

Az alapjogok szerkezetének megszilárdítása az EU-ban II  
Adatvédelem az Európai Unióban: a nemzeti adatvédelmi hatóságok szerepe

Ez a jelentés a személyes adatoknak az Európai Unió Alapjogi Chartája 8. cikkében körülírt védelmére vonatkozik.

Jogi nyilatkozat: Az FRA „Az alapjogok szerkezetének megszilárdítása az EU-ban II, Adatvédelem az Európai Unióban: a nemzeti adatvédelmi hatóságok szerepe” című jelentése magyar nyelvű fordításának közzététele a magyar Adatvédelmi Biztos önálló kezdeményezése. Az FRA nem volt abban a helyzetben, hogy a fordítás helyességét ellenőrizze. Ha az olvasónak kétségei támadnak, tanácsos az eredeti angol nyelvű változatot megtekintenie, amely a <http://www.fra.europa.eu> Internet oldalon megtalálható.

Disclaimer: This translation into Hungarian of the FRA report "Strengthening the fundamental rights architecture in the EU II, Data Protection in the European Union: the role of National Data Protection Authorities" was published by the Hungarian Data Protection Commissioner at own initiative. The FRA was not in a position to check the accuracy of the translation. Readers are advised to refer to the original English language version available on <http://www.fra.europa.eu> if in doubt.

Előszó .....	4
Vezetői összefoglaló .....	5
Az EU az adatvédelem mint alapjog területén globálisan úttörő szerepet játszik .....	5
Az EU adatvédelmi rendszerében jelentkező kihívások .....	5
Helyes gyakorlatok .....	6
Vélemények .....	7
Az EU-nak szélesítenie kell adatvédelmi rendszerét .....	7
A hatékony kikényszerítés biztosítása .....	7
A nemzeti adatvédelmi hatóságok mint független őrzők .....	7
A nemzeti adatvédelmi hatóságok mint az EU fejlődő alapjogi szerkezetének részei .....	8
Nemzeti adatvédelmi hatóságok mint hatékony mindent-egy-helyen üzletek .....	8
Jogtudatosság .....	8
1. Bevezetés .....	9
2. Az adatvédelem alapjogi normái .....	9
2.1 Adatvédelem az Egyesült Nemzetek keretében .....	9
2.2 Adatvédelem az Európa Tanács keretében .....	11
3. Adatvédelem az EU jogban .....	14
3.1 Adatvédelem a Közösség korábbi pillérjében .....	15
3.2 Adatvédelem az EU korábbi, második és harmadik pillérjében .....	18
3.3 A Lisszaboni Szerződés .....	22
4. Összehasonlító áttekintés .....	23
4.1 Adatvédelmi hatóságok .....	23
4.1.1 Függetlenség .....	23
4.1.2 Anyagi források .....	25
4.1.3 Hatáskör .....	25
4.1.3.1 Vizsgálati jogkör .....	26
4.1.3.2 Beavatkozási jogkör .....	28
4.1.3.3 Jogkörök kérelmek fogadására és bírósági eljárásokban való részvételre .....	30
4.1.3.4 Konzultációs jogkörök .....	32
4.1.4 Tevékenységek .....	34
4.2 Megfelelőség .....	35
4.2.1 Az adatvédelmi nyilvántartás és a nyilvántartásba vételi eljárás .....	35
4.2.2 Belső adatvédelmi felelős kinevezése .....	39
4.3 Szankciók, kártérítés, jogi következmények .....	40
4.3.1 Jogorvoslat .....	40
4.3.2 Szankciók .....	42
4.3.3 Kártérítés .....	44
4.3.4 A munkaviszonyra vonatkozó sajátos adatvédelmi jogszabályok .....	46
4.4 Jogtudatosság .....	47
5. A hiányosságok elemzése .....	54
5.1 Az adatvédelmi jogszabályok hiányosságai .....	54
5.1.1 Az adatvédelmi hatóságok .....	54
5.1.2 Megfelelőség .....	55
5.1.3 Szankciók, kártérítés, jogkövetkezmények .....	56
5.1.4 Jogtudatosság .....	57
5.2 Az adatvédelem problematikus területei .....	57
5.2.1 Adatvédelem a nemzetbiztonság területén .....	58
5.2.2 Az egyén egészségi állapotára vonatkozó adatok védelme .....	58
5.2.3 A kamerás megfigyelés adatvédelmi kérdései .....	59

6. Helyes gyakorlatok.....	61
6.1 Adatvédelmi hatóságok.....	61
6.2 Megfelelőség.....	62
6.3 Jogtudatosság.....	63
7. Következtetések.....	65

## **Előszó**

Az alapjogok szerkezete az Európai Unióban már hosszabb ideje kialakult, fejlődése folyamatos. Ez a jelentés az Európai Unió Alapjogi Ügynöksége (a továbbiakban: FRA) négy jelentésének egyike. Három, szorosan összefüggő kérdéssel foglalkozik, továbbá azokkal az intézményekkel, amelyek az Európai Unió alapjogi „tartóoszlopai”, nevezetesen az egyenlő bánásmód szervei, az adatvédelmi hatóságok és a nemzeti emberjogi intézmények.

Az FRA számára felettebb jelentős e felügyeleti szervek mindhárom, nemzeti szintű csoportja. A FRA ugyanis kifejezetten arra hivatott, hogy együttműködjék például a tagállamok alapjogi kérdésekben kompetens kormányzati és egyéb állami szerveivel, ide értve az adatvédelmi hatóságokat, abból a célból, hogy tökéletesítse az együttműködést nemzeti és EU szinten egyaránt. Szükség van ugyanis – különösen nemzeti szinten – az alapjogok mind hatékonyabb védelmére és támogatására az európai és nemzetközi mechanizmusokkal történő együttműködésben, amely az Európai Unióban az alapjogi szerkezet elengedhetetlen eleme.

Ez az adatvédelmi hatóságokról szóló jelentés elemzi kiemelkedő szerepüket az adatvédelem mint alapvető jog területén, továbbá értékeli hatékonyságukat, működésüket és függetlenségüket. A jelentés azért is időszerű, mert az adatvédelemhez való jog az EU-ban elkülönült alapjoggá vált (lásd Alapjogi Charta, 8. cikk), s így összefügg a magán- és a családi élet tiszteletben tartásához fűződő joggal, jóllehet attól el is különül. Az adatvédelem egyúttal az EU kulcsfontosságú vezérelvévé és az EU több tagállama jogrendszere fejlődésének hajtóerejévé is válik.

Viviane Reding, a jogérvényesülés, alapvető jogok és uniós polgárság Biztosa a közelmúltban az Európai Parlamenthez intézett írásbeli nyilatkozatában hangsúlyozta, hogy az adatvédelem különös jelentőségű az EU számára. „Szilárd meggyőződésem – mondotta –, hogy a polgárok nem bíznak Európában, ha nem gondoskodunk folyamatosan a személyes adatok illetéktelen felhasználásával szembeni védelméről, s arról, hogy a polgároknak joguk legyen dönteni adataik feldolgozásáról.” A FRA e szellemet követve teszi közzé e jelentését.

Morten Kjaerum  
igazgató

## **Vezetői összefoglaló**

### **Az EU az adatvédelem mint alapjog területén globálisan úttörő szerepet játszik**

Az EU történelmi kulcsszerepet játszott a nemzeti adatvédelmi törvények kialakításában és számos olyan jogrendszerébe való bevezetésében, melynek korábban nem volt ilyen jogszabálya. E tekintetben fontos eszköz volt a 95/46/EK irányelv (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról („adatvédelmi irányelv”).

Az EU Alapjogi Chartája – amely az Európai Unióról szóló Szerződés új, 6. cikke értelmében „ugyanolyan jogi kötőerővel bír, mint a Szerződések” – az adatvédelemről mint alapjogról a 8. cikkben rendelkezik, amely különbözik a 7. cikkben megfogalmazott magán- és családi élet tiszteletben tartásától. E tekintetben az EU Alapjogi Chartája<sup>1</sup> eltér más emberi jogi dokumentumoktól, amelyek a személyes adatok védelmét többnyire a magánszférához fűződő jog kiterjesztéseként értelmezik.

Az adatvédelem autonóm alapjogként való értelmezésével az EU elismeri a műszaki fejlődés jelentőségét, és e fejlődést az alapjogok területén igyekszik figyelembe venni. Az a kétségtelen tény, hogy életünket egyre inkább folyamatos információcsere jellemzi, és hogy folyamatos adatáramlásban élünk, azt jelenti, hogy az adatvédelem jelentősége növekszik, és a politikai és intézményi rendszer középpontja felé halad. Ezt a fejlődést világosan felismerhetjük, ha összevetjük az EU Chartát az Európa Tanács 1950. évi Európai Emberi Jogi Egyezményével (ECHR). Az ECHR 8. cikke értelmében „mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák”. Az ECHR nem tartalmaz explicit és autonóm jogot az adatvédelemre. Az adatvédelem jobbra a strasbourgi Európai Emberi Jogi Bíróság döntéseiben jelenik meg mint a magánélet védelmének egyik tényezője. Ezzel összevetve az EU Alapjogi Chartája a 8. cikkben elismeri azt a központi szerepet és jelentőséget, amelyre az adatvédelemhez fűződő jog társadalmunkban a műszaki fejlődés következtében szert tett.

Ez a tanulmány a kihívások és helyes gyakorlatok összehasonlító elemzését nyújtja az EU adatvédelmi rendszerében.

### **Az EU adatvédelmi rendszerében jelentkező kihívások**

Az EU Alapjogi Ügynöksége a következő kihívásokat azonosította az EU adatvédelmi rendszerében:

Az adatvédelmi hatóságok hiányosságai:

A legfőbb szerkezeti probléma több adatvédelmi hatóság (AVH) esetében a függetlenség hiánya. Számos tagállamban aggályos az adatvédelmi hatóságok munkájának teljes autonómiája, ami viszont hatékonyságuk és eredményességük kulcsa. A funkcionalitás szintjén számos adatvédelmi hatóság esetében az alacsony létszám és a kellő pénzforrások hiánya a legfőbb probléma. Az operativitás szintjén a legfőbb probléma számos adatvédelmi hatóság korlátozott hatásköre. Egyes tagállamokban nincs teljes hatáskörük a vizsgálatra, a feldolgozási folyamat elemzésére, jogi tanácsadásra és jogi eljárásokra.

Az adatvédelmi szabályok kikényszerítésének hiányosságai:

Néhány tagállamban az adatvédelmi törvény megsértésének szankcionálása vagy megsértése esetén a bünvádi eljárás kezdeményezése korlátozott vagy nem lehetséges. Egyes tagállamok jogrendszere kifejezetten elutasítja azt a lehetőséget, hogy az adatvédelmi jogok megsértése esetén az érintett kártérítésért folyamodjon. Ennek oka több tényező kombinációja lehet, mint például a bizonyítási teher, a kár bonyolult számszerűsítése és a felügyeleti szervek támogatásának hiánya, melyek elsősorban olyan „puha” ösztönző tevékenységgel vannak

elfoglalva, mint a nyilvántartásba vétel és a tudatosság fokozása. A tagállamokban észlelhető általános tendencia: inkább az adatvédelmi jogszabályokkal való összhang megteremtésének „puha” módszereire koncentrálnak, ahelyett hogy „kemény” eszközöket alkalmaznának és kényszerítenének ki, melyekkel az adatvédelmi jogok megsértőit azonosíthatnák, büntethetnék és az áldozatoknak okozott kár megtérítésére indíthatnák. E téren egyes tagállamokban az adatvédelmi hatóságok és más hatóságok együttműködésére is akad példa, melyek célja a helyes gyakorlat kialakításával a vizsgálatok szigorítása.

**Jogtudatosság:**

E jelentés készítése folyamán végzett kutatás során a FRA úgy találta, hogy a 27 EU tagállam közül 12-ben végeztek országos közvélemény-kutatást az adatvédelmet illetően. A közvélemény-kutatások némelyikét a nemzeti adatvédelmi hatóságok végezték. A feltett kérdések, a válaszadók száma, a közvélemény-kutatás módszere és végeredménye változatos, és nem mindig teszi lehetővé az összehasonlításukat. Mindazonáltal ezek az országos közvélemény-kutatások önmagukban véve helyes gyakorlatot igazolnak. Az Eurobarometer 2008 februárjában két adatvédelmi tárgyú közvélemény-kutatást tett közzé, melyek legfontosabb megállapítása, hogy az EU polgárok többsége aggódik az adatvédelemmel kapcsolatban, s legtöbbjüknek viszonylag ismeretlenek a nemzeti adatvédelmi hatóságok.

Az adatvédelem hiánya az EU korábbi harmadik pillérjében:

A hatékony és átfogó adatvédelem megteremtése terén az EU jelenleg azzal a hiányossággal kénytelen szembenézni, amely a korábbi EU pillérek alkotmányos rendszeréből adódik. Míg az adatvédelem magas fokú fejlettséget mutat az EU korábbi, első pillérjében, a korábbi harmadik pillér adatvédelmi rendszerét nem tekinthetjük kielégítőnek. Az EU korábbi, harmadik pillérje mindazonáltal felölel olyan területeket, mint a rendőrségi együttműködés, a terrorizmus elleni harc és a büntetőjog kérdései, ahol az adatvédelem különösen fontos és szükséges. A Lisszaboni Szerződés megkönnyíti e hiányosság kiküszöbölését. A Lisszaboni Szerződéshez csatolt 21. számú Nyilatkozat szerint a bűnügyi kérdésekben folyó bírósági együttműködés, továbbá a rendőrségi együttműködés terén a személyes adatok kezelésére és ilyen adatoknak a szabad továbbítására vonatkozó különös szabályok e területek „különleges sajátosságaira” való tekintettel szükségesnek mutatkozhatnak.

Adatvédelem alóli kivételek biztonsági és védelmi célból:

Az adatvédelmi irányelv 13. cikk (1) bekezdése jelentős kivételeket és korlátozásokat állapít meg a közbiztonságra, a védelemre, az állambiztonságra vonatkozóan (ide értve az állam gazdasági jólétét, ha a feldolgozási művelet az állam biztonságával kapcsolatos), továbbá az államnak a büntető jog területén végzett tevékenységével összefüggésben. E kivételek és korlátozások terjedelme azonban nem világos. Több tagállamban e területek teljesen ki vannak zárva az adatvédelmi törvényből meglehetősen nagy területet védelem nélkül hagyva, melynek komoly következményei lehetnek az alapjogok védelmét illetően. A Lisszaboni Szerződéshez csatolt 20. számú Nyilatkozat szerint, amikor a nemzetvédelmet közvetlenül érintő személyes adatokat védő szabályokat fogadnak el „megfelelő figyelmet” kell fordítani a tárgy különös jellemzőire.

A technika kihívása:

A közelmúlt és a folyamatban lévő technikai fejlesztések kihívásaira sürgősen választ kell adni. A kamerás megfigyelés mind közterületen, mind a munkavégzés környezetében széleskörű, ám a jogszabályi keretek ezt nem követik. A jelentés példaként megemlíti, hogy egyes tagállamokban a gyakorlatban a zártláncú televíziós (CCTV) kamerákat gyakran nem veszik nyilvántartásba vagy nem követik nyomon.

### **Helyes gyakorlatok**

Az EU Alapjogi Ügynöksége által ismert, a hatékony adatvédelmet elősegítő helyes gyakorlatok többsége egyes tagállamok adatvédelmi hatóságainak a tudatosság fokozására

irányuló tevékenysége, melynek során tanfolyamokat, szemináriumokat és előadásokat szerveznek, útmutatásokat és javaslatokat tesznek közzé, vagy tájékoztató és tanácsadó kampányokat rendeznek. Más helyes gyakorlatok a felügyeleti szervek intézményi helyzetével kapcsolatosak, nevezetesen függetlenségük mértékével, az adatvédelmi jogszabályok kikényszerítésével, magatartási szabályok készítésében való aktív közreműködéssel és ilyen szabályok kibocsátásával, továbbá nemzeti intézményekkel, civil szervezetekkel és más tagországok adatvédelmi hatóságaival való együttműködéssel.

## **Vélemények**

Az Európai Unió Alapjogi Ügynöksége a jelentésben részletezett megállapításokra és összehasonlító elemzésre alapozva a következő véleményeket fogalmazta meg:

### **Az EU-nak szélesítenie kell adatvédelmi rendszerét**

A Lisszaboni Szerződés, felszámolva az EU pillérstruktúráját, lehetőséget nyújt az EU – jelenleg csak a korábbi első pillérben – megjelenő adatvédelmi rendszerének szélesítésére az EU minden (korábbi) pillérében. Az adatvédelem korlátozása biztonsági, védelmi vagy egyéb törvényes célból az EU Alapjogi Chartájának 52. cikke értelmében lehetséges marad, de ezeket a korlátozásokat jogszabálynak kell elrendelnie, tiszteletben tartva a személyes adatok védelméhez fűződő jog lényegét és a szükségesség és arányosság követelményeit. Egyes területek teljes és maradéktalan kizárása az adatvédelmi jogszabályok hatályából alapjogi szempontból problematikus és kerülendő.

### **A hatékony kikényszerítés biztosítása**

Ez a jelentés rávilágít arra, hogy számos adatvédelmi hatóság esetében az alacsony létszám és a kellő pénzforrások hiánya okoz problémát. Az operativitás szintjén a legfőbb probléma számos AVH korlátozott hatásköre. Egyes tagállamokban nincs teljes hatásköre a vizsgálatra, a beavatkozásra, jogi tanácsadásra és jogi eljárásokra. Az AVH-knak rendelkezniük kell a szükséges erőforrásokkal, hatáskörrel és függetlenséggel ahhoz, hogy hozzájárulhassanak az adatvédelmi rendszer hatékony kikényszerítéséhez.

Az adatvédelem hatékony kikényszerítésének garanciái és a jogsértők felfedése és kivizsgálása az adatvédelmi jogsértésektől való elrettentés és megelőzésük elérésének elengedhetetlen eszköze. Ha jóval nagyobb hangsúlyt kapna a jogalkalmazás kikényszerítése, azzal egyúttal elősegítenénk a lakosság meggyőzését arról, hogy az adatvédelmi kérdéseket komolyan kell venni. Ha kizárólag a „puha” eszközökre koncentrálnánk, anélkül hogy „kemény” eszközökhöz folyamodnánk, aláássuk az egész rendszer hitelét. Ebben az értelemben a hatékony kikényszerítés hozzájárul a lakosság fokozott jogtudatosságához. Az adatvédelmi hatóságoknak az adatvédelmi rendszer kikényszerítése terén jelentős lenne a szerepe, vagy azáltal, hogy kifejezett felhatalmazásuk van a szankcionálásra, vagy azáltal, hogy szankciókat eredményező eljárásokat kezdeményeznek *ex officio*. Ez erősítené tekintélyüket és hitelüket.

### **A nemzeti adatvédelmi hatóságok mint független őrzők**

A struktúra szintjén több adatvédelmi hatóság függetlenségének hiánya a legfőbb probléma. Több országban mindemellett normatív és gyakorlati akadályok is aggodalomra adnak okot a nemzeti AVH-k tényleges, a kormány politikai ágazatától való függetlenségét illetően. A függetlenség garanciáját valójában mindenképp az AVH-k tisztségviselőinek kinevezésére és felmentésére szolgáló eljárás képezi. A pénzforrások feletti rendelkezés a felügyeleti hatóságok autonómiája biztosításának másik lényeges eleme.

Egyes tagállamokban az adatvédelmi tisztségviselőket, a parlamenti ellenzék bevonása nélkül, közvetlenül a Kormány nevezi ki, ami számos esetben felettébb kérdésessé teszi az adatvédelmi hatóság tényleges függetlenségét. Hasonló aggodalom merülhet fel azokban az országokban, ahol a felügyeleti hatóság az Igazságügyi Minisztériumhoz van csatolva. Végül más tagállamokban vegyes eljárást követnek a nemzeti adatvédelmi hatóság tisztségviselői kinevezése során, amelybe bevonják a végrehajtó, a jogalkotó és bírósági szerveket, vagy egyúttal egyéb szervezett társadalmi csoportokat is. Egyes esetekben azonban feltétlenül gondoskodni kell arról, hogy a Kormány valóban sem közvetlenül, sem közvetve ne vezérelje a jelöltek többségének kiválasztását, így ténylegesen lerontva a pluralisztikus jelölési eljárás célját.

A 95/46/EK adatvédelmi irányelv követelménye szerint az adatvédelmi hatóságok „a rájuk ruházott feladatok gyakorlása során teljes függetlenségben járnak el” [adatvédelmi irányelv, 28. cikk (1) bek.]. E ’függetlenség’ jellemzői azonban nincsenek kidolgozva. Ajánlatos lenne az irányelvben részletesen meghatározni a függetlenség garanciáit az adatvédelmi hatóságok tényleges függetlenségének gyakorlati biztosítására. Tanácsos tehát – jövőbeni revíziója során – az irányelvbe foglalni az úgynevezett „Párizsi Alapelvekre” való hivatkozást annak érdekében, hogy a függetlenség meghatározása átfogóbbá váljék.

### **A nemzeti adatvédelmi hatóságok mint az EU fejlődő alapjogi szerkezetének részei**

Az adatvédelmi hatóságoknak az EU fejlődő alapjogi szerkezete keretében elő kell segíteniük a szorosabb együttműködést és összhangot az alapjogok más őrzőivel (mint pl. a nemzeti emberjogi és egyenlő bánásmód szervezeteivel). Az EU egyik lehetősége, mellyel élve hozzájárulhat a szorosabb együttműködéshez és összhanghoz, hogy újabb kitételrel egészítse ki az adatvédelmi irányelv 28. cikkét, lehetővé téve a tagállamoknak olyan jogszabály megalkotását, melynek révén adatvédelmi hatóságuk ténylegesen nemzeti emberjogi intézményeinek szakosított egységét képezik (hasonló hatást kiváltó érdekes példa a 2000/43/EK Tanácsi Irányelv 13. cikke).

### **Nemzeti adatvédelmi hatóságok mint hatékony mindent-egy-helyen üzletek**

Az adatvédelmi hatóságok a hatékony adatvédelem kulcsszereplői, a polgárok és más személyek hatékony adatvédelmének alacsony küszöbű hozzáférési pontjaként szolgálnak. Nem csupán a korábbi első pillér részét képező kérdésekkel kell foglalkozniuk, mint ahogyan azt jelenleg néhány tagállamban teszik, hanem úgy kell kijelölni kereteiket, hogy mindent-egy-helyen üzletként működjenek a polgárok és más személyek valamennyi adatvédelmi ügyében, ide értve azokat a területeket is, amelyek korábban az EU harmadik pillérje részét képezték. Az adatvédelmi szervezetek és hatóságok szaporodása nem segíti elő létezésük tudatosulását a polgárokban. A szervezetek sokasága ugyanakkor zavaró és szükségtelenül bonyolult lehet.

### **Jogtudatosság**

Az Eurobarometer 2008 februárjában két adatvédelmi tárgyú közvélemény-kutatást tett közzé. E közvélemény-kutatások legfontosabb megállapítása, hogy az EU polgárok többsége aggódik az adatvédelemmel kapcsolatban, s legtöbbszörüknek viszonylag ismeretlenek voltak a nemzeti adatvédelmi hatóságok. Ajánlatos tehát, hogy az adatvédelmi hatóságok mint az adatvédelmi alapjog őrzői különös figyelmet szenteljenek a közvélemény előtt megjelenő arculatuk ápolására, és súlyt helyezzenek létük és szerepük tudatosulásának fokozására.



## 1. Bevezetés

Az EU Alapjogi Chartája az adatvédelemről mint alapjogról a 8. cikkében rendelkezik. Az adatvédelem tehát azoknak a kulcsfontosságú alapjogi területeknek az egyike, melyre nézve az EU-nak a jogalkotásra hatásköre van.

Ezt a jelentést az Ügynökség a FRALEX, az Ügynökség jogi szakértői csoportja közreműködésével készítette. A FRALEX nemzeti csoportjai az Ügynökség közös iránymutatásai alapján 27 országtanulmányt és egy EU/nemzetközi tanulmányt készítettek. Ez az összehasonlító jelentés e tanulmányokra épülve készült. Az országjelentések 2009 februárjában készültek el. Az összehasonlító tanulmány tervezetéről a „29-es Munkacsoport” véleményét is kértük, amely megjegyzéseket fűzött hozzá.

Ez a jelentés szorosan kapcsolódik az Európai Unió következő projektjeihez és publikációihoz:

vélemény a légiutasok adatainak nyilvántartásáról, 2008<sup>1</sup>

az Ügynökség hozzászólása az Európai Bizottság test-szkennerekkel kapcsolatos konzultációjához, 2009<sup>2</sup>

jelentés az Európai Unió tagállamai Nemzeti Emberjogi Intézményeiről – Az alapjogok szerkezetének megszilárdítása I. 2010<sup>3</sup>

EU-MIDIS Adatok a Középpontban III: Jogtudatosság és Egyenlő Bánásmód Szervek, 2010<sup>4</sup>

Ez a jelentés elsőként bemutatja az adatvédelemre vonatkozó nemzetközi jogi normákat, majd elemzi az EU adatvédelmi jogát és a Lisszaboni Szerződés hozta változásokat. Ezt követi a tagállamok adatvédelmi intézményeinek és gyakorlatának összehasonlító áttekintése. A jelentés a hiányosságok és a helyes gyakorlatok megállapításával zárul.

## 2. Az adatvédelem alapjogi normái

A személyes adatok védelmét alapjogként ismeri el több európai és nemzetközi szerződés, jogtudományi értelmezése megtalálható a nemzetközi és regionális bíróságok gyakorlatában.

### 2.1 Adatvédelem az Egyesült Nemzetek keretében

A személyes adatok védelmét, jobbra mint a magánélet védelméhez fűződő jog kiterjesztését egyetemes szinten több, az Egyesült Nemzetek égisze alatt elfogadott emberjogi eszköz is alapjogként ismeri el.<sup>5</sup>

Nevezetesen a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (PPJNE)<sup>II</sup>, melyet a világ államainak négyötöde ratifikált, a 17. cikkében védelemben részesíti a magánülethez, a családhoz, a lakáshoz és a levelezéshez fűződő jogokat, és pedig a következőképpen: „1. Senkit sem lehet alávetni a magánéletével, családjával, lakásával vagy levelezésével kapcsolatban önkényes vagy törvénytelen beavatkozásnak, sem pedig a becsülete és jó hírneve elleni jogtalan támadásnak. 2. Ilyen beavatkozás vagy támadás ellen mindenkinek joga van a törvény védelmére.” A PPJNE-hez fűzött 16. számú Általános Kommentár<sup>III</sup>

---

<sup>1</sup> Lásd [http://fra.europa.eu/fraWebsite/attachments/FRA\\_opinion\\_PNR\\_en.pdf](http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf) (hozzáférés: 2010.01.21).

<sup>2</sup> Az EU Alapjogi Ügynökségének nem publikált hozzászólása az Európai Bizottság egy konzultációjához

<sup>3</sup> Lásd <http://fra.europa.eu/> (2010.02.24.).

<sup>4</sup> Lásd <http://fra.europa.eu/eu-midis> (2010.02.24.).

<sup>5</sup> Az Emberi Jogok Egyetemes Nyilatkozatának 12. cikke védi a magánülethez fűződő jogot

kifejezetten hivatkozik a személyes adatok védelméhez fűződő jogra<sup>6</sup>. Eszerint „személyes információ gyűjtéséről és tárolásáról számítógépeken, adatbankokban vagy egyéb eszközökön, végezzék azt közhatalmi szervek vagy magánszemélyek, jogszabálynak kell rendelkeznie. Az államoknak hatékony intézkedéseket kell tenniük annak érdekében, hogy egy személy magánéletével kapcsolatos információ ne kerüljön olyan személyek kezébe, akik jogszabály alapján nincsenek felhatalmazva annak átvételére, feldolgozására és felhasználására, továbbá hogy azt soha ne használják fel az Egyezségokmánnyal összeegyeztethetetlen célra. Magánélete leghatékonyabb védelmének céljából mindenkinek joga van arra, hogy érthető formában tudomást szerezzen arról, tárolják-e, s ha igen, mely személyes adatait tárolják automatikus adatállományokban és milyen célból. Mindenkinek joga van továbbá arra, hogy tudomást szerezzen azokról a közhatalmi hatóságokról vagy magánszemélyekről és -szervezetekről, amelyek adatállományait kezelik vagy kezelhetik. Ha ilyen állományok pontatlan személyes adatokat tartalmaznak, vagy azokat a törvényes rendelkezések ellenére gyűjtötték vagy dolgozták fel, úgy mindenkinek joga, hogy helyesbítésüket vagy megsemmisítésüket kérje”. Az Emberi Jogi Bizottság esetjoga továbbá hangsúlyozza, hogy a 16. számú Általános Kommentár magánéletre vonatkozó fogalmát nem szabad szűken értelmezni.<sup>7</sup>

Ugyancsak nagy jelentőségű dokumentum az Egyesült Nemzetek Iránymutatása a számítógépesített személyes adatfájlok szabályozására, melyet a Közgyűlés 1990. december 14-i határozatával fogadott el<sup>8</sup> Az Iránymutatás<sup>IV</sup> rögzíti azokat az alapelveket, melyeknek mint minimális garanciáknak az érvényesüléséről a nemzeti adatvédelmi jogalkotásnak kell gondoskodnia. Ezek az elvek: a személyes adatok törvényes és tisztességes gyűjtése és feldolgozása, pontossága, célhoz kötöttsége, az érintett hozzáférése, az adatállományok megkülönböztetéstől való mentessége és biztonsága. Az alapelvektől való eltérésre „csak akkor adható felhatalmazás, ha az a nemzetbiztonság, közrend, közegészség vagy erkölcs, továbbá, többek között, mások jogainak és szabadságainak védelme érdekében szükséges, különösen egyes személyek zaklatása esetében (humanitárius záradék), feltéve, hogy ezekről az eltérésekről törvény vagy azzal egyenértékű jogszabály rendelkezik, melyet a belső jogrenddel összhangban hirdettek ki, kifejezetten megállapítva korlátait és gondoskodva megfelelő garanciákról is”. A megkülönböztetéstől való mentességre adható kivétel még ennél is jobban korlátozva van, és „arra felhatalmazás csak a Nemzetközi Emberi Jogi Kódexben<sup>V</sup> és egyéb releváns, az emberi jogok védelmét és a megkülönböztetés megelőzését szolgáló dokumentumokban rögzített korlátozásokkal adható. Az Iránymutatás szerint az általa védett alapelveket „mindenekelőtt valamennyi nyilvános és magántermészetű számítógépesített adatállományra, továbbá, alkalmas védintézkedésekkel és megfelelő kiigazítással, a manuális állományokra is alkalmazni kell. Különös, ugyancsak opcionális intézkedésekkel az alapelvek összessége vagy némelyike kiterjeszhető a jogi személyekre is, főleg akkor, ha egyénekre vonatkozó információt kezelnek.

---

<sup>6</sup> Lásd Emberi Jogi Bizottság, 16. számú Általános Kommentár. (Huszonharmadik ülés, 1988), az Emberi Jogok Szerződése Testületei által elfogadott Általános Kommentárok és Általános Ajánlások Gyűjteménye (U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), 10. bek.)

<sup>7</sup> Lásd pl. a Coeriel & Aurik kontra Hollandia jogeset (1994) Comm 453/1991.

