ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA JURIDICA ET POLITICA

Tomus LXII.
Fasc. 7.

HAJDÚ JÓZSEF

A munkavállalók magánszférájának védelme, különös tekintettel az adatvédelemre

SZEGED
2002

ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA JURIDICA ET POLITICA

Tomus LXII.
Fasc. 7.

HAJDÚ JÓZSEF

A munkavállalók magánszférájának védelme, különös tekintettel az adatvédelemre

SZEGED
2002

Edit

Comissio Scientiae Studiorum Facultatis Scientiarum Politicarum et Juridicarum
Universitatis Szegediensis

ELEMÉR BALOGH, LÁSZLÓ BODNÁR, JÓZSEF HAJDÚ, ÉVA JAKAB,
JENŐ KALTENBACH, TAMÁS KATONA, JÁNOS MARTONYI,
FERENC NAGY, PÉTER PACZOLAY, BÉLA POKOL, JÓZSEF RUSZOLY,
IMRE SZABÓ, LAJOS TÓTH, LÁSZLÓ TRÓCSÁNYI

Redigit
KÁROLY TÓTH

Nota
Acta Jur. et Pol. Szeged

Kiadja

a Szegedi Tudományegyetem Állam- és Jogtudományi Karának
tudományos bizottsága

BALOGH ELEMÉR, BODNÁR LÁSZLÓ, HAJDÚ JÓZSEF, JAKAB ÉVA,
KALTENBACH JENŐ, KATONA TAMÁS, MARTONYI JÁNOS,
NAGY FERENC, PACZOLAY PÉTER, POKOL BÉLA, RUSZOLY JÓZSEF,
SZABÓ IMRE, TÓTH LAJOS, TRÓCSÁNYI LÁSZLÓ

Szerkeszti
TÓTH KÁROLY

Kiadványunk rövidítése
Acta Jur. et Pol. Szeged

ISSN 0324–6523 Acta Univ.
ISSN 0563–0606 Acta Jur.

Bevezetés

A magánszféra védelmének jogi koncepciója és a vele rokon fogalmak tartalma (pl. privát élet, személyes integritás stb.) csak a történelmileg folyamatosan változó gazdasági és társadalmi körülmények, valamint az egyes társadalmak kulturális értékrendjének függvényében értelmezhető. A magánélet védelmének fejlődését vizsgálva nem tendenciákról, hanem sokkal inkább a fent említett társadalmi, gazdasági és értékrenddel kapcsolatban fennálló szoros függőségről lehet beszélni. Ez a többszörös kapcsolatrendszer nagyon sok esetben alapvetően meghatározza a munkavállalók személyiségi jogaival (privát szférájával) kapcsolatos vizsgálódások keretét.

A német filozófus és szociológus Jürgen Habermas a „Strukturwandel der Öffentlichkeit" c. munkájában mutatja be, hogy a gazdasági, társadalmi és kulturális faktorok milyen módon befolyásolják a privát és a „közösség" kategóriák kölcsönös alakulását.

A norvég Jon Bing álláspontja szerint a személyiségi jogok védelmének legkorábbi koncepciója Nagy Britanniában és az Egyesült Államokban alakult ki. Hátterében a királyi személyek, illetve a társadalom legfelsőbb köreihez tartozó személyek magánéletével kapcsolatos információk védelmét szolgáló intézkedések és szabályok álltak.[1] Ugyanakkor, napjainkban a személyiségi jogok védelme elsősorban olyan mindennapi élethelyzetekre koncentrál, amelyek a társadalom túlnyomó többségét érintik. Pl. az állampolgár és a közigazgatás viszonyrendszere, a munkavállaló és a munkáltató közötti kapcsolat, munkáltatói kontroll és megfigyelés stb. A rohamos technikai fejlődés eredményeként az egyén (munkavállaló) és a köz (munkahely) közötti határvonalat újra kell gondolni. Gondoljunk itt az információs társadalom munkavégzési viszonyaiból következő sajátosságokra (pl. távmunka stb.).

Bizonyos esetekben a jogszabályok, illetve a munkáltató jól megfontolt gazdasági érdekei diktálják, sőt néhány esetben kikényszerítik a munkavállalókról történő adatgyűjtést, illetve adatfeldolgozást.[2] Például pozitív vonatkozásban (védelmi célzattal) a terhes nők, a kisgyermekes anyák védelme stb. A piacon fennálló szüntelen és éles harc is megkívánja, hogy a hatékonyság növelése érdekében a munkáltató bizonyos adatokkal rendelkezzen a munkavállalóiról. Pl. a munkavállaló munkaminőségének ellenőrzése, a munkaerő-felvételnél a munkavégzési intenzitásának, hozzáállásának a vizsgálata stb., továbbá biztonsági szempontból történő ellenőrzése. Amikor a munkáltató ilyen, vagy ehhez hasonló információkat gyűjt, akkor az esetek túlnyomó többségében tevékenységével érinti a munkavállaló személyes (privát) szféráját. Ugyanakkor a másik oldalon – a személyiségi jogokra hivatkozva – jogszabályok korlátozzák, illetve megtiltják azt, hogy a munkáltató bizonyos információkhoz hozzáférhessen.

---

[1] BING, JON: Privacy and Surveillance Systems. Norwegian Research Center of Computers and Law, Compendium to the Erasmus course 1994, *Public Administration and Information Technology*. Oslo 1994, pp. 76–96.

[2] Megjegyzés: Az EU 95/46/EC irányelv 2(b) cikkelyének előírása szerint az adatfeldolgozás (data processing) magában foglal minden olyan lépést, amely az adatgyűjtés és az adat megsemmisítése között van.

A teljes képhez hozzátartozik még annak az említése, hogy az objektívnek tekinthető jogi védelem (pl. levéltitok stb.) maga az érintett személy érzékenysége, neveltetése, beállítódása jelentős mértékben befolyásolja azt, hogy hol húzódik meg nála a személyiségi jogok védelmének határvonala és mikortól kell azt jogilag védeni.

1. A magánszféra védelmének alapvető fogalmi, történeti és rendszertani kérdései

1.1. A magánszféra fogalmának meghatározása

Az emberi jogok katalógusán belül talán a magánszféra fogalmát a legnehezebb meghatározni.[3] A magánszférát meghatározhatjuk, mint alapvető (bár nem abszolút) emberi jogot. A magánszféra fogalmi elemei mélyen benne gyökereznek a történelmi múltban. A Bibliában is számos utalást találunk a magánszféra.[4] A héber, a klasszikus görög és a kínai kultúrákban is megjelent a magánszféra védelme.[5] Ezek a korai kezdeményezések az önrendelkezéshez való jog (right to solitude) alapján álltak. A magánszféra definíciója nagymértékben változik attól függően, hogy milyen környezetben és kontextusban használjuk. Sok országban a magánszféra védelme összemosódik az adatvédelem (data protection) kérdésével, amely a magánszférát személyhez fűződő információk kezelésére korlátozza. Ezen a meglehetősen szűk értelmezésen kívül kialakult egy olyan koncepció, amely a magánszféra védelmét az egyén köré rajzolt (quasi jogi aura) vonalként fogja fel, amely azt jelzi, hogy a társadalom egyes szereplői (állam, az állam szervei, a munkáltató, egyes állampolgárok, munkatársak, stb.) meddig hatolhatnak be az egyén személyes világába (magánszférájába).[6] Mi magunk is erre az utóbbi álláspontra helyezkedünk. Ehhez a megközelítéshez áll közel a norvég „privacy-test" felfogás is, amellyel a későbbiekben még részletesen foglalkozunk.

A magánszféra védelmének fogalmáról kialakított néhány további megközelítést – a történelmi fejlődés tükrében – a következőkben foglalhatjuk össze.

A magánszféra védelmének a joga egészen 1361-ig visszavezethető, amikor a Justice of Peace Act Angliában letartóztatást helyezett kilátásba a leskelődésért (peeping toms) és a lehallgatásért.[7] Az elmúlt évszázadok során különböző országokban eltérő speciális védelme alakult ki a magánszférának.

Például a Svéd Parlament 1776-ban fogadta el az „Access to Public Records Act"-t. Ez előírta, hogy minden egyes adat, amivel az állam rendelkezik csak jogszerű módon kerülhet felhasználásra.

Az Emberi és Polgári Jogok Deklarációja (Declaration of the Rights of Man and the Citizen) 1792-ben deklarálta, hogy a magántulajdon szent és sérthetetlen.

---

[3] JAMES MICHAEL: *Privacy and Human Rights*. UNESCO1994 p.1.

[4] RICHARD HIXSON: *Privacy in a Public Society: Human Rights in Conflict 3 (1987)*. See Barrington Moore: Privacy: Studies in Social and Cultural History (1984).

[5] Published by Science and Technology Options Assesment (STOA). Ref: project no. IV/STOA/RSCH/LP/politicon. 1.

[6] SIMON DAVIS: *„Big Brother: Britain's web of surveillance and the new technological order"*. Pan, London, 1996 p. 23.

[7] JAMES MICHAEL, p. 15.

Franciaországban először 1858-ban tiltották meg és kemény pénzbüntetéssel sújtották a magánjellegű információkat nyilvánosságra hozatalát.[8]

1890-ben az USA Legfelsőbb Bíróságának bírája, Luis Brandies a magánszféra fogalmát a következőképpen fogalmazta meg: „az egyén joga arra, hogy békén hagyják" (right to be left alone). Álláspontja szerint a magánszféra a szabadságjogok közül a leginkább fejlődik a demokratikus viszonyok között és véleménye szerint ennek a jognak az alkotmányban is helyet kellene kapnia.[9]

Az Ausztráliai Privacy Karta preambuluma kimondja, hogy „egy szabad és demokratikus társadalom megköveteli az egyén autonómiájának respektálását és mind az állami, mind a privát szervezetek hatalmát korlátozni kell, ha azok meg akarják zavarni ezt az autonómiát". A magánszféra védelme – amely garantálja az emberi méltóság megvalósulását – éppen olyan alapvető jog, mint a gyülekezéshez, vagy a szólásszabadsághoz való jog. A magánszféra védelme alapvető emberi jog és méltán elvárható a társadalom minden egyes tagjától, hogy tiszteletben tartsa azt.[10]

Alan Westin a *Privacy and Freedom* c. munkájában (1967) a következőképpen határozta meg a magánszféra fogalmát: „az emberek azon kívánsága, hogy szabadon választhassanak abban, hogy milyen körülmények között és milyen mélységig fedjék fel önmagukat, attitűdjüket és viselkedésüket mások irányában."[11]

Edward Bloustein álláspontja szerint a magánszféra az ember személyiségének az érdekkifejeződése. Védi a személyiség sértetlenségét, az egyén függetlenségét, méltóságát és integritását.[12]

Ruth Gavison véleménye szerint három fontos összetevője van a magánszférának: a titkosság, az anonimitás és az illető személy békén hagyása. Ez egy olyan pillanatnyi állapot, amelyet vagy az egyén döntése vagy más személy tevékenysége által el lehet veszíteni.[13]

Nagy Britanniában az ún. Calcutt Bizottság megállapítása szerint „sehol sem találhatunk olyan jogi meghatározást a magánszférára, amely mindenkit kielégít". Ennek ellenére a Bizottság a következő meghatározással állt elő: „Az egyén joga arra nézve, hogy az ő maga vagy családja személyes életébe történő jogtalan – fizikai vagy az információk közlésével megvalósuló – beavatkozással szemben védve legyen.[14]

1.2. A magánszféra védelmének megjelenési formái

A magánélet és ezen belül a személyiségi jogok megsértése meglehetősen változatos formában fordulhat elő az életben. E széles körön belül az alábbi négy meghatározó csoportképző elemet lehet kiemelni:

---

[8] The Rachel Affaire. Judgement of June 16, 1858, Trib. Pr. Inst. De la Seine, 1858 D.P. III. 62. Ld. JEANNE M. HAUCH: *Protecting Private Facts in France*: The Warren and Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

[9] SAMUEL WARREN and LOUIS BRANDIES: „The right to privacy", *Harvard Law Review* 4, 1890 pp. 193-220.

[10] The Australian Privacy Charter, published by the Australian Privacy Charter Group, Law School, University of New South Wales, Sydney, 1994

[11] ALAN F. WESTIN: *Privacy and Freedom*, Atheneum, New York p. 7.

[12] Privacy as an Aspect of Human Dignity, [1964] 39 New York U.L.R. 962 at 971.

[13] Privacy and the Limits of Law, [1980] 89 Yale L.J. 421, at 428.

