EURÓPAI FÜZETEK 35.

SZAKMAI ÖSSZEFOGLALÓ A MAGYAR CSATLAKOZÁSI

TÁRGYALÁSOK LEZÁRT FEJEZETEIBŐL

Dr. Oros Paulina — Dr. Szurday Kinga

Adatvédelem az Európai Unióban

Szolgáltatások szabad áramlása

A Miniszterelnöki Hivatal Kormányzati
Stratégiai Elemző Központ és a
Külügyminisztérium közös kiadványa

Európai Füzetek
A Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ
és a Külügyminisztérium közös kiadványa.

Felelős kiadó: Szeredi Péter

A szerkesztőség címe: MEH Európai Integrációs Iroda, 1055 Budapest, Kossuth tér 4.
Telefon: 441-3380
Fax: 441-3394

Lektor: Kerecsen Zsófia
Kézirat lezárva: 2003. május 5.

Grafikai terv: Szutor Zsolt
Fényképek: Csorba Gábor
Portréfotó: Csorba Gábor
Nyomás és előkészítés: Visit Nyomda & Stúdió

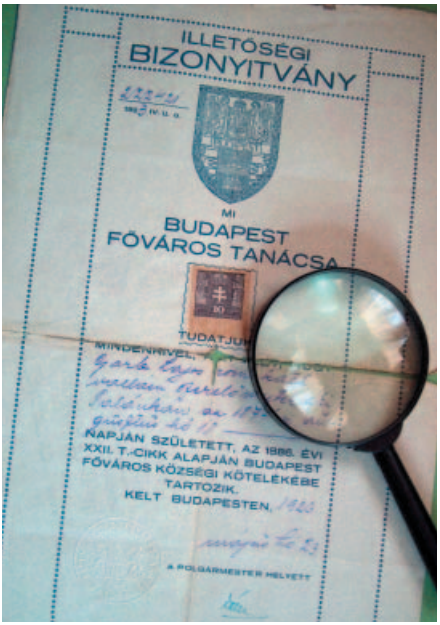
ISSN: 1589-4509
Budapest, 2003.

Kedves Olvasó!

Magyarországon a nyolcvanas években vezették be a személyi számot, ami – a számítógépek elterjedésével párhuzamosan – az adatkezelés megkönnyítését szolgálta az államigazgatás számára. Eltelt néhány év, és mire mindenki megtanulta a saját számát, eltörölték annak általános használatát.

A legtöbben azóta sem értik, miért kellett a jól működő, gyors felismerést lehetővé tevő és mindenütt használható rendszert éppen abban a pillanatban megszüntetni, amikor szinte az egész társadalom által elfogadottá vált. Pedig éppen ezzel volt baj: túl jól működött, túl gyors volt és mindenütt használható, így bármilyen számítógépes adatbázisból szinte azonnal visszakereshető volt a személyi számmal jelölt emberről összegyűjtött összes információ. Azaz nemcsak annyi, amennyire az adott esetben az ügyféllel kapcsolatban álló hivatalnak vagy szervezetnek szüksége lehetett.

Az állam megvédi saját magától az állampolgárokat: ez az európai történelemben is új dolog. Csak a XX. század hatvanas éveiben alkották meg az első adatvédelmi törvényeket a kontinensen, ahol fontosabbnak tartják a magánélet védelmét, mint az Egyesült Államokban, ahol az információáramlás szabadságának van elsőbbsége.



Nem kétséges, hogy mi, magyarok melyik oldalon állunk, amíg visszhangoznak bennünk József Attila sorai:

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

I. Az adatvédelem nemzetközi szabályozásának története

1. Az adatvédelem előzménye: információszabályozás

Az információáramlás jogi szabályozását a korszerű számítástechnika, az automatikus adatfeldolgozás fejlődése és gyors elterjedése tette szükségessé. Az információszabályozás az államigazgatás, a politika, a jog számos területét érinti; összefügg a tömegtájékoztatás, a sajtószabadság, az emberi jogok kérdésével. Célja egyrészt a technikai és kutatás-fejlesztési stratégiák összehangolása, másrészt a társadalmi, a jogi és a politikai hatások kezelése. Az információs társadalom kialakulása során – az adatok óriási tömegének rendkívül gyors és személyre szabott kezelésének lehetőségével – a társadalom tagjai könnyen „átvilágíthatóvá" váltak, ezáltal veszélybe került magánéletük védelme. Egyúttal az információs hatalom a kormányszervek és a vezető üzleti-politikai körök kezében koncentrálódott, ez pedig ellentétben áll a demokrácia azon alapelvével, hogy a társadalom szerkezete minden tagja számára átlátható legyen.

Jogállami keretek között a társadalom egészséges és demokratikus működéséhez hozzátartozik a szabad információáramlás, ugyanakkor a *magánszférát védeni kell*, szabályozni a személyhez fűződő információk nyilvánosságra hozatalát, illetve lehetővé tenni szabad áramlásukat. Az országok – hagyományaiktól függően – máshol húzzák meg a jogi szabályozás határvonalait e két érdek között. Vannak olyanok – elsősorban az Egyesült Államok –, amelyek szerint az információk szabad áramlásának van elsőbbsége: az információhoz való jog mindenekfelett áll. Mások – elsősorban az európai országok – a következetes adatvédelem mellett kötelezik el magukat: a magánszféra sérthetetlenségére helyezik a súlyt. Ezzel összefüggésben kell említést tenni a *„privacy"* (a magánélet védelme) fogalmáról, amely a személyes adatok védelménél tágabb, kiterjed a magánélet más területére is. A nemzetközi adatvédelmi gyakorlatban mindamellett a privacy-t a személyes adatok védelmével szinonim fogalomként használják.

A modern információszabályozás első lépésének *Svédország 1766-ban, a sajtószabadságról alkotott törvénye* tekinthető: ez lehetővé tette, hogy az állampolgárok betekinthessenek a hivatalos iratokba. Az adatvédelem korszerű felfogásával kapcsolatban majdnem kétszáz évvel később – a számí-

tástechnika megjelenése nyomán –, a hatvanas évek elején folytattak több országban elszigetelt *jogvitát az információszabályozás szükségességéről*. Az első európai adatvédelmi szabálygyűjtemény a Nagy-Britanniában 1966-ban kiadott *Code of Conduct.* A kontinentális jogban az első adatvédelmi törvényt a németországi Hessen tartományban fogadták el 1967-ben. Ugyanakkor az Egyesült Államokban az információ szabadságára helyezték a súlyt: 1967-ben született meg *Freedom of information* törvény első változata. Az európai adatvédelmi szabályozás kezdeteinek legjelentősebb dokumentuma az 1973. évi, svéd adattörvény. Ezt követően folyamatosan bocsátották ki az úgynevezett *első generációs adatvédelmi törvényeket:* 1977-ben Németország, 1978-ban Ausztria és Dánia alkotja meg adatvédelmi törvényét, valamint Franciaország „az informatikára, a nyilvántartásra és a szabadságjogokra vonatkozó" törvényt. E sort 1979-ben Norvégia, majd 1981-ben Izland zárta.

A *multilaterális nemzetközi egyezmények* sorában sem az ENSZ Emberi Jogok Egyetemes Nyilatkozata, sem az Emberi Jogok Európai Egyezménye nem tartalmaz közvetlen utalást a személyes adatok védelmére, de mindkét dokumentum deklarálja a magánélet védelméhez való jogot. Az első átfogó adatvédelmi jogi dokumentum a *Gazdasági Együttműködési és Fejlesztési Szervezet* (OECD) Tanácsának 1980. szeptember 30-i *ajánlása* a magánélet védelméről és a személyes adatok határátlépő áramlásáról.

2. Az Európa Tanács Adatvédelmi Egyezménye

Az Európa Tanács Parlamenti Bizottsága a hatvanas évek végén kezdte vizsgálni, hogy az Európai Emberi Jogi Bíróság, illetve a tagállamok megfelelően szavatolják-e a magánélet védelmét az információáramlás területén. Arra a következtetésre jutottak, hogy az Európai Emberi Jogi Egyezmény *nem szolgálja kellően* a személyes adatok védelmét. Ezért ajánlást dolgoztak ki, amely meghatározta, hogy az elektronikus adatbázisok működtetése során hogyan kell védeni a magánéletet. Ennek szabályai kiterjedtek a magán- és a közszektorra egyaránt.

A hetvenes években az egyes országok külön-külön megalkották saját adatvédelmi törvényüket, és ezek mintegy kikényszerítették az Európai Adatvédelmi Egyezmény elkészítését. A nemzeti adatvédelmi törvények korlátok közé szorították az adatok továbbítását, ezzel egyrészről lehetővé tették a személyes adatok védelmét, másrészről viszont veszélyeztették a nemzetközi együttműködést és kommunikációt. Ráadásul a nemzeti jogszabályok azonos alapelvekből indultak

ugyan ki, de eltérő megoldásokat és eljárásokat alkalmaztak, ami a nemzetközi adatcsere területén konfliktusokat okozott. Azt is meg kellett oldani, hogy az Európai Emberi Jogi Egyezmény 8. cikkében foglaltakat – azaz a magánélet védelméhez való jogot – kiterjesszék a személyes adatok kezelésére.

Az Adatvédelmi Egyezmény tervezetének kidolgozása 1976-ban kezdődött, ötévi munka után készült el, s 1981. január 28-án nyílt meg aláírásra. (Magyarország – elsőként a volt szocialista országok közül – 1993. május 13-án írta alá, és 1997. október 8-án ratifikálta az egyezményt, amely hazánkban 1998. február 1-jén lépett hatályba.)

