmének az egyik alapvető követelménye, hogy az érintett számára biztosítani kell, hogy az adatainak kezelését, azok továbbítását ellenőrizze, illetve megismerhesse, hogy mely személyek fértek hozzá a személyes adataihoz. Ennek érdekében az adatkezelőnek naplóznia kell, hogy a személyes adatok kezelésével kapcsolatosan milyen események történtek, milyen munkavállalója, mikor és milyen jogosultsági körrel lépett be abba a rendszerbe, amelyben a személyes adatokat kezelik. Másrészt szükséges az adatbiztonsági követelmények teljesítése érdekében annak a naplózása, hogy maga a felhasználó az webes kiszolgáló felületen keresztül mikor lépett be, mikor módosította a személyes adatait. A felhasználó adatok jegyzőkönyvezése lényeges kérdés abban az esetben, amikor az interneten elkövetett jogsértő cselekmények bizonyításának a szükségessége merül fel.

Tisztázatlan kérdés, hogy az adatkezelőnek éppen az érintett jogainak biztosítása, illetve az adatbiztonság követelményeinek teljesítése érdekében milyen mértékben lehet a saját ügyfeleinek használati szokásaihoz kapcsolódó adatokat tárolni. A naplózási tevékenység technikai célja, hogy az esetleges visszaéléseket felfedezze, másrészt a működési zavarokról is visszajelzést adjon az adatkezelő részére. Az adatkezelés jogalapjaként talán az Avtv. 5.§ (3) bekezdésében meghatározott célt lehet idézni, mely szerint személyes adat az érintett hozzájárulása alapján akkor kezelhető, ha arra az adatkezelő vagy harmadik személy jogos érdekeinek érvényesítése érdekében szükséges. De elfogadható az a megállapítás, hogy kellő pontossággal ez a kérdéskör jelenleg nem szabályozott.

### 11.8.7. Elektronikus kereskedelmi szolgáltatások adatvédelmi veszélyei

Az elektronikus kereskedelmi szolgáltatásokkal kapcsolatosan a világháló által nyújtott lehetőségek kínálják azt a platformot, amely a távollevő felek közötti kommunikáció biztosításával alkalmas közeget nyújt szerződési nyilatkozatok adására, azok elfogadására, és magára a szolgáltatás nyújtására és annak elfogadására. Az internet technikai működése felvet olyan kérdéseket, amelyeket jogi szempontból értékelni kell, hogy annak használati feltételeit a személyes adatok védelmének követelményeivel össze lehessen egyeztetni.

A szakirodalom felhívja a figyelmet arra, hogy a személyes adatok és a magánszféra veszélyeztetését<sup>334</sup> az internetes környezetben úgynevezett web-cookies negatív hatásaiban találjuk meg. A cookie egy web-szerver által produkált adatsor, amelyet a web-szerver küld, és amely a saját egyéni számítógépünk merevlemezén tárolódik. A cookie-t valójában a felhasználó maga telepíti a saját számítógépére, amikor egy szerverrel a gépe kommunikál. A cookie-k normál esetben információkat továbbítanak a felhasználóról a honlap tárhelye felé. Így van lehetőségünk arra, hogy saját felhasználói névvel és egyedi jelszóval valamilyen távoli szerveren tárolt adatbázisba beléphessünk. De a cookie-k segítségével működnek a webáruházak, ahol a virtuális térben a képzeletbeli bevásárló kosarainkba árukat helyezünk el. A cookie-k nemcsak arra alkalmasak, hogy a kiinduló számítógépet azonosíthassák, hanem arra is, hogy a számítógépes felhasználási szokásokról információt szolgáltatassanak. A problémát valójában az jelenti, hogy helyi cookie adatokat továbbít vissza a web-szerver számára anélkül, hogy azt a felhasználó észrevenné. Egyes cookie-knak igen sok negatív tulajdonsága van, így vírusprogramok továbbítására, átadására képesek, kikémlelik az e-mail címeket, személyes adatokat, vagy egy merevlemez teljes tartalmát mások számára megismerhetővé teszik. Sok esetben az online-szolgáltatók azért alakítanak ki cookie-kat, hogy vevő specifikus felhasználói profilokat

---

<sup>334</sup> Thomas HOEREN, *Grundzüge des Internetrechts*, München, Verlag C.H. Beck, 2002. 262



alakítható ki, amely abban az esetben személyes adatnak minősül, ha a felhasználó egy online szolgáltatás igénybevétele kapcsán saját nevére reklám ajánlatot kap, vagy ha saját e-mail címére érkezik a reklám. Egy direkt személyre vonatkoztatott felhasználói profil azonban csak akkor állítható elő, ha a vevőoldali szerver IP címe a felhasználó személyére enged következtetni. Ez abban az esetben fordulhat elő, ha a felhasználó IP címe egy domain névvel áll összeköttetésben. Az adatvédelmi követelményekkel egybehangzó joggyakorlat szerint a cookie-t csak azért lehessen telepíteni, hogy az az online szolgáltatást lehetővé tegye, illetve egyszerűsítse. Mivel a cookie-k egy személyre vonatkozóan „használati adatokat” tartalmaznak, a cookie adatokat lehető leghamarabb, de a mindenkori használat végeztével törölni kell. Ha a cookie nem tartalmaz egy konkrét személyre történő kapcsolódási, azonosítási támpontot, akkor a cookie-kra az adatvédelmi jog nem irányadó, de felmerül a felhasználónak a zavarására vonatkozó polgári jogi szabályok alkalmazása. Az Avtv. és Ektv. szabályai alapján egy elektronikus szolgáltatáshoz kapcsolódó felhasználói profilok kialakítására csak akkor kerülhet sor, ha ahhoz a felhasználók előzetes, és tudatos hozzájárulásukat adták. Az adatkezelés tisztességének elve megköveteli, hogy a nyújtott elektronikus szolgáltatás igénybevétele nem függhet a felhasználói profil kialakításába történő beleegyezéstől.

Az elektronikus kereskedelmi szolgáltatások speciális területe a web bug szolgáltatások, amikor a weboldalak látogatottságának a felmérése érdekében statisztikai adatokat készítenek, de ebben a munkafolyamatban nemcsak e célú adatkezelés valósult meg, hanem a szoftver egyúttal a felhasználóról is közöl adatokat. A webbug elsősorban egy-egy oldal látogatottságára vagy bannerre nézve kezel adatokat, de emellett a számítógépbe korábban bevitt és a honlapon közölt adatokat is továbbíthatja a piackutatással foglalkozó cég felé, de ez a gyakorlat nem felelt meg az adatvédelmi követelményeknek.

### 11.8.8. Outsourcing

Az e-kereskedelemben egyre gyakrabban hangoztatott előnyök szerint, az adatfeldolgozás leányvállalatok számára történő átadása megtakarításokat eredményez, mert a leányvállalat az adatfeldolgozási tevékenysége tekintetében más vállalkozások számára is végez piaci szolgáltatásokat. Az adatkezelő és az adatfeldolgozó között létrejövő vállalkozási tevékenységet outsourcing tevékenységnek nevezi a joggyakorlat. Az outsourcing szerződés keretében az adatkezelő átadja az adatkezelési tevékenységének egy részét, amely az Avtv. módosítása<sup>335</sup> óta a magyar jogban is egyedileg szabályozott vállalkozási tevékenység. Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. A törvény előírásai alapján az adatkezelési munkafázis átadható, de az adatkezelésért fennálló jogi felelősség nem. Az adatkezelő és az adatfeldolgozó között az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni. Egyébként tisztázatlan lenne a felek közötti jogviszony, mivel felmerülhetne, hogy az adatok harmadik személy részére lettek törvényi előírások ellenére átadva. Az Avtv. előírásai szerint az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel. Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért. Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe. Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a

---

<sup>335</sup> 1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni. Az adatfeldolgozásra nem adható megbízás olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

Az Avtv. törvényi fogalom meghatározásában az adatfeldolgozás olyan az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzését jelenti, amelyen nem függenek a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Annak a meghatározásában, hogy tiszta adatfeldolgozásról vagy adatkezelési tevékenység átadásáról beszélünk fontos vizsgálni, hogy a harmadik személyek milyen cselekvési lehetőségekkel bírnak az adatfeldolgozás vonatkozásában. Ennek meghatározásában az játszik szerepet, hogy az adatfeldolgozási célból átadott adatok tényleges használatára sor kerül-e. Ezt pedig akkor lehet megállapítani, ha valamilyen feladat teljesítéséhez az átadott személyes adatokat, mint segédeszközt használják.

A német adatvédelmi hatóságok gyakorlata szerint az adatfeldolgozási szerződésekben szükséges lefektetni, hogy a megbízó felel az adatvédelmi követelmények betartásáért, és a megbízott csak a megbízó utasításai szerint dolgozhatja fel a személyes adatokat. Az adatkezelőnek vizsgálnia kell az adatfeldolgozó alkalmasságát az adatbiztonsági követelmények betartása tekintetében, és ennek biztosítékait a szerződésben a feleknek le kell fektetniük. Az adatfeldolgozónak nem lehet mérlegelési jogköre az általa végrehajtandó adatfeldolgozás kialakítása tekintetében. A szerződésben szükséges lefektetni, hogy milyen biztonsági intézkedések kerültek kialakításra az adatfeldolgozó megbízhatósága érdekében. Az adatfeldolgozónak kötelezettséget kell vállalnia, hogy a konkrét adatfeldolgozással megbízott munkatársak kiválasztása során gondosan jár el, tekintettel az érzékeny adatok bizalmasságnak a fenntartására, valamint hogy rendszeresen ellenőrzi azoknak a munkatársaknak a megbízhatóságát, akik a

tényleges adatfeldolgozást végzik. Az adatkezelőnek lehetőséget kell adni arra, hogy akár az adatfeldolgozó munkatársainak a megbízhatóságát tesztelje.

## 11.9. A személyes adatok védelme és a biztonsági szolgáltatások

### 11.9.1. Biztonsági szolgáltatások, kamerás megfigyelések

A személy-, vagyon- és közbiztonsági célból alkalmazott videókamerás megfigyelés mára hatalmas iparággá fejlődött. Számos demokratikus államban, például az Egyesült Államokban és az Egyesült Királyságban részben a költségvetés finanszírozza a megfigyelő, rögzítő és adategyeztető rendszerek további fejlesztését. A rendőrség által működtetett közterület-figyelő kamerák egész városrészeket behálóznak, a bevásárlóközpontok kamerái nemcsak a vagyonvédelem, hanem a vásárlókör kiválasztásában is szerepet játszanak, a munkahelyi kamerák nemcsak a munkavállalók teljesítményének hatékonyságát kívánják növelni, hanem a munkavégzés szabályainak való állandó megfelelést is. A mindennapok során azzal a vélelemmel kell élnünk, hogy a zárt láncú kamerás megfigyelés robbanásszerű elterjedésével a társadalmi érintkezés szinte minden helyszínén megfigyel egy sokszor láthatatlan szem<sup>336</sup>. A hálózati videó-rendszerek a mai biztonságtechnikai technológiai színvonalon kiválóan alkalmasak arra, hogy több egybekapcsolt kamerával térfigyelést végezzenek, és a gyűjtött adatokat kezeljék, tárolják, archiválják, és akár különböző digitális csatornákon továbbítsák bármely felhasználó számára.

---

<sup>336</sup> 35/2002. (VII. 19.) AB határozat

### 11.9.2. Adatvédelmi jogi előírások az elektronikus megfigyelőrendszerekre vonatkozóan

A személyes adatok védelmére vonatkozó szabályokat a többször módosított 1992. évi LXIII. törvény (továbbiakban: Avtv..) rögzíti, amely részletesen szabályozza az információs önrendelkezési jog gyakorlásának feltételeit, az adatkezelők kötelezettségeit. Az információs önrendelkezési jog legfontosabb garanciája a célhoz kötöttség, ami azt jelenti, hogy személyes adatot csak világos és egyértelmű törvényes felhatalmazás alapján lehet kezelni. Az adatkezelés minden szakaszában meg kell felelni a célhoz kötöttség elvének, azaz egyszer már megszerzett adatokat az adatkezelő saját belátása vagy tetszése alapján az adatgyűjtés eredeti céljától eltérő célokra nem használhatja fel. Ha törvény nem írja elő az érintett számára a személyes adatainak átadását, akkor az érintettre vonatkozó adatokat kizárólag az ő önkéntes és tájékozott beleegyezésével lehet gyűjteni. Az érintett tájékozott beleegyezése feltételezi, hogy őt az adatkezelés céljáról, annak tartamáról, illetve az őt megillető jogokról, továbbá az adatkezelő személyéről részletesen tájékoztatták.