[14] Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, p. 7.

1. Az adatok védelme. Ide elsősorban a személyes adatok gyűjtésére és feldolgozására vonatkozó előírások és magatartások tartoznak (pl. banki információk, egészségügyi információ stb.). Ebben a dolgozatban leginkább erről a csoportról lesz szó.

2. Az emberi test védelme. Itt elsősorban fizikai értelemben az ember testére, szervezetére irányuló, vagy azt felhasználó vizsgálatokról, megfigyelésekről van szó. (pl. drog teszt, motozás stb.)

3. A kommunikáció védelme. Ez alatt elsősorban a levéltitok, telefon, e-mail és egyéb kommunikációs technika megfigyelése és ellenőrzése tartozik.

4. A terület (hely) védelme. Itt alapvetően a munkahely, lakóhely és egyéb az egyén tartózkodási helyének a tiszteletben tartásáról van szó.

A magánszféra védelmének modelljei: A magánszféra védelmének jelenleg is számos domináns modellje létezik. Néhány országban ezek közül a domináns modellek közül egyidejűleg többet is alkalmaznak. Az egyik ilyen modell az ún. *„szabályozási modell"* (regulatory modell). Ezt leginkább Európában, Ausztráliában, Hong-Kongban, Új Zélandon, Közép- és Kelet-Európában valamint Kanadában alkalmazzák. A modell lényege, hogy külön erre a célra intézményesített állami tisztviselők (pl. adatvédelmi biztos, ombudsman stb.) ösztönzik egy átfogó adatvédelmi normarendszer megvalósítását. A fenti közhivatalnokok ellenőrzik az elfogadott normák és a joggyakorlat adatvédelmi törvénnyel való egyezését, illetve nyomozást folytatnak az esetleges jogsértések felderítése érdekében. A fent nevezett hivatalnok felelős azért is, hogy ez a kérdéskör bekerüljön a közoktatásba. Hatáskörükbe tartozik az adatvédelemmel és adatáttovábbítással kapcsolatos nemzetközi kapcsolatok alakítása. Ez a modell minden olyan ország számára mintául szolgál, ahol a magánszféra védelméről (ezen belül is az adatvédelemről) külön törvényt alkottak. Ez a modell Európában is széles körben elfogadott, mivel jól segíti az EU adatvédelmi harmonizációs elképzeléseit. Ugyanakkor az is megfigyelhető, hogy ezen személyek, illetve szervek hatásköre és hatalma országonként is jelentős eltéréseket mutat és sok jelentés arról tanúskodik, hogy ezeknek a felelős személyeknek (intézményeknek) nincs elég forrásuk ahhoz, hogy megfelelőképpen érvényre tudják juttatni a magánszférával, illetve az adatvédelemmel foglalkozó jogi normák érvényesülését.

Második típusú modell: Néhány országban – pl. az USA-ban – nem egységes, hanem szektorális (sectoral laws) jellegű adatvédelmi szabályozást fogadtak el. Például külön szabályozás vonatkozik a videó kölcsönzők felvételeire, illetve a finanszírozási jellegű személyiségi jogok védelmére. Az ilyen rendszerben a jogok kikényszerítésének bonyolult mechanizmusa alakult ki. Az ilyen típusú szabályozás legnagyobb hátránya, hogy minden egyes új technológia bevezetése új jogi szabályozás megalkotását feltételezi. A gyakorlatban ez rendszerint úgy nyilvánul meg, hogy a jogalkotó jelentős mértékben lemarad a technológiai fejlődés mögött. Más országokban arra törekszenek, hogy ezek a szektorális jellegű jogi normák minél átfogóbban szabályozzák le a magánszféra és az adatvédelem kérdéskörét, ugyanakkor lehetőséget adjanak arra, hogy egyes speciális (pl. rendőrségi adatok stb.) vagy nagy érdeklődésre számot tartó kérdésben (pl. vásárlói hitelnyilvántartás stb.) még ennél is részletesebb szabályokat alkothatnak.

Más megközelítésben a magánélet és a személyiségi jogok védelmének további jellegzetes felfogásai különböztethetők meg. Az egyik legjobban megragadható eltérés az USA-beli kontra európai jogi felfogásban figyelhető meg. Az USA-ban nincs szövetségi szintű szabályozás e témakörben. Hosszú és intenzív vita alakult ki, hogy vajon a ma-

gánszféra védelme az alkotmányos vagy magánjogi kérdés-e. Ennek egy konkrétabb vetülete az idők folyamán kialakult két megközelítési mód: *a)* emberi jogi megközelítés: a személyiségi jogok védelme emberi jogi kérdés (human rights thinking) (ez az uralkodó felfogás az európai államokban, így például az EU adatvédelmi irányelve is ezt tükrözi) vagy *b)* tulajdonjogi szemlélet. Ez utóbbi felfogás értelmében a magánszférába történő beavatkozás mértéke a felek megegyezésének és/vagy pénzzel kifejezhető kompenzációjának a tárgya lehet. Természetesen a felek kölcsönös megegyezésén alapuló megállapodása az európai gondolkodástól sem idegen.

További jellemző rendszertani vonás, hogy az állami normatív szabályozást jelentős mértékben befolyásolják ágazati hatások (sector approach), továbbá nagyon gyakran a diszkriminációs szabályok közé beágyazva találjuk meg őket.[15]

2. A magánszféra sérthetetlenségéhez való jog megjelenése és védelme a nemzetközi dokumentumokban és a belső jogban

2.1. Nemzetközi szintű normák

1. Univerzális normák: A modern értelemben vett magánszféra védelmére vonatkozó szabályozás a nemzetközi dokumentumokban az Emberi Jogok Egyetemes Nyilatkozatában (1948) jelent meg először. Ez a norma különösen a területi és a kommunikációs magánszférát védte. A Nyilatkozat 12. Cikkelye kimondja, hogy „Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez."

Számos más nemzetközi emberi jogi egyezmény értelmezte és deklarálta a magánszféra védelmét, mint elidegeníthetetlen emberi jogot. Például a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya,[16] a Migráns Munkavállalókra vonatkozó ENSZ Egyezmény[17] és a Gyermekek Védelmére vonatkozó ENSZ Egyezmény.[18]

E helyen meg kell említeni az nemzetközi szinten megalkotott ún. „puha jogi" szabályokat is. Az a tapasztalat, hogy a magánszféra védelmét szolgáló belső jogi normák megalkotásakor nagyon gyakran visszanyúlnak az előzőekben említett nemzetközi jogi normákhoz, illetve a nemzetközi „puha jog" (pl. ILO Code of Practice on the protection of workers' personal data stb.) forrásaihoz. Például a finn „A munkavégzéssel kapcsolatos magánéleti kérdések védelméről" rendelkező törvény preambulumában is utal az ILO gyakorlati kódexére.[19]

Az adatvédelmet is meg lehet valósítani – legalábbis elméletben – az önszabályozás (self-regulation) különböző formáin keresztül. Ez leginkább a munkahelyi viselkedési kódexekben (code of practice) ölt testet. Ezek a törekvések a gyakorlatban nem váltották be a hozzá fűzött reményeket, ugyanis kevés, illetve egyáltalán nincs bizonyíték arra nézve, hogy ezek a kódexek rendszeresen betöltötték az eredeti rendeltetésüket. A leg-

[15] ANDERS VON KOSKULL, 2002, pp. 342–343.
[16] International Covenant on Civil and Political Rights (http://www.hrweb.org/legal/cpr.html
[17] A/RES/45/158 25 February 1991, Article 14.
[18] UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.
[19] ANDERS VON KOSKULL, 2002, pp. 342–343.

nagyobb probléma az adekvátságukkal és a kikényszerűsíthetőségükkel van. Nagyon sok országban az ún. a munkahelyi kódexek gyenge védelmet jelentenek a munkavállalóknak és hiányzik a kikényszeríthetőségük.

2. Regionális szintű normák: Az univerzális szinten elfogadott normákat rendszerint regionális szinten elfogadott normák segítségével hajtják végre, illetve finomítják. Az Emberi Jogok védelméről és a Fundamentális Szabadságjogokról Rendelkező Egyezmény[20] (1950) 8. Cikkelye a következőt mondja ki: „Mindenkinek joga van ahhoz, hogy tiszteletben tartsák a saját és családja privát életét, a lakását és a levelezését." Az állami szerveknek sem lehet felhatalmazásuk, hogy ezt a jogot megsértsék, kivéve ha erre jogszabályi felhatalmazás alapján a demokratikus társadalom működési rendje miatt nemzet- illetve közbiztonsági okból vagy az adott társadalom gazdasági jóléte, a társadalmi rend megőrzése, bűnmegelőzés, az erkölcsi rend védelme, illetve mások jogainak és szabadságának megőrzése miatt szükséges.

Az Európai Emberi Jogi Bizottság által alkotott Egyezmény (Convention created the European Comission of Human Rights) és az Európai Emberi Jogi Bíróság (European Court of Human Rights) abból a célból született, hogy az univerzális normák végrehajtását elősegítse. Az eddigi tapasztalatok azt mutatják, hogy a fenti regionális normák az univerzális egyezményekben foglalt jogokat a jogvédelmet illetően kiterjesztően, míg a korlátozásokat szűkítően értelmezik.[21]

Az Emberi Jogok Európai Egyezménye (The European Convention of Human Rights). Azokban az országokban, ahol ratifikálták ezt az egyezményt, ott a belső jog részévé vált, vagyis mindenkire nézve kötelező lesz. Az Egyezmény 8.1. cikkelye kimondja, hogy „Mindenkit megillet az a jog, hogy tartsák tiszteletben a saját és családja életét, lakását és levelezését."

Témánk szempontjából érdekes a Francia Legfelsőbb Bíróság ítélete. A Bíróság az Emberi Jogok Európai Egyezményének 8. cikkelyére alapozva arra az álláspontra helyezkedett, hogy minden embernek nemcsak magánemberként, hanem munkavállalóként is joga van ahhoz, hogy a munkaideje alatt és munkavégzés közben is tiszteletben tartsák életének a privát vonatkozású részeit.[22] Különösen vonatkozik ez a munkavállaló levelezésére. Az Egyezmény 8. cikkelye több szempontból is figyelemre méltó: egyrészt, a cikkely rendelkezik az ún. horizontális hatásról (horizontal effect); másrészt, a cikkely közvetlenül a munkahelyeken is alkalmazható, amiből az következik, hogy direktben képes csökkenteni alapvető munkáltatói előjogokat.[23]

Az Európai Emberi Jogi Bíróság (European Court of Human Rights) is kiterjesztően értelmezte az Emberi Jogok védelméről és a Fundamentális Szabadságjogokról Rendelkező Egyezmény 8. Cikelyét, amikor már nem kizárólag az állami, hanem a magánszemélyek általi beavatkozást is jogellenesnek minősítette.

„Számos angol és francia szerző nézőpontja szerint a magánszférához való jog megegyezik a „privát élethez" való joggal. Az élethez való jog (right to live) – az egyén által meghatározott mértékig – védi a személyt a külső beavatkozástól a nyilvánosságtól. A Bizottság álláspontja szerint a magánélet tiszteletéhez való jog nem fejeződik be a fent

[20] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 4 XI. 1950. http://www. Coe.fr/eng/legaltxt/5e.htm

[21] NADINE STROSSEN: *Recent US and Intl. Judicial Protection of Individual Rights: A Comparative Legal Process Analisys and Proposed Synthesis.* 41 Hastings L.J. 805 (1990).

[22] Cour de Cassation, arret No. 4164.