Az egyezmény elfogadása után az Európa Tanács a különféle ágazatokra vonatkozóan *ajánlásokat* bocsátott ki, amelyekkel jelentősen befolyásolta az európai nemzeti adatvédelmi szabályozást. Az országok számos, úgynevezett *szektorális adatvédelmi jogszabályt* alkottak.

Az adatvédelem területén az Európa Tanács egyre szorosabb együttműködést alakított ki az Európai Közösséggel. Az Adatvédelmi Egyezmény szolgált alapul az Európai Közösség 1995-ben kidolgozott adatvédelmi irányelvéhez, és az egyezmény rendelkezéseit mögöttes szabályként kell alkalmazni az irányelv mellett. Ráadásul az irányelv több kérdésben – például a független adatvédelmi hatóság jogköre – előbbre mutatott, és visszahatott az egyezményre. (Az irányelv nagy súlyt helyezett a független és megfelelően hatékony jogorvoslati eszközökkel felruházott adatvédelmi ellenőrző szerv létrehozására.)

A nemzetközi adatáramlás szabályozásában problémát okozott, hogy az Adatvédelmi Egyezmény nem rendezte a *harmadik országok joghatósága alá tartozó adatátvevők* részére történő adattovábbítás lehetőségét. Ennek következtében a tagállamok eltérő gyakorlatot alakítottak ki, amely esetenként – az egyezmény szellemével ellentétesen – túl szigorúan akadályozta az információk szabad áramlását. E problémák rendezése – nem utolsósorban a különféle európai intézmények adatvédelmi követelményeinek harmonizálása – érdekében fogadta el az Európa Tanács Miniszteri Bizottsága 2001. november 8-án az Adatvédelmi Egyezmény *kiegészítő jegyzőkönyvét* a felügyelő hatóságokról és az országhatárokat átlépő adatáramlásról.

II. Az Európai Unió adatvédelmi szabályozása

Az Európai Unió alapító szerződése 6. cikkének (2) bekezdése kimondja, hogy „az Európai Unió tiszteletben tartja az alapvető jogokat mint a közösségi jog általános alapelveit, ahogyan azokat az Európai Emberi Jogi Egyezmény garantálja, és ahogyan azok a tagállamok közös alkotmányos hagyományaiból következnek". Ebből következően tehát az EU *alapelvként ismeri el* az Európai Emberi Jogi Egyezmény 8. cikkéből fakadóan a *magánélet védelméhez való jogot*, illetve a tagállamok alkotmányain alapulóan a *személyes adatok védelméhez való jogot*. Ki kell emelni, hogy továbbra is a legfontosabb európai adatvédelmi dokumentum az Európa Tanács Adatvédelmi Egyezménye, amelyet az unió magára nézve kötelezőnek fogad el, és az Acquis Communautaire (közösségi jogi vívmányok) részeként ismer el.

A jövőre nézve az *Európai Unió Alapjogi Kartájának* 8. cikke – ezt az elvet továbbfejlesztve – már tételesen kimondja, hogy „mindenkinek joga van személyes adatai védelméhez". Deklarálja a célhoz kötöttség, a személyes adatokkal való önrendelkezés, az adatokhoz való hozzáférés és a helyesbítés jogát, valamint leszögezi, hogy független adatvédelmi ellenőrző szerv működtetésére van szükség.

Ugyanakkor azonban az unió alapvető célja a személyek, az áruk, a szolgáltatások és a tőke szabad áramlásán alapuló egységes belső piac létrehozása és működése. Ennek elérése érdekében elengedhetetlen a személyes

adatok szabad áramlásának lehetővé tétele, valamint az egyéni jogok és szabadságok azonos védelmének megteremtése.

Az Európai Unió alapító szerződése kimondja: az EU célja, hogy a büntetőügyekben a tagállamok rendőrségi és igazságügyi együttműködésük során közösen lépjenek fel a szabadság, a biztonság és az igazságosság érdekében, ami az állampolgároknak magas szintű biztonságot nyújt. Ezt szolgálja a tagállamok rendőri szervei közötti közvetlen,

illetve az *Europol* (European Police Office – Európai Rendőri Hivatal) révén megvalósuló együttműködés. E célok elérése érdekében is szükség van arra, hogy a személyes adatok szabadon áramolhassanak a tagállamok között, egyidejűleg viszont garantálni kell a védelmükhöz fűződő alapvető jog érvényesülését.

Mindezekből kiindulva az Európai Unió adatvédelmi szabályozása négy részre osztható:

- A közösségi jog területére kiterjedő hatályú általános adatvédelmi irányelv[1].
- A közösségi intézményekre irányadó adatvédelmi követelmények[2].
- A személyes adatok védelme az elektronikus kommunikációs szektorban[3] .
- Adatvédelem a büntetőügyekben való rendőrségi és igazságügyi együttműködés területén. (E speciális területtel nem foglalkozunk, mivel erre nem terjed ki az adatvédelmi irányelv hatálya.)

1 Az Európai Parlament és a Tanács 95/46 EK irányelve az egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról, Official Journal of the European Communities L 281, Volume 38, 23 November 1995. page 31.

2 Európai Közösség Alapító Szerződése 286. cikk, Regulation (EC) 45/2001 of the European Parliament and of the Council of 18. December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

3 Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunication sector replaid with effect from 31. October 2003. by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

III. Az általános adatvédelmi irányelv

1. Az irányelv előkészítése, elfogadása és nemzeti átültetése

Az Európai Parlament és a Tanács *95/46 EK irányelve* - az egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról (továbbiakban: irányelv) - tervezetét a Bizottság 1990. szeptember 13-án készítette el. A javaslat *célja* az volt, hogy az irányelv *harmonizálja* a tagállamok adatvédelmi rendelkezéseit annak érdekében, hogy azok különbözősége ne akadályozhassa az adatok áramlását a Közösségen belül. *Hatálya* kiterjedt a tagállamok területén lévő adatállományokra mind a *köz-, mind a magánszektorban.* A javaslat megfogalmazta az adatkezelés alapvető elveit. Az irányelv elfogadott szövegét 1995. október 24-én hirdették ki. Ettől számítva *három év* állt a tagállamok rendelkezésére, hogy az irányelvben foglaltakkal összehangolják belső jogukat, és megalkossák nemzeti szabályozásukat.


Kivonat

református egyház születtek és megker

anyakönyvéből az ezer

hó 20 -ik napjáról.

kötet 226 lap folyószám.

A született

A szülők

neve

1826

2. Az irányelv lényeges elemei

Az irányelv preambuluma kifejti, hogy az adatfeldolgozó rendszerek az emberiséget szolgálják azzal, hogy e rendszereknek – függetlenül a természetes személyek állampolgárságától és lakóhelyétől – tiszteletben kell tartaniuk az egyének alapvető jogait és szabadságait, nevezetesen a magánélet védelméhez fűződő jogot, és elő kell segíteniük a gazdasági és társadalmi haladást, a kereskedelem bővülését és az egyéni jólétet. Utal arra, hogy a belső piac megteremtéséhez és működéséhez az alapító szerződés 14. cikkének (2) bekezdése szavatolja az áruk, a személyek, a szolgáltatások és a tőke

szabad mozgását, amihez nemcsak a személyes adatok szabad áramlására van szükség, hanem – ezzel összefüggésben – az egyének alapvető jogainak érvényesítésére is.

Az irányelv alapvető célja tehát megfelelő *egyensúly teremtése* e két alapjog – vagyis

az egyén magánéletének védelme, illetve a személyek és szolgáltatások szabad áramlása – között. Ennek megfelelően 1. cikkének (1) bekezdése kimondja, hogy „a tagállamok ezzel az irányelvvel összhangban gondoskodnak a természetes személyek alapvető jogainak és szabadságainak a személyes adatok feldolgozásával kapcsolatos védelméről", ugyanakkor a (2) bekezdés deklarálja, hogy „a tagállamok az előzőekben biztosított védelemmel kapcsolatos okokra hivatkozva nem korlátozzák, és nem tiltják a személyes adatok szabad áramlását a tagállamok között".

3. Az irányelv hatálya

Az irányelv *tárgyi hatálya* nem terjed ki az olyan tevékenységekre, amelyek a közösségi jog hatályán kívül esnek, vagyis, amelyekről az Európai Unióról szóló szerződés V. és VI. címe rendelkezik (közös kül- és biztonságpolitika, valamint rendőri és igazságügyi együttműködés büntetőügyekben). A 3. cikk 2. pontja külön kiemeli, hogy az irányelv nem alkalmazható a közbiztonságot, a honvédelmet, az állambiztonságot és az állam büntetőjogi tevékenységét érintő adatkezelésre[4].

Az irányelv rendelkezéseit kell alkalmazni a személyes adatok teljesen vagy részben *automatizált* módon történő feldolgozására, továbbá a *nem automatizált* feldolgozásra, ha az érintett személyes adatok valamely *nyilvántartási rendszer részét képezik* vagy

4 Irányelv 3. cikk, 2. bekezdés, első fordulat
5 Irányelv 3. cikk, 1. bekezdés
6 Irányelv 3. cikk, 2. bekezdés, második fordulat
7 Irányelv 4. cikk
8 Irányelv 2. cikk
9 Irányelv 6. cikk
10 Irányelv 7. cikk

fogják képezni[5]. Nem terjed ki azonban a hatály a személyes adatok feldolgozására a természetes személy kizárólag személyes vagy háztartási tevékenysége során[6].