A polgári törvénykönyv személyiségi jogok között határozza meg a képmás védelméhez való jogot, így a magánszemély lefényképezéséhez az ő saját engedélye szükséges. A képmás elkészítéséhez az engedélyt ráutaló magatartással is meg lehet adni, így nyilvános rendezvényen való szerepléssel, vagy a képi megfigyelésről szóló előzetes tájékoztatás mellett a megfigyelt helyiségbe történő belépéssel. Vagyonvédelmi célból alkalmazott elektronikus megfigyelő rendszerekre irányadó szabályokat a többször módosított a vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról szóló 1998. évi IV. törvény legújabb módosítása tartalmazza, amelyet a köztársasági elnök indítványa alapján az Alkotmánybíróság vizsgálat alá vont, és a még ki nem hirdetett törvény

alkotmányellenességét állapította meg a 36/2005. (X.5.) határozatában. A visszaküldött törvényt az Országgyűlés az Alkotmánybíróság döntése alapján módosította.

### 11.9.3. Hálózati videó rendszerek alkalmazásának adatvédelmi kockázatai

A vagyonvédelmi célzatú hálózati videó rendszer az internet lehetőségeit felhasználó technológiákkal és digitális kamerákkal egy egységes felületbe integrálható, és létrehozható egy könnyen kezelhető elektronikus térfigyelő rendszer. Az online monitor felület alkalmas az élő képek nézésére, a rendszerbe foglalt kamerák képei a videó rendszeren keresztül könnyen tárolhatók. A képarchívum kezelő felületéről képek vagy videó részletek kimásolhatók, többszörözhetők és akár e-mailban bárhova elküldhetők. A rögzített képadatok egymással összekapcsolhatók, illetve arc- és rendszám felismerő rendszerekkel kiegészíthetők. A hálózati video rendszer technológia minden különösebb technikai akadály nélkül alkalmas arra, hogy képi adatok formájában személyes adatokat rögzítsen, és tároljon. Ezért az analóg és a digitális kamerákat egy hálózati online kezelőfelületbe integrált technológia magában hordozza azokat a technológiai alkalmazásokat, amelyek a személyes adatok védelmére veszélyt jelentenek, ha a technológia mindennapi alkalmazását nem hangolják össze az adatvédelmi előírásokkal.

### 11.9.4. Térfigyelő rendszerek telepítésének indokai

A magánterületen vagy a közönség számára nyitva álló területek vagyonvédelmi célból igénybe vehető elektronikus megfigyelőrendszer működtetése sértheti a magánszféra szabadságát és az információs önrendelkezési jogot. Az alapjogok sérelme és korlátozása abban az esetben fogadható el, ha valamilyen más alapjog érvényesülése érdekében van a korlátozásra szükség, így ha személyek testi épségének védelme, a tulajdon védelme, továbbá a közbiztonság, a közrend fenntartása indokolja. A törvényi

előírások akkor engedik meg elektronikus megfigyelőrendszernek kép-, hang-, illetőleg kép- és hangrögzítést is lehetővé tevő formáinak telepítését a közönség számára nyitva álló helyiségek, terek, nyílt területek megfigyelésére, ha az adott területen fennálló üzemi kockázati tényezők vannak. Kockázati tényezőnek számít pénz, vagy más értékes eszközök védelme, illetve áruházban folyó elárúsítási tevékenység valószínűsíti, hogy vagyon elleni szabálysértések vagy bűncselekmények, mint pl.: lopás, rongálás, rablás, sikkasztás elkövetése következhet be. Kockázatok körébe tartozhat valamilyen „veszélyes üzemi” tevékenység is, úgymint egy labor működése, kazánház vagy számítógépek üzemeltetése, amelyek konkrét balesetveszélyt hordoznak magukban. A törvény a fenti vagyon- vagy személy elleni bűncselekmények elkövetőinek észlelése, az elkövető tettenérése, illetve e jogsértő cselekmények megelőzése esetében engedi meg az elektronikus térfigyelő rendszerek telepítését, ha a bűncselekmények bizonyítása más módszerrel nem érhető el.

A törvényi előírás a személyes adatok védelmében akkor engedi meg az elektronikus térfigyelő rendszerek telepítését, ha az elektronikus térfigyelő rendszerek és eszközök alkalmazása a fenti okokból kifolyólag elengedhetetlenül szükséges mértékű. Az elengedhetetlenül szükséges mérték azt jelenti, hogy a térfigyelő rendszerek telepítési tervét úgy kell kidolgozni, hogy a térfigyelés kizárólag ezen a veszélyes vagy biztonsági kockázatot magában rejtő tevékenységekre terjedjen ki. Az épület alaprajzainak alapul vételével meg kell határozni a tervezés során, hogy a veszélyes vagy biztonsági kockázatú tevékenység mely helyiségekben folyik. A kamerákat kizárólag ezen helyiségek megfigyelésére kell koncentrálni, figyelembe véve azt, hogy a megfigyelés céljának a megfigyelés ideje alatt fenn kell állnia. Így ha például a megfigyelés kizárólag arra a célra irányul, hogy a keletkező tüzeket vagy baleseteket mihamarabb észleljék, akkor a folyamatos 24 órás megfigyelés indokolt lehet, de nem szükséges olyan képességű kamerákat felszerelni, amely alapján bármely a helyiségbe belépő személy azonosítható

feltéve, ha az ajtón történő belépés során már az adott személy belépési jogosultságát megállapították. Ha a térfelügyelésre olyan helyiségekben, vagy tanterekben kerül sor, ahol a veszélyes labor-tevékenység mellett tanórákat is tartanak, ebben az esetben, ha a laborban veszélyes tevékenységet ideiglenesen nem folytatják, vagy az oktató személyesen felügyeli a tevékenységet nem lehet elektronikus megfigyelést végezni.

A térfelügyelő rendszer működtetése során személyes adatokat, a személyiségi jogot érintő korlátozást a lehető legkisebb mértékűre kell szorítani, ami nem járhat az információs önrendelkezési jog aránytalan korlátozásával. Ez a megfogalmazás azt jelenti, hogy az elektronikus térfelügyelő rendszereket elsősorban megfigyelésre lehet felhasználni, ami nem foglalja magában azt, hogy a felvett képeket automatikusan rögzíthetnék vagy tárolhatnák. Ha a képi adatok visszakereshető formában történő rögzítését, és az adatok tárolását nem indokolja valamilyen egyértelműen azonosítható kényszerítő körülmény, akkor a képfelvételek rögzítése sérti a személyes adatokat és a személyiségi jogokat. Kényszerítő körülménynek tekintendő bűncselekmény vagy szabálysértés elkövetése, illetve baleset bekövetkezése.

Az alapjog korlátozását a lehető legkisebb mértékűre kell szorítani a térfelügyelő rendszer működése során, ami az információs önrendelkezési jog aránytalan korlátozásával nem járhat. Azaz a személy- és vagyonbiztonsági céltól eltérően nem lehet személyes adatokat kezelni, és nem lehet a térfelügyelő rendszerből nyert adatokat összekapcsolni más, az adatkezelő birtokában levő egyéb munkaügyi vagy hallgatói adatbázisokkal. Nem lehet a térfelügyelő rendszert a munkavállalók olyan típusú ellenőrzésére felhasználni, ami arra irányulna, hogy a dolgozó elhagyja-e munkaidő alatt a munkahelyét, illetve éppen mikor érkezik, vagy távozik. Ha a térfelügyelő rendszerből gyűjtött adatokat egy egyértelműen azonosítható személyhez rendelik, akkor az adatkezelőnek tájékoztatnia kell az érintettet az adatbázisok



összekapcsolásáról, kivéve akkor, ha az adatkezelés büntető- vagy szabálysértési eljárás hatósági megindításához szükséges.

Adatkezelőnek minősülő vagyonőrzési feladatot ellátó személyt tájékoztatási kötelezettség terheli a térfigyelő kamerák működéséről. Így jól látható helyen, jól olvasható módon a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon köteles az adatkezelő figyelemfelhívó jelzést, és ismertetést elhelyezni. A tájékoztatásnak többek között ki kell terjednie

- a) arra a tényre, hogy az adott területen elektronikus megfigyelőrendszert alkalmaznak (térfigyelés);
- b) az elektronikus biztonságtechnikai rendszer által folytatott megfigyelés, valamint a rendszer által rögzített, személyes adatokat tartalmazó kép- és hangfelvétel készítésének, tárolásának céljáról,
- c) az adatkezelés jogalapjáról, a felvételkészítés tényéről, annak jogi alapjáról
- d) ha felvétel készül, akkor a felvétel tárolásának helyéről, a tárolás időtartamáról,
- e) a rendszert alkalmazó (üzemeltető) személyéről,
- f) az adatok megismerésére jogosult személyek köréről,
- g) továbbá a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvénynek (a továbbiakban: Avtv..) az érintettek jogaira és érvényesítésük rendjére vonatkozó rendelkezéseiről;
- h) a vagyonőrzési feladatokat ellátó személy intézkedései által okozott jogsérelem esetén igénybe vehető eljárásokról.

A vagyonőrzési feladatokkal megbízott vállalkozás számára szükséges lenne kötelező adatvédelmi szabályzatban előírni az elektronikus térfigyelő rendszer használatának adatvédelmi követelményeit. Nemzetközi kutatások tapasztalatai mutatják, hogy a térfigyelő kamerák üzemeltetése közben a vagyonőrök „unalom űzés érdekében” olyan magatartást tanúsítanak, amelyek

a megfigyelték személyiségi jogait sérti. Ezért ellenőrzött és dokumentált keretek között kell a térfigyelő rendszer működtetését felügyelni, és az esetlegesen felvett képfelvételeket ellenőrzöten megsemmisíteni. Ágazati adatvédelmi szabályzatban kellene rendezni a tájékoztatás rendjét, illetve az adatvédelmi kifogások érdemi elbírálása érdekében a vagyonvédelmi vállalkozások által önkéntesen alkalmazott a tisztességes adatkezelést biztosító eljárási rendet lefektetni.

#### A IV. rész összegzése: Adatvédelem és a technológiai fejlődés

A személyes adatok szektorális szabályozása körében olyan személyes adatkezeléseket tekintettem át, amelyek közvetve vagy közvetlenül kapcsolódtak valamilyen informatikai technológia alkalmazásához, személyes adatok digitális kezeléséhez. Az internet és a személyes adatok védelmével kapcsolatosan kifejtettem, hogy a technológiai fejlődéssel, annak sokszínűvé válásával az internet egyre növekedő jelentőségével, sőt mindennapi használatával az adatkezelési, adatfeldolgozási kapacitás korlátlaná vált. A tíz évvel ezelőtti munkahelyi kommunikáció is alapvetően más, mint a mai, ahol az irodai napi tevékenység szerves része az online módon folytatott kommunikáció. Alapvetően megváltoztak kereskedelmi szokásaink is, mivel egyre többet vásárlunk az interneten, naponta nyílnak új online webshopok, árverési weboldalak, és a vásárlási tájékozódásban már ma az internet a társadalom egyes rétegeinek nélkülözhetetlen. Míg tíz évvel előtt biztonsági őrsgnek közvetlen jelenléte nélkülözötte a képi megfigyelést, vagy képrögzítés széleskörű technológiáit, addigra ma ilyen informatikai eszközök nélkül nem is végezhet vagyonvédelmi tevékenységet egy vállalkozó.