[23] ANDERS VON KOSKULL, 2002, pp.339–342.

meghatározott határnál, hanem – bizonyos fokig – magában foglalja más természetes személyekkel való kapcsolatteremtéshez való jogot, különösen akkor, ha ez az illető személy saját személyiségének a kialakulását és fejlődését segíti elő."[24]

A magánszférához való jog fogalmát az Amerikai Emberi Jogi Egyezmény (American Convention on Human Rights) 11. Cikkelye az Egyetemes Nyilatkozattal (Universal Declaration)[25] hasonló módon határozza meg. Az Amerikai Államok Szervezete (OAS) 1965-ben hirdette ki az Ember Jogairól és Kötelezettségeiről szóló Amerikai Egyezményt (American Declaration of the Rights and Duties of Man), amely számos emberi jog mellett a magánszféra jogi védelmét is magában foglalta.[26] A Deklarációt követően az Inter-Amerikai Emberi Jogi Bíróság (Inter-American Court of Human Rights) döntéseiben is megjelent és fokozatosan teret nyert a magánszféra jogi védelme.[27]

2.2. A magánszféra védelmének megjelenése a belső jogrendszerben

2.2.1. Alkotmányos szintű védelem

A legtöbb modern állam alkotmányában – direkt vagy indirekt formában – rögzítésre kerül a magánszféra jogi védelme. Néhány ország alkotmánya – pl. USA, Írország, India – még mindig nem szabályozza külön a magánszféra jogi védelmét. Ezekben az országokban a magánszféra védelmére vonatkozó szabályokat más jogi normák tartalmazzák. Például nemzetközi szerződések ratifikálásával [pl. Polgári és Politikai Jogok Egyezségokmánya (Convenant on Civil and Political Rights), vagy az Emberi Jogok Európai Konvenciója (European Convention on Human Rights)] kerülnek be a jogrendszerbe a szükséges szabályok. Ettől eltérően néhány államban – például Dánia[28] – a magánszféra védelmére nem vonatkoznak alkotmányos szabályok, de e helyett az emberi méltóság (human dignity) védelme kerül az alkotmány szövegébe.[29]

Az emberi jogok alkotmányos megjelenésével kapcsolatban szólnunk kell a magánszféra védelmének vertikális és horizontális dimenziójáról. Történelmileg az alkotmányokban megjelenő alapvető emberi jogok az állampolgárokat védték a közhatalommal szemben. A szakirodalomban ezt nevezik az emberi jogok vertikális dimenziójának. A történelmi fejlődés során – országonként eltérő formában és mértékben – az alapvető emberi jogok védelme tovább bővült a magánszemélyek (magánszervezetek) közötti

[24] X v. Iceland , 5 Eur. Commin H.R. 86.87 (1976).

[25] Signed Nov. 22, 1969, entered into force July 18, 1978, O.A.S. Treaty Series No. 36, at 1, O.A.S. Off. Rec. OEA/Ser. L/V/II. 23 dec rev. 2.

[26] O.A.S. Res XXX, adopted by the 9th Conference of American States, 1948 OEA/Ser/. L./V/I.4 Rev (1965).

[27] Privacy and Human Rights, An international Survey of Privacy Laws and Practice. pp. 5–7.

[28] Dániában az adatvédelmi szabályozás abból a feltételezésbol indul ki, hogy minden egyes embernek van személyes autonómiája (personal autonomy). Abban az esetben, ha az egyén valamilyen oknál fogva gyenge (kiszolgáltatott) pozícióban van a közhatalom vagy a privát szektor vonatkozásában, akkor ez az autonómia megsérül. Az állam, a munkáltató vagy másik személy (esetleg munkatárs) olyan mértékben avatkozik be a közöttük fennálló viszonyba, hogy az már hátrányosan érinti az egyén autonómiáját. Ezért ilyenkor a jog egyik legfontosabb szerepe az, hogy korlátozza a közszféra és a munkáltató polgárral (munkavállalóval) szembeni cselekvési szabadságát. (KRISTIANSEN, JENS: *Danish Report, Protection of workers personal data in the European Union. The Case of surveillance and monitoring.* Paper Seminar Lueven 2001 p. 2.)

[29] Blume, Peter ed.: Introduction, *Nordic Data Protection* Copenhagen 2001, pp. 1–9

kapcsolatokra is. Ezt nevezzük horizontális kapcsolatnak (dimenziónak). Az emberi jogok horizontális dimenziója további számos síkot foglal magában. Például az is egy horizontális hatás, amikor az állam kötelezettségének érzi, hogy az esetleges jogsértésekkel kapcsolatban védje az állampolgárok alkotmányban rögzített emberi jogait és ilyen helyzetre vonatozó szankciókat dolgoz ki.

A horizontális kapcsolatrendszer egy másik megjelenési sajátossága az ún. közvetlen hatás (direkt effect). Amennyiben a közvetlen hatás elismert, akkor az azt jelenti, hogy az alkotmányban rögzített szabály közvetlenül alkalmazható a magánszemélyek közötti viszonyokban. Miután az országok többségében nagyon sok jogszabály van hatályban, rendszerint nagyon ritkán kerül arra sor, hogy közvetlenül alkotmányos rendelkezéseket alkalmazzanak a magánszféra alanyai között. Egy másik sajátosság, amiért ezt ritkán alkalmazzák, az az, hogy az alkotmányos rendelkezések túlnyomó többsége általában nem tartalmaz szankciókat az esetleges megsértésük esetére.

2.2.2. A munkavállalók privát szféráját védő munkajogi szabályozás alapvető jellemzői

A. A személyiségi jogok védelmének konkrét megjelenési formái a munka világában

A technológiai fejlődés lehetővé teszi, hogy a munkavállalókról egyre több és egyre részletesebb információt lehessen összegyűjteni, elemezni és értékelni. Az információgyűjtés a közvetlen munkavégzés során tanúsított magatartáson túl kiterjed a munkavállaló személyiségére, viselkedésére, a munkatársaival, illetve külső harmadik személyekkel kialakított kapcsolatára.

Az új technikák lehetővé teszik a munkavállalók tevékenységének folyamatos megfigyelését és ellenőrzését. Bizonyos esetekben titkos módszerekkel gyűjtik össze és a munkavállaló által nem ismert célra használják fel az információkat.

A munkahelyeken az információs társadalom számos eszközét (pl. számítógép, telekommunikációs és audiovizuális eszközök, stb.) alkalmazzák arra, hogy a munkavállalókról adatokat gyűjtsenek. Az alábbiakban a leggyakrabban alkalmazott módszereket tárgyaljuk:

a) Az interaktív kitűző (active badge) rendszer.[30] Az egész szerkezet néhány centiméter átmérőjű. Tartalmaz egy mikroprocesszort és egy infravörös kommunikációs rendszert, amely segítségével meghatározható a viselőjének pontos helyzete és kapcsolatot tud teremteni más eszközökkel (pl. fogadja az automata telefon által átküldött hívásokat, vagy elektronikus úton ad felhatalmazást valamely épületbe vagy terembe történő belépésre, stb). Ez a rendszer számos problémát okozhat a viselőjének, ha illetéktelen kezekbe kerül. Például rákötheto egy központi számítógépre, amely automatikusan rögzíti a munkakezdést és a munka befejezését. A munkahelyen belül képesek követni és rögzíteni a munkavállaló mozgását (könyvtár, WC, más épület stb) és azt is, hogy mennyi időt töltött az egyes helyeken.

Az olyan interaktív kitűző rendszer, amely valamilyen biometrikus azonosítási elven (pl. ujjlenyomat) magában hordozza a személyiségi jogok megsértésének a lehetőségét azáltal, hogy ezeket a személyre szóló információkat összegyűjtik, illetve a munkaviszony megszűnését követően is megtartják.

[30] Nevezik még „tabs"-nak vagy „network location devices" (hálózati helymeghatározó eszköz).

b) A számítógép alapú rendszer (computer-based system). Ez a rendszer a munkáltatót informálja a munkavégzés ritmusáról (pl. mennyi ideig tart egy munkafázis, vagy mennyi feladatot sikerült elvégezni egy adott egységnyi időtartam alatt, stb). A rendszer alapulhat a végzett fontosabb munkafázisok vagy az ejtett hibák, vagy a munkaközi megszakítások gyakoriságának és tartamának számlálásán. A számítógépes ellenőrzési rendszer nemcsak a közvetlen megfigyelésre alkalmas, hanem elvégezhető segítségével többféle távoli kontroll. Például egy rendszeren belül megnézhető, hogy a munkavállaló milyen file-okkal dolgozott a kérdéses időszakban, vagy nyomon követhető az e-mail forgalma és azok tartalma, stb. Ez a számítógépes megfigyelő rendszer elsődleges rendeltetését tekintve a termelékenység és a hatékonyság növelését hivatott elősegíteni. Ugyanakkor ez a rendszer a munkavállaló folyamatos megfigyelésén alapul, ami által több esetben esély van arra, hogy megsértsék a munkavállaló személyiségi jogait.

c) Video-kamera. Elsősorban biztonsági okokból helyeznek el kamerákat a munkahely bejáratánál (pl. bank) vagy egyéb olyan helyiségekben, ahol biztonsági okból kívánatos a kamera állandó jelenléte. Ilyen esetek például, amikor a munkavállaló viselkedését, habitusát, kollégáival vagy ügyfelekkel való kapcsolatteremtését kell folyamatosan szemmel tartani. Az esetek többségében ezeket a felvételeket rögzítik, illetve a munkáltató bizonyos ideig eltárolja.

d) A telefonbeszélgetést regisztráló rendszer (telephon-call accounting system). A rendszer regisztrálja a kimenő és a bejövő hívásokat, azok időtartamát a hívott fél telefonszámát és az üzleti, illetve privát beszélgetések tartalmát. Ez a rendszer nem kizárólag csak a telefonos kommunikáció megfigyelésére alkalmazható, hanem például az e-mail forgalmat is képes regisztrálni.

e) A számítógépes, illetve hálózati vagy szatelit alapú kommunikációs eszközök segítségével a munkavállalók *munkahelyen kívüli – pl. lakásán, autójában stb. – mozgása és tevékenysége* is kontrollálható. Ezt nevezzük ún. média-térnek (media-space). Ez nem más, mint egy számítógép által vezérelt audió-viziós hálózat, amely egy adott épületen belül vagy földrajzi térségben különböző helyeken munkát végző csoportok tagjai közötti kommunikációt és együttműködést segíti elő. Ugyanez figyelhető meg a munkahelyeken belül is. Minden irodát, műhelyt behálózó audió-videós rendszerek, számítógépes hálózatok működnek. Ezek egy sor vonatkozásban elősegítik a jobb és eredményesebb munkaszervezést (mindig lehet látni, hogy ki szabad, éppen hol tart egy adott folyamat, vagy nem kell összehívni az egyes vezetőket, hanem elektronikus úton keresztül lehet eljuttatni hozzájuk a feladatokat stb. Ugyanakkor ez a nagyfokú behálózottsága a munkahelyeknek megnöveli annak az esélyét, hogy a munkavállalók személyiségi jogai megsérülnek. Ezek a rendszerek gyakorlatilag észrevétlenül és akaratlanul (nem megfigyelési szándékkal szerelik fel őket) végeznek adat- és információgyűjtést a munkavállalókról. Az ilyen típusú elektronikus rendszerek alkalmazása egy sor etikai és jogi kérdést vet fel.

f) A telemunka elterjedése azzal a következménnyel jár, hogy a *magánszféra elveszíti privát jellegét.* Mivel a munkáltató és a munkavállaló, illetve a munkatársak nem egy helyen vannak- a közöttük lévő fizikai távolság miatt egyre nagyobb a kísértés, hogy különféle kontroll-eszközöket iktassanak be a kapcsolatba, amely eredményeként a munkáltató mintegy távirányítással is képes ellenőrizni a munkavállalóit. A telemunka keretei között a korábban kizárólagosan privát jelleggel használt lakóhely egyidejűleg

testesíti meg a privát szférát és a munkahelyet. A személy 24 óráján keresztül munkavállaló is és magánszemély is. A két pozíció nem választható el egymástól. A munkavégző személyek egymással való kapcsolata és viszonyrendszere is jelentősen megváltozik ebben az új rendszerben. A telekommunikációs eszközök gazdag tárháza lehetővé teszi, hogy a munkavállaló folyamatosan a munkavégzési folyamat részese lesz, még akkor is, ha formálisan nem is tartózkodik a munkahelyén. Ez a kapcsolatrendszer potenciálisan magában hordozza a munkavállalók személyiségi jogainak a megsértését. A telemunka során egy sor olyan információ birtokába jut vagy juthat a munkáltató, amelynek semmilyen kapcsolata nincs a munkavállalói statussal.

B. A magánszféra védelme a munkaviszony létesítésekor

Általánosan elterjedt nézet, hogy a munkaviszony immanens részeként a munkáltatót megilleti a munkavállalók megfigyelésének a joga. A munkaviszony létesítésének időszakában ezt a megközelítést már csak formai okok miatt sem lehet alkalmazni, hiszen ekkor még nem áll fenn a felek között munkajogviszony. Egyik oldalról azt állíthatjuk, hogy ebben a fázisban még formálisan egyenrangú autonóm felek interakciójáról van szó, amely végállomását tekintve a munkaszerződésbe, vagy az „elválásba" torkollik, vagyis nem jön létre munkaviszony. Ugyanakkor az esetek túlnyomó részében az is nyilvánvaló, hogy ténylegesen eltérő pozícióban lévő személyek alakuló viszonyáról van itt szó. Ha tovább gondoljuk a két fél rendszerint egyenlőtlen kapcsolatát, akkor az is nyilvánvalóvá válik, hogy a kiszolgáltatottabb helyzetben lévő munkavállalónak már a felvételi eljárás időszakában is szüksége van jogi védelemre. A leggyakoribb védelmi területek a következők: korrekt bánásmód, diszkrimináció tilalma, nemek közötti egyenlőség, a személyes adatok védelme, és nagyon sokszor a nem jogi normaként megjelenő „jó munkaerőpiaci magatartás elvei" (principle on good labour market practices).