<sup>8</sup> Iránymutatás a számítógépesített személyes adatfájlok szabályozására (a Közgyűlés 1990. december 14-i 45/95 határozata)

A személyes adatok védelmét mint alapjogot Európán kívül, regionális szinten különféle regionális emberi jogi eszközök is elismerik, többnyire mint a magánélethez fűződő jog kiterjesztését.<sup>9</sup>

## 2.2 Adatvédelem az Európa Tanács keretében

Regionális szinten a személyes adatok védelmét több, az Európa Tanács égisze alatt elfogadott egyezmény tartalmazza. Ezek többségét az EU valamennyi tagállama ratifikálta, néhány esetben belső jogrendszerükben az mint legfelső alkotmányos norma jelenik meg.

Az Európa Tanács legfontosabb jogi dokumentuma az Európai Emberi Jogi Egyezmény (ECHR) – melyet minden EU tagállam ratifikált – nem említi kifejezetten a személyes adatok védelmét, az Európai Emberi Jogi Bíróság (ECtHR) kiterjedt esetjoga azonban arról tanúskodik, hogy az adatvédelem jogát az ECHR 8. cikke feleleli, mert kifejezetten elismeri a magán- és a családi élet tiszteletben tartását, éspedig a következőképpen: „1. Mindenkinnek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy 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.”

Az Európa Tanács keretében továbbá az Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (a „108. Egyezmény”)<sup>10</sup> kifejezetten elismeri a személyes adatok védelmének alapjogát. Az Egyezmény – melyet az EU minden tagállama ratifikált – kötelezi a szerződő államokat, hogy területükön minden egyén számára, tekintet nélkül nemzetiségére vagy lakóhelyére biztosítsa, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák a személyes adatainak gépi feldolgozása során (‘adatvédelem’). Az Egyezmény a személyes adatok automatizált állományaira és a személyes adatok gépi feldolgozására vonatkozik a köz- és a magánszektorban egyaránt. Rögzíti az adatfeldolgozás alapelveit, valamint az adatok minőségére vonatkozó követelményeket, nevezetesen: az adatok tárolásuk céljával arányban állnak és megfelelnek e célnak, azon nem terjeszkednek túl (az arányosság elve); pontosak, a különleges adatok kezelése bizalmas, az adatalany tájékoztatása, jog a hozzáférésre és helyesbítésre. Az Egyezmény azonban általában meglehetősen homályos és átfogó megfogalmazásokat tartalmaz, és közvetlen alkalmazása nem szükségszerű, a Szerződő Államokra bízva az érvényesítéshez szükséges intézkedések megtételét, melynek következtében az egyén a bíróság előtt azt nem idézheti fel. Ezen túlmenően az Egyezmény széles körű kivételeket állapít meg, ide értve az államoknak azt a lehetőségét, hogy eltérjenek az adatvédelmi szabályoktól, ha arról a Felek belső joga rendelkezik és egy demokratikus társadalomban szükséges.

A 108. egyezmény egy Tanácsadó Bizottságot hoz létre, amely az Egyezményhez csatlakozott Felek képviselőiből áll, kiegészítve más (ET tag vagy nem tag) államok és nemzetközi szervezetek megfigyelőivel. A Bizottság hivatott az Egyezmény rendelkezései értelmezésére és alkalmazása fejlesztésére. A Bizottság elfogadott egy, az Egyezményt Kiegészítő Jegyzőkönyvet (melyet még nem minden EU tagállam ratifikált) a Felügyelő Hatóságokról és

---

<sup>9</sup> A magánélethez fűződő jogot az Emberi Jogok és Kötelezettségek Amerikai Nyilatkozata (1948) V. cikke és az Emberi Jogok Amerikai Egyezménye (1969) is tartalmazza. Az Emberi Jogok és a Népek Jogai Afrikai Chartája (1981) a magánélethez fűződő jog kifejezett elismerését nem tartalmazza.

<sup>10</sup> Lásd 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

a Határon Átnyúló Adatáramlásról (2001), megerősítve a Felügyelő Hatóságokat és megtiltva a személyes adatok továbbítását azokba az államokba, ahol megfelelő szintű védelemről nem gondoskodnak.

Az Európa Tanács másik fontos jogeszköze az Emberi Jogokról és a Biomedicináról szóló Egyezmény (1997)<sup>11</sup> (melyet az EU nem minden tagállama ratifikált). Az Egyezmény 10. cikke megerősíti az ECHR 8. cikkében védett és a 108. Egyezményben megismételt alapelveket, rögzítve, hogy: „1. Minden személynek joga van arra, hogy magánéletét tiszteletben tartsák az egészségével kapcsolatos adataival összefüggésben. 2. Minden személynek joga van ismerni az egészségével kapcsolatosan összegyűjtött minden adatot. Ugyanakkor tiszteletben kell tartani annak a személynek az akaratát is, aki a tájékoztatása mellőzését kívánja. 3. Kivételes esetben, a beteg érdekében a törvény korlátozhatja a 2. bekezdésben meghatározott jogok gyakorlását”. Az Emberi Jogokról és a Biomedicináról szóló Egyezmény alkalmazásában továbbá az egészségre vonatkozó személyes adatok a 108. Egyezmény szerint különleges adatfajtának minősülnek, s mint ilyenekre különös szabályok vonatkoznak. Az Egyezmény mindazonáltal megengedi a magánélethez fűződő jog bizonyos korlátozását, ha egy bíróságnak egy bűncselekmény előkészítőjét kell azonosítani (a bűnmegelőzésre alapozott kivétel), apaságot vagy anyaságot kell megállapítani (mások jogainak védelmére alapozott kivétel).

Végül megemlítendő, hogy az Európa Tanács javaslatokkal és határozatokkal is segíti az egyén személyes adatai védelmére vonatkozó alapelvek további kidolgozását. Ezek a Miniszteri Bizottság által egyhangúan elfogadott eszközök ugyan jogilag nem kötelezőek, hivatkozási alapul szolgálnak minden tagállam számára. Az Európa Tanács 1972 óta nagyszámú, adatvédelmi tárgyú ajánlást és határozatot fogadott el.<sup>12 VI</sup>

E tekintetben különös figyelmet érdemel az R(87) 15. számú Ajánlás a személyes adatok rendőrségi használatának szabályozásáról<sup>13</sup>, amely a különleges személyes adatok védelmének biztosításában még a 108. Egyezménynél is tovább megy. Az Ajánlás függelékében rögzített Alapelvek egyike – 2.4 Alapelv – szerint az egyén adatainak gyűjtését csupán bizonyos emberfajtához tartozásuk, bizonyos vallási meggyőződésük, szexuális magatartásuk vagy politikai mozgalomhoz vagy szervezethez való tartozásuk alapján meg kell tiltani, feltéve, hogy azt jogszabály nem rendeli el. Efféle adatok csak akkor gyűjthetők, ha azok meghatározott adatfelvétel céljából abszolút szükségesek. Az Ajánlás függeléke számos egyéb alapelvet is rögzít, amelyek a rendőrség által végzett gyűjtést, tárolást, felhasználást, közzétét és tartós megőrzést szabályozzák. A preambulum szerint az Ajánlás szükségesnek tartja az egyensúly megteremtését az egyén érdekei és magánélethez való joga, másrészt a társadalom érdeke között a bűncselekmények megelőzése és elfojtása, valamint a közrend fenntartása céljából. Evégből az Európai Emberi Jogi Bíróság esetjogát vették tekintetbe.

---

<sup>11</sup> Lásd: 2002. évi VI. törvény az Európa Tanácsnak az emberi lény emberi jogainak és méltóságának a biológia és az orvostudomány alkalmazására tekintettel történő védelméről szóló, Oviedóban, 1997. április 4-én kelt Egyezménye: Az emberi jogokról és a biomedicináról szóló Egyezmény, valamint az Egyezménynek az emberi lény klónozásának tilalmáról szóló, Párizsban, 1998. január 12-én kelt Kiegészítő Jegyzőkönyve kihirdetéséről

<sup>12</sup> Lásd Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995), Recommendation No.R(97) 5 on the protection of medical data (13 February 1997), Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997), Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999) and Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes (18 September 2002).

<sup>13</sup> Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987).

Az ECtHR magánszférát és magánélet védelmét érintő esetjoga számos, adatvédelmi hivatkozást tartalmaz. Ebben az összefüggésben az ECtHR nem csak az ECHR 8. cikkében azt a tagállamokra rótt negatív kötelezettséget érti, hogy tartózkodjanak a magánszféra jogába való beavatkozástól, hanem azt a pozitív kötelezettséget is, amely felöleli „olyan intézkedések foganatosítását, amelyek a magánélet tiszteletben tartását hivatottak biztosítani még az egyénnek magának a kapcsolatai rendszerében is.”<sup>14</sup>

Az M.S. kontra Svédország ügyben például az ECtHR leszögezte, hogy „a személyes adatok védelme alapvetően fontos tényezője annak, hogy egy személy élvezze magán és családi élete tiszteletben tartásának jogát, melyet az Egyezmény 8. cikke garantál.”<sup>15</sup> A Leander kontra Svédország ügyben a Bíróságnak az volt az álláspontja, hogy egy egyén magánéletére vonatkozó információ tárolása egy titkos nyilvántartásban és ilyen információ kiszolgáltatása beavatkozásnak minősül magánélete tiszteletben tartásához fűződő jogába, melyet az Egyezmény 8. cikke garantál.<sup>16</sup> A Bíróság hangsúlyozta, hogy „annak a kockázatnak a tekintetében, hogy a nemzetbiztonság védelmének egy rendszere aláássa, sőt rombolja a demokráciát azért, hogy védje, a bíróságnak meg kell győződnie arról, hogy megfelelő és hatékony garanciák vannak a visszaélés ellen”. A Z. kontra Finnország ügyben a Bíróság kiemelte, hogy a személyes adatok védelme, különösen az egészségügyi adatok védelme, alapvetően fontos tényezője annak, hogy egy személy élvezze magán és családi élete tiszteletben tartásának jogát, melyet az Egyezmény 8. cikke garantál.<sup>17</sup> A Bíróság mindazonáltal elfogadta, hogy egy beteg és a közösség egésze érdekében az egészségügyi adatok bizalmas voltának védelménél többet nyomhat latban a bűntettek felderítése és üldözése, továbbá a bírósági eljárások nyilvánossága, ahol ezek az érdekek sokkal fontosabbak.

A Rotaru kontra Romania ügyben az ECtHR kifejezetten megállapította, hogy az ECHR 9. cikkét úgy kell értelmezni, hogy felölelje a 108. Egyezményben rögzített adatvédelmi garanciákat.<sup>18</sup> Megismételte azt a Leander ügyben rögzített alapelvet, hogy egy hatóság által tárolt, az egyén magánéletére vonatkozó információ tárolása és felhasználása beavatkozásnak minősül a magánélet tiszteletben tartása jogába, s hozzátette, hogy ilyen beavatkozás az is, ha megtagadják a személyes adatok helyesbítésének lehetőségét. Az Amann kontra Svájc ügyben a Bíróság megállapította, hogy ha egy kártya az egyén magánéletére vonatkozó adatokat tartalmaz és azokat egy hatóság tárolja, önmagában is a kérelmező magánélete tiszteletben tartása jogába való beavatkozásnak minősül, s a Bíróság nem tartotta szükségesnek annak mérlegelését, hogy a felvett információ különleges-e avagy nem.<sup>19</sup>

Az ECtHR a K.U. kontra Finnország ügyben nemrég leszögezte, hogy a nemzeti jogalkotó dolga megalkotni egy olyan keretrendszert, amely összhangba hozza az Internet szolgáltatások bizalmas voltát a rendellenesség vagy bűncselekmények megelőzésével, valamint mások jogainak és szabadságainak védelmével. Mivel ez a keretrendszer az adott időben még nem létezett, Finnország nem gondoskodott a kérelmező magánélete tiszteletben tartásának védelméről, mert a bizalmasság követelménye fizikai és erkölcsi jóléte felett elsőbbséget élvez, s ezért az ECtHR arra a következtetésre jutott, hogy a 8. cikket

---

<sup>14</sup> Lásd X and Y v Netherlands, judgement of 26 march 1985, para 23.

<sup>15</sup> Lásd M.S. v Sweden, judgment of 27 August 1997.

<sup>16</sup> Lásd Leander v. Sweden, judgment of 26 March 1987, para. 48.

<sup>17</sup> Lásd Z. v. Finland, judgment of 25 February 1997, para 95.

<sup>18</sup> Lásd Rotaru v Romania, judgment of 4 May 2000, para 43.

<sup>19</sup> Lásd Amann v Switzerland, judgment of 16 February 2000, para 70.

megsértette.<sup>20</sup> Az S. és Marper kontra Egyesült Királyság ügyben az ECtHR határozott a kérelmezők ujjlenyomatait, sejtmintái és DNA profiljai brit hatóságok által való megőrzésének törvényességéről azt követően, hogy egy ellenük folytatott büntetőeljárás végeztével felmentették, és szabadlábra bocsátották őket, és annak ellenére, hogy adataik megsemmisítését kérték. Az ECtHR szerint a sejtminták és a DNA profilok sok, az egyént érintő különleges információt tartalmaznak, így mind a sejtminták, mind a DNA profilok megőrzése sérti a kérelmezők magánélete tisztelőben tartásának a 8. cikk (1) bekezdésben rögzített jogát, a Bíróság megjegyezte továbbá, hogy a 8. cikkben nyújtott védelmet elfogadhatatlanul gyengíti, ha a korszerű tudományos technikák használatát bármi áron megengedik anélkül, hogy egyensúlyba hoznák e technikák kiterjedt használatának lehetséges előnyeit a magánélet fontos érdekeivel.<sup>21</sup>

Három francia ügyben, 2009-ben, megerősítve az automatizált, különösen rendőrségi célokat szolgáló feldolgozásnak kitett személyes adatok védelmének alapvető szerepét, a Bíróság arra a következtetésre jutott, hogy a kérelmezők felvétele a szexuális bűntettesek adatbázisába oly módon, ahogyan azt rájuk alkalmazták, nem ellentétes a 8. cikkel.<sup>22</sup>

### 3. Adatvédelem az EU jogban

A személyes adatok védelmét az elsődleges EU jog mint autonóm alapjogot ismeri el, amely összefügg a magán- és családi élet tisztelőben tartásának jogával, de attól különbözik. Az EU Alapjogi Chartájának 8. cikke így hangzik: „(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. (2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni. (3) E szabályok tisztelőben tartását független hatóságnak kell ellenőriznie.”<sup>23</sup> Az EU Alapjogi Chartája az Európai Unióról szóló Szerződés (EUSz) 6. cikke értelmében „ugyanolyan jogi kötéssel bír, mint a Szerződések”.

Az EU 95/46/EK adatvédelmi irányelve szerint személyes adat az azonosított vagy azonosítható természetes személyre ("érintettre") vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számmal vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén”.<sup>24</sup>

A személyes adatok védelmét mint autonóm jogot az EU Alapjogi Chartája másképp kezeli mint egyéb nemzetközi emberi jogi dokumentumok, amelyek nem kifejezetten említik az adatvédelem jogát, hanem azt jobbra a magánszférához fűződő jog kiterjesztésének tekintik.

---

<sup>20</sup> Lásd K.U. v Finland, judgment of 2 December 2008.

<sup>21</sup> Lásd S and Marper v UK, judgment of 4 December 2008.

<sup>22</sup> Lásd Bouchacourt v. France, Gardel v. France, and M.B. v. France, judgements of 17 December 2009 (not final).

<sup>23</sup> A Charta 8. cikkéhez fűzött kommentár az EU Alapjogi Charta Kommentárjában olvasható (90. oldal). A Kommentárt az EU Alapjogaival foglalkozó független szakértők hálózata dolgozta ki. Letölthető (csak angolul: Commentary of the Charter of Fundamental Rights of the European Union, prepared by the EU Network of Independent Experts on Fundamental Rights - 20 June 2006):

[http://ec.europa.eu/justice/doc\\_centre/rights/charter/docs/network\\_commentary\\_final%20180706.pdf](http://ec.europa.eu/justice/doc_centre/rights/charter/docs/network_commentary_final%20180706.pdf)

<sup>24</sup> EU 95/46/EK adatvédelmi irányelv 2 cikk (a) pont.

### 3.1 Adatvédelem a Közösség korábbi pillérjében

Az EU adatvédelmi rendszerét jelentősen befolyásolta az EU korábbi pillérmegosztási szerkezete, melyet a Lisszaboni Szerződés megszüntetett. Az adatvédelem minden egyes pillérben elkülönült eszközcsoportokban nyerte el szerkezetét. A korábbi pillérmegosztás bizonytalanságokkal járt azt illetően, hogy mely eszközök vonatkoznak az adatfeldolgozás egy-egy adott esetére.

Az EU korábbi, első pillérjének, vagyis a korábbi közösségi pillérjének fő célja az volt, hogy biztosítsa a személyes adatok szabad áramlását a tagállamok között a belső piac működése folyamán, egyúttal védve a természetes személy alapvető jogait, különösen magánszférájuk jogait személyes adataik feldolgozása során. A személyes adatok védelme nem csupán azt kívánja az EU intézményeitől és tagállamaitól, hogy tartózkodjanak a személyes adatokba való törvénytelen beavatkozástól, hanem a személyes adatok védelme biztosításának pozitív kötelezettségét is előírja számukra.

A 95/46/EK adatvédelmi irányelv (1996. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (az alábbiakban adatvédelmi irányelv) az egyik legfontosabb EK-eszköz.<sup>25</sup> Az Európai Bíróság szerint az adatvédelmi irányelv megállapította „az EU szintjén azokat az alapelveket, amelyek már az adott területen fekvő tagországok jogának részét képezték.”<sup>26</sup> Az EK adatvédelmi rendszere a következő, az adatvédelmi irányelvben lefektetett alapelveken nyugszik: (i) a személyes adatok feldolgozása jogszerű és az érintettel szemben tisztességes; (ii) feldolgozásuk célja meghatározott és jogszerű, melyet az adatgyűjtés időpontjában kell megállapítani; (iii) feldolgozásuk célja szempontjából relevánsak és nem túlzott mértékűek. Az adatok pontosak és – ahol szükséges – időszerűek; (iv) a személyes adatok feldolgozása csak akkor jogszerű, ha megfelel az irányelvben előírt feltételeknek (ha – egyéb feltételek mellett – az érintett ahhoz egyértelmű hozzájárulást adta). Ha az érintett jogait nem tartják tiszteletben, az érintett bírósági jogorvoslatot élvez, amely lehetővé teszi számára a rá vonatkozó személyes adatokhoz való hozzáférést és azok pontosítását; (v) a személyes adatok továbbítása harmadik országokba csak akkor megengedett, ha azok megfelelő szintű védelmet nyújtanak; (vi) az EU és tagállamai egy vagy több független hatóságot hoznak létre, melyek feladata a személyes adatokra vonatkozó szabályok helyes alkalmazásának biztosítása.

Az adatvédelmi irányelv „a személyes adatokon (...) végzett bármely művelet vagy műveletek összességéeként” értelmezett „adatfeldolgozást” öleli fel. A 3. cikk (1) bekezdése szerint hatálya „a személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely tároló rendszer részét képezik, vagy amelyeket egy tároló rendszer részévé kívánnak tenni” terjed ki. A 3. cikk (2) bekezdés azt a két területet jelöli meg, melyekre az Irányelv nem vonatkozik. E cikk rendelkezései szerint az Irányelv nem alkalmazandó a személyes adatok feldolgozásaira, ha azok egyrészt „a közösségi jog hatályán kívül eső tevékenységek, mint például az EUSz V. és VI. címeiben megállapítottak, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási művelet nemzetbiztonsági ügyre vonatkozik), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek,” másrészt ha az „a természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett adatfeldolgozás”.

---

<sup>25</sup> Hivatalos Lap OJ L 281, 1995.11.23., 31. oldal

<sup>26</sup> Lásd Case C- 369/98 The Queen v Minister of Agriculture Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher [2000] ECR I-06751, para 34.

Az EU másik fontos jogeszköze a 2002/58/EK Irányelv az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv).<sup>27</sup> Célja a magánélet joga védelmére vonatkozó különféle nemzeti rendelkezések harmonizálása az elektronikus hírközlési ágazatban folyó személyesadat-feldolgozásokra, biztosítva ilyen adatok, továbbá elektronikus hírközlő eszközök és szolgáltatások szabad áramlását. Az EU 2002/58/EK Irányelve a 95/46/EK Irányelvnek sajátos kiegészítése a természetes személyek személyes adatainak az elektronikus hírközlési ágazatban folyó feldolgozása tekintetében, és felöleli a jogi személyiségű előfizetők jogos érdekeinek védelmét is. Az Irányelv nem alkalmazható az EK Szerződés hatályán kívül eső tevékenységekre.

A 95/46/EK és a 2002/58/EK irányelvek címzettjei a tagállamok. Ennek megfelelően nem alkalmazhatók az EU intézményeire és szerveire. A személyes adatok védelme is egy „szerződés-adta” jog, hiszen az Európai Unió működéséről szóló szerződés 16. cikke szabályokat állapít meg a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, melyeket az Európai Unió intézményeire is alkalmazni kell. Az EK szerződés korábbi, 286. cikke alapján, melynek az Európai Unió működéséről szóló szerződés 16. cikke lépett helyébe, kihirdették az Európai Parlament és a Tanács 45/2001/EK rendeletét (2000. december 18.)<sup>VII</sup> a személyes adatok EU intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról.<sup>28</sup> A Rendelet célja a természetes személyek alapvető jogainak és szabadságainak, így különösen a magánélet tiszteletben tartásához való joguknak a védelme a személyes adatok feldolgozása vonatkozásában. E Rendeletet kell alkalmazni a személyes adatok bármely közösségi intézmény és szerv által történő feldolgozására, ha a feldolgozás részben vagy teljes egészében a közösségi jog hatálya alá tartozó tevékenységek gyakorlása során történik. E Rendelet hozta létre 2004-ben az európai adatvédelmi biztos (EDPS) intézményét.

Az EDPS független ellenőrző hatóság, melynek feladata a személyes adatok és a magánélet védelme, valamint a helyes gyakorlat elősegítése az EU intézményeiben és szerveiben. Figyelemmel kíséri a személyes adatok feldolgozását az EU igazgatási szerveinél, a magánélet védelmét érintő eljárásokra és jogalkotásra vonatkozó ajánlásokat tesz, a konzisztens adatvédelem biztosítása érdekében együttműködik hasonló hatóságokkal. Felügyeleti hatáskörében biztosítja az EU alkalmazottai és mások személyes adatai EU intézményeknél és szerveknél folyó feldolgozásának jogszerűségét. Minden egyes intézménynek vagy szervnek ki kell neveznie egy belső adatvédelmi tisztviselőt, aki a feldolgozási műveletek nyilvántartását vezeti, és jelentést tesz az EDPS-nek a különösen kockázatos rendszerekről. Az EDPS előzetesen ellenőrzi, hogy e rendszerek kielégítik-e az adatvédelmi követelményeket. Az EDPS foglalkozik továbbá a panaszokkal, és vizsgálatokat is végez. Ily módon az EDPS felügyeli a 45/2001/EK adatvédelmi rendeletet. Az EDPS tanácsokkal látja el az Európai Bizottságot, az Európai Parlamentet és a Tanácsot új jogszabály-tervezetekkel kapcsolatban, és minden egyéb, adatvédelmi tárgyú kérdésben. Az EDPS együttműködik más adatvédelmi hatóságokkal abból a célból, hogy Európában

---

<sup>27</sup> Az Európai Parlament és a 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), Hivatalos Lap OJ L 201, 2002.07.31., 37. oldal.

<sup>28</sup> Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról. Hivatalos Lap OJ L 8, 2001.12.1., 1-22. oldal.



elősegítse a konzisztens adatvédelem kialakulását. Az EDPS és a nemzeti felügyelő hatóságok együttműködésének központi színtere az úgynevezett 29-es Munkacsoport.<sup>29</sup>

A 2006/24/EK irányelv a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről intézkedik ('Adatmegőrzési Irányelv')<sup>30</sup>. Ezen irányelv célja azon tagállami rendelkezések harmonizálása, amelyek a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóinak vagy a nyilvános hírközlő hálózatok szolgáltatóinak egyes általuk előállított vagy feldolgozott adatok megőrzésére vonatkozó kötelezettségeit szabályozzák. Ez biztosítja, hogy ezen adatok az egyes tagállamok nemzeti joga által meghatározott súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából rendelkezésre álljanak.

Az Európai Bíróság számos határozatában értelmezte a 95/46/EK irányelvet. A kérdések első csoportja arra indította a Bíróságot, hogy megállapítsa ezen irányelv alkalmazásának hatályát. Az Österreichischer Rundfunk ügyben azt kérelmezték, hogy a Bíróság döntsön abban a kérdésben, hogy az adatvédelmi irányelvet kell-e alkalmazni az Ausztria Számvevőszéke valamennyi ellenőrző tevékenységére egyes jogi személyek alkalmazottai fizetése tekintetében.<sup>31</sup> A Bíróság úgy találta, hogy azt alkalmazni kell, „mert a tagállamok között bármely személyes adat áramolhat, s a 95/45 irányelv elvileg megköveteli az ilyen adatok védelmére vonatkozó szabályok betartását az adatok bármiféle feldolgozása folyamán, ahogyan azt a 3. cikk előírja”. A *Satakunnan Markkinapörssi and Satamedia* ügyben hasonló döntés született. A Bíróság leszögezte, hogy azok a személyes adatállományok, amelyek kizárólag és változatlan formában a médiában már közzétett anyagokat tartalmaznak, a 95/46 irányelv alkalmazásának hatálya alá tartoznak.<sup>32</sup>

Jogi esetek egy másik csoportja az adatvédelmi irányelv egyes rendelkezései értelmezésére vonatkozott. A Lindqvist ügyben az Európai Bíróság a személyes adatoknak az Internet mint médium által végzett feldolgozása kérdésében döntött.<sup>33</sup> Efféle információ elhelyezése az Interneten 'személyes adatok részben vagy egészben automatizált módon való feldolgozásának' minősül. Mindazonáltal a Bíróság úgy találta, hogy személyes adatok feltöltése egy Internet oldalra, nem tekinthető a 95/46 irányelv 25. cikkében szabályozott 'harmadik országba irányuló továbbításnak'. A Bíróság végül nagyon fontos döntést hozott a megkülönböztetés tilalmának alapelveire vonatkozóan a személyes adatok védelme keretében az uniós polgársággal összefüggésben.<sup>34</sup> A Bíróság álláspontja szerint a tagállamok és az Unió más polgárai megkülönböztetett kezelése, amely csak ez utóbbiakat érintő személyes adatok szisztematikus, a bűnözés elleni harc célját szolgáló feldolgozásán alapul, amely az EKSz 12. cikk (1) bekezdésében<sup>viii</sup> tiltott megkülönböztetésnek minősül.

A Bíróság szándéka, hogy egyensúlyt teremtsen a magánélet és az adatvédelem joga, továbbá más, az EK jogrendjében védett alapvető jogok és szabadságok között. Felettből érzékenyek

---

<sup>29</sup> A Munkacsoport létrehozásáról a 95/46/EK adatvédelmi irányelv 29. cikke rendelkezett. Lásd [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm)

<sup>30</sup> Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Hivatalos Lap OJ L 105 of 13.4.2006.04.13., 54. oldal.

<sup>31</sup> Lásd Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk, 2003. május 20-án kelt ítélet, Full Court, [2003] ECR I-4989.

<sup>32</sup> Lásd Case C-73/07 Satakunnan Markkinapörssi and Satamedia, 2008. december 16-án kelt ítélet.

<sup>33</sup> Lásd Case C-101/01 Bodil Lindqvist [2003] ECR I-12971.

<sup>34</sup> Lásd Case C-524/06 Huber v Bundesrepublik Deutschland, 2008. december 16-án kelt ítélet.

mutatkozott azokban az esetekben, amelyek a szólásszabadságot, közelebbről az újságírást érintik, ahol a kivételt az adatvédelem alól e célra úgy látszik kész elfogadni. Ezzel szemben nem adott világos feleletet az adatvédelem joga és a szellemi tulajdon joga közti feszültség esetében.

A Lindqvist ügyben<sup>35</sup> a Bíróságnak egyensúlyt kellett teremtenie az adatvédelem és a szólásszabadság joga között, mely jogokat, egyebek mellet, védi az ECHR 10. cikke, s mint az EU jog általános alapelvét védi az EK jogrendje is. A Bíróság szerint „az alapvető jogok különösen fontosak, amint azt a főeljárásban tárgyalt eset igazolta, melyben lényegében Lindqvist asszony munkájában az emberek úrvacsorára való előkészítése és a szabadságát képező, vallásos életet szolgáló tevékenysége során gyakorolt szólásszabadságát kellett egyensúlyba hozni azon egyének magánéletének védelmével, akiknek adatait Lindqvist asszony feltette saját Internet-oldalára”. A *Satakunnan Markkinapörssi and Satamedia*<sup>36</sup> a Bíróságot az adatvédelmi irányelv 9. cikke értelmezését kérték, mely megengedi, hogy a tagállamok a személyes adatok feldolgozása alól mentességeket és eltéréseket állapítsanak meg „kizárólag (...) újságírás, vagy irodalmi, illetve művészi kifejezés céljából (...), amennyiben azok a magánélet tiszteletben tartásához való jognak a szólásszabadságra vonatkozó szabályokkal való összeegyeztetéséhez szükségesek”. Markkinapörssi nyilvános adatokat gyűjtött a finn adóhatóságoktól, hogy azok kivonatát a Veropörssi c. újság helyi kiadásában közzétegye, s ugyanezeket az adatokat továbbította a Satamedianak egy szöveges üzenetküldő rendszerben való terjesztés céljából. Az ECJ hangsúlyozta a szólásszabadság jogának fontosságát egy demokratikus társadalomban, és úgy vélte, hogy ezt a szabadsággal, ez esetben az újságírással kapcsolatos fogalmat széles értelemben kell venni. Ezt követően rávilágított arra, hogy a belső jog szerint nyilvános dokumentumokból származó adatok feldolgozása 'újságírói tevékenységként' fogható fel, ha annak célja „információ, vélemények vagy ismeretek közzététele a nyilvánosság számára, függetlenül attól, erre mely médiumban kerül sor”. A Bíróság továbbá úgy határozott, hogy e tevékenységek nem korlátozódnak a médiavállalkozásokra, hanem kiterjednek minden, újságírással foglalkozó személyre, és jövedelemszerző célra is folytathatók.

Hasonló kérdésekkel foglalkozott az ECJ a Promusicae ügyben.<sup>37</sup> Megállapítása szerint a „2002/58 irányelv nem zárja ki azt a lehetőséget, hogy a tagállamok rendelkezzenek a személyes adatok polgári eljárás keretében való nyilvánosságra hozásának kötelezettségéről”, és a szellemi tulajdont védő jogszabályok nem „követelik, hogy a tagállamok a szerzői jog hatékony védelme érdekében rendelkezzenek a személyes adatok polgári eljárás keretében való közzétételének kötelezettségéről”. A Bíróság végül arra a következtetésre jutott, hogy „meg kell teremteni az összhangot a különféle alapvető jogok, nevezetesen egyrészt a magánélet tiszteletben tartásának joga, másrészt a tulajdon jog és mások hatékony jogorvoslathoz való joga között”.