Véleményem szerint az alapjogi védelemre épített információs önrendelkezési jog nem tud lépést tartani azzal a körülménnyel, hogy egyre több olyan jogviszony alakul ki napról-napra, amely az adatvédelem körébe

sorolódik. Az adatvédelmi törvény ugyan előírja egyes szolgáltatóknak (az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőknek és adatfeldolgozóknak; a pénzügyi szervezeteknek, a távközlési és közüzemi szolgáltatóknak), akik tömeges méretekben kezelnek személyes adatokat, hogy részletesen szabályozzák belső működésüket a személyes adatok kezelése tekintetében, de valójában állami felügyelet nélkül áll a személyes adatok védelme. De az alapvető jogok szabályozásával felruházott Országgyűlés önkéntelenül is belesodródik mulasztásos alkotmány sértésekbe, mivel az információs önrendelkezési jog egyre táguló gyakorlásának a kereteinek meghatározásával lemarad. Jelenleg leginkább a munkahelyi adatvédelem kérdése vet fel számos ponton alapjog sérelmi aggályokat, mivel a jogalkotó ebben a vonatkozásban a szektorális adatvédelmet nem szabályozta. Véleményem szerint nem vonható kétségbe, hogy a munkahelyi privacy kérdése valójában egy magánjogi jogviszonyban megjelenő információs önrendelkezési szabályozási kérdés, ami az adatvédelem közvetett drittwirkung hatásaként is megfogalmazható. Kérdés, hogy az adatvédelmi biztosunk a XXI. században a magánjog teljes területén képes lesz-e, az egyre tömegessé váló adatvédelmi jogviszonyokat kontroll alatt tartani?

## Az EREDMÉNY: Az adatvédelem módszerváltása

A dolgozatomban részletesen bemutattam a személyes adatok szabályozásának fejlődését az Európai Unió jogrendszerében, amely az elmúlt 30 évet áttekintve világon az egyik legmagasabb védelmi szintet garantálja a személyes adatok védelmének. A közösségi jogban keretjogszabályokat, illetve egyes területeken szektorális előírásokat alakítottak ki a személyes adatok egységes védelme, illetve az adatoknak belső határon történő szabad áramlása érdekében. A belső piac egységessége érdekében elfogadott személyes adatok kezelésére vonatkozó előírások a megalkotásukat követő 10 évben alkotmányos rangra emelkedtek, és a személyes adatok védelmének alapjoga helyet kapott az Európai Unió alapjogi chartájában. Az információs önrendelkezési jog európai alapjoggá vált, amely a nemzeti jogokban közösségi tényállási elem nélkül is közvetlenül felhívható. A személyes adatok védelmének működőképes garancia rendszere alakult ki azzal, hogy az európai intézmények tekintetében az Európai Adatvédelmi Biztos felügyeli a személyes adatok védelmére vonatkozó szabályok betartását. A XXI. századot kezdetektől fogva jellemi a technológiai fejlődés gyorsulása, globalizálódás fokozódása, valamint a terrorizmus nemzetközivé válása, ebben a környezetben a személyes adatok védelme különösen érzékenyé vált, mivel markáns érdekek jelentek meg az információs önrendelkezési jog eddig nem ismert mértékű korlátozása érdekében.

A magyar jogrendszer elmúlt húsz éves történetében a személyes adatok védelméhez fűződő jog szerves részévé vált alapjogi rendszerünknek, és napjainkban a közösségi joggal azonos védelmet biztosít személyes adataink tekintetében. A magyar Alkotmánybíróság több nagyhatású döntésével egyengette a személyhez fűződő adatok védelmét az univerzális személyi szám, a vagyon-nyilatkozattétel, a titkos megfigyelés, vagy éppen a sport események képi rögzítése tárgyában hozott döntéseivel. A magyar jogalkotó több szektorban, így az egészségügyben, a direkt marketing területén, vagy a

büntető eljárási szabályokban részletes előírásokat alkotott a személyes adatok védelme érdekében. Egyes területeken a szabályozás nem haladt túl a közösségi jog által megkívánt minimum szinten, mint az elektronikus hírközlés, vagy az elektronikus kereskedelem vonatkozásában. Más jogterületen így pl: a munkahelyi privacy esetében, ahol közösségi szabályozás sem létezik, nem sikerült részletes szabályokkal a személyes adatok védelmét garanciákhoz kötni. Álláspontom szerint ki kell mondani, hogy az adatvédelmi jogalkotás lemaradt a technológiai fejlődéshez képest, de a kérdés, hogy véglegesen-e.

Az alapjogvédelem fenntartása versus lemaradás a technológia fejlődéstől

Az Alkotmányban lefektetett mindenkit megillető személyes adatok védelmének alapjoga, a XXI. századi technológia világában élő jog akkor maradhat, ha az adatvédelem módszertana változik meg a magánjog területén működő adatkezelőkkel fennálló jogviszonyokban. Olyan magánjogi jogviszonyokban, ahol az érintett természetes személy az adatkezelőnek kiszolgáltatott, társadalmi, szociális viszonyrendszerben alárendelt, így a munkaviszonyokban, elektronikus hírközlési szolgáltatás igénybe vételekor, hitelezési szerződés teljesítése során, elektronikus média világában, át kell alakítani az adatvédelmi szabályozás módszertanát. Véleményem szerint az Országgyűlés által megalkotott keretjogszabályok alapján az adatvédelmi szabályok speciális ágazati megfogalmazásának kellene utat nyitni, az önszabályozás elvének érvényesülése mellett.

Ha fenntartjuk az adatvédelem kizárólag alapjogi dogmatikára épített szabályozását, azaz kizárólag az Országgyűlés törvényhozási tárgyként szabályozza a személyes adatok kezelését, ezzel együtt elvesztjük annak életszerű, a technológiai fejlődéshez igazodó alkalmazhatóságát a XXI. században. Véleményem szerint a személyes adatok alapjogának a horizontális jogviszonyokban érvényesülő drittwirkung hatásának

felismerésével eljuthatunk oda, hogy modernizáljuk az adatvédelem eszköztárát. El kell ismerni, hogy a magánjogi viszonyokban fel kell adni az információs önrendelkezési jog alapjogi érvényesítését, és helyette a tisztesség elvének a kibontását kell előtérbe helyezni azzal, hogy a védendő alkotmányos érték, azaz a személyiség szabad kibontakoztatása, az információs önrendelkezés, a tudatos beleegyezés, az adatkezelés célhoz kötöttsége fennmarad. Véleményem szerint a horizontális jogviszonyokban is alkalmazható az arányosság elvéből levezethető adattakarékosság elve, mely szerint kizárólag az adott cél elérése érdekében szükséges adatkezelésre kerülhet sor magánszemélyek közötti szerződéses jogviszonyokban.

A magyar jogalkotónak azon horizontális jogviszonyokban, amelyekben technológiai fejlődés miatt ez indokolt, felül kell vizsgálnia, hogy az adatvédelem témakörében kizárólagosan törvényhozási szinten tartja-e fenn jogalkotási kompetenciáit. Álláspontom szerint a jelenlegi rendszer fenntartásával a jogalkotó hagyja elveszti az adatvédelmi jog életszerűségét az internet, digitális képzőanyag, és tömegméretű online kommunikáció világában. Ezért a jogalkotónak az adatvédelem jogi eszközrendszerének részbeni szabályozását meg kell osztania a technológiát alkalmazókkal azzal, hogy lehetőséget ad az ágazati önszabályozásnak. Nem elegendő előírni, hogy az adatkezelők belső szabályzatokat alkossanak, hanem olyan szabályzókat kell kialakítani, amelyek megfelelő jogi környezetet biztosítanak az informatikai fejlődésnek. A törvényalkotóknak az ágazati önszabályozás elveit kellene meghatározni elsősorban az általános jogelvekre, tisztességességre, jóhiszemű joggyakorlásra, joggal való visszaélés tilalmára történő hivatkozással, másodsorban az adatvédelmi elvekre: az célhoz kötöttség, adattakarékosság, felhasználói tudatos és tájékozott beleegyezés érvényre juttatásával.

Az adatvédelem technológia szemléletű szabályozása során az alapjog szükségességi és arányossági korlátozásra épített információs önrendelkezési jogi felfogása anakronisztikussá vált, mivel nem veszi figyelembe a

technológia által nyújtott lehetőségeket. Álláspontom szerint az adatvédelem alapjogi felfogása nem egyeztethető össze sok esetben azzal a technológiával, amelynek a szabályozására törekszik. Az Európai Közösségek Bírósága is beleütközött ebbe a kérdésbe a Lindqvist ügyben, amikor az adattovábbítás fogalmát értelmezte az internet vonatkozásában. Az elektronikus technológiai eszközök, infrastruktúrák elterjedése, az elektronikus kereskedelem kialakulása, és az internet széles tömeg általi használata, újra az adatvédelem technológiai szempontokat előnybe részesítő adatvédelmi szabályozások elterjedését kell hogy hozza. Az adatvédelem technológia szemléletű szabályozása (Datenschutz durch Technik) már nem tesz különbséget állami vagy magán adatkezelő között, mivel az informatikai technológiák horizontális vagy vertikális jogviszonyoktól függetlenül kerülnek alkalmazásra. A technológiai fejlődés ezen irányát követve az adatvédelmi szabályozásnak is olyan megoldásokat kell követni, amely alkalmas a technológiai fejlődés gyors nyomon követésére. Az adatvédelem a technológiai lehetőségekhez igazodó szabályozása valódi gazdasági versenyfokozó tényező is lehetne, mivel lehetőséget adna olyan új technológiák bevezetésére, amelyek a gazdaság húzó ágazataivá válva hozzájárulnának az ország informatikai modernizálásához.

Az ágazati önszabályozásból a jogalkotó az alapjogok védelme érdekében nem vonulhat ki, hanem egyes területekre vonatkozóan megalkotott keretjogszabályokban rögzítheti azokat a tilalmazott magatartási formákat, amelyeket a tisztességesség elvével ellentétesnek tart. Alkalmazható lenne a fogyasztóvédelemben kialakult feketelista/szürkelista szabályozási módszertan. A jogalkotó egyes szerződési feltételeket, vagy magatartásokat elve tisztességtelennek tekinthetne, mivel azok súlyosan sértik a fogyasztók, felhasználók jogait, ezeket sorolná a feketelistás feltételek közé. A szürkelista körébe azok a szerződési feltételek, magatartások esnének, amelyek esetén nem egyértelmű a jogsértés fennállása, vagy amelyek a felek között az érintett részére valós előnnyel nem kompenzálják, hogy személyes adatait megosztja

az adatkezelővel, addig a jogalkotó tisztességtelennek tekinti az adatkezelést, míg annak ellenkezőjét az adatkezelő be nem bizonyítja.

Az adatvédelmi módszerváltással az ágazati önszabályozás további korlátait is szükséges meghatározni, mivel az adatvédelem alapjogi jellegű védelmétől és érvényesítésétől a vertikális jogviszonyokban, azaz az állammal szemben nem lehet visszalépni. Sőt egyre nagyobb állami információ éhséggel találjuk szembe magunkat, amely indokolja az adatvédelem alapjogi jellegének fenntartását, és fejlesztését az állammal szemben. Így ki kell zárni, hogy ágazati önszabályozás címén az állami hatóságok az adatgyűjtési hatáskörüket kötelezettségként magán adatkezelőkre ruházzák át, illetve ha erre törvényi szinten mégis sor kerül, akkor kizárólag a lehető legszükségesebb esetben kerülhessen erre sor, így ha azt az emberi élet, a közbiztonság közvetlen veszélyeztetése indokolja. Véleményem szerint a magán adatkezelők csak kivételesen váljanak az állam meghosszabbított karjaként a személyes adatok állami adatgyűjtőjévé. A fent leírtak szerint egyszerre lehet fenntartani az adatvédelem alapjogi védelmi rendszerét, és hozzáigazítani az adatvédelmi elveket a technológia fejlődéshez.