Egy új munkaerő alkalmazásánál teljesen magától értetődő igény, hogy még az alkalmazás előtt a munkáltató szeretne alaposan tájékozódni a jelöltről. Ez pedig adatok begyűjtésével és feldolgozásával, elemzésével végezhető el a leginkább. Ebben a folyamatban a következő a lényegi és vizsgálandó kérdés: vajon a lefolytatott eljárás, vagy az alkalmazott módszer mennyiben felel meg az adatvédelmi törvény – vagy az EU-s irányelv – előírásainak. Abban az esetben, ha az eljárás teljes egészében megfelel a törvényben írottaknak, akkor ezt az eljárást – e vonatkozásban – elvileg jogszerűnek kell tekinteni.

E kérdés vizsgálatánál az igazi kérdés nem az, hogy a munkáltatónak van-e egyáltalán ilyen joga, hanem sokkal inkább az, hogy a munkáltatónak ez a saját maga számára „vindikált" jog – hogy megfigyelhesse, utasíthassa, vizsgálhassa a saját munkavállalóit – milyen mélységig illeti meg őt. Ebben a körben a legfontosabb kérdés a felek jogainak és rendszerint eltérő érdekeinek az egyensúlyba hozása. A kezdetekben a munkáltató társadalmi pozíciója és a munkavégzés felügyeletéből, ellenőrzéséből származó „kiváltságok" messzire tolták ki a munkáltatói jogosultságok határát. Később, a munkajog védelmi szerepének bővülésével és az ún. eljogiasodási folyamattal (juridification)[31] egyidejűleg elindult a munkáltatóhoz való lassú felzárkózás időszaka. Ez a fejlődés

[31] Az eljogiasodás folyamata a következő: a felek között felmerülő konfliktusok egyre nagyobb számban nyer jogi megfogalmazást és a konfliktusok rendezésére jogilag szabályozott eljárási rend alakul ki.

nagyon sok tényezőre vezethető vissza, de közülük is kiemelkedik a szakszervezet munkáltatóval szemben tanúsított konfrontációs, illetve bizonyos helyzetekben kooperatív magatartása. A skandináv államokban – ahol nagyon erős a munkavállalói érdekvédelem – a munkaügyi kapcsolatok alakításának két alapvető elve és értéke: *a)* a megegyezés és *b)* a kompromisszumkészség. Ugyanakkor meg kell jegyeznünk, hogy Finnországban – köszönhetően a legutóbb elfogadott munkavállalói magánszféra törvénynek – a szociális partnerek szerepe a munkavállalók személyiségi jogainak a védelme területén visszafogottabb, mint a többi skandináv államban. A jelentős szakszervezeti szervettség okán egy további speciális kérdés is felmerül a skandináv államokban: milyen személyiségi jogi védelem illeti meg a munkavállalót a szakszervezeti tagsággal kapcsolatban (tag vagy nem tag). Az EU-s adatvédelmi irányelv erős egységesítő szándékkal kívánjaközös szabályok közé szorítani az európai országok személyiségi jogok, illetve a magánélet védelmét szabályozó normáit.

C. A munkáltatói megfigyelés, mint a munkaviszony természetes velejárója

Mint ahogy azt már a fentiekben jeleztük, a legtöbb írott munkajoggal rendelkező országban a munkáltatónak joga van ahhoz, hogy irányítsa, utasítsa és ellenőrizze a munkavállalóit. Ezek a munkajogviszony alapvető összetevői. Ezek a jogosítványok egyidejűleg a felek közötti egyenlőtlen piaci pozíciókat is érzékeltetik. Sok szerző véleménye szerint ennek a hátterében komplex társadalmi és gazdasági okok állnak. Talán ez lehet az egyik oka annak, hogy ezen munkáltatói kiváltságok jogi alapjának vizsgálata csak nagyon ritkán kerül a viták középpontjába. Ez alól a széles körben elterjedt felfogástól eltér a finn Martti Kairinen professzor véleménye, aki azt állítja, hogy a munkáltató azért viselkedhet így, mert a munkaviszony jogi alapjában implicite benne van a munkavállaló beleegyezése (implicit consent from the employee). Ezen elmélet szerint a beleegyezés egyidejűleg magában foglalja a magatartási limitek meghatározását is.[32]

Ugyanakkor, a skandináv esetjogban megtalálhatók azok az elvek, illetve limitek, amelyek segítenek meghatározni, illetve korlátozni a munkáltató megfigyelési és ellenőrzési jogát. Ezeket és a munkavállalókat védő egyéb elvekkel összhangban kell értelmezni. Például a svéd adatvédelmi biztos álláspontja szerint amikor a munkáltató a munkavállalóira vonatkozó adatokat kezel, akkor ezt a jogát (megfigyelés és ellenőrzés) nem gyakorolhatja eseti (random) jelleggel, illetve jogellenes módon, továbbá nem cselekedhet a jó munkaerőpiaci standardokkal ellentétesen.[33]

A fenti folyamatot nagyvonalakban a következőkben foglalhatjuk össze: A munkáltatók tiszteletben tartották a munkavállalók magánszférához fűződő jogait (privacy) és méltóságát (dignity). A munkáltatói ellenőrzés és az utasítási jog keretét megfelelő módon és objektív alapon alakították ki, következésképpen az nem volt eltúlzott és a jó munkaerőpiaci standardoknak is megfelelt. A munkáltató jogát alapvetően két tényező befolyásolja: *a)* a megfigyelés (ellenőrzés) indokoltsága és a másik oldalon *b)* a munkavállalónak okozott kár, illetve kellemetlenség mértéke. E két tényező arányosításának

[32] KAIRINEN, MARTTI: *Direktio-oikeuden kasitteesta.* Juhlajulkaisu Antti Johannes Suviranta 1923 30/11 1983. Työoikeudellisen yhdistyksen vuosiíikirja. Helsinki 1983 in. ANDERS VON KOSKULL: *Employment Privacy Protection* – Scandinavian Comparative Perspectives; in. Stability and Change in Nordic Labour Law, ed. Peter Wahlgren, Scandinavian Studies in Law. Volume 43, Stockholm Institute for Scandinavian Law, Stockholm 2002, pp.342–343.

[33] Personuppgifter 2001, p. 13.

eredményeként alakítható ki a munkáltató magatartásának a kerete. Ezeket nagyon gyakran kollektív szerződésben, illetve a munkaszerződésben is rögzítik. Ebből következően fontos megjegyezni, hogy abban az esetben, ha a munkáltató megsérti ezeket a közösen felállított szabályokat, akkor ezzel a magatartásával szerződésszegést valósít meg. Például Finnországban az írott jog nem rendelkezik arról, hogy a munkáltató milyen keretek között gyakorolhatja az ellenőrzés és a megfigyelés jogát. Az esetjog sem tartalmaz kimerítő iránymutatást, ugyanakkor a szomszédos skandináv országok gyakorlatát (kollektív megállapodások) veszi alapul. Ugyanakkor érdemes megjegyezni, hogy a munkáltató e vonatkozású jogainak korlátozását tekintve a kollektív szerződésekben és azok bírósági értelmezésében található fejlődés és eredmény eltérést mutat.

D. A munkahelyi nem jogi eszközök szerepe a magánszféra védelmében

A skandináv országokban a munkáltató ellenőrzési jogának korlátozásával kapcsolatban nagyon gyakran felmerül a kollektív szerződések szerepe. Másképpen fogalmazva, ezekben az országokban a kollektív szerződési rendszer történeti fejlődése kéz a kézben jár a munkáltató ellenőrzési és megfigyeléshez való jogának az alakulásával. A munkáltatók nagy érdeklődést mutattak az iránt a megoldás iránt, hogy a kollektív szerződésekbe is belekerüljenek ezek a korlátok és elvek, továbbá az iránt, hogy erre a kérdéskörre is kiterjedjen az ún. békekötelem (peace obligation). A fejlődés kezdete visszanyúlik egészen a XIX. század utolsó éveire. A munkáltatók e vonatkozású jogai a kollektív megállapodások rendszerében a kollektív szerződések és az esetjog közötti ún. „ping-pong" mechanizmus eredményeként alakult ki.

Az ötvenes évek elején a norvég Legfelsőbb Bíróság számos jelentős – a korábbi jogfelfogástól eltérő – ítéletet hozott. Ezeknek a legfontosabb sajátossága az volt, hogy a bíróság az ítéletét ún. nem jogi normában szereplő privacy elvekre (non-statutory principle of privacy) alapozta.[34] Az a tény, hogy egyébként Norvégiában is az ún. alkotott jogi normák (statutory law) a meghatározók még inkább figyelemreméltóbbá teszik az ítéleteket. Az egyik eset egy munkavállaló kamerával történő megfigyeléséről szólt.A kamerák felállítására azért került sor, mert a munkáltató azt gyanította, hogy a munkavállalója sikkaszt. A Legfelsőbb Bíróság – nem államilag alkotott normára alapozva – meghozta azt az ítéletét, amelyben kimondta, hogy a munkáltatónak nem volt joga ahhoz, hogy az esetben szereplő módon megfigyelje a munkavállalót, következésképpen a videoszalagot nem lehet bizonyítékként felhasználni a sikkasztás miatt indított bírósági eljárásban.[35]

2.2.3. Büntetőjogi szabályozás

A személyiségi jogok büntetőjogi védelmével csak említés szintjén foglalkozunk. Több ország büntetőjogában megjelenik a technikai eszközökkel végzett megfigyelés meghatározása. Például a finn Btk-ban[36] az e-mail forgalom megfigyelése a kommunikációs titoktartás megsértésének minősül.[37]

[34] Retstidende 1952, 1217, RT 1967, 1373 és 1977, 1073, feldolgozva Bing 1994, pp. 24-26, és Jakhelln 2000, 1172 ff. által.

[35] Retstidende 1991, 616.

[36] Finn Btk 38:3.

[37] ANDERS VON KOSKULL, 2002, pp.346.

3. Adatvédelem

3.1. Az adatvédelem válasza a modern kor kihívásaira

Alapvetően három olyan fő ok található, amely arra ösztönzi az államokat, hogy a magánszférára és az adatvédelemre vonatkozó átfogó jogalkotás hozzanak létre.

a) A múltban történt jogtalanságok orvoslása. Sok országban – különösen a Közép-Kelet-Európában, Dél-Amerikában, Dél-Afrikában – az elmúlt diktatórikus időszakban elkövetett magánszféra jogsértések orvoslását kívánják megvalósítani az újonnan alkotott jogszabályokkal.

b) Az elektronikus kereskedelem támogatása. Sok ország – közülük is kiemelésre érdemesek az ázsiai országok és Kanada – már elfogadott, vagy elfogadás alatt vannak olyan jogi normák, amelyek célja az elektronikus kereskedelem megvalósításának elősegítése. Ezekben az országokban felismerték, hogy állampolgáraikat aggodalommal tölti el az a tudat, hogy az elektronikus kereskedelmen keresztül világszerte ismertté válnak vagy válhatnak a személyes adataik. A magánszféra védelmét szolgáló jogszabályok egy olyan jogalkotási csomag részeként kerültek elfogadásra, amely elsődleges célja, hogy uniformizált jogi szabályozást állítson fel az elektronikus kereskedelemben résztvevők számára.

c) Annak a biztosítása, hogy a nem tagállam államok jogi normái konzisztens egységbe kerüljenek a pán-európai jogi normákkal. A legtöbb kelet- és közép-európai országban az Európa Tanács idézett egyezményével és az EU vonatkozó jogi normáival (adatvédelmi irányelv) harmonizáló jogszabályokat fogadnak el. Más régiókban – például Kanadában – annak érdekében fogadnak el új jogszabályokat, hogy kizárják az EU vonatkozó adatvédelmi irányelvének érvényesülését a kereskedelmi viszonyaikban.[38]

Mindezeken túlmenően a technológia fejlődésének ütemével a magánszféra megsértésének a lehetősége egyenes arányban növekszik. Kimutatható néhány trend, amely a magánszféra megsértése terén tapasztalható: *a)* A *globalizáció* eltöröl minden földrajzi akadályt az információk szabad áramlása elől. A globális technológia talán egyik legismertebb vívmánya az Internet. *b)* A *konvergencia* az információs rendszerek közötti technikai különbségek eltörlését jelenti. A modern információs rendszerek minden gond nélkül képesek egymással együttműködni és kapcsolatba lépni. *c) Multi-médiás* rendszerek működnek, amelyek segítségével könnyen lehet továbbítani az adatokat, illetve képeket stb. Például az írott formában rögzített szöveg scannelés után azonnal szerkesztett szövegként továbbítható, vagy egy fénykép, scannelést követően bármilyen virtuális formában tovább küldhető stb.