Az irányelv, illetve az ennek alapján kibocsátott nemzeti jogszabályok *területi hatálya* a következőképpen alakul: a tagállamoknak az irányelv rendelkezéseit kell alkalmazniuk, ha a *feldolgozást* az adatkezelőnek a *tagállam területén* – illetve azon kívül olyan területen, ahol a nemzetközi közjog alapján a belső jogát kell alkalmaznia – működő szervezete tevékenységi körében végzi. Továbbá akkor, ha az adatkezelő nem az unió területén működik, de adatfeldolgozásra a *tagország területén lévő eszközöket* használ, kivéve, ha ezek az eszközök a unió területén átmenő forgalom célját szolgálják[7]. Általános elvként mondja ki az irányelv, hogy az adatáramlás az unió területén belül nem korlátozható.

4. Az adatvédelemmel összefüggő fogalmak

Az irányelv egységesen értelmezi az adatvédelemmel összefüggő *fogalmakat*[8] – személyes adat, személyes adatok feldolgozása, személyes adat-nyilvántartó rendszer, adatkezelő, feldolgozó, harmadik fél, címzett, az adatalany hozzájárulása –, és meghatározza a személyes adatok minőségére vonatkozó alapelveket – tisztességesség, törvényesség, célhoz kötöttség, időszerűség[9] –, valamint az adatok kezelésének *feltételeit*. (Az adatkezelés alapjául szolgálhat az adatalany félreérthetetlen hozzájárulása, az adatkezelő és az adatalany által kötött vagy kötendő magánjogi szerződés, az adatkezelő törvényes kötelezettségének teljesítése, az adatalany létfontosságú érdekeinek védelme, közérdekű feladat teljesítése, az adatkezelő, illetve az adatátvevő harmadik személy hivatalos feladatának gyakorlása, vagy az adatkezelő, illetve a harmadik személy jogos érdekének érvényesítése, kivéve ha ez utóbbi érdeket az adatalanynak a személyes adatai védelméhez fűződő érdekei felülmúlják[10].)

Az irányelv alapesetként *megtiltja a különleges adatok kezelését* azzal, hogy e tilalom nem alkalmazható az irányelvben tételesen felsorolt esetekben. (Az adatkezeléshez az adatalany kifejezetten hozzájárul; vagy az a munkajogi kötelezettség teljesítéséhez; továbbá az adatalany vagy más személy létfontosságú érdekeinek védelméhez szükséges, és az adatalany a hozzájárulását cselekvőképtelensége folytán nem tudja megadni; továbbá az adatkezelést politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület, vagy nonprofit szervezet végzi saját tagjaira, vagy vele rendszeres kapcsolatban állókra nézve, és az adatokat az adatalany hozzájárulása nélkül nem továbbítják

harmadik személynek.) Külön szabályokat tartalmaz az irányelv a megelőző egészségügyi, orvosi diagnosztikai, egészségügyi ellátási, vagy ezek igazgatása céljából történő adatkezelésre, valamint a büntető ítéletek nyilvántartására vonatkozóan[11].

Az irányelv rögzíti az *adatalany jogát* a tájékoztatásra, az adataihoz való hozzáférésre, az adatok helyesbítésére, zárolására vagy törlésére[12]. Amennyiben az adatot nem az adatalanytól gyűjtik, a tájékoztatási kötelezettség alól *kivételként* jelöli meg az irányelv, ha – különösen statisztikai, történelmi vagy tudományos célú feldolgozások esetében – a tájékoztatás lehetetlen, aránytalan erőfeszítést igényel, illetve, ha a rögzítést vagy továbbítást jogszabály kifejezetten előírja. Ezekben az esetekben azonban a tagállamoknak alkalmas biztosítékokról kell gondoskodniuk[13].

Az irányelv *új jogintézményként* bevezeti az adatalany jogai érvényesítésének céljából az *adatkezelés vagy adattovábbítás elleni tiltakozás* (kifogásolás) lehetőségét. Ez elsősorban olyan esetekre vonatkozik, amikor az adatkezelés vagy az adattovábbítás az adatkezelő vagy az adatigénylő harmadik személy érdekét szolgálja, de a törvény nem teszi szükségessé az adatalany hozzájárulását[14]. Az irányelv elsősorban a *közvetlen piacszerzés céljából* történő adatkezelés esetén teszi lehetővé a kifogásolás jogának érvényesítését. Ez a gyakorlatban azt jelenti, hogy ha a közvetlen üzletszerző társaság az érintett személy, név- és lakcímadatát nyilvános adattárból (például telefonkönyvből) vagy a személyiadat- és lakcímnyilvántartástól jogszerűen megszerzi, és ajánlatával név szerint megkeresi a címzettet, akkor az érintett ez ellen a cégnél tiltakozhat, és kérheti adatainak a nyilvántartásából való törlését, aminek a megkeresett társaság köteles eleget tenni.

Különleges biztosítékot tartalmaz továbbá az úgynevezett *automatizált egyedi döntés alapján történő értékelés kizárására*[15]. Az automatizált egyedi döntés során az érintett személyről különféle adatokat gyűjtenek össze, általában úgy, hogy *kérdőíveket* töltetnek ki vele. A kérdések a személyre vonatkozó tényadatokon kívül – életkor, nem, magasság, súly, betegségek stb. –, különféle élethelyzetekkel kapcsolatos véleményét, benyomását is firtatják, valamint

11 Irányelv 8. cikk
12 Irányelv 11., 12. cikk
13 Irányelv 11. cikk, 2. bekezdés
14 Irányelv 14. cikk
15 Irányelv 15. cikk

szituációs gyakorlatokat tartalmaznak. A kitöltött kérdőíveket feldolgozzák, a válaszokat számítógépre viszik. A számítógép egy megtervezett program szerint kiértékeli a válaszokat, és létrehoz egy *személyiségprofilt*, amelyet azután mint az adott személyre jellemzőt különféle döntésekhez használnak fel. A személyiségprofil használata egyre elterjedtebb a munkavállalók alkalmazásánál, munkahelyi előmenetelnél, hitelkérelem elbírálásakor. Felhasználását azért kell korlátozni vagy garanciákhoz kötni, mert adott esetben *súlyosan sértheti a személyiségi jogokat,* illetve úgy befolyásolja a döntést, hogy az adott személyre jellemző, a számítógép által készített profiltól eltérő, szubjektív elemet figyelmen kívül hagyja.

Az irányelv a benne foglalt jogok és kötelezettségek korlátozását nemzetbiztonsági, honvédelmi, közbiztonsági okból, valamint

bűncselekmények vagy foglalkozások etikai vétségeinek megelőzése, vizsgálata, feltárása és üldözése céljából, továbbá a tagállamok vagy az Európai Unió jelentős pénzügyi vagy gazdasági érdekéből, illetve mindezek ellenőrzése céljából, valamint az adatalany vagy mások jogainak és szabadságainak védelme érdekében teszi lehetővé[16].

Az irányelv meghatározza az *adatbiztonsági követelményeket,* ezen belül mind az adatkezelő és adatfeldolgozó, mind a megbízásukból tevékenykedő személy felelősségét. Rögzíti továbbá, hogy az adatfeldolgozásra vonatkozó szerződést – különösen az adatfeldolgozásra és az adatbiztonságra vonatkozó rendelkezést – írásba kell foglalni[17].

Az irányelvben foglalt, a tagállamokhoz címzett egyik legfontosabb követelmény a *független adatvédelmi ellenőrző szerv* – vagy szervek – létrehozása, amelynek konkrét beavatkozási hatáskört kell kapnia az adatkezelésekre és adatfeldolgozásokra (elrendelheti például a jogszerűtlenül kezelt adatok zárolását, törlését vagy megsemmisítését). Kezdeményezheti továbbá az illetékes szerveknél megfelelő szankció foganatosítását[18]. Feladata még az adatkezelők által az adatkezeléseikről tett bejelentések[19] nyilvántartása, és a bennük foglaltak nyilvánosság-

16 Irányelv 13. cikk
17 Irányelv 16., 17. cikk
18 Irányelv 28. cikk
19 Irányelv 18., 19 cikk
20 Irányelv 20. cikk
21 Irányelv 18. cikk, 2. bekezdés, második fordulat
22 Irányelv 17. cikk, 1. bekezdés
23 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance)
2000/519/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary (notified under document number C(2000) 2305) (Text with EEA relevance)
2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance)
2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539) Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)
24 Irányelv 26. cikk, 1. és 2. pont
25 Irányelv 26. cikk, 4. bekezdés
26 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539)
27 2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 4540)

ra hozatala. Az irányelv lehetővé teszi, hogy az adatvédelmi ellenőrző szerv – az adatkezelő bejelentése alapján – előzetes ellenőrzést végezzen bizonyos, a tagállamok által meghatározott érzékeny adatkezelésekkel kapcsolatban[20]. A tagállamok lehetőséget kapnak arra, hogy mellőzzék a bejelentési kötelezettség előírását, ha az adatkezelő kellően független belső *adatvédelmi felelőst* bíz meg[21]. Az irányelv „bátorítja" belső adatvédelmi szabályzatok kiadását[22].

Az irányelv előírja, hogy harmadik országba – azaz nem uniós tagállamba – személyes adat csak akkor továbbítható, ha a kérdéses harmadik ország *megfelelő szintű védelmet* nyújt. Részletesen kifejti, hogy milyen szempontokat kell figyelembe venni a megfelelő védelem megítélése során. Ezen eljárás lefolytatása alapján a Bizottság *kétirányú felhatalmazással* rendelkezik. Egyrészt kimondhatja, hogy a harmadik ország nem nyújt megfelelő szintű védelmet, másrészt – ennek ellenkezőjeként – azt, hogy belső joga, illetve az általa vállalt nemzetközi kötelezettségek alapján megfelelő védelmet nyújt. Eddig a Bizottság három országról – Magyarországról, Svájcról és Kanadáról – mondta ki, hogy megfelelő védelmet nyújt (az úgynevezett *Safe Harbour* megállapodás megállapítja, hogy megfelelő a védelem az Egyesült Államok Kereskedelmi Kamaráján keresztül lebonyolított adatcseréknél is)[23].