#### Adatvédelmi biztos versus adatvédelmi hatóság

Véleményem szerint az adatvédelmi biztos jelenleg anakronisztikus szerepkörben áll, mivel az információs önrendelkezési jog védelme érdekében országgyűlési biztosként magánjogi szerződéses viszonyokban kell hatósági jogalkalmazási eszközöket alkalmaznia hatóságként, valós jogi eszköz nélkül. Az adatvédelmi biztos jogi eszközrendszere viszonylag szegényes, mivel jelenleg adattörlésre irányuló kötelezéseket rendelhet el, de a hatósági jogalkalmazáshoz hasonló joghátrányokat jelentő szankcionálási jogkörrel nem rendelkezik. Az adatvédelmi biztos mellett a Nemzeti Hírközlési Hatóság kapott az adatvédelemmel rokon területen, a kényszerű elektronikus levelezés



területén hatásköröket, de ezt egyedi esetként idézem. Véleményem szerint az adatvédelem hatósági védelme hiányzik az adatvédelem komplex állami jogvédelmi rendszeréből. Nem azt állítom, hogy az adatvédelmi biztos hatásköreit át kellene adni egy állami adatvédelmi központi hatóságnak, hanem meg kellene teremteni az információs önrendelkezési jogot érintő magánjogi jogviszonyok állami felügyeletét. Nem lenne szükséges újabb állami hatóságot erre a célra felállítani, hanem a már működő a fogyasztóvédelem, hírközlési, oktatási, munkaügyi, egészségbiztosítási államigazgatási szervek hatásköreit, így területén kellene szisztematikusan kiterjeszteni a személyes adatok védelmének tárgyköreibre. Így az adatvédelmi ombudsman visszakerülne abba az alkotmányos funkciójába, hogy az Országgyűlés „nyitott szemeként” az állami hatóságok tevékenységét ellenőrizné, és állásfoglalásaival, iránymutatásaival szolgálná az adatvédelmi jogtudat fejlesztését. Így a megoldás, az adatvédelmi biztos és az adatvédelmi hatósági jogkörök gyakorlásának összhangja lehet azzal, hogy mindegyik szervezetrendszer a rá jellemző jogi eszköztárat alkalmazhassa működése során.

### Személyiség védelem versus adatvédelmi bírászkodás

A személyiségi jogokat védő polgári jogi szabályok és a személyes adatok védelme között az egyik alapvető összefüggés, hogy mindkét esetben a jogvédelem célja, hogy az egyén személyiség szabadságát, annak kibontakoztatását, az érintett önazonosságát védje, és hatékony fellépési lehetőséget biztosítson a jogsértőkkel szemben. Ha az adatvédelem módszerváltására sor kerül, akkor az adatvédelmi bírászkodásnak is hangsúlyosabb szerephez kell jutnia, például azzal, hogy az adatvédelmi biztost megilletethné közérdekű per indítása, ha a keretjogszabálynak nem felelnek meg egyes ágazati szabályozások, vagy ha érintettek széles körének

védelmében szükséges hatékony szankciórendszer kerüljön alkalmazásra az adatvédelem területén.

Véleményem szerint a XXI. században a személyiségi jogsértések, így identitáslopás, képmással való visszaélés, becsületsértés sok esetben már az informatika világában kerülnek elkövetésre, pl: hamis levélküldéssel, belépési jelszavak megszerzésével, digitális képnek, vagy valótlan ténynek interneten történő publikálásával. Ezekben az esetekben a hagyományos személyiségvédelem jogi eszközrendszere tehetetlen, mivel olyan bizonyítási terhet ró a sérelmet szenvedett félre, amely a jogsérelem esetén elrettenti a sérelmet szenvedett felet jogainak érvényesítésétől. Mivel a személyiségi jogi védelem kiterjed a személyes adatokra, ha azoknak a feldolgozása számítógéppel vagy más módon történő adatkezeléssel és adatfeldolgozással történik, megnyílik a lehetősége annak, hogy adatvédelmi igényként határozzuk meg személyiségi jogi sérelmünket. Álláspontom szerint a polgári törvénykönyvben lefektetett személyiségi jogok megsértése esetén az Avtv.. törvény alkalmazható a lex specialis derogat legi generali elv alapján. Az adatvédelmi törvény alapján érvényesítő jogvédelmi eszközök a személyiség megsértésének azon eseteiben nyújtanak védelmet, amikor az adatvédelmi törvényben meghatározott adatkezelésre kerül sor meghatározott jogalap vagy törvényi cél nélkül. Az utóbbi években az adatvédelmi bíraskodás a magyar jogban egyre inkább kezd meghonosodni, és egyre több jogesetet is lehet találni, amikor személyiségi jogi perben az adatvédelmi törvény rendelkezései kerültek alkalmazásra. A kialakított Legfelsőbb bírósági, illetve ítéltáblai gyakorlatnak megfelelően a bíróságok széleskörűen értelmezik a személyes adat fogalmát, illetve hajlandók jogellenesnek kimondani törvényi felhatalmazás nélkül végrehajtott hatóságok közötti adattovábbítást. Véleményem szerint a jövőben a bíróságoknak egyre több esetben kell majd alkalmazni az adatvédelmi törvény rendelkezéseit, mivel a jogsértések egyre többször digitális eszközökkel, informatikai környezetben kerülnek elkövetésre, mint jogosulatlan megfigyelés vagy lehallgatás, törvényi

felhatalmazás nélküli adattovábbítás, illetve személyhez fűződő adatok jogellenes kezelése miatt. A személyes adatok védelme és a személyiség védelmi jogi eszközrendszer összhangban történő értelmezése, valamint a bírósági joggyakorlatban történő egyre tudatosabb alkalmazása vezethet oda, hogy a XXI. században hatékony jogvédelmi rendszer védje az információs önrendelkezési jogunkat.

Zárógondolat:

Az adatvédelem előtt álló XXI. századi lényeges kihívás, hogy sikerül-e egyensúlyt találni a magánszféra védelmét szolgáló elvek, így a célhoz kötött adatkezelés, az arányosság, a készletező adatgyűjtés tilalma, az információs önrendelkezés és az információs hatalommegosztás, illetve másrésről a korlátokat nem ismerő állami- és magánadatgyűjtés, a biztonságra való hivatkozás elsőbbsége, a magán-titkosszolgálatok információéhsége és saját megalkuvásunk között. Az adatvédelemnek módszerváltásra van szükség ahhoz, hogy a XXI. századi követelmények között is biztosítsa az információs önrendelkezési jogunk valódi érvényesülését. Az adatvédelmi módszerváltás akkor valósulhat meg, hogy ha a magánjogi jogviszonyokban mód nyílik az ágazati önszabályozás eszközrendszerével technológia orientált jogi környezetet kialakítására, amely az adatvédelmi elvekkel összhangban áll, illetve az adatvédelmi biztos mellé az államigazgatás is felzárkózik az információs önrendelkezési jog védelme érdekében, valamint ha a bírósági jogalkalmazás során is sikerül a klasszikus személyiségvédelmi elvek, és a személyes adatok védelmét összhangban alkalmazni.

## ZUSAMMENFASSUNG

Der Schutz von Personaldaten in Ungarn, sein Institutionssystem wird in der Arbeit mit den rechtlichen Mitteln des Datenschutzes in der Europäischen Union verglichen. Bei den allgemeinen Fragen des Datenschutzes zieht der Autor die Generationen der internationalen, europäischen und ungarischen Datenschutzregelungen zum Vergleich auf die Art heran, dass er dabei auch die Urteilpraxis des Europäischen Gerichtshofs für Menschenrechte, des Europäischen Gemeinschaftsgerichtshofs bzw. des ungarischen Verfassungsgerichts darstellt. Der Autor beschäftigt sich ausführlich mit den einzelnen Komponenten des Begriffs von Personaldaten, mit der Problematik des Datenschutzes von den nationalen Rundtischverhandlungen an bis zur Abänderung des Datenschutzgesetzes im Rahmen der Rechtsharmonisierung. Der Autor beschreibt detailliert die Vorgeschichte, die Rechtsvorschriften der Richtlinie 95/46/EG zum gemeinschaftlichen Schutz von Personaldaten, bzw. die Tätigkeit der Arbeitsgruppe Artikel 29, wo die Probleme der Rechtsschaffung zum Datenschutz angesprochen wurden. Mit der Institution des Datenschutzkommissars, der die Datenschutzkontrolle bei den gemeinschaftlichen Institutionen durchführt, werden die Befugnisse, die Tätigkeit und die Rechtspraxis der ungarischen Institution zum Datenschutz verglichen. In seiner Arbeit behandelt der Autor nicht nur die allgemeinen Fragen des Datenschutzes, seine Bestrebung besteht darin, sich auch mit den Datenschutzvorschriften zu beschäftigen, die sich auf die nichtstaatlichen Datenverwaltungsformen in den einzelnen Bereichen des gemeinschaftlichen Rechts beziehen, wobei er sich außerdem bezüglich dieser Thematik der Vergleich mit den sektoralen Bereichen des ungarischen Datenschutzes zum Ziel gesetzt hat. Die Vorschriften des gemeinschaftlichen sektoralen Datenschutzes wurden vor allem in den Bereichen des Fernmeldewesens, der Nachrichtenübermittlung, des E-Handels, bzw. im Anschluss an die dritte Säule in der Datenbehandlung bei der Polizeizusammenarbeit zur Zurückdrängung der grenzüberschreitenden Kriminalität weiterhin bei dem Asyl- und Flüchtlingswesen erarbeitet. Wenn man die Datenverwaltung zum Zwecke von Staat, Selbstverwaltung, Polizei und Strafverfolgung nicht berücksichtigt, umfasst der nationale sektorale Datenschutz allerdings ein weitaus breiteres Gebiet als den E-Handel und die Nachrichtenübermittlung, er erstreckt sich nämlich auf Persönlichkeits- und Bildnisschutz, Verwaltung von Gesundheitsdaten, Direktmarketing, Privacy am Arbeitsplatz, Datenverwaltung im Bildungswesen, bzw. auch auf den privaten Vermögensschutz. Mit ihrer Übersicht der ungarischen Datenverwaltung in dem nichtstaatlichen Sektor macht die Arbeit auf die positiven und negativen Tendenzen aufmerksam, die in der ungarischen Rechtsschaffung und Rechtsanwendung zu erfahren sind.

Felhasznált irodalom

## KÖNYVEK

*Az adatvédelmi biztos beszámolója, 1995-1996*, Adatvédelmi Biztos Irodája, Budapest, 1997

*Az adatvédelmi biztos beszámolója, 1998*, Adatvédelmi Biztos Irodája, Budapest, 1999

*Az adatvédelmi biztos beszámolója, 1999*, Adatvédelmi Biztos Irodája, Budapest, 2000

*Az adatvédelmi biztos beszámolója, 2000*, Adatvédelmi Biztos Irodája, Budapest, 2001

*Az adatvédelmi biztos beszámolója, 2001*, Adatvédelmi Biztos Irodája, Budapest, 2002

Vincent BERGER, *Az Emberi Jogok Európai Bíróságának joggyakorlata*, Budapest, HVG, 1999

DÓSA Imre, POLYÁK Gábor, *Informatikai jogi kézikönyv*, Budapest, KJK-Kerszöv, 2003

*Egy alkotmány-előkészítés dokumentumai: kísérlet Magyarország új Alkotmányának megalkotására, 1988-1990*, szerk. KILÉNYI Géza, Budapest, Magyar Tudományos Akadémia Államtudományi Kutatóközpont, 1991

*Emberi jogok*, szerk. HALMAI Gábor, TÓTH Gábor Attila, Budapest, Osiris, 2003 (Osiris tankönyvek)

*Entscheidungen des Bundesverfassungsgerichts. Studienauswahl*, hrsg. Jürgen SCHWABE, 2004

HAJDÚ József, *A munkavállalók személyes adatainak védelme az EU és a tagállamok jogában, különös tekintettel az elektronikus kommunikációra*, Szeged, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 2003 (Acta Universitatis Szegediensis) (Acta Juridica et Politica)

*Handbuch Datenschutzrecht : die neuen Grundlagen für Wirtschaft und Verwaltung*, hrsg. von Alexander ROSSNAGEL, München, Beck, 2003

F. HATÓ Katalin, *Adatbiztonság, adatvédelem [önálló tanulásra]*, Budapest, SZÁMALK, 2000

Bern HOLZNAGEL, *Recht der IT-Sicherheit, München, Beck C.H., 2003.*

Francis G. JACOBS, Robin C.A. WHITE, *The European Convention on Human Rights*, Oxford, Clarendon Press, 2002

Rosemary JAY, Angus HAMILTON, *Data Protection Law and Practice*, London, Sweet and Maxwell, 1998

Thomas HOEREN, *Grundzüge des Internetrechts*, München, Verlag C.H. Beck, 2002

JÓRI András, *Adatvédelmi kézikönyv : elmélet, történet, kommentár*, Budapest, Osiris Kiadó, Budapest, 2005 (Osiris kézikönyvek )