### **3.2 Adatvédelem az EU korábbi, második és harmadik pillérjében**

A személyes adatoknak a korábbi első pillér hatályán kívül eső tevékenységek keretében folyó feldolgozása tekintetében továbbra is komoly bizonytalanságok és hiányosságok merülnek fel. Bár a személyes adatok védelmére vonatkozó alapvető szabályokat tiszteletben kell tartani a személyes adatoknak a korábbi második és harmadik pillér keretében folyó

---

<sup>35</sup> Lásd Case C-101/01 Bodil Lindqvist [2003] ECR I-12971.

<sup>36</sup> Lásd Case C-73/07 Satakunnan Markkinapörssi and Satamedia, 2008. december 16-án kelt ítélet.

<sup>37</sup> Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, 2008. január 29-én kelt ítélet.

feldolgozása során, a személyes adatok védelmének általános jogi kerete a korábbi második és harmadik pillérben hiányzik. Ehelyett az adatvédelem szétszórva, ad hoc adatvédelmi szabályokban, a személyes adatok feldolgozására vonatkozó különféle eszközök, például a bűnügyekben folytatott rendőrségi és bírósági együttműködés keretében jelenik meg.<sup>38</sup> A korábbi második és harmadik pillérnek számos strukturális problémával és hiányossággal kellett szembenéznie, ami még tovább korlátozta az alapvető jogok hatékony védelmét. A korábbi harmadik pillér elsősorban a demokratikus ellenőrzésben mutatkozó hiányosságban szenvedett. Az Európai Parlament szerepe lényegében csupán a konzultációra korlátozódott, véleményét, ha akarta, a Tanács figyelmen kívül hagyhatta. A kezdeményezés joga továbbá megosztott a Bizottság és tagállamok között, s erre a korábbi kormányközi pillére az egyhangúság szabályát kellett alkalmazni. Másodsorban a Bíróság ellenőrzési jogköre a korábbi harmadik pillérben ugyancsak korlátozva volt. A EUSz korábbi 35(1) cikke értelmében a Bíróság előzetes döntést hozhatott a kerethatározatok érvényességéről és értelmezéséről, dönthetett az egyezmények értelmezéséről, továbbá az azokat alkalmazó eszközök érvényességéről és értelmezéséről. Ezt a döntést először a tagállamoknak kellett elfogadnia, ami tovább korlátozhatta egyes nemzeti bíróságok és ítélőszékek előzetes döntést igénylő lehetőségeit.

Harmadsorban az adatvédelmi hatóságok, pl. az EU adatvédelmi biztosa tanácsadó szerepe az első pillérhez képest ugyancsak korlátozott volt. Még ha például az Európai Bizottság meg is erősíti, hogy magára nézve kötelezőnek tartja, hogy az európai adatvédelmi biztossal konzultáljon, amikor elfogad egy, a személyes adatok védelmét érintő jogszabályalkotásra vonatkozó javaslatot [minthogy erre a 45/2001 rendelet 28. cikk (2) bekezdése kötelezi], kezdeményezési jogát a harmadik pillérben meg kell osztania a tagállamokkal, melyeknek ilyen kötelezettségük nincsen. Ez a helyzet a második pillérben még problematikusabb volt, mert a Közös Kül- és Biztonságpolitika keretében a bírósági felülvizsgálat nem létezett.

Az utóbbi években a személyes adatok cseréje különböző tagállamok rendészeti hatóságai között a rendőrségi és bírósági együttműködés mindennapi gyakorlatává vált. E tekintetben 'terrorizmus elleni harcra' választ adó, 2004. november 5-én elfogadott „Hágai Program” lefektette a „rendelkezésre állás elvét”, ami azt jelenti, hogy egyes tagállami hatóságok rendelkezésére álló információt másik tagállam megfelelő hatóságának is rendelkezésére kell bocsátani. A „rendelkezésre állás elve” a személyes adatok védelmére nézve számos következménnyel jár, és e tekintetben megfelelő biztosítékokra volt és van még mindig szükség.

Ebben a helyzetben üdvös változást hozott a Tanács 2008/977/IB kerethatározata (2008. november 27.) a bűntetőügyekben folytatott rendőrségi és igazságügyi együttműködés

---

<sup>38</sup> A személyes adatok védelmét az EUSz VI. címével (az úgynevezett III. pillér) összefüggésben lásd például a Schengeni Megállapodást végrehajtó Egyezményt (1990) ide értve a Schengeni Információs Rendszerre alkalmazandó sajátos adatvédelmi rendelkezéseket is, Hivatalos Lap OJ L 239, 2000.9.22. 19. oldal; személyes adatoknak az Europol által harmadik országokba és harmadik szervezeteknek való továbbítására vonatkozó szabályok, hivatalos lap OJ C 316, 1995.11.27., 2. oldal; az Eurojust létesítésére vonatkozó határozat (2002), Hivatalos Lap OJ L 63, 2002.3.6., 1. oldal és az Eurojust személyes adatok feldolgozására és védelmére vonatkozó eljárási szabályzatával kapcsolatos rendelkezések, Hivatalos Lap OJ C 68, 2005. 3.19., 1. oldal; Egyezmény az informatika vámügyi alkalmazásáról (1995), ide értve a személyes adatok védelmére vonatkozó váminformációs rendszerre alkalmazandó rendelkezéseket, Hivatalos Lap OJ C 316, 1995.11.27., 34. oldal; és Egyezmény az Európai Unió tagállamai bűnügyi kölcsönös segítségnyújtásáról, nevezetesen 23. cikk, Hivatalos Lap OJ C 197, 12.7.2000.07.12., 1, 15. oldal.

keretében feldolgozott személyes adatok védelméről.<sup>39</sup> Ez a Határozat az első horizontális adatvédelmi jogszabály a rendőrségi és igazságügyi hatóságok által kezelt személyes adatokat illetően. A Kerethatározat a rendőrségi és igazságügyi együttműködés keretében a személyes adatok határon átnyúló cseréjére alkalmazható. A jogszabály a személyes adatok harmadik országokba irányuló továbbítására és tagállami magánfeleknek való átadására alkalmazható szabályokat tartalmaz. A határozat szerint az EU tagállamoknak lehetősége van arra, hogy a személyes adatok védelmének az e jogszabályban megállapított biztosítékoknál magasabb szintű biztosítékokat állapítsanak. A Kerethatározat mindazonáltal önmagában nem biztosítja, hogy a magánélet és a személyes adatok védelme tiszteletben tartásának jogi garanciái teljes összhangban vannak a személyes adatok feldolgozásával második és a harmadik pillér keretében. Alkalmazási hatálya csak a bűnüldöző szervek között folyó, határon átnyúló adatcserére terjed ki, nem alkalmazható a bűnüldöző szervek adatfeldolgozására a tagállamon belül. A Kerethatározatot 2010. november 27-éig, meghozva a megfelelő intézkedéseket, valamennyi EU tagállamnak végre kell hajtania, s ki kell jelölnie egy vagy két hatóságot, amelyek területükön alkalmazását nyomon követik, s tanácsadást is nyújtanak.

A személyes adatok védelme az EU korábbi pillérstruktúrájában egyike volt azoknak a területeknek, ahol állandóan eltérő vélemények merültek fel arra nézve, adott feldolgozás vajon melyik pillérhez tartozik. Az Európai Bíróság utasnyilvántartási (PNR) ügyekben hozott ítélete szemléltette az EU adatvédelmi rendszere korábbi pillérmegosztásából fakadó problémákat<sup>40</sup>. Ezek az ügyek arra az Egyesült Államok és az EU között létrejött megállapodásra vonatkoztak, amely az Egyesült Államokba és onnan induló járatokat működtető légitársaságok foglalási és indulása ellenőrző rendszerében kezelt utasnyilvántartási ('PNR') adatok átadását szabályozza. Az adatvédelmi irányelv 25. cikke alapján hozott Megfelelőségi Határozat alapján a Tanács 2004. május 17-én úgy határozott, hogy a Megállapodás az Egyesült Államokkal megköthető. Az Európai Parlament keresetet nyújtott be a Bírósághoz, s kérte mind a Megfelelőségi Határozat, mind a megállapodás megkötésére vonatkozó határozat megsemmisítését, többek között arra hivatkozva, hogy azok sértik az adatvédelmi irányelv alapelveit és a magánélet jogát. A Bíróság megsemmisítette a Megfelelőségi Határozatot, s ezt csupán azzal indokolta, hogy annak tárgya kívül esik az adatvédelmi irányelv anyagi hatályán. Megállapította, hogy a PNR adatok átadása a 95/46 irányelv 3. cikke (2) bekezdése szerint a „közbiztonsággal és a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek” közé tartozik, s így a Megfelelőségi Határozat az Irányelv alapján nem fogadható el. A Bíróság ugyancsak megsemmisítette a Megállapodás megkötésére vonatkozó Határozatot is arra hivatkozva, hogy az nem fogadható el az EK 95. cikkére mint jogalapra hivatkozva, mert az „ugyanazoknak az adatoknak az átadásával kapcsolatos, mint a megfelelőségi határozat, és azért olyan adatfeldolgozási műveleteket céloz, amelyek kívül esnek az irányelv hatályán”. Így az EU-nak a Megállapodás megkötésére nem volt felhatalmazása. Azáltal, hogy a Bíróság a Megállapodást ily módon áthelyezte a korábbi harmadik pillérből az elsőbe, ami jelentős következményekkel jár a bírósági felülvizsgálatra és a demokratikus ellenőrzésre nézve, ítélete az egyén

---

<sup>39</sup> A Tanács 2008/977/IB kerethatározata (2008. november 27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről, Hivatalos Lap, OJ L 350, 2008.12.30., 60. oldal.

<sup>40</sup> Joined Cases C-317/04 and C-318/04, European Parliament v. Council and Commission, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721.

„adatvédelemhez fűződő jogában joghézagot alkotott”.<sup>41</sup> Ennél is jelentősebb, hogy a bírósági döntés eredményeként az EU-nak tárgyalást kellett folytatnia az USA-val és vele immár helytálló jogalapra építve új megállapodást kellett kötnie. 2007-ben a Bizottság javaslatot tett bűnüldözési célokat szolgáló utasnyilvántartási adatok használatát szabályozó Tanácsi kerethatározatra.<sup>42</sup> A francia elnökség a javaslatról az Alapjogi Ügynökség véleményét kérte, amit 2008. október 28-án meg is kapott.<sup>43</sup> Az Ügynökség véleménye szerint a PNR használatára vonatkozó javaslat hozzáadott értéke és szükségessége magyarázatra szorult, a homályos meghatározásokat kerülni kell, és megfelelő eljárási biztosítékokról is gondolkodni kell. Az Ügynökség javasolta továbbá a megkülönböztető etnikai profil kifejezett tilalmát.

Az Írország kontra Európai Parlament és Bizottság ügyben az ECJ-től ismételten azt kérelmezték, hogy foglaljon állást az EU adatvédelmi rendszerének a pillérek közti megosztásának rendszeréről.<sup>44</sup> Írország ugyanis a hírközlés adatai megőrzéséről szóló irányelvet kifogásolta azon az alapon, hogy az EK 95. cikke e jogszabály tekintetében nem a megfelelő jogalap, mert annak fő célja a súlyos bűncselekmények felderítése, üldözése és az azoktól való elrettentés, ide értve a terrorizmust is, és így azt a harmadik pillér keretében kellett volna elfogadni. A Bíróság ezt a nézetet nem osztotta, és megállapította, hogy az Irányelvet a megfelelő jogalapra hivatkozva fogadták el, mert mind célja, mint tartalma az EK 95. cikk alá tartozik. Az ügyet a PNR ítélettől elhatárolta azon az alapon, hogy a 2006/24 Irányelv a belső piacon működő szolgáltatók tevékenységére vonatkozik, és nem tartalmaz semmiféle olyan szabályt, amely bűnüldözési célú hatósági tevékenységet szabályozna, mint a PNR ügyben. A Bíróság mindazonáltal hangsúlyozta, hogy az Írország által kezdeményezett eljárás (és ezért az arról hozott ítélet) „csupán a jogalap megválasztására vonatkozott és nem alapvető jogok esetleges, a 2006/24 Irányelvben rögzített, magánszférához fűződő jog gyakorlásának beavatkozással való megsértésére”.<sup>45</sup> Néhány tagállamban kétségek merültek fel ezen irányelv és az alapvető jogok közti megfelelés tekintetében. Romániában például egy ítélesezék az Alkotmánybírósághoz fordult a román adatmegőrzési törvény állítólagos alkotmányellenessége kérdésében abban az ügyben, melyet a magánélet védelmében egy civil szervezet kezdeményezett egy távközlési társaság ellen.<sup>46</sup> A román Alkotmánybíróság 2009. október 8-án alkotmányellenesnek nyilvánította az adatvédelmi irányelvet megvalósító törvényt, és megállapította, hogy az sérti a magánélethez fűződő alapvető jogokat.<sup>47</sup> A Bíróság indokolása nem csak a törvényre magára vonatkozik, hanem megkérdőjelezi az irányelvnek az alapvető jogokkal való összeegyeztethetőségét is. Németországban jelenleg a Szövetségi Alkotmánybíróság előtt van az az ügy, amely az adatvédelmi irányelvet átültető német jogszabály és az alapvető jogok összeegyeztethetőségét kifogásolja. A bíróság, végső határozata meghozataláig, előzetes ítéletében részlegesen felfüggesztette a kifogásolt

---

<sup>41</sup> Lásd E. Guild and E. Brouwer, *The Political Life of Data – The ECJ decision on the PNR Agreement between the EU and the US*, (2006) Centre for European Policy Studies No. 109.

<sup>42</sup> COM (2007) 654.

<sup>43</sup> Lásd [http://fra.europa.eu/fraWebsite/attachments/FRA\\_opinion\\_PNR\\_en.pdf](http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf) (2010.01.22.)

<sup>44</sup> Case C-301/06 *Ireland v. European Parliament and Council*, Judgment of the Grand Chamber of 10 February 2009.

<sup>45</sup> *Ireland v. European Parliament and Council*, para 57.

<sup>46</sup> <http://www.mondonews.ro/Legea-298-de-stocare-a-datelor-telefonice-ajunge-la-CCR+id-5439.html> (07.09.2009).

<sup>47</sup> *Romania/Curtea Constituțională*, Decision nr. 1258 of 8 October 2009 of the Romanian Constitutional Court, available at: [http://www.legi-internet.ro/fiadmin/editor\\_folder/pdf/Decizie\\_curtea\\_constitutionala\\_pastrarea\\_datelor\\_de\\_trafic.pdf](http://www.legi-internet.ro/fiadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf) (24.02.2010).

jogszabályt.<sup>48</sup> 2010. március 2-én a Német Alkotmánybíróság alkotmányellenesnek nyilvánította az EU adatvédelmi irányelvet átültető jogszabályt.<sup>49</sup> Ebben a tekintetben javasolható, hogy az Európai Unió vizsgálja meg a 2006/24/EK adatmegőrzési irányelv összeegyeztethetőségét a Lisszaboni Szerződés új alapjogi normáival (lásd alább). Kívánatos lenne, ha az Európai Bíróság ismét ítéletet hozna az adatmegőrzési irányelv és az alapvető jogok összeegyeztethetősége tekintetében, amely valamennyi EU tagállamban a jobbiztonságot szolgálná.

A fő korlát, mellyel az EU-nak szembe kell néznie, ha hatékony és átfogó adatvédelmet kíván nyújtani, az EU pillérek korábbi alkotmányos szerkezetéből adódik. Míg az adatvédelem magas szintű az EU korábbi első pillérjében, az adatvédelmi rendszer az EU korábbi harmadik pillérjében nem tekinthető kielégítőnek. Mindazonáltal az EU korábbi harmadik pillérje olyan területeket ölel fel, mint a rendőrségi együttműködés, a terrorizmus elleni harc és büntetőjogi tárgyak, ahol az adatvédelem különösen fontos és elengedhetetlen.

### 3.3 A Lisszaboni Szerződés

Az adatvédelem alapvető jogával összefüggésben a Lisszaboni Szerződéssel az EU nagy előrelépést tett, mert az számos fontos javulást tartalmaz az EU szintű adatvédelemben. A Lisszaboni Szerződés mindenek előtt kötelező jogi kötőerőt rendel az Alapjogi Chartához. A Charta személyes adatok védelméről rendelkező 8. cikkének szerepe messze túl fogja haladni egy alapvető jog formális és szimbolikus kinyilatkoztatását. Az adatvédelem mint teljes jogi érvényű autonóm alapvető jog elismerése az elsődleges EU jogban, azt jelenti, hogy az adatvédelem jelentősebb szerepet játszik majd egyéb értékek és érdekek (pl. biztonsági vagy piaci érdekek) mérlegelése során, vagy midőn az EU törvényhozók és az ECJ prioritásokat határoznak meg. Egy másik jelentős előrelépés a 'pillérstruktúra' megszüntetése. Ez azt jelenti, hogy a Lisszaboni Szerződés szerint a korábbi harmadik pillérből fakadó, a döntéshozás folyamatával és a bírósági felülvizsgálattal kapcsolatos strukturális problémák, megoldódnak. Így minősített többségi szavazatra van szükség a szabadság, biztonság és jogérvényesítés területén, Az Európai Parlament szerepe megerősödött, és az ECJ teljes illetékességet nyert e terület tekintetében. Mindazonáltal megjegyzendő, hogy a Lisszaboni Szerződés 30. sz. Jegyzőkönyve szerint különös szabályok vonatkoznak az Egyesült Királyságra és Lengyelországra, korlátozva az EU Alapjogi Chartája hatását a brit és lengyel jogban. Hasonló, az EU Charta hatását a cseh jogban korlátozó törekvést tükrözött a 2009. október 29/30-án kelt Elnökségi Következtetések 2. pontja, rögzítvén, hogy az EU szerződésekhez egy jegyzőkönyvet csatolnak, mely szerint a 30. sz. Jegyzőkönyvet „módosítják annak érdekében, hogy a Cseh Köztársaságra ugyanazok a szabályok vonatkozzanak, mint Lengyelországra és az Egyesült Királyságra”.<sup>50</sup> A Lisszaboni Szerződéshez csatolt 20. sz. Nyilatkozat értelmében, ha olyan, a személyes adatok védelmére vonatkozó intézkedéseket foganatosítanak, melyeknek közvetlen hatása lehet a nemzetbiztonságra, „megfelelő figyelmet” kell fordítani a kérdés különös jellemzőire. A 20.

---

<sup>48</sup> German Constitutional Court, press release Nr 37/2008 of 19 March 2008.

<sup>49</sup> 2010 március 2-án kelt ítéletében (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Urteil vom 2. März 2010) alkotmányellenesnek nyilvánította az Adatmegőrzési Irányelvet átültető német törvényt azon az alapon, hogy az abban rögzített kötelezettségek aránytalanok. A Bíróság nevezetesen megállapította, hogy a Távközlési törvény 113. szakasza nem garantálja a tárolt adatok biztonságát, nem átlátható, mert előírja a tárolt adatok közvetlen használatát számos olyan bűncselekmény kivizsgálása, felderítése és üldözése céljából, melyet világosan nem részletez; és az érintettnek nyújtott védelem nem összeegyeztethető a Német Alkotmány követelményeivel. Lásd <http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html> (2010.02.04.).

<sup>50</sup> [http://www.consilium.europa.eu/ueDocs/cms\\_Data/docs/pressData/en/ec/110889.pdf](http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/110889.pdf) (2010.02.24.)

sz. Nyilatkozat szerint különös szabályokra lehet szükség a személyes adatok védelmére és azok szabad áramlására vonatkozóan a bűnügyekben folyó igazságügyi és rendőrségi együttműködés területén, melyek figyelembe veszik e területek „különös jellemzőit”. E jegyzőkönyvek és a személyes adatok védelmére vonatkozó nyilatkozatok tényleges hatása vitatható marad, és nem tisztázható mindaddig, ameddig a Bíróság e kérdésben esetjogot nem alkot.

## **4. Összehasonlító áttekintés**

A jelentés fő része összehasonlító áttekintést nyújt a nemzeti adatvédelmi hatóságokról, az adatvédelmi jogszabályok követelményeit érvényesítő belső gyakorlatokról, az adatvédelmi jogszabályok megsértését szankcionáló és kompenzáló jogorvoslati lehetőségekről a tagállamokban, és az EU polgárok adatvédelmi jogainak tudatosságáról. Az itt olvasható információ a FRALEX csoportja által az Ügynökség közös iránymutatásai szerint készített 27 országjelentésre épül (mindegyikük mint háttéranyag olvasható az ügynökség honlapján: <http://fra.europa.eu>). Ez az összehasonlító jelentés e tanulmányokon alapul. Az országjelentések 2009 februárjában készültek.

### **4.1 Adatvédelmi hatóságok**

Az EU minden tagállama eleget tett az adatvédelmi irányelv 28. cikk (1) bekezdés 1. mondatában rögzített követelményeknek, széles körű felhatalmazást adott egy nemzeti felügyeleti hatóságnak az adatvédelmi jogszabályok alkalmazása ellenőrzésére és tiszteletben tartásuk biztosítására. Több tagállam (pl. Ausztria, Hollandia) egy adatvédelmi hatóságot hozott létre általános hatáskörrel, és néhány egyéb ágazat-specifikus felügyeleti szervet (például az egészségügy, a posta vagy távközlés területén). Némelyikük viszont, melyek szerkezete szövetségi vagy melyekben jelentős hatalmat gyakorolnak a területi szervek (pl. Németország, Spanyolország) egy felügyelő hatóságot és több helyi ügynökséget létesítettek területi vagy szövetségi szinten megegyező funkciókkal.<sup>51</sup> Minthogy továbbá sok országban (pl. Romániában), az adatvédelmi hatóságok létrehozását megelőzően a magánélethez fűződő jogok tiszteletben tartása ellenőrzését ombudsman-intézményekre bízták, néhány tagállamban (pl. Finnországban) az ombudsman továbbra is megfelelő funkciókkal rendelkezik a személyes adatok védelmét illetően. Ebben a részben egy összehasonlító áttekintést mutatunk be. A vonatkozó helyes gyakorlatokat a 6.1 részben ismertetjük.

#### *4.1.1 Függetlenség*

Az EU tagállamok határozottan törekedtek arra, hogy megteremtsék az összhangot az adatvédelmi irányelv 28. cikk (1) bekezdés 2. mondatával, amely megköveteli, hogy a tagállamok nemzeti adatvédelmi hatóságai a rájuk ruházott funkciókat teljes függetlenséggel lássák el. Az adatvédelmi irányelv e rendelkezésének értelmezése volt a tárgya Mazák főtanácsnok véleményének. Véleménye szerint a „függetlenség” fogalma természetére nézve viszonylagosnak minősül, mert részletezni kell kihez és mely szinten kell e függetlenségnek

---

<sup>51</sup> Az összehasonlítás céljaira azonban ez a jelentés csak az állami szintű adatvédelmi hatóságokat elemzi. Megjegyezzük, hogy Németországban hasonló hatóságok léteznek tartományi szinten, felügyeleti jogkörük felöleli a köz- és magánszférát egyaránt, kiterjed a műsorszóró intézményekre vagy az egyházakra is. Egyes tartományokban ellenben a felügyelő hatóságok illetékessége csak a magánszférára terjed ki. Ez a jelentés nem foglalkozik a tartományi szintű felügyelő hatóságokkal.



viszonyulnia. Az adatvédelmi hatóságokkal kapcsolatban úgy vélte, hogy e hatóságok célját függetlenségük értékelése során figyelembe kell venni.<sup>52</sup>

Több országban mindazonáltal normatív vagy gyakorlati akadályok adnak aggodalomra okot a nemzeti felügyelő hatóságoknak a kormányzat politikai tényezőitől való tényleges függetlenségét illetően. A függetlenség garanciája tulajdonképpen elsősorban az adatvédelmi hatóságok tisztségviselői kinevezésére és elmozdítására vonatkozó eljárásban rejlik. A pénzforrások feletti rendelkezés képezi a felügyelő hatóságok autonómiának másik lényeges eleme.

Számos tagállamban (pl. Németországban, Szlovéniában) a törvényalkotó testületek választják meg az adatvédelmi hatóságok tisztségviselőit, olykor olyan eljárásban, amely a többség és az ellenzék konszenzusát igényli (pl. Görögországban). Néhány kivétellel (mint Magyarország, ahol egy alkotmányos gyakorlat megengedi, hogy a parlamenti pártok megosztozzanak a lehetséges pozíciókra való jelölésen) ez biztosítja a választott tisztségviselők magas szintű függetlenségét. Más tagállamokban viszont az adatvédelmi tisztségviselőket a parlamenti ellenzék bevonása nélkül közvetlenül a kormány nevezi ki (pl. Írországban, Luxemburgban). Ez több esetben (pl. az Egyesült Királyságban,<sup>53</sup> Litvániában, Észtországban) komoly aggodalomra ad okot az adatvédelmi hatóság tényleges függetlenségét illetően. Hasonló aggodalom merülhet fel azokban az országokban, ahol a felügyelő hatóság az igazságügyi minisztériumhoz van rendelve (pl. Dániában, Lettországban). Végül más tagállamok (pl. Franciaország, Spanyolország, Portugália, Belgium) vegyes eljárásban jelölik az adatvédelmi hatóság tisztségviselőit, egyidejűleg bevonva a végrehajtó, jogalkotó és bírósági szerveket vagy egyéb szervezett társadalmi csoportokat (pl. az egyetemek legfelsőbb tanácsát Spanyolországban). Hasonló esetekben azonban lényeges, hogy a kormány – hatékonyan meghiúsítva a pluralisztikus kinevezési eljárást – a gyakorlatban sem közvetlenül, sem közvetve nem vezérli a jelöltek többségének állítását.

Számos tagállamban (pl. Olaszországban) az adatvédelmi hatóságok tisztségviselői kinevezése hét éves időtartamra szól, tiltva visszahívásukat vagy ismételt, másodszori kinevezésüket. Egyes országokban (pl. Szlovéniában, Lengyelországban) adatvédelmi hatóságok tisztségviselői hivatalukból csak meghatározott rosszhiszemű magatartásuk alapján menthetők fel, s csak a kinevezésükre is vonatkozó eljárás keretében. Ezek a sajátos megoldások, mérsékelve a politikai befolyást és nyomást, biztosítják a felügyelő szervek magas szintű függetlenségét. Más tagállamokban (pl. Írországban) viszont a kormány közvetlenül eltávolíthatja hivatalukból az adatvédelmi biztosokat, ami aggodalomra ad okot a

---

<sup>52</sup> Mazák főtanácsnok véleménye, Case C-518/07, Commission of the European Communities v Germany (2009. október 22.). A Bizottság ezt az eljárást Németország ellen azért kezdeményezte az EU adatvédelmi irányelve helytelen, a magánszektor felügyelő adatvédelmi hatóságokra vonatkozó rendelkezése áttünetese miatt (a függetlenség hiánya). Az Európai Bíróság (Nagytanács) a C-518/07 ügyben 2010. március 9-én kelt ítélete 18. és 19. pontja szerint: „Tekintettel elsősorban a 96/46 irányelv 28. cikk (1) bekezdés második mondatára, mivel a „teljes függetlenség”-et az irányelv nem határozza meg, szokásos jelentését kell figyelembe venni. Egy hatóságra nézve a ’függetlenség’ fogalma általában olyan helyzetet jelent, amely biztosítja, hogy az érintett szerv teljes szabadságban cselekedhet, semmiféle módon nem utasítható vagy helyezhető bármiféle nyomás alá. A Német Szövetségi Köztársaság álláspontjával ellentétben semmi nem jelzi, hogy a függetlenségi követelmény kizárólag a felügyelő hatóságok és a felügyelt szervek közti viszonyra vonatkozik. Ellenkezőleg, a ’függetlenség’ fogalma kiegészül a „teljes” jelzővel, amely magában foglalja, hogy a döntéshozás hatásköre független a felügyelő hatóság bármiféle közvetlen vagy közvetett külső befolyásolásától.”

<sup>53</sup> Az Egyesült Királyságban a parlamentnek tanácsadó szerepe van, és a kiválasztott jelölt közmeghallgatására kinevezését megelőzően a Justice Select Committee (igazságügyi jelölőbizottság) előtt kerül sor. A bizottság véleménye ugyan kötelezettséggel nem bír, de a kinevezést megelőzően általában figyelembe veszik.



felügyelő szerv tényleges függetlenségét illetően, különösen a kormányzati szervek adatvédelmi jogszabályoknak megfelelő tevékenységének nyomon követése során.

A felügyelő szerv autonómiája különösen erős, ha, mint Portugáliában és Görögországban, egy, az adatvédelmi jogszabályok tiszteletben tartását felügyelő független hatóság létesítéséről és megszüntetéséről az alkotmány kifejezetten rendelkezik. Az intézményi függetlenség egyéb jelentős garanciáját nyújtja, ha az adatvédelmi hatóságot megkülönböztetett jogi személyiséggel ruházzák fel (pl. Spanyolországban, és Görögországban), vagy ha lehetősége van az alkotmánybíróságnál jogi eljárást kezdeményezni (pl. Szlovénia).

#### 4.1.2 Anyagi források

Az EU legtöbb tagállamában az adatvédelmi hatóságok a működésükhöz szükséges anyagi forrásukat az állami költségvetésből kapják (pl. Olaszországban, Franciaországban, Hollandiában, Észtországban), és gyakran az igazságügyi minisztérium költségvetéséből. Néhány tagállamban viszont a felügyelő hatóságok jelentősen növelhetik anyagi forrásaikat az adatfeldolgozó nyilvántartásba vételéből származó bevételek révén és/vagy az adatvédelmi jogszabályok megsértéséért büntetésként kirótt pénzbírságokból (pl. Luxemburgban, Máltában). Az Egyesült Királyságban a nyilvántartásba vétel díja a felügyelő hatóság adatvédelmi tevékenységének egyetlen bevételi forrása.

Számos tagállam (pl. Ausztria, Olaszország, Románia, Franciaország, Portugália) esetében a felügyelő hatóságok megfelelő finanszírozásának hiányának problémáját hangsúlyozták az országtanulmányok. Egyéb országokban, ahol az adatvédelmi hatóságok finanszírozása jelenleg aránylag jó, a következő években költségvetési megszorításokkal kell számolni (pl. Írországban, Dániában). Minthogy az adatvédelmi hatóságok feladatait mind az EU, mind a nemzeti jogrend meghatározza, a kielégítő emberi és anyagi erőforrások hiánya jelentős próbatétel a nemzeti felügyeleti rendszerek hatékonyságára nézve, ami veszélyeztetheti az érintettek alapvető jogainak védelmét. Ezért a tagállamoknak gondoskodni kell arról, hogy a nemzeti adatvédelmi hatóságok megfelelő működéséhez elegendő anyagi forrást nyújtsanak.

#### 4.1.3 Hatáskör

Az EU tagállamok kötelessége, hogy adatvédelmi hatóságaiknak megadják az adatvédelmi irányelv 28. cikk (2) bekezdésben rögzített általános hatásköröket (konzultáció a felügyelő hatóságokkal a személyes adatok feldolgozása vonatkozásában az egyének jogainak és szabadságainak védelmére vonatkozó közigazgatási intézkedések vagy rendeletek kidolgozásakor), továbbá a 28. cikk (3) bekezdésben meghatározott jogosultságokat (vizsgálati jogkör, beavatkozási jogosultság, bírósági eljárásban való részvétel joga), valamint a 28. cikk (4) bekezdésben előírt jogot (kérelmek fogadása). Mint a fenti áttekintésből kiviláglik, az adatvédelmi irányelv e rendelkezéseit teljességükben nem minden tagállam ültette át, mely helyzetben egyes nemzeti hatóságok felügyeleti feladataik ellátására csak korlátozott eszközökkel rendelkeznek. E problémát az érintett országoknak kezelniük kell.