Az irányelv tételesen felsorolja, hogy *milyen okok alapján* lehet adatokat átadni a megfelelő szintű védelmet nem nyújtó országok részére: akkor, ha az adatátvevő igazolja, hogy az egyének védelmére megfelelő biztosítékot szolgáltat, elsősorban ezt tartalmazó szerződések formájában[24]. Felhatalmazást kapott továbbá a Bizottság[25], hogy szabványszerződés-mintákat bocsásson ki, amelyeknek használata a tagállamokra nézve kötelező. A Bizottság két ilyen tartalmú határozatot hozott, egyet a harmadik országokba történő személyes adattovábbításra[26], egy másikat a harmadik országokban alapított adatfeldolgozók részére történő adatátadásokra[27].

Az irányelv előírja még, hogy legyen lehetőség *bírósági jogorvoslatra*, valamint *kárté-*

rítésre, illetve azt, hogy az irányelv alapján hozott nemzeti szabályok megsértése esetén megfelelő *szankciókat* kell alkalmazni[28].

Az irányelv két testület létrehozásáról is rendelkezik. Egyrészt a 29. cikk szerint *munkacsoport* alakult, amelynek a tagállamok ellenőrző szervei és a Közösség intézményei által létrehozott hasonló szervek képviselői, valamint a Bizottság egy képviselője a tagja. A munkacsoport *tanácsadó tevékenységet* végez, javaslatokat, illetve ajánlásokat tesz, valamint évente jelentést készít az adatvédelem helyzetéről[29]. A másik szerv a Bizottság mellett működő, a tagállamok képviselőiből és a Bizottság képviselőjéből álló *testület*, amelynek feladata a Bizottság által előkészített *tervezetek véleményezése*[30].

Az irányelv viszonylag kevés lehetőséget ad a tagállamoknak e rendelkezésektől való *eltérésre*, illetve bizonyos területek önálló szabályozásra. Ezek közül kiemelendők a következők:

- A tagállamoknak saját hatáskörben kell szabályozniuk azokra a személyes adatokra vonatkozó adatkezeléseket, amelyek kizárólag *újságírói célokat* vagy *művészeti és irodalmi kifejezés* célját szolgálják, s a magánélet védelméhez fűződő jog és a véleménynyilvánítás szabadsága egyensúlyának megteremtéséhez szükségesek[31].
- Nem tartalmaz egységes rendelkezéseket az irányelv a *nemzeti azonosító* – személyi szám – alkalmazhatóságáról, hanem a tagállamokra bízza, hogyan szabályozzák ezt a kérdést[32].
- A tagállamok az irányelvben foglaltakon túlmenően *jelentős közérdekből* – megfelelő biztosítékokról történő rendelkezés mellett – lehetővé tehetik a különleges adatok kezelését[33].
- A meghatározott célból gyűjtött személyes adatok *történelmi, statisztikai vagy tudományos célokra* történő további felhasználását az irányelv nem tekinti összeegyeztethetetlennek az eredeti céllal, illetve lehetővé teszi e célból az adatok hosszabb ideig történő megőrzését, ha a tagállamok megfelelő biztosítékról gondoskodnak[34].

5. Az Adatvédelmi Munkabizottság tevékenysége

Az Adatvédelmi Munkabizottság jelentős befolyással rendelkezik az Európai Közös-

28 Irányelv 22., 23. 24. cikk
29 Irányelv 29., 30. cikk
30 Irányelv 31. cikk
31 Irányelv 9. cikk
32 Irányelv 8. cikk, 7. pont
33 Irányelv 8. cikk, 4. pont
34 Irányelv 6. cikk 1. bekezdésének b) és e) pontja
35 Case C-369/98, 2000. szeptember 14.

ség adatvédelmi jogának továbbfejlesztésére, értelmezésére és az egységes joggyakorlat kialakítására. A megalakulása óta eltelt hat év alatt összesen 66 ajánlást, javaslatot és munkadokumentumot bocsátott ki. Ezen belül öt alkalommal értékelte az Európai Közösség előző évi adatvédelmi tevékenységét. A javaslatokat és munkaanyagokat egyrészt saját kezdeményezésre, másrészt a Bizottság által előkészített jogi dokumentumok tervezetére készített állásfoglalások alapján adta közre.

A dokumentumok tartalmilag az adatkezelés, illetve az ezzel összefüggő problémák széles körét fedik le. A munkabizottság nagy súlyt fektetett a *harmadik országokba* történő adattovábbítás *egységes gyakorlatának* kialakítására, ezzel kapcsolatban 15 dokumentumot készített. (Érdemes megjegyezni, hogy az Egyesült Államokkal végül megkötött Safe Harbour-megállapodás tárgyában négy dokumentum készült: ezek egyértelműen tükrözik az amerikai és az európai adatvédelmi felfogás és gyakorlat közötti eltéréseket, és azt, hogy a különbségek nehezen oldhatók föl.)

A munkabizottság nagy figyelmet fordít az *információs technológia* fejlődése és az *internet* térhódítása következményeként felvetődő adatvédelmi problémákra és veszélyekre. E témakörben 12 dokumentumot bocsátott ki, közülük több jelentős hatással volt az elektronikus kommunikációra vonatkozó új irányelv elkészültére.

A munkabizottság tevékenységében – megfigyelőként – 2001 óta a magyar adatvédelmi biztos is részt vesz.

6. Az Európai Bíróság esetjoga

Anglia és Wales Legfelsőbb Bíróságának kezdeményezésére az Európai Bíróság előzetes döntést hozott a mezőgazdasági, halászati és élelmiszerügyi minisztérium és a „TR & P Fischer"-ügyben[35], amely az irányelv értelmezésén alapult. A tényállás lényege a következő: Fischer farmer 1995-ben megbízást kapott egy bizonyos földterületen történő gazdálkodásra. A megbízó, illetve a korábbi tulajdonos azonban nem adott tájékoztatást neki a föld használatának előzetes történetéről. Ezekre az információkra azért lett volna szüksége, mert a közösségi jog alapján támogatást kaphatott a termékek meghatározott körére, ha megfelelő földterületen és meghatározott feltételek mellett termeli őket. Ez utóbbi feltételek között szerepel, hogy a földterület bizonyos százalékát műveletlenül kell hagyni, de ezt az előző évben be kell jelenteni az illetékes hatóságnak. A rendelet alapján a tagállamok számítógépes nyilvántartást állítanak fel egyrészt a támogatási kérelmekről, másrészt a földterületekről. Fischer úr

ahhoz, hogy a támogatási kérelmét megfelelően be tudja nyújtani, információt kért a nyilvántartás vezetésére hivatott illetékes agrárhivataltól, de ez az információ kiadását

megtagadta azzal, hogy azt csak magának az adatszolgáltatónak – az előző tulajdonosnak – vagy megbízottjának adhatja ki. A kérdés az volt, hogy a farmer vagy megbízottja által a nyilvántartás részére szolgáltatott adat harmadik személynek kiadható-e.

Az Európai Bíróság kifejtette, hogy az irányelv 7. cikk f) pontja lehetővé teszi az adatok kiadását, „ha az olyan harmadik személy jogos érdekeinek érvényesítése céljaihoz szükséges, akinek az adatot továbbítják, kivéve, ha ezeket az érdekeket az adatalany védelmet igénylő érdekei vagy alapvető jogai és szabadságai felülmúlják". A tárgyi ügyben Fischer úr az adatokat azon jogszerű érdekből kérte, hogy a támogatás igényléséhez szükséges adatszolgáltatási kötelezettségének eleget tudjon tenni, és ezeket az adatokat más módon nem tudta beszerezni. Ugyanakkor nem merült fel semmi olyan információ, amely szerint ezeknek az adatoknak a kiadása sértette volna az adatalany (korábbi tulajdonos) védelmet igénylő érdekeit vagy alapvető jogait és szabadságait. Ezért az Európai Bíróság kimondta, hogy ilyen esetekben az illetékes hivatalnak – az érintett személyek érdekeinek mérlegelése után – a föld előző használatára vonatkozó adatokat ki kell adnia az új farmer részére.

36 Rendelet 51. cikk
37 Rendelet 3. cikk
38 A rendelet 51. cikke szerint az OJ-ban történt kihirdetést (2001. január 12) követő 20. napon lépett hatályba
39 Rendelet 50. cikk

IV. A közösségi intézményekre irányadó adatvédelmi követelmények

Az Európai Uniót alapító szerződés 286. cikke szerint a szerződéssel, illetve az annak alapján létrehozott intézményeknek és szerveknek a természetes személyek védelme érdekében a személyes jellegű adatok kezelésére és ezen adatok szabad mozgására a vonatkozó közösségi aktusokat kell alkalmazniuk. A Tanácsnak *független ellenőrző szervet* kell alapítania azzal a megbízással, hogy a közösségi szerveknél és intézményeknél felügyelje az említett közösségi aktusok alkalmazását, és minden más – az adott esetben – hasznos rendelkezést elfogadjon.