KOPPÁNYI Szabolcs, *A hírközlés szabályozása az Európai Közösségben és Magyarországon*, Budapest, Osiris, 2003 (Osiris tankönyvek)

Werner LIEDTKE, *Das Bundesdatenschutzgesetz: Eine Fallstudie zum Gesetzgebungsprozess*, Bamberg. Difo-Druck, 1980

Matthias LEIST, *Verfassungsrechtliche Schranken des steuerlichen Auskunfts- und Informationsverkehrs*, Frankfurt, 2000 (Mannheimer Beiträge zum Öffentlichen Recht und Steuerrecht, 22)

- MAJTÉNYI László, *Az adatvédelem Magyarországon és az Európai Unióban*, Budapest, Magyar Posta Részvénytársaság, 1999 (A postai ágazat és az Európai Unió : integrációs füzetek) (Európai Unió füzetek)
- MAJTÉNYI László, „*A megtalált alkotmány? Az alapjogi bírászkodás első kilenc éve, Az első alkotmánybíróság és az információs szabadságok*”, Budapest, INDOK, 2000
- MAJTÉNYI László, *Az információs szabadságok: adatvédelem és a közérdekű adatok nyilvánossága*, Budapest, Complex, 2006
- Oda átra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok)
- OROS Paulina, SZURDAY Kinga, *Adatvédelem az Európai Unióban*, Budapest, Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ, Külügyminisztérium, 2003 (Európai füzetek, 35.)
- Polgári Törvénykönyv magyarázata*, szerk. GELLÉRT György, Budapest, KJK-Kerszöv, 2001
- PETRIK Ferenc, *A személyiség jogi védelme*, Budapest, Közgazdasági és Jogi Könyvkiadó, 1992
- A rendszerváltás forgatókönyve : kerekasztal-tárgyalások 1989-ben : dokumentumok*, szerk. ELBERT Márta, [et al.], Budapest, Új Mandátum Kiadó, 1999
- Rolf SCHMIDT, *Grundrechte*, Bremen, Rolf Schmidt Verlag, 2003
- Claude Elwood SHANNON, Warre WEAWER, *A kommunikáció matematikai elmélete : az információelmélet születése s távlatai*, Budapest, Országos Műszaki Információs Központ és Könyvtár, 1986
- Birte SIEMEN, *Datenschutz als europäisches Grundrecht*, Dunkcker und Humbolt, Berlin, 2005
- SÓLYOM László, *A személyiségi jogok elmélete*, Budapest, Közgazd. és Jogi Kvk., 1983.
- Brunhilde STECKLER, *Grundzüge des EDV-Rechts: das Recht der Datenverarbeitung und der online Daten*, München, Verlag Franz Vahlen, 1999
- SZLADITS Károly: Magyar Magánjog Általános rész IV. füzet, Grill Károly Könyvkiadóvállalata Budapest, 1941.
- Tízéves az Adatvédelmi Biztos Irodája*, szerk. PÉTERFALVI Attila, Budapest, Adatvédelmi Biztos Irodája, 2006
- ZLINSZKY Imre: A magyar magánjog mai érvényében különös tekintettel a gyakorlat igényeire, Franklin Társulat Budapest, 1897. 465. old
- Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1957, 31-32.

## CIKKEK, TANULMÁNYOK

- L. ABEK, *Geschichte des Datenschutzrechts = Der neue Datenschutz, Datenschutz in der Informationsgesellschaft von morgen*. Hrsg. BÄUMLER, H., Berlin, Luchterhand Verlag, 1998.
- D. BANISAR, *A Privacy védelmének modelljei = Oda átra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 9-33.
- BALOGH Zsolt György, *Az adatvédelmi törvény fejlesztésének kérdései*, Jogtudományi Közlöny, 1997/52, 6. sz. 269-276.

- Isaiah BERLIN, *A szabadság két fogalma.* = I. B., *Négy esszé a szabadságról*, Budapest, Európa, 1990. 342
- Sascha BIER, *Internet und Email am Arbeitsplatz*, Datenschutz und Datensicherheit, 2004/28, 5.
- Johann BIZER, *Private Internetnutzung am Arbeitsplatz*, Datenschutz und Datensicherheit, 2004/28, 7.
- Ulf BRÜHANN, *Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem*, Datenschutz und Datensicherheit 2004/28, 4.
- Franz BÜLLINGEN, *Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich*, Datenschutz und Datensicherheit, 2005/29, 9.
- Peter CHURCH, *Overview of Direct Marketing Legislation in the EU and UK*, World Data Protection Report, 2003/07
- Daniel COOPER, *EU Data Retention Proposals in the Headlines*, World Data Protection Report, 2005/05
- Richard CUMBLEY, *European Union: Report on the Implementation of Safe Harbor*, World Data Protection Report, 2004/11
- DUDÁS Gábor, *Az adatvédelem és a titokvédelem néhány gyakorlati kérdése*, Belügyi Szemle 1999/47, 11. sz. 3-15.
- Demetrios ELEFThERIOU, *A Guide to US Federal Data Protection Laws*, World Data Protection Report, 2005/02
- Andre FIEBIG, *Some Judicial Guidance in the Interpretation of European Data Privacy Directive*, World Data Protection Report, 2003/12, 6
- David H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, 1989. = *Odaátra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 55-69.
- Robert M. HAYES, *Az információ mérése*, Könyvtári Figyelő, 1994/40, 3. sz. 398.
- HEGEDŰS Bulcsú, *Hogyan működtethető kamera a munkahelyen*, Munkajog, 2005. 6. sz.
- Peter J. HUSTINX, *A considerable step forward<sup>d</sup>* : EDPS Opinion on the proposal for a framework decision for data protection in the third pillar
- Peter J. HUSTINX, *Data Protection in the EU*. [www.edps.eu.int](http://www.edps.eu.int) ; 2006.12.15.
- Peter J. HUSTINX, *Megfelelő védelem – A 29. cikk Adatvédelmi Munkacsoport 6/99. sz. véleménye* = Tízéves az Adatvédelmi Biztos Irodája, szerk. PÉTERFALVI Attila, Budapest, Adatvédelmi Biztos Irodája, 2006, 79-89.
- Ehmann HORST, *Prinzipien des deutschen Datenschutzrechts – unter Berücksichtigung der Datenschutzrichtlinie der EG vom 24.10.95 (Teil I und teil II) Recht der Datenverarbeitung 1998 heft 6*
- Werner HÜLSMANN, *Gegen EU-Vorratsdatenspeicherung*, Datenschutz und Datensicherheit, 2004/28, 12.
- Hansjürgen GARTSKA, *Datenschutz*, Aufbruch zu neuen Ufern
- KISS Éva, *A személyiségi jogok védelme – nemzetközi kötelezettségeink*, Magyar Jog, 1992. 10.

- Michael KLOPHER, *Pressefreiheit statt Datenschutz., Datenschutz statt Pressefreiheit?*; Zeitschrift für Medien und Kommunikation, 2003. 6. 511-523.
- Michael KLOPHER, *Informationszugangsfreiheit und Datenschutz, zwei Säulen des Rechts der Informationsgesellschaft*, Öffentliche Verwaltung, 2003 März, Heft 6. 211-231.
- Michael KLOPHER, *Videoaufnahmen und Videoaufzeichnungen als Rechtsproblem*, Deutsches Verwaltungsblatt, 1998/113, Heft 6.
- KOVÁCS Vendel, *Gazdasági kémkedés és adatvédelem*, Belügyi Szemle, 1996/46. 2. sz 19-24
- KÖHALMY Kata, *Adatvédelem a helyi közigazgatásban = Odaátra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 109-121.
- KÖNYVES-TÓTH Pál, *Adatvédelem és szabad adatáramlás*, Figyelő, 1990.
- KÖNYVES-TÓTH Pál, *Adatvédelem és információszabadság*, Világosság, 1990. 8-9. sz. 621.
- Detlen KRÖGER, *Informationsfreiheit im Gemeinschaftsrecht*, Datenschutz und Datensicherheit, 2003/1, 29-34
- Christopher KUNER, *The Commission's First Report on Implementation of the EU Data Protection Directive*, World Data Protection Report, 2003/08
- LAKATOS Miklós, *A személyiség joga, az állam működőképességének a joga*, Valóság, 1993/36, 3. sz.
- LAKATOS Miklós, *Az adatvédelem jogi szabályozása a magyar népszámlálások tükrében = Népszámlálások az ezredfordulón*, szerk: KEPECS József, Budapest, KSH, 1998, 794-811.
- LAKATOS Miklós, *Információszabadság - adatvédelem – statisztika*, Statisztikai Szemle 1996. 4. sz. 293-303.
- LAKATOS Miklós, *Információszabadság - adatvédelem – statisztika*, Statisztikai Szemle, 1999. 8. sz. 6674-680.
- Sabine LEUTHEUSSER, *Verfassungsrechtliche Schranken des Grossen Lauschangriffs* Datenschutz und Datensicherheit, 2005/29, 6.
- MAJTÉNYI László, *Az információs szabadságok és az adatvédelem*, Világosság 2002. 2. sz.
- MAJTÉNYI László, *A két szabadság*, Élet és Irodalom, 1999. 16. sz. 4.
- MAJTÉNYI László, *Az adatvédelem és az információszabadság Magyarországon = Az ombudsman szerepe és feladatai a közép- és kelet-európai országokban a rendszerváltás után*, Budapest, Országgyűlési Biztosok Hivatala, 1997, 80-86.
- MAJTÉNYI László, *Adatvédelem, információszabadság, sajtó*, Világosság 1997. 2. sz. 3-23.
- MAJTÉNYI László, *Adatvédelem, információszabadság, üzleti titok = A matematikától a kriminálinformatikáig Emlékkönyv dr. Kovacsicsné Nagy Katalin emlékére*, Budapest, 2001, 153-157.
- MAJTÉNYI László, *Az adatvédelem és az információszabadság az Alkotmányban*, Acta Humana 1995.18/19.
- MAJTÉNYI László, *Az adatvédelmi ombudsman - az adatvédelmi törvényhozás*, Magyar Közigazgatás 1990. 8. sz. 695-701.



MAJTÉNYI László, *Az adatvédelem ügye Kelet-Közép Európában = Oda átra nyíló ajtó*, szerk. U.Ö., Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 151-170.

MAJTÉNYI László, *Az információs jogok = Emberi jogok, szerk. HALMAI Gábor, TÓTH Gábor Attila, Budapest, Osiris, 2003* (Osiris tankönyvek), 577-637.

MAJTÉNYI László, *Az információs szabadságjogok Magyarországon*, Világosság, 1998/39, 10. sz. 49- 61.

MAJTÉNYI László, *Az "első" Alkotmánybíróság és az információs szabadságjogok = Alkotmánybíráskodás tíz éve*, Budapest, 2000,

Thomas MAIER, *Der Zugang zu den Teilnehmerdaten*, Europäisches Telekommunikationsrecht Kommunikation und Recht, 2005/8, 362.

MEZŐ István, A dokumentumokhoz való hozzáférés az Európai Unió jogában / World Wide Web Online változata is megjelenik eVilág : az információs társadalom folyóirata. - 2 : 11 (2003), p. 14-19.

MEZŐ István, Az információs szabadság és a computerprogramok szerzői jogi védelme In: *Studia iurisprudentiae doctorandorum Miskolciensium = Miskolci doktoranduszok jogtudományi tanulmányai* /[szerk. STIPTA István]. - Miskolc :Bíbor, 2004. - p. 29-44. - (Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola Kiadványsorozata ; 5/2.)

MEZŐ István, Információs hatalommegosztás; Doktoranduszok fóruma : Miskolc, 2002. november 6. /[szerk. LehoczkyLászló]. - Miskolc : Miskolci Egyetem Innovációs és Technológiai Transzfer Centruma, 2003. - p. 148-154

MEZŐ István, Információs szabadságjogok a magyar alkotmánybíróság gyakorlatában in: *Studia iurisprudentiae doctorandorum Miskolciensium = Miskolci doktoranduszok jogtudományi tanulmányai* /[szerk. STIPTA István]. - Miskolc :Bíbor, 2002. - p. 23-58. - (Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola Kiadványsorozata ; 2/2.)