A különféle nemzeti adatvédelmi hatóságok hatáskörét elemezve általánosságban két uralkodó tendenciát különböztethetünk meg, melyeket a tagállamok az adatvédelmi irányelv átültetésében követtek. Több tagállam (pl. Finnország, Svédország, Írország, Egyesült Királyság) a felügyelő ügynökségek megelőző és kezdeményező szerepét hangsúlyozták, kiemelve *ex-ante* szerepüket a személyes adatok védelmének biztosításában, más tagállamok (pl. Lettország, Cseh Köztársaság, Görögország) elsőbbséget adott az adatvédelmi hatóságok *ex-post facto* végrehajtó és ellenőrző funkciójának, és reaktív kötelezettséget rótt rájuk az adatvédelmi jogszabályok tiszteletben tartásának felügyelete tekintetében. A felügyelő szervekre bízott hatáskörök természete ezért ennek megfelelően változatos, azokat elsősorban

a 'puha' megelőző eszközök, másodsorban a 'keményebb' eszközök jellemzik. Mindazonáltal ezeket a különbségeket nem szabad túlhangsúlyozni, vannak ugyanis országok (pl. Dánia, Hollandia, Szlovénia), melyek eszközei e két szélső között helyezkednek el, felhatalmazván adatvédelmi hatóságukat arra, hogy segítsék és biztosítsák az adatvédelmi jogszabályoknak való aktív megfelelést, egyidejűleg megadván számukra a jogsértések üldözésének és büntetésének jogát. Mi több, az országok közti különbségeken túl számos közös vonás is megfigyelhető, mint az a következő négy alfejezetből kiviláglik.

#### **4.1.3.1 Vizsgálati jogkör**

Az adatvédelmi irányelv 28. cikk (3) bekezdés első albekezdése értelmében a felügyelő hatóságoknak vizsgálati jogkörrel kell rendelkezniük, amely felöleli az adatfeldolgozási műveletek tárgyát képező adatokhoz való hozzáférés jogát, továbbá a felügyeleti feladatok ellátásához szükséges adatok gyűjtésének jogát. A következő 1. táblázat áttekinti az adatvédelmi hatóságokra vonatkozó fent említett rendelkezések átültetését a belföldi jogba, bemutatván, rendelkeznek-e az adatvédelmi hatóságok következő jogosultságokkal: a) igényelhetnek-e az adatok feldolgozójától, kezelőjétől, érintettjétől információt vagy dokumentumot; b) hozzáférhetnek-e az adatfeldolgozó vagy az adatkezelő adatbankjaihoz és nyilvántartási rendszerihez; c) végezhetnek-e házkutatást és hajthatnak-e végre lefoglalást az adatfeldolgozó vagy adatkezelő helyiségeiben végzés nélkül; d) végezhetnek-e házkutatást és hajthatnak-e végre lefoglalást az adatfeldolgozó vagy adatkezelő helyiségeiben végzést követően; e) végezhetnek-e auditot annak ellenőrzésére, hogy az adatfeldolgozó vagy adatkezelő tiszteletben tartja-e a jogszabályokat, és annak biztosítására, hogy az adatfeldolgozást azokkal megfelelő összhangban végzi.

1. táblázat  
Vizsgálati jogkörök

tagállam	Információ és dokumentumok igénylése	Hozzáférés adatbankokhoz és nyilvántartási rendszerekhez	Házkutatás és lefoglalás bírósági végzés nélkül	Házkutatás és lefoglalás bírósági végzéssel	Audit végzése
Bulgária	X	X	X		X
Belgium	X	X	X		X
Cseh Köztársaság	X	X	X		X
Dánia	X	X	X		X
Németország	X	X	X	X <sup>54</sup>	X
Észtország	X	X	X		X
Görögország	X	X	X		X
Spanyolország	X	X	X		X
Franciaország	X	X		X	X
Írország	X	X	X		X
Olaszország	X	X	X <sup>55</sup>	X	X
Ciprus	X	X	X		X
Lettország	X	X	X		X
Litvánia	X	X	X		X
Luxemburg	X	X	X		X
Magyarország	X	X	X		X
Málta	X	X		X	X
Hollandia	X	X	X		X
Ausztria	X	X	X		X
Lengyelország	X	X	X		X
Portugália	X	X	X		X
Románia	X	X			X
Szlovénia	X	X	X		X
Szlovákia	X	X	X		X
Finnország	X	X	X		X
Svédország	X	X	X		X
Egyesült Királyság	X			X	X <sup>56</sup>

Amint azt az 1. táblázat mutatja, a tagállamok adatvédelmi ügynökségei túlnyomó többsége felügyelheti, hogy az adatfeldolgozást végző magán- vagy közjogi személy tiszteletben tartja-e az adatvédelmi jogszabályokat, sőt auditálhatja az érintett feleket, vizsgálatot végezhet,

<sup>54</sup> Ezek az adatok a szövetségi adatvédelmi biztosra vonatkoznak. Nem vonatkoznak a tartományi adatvédelmi biztosokra és a magánszférát felügyelő hatóságokra.

<sup>55</sup> Bírósági végzésre Olaszországban általában nincs szükség, ha a házkutatást egy személy otthonában vagy egy másik magánlakásban e személy hozzájárulásával végzik. Ellenkező esetben a bíró felhatalmazására van szükség.

<sup>56</sup> Az Egyesült Királyság adatvédelmi hatósága csak az adatkezelő kérelmére hajthat végre auditot, kívánsága ellenére nem. A jogkör ezért nem alkalmas a jogszabályok tiszteletben tartása ellenőrzésére.

elrendelheti információ átadását; elrendelheti a működéssel kapcsolatos adatok és dokumentumokhoz való hozzáférést; és az adatokról és dokumentumokról másolatot készíthet. Ezek a jogkörök *proprio motu* vagy annak az érintettnek a kérelmére vagy kívánságára gyakorolhatók, akinek személyes adataihoz fűződő jogait állítása szerint megsértették. A tagállamok túlnyomó többségében az adatvédelmi hatóságok jogkörük gyakorlása során vagy az adatvédelmi jogszabályok megsértése felfedésének céljából beléphetnek (szükség esetén rendőri segítséggel) azokba a helyiségekbe és bármely más helyre, ahol adatfeldolgozást végeznek, lefoglalhatják az ahhoz szükséges berendezéseket, vizsgálatot végezhetnek és bizonyítékokat vehetnek fel (még az adatkezelő hozzájárulása hiányában is) anélkül, hogy előzetesen bírósági végzés igénylésére lenne szükség.

#### **4.1.3.2 Beavatkozási jogkör**

Az adatvédelmi irányelv 28. cikk (3) bekezdése második albekezdése szerint az adatvédelmi szerveknek beavatkozási jogkörrel kell rendelkezniük, felölve többek között a különleges adatokon végzett feldolgozási műveletek megkezdése előtti véleményezés jogát, e vélemények megfelelő közzétételének biztosítását, az adatok zárolásának, törlésének vagy megsemmisítésének elrendelését, az adatfeldolgozás átmeneti vagy végleges tilalmát, az adatkezelő figyelmeztetését vagy megrovását. A következő 2. táblázat áttekinti az adatvédelmi hatóságokra vonatkozó fent említett rendelkezések átültetését a belföldi jogba, bemutatván, rendelkeznek-e az adatvédelmi hatóságok következő jogosultságokkal: a) az adatkezelő által bejelentett feldolgozási műveletek nyilvántartásba vétele; b) olyan feldolgozási műveletek engedélyezése az adatvédelmi jogszabályok követelményeinek való megfelelés előzetes megvizsgálását követően, amelyek külön kockázatot jelenthetnek az érintettek jogaira és szabadságaira nézve; c) a személyes adatok feldolgozásának leállítását; d) az adatok törlésének vagy megsemmisítésének elrendelése; e) az adatkezelő figyelmeztetése vagy megrovása (elrendelve pl. sajátos technikai és szervezési intézkedések megtételét a vonatkozó jogszabály megsértésének megelőzése érdekében).

## 2. táblázat

## Beavatkozási jogkörök

tagállam	Feldolgozási műveletek nyilvántartásba vétele	Különösen kockázatos feldolgozási műveletek engedélyezése	Feldolgozási műveletek leállítása	Adatok törlésének vagy megsemmisítésének elrendelése	Az adatkezelő figyelmeztetése vagy megrovása
Bulgária	X	X	X	X	X
Belgium	X	X			
Cseh Köztársaság	X	X	X	X	X
Dánia	X	X	X	X	X
Németország	X	X	X <sup>57</sup>		X
Észtország	X	X	X	X	X
Görögország	X	X	X	X	X
Spanyolország	X		X	X	X
Franciaország	X	X	X	X	X
Írország	X	X	X	X	X
Olaszország	X	X	X	X	X
Ciprus	X		X	X	X
Lettország	X		X	X	X
Litvánia	X	X	X	X	X
Luxemburg	X	X	X	X	X
Magyarország	X	X	X	X	X
Málta	X	X	X	X	X
Hollandia	X	X	X	X	X
Ausztria	X	X	X	X	X
Lengyelország	X	X	X	X	X
Portugália	X	X	X	X	X
Románia	X	X	X	X	X
Szlovénia	X	X	X	X	X
Szlovákia	X	X	X	X	X
Finnország	X	X	X	X	X
Svédország	X	X	X		X
Egyesült Királyság	X		X	X	X

<sup>57</sup> 2009 szeptember 1-jétől a felügyelő hatóságok, bizonyos feltételek mellett, jogosultak a feldolgozási műveletek leállítására.

A 2. táblázat a beavatkozási jogkör tekintetében az EU tagállamok adatvédelmi hatóságai bizonyos konvergenciáját mutatja. Néhány, a különleges adatok feldolgozási műveletei előzetes ellenőrzését illető kivétellel, melyről *de jure* vagy *de facto* egyes országokban nem rendelkeztek, a bejelentett adatfeldolgozási műveletekről minden felügyelő szervnek nyilvántartást kell vezetnie. Belgium és részben Németország kivételével elrendelhetik, hogy a magánjogi adatkezelő hagyja abba a jogsértő feldolgozási műveletek végzését, és helyesbítsen, töröljön, vagy zároljon egyes, ily módon feldolgozott adatokat; megtilthatják, hogy a magánjogi adatkezelő sajátos adatfeldolgozási eljárásokat alkalmazzon, ha jelentős a kockázata annak, hogy az adatok feldolgozása a vonatkozó jogszabályokat sérti; elrendelhetik, hogy a magánjogi adatkezelő sajátos technikai és szervezési biztonsági intézkedéseket foganatosítson az adatok jogellenes feldolgozása, az adatok esetleges vagy jogellenes megsemmisítése vagy megváltoztatása, az adatokkal való visszaélés vagy egyéb jogellenes módon való feldolgozás megelőzése érdekében; végül tiltó értesítést vagy egy kötelező érvényű végzést bocsáthatnak ki, ha az adatkezelő sérti a vonatkozó jogszabályokat.<sup>58</sup>

#### **4.1.3.3 Jogkörök kérelmek fogadására és bírósági eljárásokban való részvételre**

Az adatvédelmi irányelv 28. cikk (4) bekezdés első mondata értelmében a felügyelő hatóságokat fel kell hatalmazni arra, hogy foglalkozzanak a személyes adatok feldolgozása vonatkozásában az egyének jogainak vagy szabadságainak védelmével kapcsolatos, bármely személy vagy az őt képviselő szervezet által benyújtott kérelmekkel, s hogy a kérelem elbírálásáról az érintett személyt értesítsék. A 28. cikk (3) bekezdése harmadik albekezdése szerint az adatvédelmi hatóságok a nemzeti rendelkezések megsértése esetén részt vehetnek bírósági eljárásokban, és e jogsértéseket igazságszolgáltatási hatóságok elé terjeszthetik. Végül a 28. cikk (3) bekezdés második albekezdése szerint az ügyet a nemzeti parlament vagy más politikai intézmény elé terjeszthetik. A következő 3. táblázat áttekinti az adatvédelmi hatóságokra vonatkozó fent említett rendelkezések átültetését a belföldi jogba, bemutatóan, rendelkeznek-e az adatvédelmi hatóságok következő jogosultságokkal: a) az érintett kérelmeinek és panaszainak fogadása és kivizsgálása; b) a rendőrség vagy az igazságszolgáltatási hatóságok tájékoztatása az ügyről; c) az ügynek közvetlenül az igazságszolgáltatási hatóságok elé terjesztése, a kérelemhez félként csatlakozva (vagyis *stricto sensu* részvétel bírósági eljárásban); d) saját jogon eldönthetik, történt-e jogsértés vagy nem (szankció alkalmazásának lehetőségével), ily módon kvázi-igazságszolgáltatási funkciót látva el; e) az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése, javaslatot téve különösen a vonatkozó adatvédelmi jogszabályok módosítását célzó törvényalkotó vagy szabályozó intézkedésekre, válaszul a végrehajtásukból adódó sürgető problémákra és a számítógépi feldolgozási technikák fejlődésére.

---

<sup>58</sup> Ez a megállapítás a tartományi adatvédelmi biztosok és/vagy felügyelő hatóságok magánszférára korlátozott illetékességére vonatkozik, a szövetségi adatvédelmi biztosra nem.

### 3. táblázat

#### Jogkörök kérelmek fogadására és bírósági eljárásokban való részvételre

tagállam	Kérelmek és panaszok fogadása és kivizsgálása	A rendőrség vagy az igazságszolgáltatási hatóságok tájékoztatása	Az ügynek közvetlenül az igazságszolgáltatási hatóságok elé terjesztése	Döntés saját jogon a kérelem érdeméről	Az ügy nemzeti parlament elé terjesztése
Bulgária	X	X	X	X	
Belgium	X	X	X	X	X
Cseh Köztársaság	X	X	X	X	
Dánia	X	X		X	
Németország	X	X	X <sup>59</sup>	X <sup>60</sup>	X
Észtország	X			X	X
Görögország	X	X		X	X
Spanyolország	X	X		X	X
Franciaország	X	X		X	X
Írország	X		X		
Olaszország	X	X		X	X
Ciprus	X	X		X	
Lettország	X		X	X	
Litvánia	X	X		X	X
Luxemburg	X	X	X	X	
Magyarország	X	X			X
Málta	X	X	X	X	X
Hollandia	X	X		X	
Ausztria	X		X	X	
Lengyelország	X	X		X	
Portugália	X	X		X	
Románia	X	X	X	X	
Szlovénia	X	X	X	X	
Szlovákia	X	X		X	X
Finnország	X	X	X	X	X
Svédország	X	X	X		
Egyesült Királyság	X	X			

<sup>59</sup> Ez az adat nem a szövetségi adatvédelmi biztosra, hanem a tartományok adatvédelmi hatóságaira vonatkozik.

<sup>60</sup> Ez az adat nem a szövetségi adatvédelmi biztosra, hanem a tartományok adatvédelmi hatóságaira vonatkozik.

A táblázat rámutat néhány eltérésre az EU tagállamok adatvédelmi hatóságai között. Minden felügyelő szerv fel van hatalmazva érdekelt felek panaszai fogadására, melyek állítása szerint személyes adataihoz fűződő jogait megsértették, és ennek megfelelően kötelességük a kérelmezőknek záros határidőn belül választ adni. Mindazonáltal, ha a vizsgálat végeztével a kérelem megalapozottnak tűnik, csak néhány adatvédelmi hatóság kezdeményezhet önálló jogi eljárást az illetékes ítélőszéknél (nevezetesen még az alkotmánybíróságnál is, mint Szlovénia esetében) vagy gyakorolhat kvázi-igazságszolgáltatási funkciót, döntvén a panaszos ügyének érdekében (mint az igazságszolgáltatási hatóságok alternatív fóruma). A kvázi-igazságszolgáltatási jogkörrel rendelkező adminisztratív felügyelőszervek határozatát bármely ügyben mindenkor felülvizsgálhatják a rendes bíróságok, ami az adatvédelmi irányelv 28. cikk (3) bekezdés 2. albekezdésben előírt jogi szabályozás szükséges velejárója.

#### **4.1.3.4 Konzultációs jogkörök**

Az adatvédelmi irányelv 28. cikk (2) bekezdése szerint a nemzeti jogalkotó és közigazgatási szerveknek a személyes adatok feldolgozása vonatkozásában az egyének jogainak és szabadságainak védelmére vonatkozó közigazgatási intézkedések vagy rendeletek kidolgozásakor a felügyelő hatóságokkal konzultálniuk kell. Az adatvédelmi hatóságok általános feladata, mely szerint adatfeldolgozási műveleteket végző magánjogi feleknek tanáccsal és információval szolgál, továbbá ágazat-specifikus ajánlásokat bocsát ki, az adatvédelmi irányelv céljaiból levezethető. Végül az adatvédelmi irányelv 25. cikke különös szabályokat rögzít a személyes adatok nem EU tagállamokba (vagyis harmadik országokba) irányuló továbbítására vonatkozóan. A következő 4. táblázat tájékoztatást nyújt a nemzeti adatvédelmi hatóságok konzultációs jogköreiről, bemutatóan, rendelkeznek-e az adatvédelmi hatóságok következő jogosultságokkal: a) a jogalkotó és/vagy a közigazgatási szervek *de jure* vagy *de facto* ténylegesen és minden esetben megkérlik-e véleményüket adatvédelemmel kapcsolatos egyéni jogokat érintő törvények vagy rendeletek elfogadását megelőzően; b) a jogalkotó és/vagy közigazgatási szervek, ha úgy döntenek, megkérhetik-e véleményüket adatvédelemmel kapcsolatos egyéni jogokat érintő törvények vagy rendeletek elfogadását megelőzően; c) nyújthatnak-e tanácsot vagy tájékoztatást a feleknek (pl. jogait és kötelezettségeiket illetően); bocsáthatnak-e ki általános ajánlásokat és véleményeket az adatvédelmi jogszabályok ágazat-specifikus alkalmazásának és betartásának fokozása érdekében (pl. magatartási kódexek kidolgozásának elősegítése); e) adhatnak-e felhatalmazást személyes adatok harmadik országokba irányuló továbbítására.



#### 4. táblázat

##### Konzultációs jogkörök

tagállam	Véleményüket a törvényhozásnak vagy közig. szerveknek meg kell kérniük	Véleményüket a törvényhozás vagy közig. szervek megkérhetik	Nyújthatnak-e tanácsot vagy tájékoztatást a feleknek	Bocsáthatnak-e ki általános ajánlásokat és véleményeket	Adhatnak-e felhatalmazást adatok harmadik országokba irányuló továbbítására
Bulgária	X		X	X	
Belgium	X	X	X	X	
Cseh Köztársaság		X	X	X	
Dánia		X		X	
Németország	X	X	X	X	X <sup>61</sup>
Észtország	X		X	X	
Görögország	X	X	X	X	X
Spanyolország	X		X	X	X
Franciaország	X	X	X	X	X
Írország		X	X	X	X
Olaszország	X	X	X	X	X
Ciprus	X <sup>62</sup>		X	X	X
Lettország	X		X	X	
Litvánia		X	X	X	X
Luxemburg	X		X	X	X
Magyarország		X	X	X	X <sup>63</sup>
Málta		X	X	X	X
Hollandia	X		X	X	X
Ausztria	X		X	X	X
Lengyelország		X	X	X	
Portugália	X		X	X	X
Románia		X	X	X	X
Szlovénia		X <sup>64</sup> IX	X	X	X
Szlovákia		X	X	X	X
Finnország	X	X	X	X	
Svédország	X	X	X	X	X
Egyesült		X	X	X	X <sup>65</sup> X

<sup>61</sup> A német felügyelő szervek adhatnak felhatalmazást, de az nem minden esetben kötelező vagy szükséges.

<sup>62</sup> A ciprusi adatvédelmi hatóság értelmezése szerint a 138(I)/2001 törvény 23(i) szakasza feljogosítja őt a konzultációra a jogszabály előkészítése folyamán. A gyakorlatban a jogalkotó és a közigazgatás személyes adatok védelme tárgyában mindig megkéri véleményét.

<sup>63</sup> Egyes jelek azt mutatják, hogy ezt a jogkört csorbítja a hatékony alkalmazás hiánya.

<sup>64</sup> SK-ban az adatvédelmi hatóság véleményét egy, adatvédelmet érintő jogszabály elfogadását megelőzően *de facto* minden esetben megkérlik, bár erre nincs törvényi kötelezés.

<sup>65</sup> A gyakorlatban ezzel a jogkörrel ritkán élnek, ha egyáltalán. Lásd national thematic study on assessment of data protection measures and relevant institutions, UK, hozzáférés: <http://fra.europa.eu> (2010.02.24.).

Királyság					
-----------	--	--	--	--	--

Amint azt a 4. táblázat mutatja, minden tagállam felhatalmazta belföldi felügyelő ügynökségét arra, hogy tanácsot adjon magánjogi feleknek az adatvédelmi jogszabályok alkalmazását illetően. Az adatvédelmi hatóságoknak kvázi-jogalkotó hatáskörük is van általános, szektor-specifikus szabályok megállapítására, magánjogi felek magatartási kódexei kidolgozásának elősegítésére, és véleményezésre vagy ajánlás kibocsátására az adatfeldolgozás területén működő köz- és magánjogi szereplők részére. Ezeknek az intézkedéseknek azonban jogi kötelező ereje általában nincsen. Ugyanakkor sok tagállam csak konzultatív funkciót rendel a felügyelő szervekhez, melynek keretében tanáccsal szolgálhat a végrehajtó és jogalkotó szerveknek a személyes adatokat érintő jogszabályok előkészítése során. A törvény- és rendelettervezetekkel kapcsolatos tanácsadás opcionális, vagy (mint Franciaország, Olaszország, Németország, Ausztria, Görögország esetében) szigorú jogszabályi kötelezettség csak a végrehajtási rendeletek kidolgozására vonatkozik. Az adatvédelmi hatóságoknak a személyes adatok védelmére potenciálisan negatív hatást gyakoroló jogszabály vagy útmutatás elfogadását megelőző véleményezési jogkörének hiánya jelezheti, hogy a politikai döntéshozás során elmulasztották a magánélet védelmének maradéktalan értékelését. Javasolható tehát, hogy a tagállamok biztosítsák a felügyelő szervek konzisztens részvételét a politikai döntéshozásban.

#### *4.1.4 Tevékenységek*

Az EU tagállamok felügyelő hatóságai rendszerint számos olyan tevékenységet végeznek, amelyek a magánélettel kapcsolatos nemzeti jogszabályokra, valamint a személyes adatok védelme kultúrájának terjesztésére irányul. Először is az adatvédelmi hatóságok tájékoztatják a közvéleményt és az állami intézményeket a magánülethez fűződő jogokkal kapcsolatos kihívásokról, a felügyelő szervnek e kihívásokra válaszoló intézkedéseiről, és védelmük fejlesztéséhez szükséges lépésekről. Az adatvédelmi irányelv 28. cikk (5) bekezdése kötelezi a felügyelő szerveket, hogy tevékenységükről rendszeresen jelentést készítsenek, s azt nyilvánosságra hozzák. Ezért minden adatvédelmi hatóság éves jelentést tesz közzé a magánülethez fűződő jogok védelmének a belföldi jogrendszerben tükröződő helyzetéről, egyes országok (pl. Olaszország) havi hírlevelet ad ki, amely a legfrissebb döntéseket és elfogadott jogszabályokat tartalmazza. Egyes országokban (pl. Spanyolországban, az Egyesült Királyságban, Olaszországban) az éves jelentést közzéteszik, olykor bemutatják a jogalkotónak, alkalmat adva a médiának arra, hogy az eseményről beszámoljon.

A nemzeti felügyelő hatóságuk különleges feladata a magánülethez és a személyes adatokhoz fűződő jogok tudatosságának fokozása az EU polgárainak körében. Ez a tevékenység felettébb fontos, hiszen az adatvédelmi jogszabályok hatékonysága csak akkor biztosítható, ha az egyének tudatában vannak alapvető jogaiknak, és tevékenyen részt vesznek érvényesítésükben. Amint azt alább elemezzük, a nagyközönség számos tagállamban vagy nagymértékben tudatlan saját jogait illetően, (pl. Lengyelországban, Máltában), vagy úgy véli, a magánülethez fűződő jogok védelme jó, s a rendszer fejlesztésére csekély mértékben van szükség (pl. Dániában, Finnországban), vagy úgy tartja, egyéb jogok, mint a jog az információhoz nagyobb súllyal esnek latba, mint az adatvédelmi jogok (pl. Svédországban). Az adatvédelmi hatóság ezért tevékeny részt vállalnak a tudatosság fokozásában. Néhány kivételtől eltekintve (pl. Litvánia, Bulgária, Szlovákia) szakosított felhasználóbarát honlapot működtetnek, ahol minden vonatkozó jogszabály, s az ügynökség véleményei és döntései megtalálhatók, és folyamatosan frissítik őket. A felügyelő szervek sok országban a népesség egy-egy szelete számára konferenciákat, kezdeményezéseket és szakmai programokat

finanszíroznak, megcélózván pl. egyetemi hallgatókat vagy munkavállalókat (pl. Szlovéniában, Hollandiában).

Az EU szintjén a nemzeti felügyelő hatóságok együttműködnek egymással és közösen dolgoznak a személyes adat-feldolgozás vonatkozásában az egyének védelmével foglalkozó munkacsoport keretében, amely az adatvédelmi irányelv 29. cikk (1) bekezdése első mondata alapján jött létre (ismert elnevezése: 29-es munkacsoport). A 29. cikk (2) bekezdés értelmében a munkacsoport tagjai az európai adatvédelmi biztos, a tagállamok nemzeti felügyelő hatóságai egy-egy képviselője és a Bizottság egy képviselője. A munkacsoport tanácsadói státusszal rendelkezik, tevékenységét függetlenül végzi. A 30. cikk (1) bekezdés szerint megvizsgál minden, az irányelv értelmében elfogadott nemzeti intézkedés alkalmazása körébe tartozó kérdést azok egységes alkalmazása érdekében; véleményt nyilvánít a Bizottság felé az EU és a harmadik országok védelmének szintjéről; tanácsot ad a Bizottságnak az ezen irányelv javasolt módosításaival, a személyes adatok feldolgozása tekintetében a természetes személyek jogainak és szabadságainak biztosítását célzó további vagy különleges intézkedésekkel, és az e jogokat és szabadságokat érintő, egyéb javasolt EU intézkedésekkel kapcsolatban; véleményt nyilvánít az EU szinten kidolgozott eljárási szabályzatokról. A munkacsoport véleményeit és ajánlásait nemzeti adatvédelmi hatóságok rendszerint figyelembe veszik, azokra hivatkoznak, és különösen hasznosak a személyes adatok védelmét érintő EU szabályok fejlesztésében, hiszen azok minden nemzeti felügyelő szerve egységesen vonatkoznak.<sup>66</sup>

## 4.2 Megfelelőség

Ebben a részben összehasonlító áttekintést nyújtunk. A helyes gyakorlatot ezzel összefüggésben mutatjuk be alább, a 6.2 részben.

### 4.2.1 Az adatvédelmi nyilvántartás és a nyilvántartásba vételi eljárás

Az adatvédelmi irányelv 2. cikke értelmében a 'személyes adatok feldolgozása' ('feldolgozás') a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés. Az adatvédelmi irányelv 5 – 8. cikke részletezi a személyes adatok feldolgozása jogszerűségének általános szabályait és elveit, az adatfeldolgozás törvényes voltának követelményeit és ezen adatok feldolgozásának különleges fajtáit. Ezzel összefüggésben a 18 – 20. cikk elrendeli a felügyelő hatóság értesítésének kötelezettségét, továbbá azoknak az adatfeldolgozási műveleteknek az előzetes ellenőrzését, amelyek külön kockázatot jelenthetnek az érintettek jogaira és szabadságaira nézve.

A nemzeti tematikus tanulmányok részletesen értékelik az olyan adatvédelmi normáknak való megfelelést, mint az adatvédelmi nyilvántartásra és a nyilvántartásba vételre vonatkozó szabályok. E tanulmányok nagy többsége tartalmazta a nyilvántartásba vételre irányuló és az elfogadott bejegyzési kérelmek számára vonatkozó adatokat a 2000 – 2007. időszakban. Néhányuk ezen és az érintett nemzeti hatóságoktól származó adatok alapján elemzést és

---

<sup>66</sup> Az egyesült Királyságban a munkacsoport véleményeit és ajánlásait az adatvédelmi hatóságok nem tekintik kötelezőnek, jóllehet olykor azokra mint informális útmutatásra hivatkoznak.

kvalitatív értékelést is tartalmazott. Ezek az adatok indikátorul szolgáltak a megfelelés értékeléséhez. Egyéb indikátorok felölelik a nemzeti hatóságok gyakorlatát, a nemzeti jogszabályoknak való megfelelés fokát és az irányelvnek való meg nem felelés tipizált eseteit. Az EU tagállamok többsége (Bulgária, Litvánia, Ausztria, Írország, Finnország, Dánia, Svédország, Luxemburg, Cseh Köztársaság, Spanyolország, Olaszország, Málta, Hollandia, Lengyelország, Románia, Szlovénia, Ciprus, Észtország, Görögország, Portugália, Lettország és Németország) kidolgozta azt a jogi keretet, amely hatékonyan átülteti az adatvédelmi irányelv előírásait. Hatékony átültetésen azt értjük, hogy a nemzeti jogszabályok *prima facie* megfelelnek az irányelv követelményeinek. A nemzeti jogszabályok tényleges megfelelésének hatékonysága az egyes tagállamokban eltérő, és az alább olvasható elemzés tárgyát képezi. Másrészt öt tagállam (Franciaország, Magyarország, Szlovákia, Egyesült Királyság és Belgium) jogszabályai hiányosságokról árulkodnak, amely az adatvédelmi irányelv és a nemzeti rendelkezések közti ellentmondásokra utal. A megfelelés értékelése azonban felettébb problematikus. Több esetben a nemzeti AVH-k alacsony létszáma azzal jár, hogy képtelenek a terület helyzetének szisztematikus és statisztikai számbavételére. Még ha ilyen statisztikai adatokkal rendelkeznek is, azok nem mindig helytállóak és elegendők a helyzet megfelelő számbavételéhez. Ezért lehetetlen volt a megfelelés fokának aggregált, EU szintű és átfogó értékelése, és/vagy a jog vagy a gyakorlat problematikus területeinek feltárása. Ebből a felettébb zavaros képből, a feltárt problémák némelyikének bemutatására a nemzeti tematikus tanulmányokból az irányelvnek való megfelelés nyilvánvaló hiányosságait emeltük ki.