A fejlett országokban az információ és kommunikáció technológia területén a politikák konvergenciájának sebessége jelentősen megnőtt. A különböző megfigyelési technikák spektrumát tekintve – telefonlehallgatás, elektronikus személyes azonosító rendszerek, adatfelkutatás és összegyűjtés stb – a nyugati társadalmak jelentős előnyre tettek szert. A fejlődő országok kormányai ezeket a fejlett országokat tekintik mintának és tőlük kapják azokat a megfigyelési eszközöket, rendszereket, amelyeket ezt követően

[38] Privacy and Human Rights, An international Survey of Privacy Laws and Practice. pp. 1–2.

maguk is alkalmaznak. A kormányoknak és az állampolgároknak egyaránt hasznosak lehetnek az információs társdalom vívmányai. Ezek jelenlétét napjainkban mind a köz-, mind pedig a magánszférában megtalálhatjuk. A új, ún. „intelligens kártyák" (smart card) programok segítségével egy chip kártyán lehet szinte az összes releváns adatot lehet tárolni. Ez jelentős mértékben csökkentheti az ügyintézés idejét. Az Internet tömeges elterjedése forradalmi változásokat idézhet elő a közszférában (pl. elektronikus kormányzás bevezetése), de a magánszférában (pl. elektronikus aláírás, adatbázisok megléte stb.) is.

Ugyanakkor ezek a változások megfelelő merészséget kívánnak meg a felektől és újabb jogalkotást a jogalkotóktól. Az, hogy egy adott kormány képes-e kidolgozni az új jogi kereteket nagymértékben függ attól, hogy mennyire akarja és képes rajta tartani a kezét a globális digitális gazdaság ütőerén, továbbá attól, hogy mennyire képes felismerni a magánszféra védelmének a szükségességét.

Abban a korban élünk, amikor a technológiai fejlődés eredményeként mind az állami, mind pedig a magánszférában lehetővé válik az emberek tömeges méretű megfigyelése, rájuk vonatkozó adatok gyűjtése, elemzése stb. A magánszféra védelme ezért az individuális emberi jogok egyik meghatározó elemévé vált. Különböző nemzetközi felmérések készültek arra vonatkozóan, hogy milyen formában és mértékben sértik meg az egyes polgárok személyiségi jogait, illetve magánszféráját. Az is tapasztalható, hogy egyre több országban születnek a kérdést szabályozó jogi normák. A jogi aktivizálódás (jogalkotás és alkalmazás) mögött az egyik legfontosabb tényező, hogy az érintettek megértik, hogy a személyiségi jogok védelme egy olyan alapvető emberi jog, amelyet senkinek nincs joga megsérteni. A magánélet (privacy) jelentésének kifejtésénél olyan fogalmak kerülnek előtérbe, mint a méltóság (dignity), a szólásszabadság vagy az egyesülési szabadság stb. Ezek eredetüket tekintve elsősorban a különböző szintű és típusú nemzetközi normákban jelennek meg és az egyes államokba történő „beszivárgásukat" követően – rendszerint – alkotmányos védelemben részesülnek. A személyiségi jogok védelmét szolgáló jogalkotás szükségességét alapvetően a rohamos léptekben terjedő technológiai fejlődés motiválja. Míg korábban egy-egy személyes adat sorsát viszonylag könnyen nyomon követhette volna a polgár, addig napjainkban a nagy teljesítményű számítógépek világában az adatfeldolgozás, elemzés, továbbítás stb. – országhatárokat nem ismerve – pillanatok műve lehet. Napjainkban minden egyes állampolgárról számalan formában – egészségügy, közlekedés, munkavégzés, pénzügyi műveletek, turizmus stb. – kerülnek az információk összegyűjtésre és feldolgozásra. A nagy sebességű számítógépes hálózatok következtében az adatok globális szinten kerülnek felhasználásra. Senki nem tudhatja, hogy pontosan – direkt vagy indirekt formában – hol és milyen mennyiségű adatot gyűjtöttek róla. Ehhez társul a munka világában – elsősorban a menedzsment oldaláról – a mindent átható verseny és hatékonyság növelésének az igénye. Ennek az egyik egyenes következménye, hogy a munkáltató a munkaidő minden egyes pillanatában szeretné tudni, hogy mit csinál a dolgozója, hogy végzi a munkáját, milyen hatékonyságnöveléssel lehetne még tovább fokozni a teljesítményét, mennyi időt tölt pihenéssel, stb. Mindennek az ellenőrzésére egyre több és kifinomultabb eszközrendszer áll a munkáltató rendelkezésére.

Ugyanakkor, az is megállapítható, hogy a jogalkotás rendszerint nem képes lépést tartani ezzel az óriási léptékű fejlődéssel, következésképpen az alkalmatlan jogi védelem eredményeként a munkáltatók sok esetben olyan nem szabályozott területeken végzik a tevékenységüket, amely végső soron sérti a munkavállalók és környezetük érdekét és

jogait. A munkavállalók az esetek túlnyomó többségében sebezhetők és a munkáltató különféle vizsgálataival, adatgyűjtésével és elemzésével, nyílt vagy rejtett megfigyeléseivel, stb. szemben tehetetlenül állnak szemben.

A munkavállalók jogi védelmét szolgáló szabályozás „hezitálása" mögött – elsősorban Nagy-Britanniára igaz ez a kijelentés – az a tény áll, hogy a munkavégzés a munkáltató általi folyamatos nyomon követése a munkaviszony egyik immanens része. Ezért sokan azzal érvelnek, hogy a munkáltatónak joga van ahhoz, hogy különféle módszerek segítségével meggyőződjön arról, hogy a munkavállalója hogyan dolgozik. Ugyanakkor a munkavégzés körülményeinek változása (egyre több számítógéppel végzett munka, elektronikus megfigyelési rendszerek, nyilvántartás stb.) és ezzel egyidejűleg az IT technológia több, mint rohamos fejlődése a munkáltató ellenőrzési terét (megfigyelését) nagyon jelentős mértékben kiterjesztették. Álláspontjuk szerint ez a megfigyelés a munkavállalóra mindenkor és minden tevékenységére kiterjed. Például mini kamerák figyelik minden egyes lépést, elektronikus személykövetők figyelik minden mozdulatát a munkahelyen, a különböző telefonra szerelhető eszközök másodpercek alatt elemzik a telefonhívásait, a munkaviszony létesítésekor és azt követően folyamatosan különféle teszteket (pszichológiai teszt, intelligencia teszt, viselkedési teszt, teljesítményi teszt, szakmai elkötelezettséget mérő teszt, személyiségi teszt, a munkáltatóhoz fűződő lojalitásának az ellenőrzése stb.) kell megoldania. Ezen tesztek túlnyomó többségét elektronikus formában végzik el. Ebből az is következik, hogy minden egyes adat nyilvántartásra kerül és bármikor elővehető és felhasználható. Összefoglalva bátran állíthatjuk, hogy a mai világban a munkavállalók folyamatos megfigyelése és ellenőrzése a munkahelyi (munkavégzési) környezet egyik elválaszthatatlan részévé vált.

3.2. Az adatvédelemre vonatkozó regionális normák

A magánszféra átfogó védelmét megfogalmazó jogi szabályozás az 1960 és 70-es évektől kezdve erősödik fel. Ennek a hátterében elsősorban az információs technológiák (angol rövidítése: IT) elterjedése állt. A személyes adatok gyűjtésére és feldolgozására kialakított számítógépek, illetve hálózatok teljesítőképessége rohamosan nőtt. Ezzel párhuzamosan a felhasználók is egyre bonyolultabb elvárással léptek fel a számítógépes rendszerekkel szemben. Ezzel egyidejűleg a jogalkotás szintjén is megfogalmazódott a személyes adatok jogi védelmének a szükségessége. Ez elsősorban az adatok gyűjtésére és kezelésére terjedt ki. Sok ország alkotmányában is megjelentek ezek az új emberi jogok. Az e területen kialakult modern jogalkotás genezise a német Hesse tartományban (1970) elfogadott első adatvédelmi törvényre vezethető vissza. Ezt követte a svéd jogalkotás (1973), majd az USA (1974), Németország (1977) és Franciaország (1978).[39]

A fent említett korai, nemzeti jogszabályok két nagyon fontos nemzetközi jogi dokumentum megalkotására hatottak megtermékenyítőleg. Az egyik volt az Európa Tanács egyezménye [Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981)].[40] A másik dokumentum az OECD Iránymutatása volt [Guidelines Governing the Protection of Privacy and Transborder Date Flows of

[39] DAVID FLAHERTY: *Protecting Privacy in surveillance societies*. University of North Carolina Press, 1989.

[40] http://coe.fr/eng/legaltxt/108e.htm

Personal Data (1981)],[41] amely az elektronikus adatvédelemre és felhasználásra vonatkozó speciális szabályokat tartalmaz. Nagyon sok országban ezek a nemzetközi dokumentumok képezik a hazai adatvédelmi normák esszenciális alapját. Ezek a normák a személyhez fűződő információkat (personal information) adatoknak tekintik, amelyek a megszerzéstől a tároláson keresztül a felhasználásig jogi védelemben részesülnek. Ezen normák szabályozási logikájának sarkpontja, hogy az érintett személyek számára elérhetők és módosíthatók az összegyűjtött adatok. Az adatvédelemre vonatkozó normák alapjait tekintve azonos elvek és szabályozás mentén épülnek fel. Rendszerint csak a védelem fokában mutatkoznak eltérések. Az összes norma előírja a következő pontokat: *a)* az adatokat korrekt és jogszerű módon kell megszerezni; *b)* csak az eredeti célkitűzésben (előre meghatározott) cél(ok)ra lehet felhasználni; *c)* adekvát, releváns és az eredeti célkitűzést meg nem haladónak kell lennie és *d)* meg kell semmisíteni, miután az eredeti célkitűzésben szereplő feladatát betöltötte.

Ugyanakkor, ezen regionális szintű nemzetközi normák elfogadását követően ezek szolgáltak alapul az egyes államoknak. A saját belső jogi szabályozásuk kialakításakor elsősorban az OECD és az Európa Tanács, majd az EU által bemutatott modelleket vették alapul.

3.2.1. Az OECD adatvédelemre vonatkozó szabályozása: Az OECD Tanács ajánlása a magánélet védelmét és a személyes adatok határátlépő áramlását szabályozó irányelvekre

A határátlépő adatáramlással foglalkozó OECD program az 1969-ben kezdeményezett, a számítógépeknek az állami szektorbeli használatával foglalkozó tanulmányokból ered. Egy szakértő bizottság, az Adatbank Munkaközösség a magánélet különböző aspektusait elemezte és tanulmányozta, így például annak a digitális információkhoz, a közigazgatáshoz, a határátlépő adatáramláshoz és az általános politikai összefüggésekhez való kapcsolatában.

E munka eredményeként egy lehetséges nemzetközi cselekvési program megvalósítása érdekében egy sor irányelv kidolgozására került sor. Ezek az irányelvek elismerték, hogy

a) szükség van az országok közötti általános és folyamatos, zavartalan információáramlásra;
b) az országoknak jogos érdeke az olyan adatok továbbításának megelőzése, amelyek biztonságukat veszélyeztetik, vagy ellentétesek a közrendre és közszeméremre vonatkozó törvényeikkel, vagy sértik állampolgáraik jogait;
c) az információnak gazdasági értéke van, s az „adat-kereskedelemnek" is részesednie kell a védelemben a tisztességes verseny elfogadott szabályai alapján;
d) biztosítékokra van szükség az adatok magántulajdonának megsértésével és a személyes információkkal való visszaéléssel szemben, és
e) nagy jelentőséggel bír, hogy az országok elkötelezzék magukat a személyes információk védelmére vonatkozó alapvető elvek együttese, mint közös mag mellett.