MEZŐ István, Áttekintés az információs szabadság kialakulásáról és hazai fejlődéséről in: *Studia iurisprudentiae doctorandorum Miskolciensium = Miskolci doktoranduszok jogtudományi tanulmányai* /[szerk. STIPTA István]. - Miskolc :Bíbor, 2002. - p. 111-133. - (Miskolci Egyetem Deák Ferenc Állam- ésJogtudományi Doktori Iskola Kiadványsorozata ; 1/2.)

MEZŐ István, Vázlat a környezeti információkhoz való hozzáférés európai és hazai szabályrendszeréről, tekintettel az adatvédelmi biztos gyakorlatára in: *A környezetvédelmi szabályozás elmélete és gyakorlata : a környezeti adatokhoz való hozzáférés lehetőségei a magyar közigazgatásban című konferencia előadásai* /[szerk. Fodor László]. - Debrecen : Lícium-Art, 2004. - p. 161-178. - (Debreceni konferenciák ; 2.)

MEZŐ István, A dokumentumokhoz való hozzáférés az Európai Unióban in: *Collectio Iuridica Universitatis Debreceniensis*. - 4 (2005), p. 151-180.

MEZŐ István, Vázlat az információs szabadságjogok kialakulásáról, Doktoranduszok fóruma : Miskolc : 2001. november 6. /[szerk. LehoczkyLászló]. - Miskolc : Miskolci Egyetem Innovációs és Technológia Transzfer Centrum, 2002. - p. 189-194.

George MOORE, *Data Protection and Personal Genetic Information*, World Data Protection Report, 2003/03

OCSKOVSZKY János, *Az államtitokról és a szolgálati titokról szóló új jogi szabályozás sajátosságai*, Belügyi Szemle, 1996/46. 3. sz. 17-27.

- Tanguy von OVENSTRAETEN, *The Implementation of EU Data Protection Legislation in the Accession Countries*, World Data Protection Report, 2004/09
- PÉTERFALVI Attila, *A személyes adatok védelméről és közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításai* = Tízéves az Adatvédelmi Biztos Irodája, szerk. PÉTERFALVI Attila, Budapest, Adatvédelmi Biztos Irodája, 2006, 21-39.
- Charles, RAAB, *Gondolatok az információs jogok magyarországi tapasztalatairól = Odaátra nyíló ajtó*, szerk. MAJTÉNYI László, Budapest, Adatvédelmi Biztos Irodája, 2001 (Információs szabadságok), 33-55.
- Philipp, RAETHER, *Die EU-US Flugdaten Affaere*, Datenschutz und Datensicherheit, 2004/28, 8.
- Alexander ROSSNAGEL, *Modernisierung des Datenschutzrechts: Empfehlungen eines Gutachtens für den Bundesminister Rechts der Datenverarbeitung*, 2002. 2, 61-70.
- Alexander ROSSNAGEL, Gerit HARNUNG, *Biometrische Daten in Ausweisen*, Datenschutz und Datensicherheit, 2005/29, 2.
- Heather ROWE, *The Transfer of Personal Data Regarding Airline Passengers from the EU to the U.S.*, World Data Protection Report, 2004/03, 13.
- SASSE: *Sinn und Unsinn des Datenschutzes*, 1976. Neue Juristische Wochenzeitschrift 1971
- Peter SCHAAR, *Datenschutzpolitische Strategiepapier*, Datenschutz und Datensicherheit, 2004/28, 12.
- Philip SCHOLZ, *Datenschutz bei Data Warehousing und Data Mining* = Handbuch Datenschutzrecht : die neuen Grundlagen für Wirtschaft und Verwaltung, hrsg. von Alexander ROSSNAGEL, München, Beck, 2003
- SÓLYOM László, *Egy új szabadságjog: az információs szabadság*, Világosság, 1988. 1. sz.
- SÓLYOM László, *Adatvédelem és személyiségi jog*, Világosság, 1988. 1. sz.
- SÓLYOM László, *Az ombudsman „alapjog értelmezése” és „normakontrollja”*, Fundamentum, 2001/5, 2. sz. 14-23.
- Blair STEWART, *The Economics of Data Privacy*, World Data Protection Report 2004/12.
- SZÉKELY Iván, *Az egyén és az információs hatalom*, Eszmélet, 1995/7, 27. sz. 124-141.
- SZURDAY Kinga, *Az adatvédelmi jogi szabályozás szerepe, feladatai és hatása a közigazgatásra és a versenyszférára*, Magyar Jog, 1994. 11 sz. 661-665.
- Henriette TIELEMANS, *EU Data Privacy Notices*, World Data Protection Report, 2001/05
- Marie-Theres TINNEFELD, *Menschenwürde, Biomedizin und Datenschutz. Von der Zeit zu handeln* = Zeit und kommunikative Rechtskultur in Europa. Im Spiegel von Deutschen und Polen, hrsg. Siegfried LAMNEK, Marie-Theres TINNEFELD, Baden-Baden, 2000
- Marie-Theres TINNEFELD, Heidi SCHUSTER, *Mangel an Vertrauen in die Telekommunikation*, Datenschutz und Datensicherheit, 2005/29, 79.
- Ellen TEMPERTON, *Workplace Monitoring in Europe*, World Data Protection Report, 2001/04. 18.
- Dietmar WOLFF, *Direktwerbung und Datenschutz*, Rechts der Datenverarbeitung, 1999, Heft 1. 9-12.
- Peter WEDDE, *Schutz vor verdeckten Kontrolle im Arbeitsverhältnis*, Datenschutz und Datensicherheit, 2004/28, 1.

Martin ZILKENS, *Datenschutz am Arbeitsplatz*, Datenschutz und Datensicherheit, 2005/29, 5.

ZLINSZKY Imre: *A magyar magánjog mai érvényében különös tekintettel a gyakorlat igényeire*, Franklin Társulat Budapest, 1897

ZSCHERPE, *Datenschutz im Internet – Grundsätze und Gestaltungsmöglichkeiten für Datenschutzerklärungen*, Kommunikation und Recht, 2005/6 264-269.

WARREN/BRANDEIS, *The right to privacy*, Harvard Law Review 1890, 196.old.

### **Internetes források**

[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2005/05-04-21\\_Data\\_Protection\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2005/05-04-21_Data_Protection_EN.pdf)

[www.datatilsynet.dk](http://www.datatilsynet.dk)

[www.dp.gov.ee](http://www.dp.gov.ee)

[www.tietosuoja.fi](http://www.tietosuoja.fi)

[www.uouu.cz](http://www.uouu.cz)

[www.dsk.gv.at](http://www.dsk.gv.at)

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp109\\_hu.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp109_hu.pdf)

[http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp104\\_de.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_de.pdf)

<http://www.jrc.es/FutureBottlenecksStudy.pdf>

<http://www.arukuldok.hu/>

### **Európai adatvédelmi ajánlások és irányelvek**

Az Európai és a Tanács 95/46/EK irányelve (1995. október 24) a személyes adatok feldolgozása vonatkozásában az egyén védelméről és az ilyen adatok szabad áramlásáról, Celex:31995l0046; Official Journal L.281, 1995.11.23. 0031.-tól 0050.-ig. [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:22000D1123\(08\):HU:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:22000D1123(08):HU:HTML) ; 2006.11.18

Az Európai és a Tanács 96/9/EK irányelve (1996. március 27.) irányelv az adatbankok jogi védelméről

Az Európai Parlament és a Tanács 1997. május 20-i 97/7/EK irányelve a távollevők között kötött szerződések esetén a fogyasztók védelméről. Az irányelvet a 17/1999 (II.5) Korm. Rendelet implementálta

Az Európai Parlament és a Tanács 97/66/EK irányelve (1998. szeptember 24.) a személyes adatok feldolgozásáról és a magánélet védelméről a távközlési ágazatban. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:22003D0080:HU:NOT> ; 2006.10.24

Az Európai Parlament és Tanács 2002/22/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról („Egyetemes szolgáltatási irányelv”)

AZ Európai Parlament és Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról („Keretirányelv”)

Az Európai Parlament és Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv”)

Az Európa Tanács Határozata a magánszektor adatbankjaiban tárolt személyes adatok védelméről [EU\_R22/73]

(Council of Europe \_ Resolution (73)22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 1973.).

<http://tinyurl.com/3fsz9> ; 2006.11.18.

Az Európa Tanács Határozata az állami szektor adatbankjaiban tárolt személyes adatok védelméről [EU\_R29/74]

(Council of Europe \_ Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 1974.).

<http://tinyurl.com/36olj> ; 2006.11.15.

Bericht der Kommission, Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46)

Brüssel, den 15.5.2003. KOM (2003) 265. [http://eur-lex.europa.eu/LexUriServ/site/de/com/2003/com2003\\_0265de01.pdf](http://eur-lex.europa.eu/LexUriServ/site/de/com/2003/com2003_0265de01.pdf) ; 2007.11.20.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.:108.

Communication de la Commission relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté et à la sécurité des systèmes d'information, SYS 287. Commission de Communautés Européennes COM (90) 314 final SYN 287 et 288 Bruxelles le 13 septembre 1990

Draft Framework Decision on the retention of data processed and stored in connection with provision of publicly available electronic communications service or data on public communication networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (Doc 8958/04; <http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>

Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final)

Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24. October 1995. . [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp114\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf) ; 2006.11.02.

2000/497/EC: Commission Decision of 27. December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC

2000/519/EC: Commission Decision of 26. July 2000 pursuant to Directive 95/46/EC of the European Parliament and of Council on the adequate protection of personal data provided in Hungary. [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l\\_215/l\\_21520000825en00040006.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00040006.pdf) ; 2006.11.05.

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked question issued by the US Department of Commerce. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML> ; 2006.10.30.

Opinion 6/99 Working Party on the protection of individuals with regard to the processing of personal data, *Concerning the level of personal data protection in*

*Hungary.* Adopted on 7 September 1999.

<http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1999/F/4> ; 2006.11.10.

C-450/00: Action brought on 6 December 2000 by the Commission of the European Communities against the Grand Duchy of Luxembourg. [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/c\\_045/c\\_04520010210en00110011.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/c_045/c_04520010210en00110011.pdf) ; 2006.01.06.

C-101/01 Az Európai Bíróságnak Lindqvist-ügyben 2003. november 6-án hozott ítélete <http://curia.europa.eu/jurisp>; 2006.12.11.

C-465/00 Az Európai Bíróság „Österreicher Rundfunk és mások” (“Rechnungshof”) (a C-465/00., C-138/01. és C-139/01. egyesített ügyek, 2003. május 20-i ítélet, teljes kamara, (2003) ECR I-4989) ügyben hozott ítélete, ECR [2003] I-04989, (71) és (72) bekezdés. [http://eur-lex.europa.eu/LexUriServ/site/de/oj/2003/c\\_171/c\\_17120030719de00030004.pdf](http://eur-lex.europa.eu/LexUriServ/site/de/oj/2003/c_171/c_17120030719de00030004.pdf) ; 2006.12.11

C-318/04 Európai Parlament kontra az Európai Közösségek Bizottsága. <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=hu> ; 2006.10.25.