Bulgária átültette az adatvédelmi irányelv vonatkozó rendelkezéseit, de a személyes adatok kezelői nyilvántartásba vételének gyakorlata azt mutatja, hogy a nemzeti hatóság létrejötté óta nem készítette fel adminisztratív kapacitását e kötelezettség megfelelő ellátásra.<sup>67</sup> A nemzeti hatóság még mindig képtelen hatékonyan kezelni a nagyszámú nyilvántartásba vételi kérelmet. A nyilvántartásba vételi kérelmek száma aránytalan abban az értelemben, hogy a nyilvántartásba vételek száma a nyilvántartásba vételi kérelmek számához viszonyítva aránytalanul alacsony.<sup>68</sup>

Lengyelországban a nemzeti jogszabályok szerint minden, adatfeldolgozással foglalkozó személy köteles adatnyilvántartó rendszerét a nemzeti adathatóságnak bejelenteni, mely hatóság az állami szakszolgálatok (pl. hírszerző szolgálatok) által feldolgozott adatokat illetően korlátozott vizsgálati hatáskörrel rendelkezik. Még ha egy adatokat feldolgozó személy a nyilvántartásba vételre nem is köteles, köteles teljesíteni az adatok feldolgozására vonatkozó feltételeket. A különleges adatok feldolgozása mint főszabály tilos, kivéve azokat, amelyek főleg az adatvédelmi irányelv hatálya alá tartoznak. A feltárt fő probléma, hogy az adatokat feldolgozó személyek nincsenek tudatában nyilvántartásba vételi kötelezettségüknek. Ezek a személyek számos esetben elmulasztották adattároló rendszereik bejelentését a nyilvántartásba, ugyanakkor további hibák mutatkoznak a nyilvántartásba vétel szakaszában. Különleges adatok feldolgozása két jelentős esetben járt problémával. Az egyik roma gyerekek adatainak gyűjtésével kapcsolatos. Ez alkalommal a nemzeti hatóság elrendelte a roma gyerekeket érintő adatok törlését, melyeket tudomásuk és hozzájárulásuk nélkül

---

<sup>67</sup> 2003 decemberében a nemzeti hatóság négy alkalmazottjának 227 251 kérelemmel kellett szembenéznie. A Bulgár Köztársaság személyesadat-védelmi bizottságának éves jelentése (2002-2003), 11-12. oldal. Bulgár nyelven lásd <http://www.cdpd.bg/godishniotcheti.html> (2009.01.10.).

<sup>68</sup> 2006-ban például a kérelmek száma 274 446-ra emelkedett, a bejegyzések száma pedig 31 970-re. A Bulgár Köztársaság személyesadat-védelmi bizottságának éves jelentése (2005), 17. oldal. Bulgár nyelven lásd <http://www.cdpd.bg/godishniotcheti.html> (2009.01.10.).

dolgoztak fel.<sup>69</sup> A másik eset különféle nemzeti és etnikai kisebbségek által választásra jelölt személyek adatai feldolgozására vonatkozik. A nemzeti hatóság elrendelte a nem hivatalos forrásból, az érintett hozzájárulása nélkül szerzett adatok feldolgozásának felfüggesztését.<sup>70</sup> A nemzeti hatóság 2007. évi jelentése a közigazgatás egyes ágazataiban az adatvédelmi normáknak való megfelelés hiányát tárta fel.<sup>71</sup> A közbiztonsági ágazatban az adatvédelem területén különös hiányosságok nem mutatkoztak, intézményei, úgy tűnik, a jogszabályoknak megfelelnek. A különféle kereskedelmi területeken adatfeldolgozást folytató személyek, közegészségügyi intézmények, bankok és pénzügyi szervezetek nem teljesen felelnek meg a jogszabályoknak.

A görögországi jogszabályok kezdetben általános bejelentési kötelezettséget írtak elő, kiküszöbölve így a nyilvántartási és bejelentési eljárásokra alkalmazható, az adatvédelmi irányelvben rögzített kivételek és egyszerűsítések lehetőségét. A jogszabály későbbi módosítása bevezette a kivételek lehetőségét, amit a bejelentések számának drasztikus csökkenése követett. A görög jogalkotó nem élt az adatvédelmi irányelvnek a belső magánélet- vagy adatvédelmi felelős kinevezésére vonatkozó lehetőségével. A munkáltató–munkavállaló kapcsolatát jellemző erőviszonyok inherens aszimmetriája következtében a nemzeti hatóság elveti az egyén hozzájárulását mint olyan alapot, amely önmagában véve legitimizálja a személyes adatok feldolgozását.<sup>72</sup> Ami a nemzeti adatvédelmi hatóság határozatainak végrehajtását illeti, az adatkezelők az esetek nagy többségében annak nem tesznek eleget. Egyik ilyen súlyos eset, amely komoly aggodalomra adott okot és felháborodást váltott ki a nagyközönség körében, amikor a görög rendőrség zárláncú televíziós (CCTV) kamerákkal filmezett politikai demonstrációkat a nemzeti hatóság jogerős, a kamerák közterületi használatára vonatkozó határozata ellenére<sup>73</sup>, miközben az AVH rendelkezése az államtanács teljes ülése előtt feküdt.<sup>74</sup> Mi több, a hatóság ellenőreit, akiknek a hatóság határozata végrehajtását kellett volna megvizsgálniuk, nem engedték be a rendőrség helyiségeibe. A hatóság vezetője és legtöbb tagja ezt követően felajánlotta lemondását.

Ami az Egyesült Királyságot illeti, a hírek szerint az Európai Bizottság vizsgálatot indított, mert állítólag elmulasztották az irányelv harmincöt cikke közül tizenegynek, rendelkezései közel harmadának a megfelelő átültetését.<sup>75</sup> Ámbár a kormány azt állítja, hogy az irányelvet

---

<sup>69</sup> 2007. október 12-én kibocsátott döntés, lásd: GI-DEC-DOLiS-218/07/5787, 5788.

<sup>70</sup> 2007. november 23-án kibocsátott döntés, lásd: GI-DOLiS-430/103/07/6592.

<sup>71</sup> E hiányosságok: adattárolás nem megfelelő feltételek mellett, pl. polcokon és zár nélküli fiókokban; olyan IT rendszerek használata, melyek gyakorta nem teljesítik a jogszabályban előírt technikai követelményeket; elszigetelt esetekben olyan IT rendszerek használata, amely hozzáférést engedett adattárakhoz arra nem felhatalmazott személyeknek; közigazgatási eljárások során gyűjtött adatok felhasználása a meghatározott céltól eltérően; elszigetelt esetekben személyek adatainak közzététele az Interneten előzetes hozzájárulás nélkül.

<sup>72</sup> Ezt a felfogást az Európai Bizottság is magáévá tette a Possible content of a European framework on protection of workers' personal data, Brussels 2002. jelentésben (Munkavállalók személyes adatai feldolgozásának európai kerete lehetséges tartalma).

<sup>73</sup> A nemzeti adatvédelmi hatóság 58/2005. határozata (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα), [http://www.dpa.gr/portal/page?\\_pageid=33,15453&\\_dad=portal&\\_schema=PORTAL](http://www.dpa.gr/portal/page?_pageid=33,15453&_dad=portal&_schema=PORTAL) (2008.02.19.).

<sup>74</sup> A görög közrendvédelmi minisztérium az államtanácsnak a hatóság határozata megsemmisítését indítványozta.

<sup>75</sup> 'Európa azt állítja, hogy az Egyesült Királyság elrontotta az adatvédelmi irányelv harmadát', Out-Law News, 2007. szeptember 17, olvasható: <http://www.out-law.com/page-8472> (2009.01.26). Bár ez nem több, mint egy cikk a médiában, a cikk az érintett hatóságoktól az információszabadság törvénye alapján kapott információra épül, mind az Egyesült Királyság kormánya, mint a Bizottság megerősítette, hogy különféle, közelebbről nem meghatározott kérdések vita tárgyát képezték. Az Out-Law által szerzett információ szerint azonban a 2, 3, 8, 10, 11, 12, 13, 22, 23, 25, és 28. cikkek átültetése nem megfelelő.... Ezek a cikkek a következő kérdéseket szabályozzák: az irányelvben használt meghatározások (pl. a személyes adat értelmezése); az irányelv hatályának kiterjesztése a manuális adatállományokra; a különleges személyes adatok feldolgozásának feltételei;

teljes egészében átültette, számos hiányosságra derült fény.<sup>76</sup> Még inkább problematikus az adatvédelmi hatóságnak az a felfogása, mely szerint nem feladata annak biztosítása, hogy a nemzeti jogszabályok az EK irányelvvel összhangban értelmezze, vagy rámutasson, a nemzeti jogszabályok hol nem tesznek eleget az adatvédelmi irányelv követelményeinek.<sup>77</sup>

Németország mind szövetségi, mind tartományi szinten átültette az adatvédelmi irányelvet a belső jogba. Nem közigazgatási szervek kötelesek automatizált adatfeldolgozási műveleteiket megkezdésüket megelőzően bejelenteni a felügyelő hatóságnak vagy az illetékes adatvédelmi biztosnak. A Szövetség közigazgatási szervei ezeket a műveleteket a nemzeti hatóságnak jelentik be. A bejelentési kötelezettség nem vonatkozik arra az adatkezelőre, amely belső adatvédelmi felelőst nevezett ki. Úgy tűnik, a magánjogi társaságok jelentős része, bár az adatvédelmi felelős kinevezése törvényes kötelezettségük, e kötelezettségnek nem tesznek eleget, azok viszont, amelyek kötelezettségüknek megfelelően kineveznek adatvédelmi felelősöket, gyakorta nem támogatják a kinevezettek hatékony és tényleges munkáját. Az sem hagyható figyelmen kívül, hogy a közepes vállalkozásoknál még mindig számos adatvédelmi probléma merül fel. Tulajdonítható ez annak a ténynek, hogy a kinevezett adatvédelmi felelős, ha egyáltalán létezik, az őt erre felkészítő kiképzésre vagy feladatai megfelelő ellátására fordítható idő hiányában nem képes kezdeményezni a gyakorlat megváltoztatását. A közelmúlt botrányos, mind a magán-, mind a közjogi intézmények körében feltárt esetei az adat- és magánélet-védelem széleskörű és súlyos megsértésére mutattak.<sup>78</sup> Ezekben az esetekben, többek között, kikémlelve vagy videóval titkon megfigyelve az alkalmazottakat, vagy munkahelyén átkutatva az alkalmazottak számítógépesített profiljait súlyos sérelmet szenvedtek a magánélethez fűződő jogok. Más esetekben példátlan mennyiségű adattal

---

az egyén tájékoztatása a tisztességes adatfeldolgozás jegyében; az érintettet megillető jogok; kivételek e jogok köréből; az egyén lehetősége a jogorvoslatra jogsértés esetén; a szervezetek felelőssége az adatvédelmi jogszabályok megsértéséért; személyes adatok továbbítása az Európai Unión kívülre; az információs biztos hatáskörei.' (2010.11.18.)

<sup>76</sup> Pl. D. Korff (2008) 'UK Data Sharing: European Conflict' (Adatmegosztás az Egyesült Királyságban: európai konfliktus), in: Data Protection Law & Policy, 12. oldaltól). Egyéb kérdések is felmerültek a következő lábjegyzetben említett vizsgálódás során, valamint R. Thomas és M. Walport (2008) Data Sharing Review Report-jában (Jelentés az adatmegosztásról). Lásd <http://www.justice.gov.uk/docs/data-sharing-review-report.pdf> (2009.01.26.).

<sup>77</sup> Jonathan Bamford, az Információs Biztos helyettese a House of Commons Select Committee (az alsó ház jelölő bizottsága) az elektronikus betegrekordokat a nemzeti egészségügyi szolgálat kezdeményezésére tárgyaló meghallgatásán felvetett kérdésre 2007. májusában ezt a választ adta: 'Ha van bármi tennivaló, mint most, az EU adatvédelmi irányelvnek az Egyesült Királyság adatvédelmi törvényébe való megfelelő átültetése tekintetében, úgy ez az igazságügyi minisztérium dolga, mert ez az a szerv, amely felelős az irányelv átültetéséért a belső jogba. Ha ezzel kapcsolatban felmerült aggályokra az igazságügyi minisztériumnak kell választ adnia. Az információs biztos feladata az Egyesült Királyság adatvédelmi törvénye alkalmazása... Ha tényleges aggályaik vannak [az irányelv megfelelő átültetését illetően], fontos lenne e meghallgatás keretében az igazságügyi minisztériummal beszélniük.' Felelet a 176. kérdésre a jelölőbizottság meghallgatásán (2007.május 10.). Teljes egészében olvasható: <http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmhealth/422/7051002.htm> (26.01.2009.01.26.).

<sup>78</sup> Lásd: <http://www.heise.de/tp/r4/artikel/28/28579/1.html> (09.01.29), <http://www.dorstenerzeitung.de/nachrichten/politik/blickpunkt/art302.350317> (09.01.29), <http://www.tagesschau.de/inland/datenschutz110.html> (09.01.29), <http://www.sol.de/news/welt/tagesthema/Datenschutz:art7325.2705543> (09.01.29), <http://www.ruhrnachrichten.de/nachrichten/politik/blickpunkt/art302.433610> (09.01.29), <http://ez.omg.de/?id=20&nid=29923> (09.01.29), <http://www.handelsblatt.com/unternehmen/handel-dienstleister/rasterfahndungbei-der-bahn:2136145> (09.01.29).

kereskedtek az érintett előzetes hozzájárulása nélkül.<sup>79</sup> A kellő intézkedések, pl. a büntető eljárás hiánya, gyakran súlyosbítja a problémát.

#### 4.2.2 Belső adatvédelmi felelős kinevezése

Ami a belső adatvédelmi felelős kinevezését illeti, azt általános követelményként a nemzeti jogszabályok többsége elrendeli, anélkül, hogy azt a területen szerzett szakértelemhez vagy tapasztalathoz kötné. Dániában, Olaszországban és Görögországban a jogszabályok nem rendelkeznek belső adatvédelmi felelős kinevezéséről. Belgiumban a vonatkozó királyi rendelet hallgat a belső adatvédelmi felelős kinevezésének feltételeiről. Az adatvédelmi törvény végrehajtására kiadott, 2001. február 12-án kelt királyi rendelet indokolása kifejezetten állítja, hogy ilyen személy kinevezésének eszméjét Belgiumban nem támogatják. Ausztriában a jogszabály nem tartalmaz semmiféle kötelezettséget a belső adatvédelmi felelős kinevezésére, jóllehet a szakszervezetek támogatták ilyen belső adatvédelmi felelős kinevezését a közigazgatási ágazatban. Más tagállamok jobbára két csoportra oszthatók: a) amelyek nemzeti jogszabályaik bizonyos követelményeket írnak elő és b) amelyek nem. Néhány tagállam nemzeti jogszabályai (Ciprus,<sup>80</sup> Bulgária, Észtország, Litvánia, Írország, Svédország, Szlovénia, Románia, Finnország,<sup>81</sup> Portugália és az Egyesült Királyság) semmiféle, az adatvédelmi felelős kinevezésének követelményeire vonatkozó rendelkezést nem tartalmaznak. A többi tagállam (Franciaország, Luxemburg, Málta, Hollandia, Lengyelország, Magyarország, Szlovákia, Németország) nemzeti jogszabályai kifejezetten rendelkeznek az adatvédelmi felelősök függetlenségéről vagy a területen szerzett kellő ismeretekről és szakértelemről. Megjegyzendő, hogy ezeket a követelményeket tovább nem részletezik. Csupán Magyarország és Lettország képez kivételt, ahol a belső adatvédelmi felelősnek jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő felsőfokú végzettséggel kell rendelkeznie ahhoz, hogy az adatkezelő vagy a technikai adatfeldolgozást végző szervezetben kinevezést vagy megbízást kapjon.

Az adatvédelmi felelős kinevezési követelményei értékelése során nem feledkezhetünk meg arról, hogy az EU jogszabályok nem tartalmaznak különleges követelményeket. Mindazonáltal nyilvánvaló, hogy a sajátos szakértelemmel és/vagy sajátos tudatosságfokozó képességekkel rendelkező személy kinevezése pozitívan biztosítja a vonatkozó jogszabályok tiszteletben tartását és maradéktalan alkalmazását. Az adatvédelmi felelősök képességeitől és szakértelme szintjétől eltekintve, hangsúlyozni kell, hogy alkalmazásuk a közigazgatási ágazatban nem befolyásolja a nemzeti adatvédelmi hatóság függetlenségét. Egy tagállam továbbá útmutatások kibocsátásának lehetőségével élt, másik kettő (Svédország, Szlovákia) pedig szakmai kiképzést nyújt az adatvédelmi felelősöknek. Végül megjegyezzük, hogy megfelelést illető bizonyítékokat e területen nem találtunk.

---

<sup>79</sup> Lásd <http://www.aufrecht.de/news/view/article/illegaler-handel-mit-adress-undkontodaten-sprengt-alle-grenzen.html> (09.01.29)

<sup>80</sup> Ciprusban az adatvédelmi jogszabály rendelkezik arról, hogy a nemzeti adatvédelmi hatóság hivatali személyzetének rendeletekben előírt képesítéssel kell rendelkeznie. Ilyen rendeletek kiadására mindezidáig nem került sor.

<sup>81</sup> Adatvédelmi felelős kinevezésére vonatkozó kifejezett rendelkezést csupán a következő két törvény tartalmaz: törvény a betegek adatainak elektronikus feldolgozásáról a társadalmi és egészségügyi szolgálatoknál, törvény az elektronikus orvosi receptekről (Laki sähkõisestä lääkemääräyksestä, Lag om elektroniska recept, 61/2007 sz. törvény). Ezek a törvények előírják, hogy társadalmi és egészségügyi szolgáltatást nyújtó szervezetek, Finnország társadalombiztosító intézete (KELA) és az orvosjogi ügyek nemzeti hatósága adatvédelmi felelőst nevezzenek ki.

### **4.3 Szankciók, kártérítés, jogi következmények**

Minden EU tagállami átültette nemzeti jogrendszerébe az adatvédelmi irányelv „Bírósági jogorvoslat, felelősség és szankciók” című III. fejezetét. Eszerint a nemzeti hatóságoknak gondoskodniuk kell a személyes adatokat érintő jogszabályokban garantált jogok tiszteletben tartásának biztosítása érdekében a megfelelő és hatékony jogorvoslatról; meg kell állapítaniuk az adatvédelmi jogszabályok megsértése esetén kiszabható kellő és arányos szankciókat; rendelkezniük kell arról, hogy aki személyes adatai jogsértő feldolgozása során kárt szenvedett, kártérítésre legyen jogosult. Minthogy azonban az adatvédelmi irányelv a jogorvoslat, felelősség és szankciók tekintetében csak a tagállamok által követendő célt rögzíti anélkül, hogy részletezné azok sajátos követelményeit, a nemzeti adatvédelmi jogszabályok a kérdést különféleképpen szabályozzák. Vonatkozik ez mind a bírósághoz fordulásra és a kártérítésre, mind a jogsértőnek a személyes adatokhoz fűződő jogok megsértéséért való elítélésére és megbüntetésére.

#### *4.3.1 Jogorvoslat*

Az adatvédelmi irányelv rögzíti a tagállamoknak azt az általános kötelezettségét, hogy biztosítsák „a közigazgatási jogorvoslat sérelme nélkül (...) mindenki számára a jogorvoslathoz való jogot bármely jogának megsértése esetén”. A következő 5. táblázat részletezi azokat a módszereket, melyekkel a nemzeti jogrendszerek gondoskodnak az EU jognak való megfelelésükről. E módszerek: a) közigazgatási jogorvoslat az adatvédelmi hatóságnál; b) nem bírósági jogorvoslat a felügyelő szervnél (mint a per alternatívája, mely, ha már megkezdődött, kizárja az igény bíróság előtti érvényesítését; c) bírósági jogorvoslat rendes bíróság vagy ítélszék előtt.



5. táblázat  
Jogorvoslat

tagállam	Közigazgatási jogorvoslat az adatvédelmi hatóságnál	Nem bírósági jogorvoslat a felügyelő szervnél	Bírósági jogorvoslat a rendes bíróság vagy ítélesezék előtt
Bulgária	X		X
Belgium		X	X
Cseh Köztársaság	X		X
Dánia	X		X
Németország	X		X
Észtország	X		X
Görögország	X	X	X
Spanyolország	X		X
Franciaország	X		X
Írország	X		X
Olaszország	X	X	X
Ciprus	X		X
Lettország	X		X
Litvánia	X		X
Luxemburg	X		X
Magyarország	X <sup>82</sup>		X
Málta	X		X
Hollandia	X		X
Ausztria	X		X
Lengyelország	X		X
Portugália	X		X
Románia	X		X
Szlovénia	X		X
Szlovákia	X		X
Finnország	X		X
Svédország	X		X
Egyesült Királyság	X		X

Az egyének valamennyi tagállamban konkrét jogsértés ellen panaszt nyújthatnak be a nemzeti adatvédelmi hatóságokhoz, és általános, jogsértést kifogásoló panasszal is élhetnek. A jogrend egyik alapelve az a jog, melyet ugyancsak minden tagállam elismer, hogy jogi eljárás kezdeményezhető a rendes bíróság előtt a vita bírósági eldöntése céljából. Ez gyakran egyszerűsített bírósági eljárásban is elérhető (pl. Olaszországban, Belgiumban). Valójában azonban sok tagállamban (Finnországban, Ausztriában, Lettországban, Észtországban) bírósági jogorvoslatért, bár elvileg tehetnék, a panaszosok nem folyamodnak. Csak Belgium, Olaszország és Görögország engedi meg, hogy az érintett a vita rendezésére a bírósághoz forduljon, vagy panaszt nyújtson be az adatvédelmi hatósághoz, amely kvázi-bírósági eljárásban gyors és költséghatékony jogorvoslatot kínál.

<sup>82</sup> Magyarországon az adatvédelmi hatóságnak korlátozott hatásköre van közigazgatási jogorvoslat nyújtására, de végrehajtását nem kényszerítheti ki.

#### 4.3.2 Szankciók

Az adatvédelmi irányelv 24. cikke kötelezi a tagállamokat arra, hogy megállapítsák az adatvédelmi jogszabályok „megsértése esetén kiszabható szankciókat”. Ennek az általános rendelkezésnek a végrehajtása az egyes államokban mindazonáltal felettebb változatos. A belső jog és gyakorlat hatása e tekintetben a büntető és közigazgatási jogszabályok területén kétségtelenül különösen jelentős, és befolyásolta egyrészt a tagállamok jogalkotóinak kezdetben uralkodó felfogását, másrészt ezt követően a közigazgatási és bírósági hatóságoknak a jog értelmezésében és végrehajtásában mutatkozó szemléletét. Minthogy lehetetlen az adatvédelmi jogsértések szankcionálásával (és büntetésével) kapcsolatos nemzeti (közigazgatási és büntető) jog átfogó összehasonlítása, elemzésünk azokra az intézményekre összpontosít, amelyek szankciók kiszabására felhatalmazással rendelkeznek, továbbá az általuk kiróható főbb szankciókra.

Az adatvédelmi hatóságok által kiszabható szankciók változatosak. Az adatvédelmi hatóságok, amellet hogy megtehetik a 3.1.3.2 részben ismertetett intézkedéseket (az adatkezelő és adatfeldolgozó figyelmeztetése vagy megrovása, a személyes adatok feldolgozása felfüggesztésének, bizonyos adatok zárolásának vagy törlésének elrendelése) pénzbeli szankciók kiszabására is fel vannak hatalmazva. A bíróságok ugyancsak kiszabhatnak pénzbeli szankciókat, valamint börtönbüntetést vagy annak alternatívájaként felfüggesztett börtönbüntetést vagy közmunkát. A következő 6. táblázat az egyes jogrendszerekben rögzített, az adatvédelmi jogszabályok megsértéséből adódó következményeket mutatja be: a) az adatvédelmi hatóság által kirótt közigazgatási bírság; b) a bíróság által kiszabott büntetés; c) bíróság által megállapított börtönbüntetés vagy annak alternatívája. Megjegyezzük, hogy a veszteség- vagy kártérítési kötelezettséget alább külön elemezzük.

6. táblázat  
Szankciók

tagállam	Az adatvédelmi hatóság által kirótt közigazgatási bírság	A bíróság által kiszabott büntetés	A bíróság által megállapított börtönbüntetés
Bulgária	X		X
Belgium		X	
Cseh Köztársaság	X		
Dánia		X	X
Németország	X <sup>83</sup> <sub>83</sub>	X	X
Észtország	X		X
Görögország	X	X	X
Spanyolország	X		
Franciaország	X	X	X
Írország	X	X	
Olaszország	X	X	X
Ciprus	X	X	
Lettország	X	X	
Litvánia		X	
Luxemburg	X	X	
Magyarország		X	X
Málta	X	X	X
Hollandia	X	X	X
Ausztria		X	X
Lengyelország		X	X
Portugália	X		X
Románia	X	X	
Szlovénia	X	X	X
Szlovákia	X	X	X
Finnország	X	X	X
Svédország		X	X
Egyesült Királyság		X	X

Amint azt a 6. táblázat bemutatja, az adatvédelmi hatóságok csak néhány tagállamban vannak felhatalmazva arra, hogy gazdasági szankciókat rójanak ki (és határozatuk ellen akkor is mindig fellebbezés nyújtható be a közigazgatási bíróságokhoz). Más tagállamokban (pl. Belgiumban, az Egyesült Királyságban) az AVH-k csak barátságos megoldásról tárgyalhatnak a jogsértőkkel. A közigazgatási szankciók hatékonysága ezért több tagállamban kérdéses, mert a bírság összege túl csekély vagy a bírság kivetésére csak ritkán kerül sor, ezért visszatartó ereje is gyenge. Más tagállamokban (pl. Ausztriában, az Egyesült Királyságban, Dániában, Franciaországban) inkább a bírósági hatóságok gyakorlata nélkülözi a visszatartó erőt. Így néhány tagállamban (pl. Észtországban) a bírósági hatóságok valójában soha nem alkalmaztak büntető szankciókat.

---

<sup>83</sup> 2008-ban például 1.4 millió euróra rúgott a LIDL kereskedelmi vállalkozása kiszabott közigazgatási bírság, melyet a LIDL elfogadott.

### 4.3.3 Kártérítés

Az adatvédelmi irányelv 23. cikk (1) bekezdés szerint a tagállamoknak „rendelkezniük kell arról, hogy mindenki, aki jogellenes adatfeldolgozási művelet vagy az ezen irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett károkért”. A polgári felelősséget azonban a vonatkozó nemzeti jogeszközök eltérően szabályozzák attól függően, hogy – a tagállam döntése szerint – egy kifejezetten adatvédelmi ügyben szenvedett kárért járó kártérítési kötelezettséget szabályoznak, vagy csupán kiterjesztették a polgári felelősség általános keretét a személyes adatok védelmére is. A következő 7. táblázat bemutatja a tagállamokban az adatvédelmi irányelv átültetésére választott legfontosabb megoldásokat a következők szerint: a) a polgári felelősség általános keretének kiterjesztése (mikor is a felperes viseli mind a szenvedett kár bizonyításának terhet, mind a peres eljárás költségének kockázatát); b) a polgári felelősség általános keretének kiterjesztése, de a bizonyítási teher megfordításával (mikor is az adatkezelő, részben vagy egészben, mentesül a felelősség alól, ha bizonyítja, hogy a kárt okozó eseményért nem felelős; c) a polgári felelősség sajátos keretének alkalmazása.

7. táblázat  
Kártérítés

tagállam	A polgári felelősség általános keretének kiterjesztése	A polgári felelősség általános keretének kiterjesztése a bizonyítási teher megfordításával	A polgári felelősség sajátos alkalmazása
Bulgária	X		
Belgium			
Cseh Köztársaság	X		
Dánia		X	
Németország		X	X
Észtország	X		
Görögország			X
Spanyolország	X		
Franciaország	X		
Írország	X		
Olaszország		X	
Ciprus	X		
Lettország	X		
Litvánia	X		
Luxemburg	X		
Magyarország			X
Málta	X		
Hollandia	X		
Ausztria	X		
Lengyelország	X		
Portugália	X		
Románia	X		
Szlovénia	X		
Szlovákia	X		
Finnország	X		
Svédország		X <sup>84</sup>	X
Egyesült Királyság		X	

Amint azt a 7. táblázat mutatja, kártérítés jár minden olyan esetben, amikor a személyes adatok feldolgozását az adatvédelmi jogszabályokkal nem összhangban végzik. A legtöbb tagállamban kártérítés elméletileg a szokásos, polgári felelősséggel kapcsolatos általános rendelkezésekkel szabályozott bírósági eljárásban nyerhető, még ha számos tagállamban (pl. Cipruson, Máltán, Portugáliában, Lettországon) adatvédelmi ügyekben kártérítés megítélésére nem találtunk példát, vagy nagyon csekély kártérítési per zajlott bírósági hatóságok előtt (pl. Finnországban, Észtországban). Több tagállamban a polgári felelősség általános rendelkezéseit alkalmazzák az adatvédelmi ügyekben, kivéve a bizonyítási teher megfordítását, amely a felperesről az alperesre (az adatfeldolgozóra vagy az adatkezelőre) száll át. Végül néhány országban a kártérítésre sajátos kereteket alkottak. Nevezetesen a

<sup>84</sup> A svéd adatvédelmi törvény a kártérítésre vonatkozó sajátos rendelkezéseket tartalmaz, de az eljárás a polgári esetek meglévő keretei közé tartozik.

szigorú felelősség szabályát kell alkalmazni az adatfeldolgozóra vagy az adatkezelőre Görögországban és Németországban (de csak a közjogi adatfeldolgozó és adatkezelő tekintetében). Ekkor a felelősség nem függ a szándéktól vagy gondatlanságtól, hanem pusztán a jogszabálysértéssel okozott kártól. Belgiumban, a hírek szerint, egyes bíróságok megítélhetik a kártérítést az első fokú bíróság elnöke előtt folyó gyorsított eljárásban. Svédországban az igazságügyi minisztérium nem bírósági eljárásban ítélt meg kártérítést, ha a jogsértést kormányzati vagy közigazgatási szervek követik el. Magyarországon az adatvédelemmel kapcsolatos bírósági eljárások illetékmentesek<sup>XI</sup>, és a szigorú felelősséghez hasonló szabályok érvényesek az adatkezelő vagy adatfeldolgozó felelősségének mérlegelésére.

Az adatvédelemhez fűződő jogok megsértéséért felelős adatkezelőre vagy adatfeldolgozóra kiróható kártérítés eljárása és anyagi mértékének megállapítása a tagállamokban a polgári felelősséggel kapcsolatos eltérő jogszabályok és bírósági gyakorlatok következtében változatos képet mutat, s így ebben az összehasonlító jelentésben nem elemezhető. Mi több, az adatvédelmi ügyekben kirótt kártérítés mértéke a legtöbb tagállamban nem ismeretes (Magyarország, Svédország, Szlovénia, Románia, Cseh Köztársaság, Egyesült Királyság, Portugália, Lengyelország, Hollandia, Málta, Luxemburg, Litvánia, Lettország, Olaszország, Írország, Görögország, Németország, Franciaország, Finnország, Észtország, Dánia, Ciprus, Bulgária, Belgium és Ausztria). Mindazonáltal érdemes kiemelni, hogy számos tagállamban (Olaszország, Szlovénia, Németország, Görögország, Egyesült Királyság, Litvánia, Svédország és Magyarország) nem anyagi kár, például az okozott szorongás esetében is kártérítést lehet megállapítani önmagában vagy az anyagi veszteséggel együtt.

#### *4.3.4 A munkaviszonyra vonatkozó sajátos adatvédelmi jogszabályok*

Az érintett alapvető jogainak és méltóságának tiszteletben tartása különösen fontos a munkáltató-munkavállaló viszonyában. Egyrészt azért, mert a munkavállaló magánéletének és személyes adatainak védelme megkerülhetetlen előfeltétele olyan alapvető jogok biztosításának, mint a szakszervezeti tagság és a részvétel közös cselekményekben. Másrészt, mert az egyének viselkedésének megfigyelésére és ellenőrzésére szolgáló fejlett technikák némelyikét (pl. kamerás felügyelet és távoli e-mail ellenőrzés) túlnyomórészt munkaköri környezetben alkalmazzák. Ezért a tagállamoknak olyan jogi rendelkezésekkel kell kiegészíteniük jogszabályaikat, amelyek a munkaköri környezetben védik az adatokat, kompenzálva így a munkaszerződést kötő felek inherens egyenlőtlenségét azáltal, hogy szigorúbb követelményeket állapítanak meg a munkáltató részére az adatvédelmi rendelkezések tiszteletben tartása céljából.