[41] OECD, Guidelines Governing the Protection of Privacy and Transborder Date Flows of Personal Data, Paris, 1981.

1978 elején megalakult egy új ad hoc szakértőcsoport, a Határátlépő Adatáramlás és a Magánélet Védelme Szakértőcsoportja, az OECD keretében, amely azt az utasítást kapta, hogy dolgozzon ki irányelveket a határátlépő adatforgalom, valamint a magánélet és a személyes adatok védelmének alapvető szabályaira, hogy ezáltal könnyebb legyen összehangolni a nemzeti jogrendszereket, de anélkül, hogy ezzel kizárná egy későbbi nemzetközi egyezmény létrehozását. E munkát az Európa Tanáccsal és az Európai Közösséggel szoros együttműködésben 1979. július elsejéig kellett elvégezni. A Szakértőcsoport Kirby főbíró (Ausztrália) elnökletével és dr. Peter Seipel (konzulens) segédkezésével több tervezetet készített, és számos jelentést, például e terület jogi megközelítéseinek összehasonlító elemzését vitatta meg. Különös súllyal foglalkoztak a következő kulcskérdésekkel:

a) A külön meghatározandó-e az ún. érzékeny információk kérdése.[42]
b) Az automatizált adatkezelés kérdése.[43]
c) A jogi személyek adatvédelmének kérdése.[44]
d) A jogorvoslat és a szankciók kérdése.[45]
e) Az alap-gépezet vagy a gyakorlatba ültetés kérdése.[46]
f) A jogrendszer megválasztásának kérdése.[47]
g) A kivételek kérdése.[48]
h) A részrehajlás kérdése.[49]

A Szakértőcsoport munkája során szoros kapcsolatot tartott az Európa Tanács megfelelő szerveivel. Mindent elkövettek annak érdekében, hogy elkerüljék a két szervezet által készített szövegek szükségtelen eltérését egymástól; így a védelem alapelveinek felsoro-

---

[42] Felmerült ugyanis az a kérdés, hogy az irányelvek általános természetűek legyenek-e, vagy olyan szerkesztésűek hogy a különböző adat-, illetve tevékenység-típusokkal (pl. hitelinformációs jelentésekkel) foglalkozzanak. Valószínűleg nem is lehet megjelölni az adatoknak egy olyan csoportját, amelyet általában érzékenynek lehet minősíteni. Mindenképpen differenciálásra van szükség.

[43] Az a megközelítés, amely szerint az automatizált adatkezelés a probléma fő oka megkérdőjelezhető, következésképpen erősen vitatott.

[44] Néhány ország törvénye ugyanúgy védi a jogi személyekre vonatkozó adatokat, mint a természetes személyekhez fűződőeket.

[45] Az ellenőrzési mechanizmus megközelítései nagyon különbözők: például az egyik rendszer külön létrehozott engedélyező és felülvizsgáló hatóságra épül, míg a másik a nyilvántartók önkéntes fegyelmére és a hagyományos bírói jogorvoslatra hagyatkozik.

[46] Az alapelvek közös magjának és részletezésük megfelelő szintjének megválasztása nehézségeket okoz. Például az, hogy az adatbiztonsági kérdések (az adatok védelme illetéktelen beavatkozástól, tűztől és hasonló eseményektől) milyen mértékben tekintendők a magánélet-védelmi komplexum részének, vitatható; eltérhetnek a vélemények a megőrzés időhatárát illetőleg, az adatok törlésének követelményeiben, és ugyanez vonatkozik az adatok meghatározott célhoz kötöttségére. Különösen nehéz éles határvonalat húzni az alapelvek és célok szintje és az alsóbb szintű „mechanizmus" közé, mely utóbbiak az országos szintű alkalmazásra hagyandók.

[47] A határátlépő adatáramlás összefüggésében a joghatóság megválasztásának, az alkalmazandó jog és a külföldi ítéletek elfogadásának problémája összetettnek bizonyult. Mindazonáltal felmerült az a kérdés, hogy ebben a stádiumban kell-e és milyen mértékben ún. nem-kötelező természetű irányelveket előterjeszteni.

[48] Hasonlóképpen, a kivételek kérdésében is megoszolhatnak a vélemények Legyenek-e egyáltalán ilyenek? Ha igen, akkor meg kell-e határozni a kivételek kategóriáit, vagy inkább a kivételek általános korlátait kell megfogalmazni?

[49] Végül, a személyes adatok védelme és határátlépő szabad áramlása között feloldhatatlan ellentét van. A hangsúlyt lehet az egyikre vagy a másikra helyezni, de ennek ellenére nehézségbe ütközhet a magánélet védelmének érdekeit megkülönböztetni a kereskedelem, a kultúra, a nemzeti szuverenitás, munkáltató stb. érdekeitől.

lása sok tekintetben azonos. Másfelől viszont néhány különbség is található. Először is, az OECD Irányelvek jogilag nem kötelezők, míg az Európa Tanács által készített egyezmény jogilag kötelező lesz azon országok között, amelyek ratifikálják Ez viszont azt jelenti, hogy a kivételek kérdését az Európa Tanács részletesebben tárgyalja. Ami a jogalkalmazás területét illeti, az Európa Tanács Egyezménye főként a személyes adatok automatizált kezelésével foglalkozik, míg az OECD Irányelvek úgy vonatkoznak a személyes adatokra, mint amelyek veszélyeket rejtenek a magánéletre és a személyes szabadságjogokra, tekintet nélkül kezelésük módjára és eszközeire. A részletek szintjén a védelemnek a két szervezet által javasolt alapelvei bizonyos szempontból eltérnek, és az alkalmazott terminológia is némely tekintetben különbözik A folyamatok együttműködés intézményi kereteit az Európa Tanács Egyezménye részletesebben tárgyalja, mint az OECD Irányelvek.

Nemcsak az OECD központban történt normaalkotási folyamatban figyelhető jelentős fejlődés, hanem a tagállamokban is. Az OECD-tagországok több mint egyharmada már hozott egy vagy több olyan törvényt, amelynek célja, többek között, hogy védje az egyéneket a rájuk vonatkozó adatokkal történő visszaélésekkel szemben, és felruházza őket az adatokhoz való hozzáférés jogával, hogy ellenőrizhessék azok helytálló és pontos voltát. A föderális rendszerű országokban ilyenfajta törvények fellelhetők mind szövetségi, mind tagállami vagy tartományi szinten. Az ilyen törvényeknek a különböző országokban más és más elnevezésük van. Így az európai kontinensen általában „adattörvények"-ről *(data laws),* vagy „adatvédelmi törvények"-ről *(data protection laws; lois sur la protection des données)* beszélnek, míg az angol nyelvterület országaiban a „magánélet védelmét szolgáló törvények" *(privacy protection laws)* elnevezés a szokásos. Ezen jogszabályok túlnyomó többségét 1973 után hirdették ki. Jelenleg is megfigyelhető ennek a területnek az intenzív fejlődése. Azok az országok, amelyeknek már vannak e tárgyban alkotott jogszabályaik, a védelem új területei felé fordulnak, vagy a meglévő jogszabályok felülvizsgálatával és kiegészítésével foglalkoznak. Más országokban csak napjainkban kerül sor az ilyen vonatkozású normák megalkotására.

Az egyes országok által a magánélet és a személyes szabadságjogok kérdésében követett megoldások sok közös vonást mutatnak. Így fellelhetők azok az alapvető érdekek és értékek, amelyeket általánosságban a védelem elemi alkotórészeinek fogadnak el. Néhány ilyen fő elv: *a)* a személyes adatok gyűjtésének az adatgyűjtő céljához és más hasonló kritériumokhoz igazodó korlátozása; *b)* az adatok felhasználásának a nyilvánosan meghatározott célokra történő korlátozása; *c)* azon eszközök megteremtése, amelyek lehetővé teszik, hogy az egyén tudomást szerezhessen az adatok létezéséről és tartalmáról, továbbá hogy helyesbíttethesse azokat; *d)* valamint azon felek megjelölése, amelyek felelősek a magánélet védelmére vonatkozó szabályok és döntések tiszteletben tartásáért. Megállapítható, hogy a személyes adatokkal kapcsolatos, a magánélet és a személyes szabadságjogok védelmét szolgáló jogszabályok arra törekszenek, hogy lefedjék a teljes ciklust az adatgyűjtéstől az adatok törléséig, mindeközben a lehető legnagyobb mértékben biztosítva az egyén tudatosságát, részvételét és ellenőrzési lehetőségét.

Az egyes országok nyilvánvalóan eltérő szemlélete a törvényekben, törvénytervezetekben és javaslatokban olyan kérdésekben nyilvánul meg, mint a jogi szabályozás hatálya, a védelem különböző elemeinek súlyozása, a fenti tágan értelmezett elvek részletes gyakorlati alkalmazása és a végrehajtás lebonyolítása. Így eltérnek a vélemények az engedélyezés feltételeit illetően, és a különleges felügyelő testületek („adatfelügyelő hatóságok") ellenőrző mechanizmusának vonatkozásában. Az ún. érzékeny adatok kate-

góriáit eltérő módon határozzák meg, de eltérnek a nyitottságot és a személyes részvételt biztosító módszerek is, hogy csak néhány példát említsünk Természetesen a személyes adatok védelmének jogalkotási szemlélete és a jogi keretek konkrét megformálása tekintetében is a különbözőség irányába hatnak a jogrendszerek hagyományosan meglévő eltérései.

3.2.1.1. Az OECD Ajánlás rendelkezéseinek bemutatása

A. Az Ajánlás szerkezete

A Gazdasági Együttműködési és Fejlesztési Szervezetnek (OECD) a magánélet és a személyes adatok védelmére vonatkozó ajánlását 1980. szeptember 30-án fogadták el. Előzményének tekinthető az OECD 1960. december 14-i Egyezményének 1.(c), 3.(a) és 5.(b) pontja. A norma megalkotásánál figyelembe vették, hogy annak ellenére, hogy az egyes nemzeti törvények és politikák különbözőek lehetnek, a Tagállamok közös érdeke a magánélet és személyes adatok védelme, valamint olyan alapvető, de egymásnak ellentmondó érdekek összehangolása, mint amilyenek a magánéletben és a szabad információáramlásban megnyilvánulnak. A személyes adatok automatikus feldolgozása és a nemzeti határokat átlépő áramlása az országok közötti kapcsolatok új és egyre újabb formáit hozza létre, és egymással összhangban álló szabályozást és gyakorlatot kíván. Ugyanakkor gyakorlati problémaként vetődött fel, hogy a magánélet védelmére és az államhatárokon átlépő személyes adatok áramlására vonatkozó nemzeti és nemzetközi normák némely esetben hátráltathatják a zavartalan adatáramlást. Ezen felismeréstől vezérelve az OECD elhatározta, hogy elősegíti a szabad információáramlást a Tagállamok között és elhárítja a Tagállamok gazdasági és társadalmi kapcsolatai fejlődését hátráltató indokolatlan akadályokat. Ugyanakkor az is megfogalmazásra kerül, hogy a Tagállamok törekedjenek a személyes adatok határátlépő áramlását hátráltató indokolatlan akadályok elhárítására és ilyen akadályoknak a magánélet védelme ürügyén való létrehozása elkerülésére. A megalkotott norma két részből áll: maga az Ajánlás és a szerves részét képező Függelék, amelyben a tagállamok belső szabályozásánál követendő – a magánélet és a személyes szabadságok védelmére vonatkozó szempontokat felölelő – irányelveket fogalmazták meg.

Az Ajánlások függelékében lefektetett Irányelvek öt részből állnak. Az első rész fogalom meghatározásokat tartalmaz, és körülírja az Irányelvek hatályát, jelezve, hogy ezek minimális követelményeket képviselnek. A második rész nyolc alapelvet tartalmaz a magánélet és a személyes szabadságjogok nemzeti szintű védelméről. A harmadik rész a nemzetközi alkalmazás elveivel foglalkozik, vagyis azokkal az elvekkel, amelyek főként a Tagországok közti viszonyokat érintik. A negyedik rész az előzőekben kifejtett alapelvek gyakorlatba ültetésével foglalkozik általános megfogalmazásban, és leszögezi, hogy ezeket az elveket tilos diszkriminatív módon alkalmazni. Az ötödik rész a Tagországok egymásközti kölcsönös segítségnyújtásával foglalkozik, főként információcsere révén és oly módon, hogy kerüljék a személyes adatok védelmének mással össze nem egyeztethető nemzeti szabályozásokat.