Ennek megfelelően adta ki az Európai Parlament és a Tanács 2000. december 18-án a *45/2001 EK rendeletet* (a továbbiakban: rendelet) az egyének védelméről az Európai Közösség intézményei és testületei által történő személyes adatkezelés tekintetében. A rendelet a tagállamokra *kötelező*, és *közvetlenül alkalmazandó*[36]. Ez annyit jelent, hogy jogokat és kötelezettségeket keletkeztet a Közösség intézményeivel és testületeivel kapcsolatba kerülő tagállami állampolgárok, illetve intézmények számára a személyes adatok kezelése során. (Tehát, ha egy uniós állampolgár panaszt tesz a közösségi állampolgári biztosnál vagy az Európai Bírósághoz fordul, joga van személyes adataira a rendelet szerinti védelmet igényelni.)

1. A rendelet hatálya

A rendelet hatálya a *közösségi intézményekre és testületekre* terjed ki, ha személyes adatokat kezelnek, egészben vagy részben a közösségi jog hatálya alá tartozó tevékenységük során. Az Európai Közösség intézményei és testületei, különösen a Bizottság, mindennaposan cserélnek személyes adatokat a tagállamokkal a Közös Agrárpolitika ügyében, a vámeljárás során, a Strukturális Alapokkal kapcsolatban és a Közösség működésének más területein. A Bizottság hangsúlyozza, hogy e tevékenységeknél figyelemmel kell lenni az általános adatvédelmi irányelv és a telekommunikációs irányelv rendelkezéseire is.

A rendelet *tárgyi hatálya* az egészben vagy részben automatikus módon végzett adatkezelésre, továbbá a valamely nyilvántartási rendszer részét képező, nem automatikus módon végzett adatkezelésre terjed ki[37]. A Közösség intézményeinek és testületeinek a rendelet hatálybalépésétől[38] számított *egy éven belül* kellett rendszereiket összhangba hozni rendelkezéseivel[39].

2. A rendelet lényeges elemei

A rendelet az adatvédelem alapvető elveit és követelményeit az irányelv rendelkezéseivel azonos tartalommal szabályozza. Szabályozási köre azonban szélesebb, mert kitér arra is, hogyan kell védeni a személyes adatokat a belső telekommunikációs hálózatok működtetése során. Ennek alapjául a 97/66 EK irányelvnek az a része szolgált, amely a személyes adatoknak a telekommunikációs szektorban való védelmét szabályozza.

A rendelet *eltérően szabályozza* az adatok továbbítását az alábbi esetekben:

- Az Európai Közösség szervei és intézményei között akkor lehet adatot továbbítani, ha a személyes adat az *igénylő intézmény hatáskörébe tartozó feladat jogszerű teljesítéséhez* szükséges (a jogszerűségért mind az adatátadó, mind az adatátvevő felelősséggel tartozik)[40].
- Az irányelv alapján kiadott nemzeti rendelkezések hatálya alá tartozó szervek részére adat akkor továbbítható, ha az adatot kérő

igazolja, hogy a továbbítás *közérdeken* alapul, vagy *közigazgatási feladatai* ellátásához szükséges; vagy, ha a kérelmező igazolja az igényelt adatok szükségességét, és nincs ok feltételezni, hogy az adatalany jogszerű érdekei sérülnének[41].

40 Rendelet 7. cikk
41 Rendelet 8. cikk
42 Rendelet 9. cikk
43 Rendelet 24., 25. cikk
44 Az Európai Parlament, a Tanács és a Bizottság 2002. július 1-jei 1247/2002 EK határozata az európai adatvédelmi felügyelő feladatainak ellátásához szükséges szabályokról és általános feltételekről
45 Rendelet 42–48. cikk
46 Rendelet 33. cikk

• Olyan országok vagy nemzetközi szervezetek részére, amelyek nem tartoznak az irányelv hatálya alá, akkor továbbíthatnak személyes adatokat a Közösség intézményei, ha az adatigénylő *megfelelő védelmet* szavatol. A rendelet részletezi a megfelelő védelem megállapításának szempontjait, illetve tételesen meghatározott esetekben akkor is lehetővé teszi az adatok továbbítását, ha a megfelelő védelemre nincs garancia. Ez utóbbi esetekben az európai adatvédelmi felügyelő is engedélyezheti az adatok továbbítását, ha a védelemre megfelelő biztosítékok állnak rendelkezésre[42].

A rendelet *kétszintű belső adatvédelmi ellenőrző rendszert* hozott létre. Minden közösségi intézményben és testületben ki kell nevezni legalább egy *adatvédelmi hivatalnokot,* akinek az a feladata, hogy függetlenként szavatolja a rendeletből adódó adatvédelmi követelmények teljesítését; az adatalanyokat és adatkezelőket megfelelő módon tájékoztassa jogaikról és kötelezettségeikről; teljesítse az európai adatvédelmi felügyelő megkeresését, illetve előzetesen bejelentse neki az adatkezelést; valamint vezesse az adatvédelmi nyilvántartást. Függetlenségét garantálja, hogy senkitől sem fogadhat el utasítást, és állásából csak az európai adatvédelmi felügyelő hozzájárulásával menthető fel[43].

A rendelet létrehozta az *európai adatvédelmi felügyelő* intézményét, akit (és helyettesét) a Bizottság által – a jelölésre történő nyilvános felhívás alapján készített listából – az Európai Parlament és a Tanács közös döntéssel nevez ki öt évre. Megbízatása alól csak akkor menthető fel, ha az Európai Bíróság – az Európai Parlament, a Tanács vagy a Bizottság kezdeményezésére lefolytatott eljárásban – megállapítja, hogy már nem teljesíti a tisztség betöltésének követelményeit, illetve súlyos hivatali kötelességmulasztásban vétkes. Az európai adatvédelmi felügyelő és helyettese jövedelméről, a kinevezését megelőző eljárásról és székhelyéről az Európai Parlament, a Tanács és a Bizottság külön határozatban rendelkezett[44].

Az európai adatvédelmi felügyelő felelős azért, hogy a természetes személyek személyes adataik védelméhez való jogát az Európai Közösség intézményei megfelelően biztosítsák. Ennek teljesíthetősége érdekében jogai hasonlóak az irányelv szerint meghatározott jogokhoz. Ezenkívül az Európai Bírósághoz fordulhat, illetve a Bíróság előtt folyó eljárásba beavatkozhat[45]. A rendelet külön kiemeli, hogy a közösség intézményeinek alkalmazottai közvetlenül jelezhetik az európai adatvédelmi felügyelőnek, ha a rendeletben meghatározott adatvédelmi követelmények megsértését észlelik[46].

V. Adatvédelem és az elektronikus kommunikáció

Az irányelv a személyes adatok védelmének alapvető elveit rögzíti, amelyek irányadók a személyes adatok automatikus feldolgozásának minden, az irányelv hatálya alá tartozó területére. Nem foglalkozik azonban az új telekommunikációs szolgáltatások elterjedésével, a felhasználók személyes adatainak és magánéletének védelme területén felvetődő speciális kockázatokkal. Felismerve, hogy szükség van e területen – az irányelvben megfogalmazott általános követelmények érvényesülése mellett – *speciális szabályokra* is, az Európai Parlament és a Tanács megalkotta a *97/66 EK irányelvet* a személyes adatok feldolgozásáról és a magánélet védelméről a telekommunikációs szektorban (a továbbiakban: *telekommunikációs irányelv)*, amelynek átültetésére a tagállamok részben 1998. október 24-ig, részben 2000. október 24-ig kaptak időt a szükséges jogszabályok megalkotására.

A telekommunikációs irányelv *hatálya* kiterjed a személyes adatok kezelésére és feldolgozására, a nyilvános telekommunikációs hálózatokon keresztül a nagyközönség számára hozzáférhető telekommunikációs szolgáltatásokra (kivéve a rádió- és televízióműsorok szolgáltatását), különös tekintettel az ISDN- és a nyilvános digitális mobilhálózatokra. Hatálya alá tartozik a hívó fél és a kapcsolódó vonal kijelzése, az automatikus hívásátirányítás a digitális központokhoz kapcsolódó előfizetői vonalakon és – ha ez műszakilag lehetséges és nem igényel aránytalanul nagy gazdasági erőfeszítést – az analóg központokon is[47].

1. A telekommunikációs irányelv főbb rendelkezései, általános követelmények

1.1. A biztonság

A telekommunikációs szolgáltató cég – szükség esetén a telekommunikációs hálózatok szolgáltatójával – köteles megfelelő *műszaki és szervezési intézkedéseket* tenni szolgáltatásainak biztonsága érdekében. Ha rend-

47 Telekommunikációs irányelv 3. cikk
48 Telekommunikációs irányelv 4. cikk
49 Telekommunikációs irányelv 5. cikk és 14. cikk (1) bekezdés

kívül nagy a veszélye annak, hogy valaki megsérti a hálózat biztonságát, akkor a kockázatokról és a lehetséges ellenintézkedésekről, valamint ezek költségeiről a telekommunikációs szolgáltató köteles *tájékoztatni előfizetőit*[48].

1.2. A kommunikáció titkossága

A tagállamok jogi szabályozással kötelesek megteremteni a nyilvános telekommunikációs hálózatokon és a nagyközönség számára hozzáférhető telekommunikációs szolgáltatásokon keresztül lebonyolított kommunikáció titkosságát. Különösen *meg kell tiltani* a kommunikáció megfigyelését, lehallgatását, tárolását, illetve a más módokon történő – az érintett felhasználók beleegyezése nélküli – beavatkozást vagy megfigyelést, kivéve, ha azt nemzeti jogszabály lehetővé teszi.

Jogszabály lehetővé teheti a kommunikáció tartalmának *megismerését és felhasználását* törvényes üzleti tevékenység során – kereskedelmi tranzakciók bizonyítékaként – vagy más üzleti kommunikációkról készített rögzítéseknél, továbbá a nemzetbiztonság, a honvédelem és a közbiztonság védelme, valamint a közvádas bűncselekmények, a telekommunikációs rendszer jogosulatlan felhasználásának üldözése érdekében[49].