### **Felhasznált jogszabályok**

Magyar jogszabályok

Törvények

1869.évi. III. törvény a népszámlálásról

1897.évi XXXV törvény a m. kir. központi statisztikai hivatalról

1952. évi III. törvény a polgári perrendtartásról

1959. évi IV. törvény a Polgári Törvénykönyvről

1972. évi V. törvény a Magyar Köztársaság ügyészségéről

1992. évi XXIII. törvény a köztisztviselők jogállásáról

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról

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

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

1993. évi XXXI törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről

1993. évi LIX. törvény az állampolgári jogok országgyűlési biztosáról

1993. évi XCIII. törvény a munkavédelemről

1994. évi XXXIV. törvény a Rendőrségről

1995. évi LXV. törvény az államtitokról és a szolgálati titokról

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

1997. évi XXXII. törvény a határőrizetről és a Határőrségről

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

1998. évi XI. törvény az ügyvédekről

1998. évi XIX. törvény a büntetőeljárásról

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

2003. évi III. törvény az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról

2003. évi C. törvény az elektronikus hírközlésről

2004. évi XIX. törvény a Vám- és Pénzügyőrségről

2005. évi XC. törvény az elektronikus információszabadságról

#### Kormányrendeletek

17/1999 (II.5) Korm. Rendelet a távollevők között kötött szerződésekről

233/2001. (XII. 10.) Korm. rendelet a közszolgálati jogviszonnyal összefüggő adatkezelésre és a közszolgálati nyilvántartásra vonatkozó szabályokról

226/2003. (XII. 13.) Korm. rendelet az elektronikus hírközlési szolgáltató adatkezelésének különös feltételeiről, az elektronikus hírközlési szolgáltatások adatbiztonságáról, valamint az azonosítókijelzés és hívásátírányítás szabályairól

257/2000. (XII. 26.) Korm. rendelet a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvénynek a szociális, valamint a gyermekjóléti és gyermekvédelmi ágazatban történő végrehajtásáról

180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről

#### Miniszteri rendeletek

11/1990. (VI. 13.) IM rendelet az egyházak nyilvántartásának ügyviteli szabályairól

15/1989. (X.7) KeM rendelet az egyes kereskedelmi tevékenységek gyakorlásáról

33/1998. (VI. 24.) NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről

## AB határozatok

2/1990. (II.18) AB határozat Közzétéve a Magyar Közlöny 1990. évi 16. számában

11/1990. (V.1.) AB határozat Közzétéve a Magyar Közlöny 1990. évi 40. számában

18/1990 (VIII.1) AB határozat Közzétéve a Magyar Közlöny 1990. évi 74. számában

20/1990. (X.4.) AB határozat Közzétéve a Magyar Közlöny 1990. évi 98. számában

15/1991 (IV.13) AB határozat Közzétéve a Magyar Közlöny 1991. évi 39. számában

74/1992. (XII.28) AB határozat Közzétéve a Magyar Közlöny 1992. évi 133. számában, AB közlöny, I. évf. 11-12. szám

21/1993 (IV.2.) AB határozat Közzétéve a Magyar Közlöny 1993. évi 38. számában, AB közlöny, II. évf. 3. szám

29/1994. (V.20.) AB határozat Közzétéve a Magyar Közlöny 1994. évi 55. számában, AB közlöny, III. évf. 5. szám

34/1994. (VI. 24.) AB határozat Közzétéve a Magyar Közlöny 1994. évi 55. számában, AB közlöny, III. évf. 5. szám

60/1994. (XII.24.) AB határozat Közzétéve a Magyar Közlöny 1994. évi 124. számában, AB közlöny, III. évf. 12. szám.

46/1995 (VI.30.) AB határozat Közzétéve a Magyar Közlöny 1995. évi 56. számában, AB közlöny, IV. évf. 6-7. szám

58/1995 (IX.15) AB határozat Közzétéve a Magyar Közlöny 1995. évi 76. számában, AB közlöny, IV. évf. 8-9. szám

30/1997. (IV.29.) AB határozat Közzétéve a Magyar Közlöny 1997. évi 37. számában, AB közlöny, VI. évf. 4. szám

16/2001. (V.25.) AB határozat Közzétéve a Magyar Közlöny 2001. évi 59. számában, AB közlöny, X. évf. 5. szám

35/2002. (VII.19.) AB határozat Közzétéve a Magyar Közlöny 2003. évi 69. számában, AB közlöny, XII. évf. 6-7. szám

940/B/2003. AB határozat Közzétéve a Magyar Közlöny 2007. évi. 7. számában, AB közlöny, XVI. évf. 1.

12/2004. (IV. 7.) AB határozat Közzétéve a Magyar Közlöny 2004. évi 63. számában, AB közlöny, XIII. évf. 5.

36/2005. (X.5) AB határozat Közzétéve a Magyar Közlöny 2005. évi 130. számában, AB közlöny, XIV. évf. 9.

## Bírósági határozatok

BH2006. 280 Az előzetes letartóztatás egy év utáni fenntartására ad okot - egyebek mellett - ha az ügyben a sértett és (vagy) a tanúk - a vádlottak részéről történő - megfenyegetésére adatok merülnek fel, s emiatt a bizonyítási eljárás folytatása veszélybe kerül [1998. évi XIX. törvény 132. § (1) bek. b) pont, 129. § (2) bek. c) pont].

BH2004. 170 I. Magántitok minden olyan bizalmas, - csak szűk körben, illetve beavatottak előtt ismert személyi, családi, vagyoni helyzetre, egészségi állapotra, szokásokra vonatkozó tény vagy adat, amelynek nyilvánosságra hozatala a sértettre érdeksérelemmel jár.

BH2000. 293 A közszereplőről készült, karikatúrának minősülő fényképfelvétel nyilvánosságra hozatala nem sérti a képmáshoz való jogot, és az ezáltal kifejezett vélemény sem sért becsületet vagy emberi méltóságot, ha a véleménynyilvánítás nem indokolatlanul bántó, sértő vagy lealacsonyító [1959. évi IV. törvény 76. §, 80. § (1)-(2) bekezdés].

BH2000. 485 A birtokháborító magatartásról készült videofelvétel bizonyítékként való felhasználása nem minősül visszaélésnek, és nem sérti a személyhez fűződő jogokat [1959. évi IV. törvény 80. § (1)-(2) bekezdés].

BH1985. 57. I. A személyhez fűződő jogok megsértése megvalósulhat a képmás vagy hangfelvétel visszaéléssel történő elkészítésével is. Ha a lakó a falon áthallatszó hangos kijelentéseket tesz a szomszédos lakás lakójának személyével kapcsolatban, és ez utóbbi erről a saját lakásában elhelyezett hangfelvevő berendezéssel felvételt készít, ez a magatartás nem jelent más jogvédelemben érintett körében történő illetéktelen behatolást (jogsértést).

LB Pfv. IV.21. 327/1993. Bírósági Határozatok Közleménye 1994

Legf. Bír. Pfv.IV.22.415/1999. Bírósági Határozatok Közleménye 1999

Debreceni Ítéltábla Pf.II.20.516/2008/4

*Legfelsőbb Bíróság Pfv.IV.21.478/2007/4.szám*

Pécsi Ítéltábla Pf.I.20.185/2009/3. szám

### **Felhasznált adatvédelmi biztos állásfoglalások**

Az adatvédelmi biztos ajánlása a közfeladatot ellátó személyek feladatkörével összefüggő személyes adatai nyilvánosságára vonatkozó jogszabályok összhangjának megteremtéséről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=1234\\_H\\_2006](http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=1234_H_2006) ; 2006-10-30

Az álláshirdetésekkkel, valamint a magán-munkaközvetítők tevékenységével kapcsolatos adatvédelmi biztosi ajánlás. [http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=167\\_A\\_2006-3](http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=167_A_2006-3) ; 2006.03.01.

A köztisztviselői törvény szabályai szerinti vagyonyilatkozat-tételi eljárás egyes adatvédelmi kérdéseiről szóló adatvédelmi biztosi ajánlás.

<http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=9177> ; 2005.03.29.

Az anonim HIV szűrővizsgálatok eljárását érintő adatvédelmi biztosi ajánlás.

[7http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=9178](http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=9178) ; 2004.09.27.

Az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltáráról szóló 2003. évi III. törvény alapján az információs önrendelkezési jog és az információszabadság érvényesülésével kapcsolatban lefolytatott vizsgálat eredményét összefoglaló adatvédelmi biztosi ajánlás.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=813\\_K\\_2003](http://abiweb.obh.hu/abi/index.php?menu=aktualis/ajanlasok&dok=813_K_2003) ; 2003.12.15.

Az internetes állelél küldő szolgáltatás adatvédelmi összefüggéseiről szóló adatvédelmi biztosi ajánlás. [http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/M/2&dok=212\\_A\\_2003](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/M/2&dok=212_A_2003) ; 2003.04.13.



Az országgyűlési vizsgálóbizottságok – különösen a 41/2002. (VII. 12.) OGY határozattal létrehozott, a rendszerváltás utáni első, szabadon választott Magyar Országgyűlés megalakulását követően kormányzati politikai szerepet betöltő személyeknek az előző politikai rendszer állambiztonsági tevékenységében való részvételének tényeit és körülményeit vizsgáló bizottság –adatkezelésére vonatkozó adatvédelmi biztosi ajánlás.

<http://abiweb.obh.hu/abi/index.php?menu=aktualis/archivum/ajanlasok&dok=9271> ; 2002.08.00

Az országgyűlési és a helyhatósági képviselőjelölt-ajánlással és a választási kampánnyal kapcsolatos adatvédelmi biztosi ajánlás.

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2002/5/2&dok=381\\_H\\_2002](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2002/5/2&dok=381_H_2002) ; 2002.07.23.

Az Internettel összefüggő adatkezelések egyes kérdéseiről szóló adatvédelmi biztosi ajánlás.

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=406\\_K\\_2000](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=406_K_2000) ; 2001.02.01.

A közérdekű bejelentők, panasztevők személyes adatainak kezelésével kapcsolatos adatvédelmi biztosi ajánlás.

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/M/1/1&dok=833\\_K\\_2000](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/M/1/1&dok=833_K_2000) ; 2000.12.29.

A megfigyelés, adatgyűjtés céljából üzemeltetett képfelvevő, -rögzítő berendezésekkel kapcsolatos adatvédelmi biztosi ajánlás.

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/II/1/2&dok=beszamolok\\_2003\\_IIA3](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/II/1/2&dok=beszamolok_2003_IIA3) ; 200.12.20.

Adósság- és követelésbehajtással foglalkozó gazdasági társaságok személyes adatok kezelésének gyakorlatával kapcsolatos adatvédelmi biztosi ajánlás.

[http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/M/1/1&dok=34\\_A\\_2000](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/M/1/1&dok=34_A_2000) ; 2000.06.19.

Állásfoglalás az október 23.-i zavargásokkal kapcsolatban a kórházaknak küldött rendőrségi megkeresések adatvédelmi kérdéseiről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1734\\_K\\_2006-2](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1734_K_2006-2) ; 2006.10.30.

Állásfoglalás a kuruc.info honlap adatkezeléséről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1578\\_K\\_2006-2](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1578_K_2006-2) ; 2006.10.13.

Állásfoglalás a társadalombiztosítási szervek által történő egyes adatkezelésekről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1301\\_A\\_2006-9](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1301_A_2006-9) ; 2006.10.09.

Állásfoglalás a munkavállalók által küldött elektronikus levél megismerhetőségéről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1393\\_K\\_2006-5](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1393_K_2006-5) ; 2006.10.02.

Állásfoglalás az egykori állambiztonsági szolgálatok által megfigyeltek és megfigyelőik irat-megismerési jogáról.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1438\\_K\\_2006-3](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=1438_K_2006-3) ; 2006.10.02.

Állásfoglalás a prostituáltak rendőrségi és adóhatósági ellenőrzéséről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=2330\\_A\\_2005](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=2330_A_2005) ; 2006.06.08.

Állásfoglalás az egészségügyi adatokon végzett tudományos kutatás adatvédelmi feltételeiről.

<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=11280> ; 2006.05.19.

Állásfoglalás a 2006. évi országgyűlési választások adatvédelmi szempontú értékeléséről.

[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=750\\_H\\_2006](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=750_H_2006) ; 2006.05.19.

Állásfoglalás a hitelintézetek direkt marketing célú adatkezelési gyakorlatáról.  
[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=379\\_H\\_2006-1](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=379_H_2006-1) ;  
2006.03.07.

Állásfoglalás a pozitív adóslistával kapcsolatban.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=10706> ; 2006.01.30.

Állásfoglalás a személyazonosító igazolványok fénymásolásával kapcsolatos banki gyakorlatról.  
[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=z\\_8](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=z_8) ; 2006.01.13.

Az Adatvédelmi Biztos és a Magyar Energia Hivatal közös állásfoglalása a telefonos ügyfélszolgálatokon történő hívásrögzítések szabályaival kapcsolatban.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=10707> ; 2005.12.08.

Állásfoglalás a szexuális úton terjedő fertőző betegségben szenvedő betegek adatainak kezelésével összefüggésben folytatott adatvédelmi biztosi vizsgálat eredményéről.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=9215> ; 2005.11.15.

Állásfoglalás a személyazonosító igazolvány mobilszolgáltatók általi másolásáról  
[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=619\\_H\\_2004](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=619_H_2004) ;  
2005.08.24.