Az adatvédelmi irányelv 8. cikk (1) bekezdés tiltja a szakszervezeti tagságra vonatkozó személyes adatok feldolgozását, s számos tagállam (Olaszország, Magyarország, Spanyolország, Szlovénia, Szlovákia, Cseh Köztársaság, Portugália, Lengyelország, Hollandia, Luxemburg, Lettország, Írország, Görögország, Finnország, Belgium) ugyancsak sajátos rendelkezésekkel (vagy a munkavállalásra vonatkozó, vagy az általános adatvédelmi jogszabályokban) garantálja a magánélet és a személyes adatok védelmének szigorúbb feltételeit a munkaviszony keretében. E rendelkezések részletezik az adatvédelmi hatóságok szerepét, felhatalmazva őket arra, hogy általános szabályokat és útmutatásokat fogalmazzanak meg, különösen a magánjogi társaságok számára. A szakszervezetek pedig, míg tanácsadással szolgálnak a munkavállalóknak adataik védelme tekintetében, gyakran közvetlenül részt vesznek a munkáltatókkal folytatott, a személyes adatokat tartalmazó rendszer létrehozását célzó előzetes tárgyalásokon, majd ezt követően ellenőrizhetik annak tiszteletben tartását is. Mindazonáltal különféle hiányosságok mutatkoznak a munkaviszony keretében kezelt adatok védelme tekintetében. Először is több tagállamban (Svédország, Románia, Egyesült Királyság, Bulgária, Málta, Litvánia, Ciprus, Franciaország, Észtország, Dánia, Ausztria és Németország

a magánjogi környezetben) a munkavállalók védelmét növelő sajátos szabályozás még mindig hiányzik. Am ha ilyen szabályozás létezik is, aggályok merülnek fel a szakszervezetek ellenőrzési szerepe hiányát (pl. Cseh Köztársaság, Lettország, Írország), a munkáltató kizárólagos, a személyes adatok feldolgozásának célját megállapító jogosultságát (pl. Lengyelország), továbbá a kisvállalkozásoknak a munkaviszony keretében feldolgozott adatok szigorú szabályainak alkalmazása alól való mentesítését illetően (pl. Hollandia). Végül egyéb országokban (pl. Finnország) – jóllehet a munkaviszony keretében kezelt személyes adatok védelme mindmáig kielégítő volt – függőben vannak azok a jogszabályi reformok, amelyek révén jelentősen gyengülnek a jelenlegi normák, megengedve a munkáltatónak, hogy bizonyos feltételek mellett ellenőrizze a munkavállaló által küldött vagy fogadott e-mail-ek címzettjeit, valamint az üzenethez csatolt dokumentumok típusát, az üzenet tartalmát azonban nem.<sup>85</sup> A finn törvénytervezet<sup>XII</sup> értelmében a vállalkozásoknak joga lesz arra, hogy a kommunikációs hálózatukban megjelenő azonosító adatokat feldolgozzák az üzleti titok megsértése, az illetéktelen felhasználás és egyes más bűncselekmények felderítése céljából.

#### 4.4 Jogtudatosság

Ebben a részben a Jelentés ismerteti az Eurobarométer közvélemény-kutatásainak és a tagállamokban végzett más tanulmányoknak és közvélemény-kutatásoknak az eredményeit, áttekintést nyújtva a nagyközönség adatvédelmi jogai tudatosságáról. Megvizsgálja továbbá a jogtudatosság és az alábbiak viszonyát:

adatvédelmi hatóságok, hatásköreik, feladataik, forrásaik és tevékenységük

adatvédelmi jogszabályoknak való megfelelést jelző gyakorlatuk

szankciókkal, kártérítéssel és adatvédelmi ügyek jogi következményeivel kapcsolatos gyakorlatuk

Az 5.1.4 szakaszban a jogtudatosság hiányosságait taglalja a dokumentum, a 6.3 szakaszban pedig a jogtudatossággal kapcsolatos helyes gyakorlatokat ismerteti.

2008 februárjában két Flash Eurobarometer közvélemény-kutatást tettek közzé: 225. számú – „Adatvédelem az Európai Unióban a polgár szemszögéből”<sup>86</sup> és 226. számú – „Adatvédelem az Európai Unióban az adatkezelő szemszögéből”<sup>87</sup>

Az első közvélemény-kutatás tárgykörei: a nagyközönség általános felfogása és aggodalmai az adatvédelemről; bizalmuk a személyes adataikat birtokló különféle szervezetek iránt; adatvédelmi jogaik tudatossága és a nemzeti adatvédelmi hatóság ismerete; az Interneten folyó adatforgalom észlelt biztonsága és az adatbiztonságot fokozó eszközök használata; viszonyulás adatvédelmi jogaik korlátozásához a nemzetközi terrorizmus fényében. A közvélemény-kutatás során 27 000 személlyel készítették interjút az EU 27 tagállamában (országoként 1 000 interjú) főleg telefonon a helyhez kötött telefon számát használva (kilenc tagállamban azonban a helyhez kötött telefontal való lefedettség csekélynek mutatkozott, ezért a minta telefonos és személyes interjúk keverékéből áll).

A közvélemény-kutatás a következő megállapításokra jutott:

A válaszadók többsége EU szerte azt mondta, nagyon vagy meglehetősen aggódik személyes adatai kezelését illetően. Mindazonáltal az aggodalom mértéke megegyezik azzal, amit az Eurobarometer egy korábbi közvélemény-kutatása mutatott.

---

<sup>85</sup> Lásd: a finn kormány törvényjavaslata HE 48/2008.

<sup>86</sup> Data Protection in the European Union: Citizens' perceptions. Flash Eurobarometer No 225 ([http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf)) (2009.02.21.).

<sup>87</sup> Data Protection in the European Union: Data controllers' perceptions. Flash Eurobarometer No 226 ([http://ec.europa.eu/public\\_opinion/flash/fl\\_226\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf)) (2009.02.21.).

A válaszadók legnagyobb fokú bizalmát élvezték az egészségügyi szolgáltatások, az orvosok és a közintézmények.

A válaszadók többsége kérdésesnek tartotta, hogy országukban a nemzeti jogszabályok képesek megküzdeni Interneten megjelenő személyes információik használatával.

Míg a válaszadók többsége, úgy tűnt, tudatában van személyes adatait érintő jogainak és a vonatkozó jogszabályok létezésének, a válaszadóknak csak átlag 28%-a tudott a nemzeti adatvédelmi hatóság létezéséről.

A második közvélemény-kutatás keretében az adatkezelők adatvédelemről alkotott felfogását vizsgálták az EU 27 tagállamában. E közvélemény-kutatás tárgykörei felölelték a nemzeti adatvédelmi jogszabályokról alkotott felfogást; az adatvédelemmel és a személyes adatok továbbításával kapcsolatos házon belüli gyakorlatokat; a magánélettel és az adatvédelemmel kapcsolatos eljárásokból származó újabb tapasztalatokat; az adatvédelmet szabályozó jogszabályi keretek jövőjét; az adatvédelmet a nemzetközi terrorizmus fényében.

Ez a közvélemény kutatás az alábbi következtetésekhez vezetett:

Azoknak a válaszadóknak a többsége, akik vállalkozásuknál az adatvédelmi kérdésekért viselnek felelősséget, azt mondta, alaposan vagy némiképp ismeri a nemzeti adatvédelmi jogszabályok rendelkezéseit (56%).

A válaszadók azonos hányada (56%) úgy vélte, hogy a nemzeti adatvédelmi jogszabályok a polgároknak közepes szintű védelmet nyújtanak, míg 28%-uk a védelmi szintet 'magasnak', 11%-uk 'alacsonynak' tartotta.

A válaszadók 50%-ának a véleménye szerint a hatályos jogszabályok felettébb alkalmatlanok vagy egyáltalán nem alkalmasak arra, hogy megküzdjenek a személyes információk növekvő mértékű cseréjével.

A túlnyomó többség (91%) szükségesnek tartotta az adatvédelmi jogszabályok követelményeit. A válaszadók harmada (35%) szerint a követelmények néhány szempontból túl szigorúak.

Megoszlottak a vélemények arról, hogy megfelelő-e a nemzeti jogszabályok harmonizációja a személyes adatok szabad áramlását és azokat az eltéréseket illetően, ahogyan a tagállamok EU szerte értelmezik az adatvédelmi jogszabályokat (e két kérdésben nagyszámú megkérdezettnek nem volt határozott véleménye).

Az interjúalanyok tizenhárom százaléka az EU-27-ben azt mondta, hogy rendszeres kapcsolatuk van a nemzeti adatvédelmi hatósággal, arányuk azonban a legmagasabb, 41% volt Olaszországban és a legalacsonyabb, 1% Ausztriában.

A nemzeti adatvédelmi hatóságokkal való kapcsolatfelvétel legtöbbször említett oka: útmutatás kérése (a rendszeres kapcsolattartók 60%-a jelölte meg ezt az okot) vagy egy bejelentés (56%).

A tagállamok statisztikai adatainak értékelése tekintetében megjegyzendő, hogy nemzeti közvélemény-kutatások a 27 tagállam közül csak 12-ben állnak rendelkezésre. Ezekre a közvélemény-kutatásokra egyes esetekben a nemzeti adatvédelmi hatóságok adtak megbízást. A feltett kérdések, a válaszadók száma, a módszer, a minta kiválasztása és a végeredmények eltérőek, és nem mindig teszik lehetővé eredményeik felhasználását ebben az összehasonlító tanulmányban.

Néhány tagállam jogtudatosságra vonatkozó nemzeti közvélemény-kutatásai hozzáférhetők (Svédország, Dánia, Finnország, Franciaország, Ausztria, Spanyolország, Írország, Lettország, Hollandia, Szlovénia, Magyarország, Szlovákia, Egyesült Királyság), a többi azonban nem



(Luxemburg, Litvánia, Bulgária, Németország, Cseh Köztársaság, Olaszország, Málta, Lengyelország, Románia, Ciprus, Észtország, Görögország, Belgium, Portugália).

A személyes adatok védelmére vonatkozó rendszeres közvélemény-kutatások készülnek Szlovákiában. Eredményeiket a nemzeti adatvédelmi hatóság jelentései tartalmazzák. Közülük kettőt (a 2005-ben<sup>88</sup> és a 2007-ben<sup>89</sup> készített közvélemény-kutatást) az AVH honlapján közzé is tettek.<sup>90</sup> Mindkét közvélemény-kutatást a 18 év feletti lakosság országos reprezentatív mintáján végezték (2005-ben a minta nettó 1 238, 2007-ben nettó 1 131 megkérdezettet tartalmazott). 2007-ben a válaszadók 51%-a úgy nyilatkozott, hogy tudatában van adatvédelmet érintő jogainak, és közel 50% tudott a személyes adatok védelmének hivataláról mint illetékes nemzeti hatóságról (ami 5%-kal magasabb, mint az előző, 2005- évi közvélemény-kutatás megfelelő adata). A közvélemény-kutatások eredményeire alapozva állítható, hogy a nagyközönség továbbra sincs teljes tudatában a személyes adatok védelmére vonatkozó kérdéseknek, s ezeket széles körben nem is vitatja.

Lettországból két közvélemény-kutatást végeztek, 2003-ban és 2005-ben (mindkettőt az állandó lakosokból választott, mintegy 1000 megkérdezettet tartalmazó rétegzett reprezentatív mintán). Az összehasonlító tanulmányunk céljához illeszkedő eredmények: 29,5% (23,3% 2003-ban) tudott a nemzeti adatvédelmi hatóság létezéséről; 19,5% (14,5% 2003-ban) már volt olyan helyzetben, melyben adatait jogsértő módon dolgozták fel, ami így vélhetően anyagi vagy erkölcsi kárt okozott; 13,5% (6,4% 2003-ban) tapasztalta, hogy több adatot kértek tőle, mint szükséges; a válaszadók 22,9%-a igényelt személyét érintő információt intézményektől vagy vállalkozásoktól, többségük (66,2%) sikerrel, 32,5%-uknak azonban megtagadták az információ kiadását. A közvélemény-kutatás eredménye azt mutatja, hogy az adatvédelmi tudatosságot fokozni kell mind az állami intézmények, mind pedig általában a nagyközönség körében.

Svédországban a nemzeti adatvédelmi hatóság rendszeres kutatásokat végez mind a köz-, mind a magánjogi szektorban, valamint társadalmi csoportokban. Három újabb tanulmány áll rendelkezésre. Az első a vidéki egészségügyi hatóságoknak a betegek adatai hozzáférését illető adatvédelmi tudatosságára vonatkozik.<sup>91</sup> A második egy kérdőíves felmérést elemzett, melyet 103 vállalkozásnak és közigazgatási hatóságnak küldtek meg. Kérdései a munkáltatónak a munkavállaló Internet-használatával, e-mail-forgalmával és – ha ilyenek rendelkezésre álltak – biometrikus adatok vagy térfigyelő kamarák felvételeinek feldolgozásával kapcsolatosak.<sup>92</sup> A harmadik tanulmány azt elemezte 14-18 éves fiatalok körében, mennyire vannak tudatában adatvédelmi jogszabályoknak és jogaiknak tudatosságára irányult (533 megkérdezett, kvóta szerinti kiválasztással). A válaszadók online kérdőívet töltöttek ki.<sup>93</sup> Ezeket azonban a nemzeti tanulmányok nem mutatták be, s nem is elemezték, ezért magyarázatot sem fűzhetünk hozzájuk.

Dániából két tanulmány áll rendelkezésre. Az egyiket nemrégiben a „Magánszféra erősítésének hatása a biztonsági kutatásra és technológiára” című projekt keretében készítette a Privacy and Security Technology (PRISE), mely szerint társadalmi vitára van szükség az új biztonsági technikák alkalmazásának kérdésében. A másik egy, a Bűnmegelőzési Tanács által

---

<sup>88</sup> [http://www.dataprotection.gov.sk/buxus/docs/sprava\\_5\\_2005\\_prieskum\\_vm1.pdf](http://www.dataprotection.gov.sk/buxus/docs/sprava_5_2005_prieskum_vm1.pdf) (2009.01.23.).

<sup>89</sup> [http://www.dataprotection.gov.sk/buxus/docs/zaverecna\\_sprava\\_07.pdf](http://www.dataprotection.gov.sk/buxus/docs/zaverecna_sprava_07.pdf) (2009.01.23.).

<sup>90</sup> [http://www.dataprotection.gov.sk/buxus/generate\\_page.php?page\\_id=421](http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=421) (2009.01.22.).

<sup>91</sup> Angol nyelvű összefoglaló: Report 2005:1 <http://www.datainspektionen.se/Documents/rapport-accessibility-to-patients-data.pdf> (2009.01.29.).

<sup>92</sup> Monitoring in Working Life Report 2005:3, Angol nyelvű összefoglaló: <http://www.datainspektionen.se/Documents/rapport-monworklife-summary.pdf> (2009.01.27.).

<sup>93</sup> <http://www.datainspektionen.se/Documents/rapport-ungdom-2009.pdf> (2009.01.27.).

2005-ben végzett, kamerás megfigyelésre vonatkozó közvélemény-kutatás, melynek keretében 994 válaszadóval készült interjú. Az elemzés azt mutatta, hogy „a dánok általában pozitívan viszonyulnak a kamerás megfigyeléshez. A nők a férfiaknál jobban aggódnak a bűnözés miatt. A magasabb iskolai végzettségűek inkább a magánéletbe való beavatkozás miatt aggódnak.”<sup>94</sup> Az elemzés általában azt sugallja, hogy a dán lakosság nem különösebben aggódik a magánélet védelme miatt, alapvetően bízik az adatait kezelő kormány- és a hatósági szervezetben, és úgy tartja, a bűnmegelőzés és a biztonság fontosabb, mint a magánélet megfoghatatlan és absztrakt eszméje.

Írország nemzeti adatvédelmi hatósága 2008-ban 1 000 megkérdezettet felölölő mintán végzett közvélemény-kutatása (amely az 1997-ben, 2002-ben és 2005-ben végzett hasonló kutatásokat követte) omnibusz felmérés részét képező személyes interjúkon alapult.<sup>95</sup> A közvélemény-kutatás kulcsfontosságú megállapítása: a népesség kétharmada (65%) már tapasztalt valamiféle beavatkozást magánéletébe, leggyakrabban kéréstlen kereskedelmi reklámot tartalmazó üzenet formájában.<sup>96</sup> Sok más egyéb közül a jó egészségügyi szolgáltatást (a válaszadók 89%-a) és a bűnmegelőzést (87%) tartották a legfontosabb, őket érintő kérdésnek, amit a személyes információ bizalmas volta követett (84%). Míg a megkérdezettek fele érezte úgy, hogy mind a köz-, mind a magánjogi szférában megfelelő az ellenőrzés, amely visszatartja a munkaadókat attól, hogy nem megfelelő célból személyes információkhoz férjen hozzá, mintegy ötödüknek kétségeik voltak az ellenőrzés hatékonyságát illetően. A válaszadók legfontosabbnak tartották az egészségügyi, a pénzforgalmi és a hitelkártya adatok bizalmas voltának biztosítását. Ötvennyolc százalékuk tudott a nemzeti adatvédelmi hatóság létezéséről. A nemzeti AVH úgy nyilatkozott, hogy a jövőben e közvélemény-kutatás eredményeit hasznosítani fogja a hivatal munkájában.<sup>97</sup>

Franciaországban a Commission Nationale de l’Informatique et des Libertés (CNIL) évente végez közvélemény-kutatást a nagyközönség körében a CNIL és jogaik tudatosságát illetően, és pedig a 18. életévét betöltött lakosság 1 000 főt felölölő reprezentatív mintáján. E közvélemény-kutatás szerint 2007-ben a franciák 61%-a úgy vélte, az adatgyűjtés sérti magánélethez fűződő jogaikat, s ezért több védelmet szeretnének.<sup>98</sup> Emellett 2004 júniusában 32%, 2005 decemberében 37%, 2007 novemberében 50% állította, hogy tudomása van nemzeti adatvédelmi hatóságokról,<sup>99</sup> s minden második tudott feladatairól is. Mindössze 26% érezte úgy, hogy személyes adatai védelmét illetően eléggé tájékozott, míg a válaszadók 72%-a úgy vélte, tájékoztatásuk nem megfelelő.<sup>100</sup>

2008 júliusában köztéri személyes interjút készítettek 1 213 válaszadóval (kvóta szerinti kiválasztással) az osztrák népesség adatvédelembe helyezett bizalmát illetően, s a közvélemény-kutatás eredményeit nyilvánosságra hozták.<sup>101</sup> Ezek szerint az osztrákok

---

<sup>94</sup> TV-overvågning – Fakta om TV-overvågning i Danmark. Det Kriminalpræventive Råd, Februar 2005. Available in Danish at: [http://www.dkr.dk/ftp\\_files/WEBDOX/PDF/dkr\\_mat\\_083.pdf](http://www.dkr.dk/ftp_files/WEBDOX/PDF/dkr_mat_083.pdf) (03.02.2009).

<sup>95</sup> A teljes közvélemény-kutatást lásd [http://www.dataprotection.ie/docs/Public\\_Awareness\\_Survey\\_2008/794.htm](http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008/794.htm) (09.01.10.).

<sup>96</sup> A közvélemény-kutatás eredményeit bemutató tanulmányt lásd [http://www.dataprotection.ie/docs/Public\\_Awareness\\_Survey\\_2008\\_Report/821.htm](http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008_Report/821.htm) (2010.02.24.).

<sup>97</sup> Sajtóközlemény (08.08.12.): <http://www.dataprotection.ie/viewdoc.asp?DocID=815>. (10.01.09.).

<sup>98</sup> CNIL, 2008/01/25, „a franciák 61%-a úgy véli, hogy a számítógépesített adatállományok sértik magánélethez fűződő jogaikat”, in: <http://www.cnil.fr> (19.11.2008).

<sup>99</sup> CNIL, Annual Report 2007, p. 39.

<sup>100</sup> CNIL, Annual Report 2007, p. 39.

<sup>101</sup> Vertrauen der ÖsterreicherInnen in den Datenschutz (az osztrákok adatvédelembe vetett bizalma), lásd: <http://www.oekonsult.eu/datensicherheit2008.pdf> (2009.01.04.).

számára az adatvédelmet és a megfigyelést érintő kérdések nagymértékben ismeretlenek: a válaszadók 77%-a elismerte, e téren többé-kevésbé tudatlan; 92% azt állította, nincs tudomása, (személyes) adatai gyűjtéséről, s azok közül a válaszadók közül, akiknek van, 76% úgy vélte, az osztrák népeiséget nem eléggé tájékoztatják az adatvédelemről, az adatokkal való visszaélés kockázatairól vagy a vonatkozó jogszabályi feltételekről. A kamerás megfigyelést illetően a válaszadók 55%-a úgy nyilatkozott, hogy amennyiben a videokamerákat események, továbbá gyakorlatilag minden személy viselkedésének megfigyelésére és rögzítésére használják, úgy azt inkább a modern élet részének, mintsem alapvető jogaik megsértésének tekintik. Egy másik, a köztéri kamerás megfigyeléssel kapcsolatos tanulmány (1 237 válaszadó, a fent említett tanulmány készítésekor alkalmazott módszer) a válaszadó közel 81%-a úgy nyilatkozott, hogy elfogadják a járó-kelők kamerás megfigyelését, és 90%-uk elismerte, hogy hozzájárult a megfigyelő kamerák mindenkori jelenlétéhez.<sup>102</sup>

Két tanulmány áll rendelkezésre Spanyolországból. Az első címe: „Tanulmány a kis- és közepes spanyol vállalkozásoknak a személyes adatok védelméről szóló alapvető törvény és az új rendeletek szabályainak való megfelelése mértékéről”.<sup>103</sup> E tanulmány megállapításai szerint a kis- és közepes vállalkozások 96%-ának vannak személyes adatokat tartalmazó nyilvántartásai, melyek 78%-a elektronikus, így mindegyikük az adatvédelmi jogszabályok hatálya alá tartozik (az eredmények 250 kis- és közepes, legfeljebb 50 munkavállalót foglalkoztató vállalkozás rétegzett mintáján készített telefonos interjúkon alapulnak). A spanyolországi kis- és közepes vállalkozások pozitíve viszonyulnak az adatvédelemhez: a felméréssel érintett vállalkozások 82%-a megerősítette, tudatában van annak, hogy eleget kell tennie a vonatkozó jogszabályoknak, míg 79%-a úgy nyilatkozott, hogy szándékában áll anyagi és ember erőforrást áldozni az adatvédelmi jogszabályok megfelelő végrehajtására. Baszkföld helyi adatvédelmi ügynöksége 2008-ban készített értékes tanulmánya a baszkföldi társadalomnak az adatvédelemről alkotott felfogásával foglalkozik (600 válaszadót felölelő rétegzett mintán végzett telefonos interjú alapján).<sup>104</sup> Eredményei szerint ennek az autonóm közösségnek a 37%-a nagyon vagy meglehetősen aggodalmasnak tartja a polgárok személyes adatainak a közigazgatási szervek és magánvállalkozások által való felhasználását.

Hollandiában a magánélethez fűződő jogokkal és ismeretükről alkotott felfogással több közvélemény-kutatás is foglalkozott.<sup>105</sup> Egy 1989-es közvélemény-kutatás szerint a polgároknak az volt a véleménye, hogy magánélet védelme van olyan fontos, mint a jó egészségügyi szolgáltatás, a tiszta környezet, valamint a munkanélküliség és a bűnözés elleni harc.<sup>106</sup> Egy 1999-es közvélemény-kutatás a polgárok három csoportját különböztette meg: 1) egyrészt azokat a polgárokat, akik szerint az információs technológiákra szükség van és nem látnak problémát a magánélet tekintetében (19%); 2) másrészt azokat, aki úgy vélik, az információs technológiák egyre több magánéleti problémát vetnek fel (35%); 3) harmadrészt

---

<sup>102</sup> Big Brother. Gefahr oder Normalität (A nagy testvér: veszély vagy rendes állapot), lásd: [http://www.oekonsult.at/bigBrother\\_gesamtergebnisse\\_final.pdf](http://www.oekonsult.at/bigBrother_gesamtergebnisse_final.pdf) (15.01.2009).

<sup>103</sup> Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos y el nuevo Reglamento de Desarrollo, Instituto Nacional de Tecnologías de la Comunicación [Nemzeti Hírközléstechnikai Intézet], July 2008, lásd: [http://www.inteco.es/Seguridad/Observatorio/Estudios\\_e\\_Informes/Estudios\\_e\\_Informes\\_1/estudio\\_lopd\\_py\\_mes](http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_lopd_py_mes) (08.01.2009).

<sup>104</sup> La protección de datos personales. Lásd: [http://www.avpd.euskadi.net/s04-5249/es/contenidos/informacion/estudio/es\\_cuali/adjuntos/informe.pdf](http://www.avpd.euskadi.net/s04-5249/es/contenidos/informacion/estudio/es_cuali/adjuntos/informe.pdf) (08.01.2009).

<sup>105</sup> Lásd még Sjaak Nouwt (2005), Privacy voor doe-het-zelvers, The Hague: Sdu, ITeRSeries Vol. 73. <http://arno.uvt.nl/show.cgi?fid=41691> (27.01.2010).

<sup>106</sup> Holvast, Jan, Henny van Dijk and Gerrit Jan Schep (1989), Privacy Doorgelicht, Den Haag: SWOKA.

azokat, akik úgy gondolják, hogy az információs technológiák veszélyeztetik a magánéletet (47%).<sup>107</sup> Egy 2008-es közvélemény-kutatás a szabadságokra és a szolidaritásra irányult, s arra a következtetésre jutott, hogy a válaszadók 51%-a szerint a holland kormány megfelelően védi a magánélethez fűződő jogokat, míg 43% úgy gondolta, hogy a kormánynak erre több gondot kellene fordítania (az eredmények egy Internet háztartási panelből vett véletlen háztartási mintán alapulnak, s a közvélemény-kutatást számítógéppel segített önkitöltős interjúval végezték. A válaszadók életkora 13 év vagy több, a minta nettó 967 interjúalanyt ölelt fel).<sup>108</sup> 2009 januárjában tették közzé a nemzeti adatvédelmi hatóság megbízásából készített közvélemény-kutatás eredményeit (amely 2 016 válaszadót felölelő online felmérésen alapul). A *Nincs titkolnivalónk, mégis félünk* c. jelentés értékeli a holland polgároknak a személyes adataik gyűjtéséről és feldolgozásáról alkotott felfogását.<sup>109</sup> A polgárok többsége kész felfedni személyes adatait, ám ez nem jelenti azt, hogy nincsenek tudatában magánélethez fűződő jogaikkal. A legtöbb polgár ugyan tudatában van jogainak, de adataik kiszolgáltatására való hajlandóságukat inkább úgy kell tekinteni, mint ami elkerülhetetlen, és mint belenyugvást, s nem mint az adatok helyes kezelésébe vetett bizalmat. A csoportos megbeszéléseken ugyanis a válaszadók a személyes adatok feldolgozásának veszélyeivel kapcsolatos aggályaiknak adtak hangot, jóllehet a gyakorlat megváltoztatását súlyos feladatnak tartották. Az ellenőrzést és az átláthatóságot az adatfeldolgozás elfogadását tekintve fontosnak látták, és érdekeltységüket fejezték ki nyilvántartott személyes adataik rendszeres felülvizsgálatát illetően. Végül meglehetősen nagyobb bizalmat tápláltak személyes adataik megfelelő felhasználása és feldolgozása iránt, ha azt a kormányzati szervek, s nem magánvállalkozások vagy –intézmények végzik.

A Szlovéniában végrehajtott közvélemény-kutatás szerint a nemzeti adatvédelmi hatóságot a legmegbízhatóbb állami intézményeknek minősítették.<sup>110</sup> Más felmérés e tárgyban jelen összehasonlító tanulmány készítőinek nem állt rendelkezésére.

Magyarországon az alkotmánnyal kapcsolatos tudatosságra és az alkotmány ismeretére vonatkozó közvélemény-kutatást végeztek 2005-ben (1 000 válaszadót felölelő reprezentatív mintán).<sup>111</sup> A válaszadók 8,1%-a úgy vélte „a jelenlegi alkotmány szerint a magánélethez fűződő jog gyakorlása egyáltalán nem lehetséges; 56,5%-a szerint az csak korlátozottan gyakorolható; és 33,5% szerint az a legnagyobb mértékben gyakorolható”. Arra a kérdésre, kell-e vagy nem változtatni a magánélet védelmének szintjén, a válaszadók 38,9%-a úgy vélte, hogy a védelem szintje megfelelő, 58,3% magasabb szintű védelmet kívánt volna.<sup>112</sup> 2008-ban az Országgyűlési Biztos Hivatala adott közvélemény-kutatásra megbízást az

---

<sup>107</sup> Smink, G.C.J., A.M. Hamstra and H.M.L. van Dijk (1999), *Privacybeleving van burgers in de informatiemaatschappij*, Den Haag: Rathenau Instituut, Werkdocument 68.

<sup>108</sup> Dieter Verhue, Harmen Binnema & Rogier van Kalmthout (2008), *Nationaal Vrijheidsonderzoek. Meting 2008. Opiniedeel, April 2008, p. 36.* [http://www.4en5mei.nl/mmbase/attachments/158819/p4751\\_vrijheidsonderzoek\\_opiniedeel\\_v4\\_read\\_only.doc](http://www.4en5mei.nl/mmbase/attachments/158819/p4751_vrijheidsonderzoek_opiniedeel_v4_read_only.doc) (27.01.2010).

<sup>109</sup> J. Koffi jberg et al. (2009), *Niets te verbergen en toch bang; Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Amsterdam: Regioplan, publication number 1774. [http://www.cbweb.nl/downloads\\_rapporten/rap\\_2009\\_niets\\_te\\_verbergen\\_en\\_toch\\_bang.pdf](http://www.cbweb.nl/downloads_rapporten/rap_2009_niets_te_verbergen_en_toch_bang.pdf) (27.01.2010).

<sup>110</sup> [http://www.ip-rs.si/index.php?id=272&tx\\_ttnews\[tt\\_news\]=621](http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=621) (30.12.2008).

<sup>111</sup> A közvélemény-kutatást az Eötvös Károly Intézet és az Eötvös Loránd Tudományegyetem Jogsziológiai Intézete közösen végezte.

<sup>112</sup> Majtényi László: *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága.* 2006, Budapest, Complex Kiadó. pp. 58-61.

országgyűlési biztos intézménye ismertségének és megítélésének felmérése céljából.<sup>113</sup> A felmérés (1 000 válaszadót felölelő minta) szerint a biztos intézmény aktív ismertsége a polgárok körében 1998 óta 15%-ról 2007-ben 32%-ra emelkedett; a válaszadók 59%-ának volt ismerete a nemzeti AVH-ról; a válaszadók 11%-a egészen biztosan, további 28%-a pedig valószínűleg a hivatalhoz fordulna jogorvoslatért jogai megsértése esetében. A társadalomnak a fontosabb közintézményekbe vetett bizalmát illetően – a válaszadók 52%-a bízik a biztos intézményben – az országgyűlési biztos intézményébe vetett bizalmi index a harmadik helyet foglalja el.