1.3. Forgalmazási és számlázási adatok

A beszélgetés befejezése után *törölni* vagy *anonimizálni* kell azokat az előfizetőkre és a felhasználókra vonatkozó adatokat, amelyeket a telekommunikációs szolgáltató cégek a hívások létrehozása céljából dolgoznak fel és tárolnak.

Az előfizetők és a felhasználók részére történő kiszámlázás és a kapcsolódó díjak beszedése céljából a *következő adatok dolgozhatók fel:*

- az előfizetői állomás száma vagy más azonosítója;
- az előfizető címe és az állomás típusa;
- az elszámolási időszakban elszámolható összes egység száma;
- a hívott előfizetői szám, típus, kezdő időpont, a lefolytatott beszélgetés időtartama és/vagy a továbbított adat terjedelme;

- a hívás/szolgáltatás dátuma;
- a fizetéssel kapcsolatos egyéb információk (mint előzetes fizetés, részletfizetés, szétkapcsolás és figyelmeztetések).

Ezek az adatok a számla kiküldésének határidejéig, illetve a díjtartozás elévüléséig tárolhatók. A telekommunikációs cég – az előfizető beleegyezésével – marketingcélból is feldolgozhatja ezeket az adatokat.

Az adatok *átadhatók*:

- azoknak, akik a telekommunikációs cég megbízása alapján a számlázást, a forgalmazás kezelését, az ügyfél-tájékoztatást, illetve a csalások feltárását végzik;
- nemzeti jogszabály rendelkezése szerint a számlázási és forgalmazási jogviták rendezésére hatáskörrel rendelkező szervek részére;
- nemzeti jogszabály rendelkezése szerint a nemzetbiztonság, a honvédelem és a közbiztonság védelme, valamint a közvádas bűncselekmények és a telekommunikációs rendszer jogosulatlan felhasználásának üldözése érdekében az arra hatáskörrel rendelkező szerveknek.

Az előfizetőknek joguk van arra, hogy *részletezett számlát* kapjanak. Jogi szabályozással össze kell hangolni az előfizetők részletes számlához való jogát a hívást kezdeményező felhasználóknak és a hívott előfizetőknek a magánélet sérthetetlenségéhez fűződő jogával[50].

1.4. A hívó fél és a kapcsolódó vonalak kijelzése

A telekommunikációs irányelv részletes rendelkezéseket tartalmaz arra, hogy miként lehet a hívó fél azonosítását kiküszöbölni, illetve, hogy miként utasíthatja el ebben az esetben a hívott fél a hívást. Ezekről a lehetőségekről a szolgáltató cégeknek tájékoztatniuk kell a nyilvánosságot.

Megfelelő jogi szabályozással lehetővé kell tenni, hogy a telekommunikációs szolgáltatók felülbírálhassák a hívó fél azonosítása kijelzésének kiküszöbölését:

50 Telekommunikációs irányelv 6., 7. cikk
51 Telekommunikációs irányelv 8., 9, 10.cikk
52 Telekommunikációs irányelv 11. cikk
53 Telekommunikációs irányelv 12. cikk
54 3/97. ajánlás a névtelenségről az interneten, 1/99. ajánlás a személyes adatoknak szoftver és hardver által végzett, rejtett és automatikus kezeléséről az interneten, 2/2000. vélemény a telekommunikációs jogi keret általános felülvizsgálata kapcsán, 7/2000. vélemény a Bizottság 2000. július 12-i javaslatáról a személyes adatok kezeléséről és a privát élet védelméről az elektronikus kommunikációs szektorban, 2/2002. vélemény az egyéni azonosítók használatáról a telekommunikációs terminál eszközökben, az Ipv6 példája, 2002. május 30-i munkadokumentum az EU adatvédelmi nemzetközi alkalmazásának meghatározásáról a nem EU-tagállamokban alapított weboldalakon kezelt személyes adatok védelméről.
55 R (99) 5. sz. ajánlás a magánélet védelméről az interneten. Iránymutatások az egyének védelméről és a személyes adatoknak az információs highway-n történő gyűjtéséről és kezeléséről.

- Ideiglenesen, az előfizető kérésére, a rosszindulatú vagy kellemetlenkedő hívások nyomon követése érdekében. Ilyenkor – a nemzeti jogszabályok alapján – a hívó fél azonosítására alkalmas adatokat tárolják, és az ott meghatározottak szerint hozzáférhetővé teszik azokat.
- Hívásonként olyan szervezetek számára, amelyek segélykérő hívásokkal foglalkoznak, illetve a bűnüldöző szervek, a mentőszolgálatok és a tűzoltóság részére az ilyen jellegű hívások azonosítása céljából[51].

1.5. Az előfizetők adatait tartalmazó telefonkönyvek

A nyilvános vagy az információs szolgálatokon keresztül hozzáférhető, nyomtatott vagy elektronikus telefonkönyvek az előfizető félreérthetetlen hozzájárulása nélkül csak annyi adatot tartalmazhatnak róla, amennyi az azonosításához feltétlenül szükséges.

Az előfizetőnek joga van kérni, hogy neve külön költség nélkül kimaradjon a nyomtatott vagy elektronikus telefonkönyvből; kérheti annak jelzését, hogy személyes adatait nem használhatják föl direkt marketing céljaira, illetve azt, hogy ne teljes lakcíme szerepeljen a listán[52].

1.6. Nem kívánt hívások

Az emberi beavatkozás nélküli, automatizált hívórendszerek csak akkor alkalmazhatók direkt marketing céljára, ha ehhez az előfizetők előzetesen hozzájárultak. A más eszközökkel lebonyolított direktmarketing-célú hívások korlátozása a tagállamok hatáskörbe tartozik. A tagállamoknak garantálniuk kell továbbá a nem természetes személy előfizetők legitim érdekeinek védelmét is a nem kívánt hívásokkal szemben[53].

2. Az elektronikus irányelv

Az elektronikus kommunikációs szolgáltatások és technológiák rohamos fejlődése szükségessé tette, hogy a Bizottság a telekommunikációs irányelv módosítására új javaslatot terjesszen elő a Parlamentnek, illetve a Tanácsnak. Ennek kimunkálására és továbbfejlesztésére jelentős befolyása volt az Adatvédelmi Munkabizottságnak, amely több ajánlást és véleményt bocsátott ki[54]. Ezen túlmenően a közösségi jogalkotók irányadónak tekintették az Európa Tanácsnak az internet használata során felvetődő adatvédelmi kérdésekkel foglalkozó ajánlását is[55]. Ennek eredményeként alkották meg az Európai Parlament és a Tanács 2002. július 12-i *2002/58 EK irányelvét* a személyes adatoknak az elektronikus kommunikációs ágazatban történő feldolgozásáról és a magánélet védelméről (a továbbiakban: *elektronikus irányelv)*, amely a telekommunikációs irányelv helyébe lépett. Az új irány-

elv átültetéséhez szükséges jogszabályokat a tagállamoknak 2003. október 31-ig kell megalkotniuk[56].

Az új irányelv jelentősége abban áll, hogy a telekommunikációs irányelv rendelkezéseinek hatályát kiterjesztette a *közcélú elektronikus kommunikáció teljes körére* – beleértve az internetet is –, függetlenül az igénybe vett technikai megoldásoktól. Nem tartozik viszont a hatálya alá a közcélú hírközlési hálózaton keresztül nyújtott műsorszolgáltatás. A telekommunikációs irányelvben megfogalmazott tartalmi rendelkezéseket szinte változatlan tartalommal építették be az új irányelvbe, amely ezen túlmenően kiegészült a következő dolgok meghatározásával *a forgalmi,* illetve a *helymeghatározási adat*, a *kommunikáció*, a *hívás*, az *értéknövelt szolgáltatás* és az *elektronikus levél* fogalmának definíciója[57].

Az *előfizetői* vagy a *felhasználói végberendezésen tárolt információkhoz az elektronikus kommunikációs hálózat útján történő hozzáférés,* vagy az ott, ilyen módon történő információtárolás korlátozása[58]. Az irányelv preambuluma kifejti, hogy az elektronikus távközlési hálózatok felhasználóinak végberendezései és az azokon tárolt minden információ a felhasználók magánszférájának részét képezik, amely megköveteli az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény szerinti védelmet. Az úgynevezett kémszoftverek, webpoloskák, rejtett azonosítók és más hasonló eszközök a felhasználó tudta nélkül hozzáférhetnek a felhasználó végberendezéséhez információszerzés, rejtett információk tárolása vagy a felhasználó tevékenységeinek követése céljából, és ez súlyosan sértheti a felhasználóknak a magántitokhoz való jogát. Ezeket az eszközöket *kizárólag törvényes* céllal, az érintett felhasználók tudtával lehet alkalmazni.

A preambulum kitér arra is, hogy az ilyen eszközök – mint például az úgynevezett cookie-k – törvényes és hasznos eszközök lehetnek, például a honlaptervezés és a hirdetés hatékonyságának elemzése, valamint az on-line ügyletekben részt vevő felhasználók azonosítása során. Törvényes célú használatuk azzal a feltétellel engedélyezhető, hogy a felhasználók – a 95/46/EK irányelvnek megfelelően – világos és pontos információt kapnak a cookie-k vagy a hasonló eszközök cél-

56 Elektronikus irányelv 17. cikk, 1. bekezdés
57 Elektronikus irányelv 2. cikk b), c), d) g) és h) pontja
58 Elektronikus irányelv 5. cikk, 3. bekezdés
59 Elektronikus irányelv Preambulum 24., 25. pont
60 Elektronikus irányelv 9. cikk.
61 Elektronikus irányelv Preambulum 26–28. pont
62 Adatvédelmi Munkabizottság 2/2002. sz. véleménye

járól. A felhasználók figyelmét fel kell hívni az általuk használt végberendezésen elhelyezett információkra. A felhasználóknak lehetőséget kell adni arra, hogy megtagadják a cookie-k vagy hasonló eszközök tárolását végberendezésükön. Ez különösen fontos, ha az eredeti felhasználón kívül más felhasználók is hozzáférhetnek a végberendezéshez, és ezáltal minden, a berendezésen tárolt magánjellegű információhoz is[59].