B. Az Ajánlás célkitűzései

Az Irányelvek magvát azok az elvek alkotják, amelyek a Függelék második részében találhatók. Két lényeges alapelvről van szó: a magánélet és a személyes szabadságjogok védelméről és a személyes adatok szabad áramlásának elősegítéséről. Az Irányelvek e két érték egyensúlyára törekszenek; s noha elismerik annak szükségességét, hogy a személyes adatok országok közti szabad áramlását valahogy korlátozni kell, keresik az ilyen okok csökkentésének módját, ezáltal is erősítve az országok közötti szabad információáramlás eszméjét.

Az Irányelvek negyedik és ötödik része azon elveket tartalmazza, amelyek révén elérhető, hogy

a) az országos intézkedések hatásosan védjék a magánéletet és a személyes szabadságjogokat;
b) a gyakorlatban ne tegyenek tisztességtelen megkülönböztetést az egyének között; és
c) létrejöjjenek a személyes adatok áramlására vonatkozó folyamatos nemzetközi együttműködés és az összeférhető eljárások alapjai a személyes adatok határátlépő áramlásának bármely szabályozásában.

C. Jogi személyek, csoportok és hasonló személyiségek

Egyes országok úgy vélik, hogy a személyekre vonatkozó adatok kívánatos védelme hasonló természetű lehet, mint az a védelem, amelyet az üzleti vállalkozások, társaságok és csoportok adatai kívánnak meg, akár jogi személyiséggel bírnak azok, akár nem. Számos ország tapasztalata is igazolja, hogy a személyes és nem-személyes adatok között nagyon nehéz világos határvonalat húzni. Például egy kis vállalatra vonatkozó adatok a tulajdonost vagy a tulajdonosokat is érinthetik, és többé-kevésbé érzékeny természetű információt nyújthatnak. Ilyen esetekben javasolható az elsősorban személyes adatok számára nyújtott védelem kiterjesztése a testületekre.

Hasonlóképpen vitatható az is, hogy milyen mértékben igényelnek fokozott védelmet azok az emberek, akik valamilyen különleges csoporthoz tartoznak (például korlátozott szellemi képességű személyek, bevándorlók, nemzeti kisebbségek), az ilyen csoportra vonatkozó információk elterjedése ellen.

Másfelől az irányelvek tükrözik azt a nézetet, hogy a személyes integritás és *privacy* fogalomköre sok tekintetben különleges, és nem szabad úgy kezelni, mint személyek csoportjának integritását vagy cégek biztonságát és titkosságát. E védelmek szükségessége nem egyforma, és különbözőek azok az információpolitikai keretek is, amelyek között a megoldásokat meg kell alkotni, s az érdekeket egymással szemben kiegyensúlyozni. Az OECD Szakértőcsoport egyes tagjai javasolták, hogy lehetővé kellene tenni az Irányelvek hatályának kiterjesztését jogi személyekre (vállalatokra, társaságokra) is. Ez a javaslat azonban nem talált elegendő egyetértésre. Így, az Irányelvek hatásköre az egyénekre vonatkozó adatokra korlátozódik, és a Tagországokra marad a választóvonalak meghúzása, és a vállalatokkal, csoportokkal és hasonló testületekkel kapcsolatos elvek meghatározása.

3.2.1.2. Automatizált és nem-automatizált adatok

A múltban az OECD tevékenysége a magánélet védelmében és az ezzel rokon területeken az automatizált adatkezelésre és a számítógépes hálózatokra összpontosult. Az Ajánlást kidolgozó Szakértőcsoport különleges figyelmet szentelt annak a kérdésnek, hogy az Irányelvek szorítkozzanak-e az automatizált és számítógéppel segített adatkezelésre. Számos indokkal lehet ezt a felfogást védeni, így azzal, hogy a személyes magánéletre különleges veszélyt jelent az automatizálás, a számítógépesített adatbankok és az automatizált adatkezelés egyre növekvő dominanciája, különösen az országok közötti adatforgalomban.

Másfelől viszont a Szakértőcsoport arra a következtetésre jutott, hogy az Irányelveknek a személyes adatok automatizált kezelésére való korlátozása jelentős hátrányokkal járna. Kezdjük mindjárt azzal, hogy a meghatározások síkján nehéz tisztán megkülönböztetni az automatizált és nem-automatizált adatkezelést. Itt vannak például a „kevert" adatkezelési rendszerek, és az adatkezelés folyamatában vannak stádiumok, amelyek egyaránt vezethetnek automatizált és nem-automatizált kezeléshez. E nehézségeket tovább bonyolítja a folyamatos technikai fejlődés, mint például azoknak a félautomata módszereknek a bevezetése, amelyek mikrofilm vagy mikroszámítógépek alkalmazásán alapulnak, mely utóbbiakat egyre növekvő mértékben használhatnak olyan magáncélokra, amelyek ártalmatlanok is, ellenőrizhetetlenek is. Továbbmenve, ha kizárólaga számítógépekre összpontosítanak, az Irányelvek ellentmondásossághoz, joghézagokhoz és a nyilvántartók számára olyan lehetőségekhez vezethetnek, hogy az Irányelveket gyakorlatba ültető szabályokat úgy kerüljék meg, hogy azon célokra, amelyek ezeket sérthetik, nem-automatizált módszereket használnak.

Következésképpen, az Irányelvekben kifejezett, a magánélet és a személyes szabadságjogok védelmének elvei az adatkezelésre általánosan érvényesek, tekintet nélkül az alkalmazott konkrét technológiára. Ilymódon az Irányelvek a személyes adatokra is általánosan vonatkoznak,[50] vagy pontosabban azon személyes adatokra, amelyek, vagy kezelésük módja, vagy természetük, vagy összefüggéseik miatt veszélyt jelentenek a magánéletre és a személyes szabadságjogokra.

3.2.1.3. Az Irányelvek hatálya

Az OECD Irányelvei olyan személyes adatokra[51] vonatkoznak,[52] függetlenül attól, hogy azok az állami vagy a magánszektorban jelennek-e meg, amelyek feldolgozásuk módja vagy természetük vagy felhasználásuk környezete miatt, veszélyeztetik a magánéletet és a személyes szabadságokat.[53] Az Irányelvek nem értelmezhetők úgy, hogy gá-

[50] Megjegyzendő azonban, hogy az Irányelvek nem képezik a magánélet általános védelmére vonatkozó elvek gyűjteményét; a magánélet megsértésének olyan esetei, mint például a rejtett kamerával történő fényképezés, a fizikai bántalmazás, a rágalmazás, kívül esnek érvényességi körükön, hacsak e tettek nincsenek valamilyen módon kapcsolatban személyes adatok kezelésével.

[51] „Személyes adat" minden olyan információ, amely azonosított vagy azonosítható egyénre (adatalanyra) vonatkozik.

[52] Az Irányelvek olyan adatokkal foglalkoznak, amelyek meghatározott vagy azonosítható egyénekre vonatkoznak. Az olyan adatgyűjtemények, amelyek a fentiekre nem nyújtanak lehetőséget (statisztikai adatgyűjtemények név nélküli formában), nem tartoznak ide.

[53] A második kritérium bonyolultabb, és egy meghatározott tényszerű kockázati elemmel kapcsolatos, ti. azzal, hogy az adatok veszélyt jelentenek a magánéletre és az egyéni szabadságjogokra. Ezek a veszélyek az

tolják: *a)* különféle olyan védelmi intézkedéseknek a személyes adatok különböző kategóriáira vonatkozó alkalmazását, amely természetüktől vagy gyűjtési, tárolási, feldolgozási vagy terjesztési környezetüktől függ; *b)* az Irányelvek alkalmazási köréből való kizárását olyan személyes adatoknak amelyek nyilvánvalóan nem veszélyeztetik a magánéletet és személyes szabadságokat; és *c)* az Irányelveknek csupán a személyes adatok automatikus feldolgozására való alkalmazását.

Az OECD irányelveket minimális követelményeknek kell tekinteni, melyek a magánélet és a személyes szabadságok védelme érdekében további intézkedésekkel kiegészíthetők.

Kivételek az Irányelvek hatálya alól: *Kivételekről rendelkezni olyan Irányelvek alól, amelyek egy nem-kötelező Ajánlás részei, fölöslegesnek tűnik. A Szakértőcsoport mégis helyesnek tartotta, hogy belefoglaljon egy ezzel a tárggyal foglalkozó rendelkezést, azzal, hogy két általános kritérium vezesse a nemzeti politikát, amikor az Irányelvek hatályát korlátozza: olyan kevés kivételt kell tenni, amilyet csak lehet, és ezeket nyilvánosságra kell hozni (pl. közzétenni a hivatalos kormányzati közlönyben).*

3.2.1.4. A nemzeti alkalmazás alapelvei

Az alapelvekkel kapcsolatban bevezető megjegyzésként rámutatunk, hogy az itt tárgyalandó alapelvek egymással kölcsönösen összefüggnek és részben fedik is egymást. Így azok a megkülönböztetések, amelyeket az elvek az adatkezelés egyes műveletei és stádiumai között tesznek valamelyest mesterségesek, és lényeges, hogy az elveket együtt, mint egészet kezeljük és tanulmányozzuk.

A. Az adatgyűjtés korlátozásának elve

„A személyes adatok gyűjtését korlátozni kell, és ilyen adatok megszerzése csak törvényes és tisztességes eszközökkel történhet, s ha lehetséges, az adatalany tudtával és beleegyezésével."

Az adatgyűjtés korlátozásának elve két kérdéssel foglalkozik: a) az olyan adatok gyűjtésének korlátozásával, amelyek természetük, kezelésük módja vagy felhasználásuk összefüggései miatt különösen érzékenynek tekinthetők és b) az adatgyűjtés módszereinek követelményeivel.

Az első kérdéssel kapcsolatban gyakran hangoztatnak eltérő nézeteket. Azt lehetne mondani, hogy lehet és kívánatos is felsorolni azokat az adat-fajtákat vagy kategóriákat, amelyek önmagukban véve érzékenyek, és amelyek gyűjtését korlátozni vagy éppen tiltani kellene. Az európai jogalkotásban vannak is ilyen precedensek (például, faj, vallási meggyőződés, büntetett előélet). Másrészt viszont úgy is lehet gondolkodni, hogy nincsenek olyan adatok, amelyek önmagukban „magántermészetűek" vagy „érzékenyek", de azzá lehetnek összefüggéseik vagy a felhasználásuk következtében. Ezt a nézetet tükrözi például az Egyesült Államok privacy-törvényhozása.

---

automatizált adatkezelés alkalmazásának következményeképp (tehát az adatfeldolgozás módja következtében) állhatnak elő, de a lehetséges veszélyforrások széles választéka tartozik ide. Így olyan adatok amelyek magukban véve egyszerűek és tényszerűek, valamilyen összefüggésben az adatalannyal szemben offenzív jelleget ölthetnek Másfelől, az Irányelvek 2. §-ában a veszély úgy van meghatározva, hogy szándéka szerint kizárja a nyilvánvalóan ártatlan természetű adatgyűjtést (pl. a személyes jegyzetfüzeteket).

A Szakértőcsoport megvitatott számos érzékenységi kritériumot, mint például a hátrányos megkülönböztetés kockázatát, de nem talált lehetőséget egyetlen, egyetemesen érzékenynek tekintett adatcsoport meghatározására sem. Következésképpen ez az elv mindössze egy olyan általános állítást tartalmaz, mely szerint a személyes adatok gyűjtésének korlátokat kell szabni. Ez mindenesetre egy megerősítő ajánlás a törvényhozóknak arra vonatkozólag, hogy határozzák meg azokat a korlátokat, amelyek véget vetnek a személyes adatok válogatás nélküli gyűjtésének. A korlátok mibenléte nincs szó szerint megadva, de értelemszerűen a következőkkel lehetnek kapcsolatosak:

- az adatminőség szempontjai (vagyis hogy a gyűjtött adatokból megfelelően jó minőségű információt lehessen nyerni, hogy az adat gyűjtése helyes információs keretek között történjen stb.);
- az adatfeldolgozás céljához kapcsolódó korlátok (vagyis hogy csak az adatok bizonyos kategóriáit gyűjtsék, és hogy az adatgyűjtés lehetőleg korlátozódjék a meghatározott cél eléréséhez szükséges minimumra);
- a különösen érzékeny adatok „megpántlikázása" minden egyes Tagországban a közgondolkodás és a hagyományok alapján;
- bizonyos adatkezelők adatgyűjtő tevékenységének korlátozása;
- polgári jogi megfontolások.