Az Egyesült Királyságban az Információs Biztos Hivatala közvélemény-kutatásokat végez az adatvédelem társadalmi ismertségének nyomon követésére. A legfrissebb eredmények szerint tíz százalékponttal csökkent (a 2006. évi 49%-ról 39%-ra 2007-ben) azoknak a válaszadóknak az aránya, akik úgy vélik, a hatályos jogszabályok megfelelően védik a személyes adatokat. A 2007-ben végzett közvélemény-kutatás keretében 1 223 telefonos interjú készítették. Kvóta szerinti kiválasztással tervezett mintával gondoskodtak arról, hogy a válaszadók köre felölelje a nem, életkor, etnikum és egyéb jellemzők alapján képzett sajátos csoportokat. A 2004 és 2007 között végzett közvélemény-kutatások eredményei azt mutatják, hogy a válaszadóknak az információk megismerésére vonatkozó joguk tudatossága (ha adott eset erre ösztönzi) 2004 óta 74%-ról 90%-ra emelkedett, s úgy vélték, joguk van a szervezetek által róluk tárolt információ megismeréséhez. Amikor a válaszadókat arra kérték, értékeljenek egy személyes adataik kezelésével kapcsolatos tipikus aggodalmakat felsoroló listát, a válaszadók 83-94%-a minden esetben az állította, hogy nagyon vagy meglehetősen aggódnak. A legtöbb aggodalom mutatkozott a személyes adatok más szervezeteknek való továbbításával és eladásával, továbbá a személyes adatok biztonságával szemben.<sup>114</sup>

A fenti kutatási eredményeket egészíti ki az Eurobarometer közvélemény-kutatásainak egy fontos megállapítása, mely szerint a nemzeti hatóságok az EU polgárok számára viszonylag ismeretlenek. Ezt alapvető problémának tekinthetjük, ami magyarázza a rájuk ruházott jogosultságok ismeretének hiányát. Következésképpen az ismertségnek ez a hiánya jogtudatosságuk és az adatvédelmi hatóságok hatáskörei, feladatai, erőforrásai és tevékenysége ismertségének hiányához vezet.

A, jogtudatosságra – ideértve az adatvédelmi jogszabályoknak megfelelő gyakorlatok, továbbá a szankciók, kártérítés és jogkövetkezményekkel kapcsolatos gyakorlatok ismertségét – vonatkozó legfontosabb információforrást az Eurobarometer és más szervezetek közvélemény-kutatásai képezik. A spanyol Nemzeti Hírközléstechnikai Intézet által végzett közvélemény-kutatás (lásd fentebb) némi utalást tartalmaz a nemzeti jogszabályok által előírt nyilvántartásba vételi kötelezettség ismertségéről. Mint fentebb említettük, a felméréssel érintett vállalkozások 82%-a megerősítette, tudatában van annak, hogy eleget kell tennie a vonatkozó jogszabályoknak, míg 79%-a úgy nyilatkozott, hogy szándékában áll anyagi és ember erőforrást áldozni az adatvédelmi jogszabályok megfelelő végrehajtására. Ezek az adatok biztatóak, különösen abban a tekintetben, hogy az Eurobarometer közvélemény-kutatása szerint a vállalkozásoknál az adatvédelmi kérdésekért felelősséget viselő személyek

---

<sup>113</sup> Szonda Ipsos Média-, Vélemény- és Piackutató Intézet, [http://www.obh.hu/szonda\\_ipsos\\_OBH.doc](http://www.obh.hu/szonda_ipsos_OBH.doc) (26.01.2009.01.26.).

<sup>114</sup> Report on Information Commissioner's Office Annual Track 2007, p. 7, para. 4.2. Lásd: [http://www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/ico\\_annual\\_track\\_2007\\_individuals\\_report.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_track_2007_individuals_report.pdf). (24.02.2010). A közvélemény-kutatás keretében felelt kérdések és a válaszok részletei e jelentésben olvashatók.

56,1%-a némiképp, 30,2%-a nem igazán, s csak 13,1%-a ismeri alaposan a nemzeti adatvédelmi jogszabályok rendelkezéseit.

## **5. A hiányosságok elemzése**

A jelentés e részében elemzi a személyesadat-védelmi rendszerben EU és nemzeti szinten mutatkozó hiányosságokat. Először az adatvédelmi hatóságok körüli kihívásokkal foglalkozik, majd a vonatkozó jogszabályoknak való megfeleléssel, jogorvoslattal, és a magánélethez fűződő jogok megsértésével kapcsolatos kártérítéssel és szankciókkal, valamint a jogtudatosság fokozását célzó tevékenységgel. Ezt követően azonosítja a jelentés azokat a fő területeket, amelyeket az adatvédelmi jogszabályok alkalmazási köréből kizártak, hatálya alól mentesítettek, vagy egyébként nem tartoznak e jogszabályok alkalmazása körébe.

### **5.1 Az adatvédelmi jogszabályok hiányosságai**

#### *5.1.1 Az adatvédelmi hatóságok*

Néhány hiányosság mutatkozik az adatvédelmi hatóságok szervezete, működése és gyakorlata tekintetében. Strukturális szinten a legfőbb probléma több felügyelő hatóság függetlenségének hiányából adódik. Több tagországban (pl. Litvánia, Lettország, Észtország, Írország, Egyesült Királyság) aggodalomra ad okot az AVH tisztségviselői tényleges alkalmassága feladatai teljes önállósággal való ellátására. E hiányosságot leginkább a tisztségviselők jelölését vagy kinevezését szolgáló eljárás magyarázza, amikor is a kormány kizárólagos jogosultsága a tisztségviselőknek a jogalkotó javaslatát, véleményét vagy egyetértését nélkülöző kiválasztása, mint azt a 3.1.1 részben kifejtettük, ami a felügyelők tényleges alárendeltségének vagy kirekesztettségének kockázatát jelentősen fokozza. Megoldásul a jelölési/kinevezési eljárás reformja kínálkozik. Az adatvédelmi irányelv további lehetséges módosításával a függetlenség követelményei pontosíthatók és részletezhetők /lásd jelenleg a 28. cikk (1) bekezdés/.

A funkcionalitás szintjén több adatvédelmi hatóság esetében az alacsony létszám és a kellő pénzforrások hiánya a legfőbb probléma. Az AVH számos tagállamban nem képes feladatai maradéktalan ellátásra, mert az anyagi és emberi erőforrások korlátozottan állnak rendelkezésére. Ez a helyzet Ausztriában, Bulgáriában, Romániában, Cipruson, Franciaországban, Görögországban, Olaszországban, Lettországban, Hollandiában, Portugáliában és Szlovákiában. Az pénzügyi függetlenség és a szakképzett hivatásos személyi állomány a felügyelő hatóságok számára nemcsak elengedhetetlen eleme a személyes adatokhoz fűződő jogok hatékony védelmének, hanem egyúttal előfeltétele a kormány akaratától való tényleges függetlenségének is. A jogszabályi reformok az AVH költségvetése növelésére és emberi erőforrásai kiválasztására irányulhatnak (lehetővé téve például, hogy különleges szakértelemmel rendelkező személyeket alkalmazzanak).

Az operativitás szintjén számos felügyelő ügynökség korlátozott hatásköre ad aggodalomra okot. Egyes tagállamokban az adatvédelmi hatóságoknak nincs teljes hatáskörük vizsgálatok folytatására, az adatfeldolgozási műveletekbe való beavatkozásra, jogi tanácsadásra és jogi eljárásokban való részvételre, amint azt az adatvédelmi irányelv 28. cikk (2), (3) és (4) bekezdései részletezik. Ausztriában, Magyarországon és Lengyelországban a felügyelő szervek nem kényszeríthetik ki az adatfeldolgozó vagy -kezelő jogellenes tevékenysége megszüntetésére vonatkozó döntéseik végrehajtását. Belgiumban és Németországban nem rendelhetik el az adatok zárolását, törlését vagy megsemmisítését, sem a feldolgozás ideiglenes felfüggesztését vagy végleges megszüntetését. Az Egyesült Királyságban és Franciaországban bírósági végzés nélkül nem léphetnek be azokba a helyiségekbe, ahol személyes adatok feldolgozása folyik. Sok országban (pl. Írországban, Lengyelországban, a



Cseh Köztársaságban, Litvániában, Magyarországon, Máltán, Olaszországban, Franciaországban, Romániában, Szlovéniában, az Egyesült Királyságban, Ausztriában, Görögországban) a jogalkotó a felügyelő szervekkel csak esetlegesen konzultál magánéletet vagy adatvédelmet érintő jogszabálytervezetek készítése során, mert a jogalkotónak ez nem kifejezett kötelezettsége. Az adatvédelmi irányelv követelményeinek teljességet nélkülöző átültetése, amellyel, hogy sérti az EU jogot, a nemzeti adatvédelmi rendszer jelentős hiányossága, amely veszélyezteti a rendszer hatékonyságát. Minthogy az EU jog az adatvédelmi hatóságok hatásköréről felettébb világosan rendelkezik, a nemzeti jogszabályokat szükség esetén módosítani kell, hogy a belső szabályok megfeleljenek az EU szinten rögzített követelményeknek.

### *5.1.2 Megfelelőség*

Különböző hiányosságok mutatkoznak a vonatkozó adatvédelmi jogszabályok tényleges megfelelése tekintetében, főleg az adatfeldolgozási műveleteket végző köz- és magánjogi szereplők nyilvántartásba vételi kötelezettségét illetően. Jóllehet az adatvédelmi jogszabályok tényleges megfelelésének értékelése megbízható és pontos információ hiányában számos tagállamra nézve nehézkes, úgy tűnik, egyes országokban (pl. Bulgáriában, Dániában, Lettországon, Hollandiában, Portugáliában, Szlovákiában, Romániában) új tántorg a magánéleti jogok védelméről alkotott felfogás, amely formálisan összhangban van az EU és a nemzetközi jog követelményeivel, és azok tényleges védelmét rögzítő hatályos jogi rendelkezések között. Az adatvédelmi jogszabályok megfelelése például meglepően alacsony Észtországban és Romániában. Legtöbb országban viszont az egyes fogalmak (pl. 'személyes adat', 'adatállomány', 'feldolgozás') világos meghatározása (vagy egységes értelmezése) bizonytalanságokhoz vezet abban a tekintetben, hogy mely tevékenységek tartoznak a személyes adatokat érintő jogszabályok hatálya alá. A 29-es Munkacsoport kulcsszerepet játszik e homályos fogalmak egységes értelmezése terén, ám ez a folyamat attól is függ, elfogadják-e és alkalmazzák-e ezeket az értelmezéseket a tagállamokban. Bonyolultsághoz és ellentmondásokhoz vezethet, ha az adatvédelmi rendelkezéseket különféle ágazat-specifikus jogszabályok között osztják szét, mint Finnországban és Görögországban. E szempontból, míg az adatvédelmi jogszabályok érvényesítése az érintett felekkel szemben megfelelően szolgálhatja az első probléma megoldását, a jogszabályok módosításával, vagyis a homályos rendelkezések cseréjével és a jogrendszer egyszerűsítésével segíthetünk a másodikon. Az adatvédelmi jogszabályok bonyolultságával és bizonytalanságával kapcsolatos hiányosságok nagymértékben az adatvédelmi irányelv szövegezésében rejlenek; ennek legjobb megoldását ezért EU szinten kereshetjük.

Egyes tagállamokban (mindenek előtt az Egyesült Királyságban) a legfőbb probléma abból adódik, hogy az adatfeldolgozási műveletek megkezdését megelőzően széles körűen figyelmen kívül hagyják az adatvédelmi hatósághoz való bejelentés alapvető kötelezettségét. Visszatérő példa a térfelügyelő kamerák esete: Ausztriában, Bulgáriában, Franciaországban, Litvániában, a Cseh Köztársaságban és Svédországban a térfelügyelő kamerák nagy többségét nem jelentik be, ezért a nemzeti felügyelő szervek azokat nem is felügyelhetik vagy ellenőrizhetik. Egy másik felettébb aggályos terület az Internet (pl. Spanyolország és Szlovénia). Az adatfeldolgozó vagy adatkezelő bejelentési kötelezettségének figyelmen kívül hagyása nem annyira tudatos mulasztás, mint inkább a jogszabályok kellő ismeretének hiánya. Ez a hiányosság sajátos kihívást jelent az adatvédelmi jogszabályok hatékonyságával szemben. Azoknak a nehézségeknek ellenére, amelyekkel a jogalkotónak szembe kell néznie midőn lépést akar tartani a korszerű technikai fejlesztésekkel, újabb, az adatvédelemhez fűződő jogokra hatást gyakorló technikákat (kamerás megfigyelés, telefonlehallgatás, sejtminiták vagy DNA kód rögzítése) szabályozó rendelkezésekkel kell kiegészíteni vagy javítani a jogszabályokat, s erre sürgősen szükség van (azért is, hogy elkerülhető legyen az

adatvédelemhez fűződő jogoknak a vagyoni helyzet alapján való megkülönböztetése, mint a Cseh Köztársaságban).<sup>115</sup>

### 5.1.3 Szankciók, kártérítés, jogkövetkezmények

Bizonyos problémák adódnak a jogorvoslatok, szankciók és kártérítés belföldi rendszeréből, valamint az adatvédelmi szabályok alkalmazásából a foglalkoztatás terén. Az adatvédelmi hatóságok által kiszabható szankciók az egyes országokban különfélék, egyrészt mert a bírságoknak korlátozott a visszatartó ereje, másrészt mert kiszabásukra ritkán kerül sor, vagy az adatvédelmi szervek egyszerűen nem dolgozták ki kiszabásuk gyakorlati szabályait (Lengyelország, Ausztria, Egyesült Királyság, Finnország, Magyarország, Litvánia, Dánia, Belgium). Az adatokhoz való jogosulatlan hozzáférésnek az adatkezelő vagy -feldolgozó által való jelentését illető jogszabályi kötelezettség hiánya néhány tagállamban (pl. Írországból) fokozhatja a végrehajtás rendszerének hiányosságait. Néhány tagállamban (pl. Németország, Lettország, Hollandia, Lengyelország, Egyesült Királyság, Ausztria, Franciaország, Magyarország) az adatvédelem megsértése esetén a szankcionálásnak és büntető eljárás indításának lehetősége felettébb korlátozott. Károkozás tekintetében számos tagállamban (pl. Finnország, Írország, Hollandia, Egyesült Királyság, Ciprus, Málta, Lengyelország, Lettország, Észtország és Svédország, a magánjogi személytől nyerhető kártérítést illetően) a nemzeti jogrendszer kifejezetten kizárja az adatvédelmi jogok megsértésével okozott kár megtérítését több olyan tényezőre való hivatkozással, mint a bizonyítási teher, a kár megszerzésének megállapítása, a – főleg az adatvédelmet elősegítő tevékenységet folytató – felügyelő szervek támogatásának hiánya. Míg az *ex ante* „puha” módszerek alkalmazása a megfelelés biztossága érdekében helyes gyakorlatnak tekinthető, elengedhetetlen, hogy a tagállamok „kemény” jogi eszközökkel is rendelkezzenek, hogy azokat, akik a magánéletükbe fűződő jogokat megsértik, megbüntethessék, és az áldozatokat ért kár megtérítésére kötelezhessék. A jogszabályi reformok, főleg nemzeti szinten, megfelelő szerepet játszhatnak azáltal, hogy – jogorvoslat formájában – hatékonyabb és átfogóbb jogi ellenszerről gondoskodnak. Ezzel egyidejűleg az adatvédelmi jogok tudatosságának fokozása az érintettek, a bírók és az ügyészek körében hozzájárulhat az adatvédelmi jogszabályok megsértését büntető hatályos rendelkezések jobb végrehajtásához.

Sok tagállamban (Belgium, Svédország, Románia, Egyesült Királyság, Bulgária, Málta, Litvánia, Ciprus, Franciaország, Észtország, Dánia és Ausztria) még mindig hiányoznak a munkaviszony keretében kezelt adatok védelmét szolgáló sajátos jogszabályok, elmulasztván így elismerni, hogy különös adatvédelmi rendelkezésekre van szükség a személyes adatok felhasználásának szabályozására a foglalkoztatási ágazatban. Ennek következtében egyes országokban sérelmet szenvednek az egyén személyes jogai (pl. Cipruson, Svédországban és Németországban), mert rejtett videokamerákkal figyelik meg munkahelyükön a dolgozókat. Más tagállamokban (pl. Finnország) ellenben, jóllehet a jogi keretek mindmáig megfelelőek voltak, a jogszabályok új keletű módosítása valójában gyengítette a védelmet a foglalkoztatási környezetben.<sup>116</sup> Az EU, a társadalmi piacgazdaság elveinek talaján állva, nagy jelentőséget tulajdonít a munkának, és a munkavállalók szabad mozgása egyike az EU szerződésekben elismert alapvető szabadságoknak. Minthogy a tagállamok eltérő jogszabályi kedvezőtlen hatást gyakorolhatnak a belső piac működésére, az EU beavatkozása ebbe az ágazatba a foglalkoztatási környezetben kezelt személyes adatok védelmét szolgáló minimális

<sup>115</sup> Bővebben lásd az un. 'openCard' eset: <http://opencard.praha.eu/jnp/en/home/index.html> (23.01.2009).

<sup>116</sup> <http://www.hs.fi/english/article/Lex+Nokia+passes+in+Parliament+-+government+party+ranks+split/1135244038215> (09.03.2009).



követelmények meghatározása céljából, felettébb kívánatos lenne. Ez ugyanakkor, tiszteletben tartva a szubszidiaritás elvét, a dolgozók alapvető jogai teljes körű védelmének biztosítása szempontjából is lényeges, hiszen ezt a tagállamok közös alkotmányos hagyományai és a vonatkozó EU jogszabályok is elismerik.

#### *5.1.4 Jogtudatosság*

Fentebb, a 4.4. részben összehasonlító áttekintést adott a jelentés a jogtudatosságról. Alább, a 6.3 részben a jogtudatossággal kapcsolatos helyes gyakorlatokat tárgyalja. Az adatvédelmi hatóságok általában folytatnak jogtudatosságot fokozó tevékenységet az érintettek különféle köreiben.

Mindazonáltal néhány negatív példa is azonosítható (pl. Észtország, Románia), ahol az adatvédelmi hatóságok tudatosságfokozó tevékenységet nem folytatnak. Számos tagállamban (pl. Litvániában, Bulgáriában, Szlovákiában) a felügyelő hatóságok mindezülig nem hoztak létre felhasználóbarát és/vagy átfogó, frissített Internetes oldalt, ahol a nagyközönség hozzáférhet minden, adatvédelemre vonatkozó információhoz, s ahol az adatvédelmi hatóság véleményei és szabálytervezetei rendelkezésre állnak. Aggodalomra ad okot továbbá az adatvédelmi hatóság tevékenységének nyilvánossága és átláthatósága egyes országokban (pl. Bulgária, Málta), különösen amikor a felügyelő hatóság barátságos vitarendezési megoldásokról tárgyal az adatvédelmi jogszabályok megsértőivel anélkül, hogy ezt nyilvánosságra hozná (pl. az Egyesült Királyságban). Végül több tagállamban (pl. Ausztria, Görögország) míg a felügyelő hatóság működése általában szólva kielégítő, felettébb hosszú időbe telik, míg az érintett megkapja az információt, gyakran azért, mert az AVH nem rendelkezik elegendő erőforrással ahhoz, hogy minden, az érintettektől érkező kérelemre gyorsan válaszoljon. Kétséges ezért, hogy egy újabb jogalkotás, akár EU, akár nemzeti szinten, javíthat a jelenlegi helyzeten. Inkább az adatvédelmi hatóságoknak kellene munkájukat átszervezniük ahhoz, hogy az érintettek azonnali támogatást nyújtsanak. Hozzáálláson kellene tehát változtatniuk tevékenységük nyilvánossága és az érintett felek adatvédelemhez fűződő jogaik tudatosságának fokozása érdekében. Az adatvédelmi hatóságoknak e hiányosságok kiküszöbölése céljából fel kellene ismerniük a jogtudatosság fokozásában játszott gyakorlati szerepük jelentőségét, készségesen tanulva más európai felügyelő hatóságok helyes gyakorlatából.

Ennél is nagyobb probléma, hogy néhány tagállam (pl. Egyesült Királyság) adatvédelmi hatósága szerint nem feladatuk nemzeti adatvédelmi jogszabályaiknak az EU- és más nemzetközi, személyes adatok védelmét szolgáló jogszabályokkal konzisztens értelmezése. (még ha a nemzeti jogszabályok nagymértékben a vonatkozó EU és nemzetközi rendelkezések belföldi alkalmazásával járnak is). A nemzeti adatvédelmi hatóságok működése valójában jelentősen hozzájárul az adatvédelemhez fűződő jogok alapelveinek egységes értelmezéséhez. Helyes gyakorlatként dicsérhető ezért (spontán) konvergenciájuk nemcsak a különféle jogrendszerek konzisztenciájának biztosítása terén, hanem a magánélethez fűződő jogok védelmére vonatkozó megfelelő szabályok megalkotása tekintetében is. A jogszabályok ereje e téren korlátozott: a nemzeti felügyelő hatóságok megközelítésén kell változtatni, s inkább a kultúra, mint a politika vagy jogalkotás szintjén.

## **5.2 Az adatvédelem problematikus területei**

Ezen rész azonosítja azokat a fő problematikus területeket, amelyeket az adatvédelmi jogszabályok alkalmazási köréből kizártak, hatálya alól mentesítettek, vagy egyébként nem tartoznak e jogszabályok alkalmazása körébe. E tekintetben három széles kategóriát kell említeni: a nemzetbiztonsággal kapcsolatos tevékenységek (pl. hírszerzés, katonai tevékenységek) kizárása az adatvédelem rendszeréből; egyéni egészségügyi adatok védelme; és a kamerás megfigyelés.

### *5.2.1 Adatvédelem a nemzetbiztonság területén*

Az adatvédelmi irányelv 13. cikke (mentességek és korlátozások) (1) bekezdése rögzíti, hogy a „tagállamok jogszabályokat fogadhatnak el a 6. cikk (1) bekezdésében, a 10. cikkben, a 11. cikk (1) bekezdésében, valamint a 12. és a 21. cikkben foglalt jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás az alábbiak biztosításához szükséges: a) nemzetbiztonság; b) honvédelem; c) közbiztonság”.

Az adatvédelmi irányelv 13. cikk.(1) bekezdésének a)-c) pontjai egymással összefüggésben állnak. Egyes tagállamokban (Luxemburg, Dánia, Írország, Románia, Görögország és Portugália) ezeket mint az adatvédelmi jogszabályok hatálya alól kizárt fő területekként azonosították, ami az adatvédelmi irányelv 13. cikke szövegezésének a következménye. Mindazonáltal e rendelkezés értelmezése tekintetében három fontos kérdést kell megvizsgálnunk.

Először is a szövegezés a biztonság tekintetében „korlátozásra” ad lehetőséget. Ez azonban nem egyenértékű az irányelv alkalmazásának hatálya alól való „mentességgel”. Egy nyelvtani értelmezés nem az egyetlen oka annak a megállapításnak, hogy a végrehajtó hatalom különféle ágazatainak tevékenységi területe az irányelv hatálya alá tartozik.

Másodszor az irányelv preambulának első bekezdése szerint az emberi jogok európai egyezménye a személyes adatok védelmének hátterét képezi. A preambulum harmadik bekezdése továbbá kifejezetten rögzíti, hogy az egyének alapvető jogait is biztosítani kell. Amint azt ennek az összehasonlító tanulmánynak más részeiben is említettük, az emberi jogok és az egyén sérthetlenségének védelme az adatvédelem alapvető feltétele.<sup>117</sup>

Harmadszor az irányelv építménye általában és lényegében nem arra szolgál, hogy abból egy olyan, nem felügyelt részt faragjanak ki, melyben az államok a jogi követelmények körén kívül működhetnek. Ellenkezőleg, nemzetbiztonsági kérdésekkel szemben arányossági próbát kell végezni, vagyis egyensúlyt kell teremteni az alapvető jogok és egyéb érdekek között, s nem egyszerűen figyelmen kívül hagyni az előzőt.

Negyedszer az irányelvet az EU alapjogi Chartája 8. cikkével összefüggésben kell értelmezni, mely az Európai Unióról szóló szerződés új, 6. cikkének megfelelően „ugyanolyan jogi kötőerővel bír, mint a Szerződések”. A 8. cikk csak a Charta 52. cikkében rögzített feltételek mellett korlátozható. Az adatvédelmi irányelv 13. cikk (1) bekezdése széleskörű kivételekről és korlátozásokról rendelkezik a közbiztonság, a honvédelem és a nemzetbiztonság (beleértve az ország gazdasági jólétét is, ha a feldolgozási művelet nemzetbiztonsági ügyre vonatkozik), valamint a büntetőjog területén végzett állami tevékenységek tekintetében. E korlátozások és kivételek terjedelme azonban nem világos. Egyes tagállamokban e területeket mindösszesen kiemelik az adatvédelmi jogszabályok hatálya alól, ami meglehetősen nagy, szabályozatlan területet hagy súlyos következményekkel az alapvető jogok védelme tekintetében. A Charta 52. cikke szerint a „Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, és e jogok lényeges tartalmának tiszteletben tartásával korlátozható”. Következésképpen a nemzeti jogalkotónak az a döntése, hogy általános kivételt állapít meg a végrehajtó hatalom egyes ágazatai (pl. a hírszerzés vagy a honvédelmi minisztérium) részére, nem illeszthető bele az adatvédelmi irányelv normatív keretébe.

### *5.2.2 Az egyén egészségi állapotára vonatkozó adatok védelme*

Több országban (pl. Svédországban, Bulgáriában és Szlovéniában) aggályok merültek fel az egészségi állapotra vonatkozó adatok védelme tekintetében. Az adatvédelmi irányelv 8. cikk

---

<sup>117</sup> Lásd: 2.2. Adatvédelem az Európa Tanács keretében.

(2) bekezdése arra kötelezi a tagállamokat, hogy tiltsák<sup>XIII</sup> az egyén egészségi állapotára vonatkozó adatok feldolgozását. A 8. cikk (3) bekezdése e kötelezettség alól mentesít, „ha az adatok feldolgozása megelőző egészségügyi, orvosi diagnosztikai célból, gondozás vagy feldolgozás alkalmazása vagy egészségügyi szolgáltatások igazgatása céljából szükséges, és ha az adatokat a nemzeti jog vagy az illetékes nemzeti testületek által meghatározott szakmai titoktartási kötelezettség alá eső egészségügyi szakember vagy azzal egyenértékű titoktartási kötelezettség alá eső más személy dolgozza fel.”

Az, hogy az egészségügyi szakemberek a beteg minden adatához hozzáférhetnek, fokozza a hatékonyságot, és – amikor az idő fontos szerepet játszik – szükséghelyzetben is alkalmazható. Ez azonban azzal jár, hogy többen is hozzáférhetnek a különleges adatokhoz (ami a személyes sérthetlenség fokozott sérelmét jelenti, növekszik továbbá a különleges adatok kiszivárogtatásának kockázata. A hozzáférhetőség eldönthető például a pozíció, a szakorvosi képesítés és a meghatározott együttműködés alapján). Az ugyanahhoz a szervezethez tartozó, rendszeresen együttműködő részlegeknek indokolt hozzáférniük egymás adataihoz, feltéve, hogy bizalmas kezelésükről gondoskodtak. A felhasználó azonosításának meg kell felelnie a biztonsági korlátozásoknak.

Egy EU-jogszabály nyújtotta kényszerzubbonyszerű megoldás súlyos, nemkívánatos hatást gyakorolhat a tagállamok egészségügyi ágazatára. Helyesebbnek látszik arra törekedni, hogy az egészségügyi szakemberek titoktartásra és a magánélet védelmére vonatkozó kötelezettségének szabályai összhangban legyenek az irányelv céljaival, gondoskodván az egyének jogainak hatékony védelméről, anélkül hogy egyúttal gyengítenénk egészségi állapotához fűződő jogait.<sup>118</sup>

Néhány tagállamban a jogalkotók e tárgyban jogszabálytervezeteket készítettek. Belgiumban például rendeletet javasoltak egy „e-health” platform létrehozására,<sup>119</sup> <sup>XIV</sup> melynek keretében egészségügyi és egyéb adatok cserélhetők egészségügyi szakemberek és intézetek között az egészségügyi rendszer egyszerűsítése és fejlesztése céljából. A rendszer alkalmas gyógyszerkészítmények elektronikus receptjeinek továbbítására is. Mivel azonban ezzel orvosok, kórházak, egészségbiztosító szervek és egyes társadalombiztosító intézmények is élhetnek, kérdéses, hogy a betegek magánélete elegendő védelemben részesül. Az egészségi állapot különleges területét érintő nemzeti jogszabályok tervezésekor az érintettek jogait gondosan mérlegelni kell.

### 5.2.3 A kamerás megfigyelés adatvédelmi kérdései

Mint fentebb már említésre került, a kamerás megfigyelés aggodalomra ad okot. Ausztriában a térfelügyelő kamerák túlnyomó többségét egyáltalán nem jelentik be, ezért a nemzeti adatvédelmi hatóságok azokat nem is felügyelhetik vagy ellenőrizhetik. Németországban a hírek szerint egyes munkahelyeken rejtett kamarákkal figyelik meg a dolgozókat. A személyes önrendelkezési jogot is gyakran sérti, ha hiányos az érintett tájékoztatása adatai felhasználásáról és/vagy feldolgozásáról. A munkahelyi kamerás megfigyelés egyik nevezetes esete: Ciprus Nemzeti Versenyhatósága vezetője megfigyelte ügyintézőit, ami végül is

---

<sup>118</sup> Lásd a 29-es munkacsoport WP131 számú, 2007. február 15-én kelt munkadokumentumát az elektronikus egészségügyi nyilvántartásban (EHR) tárolt, egészségi állapotra vonatkozó személyes adatok feldolgozásáról: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm) (2010.11.25.).

<sup>119</sup> Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 33/2008 (24.09.2008), available at [www.privacycommission.be/nl/docs/Commission/2008/advies\\_33\\_2008.pdf](http://www.privacycommission.be/nl/docs/Commission/2008/advies_33_2008.pdf) (24.01.2009); Commission de la protection de la vie privée, Avis no. 33/2008 (24.09.2008), available at [www.privacycommission.be/fr/docs/Commission/2008/avis\\_33\\_2008.pdf](http://www.privacycommission.be/fr/docs/Commission/2008/avis_33_2008.pdf) (24.01.2009) (French).

lemondásához vezetett. Emlékezetes, hogy Görögországban a nemzeti adatvédelmi hatóságtól megtagadták a rendőrség helységeibe való belépést. Az Egyesült Királyságban a kamerák köztéri használatát csak csekély mértékben korlátozzák, s több térfelügyelő kamera van ebben a tagállamban, mint a világon bárhol másutt.<sup>120</sup>

Az adatvédelmi irányelv a kamerás megfigyelésre vonatkozó részletes útmutatást nem tartalmaz. A preambulom 14. bekezdése így szól: „a természetes személyek hang- és képadatainak felvételére, továbbítására, feldolgozására, rögzítésére, tárolására és közzétételére használatos módszereknek az információs társadalom keretén belül történő fejlesztésének fontosságát figyelembe véve ennek az irányelvnek alkalmazhatónak kell lennie az ilyen adatokhoz kapcsolódó feldolgozásra”. Ez úgy is értendő, hogy ilyen adatok általában kimerítik a 'személyes adat' értelmezését, ahogyan erről az adatvédelmi irányelv 2. cikke rendelkezik, s így az egyén e tekintetben az EU jogszabályok biztosította védelmet élvezheti.