Az *előfizetőkkel kapcsolatos,* elektronikus kommunikációs hálózatok által feldolgozott, a csatlakoztatáshoz és az információ továbbításához szükséges *helymeghatározási adatok*[60] a természetes személyek magánéletére vonatkozó információkat is tartalmaznak. Az ilyen adatokat kizárólag a számlázás és az összekapcsolási díj kifizetése céljából, a szolgáltatás nyújtásához szükséges mértékig lehet tárolni, és csak korlátozott ideig. Az elektronikus kommunikációs szolgáltatónak – elektronikus kommunikációs szolgáltatások értékesítése vagy értéknövelt szolgáltatások nyújtása céljából – minden további feldolgozásukra kizárólag akkor van lehetősége, ha ehhez az előfizető – pontos és teljes körű tájékoztatás alapján – hozzájárult. A tájékoztatásban ki kell térni az elvégezni kívánt további adatfeldolgozási típusokra, valamint arra, hogy az előfizető az ilyen adatfeldolgozáshoz nem köteles hozzájárulni, és hozzájárulását visszavonhatja.

A *marketing kommunikációs* szolgáltatásokhoz vagy az *értéknövelt* szolgáltatásokhoz felhasznált forgalmi adatokat a szolgáltatás teljesítése után ugyancsak törölni kell, vagy anonimmá kell tenni. A szolgáltatóknak mindig tájékoztatniuk kell az előfizetőket az általuk feldolgozott adatok típusáról, valamint az adatfeldolgozás céljáról és időtartamáról.

A *kommunikáció befejezésének pontos ideje* – amikor a forgalmi adatokat a számlázási célok kivételével törölni kell – függhet az elektronikus távközlési szolgáltatás típusától. Például egy telefonhívásnál az átvitel befejeződik, amint bármelyik felhasználó megszakítja a kapcsolatot, az elektronikus levelezésnél pedig akkor, ha a címzett megkapta az üzenetet (általában szolgáltatója szerveréről). Amennyiben a forgalmi adatokra már nincs szükség a kommunikáció átviteléhez, a törlésükre vagy anonimmá tételükre vonatkozó kötelezettség nem ütközik az olyan internetes eljárásokkal, mint az IP-címek elraktározása a domainnév-rendszerbe, vagy az IP-címek mentése a cache-memóriába, illetve a bejelentkezési információknak a hálózatokhoz vagy szolgáltatásokhoz való hozzáférését szolgáló használata[61]. Lényeges, hogy az IP-címek az Adatvédelmi Munkabizottság álláspontja szerint egyértelműen személyes adatoknak minősülnek[62].

3. Az internettel kapcsolatos további adatvédelmi iránymutatások

A számítógépes világháló használatához fűződő adatvédelmi kérdésekkel kapcsolatban két további dokumentum érdemel említést: Az Európai Unió Adatvédelmi Munkabizottságának *3/97. számú ajánlása* a névtelenségről az interneten, valamint az

Európa Tanács *R (99) 5. számú ajánlása* a magánélet védelméről az interneten. (Irányelvek az egyének védelméről és a személyes adatoknak az információs highway-n történő gyűjtésével és kezelésével kapcsolatban.)

3.1. Az Európai Unió Adatvédelmi Munkabizottságának 3/97. számú ajánlása

A munkabizottság az *internetfelhasználás adatvédelmi kockázatai* és az *anonim internethasználat* elemzése alapján a következő fő következtetéseket vonta le:

- Az anonimitás lehetőségének választása elengedhetetlen ahhoz, hogy az egyének megtarthassák személyes adataik ugyanazon védelmét az *on-line* alkalmazásnál, mint amit *off-line* esetben élveznek.
- Az anonimitás *nem minden körülmények között* alkalmazható. Meg kell határozni azokat a körülményeket, amelyek esetén a felhasználó névtelen maradhat, és azokat, amikor az anonimitás akadályozza az alapvető jogok arányosságának érvényesülését. Nemcsak a személyes adatok védelmére kell figyelemmel lenni, hanem a véleménynyilvánítás szabadságára, illetve más fontos közérdekű célokra (mint a bűnözés megelőzése). Azoknak a jogi korlátozásoknak, amelyeket a kormányok elrendelhetnek a névtelenség joga érvényesülésének, illetve az erre irányuló technikák használatának érdekében (például rejtjelezés alkalmazása) mindig arányosnak, és a meghatározott közérdek védelméhez szükséges mértékűnek kell lenniük.
- A passzív *böngészést* a világháló weboldalain, az *áruk és szolgáltatások vásárlását* az interneten keresztül anonim módon is lehetővé kell tenni.
- Az egyének valamilyen kontrolljára szükség van a közreműködő tartalmú on-line nyilvános szolgáltatásoknál. De azt követelni, hogy a személy minden esetben azonosítsa magát, aránytalan és nem praktikus. Más megoldásokat kell tehát előnyben részesíteni.

- Az *internet-hozzáférés névtelen módja* (például nyilvános internetkioszkok, előre fizetett hozzáférő kártyák) és az *anonim fizetési mód* a tényleges on-line anonimitás két lényeges eleme.

3.2. Az Európa Tanács R (99) 5. számú ajánlása

Az internetszolgáltatók kötelezettségei:

- Alkalmas *eljárások* és a *rendelkezésre* álló, elsősorban minősített technológiák használata az érintett személyek magánéletének védelme érdekében, különösen az adatok sértetlenségének és titkosságának, valamint a hálózat és a szolgáltatások fizikai és logikai biztonságának szavatolásával.
- Az előfizetés, illetve a használat megkezdése előtt a *felhasználók tájékoztatása* azokról a magánéletet érintő *kockázatokról*, amelyek az internet használatával járnak. Ezek a kockázatok érinthetik az adat sérthetetlenségét, titkosságát, a hálózat biztonságát vagy a magánélet más sérelmét (mint az adatok burkolt gyűjtése vagy regisztrálása).
- A *felhasználók tájékoztatása* azokról a *technikai lehetőségekről,* amelyeket jogszerűen használhatnak az adatokra és a kommunikációra ható kockázatok mérséklésére. Ilyen lehet a legálisan alkalmazható *rejtjelezés* és a *digitális aláírás*.
- Az előfizetések elfogadása és a felhasználók internethez kapcsolódása előtt informálni kell a felhasználókat a világhálóhoz történő *névtelen hozzáférés lehetőségéről*, a szolgáltatások használatának és a díjfizetésnek az anonim módjairól (például előre fizetett hozzáférő kártya). Ha törvény megengedi, *álnév* használatának lehetőségét kell ajánlani (amikor a valódi személyazonosságot csak a szolgáltató ismerheti meg). Tájékoztatni kell őket azokról a *programokról*, amelyek abban segítenek, hogy névtelenül kutassanak és böngésszenek a világhálón. Olyan módon kell szerkeszteni a rendszert, hogy elkerülhető vagy minimalizálható legyen a személyes adatok használata.
- A szolgáltató nem olvashatja el, nem módosíthatja vagy nem törölheti a másoknak küldött üzeneteket.
- Nem engedhető meg semmilyen beavatkozás az üzenetek tartalmába, kivéve, ha ezt a beavatkozást jogszabály rendeli el, és közigazgatási szerv végzi.
- A felhasználókról adatot gyűjteni, feldolgozni és tárolni csak akkor szabad, ha az egyértelmű, meghatározott és jogszerű célból szükséges.
- Az adatok nem továbbíthatók, kivéve, ha továbbításukat jogszabály rendeli el.
- Az adatok nem tárolhatók tovább, mint ameddig az adatkezelés céljának eléréséhez szükség van a tárolásukra.
- A szolgáltató nem használhatja az adatokat saját reklám- vagy piaci céljaira, kivéve,

ha az érintett – az erről történő megfelelő tájékoztatás után – nem tiltakozott, illetve, ha a forgalmazott vagy szenzitív adatokra egyértelmű hozzájárulását adta.

- A szolgáltató felelős az adatok megfelelő használatáért. A bemutatkozó oldalon világos *tájékoztatást* kell adnia *adatvédelmi politikájáról*. A tájékoztatásnak tartalmaznia kell az adatvédelmi gyakorlat részletes magyarázatát. Mielőtt a felhasználó megkezdi a szolgáltatás használatát, amikor az oldalra látogat – és amikor csak kéri –, tájékoztatni kell arról, hogy ki a szolgáltató, milyen adatokat gyűjt, dolgoz fel és tárol, milyen módon, milyen célból és milyen hosszú ideig őrzi azokat. Ha szükséges, kérni kell a felhasználó hozzájárulását. Az érintett személy kérelmére azonnal helyesbíteni kell a pontatlan adatokat, és törölni kell azokat, ha túlzók, időszerűtlenek vagy tovább nem kívánatosak, illetve le kell állítani az adatok feldolgozását, ha a használó tiltakozik ellene. Minden módosításról értesíteni kell azokat a harmadik személyeket, akiknek az adatot továbbították. El kell kerülni a rejtett adatgyűjtést.
- A felhasználók részére szolgáltatott információnak pontosnak és időszerűnek kell lennie.
- Az adatok világhálós oldalon való publikálása sértheti más személyek magánéletét, illetve ezt a jog is tilthatja.
- Mielőtt adatot külföldre továbbítanak, tanácsot kell kérni – például az adatvédelmi hatóságtól –, hogy a továbbítás megengedhető-e. A szolgáltató kérheti, hogy az átvevő adjon megfelelő védelmet, amelyre az adatok védelméhez szükség van.