Állásfoglalás a munkahelyi drogtesztokról.  
[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=1994\\_H\\_2004-6](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=1994_H_2004-6) ;  
2005.06.22.

Állásfoglalás az Állambiztonsági Szolgálatok Történeti Levéltárában kezelt dosszié iratának közzétételéről. <http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2005&dok=9224> ;  
2005.01.31.

Állásfoglalás a pozitív adóslista felállításával kapcsolatban.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2004&dok=9227> ; 2004.06.23.

Állásfoglalás az Európai Parlament tagjainak választásával összefüggő adatkezelésekről.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2004&dok=9228> ; 2004.04.07.

Állásfoglalás az érdekképviselési tagságra vonatkozó, illetve a tisztségviselésre utaló különleges adatok kezeléséről.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2004&dok=9229> ; 2004.02.26.

Állásfoglalás a Malév Rt. utasai személyes adatainak továbbításáról.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2004&dok=9230> ; 2004.01.06.

Állásfoglalás a roma lakosság egészségügyi állapotával kapcsolatos felmérésről.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2003&dok=pan> ; 2003.12.13.

Állásfoglalás az országos, illetve helyi népszavazásokhoz, népi kezdeményezésekhez kapcsolódó, valamint egyéb aláírásgyűjtések adatvédelmi szempontjairól.  
[http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2003&dok=1330\\_H\\_2003\\_1](http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2003&dok=1330_H_2003_1) ;  
2003.12.14.

Állásfoglalás az ORFK Köztársasági Őrezred közreműködéséről a népszámlálásban.  
<http://abiweb.obh.hu/abi/index.php?menu=aktualis/archivum/allasfoglalasok&dok=9307> ; 2001.05.00.

Állásfoglalás az országgyűlési képviselők vagyoni helyzetét vizsgálóbizottság létrehozásáról szóló 103/2000.(XII.20.) OGY határozattal kapcsolatban.  
[http://abiweb.obh.hu/abi/index.php?menu=aktualis/archivum/allasfoglalasok&dok=99\\_A\\_2001-2](http://abiweb.obh.hu/abi/index.php?menu=aktualis/archivum/allasfoglalasok&dok=99_A_2001-2) ;

## Rövidítések jegyzéke

<b>ABMG</b>	Autobahnmautgesetz für schwere Nutzfahrzeuge
<b>Abtv.</b>	az Alkotmánybíróságról szóló 1989. évi XXXII. törvény
<b>Obtv.</b>	az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény
<b>Alkotmány</b>	a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény
<b>Avtv.</b>	a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény
<b>Be.</b>	a büntetőeljárásról szóló 1998. évi XIX. törvény
<b>BDSG</b>	Bundesdatenschutzgesetz (német szövetségi adatvédelmi törvény)
<b>BGB</b>	Bürgerliches Gesetzbuch (német polgári törvénykönyv)
<b>Btk.</b>	a Büntető Törvénykönyvről szóló 1978. évi IV. törvény
<b>BverfG</b>	Bundesverfassungsgericht
<b>BverfGE</b>	Entscheidungssammlung des BverfG (jahr, Seite)
<b>EJEB</b>	Emberi Jogok Európai Bírósága
<b>EK</b>	Európai Közösség
<b>EKB</b>	Európai Közösségek Bírósága
<b>EU bü. tv.</b>	az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2003. évi CXX. Törvény
<b>ff.</b>	fortfolgende
<b>GG</b>	Grundgesetz (német alaptörvény)
<b>Ket.</b>	a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. Törvény
<b>Ktv.</b>	a köztisztviselők jogállásáról szóló 1992. évi XXIII. törvény
<b>Kjtv.</b>	az országgyűlési képviselők jogállásáról szóló 1990. évi LX. törvény
<b>Kütv.</b>	kutatás és közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény
<b>OECD</b>	Organisation for Economic Co-operation and Development, Gazdasági Együttműködési és Fejlesztési Szervezet
<b>Ptk.</b>	A Polgári Törvényről szóló 1959. évi IV. törvény
<b>TDDSG</b>	Teledienstschutzgesetz(a távközlési szolgáltatások adatvédelmi törvénye)
<b>TKG</b>	Telekommunikationsgesetz (német távközlési törvény)

## **Tárgymutató**

### **A**

Abel 31,  
adat 42,  
adatbiztonság 128, 142  
adatkezelő 7, 16  
adatkezelés 83, 139, 148  
-törvényessége 83  
-célhoz kötöttsége 20, 83, 127, 158, 179  
-jogalapja 20, 84, 157  
adatfeldolgozó 90  
adatfeldolgozás 80, 90, 149, 157  
adattakarékosság 103, 207  
adattovábbítás 141  
-harmadik országba 91, 162  
adatvédelem  
-európai alapjog 116  
-fogalma 33  
-fejlődése 25  
-generációi 30  
-kereset 215  
-kontroll 94,  
-i biztos 146, 164, 168, 169  
-i jogok 143,  
-i törvény Avtv., 133, 136, 137  
-i novellája 155  
-i nyilvántartás 174  
-i szerződés 296  
-i törvény felülvizsgálata 153  
alapjog  
-horizontális jellege 12, 15  
-fejlődése 72  
-védelem 165  
Alkotmány 128, 130  
Alkotmánybíróság 51, 175, 178,  
Antall-Tölgyesi paktum 130  
Amman 61  
automatizált döntés 88, 159

### **Á**

Allambiztonsági Szolgálatok Történeti  
Levéltára 49  
allamtitok 43  
átvilágítási törvény 49

### **B**

Balás P. Elemér 212  
Banisar 24,  
bejelentési kötelezettség 91  
belső adatvédelmi felelős 161  
belső piac joga 201  
belső piaci önszabályozás 274  
belső adatvédelmi szabályzat 262  
BDSG Német Szövetségi Adatvédelmi  
törvény 28  
bizonyítási teher 146,  
BGH Bundes Gerichthof Német Szövetségi  
Bíróság

BVerGE Német Szövetségi Alkotmánybíróság  
Határozatainak Tára  
BVerGG Törvény a Német Szövetségi  
Alkotmánybíróságról  
BVerG Német Szövetségi Alkotmánybíróság  
14, 29, 33, 132,

### **C**

Caroline von Hannover ügy 15, 62  
Cégtörvény Ctv  
cégjegyzék 52  
cookie 293  
credit büro 275

### **D**

Drittwirkung hatás 199  
-közvetett 13,  
-közvetlen 13,  
direkte Anwendung 108  
direkt marketing 137, 265  
domain-név 283  
drogfogyasztók adatai 235, 238

### **E**

egészségügyi személyes adat 230  
egészségügyi iratkezelés 234  
EK adatvédelmi irányelv, Irányelv 74, 76  
-célja 76  
-hatálya 78  
-jogcímei adatkezelésnek 83  
EKB Európai Közösségek Bírósága 109  
elektronikus  
-hírközlés 206, 260  
-levelezés 209, 255, 288  
-levél titok 254  
-kereskedelem 205, 285, 293  
-megfigyelőrendszer 297  
előfizetői  
-szerződés 262  
-címlista 265  
előzetes ellenőrzés 173  
ENSZ 56  
Eurodac 101  
Európai Adatvédelmi Biztos 100.  
Európai Emberi Jogi Egyezmény 104, 213  
Európai Emberi Jogi Bíróság EEJ Bíróság,  
Európai Unió Alapjogi Chartája 73,  
Európa Tanács Adatvédelmi Egyezménye 37,  
66  
Eüatv 48

### **F**

fogalmi adatok 204

### **G**

genetikai adatok 40  
GG lásd német alaptörvény 33,

### **I**

információ 42

információs  
-önrendelkezési jog 8, 9, 17, 20, 29, 33,  
35,48,51,73,117,125,132,154,164,179  
-hatalommegosztás 35, 132, 178, 199  
-törvénytervezet 126  
internet 282, 290  
-szolgáltató 284, 287  
IP cím 283, 294

## J

Jogi személyek adatvédelme 53  
Jóri András 7, 30, 38, 80, 89  
József Attila 6,

## H

Hajdú József 77,  
hely-meghatározási adat: GPRS 208  
Herbert Krüger 13,  
hesseni adatvédelmi törvény 25, 27  
horizontális jogviszony 12  
hitelinformációs rendszer 274

## K

kártérítés 145, 215  
Klass 60, 196  
KHR központi hitelinformációs rendszer 275  
Kerekasztal tárgyalások 129  
képmásvédelem 216, 217  
képarchívum 298  
kommunikációs önrendelkezési jog 19  
Konvenció lásd Európai Emberi Jogi  
Egyezmény 58  
Koppányi Szabolcs 205  
közérdekű adat 43, 147,  
közérdekből nyilvános adat 156  
közszerelő 192, 221  
közszerelés 218  
közvélemény kutatás 268  
különleges adat 84, 85, 138  
-val való visszaélés 224

## L

lakcím-nyilvántartási törvény 267  
Leander ügy 59  
Legfelsőbb Bíróság 221  
légi utasok adatai 115  
lelkiismereti szabadság 39, 187,  
levéltári törvény 147,  
Lindqvist 110  
Lüth ítélet 14,

## M

magánélethez való jog, 22, 61, 62, 65,  
-korlátozása 107  
Majtényi László 30, 67, 68, 131,133  
mikrocenzus ítélet 33,  
minősített adat 43  
megfigyelés  
-titkos 206  
-kamerás 297

29-es munkacsoport 97, 152  
munkahelyi privacy 239, 243  
Mt 240

## N

Német Alaptörvény GG  
nemzetbiztonsági ellenőrzés 189  
népszámlálási ítélet lásd: Volkszählungsurteil  
népszámlálás 118

## Ny

nyilvántartás 214  
nyilvántartási jog 118  
nyilvánosságra hozatal 219, 290

## O

OECD 55  
O.J Official Journal 10.  
Oros Paulina 67  
Orwell George, 8,  
outsourcing 252, 295

## Ö

Österreichische Rundfunk 105

## P

PET 32,  
Petrik László 126, 131, 213  
polgráfos vizsgálat 249  
pozitív adólista 278  
privacy 25  
-act 26  
-right to privacy 26

## R

Rechnungshof ügy 105  
rendőrségi adatkérés 236  
Rosnagel 31, 41, 89,

## S

Safe Harbor 93  
sajtó 229  
sajtószabadság 225,  
Schmidt, Rolf 34,  
Scholz, Philip 89  
Siemen, Birte 65, 66  
Sólyom László 9, 25, 30, 36, 129, 166, 176  
spam 289  
sport hulliganizmus 191  
Standard Contractual Causes 93  
Statisztikai  
-adatszolgáltatás 124  
-hivatal 121  
-törvény 123  
Stauder 103  
Strasbourg-i Bíróság, lásd EEJ Bíróság 62

## Sz

szektorális adatvédelem 31, 48, 125, 137, 152

személyes adat 36, 41, 158  
-amszterdami szerződésben 99  
-büntető jogi védelme 223  
-feldolgozása (EK Irányelv szerint) 80,  
-nyilvánosságra hozatala 251,  
-reindividualizálása 45  
-védelme 125  
személyiségi jog 125,  
személyiség profil 181, 259  
személyi szám 175  
szféra elmélet 85.  
Szladits 211

## **T**

tájékoztatási kötelezettség 207, 261  
távközlés 202  
telekommunikációs irányelv 202  
telemarketing 272  
tilalmi lista 271  
tiltakozási jog 87  
tisztesség követelménye 83,  
Tinnefeld 40, 260  
titok 43, 212  
titoktörvény 43, 147, 151  
titkos megfigyelés 65, 264  
titkos nyomozati eszközök 193  
TKG Telekommunikationsgesetz 50  
tudományos célú adatkezelés 237, 268

## **Ü**

ügyvédi titok 44, 248  
üzleti titok védelme 249

## **V**

vagyon-nyilatkozat 183, 252  
vagyonvédelem 257  
vélemény-nyilvánítási szabadság 283  
Volkszahlurteile 29, 33

## **Z**

Zlinszky 211

## **W**

Warren/Brandeis 21, 211  
webáruház 293  
webkamera 258  
webpoloska 207  
Westin, Alan F 22,  
Wiener, Norbert 26