Mindazonáltal az adatvédelmi irányelv 33. cikke úgy rendelkezik, hogy a „Bizottság megvizsgálja ezen irányelvnek különösen a természetes személyekkel kapcsolatos hang- és képadatok adatfeldolgozására történő alkalmazását, és benyújtja az informatika terén elért fejlesztéseket figyelembe véve az információs társadalom elért fejlődési szintjére tekintettel szükségesnek bizonyuló megfelelő javaslatokat.” Nyilvánvaló tehát, hogy az EU különös hangsúlyt fektet a kamerás megfigyelésre. Megjegyezzük továbbá, hogy e tekintetben a 29-es munkacsoport is szolgált némi útmutatással.<sup>121</sup> Figyelembe véve a hang-és képmásadatok belső technikai sajátosságait, valamint ezek messze ható potenciális hatását az egyén jogaira, meggondolás tárgyát képezi egy sajátos EU-jogszabály megalkotása.

A jogalkotó néhány országban az utóbbi időben bekapcsolódott e folyamatba, de kétséges, hogy a megfelelő utat választották. Dániában 2007. júniusában két jogszabályt fogadtak el a kamerás megfigyelés tárgyában. Az egyik magánvállalkozásoknak ad széles felhatalmazást arra, hogy az ingatlanukhoz tartozó területeken kamerás megfigyelést alkalmazzanak. A megfigyelő eszközöknek használatbavételüket megelőző bejelentése az adatvédelmi hatósághoz már nem kötelező. A második a rendőrségi hírszerző szolgálatoknak ad széles körű jogosultságot arra, hogy katonai hírszerző szolgálatokkal információt cseréljenek és egyéb közintézményektől, pl. kórházaktól, iskoláktól, könyvtáraktól, szociális intézményektől stb. bírósági végzés nélkül információt gyűjtsenek, továbbá széles körű jogosultságot ad a rendőrségnek arra is, hogy közjogi és magánjogi felektől megfigyelő kamerák üzembeállítását és használatát követelje.

A kamerás megfigyeléssel kapcsolatos adatvédelem széles körű vita tárgyává vált: kell-e korszerűsíteni az adatvédelmi jogszabályokat ahhoz, hogy lépést tartsunk a technikai fejlődéssel. Az új keletű és folyamatban lévő technikai fejlesztések (többek között: „számítási felhő” és „autonóm számítástechnika”, ECT-beültetés az emberi testbe, nanotechnológiák, agy/gép interfész) kihívásaira sürgősen választ kell adni. Az internet és az új közösségi hálózati technikák, pl. a „facebook” és a „twitter”, személyes adatokkal kapcsolatos alapvető jogok védelmére gyakorolt hatását ugyancsak megfelelően figyelembe kell venni. Az egyén „digitális azonosságának” jelentőségét pedig aligha lehet túlhangsúlyozni,<sup>122</sup> hiszen manapság

---

<sup>120</sup> <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm#a41>, at para 213 (06.10.2009).

<sup>121</sup> Lásd a 2002. november 25-én kelt, WP67 számú munkadokumentum [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2002/wp67\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf) (24.02.2010); opinion 4/2004, WP 89 from 11 February 2004, [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp89\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf) (24.02.2010)

<sup>122</sup> Report with a proposal for a European Parliament recommendation to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)), Committee on Civil Liberties, Justice and Home

az egyén általános azonossága és személye lényeges komponensét képezi, s mint ilyen, a személy „hagyományos” jellemzőivel megegyező szintű védelmet érdemel. A digitális azonosság kibogozhatatlanul kötődik az egyén „digitális létezéshez”. A széles kibernetikai térben az egyén alkothatja meg jelenlétének jellemzőit, és ott olyan tevékenységet végezhet, amely korábban csak a „valóságos” köztéren volt elképzelhető. E tekintetben különös figyelmet kell fordítani Internet Irányító Fórum működésére és az „Internetre vonatkozó törvényre”, ahogyan arra az Európai Parlament egyik, a biztonság és az alapvető szabadságjogok Interneten történő megerősítéséről szóló határozata hivatkozik.<sup>123</sup>

## 6. Helyes gyakorlatok

A jelentés e részében röviden áttekintjük az EU tagállamaiban követett, adatvédelmet szolgáló helyes gyakorlatok legjobbait, kiemelve a pozitív nemzeti példákat az adatvédelmi hatóságok, a megfelelőség, a jogorvoslatok és a jogtudatosság tekintetében. A „helyes gyakorlat” példáinak kiválasztása elismeri egy gyakorlat értékét és hozzájárul az állandó fejlődés kultúrájának támogatásához. A „helyes gyakorlat” kiválasztása azonban nem feltételezi, hogy azt az Ügynökség tüzetesen megvizsgálta.

### 6.1 Adatvédelmi hatóságok

A helyes gyakorlatok az adatvédelmi hatóságok tekintetében vagy a felügyelő szervek szerkezetére vagy tevékenységére vonatkoznak. Egyrészt több tagállam sajátos jogkörökkel ruházta fel nemzeti adatvédelmi hatóságait, s egyúttal nagyfokú függetlenséget biztosított számukra. Másrészt az adatvédelmi hatóságok együttműködésre léptek három kategóriába sorolható érdekelt felekkel: állami intézményekkel, e téren aktív civil szervezetekkel és más tagállamok adatvédelmi hatóságaival.

Az adatvédelmi hatóságok függetlensége a magas szintű adatvédelem lényeges tényezője. E szempontból ezért azok a szerkezeti intézkedések, melyek határozott jogi személyiséggel ruházzák fel a felügyelő szervet (mint Spanyolországban és Máltán tették), vagy jogkörét és feladatát az alkotmány rögzíti (mint Portugáliában és Görögországban), pozitív példái a felügyelő szervek függetlensége fokozásának. Még ha azokat a jogalkotó is választja, a tisztségviselők függetlenségét az nem feltétlenül biztosítja, a többség és az ellenzék egyetértését igénylő eljárás (pl. Görögországban) helyes gyakorlatnak tekinthető. Az adatvédelmi hatóság nagyfokú autonómiáját biztosító, Szlovéniában követett helyes gyakorlat továbbá, ha *locus standi* jogosultságot élvez, melynek alapján jogszabály alkotmányosságának vizsgálatát kezdeményezheti az alkotmánybíróságnál.

Az adatvédelmi hatóság jogosultsága arra, hogy aktívan bekapcsolódják a magatartási kódexek előkészítésébe, helyes gyakorlatnak tekinthető. Az adatvédelemmel kapcsolatos magatartási kódexek szerkesztésében való részvétel nemcsak a polgárok általános védelmének fokát növeli, hanem hozzájárul a nemzeti hatóságok egyre szélesedő társadalmi megjelenéséhez is, cselekvő részvételük ezért tanácsolható. Írországban például, a belföldi jogalkotó feljogosítja a nemzeti adatvédelmi hatóságot arra, hogy jogszabályalkotásra javaslatot tegyen és jogszabálytervezetet készítsen, amely, ha a jogalkotó elfogadja, jogi kötőerővel fog rendelkezni.<sup>124</sup>

---

Affairs, [http://www.europarl.europa.eu/meetdocs/2004\\_2009/documents/dv/a6-0103\\_2009\\_/a6-0103\\_2009\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/a6-0103_2009_/a6-0103_2009_en.pdf) (07.03.2009).

<sup>123</sup> T6-0194/2009 dated 26 March 2009.

<sup>124</sup> Írország adatvédelmi törvénye, 13. cikk

Az egyes közigazgatási szervek és az AVH-k együttműködése és rendszeres kapcsolata hozzájárulhat az adatvédelmi rendszer egészének zökkenőmentes működésének biztosításához. Németországban például széleskörű képzési programokat szerveznek egy adatvédelmi akadémia keretében, amely átfogó és rendszeres tanfolyamokat dolgozott ki a közigazgatás valamennyi területére.

A szoros együttműködés és kapcsolat az adatvédelem területén aktív civil szervezetekkel számos előnnyel jár. A civil szervezetek egyrészt abban a helyzetben vannak, hogy jelezhetik az adatvédelmi jogszabályok rendszeres és/vagy kirívó megsértését a nemzeti hatóságoknak és a nagyközönségnek egyaránt. Ily módon afféle informális felügyelő szerv szerepét játszhatják. Egyes esetekben hatékonyan hozzájárulnak az adatvédelem átfogó ellenőrzéséhez. A civil szervezetek másrészt 'alulról felfelé' irányuló információs csatornaként szolgálnak, lehetőséget nyújtva az aktív polgároknak arra, hogy javaslatot tegyenek a jogszabályok módosítására. E szempontból a magyar adatvédelmi hatóság a hírek szerint kész a civil szervezetek támogatására és a velük való együttműködésre. 2000-ben például véleményezte a Magyar Helsinki Bizottság által készített, roma jogokkal kapcsolatos kutatási program adatvédelmi tervét, s 2004-ben a hatóság munkatársai a Társaság a Szabadságjogokért nevű szervezettel együttműködésben számos közegészségügyi szervezetnél azt vizsgálták, hogy a HIV vizsgálatokat ténylegesen névtelenül és ingyenesen végezték-e, ahogyan azt állították. Megállapításaik alapján az adatvédelmi biztos ajánlást bocsátott ki.<sup>125</sup>

Végül az együttműködés és állandó kapcsolat más (EU és nem EU) államok adatvédelmi hatóságaival ugyancsak hasznos. Az EU szintjén ez főleg az adatvédelmi irányelv 29. cikke alapján létrehozott munkacsoport keretében valósul meg. Ez a fórum képezi azt a szükséges intézményi keretet, amely módot nyújt az AVH-knak arra, hogy vonatkozó jogszabályaik alkalmazását összehangolják. Ugyancsak ösztönözni kell a két- és többoldalú együttműködést az EU-n belül és nem EU országokkal a területi szomszédság vagy a nyelvi rokonság alapján. Jó példa erre Portugália, ahol spanyol kollégákkal informális éves találkozót szerveznek az adatvédelem főbb fejleményeinek megvitatása céljából.

## 6.2 Megfelelőség

A megfelelést tekintve a helyes gyakorlatok az adatvédelmi hatóságok erőteljes cselekvőképességéből származik, lehetővé téve a jogsértők felfedését és büntetését. Olaszországban e helyes gyakorlat egy érdekes példája a nemzeti ügynökség és a rendőrség együttműködése, melynek alapja a Pénzügyi Rendőrség egy *ad hoc* nyilatkozata. Romániában ehhez hasonlóan az adatvédelmi hatóság együttműködési megállapodást kötött olyan közigazgatási szervekkel, mint a Nemzeti Fogyasztóvédelmi Hatóság, a Román Rendőrség Általános Felügyelősége, a Pénzügyőrség, a Hírközlési és Informatikai Minisztérium és a Nemzeti Cégnyilvántartó Hivatallal.

A holland rendszer érdekes jellemzője a kormánynak az a kötelezettsége, hogy – a nemzeti jogszabály hatálybalépését követő öt éven belül – jelentést nyújtson be a holland parlamentnek a jogszabály gyakorlati hatékonyságáról és hatásáról. Ezt az értékelést a holland AVH két lépésben hajtotta végre. Az értékelés első szakaszát, amely a másodlagos forrásokra vonatkozott, 2007-ben zárták le, és az erről készített jelentést benyújtották a parlamentnek a

---

<sup>125</sup>

<http://beszelo.c3.hu/03/11/04zadori.htm> (2009.01.28.); [http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/M/2&dok=1454\\_H\\_2004](http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/M/2&dok=1454_H_2004) (2010.10.26.).



„Személyes adatok védelméről szóló törvény első fázisának értékelése” címmel.<sup>126</sup> A második szakaszban esettanulmányokat és interjúkat készítettek a személyes adatok védelméről szóló törvény gyakorlati hatékonyságáról. A jelentést 2009 februárjában tették közzé.<sup>127</sup>

### 6.3 Jogtudatosság

Fentebb, a 4.4 részben összehasonlító áttekintést nyújtott a jelentés a jogtudatosságról, és az 5.1.4 részben a jogtudatosság hiányosságait taglalta. Számos helyes gyakorlatra bukkantunk a nemzeti adatvédelmi hatóságok jogtudatosságot fokozó tevékenysége körében. Először is sok nemzeti ügynökség felhasználóbarát honlapot hozott létre, ahol az adatvédelemmel kapcsolatos információk fellelhetők, s melyek gyakorta több nyelven is olvashatók. A helyes gyakorlatok második csoportja az AVH-k oktatási tevékenységét öleli fel, amely a magánéleti kultúrát terjeszti különösen, de nem kizárólag, az ifjabb nemzedék körében. Szakmai tanfolyamokat, szemináriumokat és előadásokat szerveznek az adatfeldolgozási műveleteket végző szereplők számára. Az ilyen szereplők számára készített útmutatók ugyancsak az adatvédelmi hatóságok helyes gyakorlatát képezik. Végül külön díjakat ítélnék oda, mellyel ugyancsak az adatvédelmi jogszabályoknak való megfelelést támogatják.

A jogalkotás hatékonysága fokozása és a hatékony jogorvoslathoz jutás elősegítése céljából sok nemzeti AVH gondosan szerkesztett Internet lapokat és oldalakat hozott létre. Ezeket felkeresve hozzáférhetőek a jogalkotó hivatalos dokumentumai, bejelenthető a személyes adatok feldolgozása, tanács és/vagy információ kérhető és kapható, és panasz is benyújtható. Németországban például Schleswig-Holstein Független Adatvédelmi Központja (melyet szinte minden németnyelvű AVH támogat) honlapja széleskörű információt tartalmaz a legújabb fejleményekről, bírósági esetekről, jelentésekről és sajtóközleményekről, továbbá egy adatbázist a kulcsfontosságú koncepciókról.<sup>128</sup> Egy másik, sok mindenre kiterjedő honlapon tájékoztatást kapunk arról, hogyan védjük magunkat adatvédelmi jogaink megsértése esetén, amely un. „multiplikátor hatás”-t kifejtve oktatóknak és egyéb személynek is hasznos.<sup>129</sup> Mind Spanyolországban<sup>130</sup>, mind Olaszországban olyan adatátviteli rendszer működik, amely alkalmas az adatállományok bejelentésére az Interneten.

Sok esetben a hivatalos Internet-lap többnyelvű, egyrészt az adott tagállam nyelvi rendszere miatt, ami több nyelv használatát igényli, másrészt egy angol nyelvű változattal szélesítik a lapot látogatók körét. E gyakorlat követése – a 27 tagállam polgárainak szabad mozgását tekintve az EU területén – felettébb ajánlatos. Luxemburgban például a nemzeti AVH többnyelvű Internet-lapja meglehetősen terjedelmes és bőséges tájékoztatást nyújt az érintetteknek, az adatkezelőknek, az adatfeldolgozóknak és a jogalkotóknak egyaránt.<sup>131</sup> Finnország adatvédelmi hatóságának honlapja ugyancsak jelentős, többnyelvű információs csatorna.<sup>132</sup>

---

<sup>126</sup> G. Zwenne et al. (2007), Eerste fase evaluatie Wet bescherming persoonsgegevens: [http://www.wodc.nl/images/1382a\\_volledige\\_tekst\\_tcm44-61969](http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969) (24.02.2010). An Angol nyelvű összefoglaló a jelentés 207. oldalán olvasható.

<sup>127</sup> H.B. Winter et al. (2008), Wat niet weet wat niet deert, WODC 2008, <http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2efase.aspx#> (24.02.2010).

<sup>128</sup> <https://www.datenschutzzentrum.de/> (2010.10.26.)

<sup>129</sup> <http://www.datenparty.de/> (30.01.09).

<sup>130</sup> [https://212.170.242.196/portalweb/canalresponsable/inscripcion\\_ficheros/Notificaciones\\_tele/que\\_es/index-ides-idx.php.php](https://212.170.242.196/portalweb/canalresponsable/inscripcion_ficheros/Notificaciones_tele/que_es/index-ides-idx.php.php) (24.02.2010).

<sup>131</sup> <http://www.cnpd.lu/fr/> (24.02.2010).

<sup>132</sup> [www.tietosuoja.fi](http://www.tietosuoja.fi) (24.02.2010).

Egyes nemzeti AVH-k által kidolgozott oktatási politika sokoldalú innovatív elemet tartalmaz. Az oktatás minden, az elemi iskolától az egyetemig terjedő szintjének kínált programok az adatvédelem tudatosságának fokozására ösztönöznek. Másrészt a társadalom különböző korosztályai sajátos igényeihez illeszkedő programok hasznos visszacsatolással szolgálhatnak a társadalom különböző szintjei jellemzői és szükségletei tekintetében. A tömegközlelési eszközök ugyancsak széles lehetőséget nyújtanak TV-programok további készítésére, interaktív Internet-lapok szerkesztésre és egyéb kezdeményezések megvalósítására. A Cseh Köztársaságban például az AVH folyamatban lévő projektuma „Személyes adatok védelme az oktatásban” című programjával a gyerekeket és az ifjúságot vette célba. A nemzeti hatóság 2006-ban továbbá részt vett egy adatvédelmi tárgyú TV-sorozat elkészítésében, melynek címe: „A tudatlanság nem mentség – Titkai mindannyiunknak vannak” (a 2006. évi jelentés szerint minden epizódnak közel 160 000 – 310 100 nézője volt).<sup>133</sup> Ugyancsak helyes, az oktatásban követett gyakorlat, amikor az adatvédelmi hatóság szakértői részt vesznek az érdekcsoportoknak szervezett előadásokon és szemináriumokon. Ez a helyzet Finnországban, ahol az AVH az adatkezelőknek szóló magazint tesz közzé, évente négyszer, s ezen felül telefonon tanácsadással is szolgál. Portugáliában és Belgiumban az AVH-k joghallgatókat és végzett jogászokat fogadnak szakmai gyakorlatra, hogy tevékenységük tekintetében jártasságra tegyenek szert. Olaszországban sajátos kommunikációs kezdeményezéseket indítottak különös tekintettel az ifjúságra /ezek egyike esetében az AVH az Oktatási Minisztériummal (Ministero dell’Istruzione) együttműködve útmutatást dolgozott ki a mobiltelefonok megfelelő használatára és a megfigyelő kamerák iskolai alkalmazására). Különböző adatkezelő rendszerek létesítését segítő útmutatások és tanácsok nyújtása fontos és egyre növekvő feladat. A spanyolországi AVH igen aktív az adatvédelmet érintő több területen. Útmutatással szolgálnak a gyermekjogok és a szülők feladatai,<sup>134</sup> az adatbiztonsági intézkedések,<sup>135</sup> az adatkezelések,<sup>136</sup> az adatvédelem mint alapvető jog,<sup>137</sup> a városi tanácsoknál,<sup>138</sup> az állami iskolákban és egyetemeken, a szakmai egyesületeknél, a közegészségügyi és az állami szociális szolgálatoknál kezelt személyes adatok tekintetében. Ugyanez érvényes Észtországra<sup>139</sup> és Olaszországra nézve is. Franciaországban és az Egyesült Királyságban<sup>140</sup> az adatvédelmi hatóságok a foglalkoztatás területén kezelt adatok védelmére vonatkozó útmutatót adtak ki.

A tudatosság fokozását célzó helyes gyakorlatok közül ki kell emelni a nemzeti AVH-k tájékoztató és tanácsadó kampányait a ’spam’ vagy kéretlen e-mail-ekkel szemben. Franciaországban például az adatvédelmi hatóság célja az volt, hogy összegyűjtse és

---

<sup>133</sup> <sup>133</sup> Lásd Výroční zpráva za rok 2006 (Éves Jelentés, 2006) 2. oldal, [http://www.uouu.cz/vz\\_2006.pdf](http://www.uouu.cz/vz_2006.pdf) (02.01.2009).

<sup>134</sup> [https://www.agpd.es/portalweb/canal\\_joven/common/pdfs/recomendaciones\\_menores\\_2008.pdf](https://www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf) (09.01.2009)

<sup>135</sup> [https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia\\_seguridad\\_datos\\_2008.pdf](https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf) (09.01.2009).

<sup>136</sup> [https://212.170.242.196/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia\\_responsable\\_ficheros.pdf](https://212.170.242.196/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf) (09.01.2009).

<sup>137</sup> [https://212.170.242.196/portalweb/canal\\_joven/common/pdfs/FOLLETO.pdf](https://212.170.242.196/portalweb/canal_joven/common/pdfs/FOLLETO.pdf) (09.01.2009)

<sup>138</sup>

[http://www.madrid.org/cs/Satellite?c=CM\\_Publicacion\\_FA&cid=1114180060765&idPage=1109266885968&language=es&pagenome=APDCM%2FCM\\_Publicacion\\_FA%2Ffi\\_chaPublicacionAPDCM](http://www.madrid.org/cs/Satellite?c=CM_Publicacion_FA&cid=1114180060765&idPage=1109266885968&language=es&pagenome=APDCM%2FCM_Publicacion_FA%2Ffi_chaPublicacionAPDCM) (24.02.2010).

<sup>139</sup> <http://www.aki.ee/est/?part=html&id=56> (23.01.2009).

<sup>140</sup> A legfontosabb útmutatók a kis- és közepes vállalkozások részére, a munkáltató-munkavállaló viszony terén mind a magán-, mind a közjogi szektorban, továbbá a bankok ügyfélkapcsolatai, a helyi hatóságok dokumentumainak közzététele és terjesztése, a kábítószer-fogyasztás klinikai vizsgálata és a hűségkártyák tekintetében készültek.



feldolgozza az Internet-használók panaszait, és továbbítja őket a „spam” ellenes kampányban résztvevő szereplőkhöz, többek között a közintézményeknek és politikai szervezeteknek és szakembereknek különböző küldetésüknek és adottságuknak megfelelően.<sup>141</sup> A spanyol felügyelő hatóság közvetlenül részt vett tájékoztató útmutatók<sup>142</sup> és egy, a spam elleni harcra vonatkozó javaslatokat tartalmazó Tízparancsolat<sup>143</sup> megfogalmazásában.

További helyes gyakorlat az AVH-k által alapított díjak odaítélése. Szlovéniában – az Európai Adatvédelmi Nap alkalmából – a nemzeti felügyelő szerv évről évre kiválasztja azt a magánvállalkozást vagy közjogi szervet, amelynek a személyes adatok védelme terén folytatott tevékenységét a legsikeresebbnek véli, s kitünteti a „helyes gyakorlat” díjjal. Ezt e téren követendő példának tartjuk.<sup>144</sup> Franciaországban a nemzeti felügyelő szerv az adatfeldolgozásért, adatállományokért és az egyéni szabadságokért elnevezésű doktori díjat alapított, mellyel 7 000 euro is jár. Hasonló célt követve 2008-ban elfogadtak egy Nobel díj alapítására vonatkozó javaslatot az adatvédelem és a szabadságok területén, melyet 2010-től kezdve ítélnek oda.<sup>145</sup> Spanyolországban továbbá díjat alapítottak, melyet annak az európai közintézménynek ítélnek oda, amely a helyes gyakorlatok legjobbját alkalmazza.

## 7. Következtetések

Számos megoldás kínálkozik mind EU-s, mind hazai szinten a jelenlegi adatvédelmi rendszerrel szemben jelentkező legnyomasztóbb kihívásokra. Míg szükség van nemzeti intézkedésekre, az EU szerte koordinált és összehangolt megközelítés sikeresebben erősítheti a személyes adatok védelmét.

Az EU intézmények szerepe e téren különösen fontos, s az Európai Parlament is élénk érdeklődést tanúsít az adatvédelem iránt.<sup>146</sup> Az Európai Parlamenthez fordulunk, hogy az EU Tanácsával és az Európai Bizottsággal közösen olyan jogszabályi reformot hajtsanak végre, amely garantálja az adatvédelmi rendszer hatékonyságát. E tekintetben reményt keltő, hogy a jogérvényesülés, alapvető jogok és uniós polgárság biztosa hangsúlyozta az adatvédelem fontosságát és az EU adatvédelmi normáinak korszerű és átfogó jogeszközzé való átalakítását.<sup>147</sup> Az Európai Bíróság ugyancsak cselekvő hozzáállást tanúsít az adatvédelem tekintetében. Így ez idáig a belső piaci harmonizáció egyik jogszabályát (az adatvédelmi irányelvet) oly módon értelmezte, amely elősegíti az alapvető jogok védelmét a Közösségen belül. E tekintetben az adatvédelmi irányelvnek olyan kiterjesztő olvasatát nyújtotta, ami túlnő a gazdasági tevékenységeken és a védelem alóli kivételek korlátozott értelmezésén.

A hatályos adatvédelmi jogszabályok fejlesztését szolgálja a nemzeti adatvédelmi hatóságok és a 29-es Munkacsoport együttműködése is. A Munkacsoport véleményeinek és ajánlásainak

---

<sup>141</sup> Lásd: a 2007.10.30-án aláírt társulási megállapodás a francia AVH és a Signal Spam között.

<sup>142</sup> [https://www.agpd.es/portalweb/canaldocumentacion/lucha\\_contra\\_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf](https://www.agpd.es/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf) (09.01.2009).

<sup>143</sup> [https://212.170.242.196/portalweb/canaldocumentacion/lucha\\_contra\\_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam\\_guia.pdf](https://212.170.242.196/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam_guia.pdf) (09.01.2009).

<sup>144</sup> <http://www.lek.si/slo/mediji/sporocila-za-javnost/3849/> and <http://www.ip-rs.si/novice/detajl/nagrajenca-ob-2-evropskem-dnevu-varstva-osebni-podatkov-stazavod-za-zdravstveno-zavarovanje-slove/> (30.12.2008).

<sup>145</sup> IPA Declaration «International Privacy Association» on the creation of a Nobel Prize in the field of Data protection and liberties, to be awarded annually by the global conference of authorities on the protection of data. [http://www.privacyconference2008.org/index.php?language=2&page\\_id=1](http://www.privacyconference2008.org/index.php?language=2&page_id=1) (12.12.2008).

<sup>146</sup> Note for example the Proposal of the European Parliament Committee on Civil Liberties, Justice and Home Affairs for a European Parliament recommendation to the Council on strengthening security and fundamental freedoms on the internet (2008/2160(INI)).

<sup>147</sup> Lásd Notice to Members of the European Parliament, 7.1.2010, doc. PE431.139v02-00, [http://www.europarl.europa.eu/hearings/static/commissioners/answers/redirecting\\_replies\\_en.pdf](http://www.europarl.europa.eu/hearings/static/commissioners/answers/redirecting_replies_en.pdf) (23.02.2010).

figyelembe vétele az AVH-k által hozzájárul egy közös, a személyes adatok védelmét magas szinten biztosító EU normarendszer létrejöttéhez. Az európai adatvédelmi biztosnak is az a feladata, hogy segítse a természetes személyek alapvető jogainak és szabadságainak, különösen magánéletükhöz fűződő jogaiknak a tiszteletben tartását a Közösség intézményeinél és szerveinél. Az európai adatvédelmi biztos alkotmányos feladata különös jelentőségre tesz szert, amikor egy új jogszabály megalkotása során hatékonyan hozzájárul az Unió polgárai alapvető szabadságai védelméhez.

Fejleszteni kell továbbá az AVH-k függetlenségét, hatékonyságát, erőforrásait és jogosultságait, hiszen mint az adatvédelem őrzői, kulcsszerepet játszanak a nagyközönség szemében. Az adatvédelmi rendszer teljes egészében e hatóságok iránt táplált széleskörű bizalom függvénye. Nehéz lesz meggyőzni a polgárokat arról, hogy adatvédelemmel és magánéletükkel kapcsolatos aggodalmaikat komolyan veszik, ha kétségeik vannak az adatvédelmi hatóságok függetlenségét illetően, vagy ha nem látják, hogy e hatóságok rendelkeznek mindazokkal az erőforrásokkal, amelyek feladataik tényleges és hatékony végrehajtásához szükségesek.

Az adatvédelmi hatóságok az EU alapjogi szerkezetének azért is kulcsfontosságú részét képezik, mert az EU úttörő szerepet játszik az adatvédelem mint alapvető jog tekintetében, s mert az EU-nak jelentős szerepe volt és van számos tagállam adatvédelmi rendszere fejlesztésében. Az adatvédelem továbbá az EU fő politikai területének egyike, ahol az alapvető jogokat illetően jogalkotói hatáskörrel rendelkezik. Következésképpen az adatvédelmi rendszer általános hatékonysága kedvező hatást gyakorolhat a nagyközönségnek az EU-ról mint az alapvető jogok őrzőjéről alkotott felfogására.

\*\*\*\*\*

---

A fordító megjegyzései

<sup>I</sup> Az Európai Unióról szóló szerződés, az Európai Unió működéséről szóló szerződés és az Európai Unió Alapjogi Chartája letölthető: <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:HU:HTML>

<sup>II</sup> 1976. évi 8. törvényerejű rendelet az Egyesült Nemzetek Közgyűlése XXI. ülészakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről

<sup>III</sup> Lásd: [http://www.unhcr.ch/tbs/doc.nsf/\(Symbol\)/23378a8724595410c12563ed004aeecd?Opendocument](http://www.unhcr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument)

<sup>IV</sup> Lásd <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html>

<sup>V</sup> A Nemzetközi Emberi Jogi Kódex (International Bill of Human Rights) az Egyesült Nemzetek Közgyűlése egy határozatát és két nemzetközi szerződését felölelő informális elnevezése. Tartalma: Az Emberi Jogok Egyetemes Nyilatkozata (1948), a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (1966) két Opcionális Jegyzőkönyvével egyetemben, valamint a Gazdasági, Szociális és Kulturális Jogok Nemzetközi Egyezségokmánya (1966).

<sup>VI</sup> Hivatalos magyar fordításuk nincs

<sup>VII</sup> Letölthető (angol - magyar):

<http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&lng1=en,hu&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=258038:cs&page=1&hwords=>

<sup>VIII</sup> Az EK Sz (korábbi) 12. cikke megfelel az EU működéséről szóló szerződés 18. cikkének felel meg.

<sup>IX</sup> Valószínűleg hibás, mert a lábjegyzet a szövegtől eltérően SK-ra (Slovakia-ra), s nem SL-re (Slovenia-ra) hivatkozik.

<sup>X</sup> A lábjegyzet hivatkozik a nemzeti tematikus tanulmányokra, megadva lelőhelyüket is (<http://fra.europa.eu>), ahol sajnos nem találtam egyetlen országjelentést sem.

<sup>XI</sup> 1990. évi XCIII. törvény az illetékekről, 57. § (1) Illetékmentes a polgári ügyekben: o) a személyes adatok védelmével, illetve a közérdekű adatok nyilvánosságával összefüggésben indított per;

<sup>XII</sup> Olvasható: <http://lexuniversal.com/en/news/5305>

<sup>XIII</sup> Az irányelvnek az EU hivatalos lapjában közzétett magyar szövege szerint (sajnos) "*megtılthatják*". Erről egyébként a 8. cikk (1) bekezdése rendelkezik.

<sup>XIV</sup> A lábjegyzetben megadott Internet címről letölthető dokumentum sajnos nem e-health, hanem: Avis n° 33/2008 du 24 septembre 2008 Objet : Projet d'arrêté royal fixant les modalités de traitement des données à caractère personnel et des informations de la police intégrée, structurée à deux niveaux dans le cadre de la banque de données nationale générale (A/2008/033)