A felhasználó felelős:

- az adatfeldolgozásért, ha jogtalanul feltölt vagy letölt;
- az általa küldött rosszindulatú üzenetekért.

Az ajánlás azt is rögzíti, hogy az elektronikuslevél-cím személyes adat, amelyet ennek megfelelően kell védeni.

VI. A magyar jogi szabályozás és az Európai Közösség adatvédelmi irányelvei

Az Európai Bizottság több országjelentésben kifejtette, hogy a magyar adatvédelmi szabályozás alapvetően megfelel az adatvédelmi irányelv követelményeinek, és csak néhány rendelkezés módosítására vagy kiegészítésére lesz szükség a csatlakozás időpontjáig. Ezt az álláspontot támasztja alá az is, hogy a Bizottság *megfelelő védelmet nyújtó országnak* minősítette hazánkat. Különösen a független adatvédelmi ellenőr intézményének létét és működését tekintették példaértékűnek.

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló *1992. évi LXIII. törvény* (a továbbiakban: Atv.) módosítására és kiegészítésére a következő területeken van szükség azért, hogy teljesen megfeleljen az irányelvnek:

Az Atv. jelenleg nem tartalmaz konkrét rendelkezéseket a *törvény hatályát* illetően, az általános joghatósági elvek érvényesülnek rá, illetve a tárgyi hatályra az Atv. egyes konkrét rendelkezéseiből lehet következtetni. Indokolt a törvény személyi, tárgyi és területi hatályát pontosan meghatározni, figyelembe véve az irányelv 3. cikk 2. és 4. cikk c/1. pontját. Ennek megfelelően ki kell mondani, hogy a törvény hatálya kiterjed

- *a Magyar Köztársaság területén folytatott* minden adatkezelésre és adatfeldolgozásra, tekintet nélkül az adatkezelő, illetve az adatfeldolgozó állampolgárságára, honosságára, székhelyére, telephelyére vagy lakóhelyére;
- továbbá arra a nem a Magyar Köztársaság területén működő adatkezelőre, aki adatfeldolgozásra a *Magyar Köztársaság területén lévő eszközt* használ fel. E szabály alól az Európai Unióba történő belépés után kivétel lesz az az eset, ha ez az eszköz csak a Magyar Köztársaság vagy az Európai Közösség területén átmenő adatforgalom célját szolgálja.

Nem terjed ki a törvény hatálya a természetes személy kizárólag személyes vagy háztartási tevékenysége során keletkezett saját célra kezelt adataira.

Pontosítani kell a törvény *fogalomrendszerét.* Így a személyes adat fogalmát ki kell egészíteni annak részletezésével, hogy különösen mely esetekben tekinthető azonosíthatónak a természetes személy.

Az irányelv politikai véleményre vagy pártállásra vonatkozó adaton kívül *különleges adatnak* tekinti – a jelenlegi hazai szabályozásban foglaltakon túlmenően – a

szakszervezeti tagsággal összefüggő adatot is. Ezért a szabályozást ki kell egészíteni ennek az adatkörnek a különleges adattá minősítésével.

Az *adatkezelés fogalmát pontosítani* kell, és ki kell egészíteni a fogalomrendszert a személyesadat-nyilvántartó rendszer és az adatállomány fogalmával.

Meg kell határozni, hogy mit értünk az *adatalany hozzájárulása* alatt, és ki kell mondani, hogy a hozzájárulásnak félreérthetetlennek kell lennie.

Az *adatkezelés lehetőségét* ki kell egészíteni azon szerződéses jogviszonyok körére, amelyekben az érintett magánszemély félként szerezhet jogokat vagy kötelezettségeket.

A hazai adatvédelmi jogba is be kell vezetni az érintett *tiltakozásának lehetőségét* adatai kezelése vagy továbbítása ellen.

Az *adatkezelések jogalapjával* kapcsolatban – az érintett hozzájárulását és a törvényi elrendelést meghatározó alapelvet fenntartva – nevesíteni kell azokat a főbb esetköröket, amelyek különösen megalapozhatják a személyes adatok jogszerű kezelését.

Az irányelvben foglalt követelményeknek megfelelően indokolt előírni, hogy az *állam bűnüldözési, államigazgatási és bírósági feladatainak* ellátása céljából kezelt bűnügyi adatokat, továbbá államigazgatási, szabálysértési és a polgári peres ügyekre vonatkozó adatokat tartalmazó adatállományokat kizárólag állami vagy helyi önkormányzati szerv kezelheti és dolgozhatja fel.

Az adatfeldolgozás *formai követelményeként* kell előírni, hogy az arra vonatkozó megbízási szerződést írásba kell foglalni.

A *külföldre történő adattovábbítás* szabályait teljesen át kell dolgozni. Ki kell mondani, hogy az Európai Unió országaiba történő adattovábbítást nem szabad korlátozni, arra ugyanazok a szabályok vonatkoznak, mint az országon belüli adattovábbításra. A harmadik országokba való adattovábbítás során meg kell különböztetni a megfelelő védelmet nyújtó és az e körbe nem tartozó országokba történő adatátadás feltételeit. Ez utóbbi államokkal szemben továbbra

is indokolt fenntartani azt a követelményt, hogy csak akkor adunk át adatokat, ha megfelelő szabályok garantálják védelmüket ezekben az országokban is.

Az *automatizált egyedi döntéssel* kapcsolatos szabályozást jelenleg hatályos adatvédelmi jogunk nem ismeri. Ezért az erre vonatkozó követelményeket ki kell dolgozni, és ennek során ki kell mondani, hogy az adatalany személyes jellemzőit értékelni automatikus döntés alapján csak akkor szabad, ha törvény – az adatalany álláspontja érvényesítésének szavatolásával – lehetővé teszi.

Az *adatalany jogai érvényesítésének korlátozási lehetőségét* ki kell egészíteni a foglalkozások gyakorlásával összefüggő – jogszabályban vagy törvényen alapuló belső szabályzatban (például ügyvédek etikai kódexe) meghatározott – fegyelmi vagy etikai vétségek, illetve munkajogi kötelezettségszegés megelőzésével, vizsgálatával, feltárásával és üldözésével. A csatlakozás időpontjában történő hatálybalépéssel lehetővé kell tenni a korlátozást az Európai Unió valamely tagállama vagy az unió jelentős gazdasági vagy pénzügyi érdekei – beleértve a monetáris, költségvetési és adózási érdekeit – védelmének és ellenőrzésüknek vagy felügyeletüknek céljával.

Az *adatvédelmi biztos* jogait meg kell erősíteni, és ki kell egészíteni. Lehetővé kell tenni, hogy az adatvédelmi biztos elrendelhesse az adatok zárolását, törlését vagy megsemmisítését, ideiglenesen vagy véglegesen megtilthassa feldolgozásukat. Az adatvédelmi biztos ilyen tartalmú érdemi döntéseivel szemben meg kell teremteni a bírósághoz fordulás lehetőségét. Meg kell határozni, hogy milyen adatkezelés megkezdése előtt kell lehetővé tenni, hogy az adatvédelmi biztos előzetes bejelentés alapján megvizsgálja.

Az irányelvben foglaltaknak és a nemzetközi gyakorlatnak megfelelően elsősorban a nagy állami és piaci adatkezelő szervezeteken – például bankok, biztosítók – belül *belső adatvédelmi felelős* kinevezését és belső adatvédelmi és adatbiztonsági *szabályzat* készítését célszerű előírni.

A telekommunikációs irányelv harmonizálása megtörtént a hírközlésről szóló 2001. évi XL. törvénnyel, az elektronikus irányelv átültetése pedig a közeljövő feladata.

VII. További információforrások

Igazságügyi Minisztérium
http://www.im.hu

Európai Bizottság
http://europa.eu.int/comm/index_en.htm

Európai Parlament
http://www.europarl.eu.int

Európai Tanács
http://ue.eu.int/en/summ.htm

Európai Bíróság
http://www.curia.eu.int

Az adatvédelem szabályozása az Európai Unió alapértékeivel függ össze. Az unió megteremtésének elsőrendű célja volt egy olyan közös piac létrehozása, amelyben a személyek, az áruk, a tőke és a szolgáltatások belső határok nélkül, szabadon áramolhatnak. Mindehhez szükség volt és van az információtovábbítás szabadságára is. Az adatok átadásának ellenőrzése különösen nehéz azóta, hogy általánossá vált az egész világot behálózó, rendkívül gyors információtovábbítást lehetővé tevő internet használata. Az adatvédelmi szabályoknak egyfelől az információszabadságot, másfelől a magánélet védelmét kell szolgálniuk. Hazánknak az unióhoz való csatlakozása után át kell vennie az EU szabályait. Ez nem lesz nehéz feladat, mert Magyarország – Svájc és Kanada mellett – egyike annak a három országnak, amelyről az Európai Bizottság megállapította: megfelelő védelmet nyújt az információk továbbítására.

Dr. Oros Paulina
főosztályvezető-helyettes
Igazságügyi Minisztérium

Dr. Szurday Kinga
szakmai tanácsadó
Igazságügyi Minisztérium