Az alapelv második része (adatgyűjtési módszerek) az olyan gyakorlat ellen irányul, amelybe beletartozik például rejtett adatrögzítő (például magnetofon) használata, vagy az adatalany félrevezetése azért, hogy információt szolgáltasson. Az adatalany tudomása vagy egyetértése lényegi szabály, a tudomás a minimális követelmény. Viszont az egyetértést, gyakorlati okokból, nem lehet mindig feltételül szabni. Emellett az alapelv tartalmaz egy emlékeztetőt is („ahol helyénvaló") arról, hogy vannak helyzetek, amikor gyakorlati vagy politikai okokból az adatalany tudomása és hozzájárulása nem tekinthető szükségesnek. Példaként megemlíthető a nyomozási tevékenység vagy a címjegyzékek rutinszerű aktualizálása.

B. Az adatminőség elve

„A személyes adatoknak felhasználási céljaikkal összhangban, és ezeknek a céloknak megfelelő mértékben pontosnak, teljesnek és aktuálisnak kell lenniük."

Az adatok lényegességével kapcsolatos követelmények különbözőképpen ítélhetők meg. Sőt, a kidolgozást végző Szakértőcsoport egyes tagjai haboztak vajon az ilyen követelmények egyáltalán beleillenek-e a magánélet védelmének keretébe. A Csoport végkövetkeztetése olyan irányú volt, hogy az adatoknak felhasználásuk céljával kell összefüggniük. Például véleményekről szóló adatok félrevezetők lehetnek, ha olyan célokra használják fel ezeket, amelyekkel semmilyen összefüggésük nincs, és ugyanez vonatkozik a kiértékelt adatokra is. Az adatminőség elve foglalkozik még a pontossággal, teljességgel és időszerűséggel – mindezek az adatminőség fogalmának fontos elemei. Ebben a vonatkozásban a követelmények az adatok céljához kötődnek azaz nem terjednek messzebbre, mint amennyire felhasználásuk célja szempontjából szükséges. Így, gyakran kell gyűjteni vagy megőrizni történeti adatokat; ilyen esetek társadalomkutatás, beleértve a társadalom fejlődésének úgynevezett longitudinális tanulmányozását, történelmi kutatás és levéltári munka. A „cél-tesztelés" gyakran együtt jár annak vizsgá-

latával, hogy a pontatlanság, a teljesség hiánya, az elavultság ártalmára lehet-e az adatalanynak.

C. A célhoz kötöttség elve

„A személyes adatok gyűjtésének a célját az adatgyűjtés időpontjánál nem később meg kell adni, és ezt követő felhasználásukat korlátozni kell, mely korlát ezeknek a céloknak vagy ezekkel a célokkal nem összeegyeztethetetlen más céloknak a megvalósulásáig terjedhet, feltéve, ha a megváltoztatott cél minden egyes változás alkalmával meg van adva."

A célhozkötöttség elve szorosan összefügg az előző adatminőségi és az utána következő felhasználás-korlátozási elvvel. A célhozkötöttség elve alapjában véve azt írja elő, hogy az adatok gyűjtését megelőzően, de legkésőbb megkezdésével egyidőben meghatározhatók legyenek azok a célok, melyekre az adatokat felhasználni kívánják és hogy a célok későbbi módosulását ugyanígy meghatározzák. Az ilyen célmeghatározás különböző választható vagy kiegészítő módokon történhet pl. nyilatkozat, az adatalany tájékoztatása, jogszabály-alkotás, végrehajtási rendelet vagy felügyeleti testületek által kibocsátott engedély formájában. A célhozkötöttség és az adatminőség elvei értelmében új célokat nem lehet önkényesen bevezetni, változtatni csak az eredeti célokkal összeegyeztethetően szabad. Végül: amikor az adatok már nem szolgálják a célt, és ha ez megvalósítható, szükségessé válhat megsemmisítésük (törlésük) vagy anonim alakra hozásuk. Ennek indoka az, hogy az érdektelenné vált adatok feletti ellenőrzés megszűnhet, ez pedig az eltulajdonítás, illetéktelen másolás és hasonlók kockázatához vezethet.

D. A korlátozott felhasználás elve

„A személyes adatokat nem szabad felfedni, hozzáférhetővé tenni vagy egyéb olyan módon felhasználni, amely eltér az adatgyűjtés eredeti célkitűzésétől (ld. részletesebben „A célhozkötöttség elvéről írottakat"), kivéve: a) az adatalany beleegyezésével; vagy b) ha a törvény azt úgy rendeli."

Ez az elv különféle felhasználásokkal foglalkozik, beleértve az olyan nyilvánosságra hozatalt, amely eltér a rögzített céloktól. Például az adatokat az egyik számítógéptől a másikhoz lehet továbbítani, ahol meg nem engedett célokra használhatják fel felügyelet nélkül, és így tárhatják a szó szoros értelmében a nyilvánosság elé. Általános szabály, hogy a kezdetben, vagy azt követően megjelölt cél eldönti az adatok felhasználását. Két általános kivétel ismert: az adatalany (vagy megbízottjának) hozzájárulása, és a törvényi felhatalmazás (ideértve például a felügyeleti hatóságok által adott engedélyeket is). Például, előírható lehet, hogy olyan adatok, melyeket igazgatási döntéshozatal céljából gyűjtöttek, elérhetők legyenek kutatási, statisztikai és szociális tervezési célokra.

E. A biztonság elve

„A személyes adatokat ésszerű biztonsági intézkedésekkel védelmezni kell olyan veszélyek ellen, mint elvesztés vagy illetéktelen hozzáférés, megsemmisülés, felhasználás, módosítás vagy megismerés."

Elöljáróban megjegyezzük, hogy az adatbiztonság és az adatvédelem nem azonos fogalmak. Az adatok felhasználásának és közlésének korlátait azonban biztonsági ga-

ranciákkal kell megerősíteni. Ezek a biztosítékok *fizikaiak,* (például zárt ajtók és személyazonossági lapok), *szervezetiek,* (mint az adatokhoz hozzáférés hierarchiája), és – különösen számítógépes rendszerekben – *információs intézkedések* (mint pl. rejtjelezés és a szokatlan tevékenység esetén aktiválódó megfigyelő és reagáló program). Hangsúlyozni kell, hogy a szervezeti jellegű intézkedések magukban foglalják az adatfeldolgozással foglalkozó személyzet titoktartási kötelezettségét. Ezen elv hatálya széleskörű. Ugyanakkor, az itt felsorolt esetek bizonyos mértékig átfedik egymást (pl. hozzáférés/nyilvánosságra hozás). Az adatok „elvesztése" fogalmába beleértendők például az adatok véletlen törlése, az adathordozó (és ezzel az adatok) tönkretétele és az adathordozó eltulajdonítása. A „módosítás" alatt illetéktelen adatbevitel, a „felhasználás" alatt illetéktelen másolás értendő.

F. A nyíltság elve

„A személyes adatokra vonatkozó fejleményeket, a velük folytatott gyakorlatot és politikát nyíltan kell kezelni. A személyes adatok létezésének, természetének és felhasználásuk fő céljának, valamint az adatkezelő[54] *személyének és állandó tartózkodási helyének megismerésére egyszerű módszereket kell kidolgozni."*

A nyíltság elvét a személyes részvétel elve előfeltételének lehet tekinteni; ahhoz, hogy ez utóbbi elv érvényesülhessen, a gyakorlatban tájékozódási lehetőséget kell kapni a személyes adatok gyűjtéséről, tárolásáról és felhasználásáról. Néhány példa a teljesség igénye nélkül, ennek elérésére: rendszeres önkéntes tájékoztatás az adatkezelők részéről, a személyes adatok kezelésével kapcsolatos tevékenységek publikálása hivatalos közlönyökben, és bejegyeztetés a hivatalos szerveknél stb. Az „egyszerű módszerek" kifejezés úgy értendő, hogy az egyéneknek aránytalan költség- és időráfordítás, utazás és előzetes ismeretek nélkül kell tudniuk hozzájutni az információhoz.

G. A személyes részvétel elve

„Az egyénnek legyen joga arra, hogy: a) az adatkezelőtől vagy másképpen bizonyságot nyerjen arról, van-e az adatkezelőnek rá vonatkozó adata vagy nincs; b) a rá vonatkozó adatokat megkapja, éspedig elfogadható időn belül, méltányos díj ellenében, ha ilyen egyáltalán van, elfogadható módon és számára könnyen elérhető formában; c) az (a) és (b) alpontok szerinti igényének elutasítása indokait megismerje, és az elutasítást kifogásolja; és d) kifogásolhassa a rá vonatkozó adatokat és, ha a kifogásolás helyénvaló, az adatokat töröltethesse, helyesbíttethesse, kiegészíttethesse vagy módosíttathassa."

Azt tartják, hogy az egyén joga ahhoz, hogy a személyes adatokhoz hozzáférjen, és azokkal szemben kifogást emelhessen, a magánélet védelmének talán legfontosabb biztosítéka. Követelmény, hogy a hozzáférés jogának mint szabálynak a gyakorlása általában legyen egyszerű. Ez – többek között – azt jelenti, hogy része kell legyen az adatkezelő vagy képviselője mindennapos tevékenységének, és jogi vagy más hasonló eljárás ne kelljen hozzá. Egyes esetekben indokolt lehet az adatok közvetett hozzáférhetőségéről gondoskodni; például az egészségügy területén a gyakorló orvos lehet a közvetítő.

[54] „Adatkezelő" az a fél, aki a nemzeti törvények szerint illetékes a személyes adatok tartalmáról és felhasználásáról határozni, tekintet nélkül arra, hogy ilyen adatok gyujtését, tárolását, feldolgozását vagy terjesztését saját maga vagy megbízottja végzi.

Egyes országokban felügyeleti szervek, mint például az adatfelügyeleti hatóságok nyújthatnak hasonló szolgáltatást. Azt a követelményt, hogy az adatot elfogadható időn belül kell közölni, különbözőképpen lehet teljesíteni. Például az az adatkezelő, aki rendszeres időközönként szolgáltat információt az adatalanyoknak felmenthető az alól, hogy egyedi kérésekre azonnal válaszoljon. A közlés „elfogadható módja", többek között, azt jelenti, hogy a földrajzi távolságra megfelelő figyelemmel kell lenni. Továbbá, ha a hozzáférés teljesítésére idő-intervallumok vannak előírva, akkor az ilyen időközöknek ésszerűeknek kell lenniük.

Az indokok megismeréséhez való jogot ki kellene terjeszteni minden, a személyes adatokkal kapcsolatos negatív döntésre.

A kifogásoláshoz való jog hatálya tág, és magában foglalja az elsőfokú kifogásolást az adatkezelőknél éppúgy, mint – a nemzeti eljárási szabályok szerint – a későbbieket a bíróságoknál, közigazgatási testületeknél, szakmai szervezeteknél vagy egyéb intézményeknél. A kifogásolás joga nem jelenti azt, hogy az adatalany meghatározhatja, hogy milyen jogorvoslat jár (helyesbítés, az adat vitatott voltának jelzése stb.).

H. A felelősség elve

„Az adatkezelőnek felelősnek kell lennie azoknak az intézkedéseknek a betartásáért, amelyek a fenti elveket tükrözik."

Az adatkezelő határoz az adatok és az adatfeldolgozás felől. Az adatok feldolgozása az ő javára történik. Ennek megfelelően lényeges, hogy a nemzeti törvényhozás is az adatkezelőt tegye felelőssé a magánélet-védelmi szabályok és döntések megtartásáért, és e kötelezettsége alól ne mentesítse az, ha az adatok feldolgozását az ő megbízásából más, mondjuk egy szolgáltató iroda végzi. Másfelől viszont az Irányelvek semmilyen kitétele nem mentesíti a szolgáltató iroda személyzetét, a „függő felhasználók"-at és másokat a felelősség alól.

3.2.1.5. A nemzetközi alkalmazás alapelvei: szabad áramlás és törvényes korlátozások

a) „A Tagországoknak figyelembe kell venniük milyen következményekkel jár a személyes adatok belföldi feldolgozása és re-exportja."

Az országon belüli feldolgozást illetően e pontnak két fontos vonatkozása van. Az első az Irányelvek szellemével ellentétes liberális politika ellen irányul, amely megkönnyíti a más Tagországok védelmi jogszabályainak megkerülésére vagy megsértésére irányuló kísérleteket. Mindazonáltal ilyen megkerülést, vagy megsértést, noha valamennyi Tagország elítéli ezeket, ez a szakasz külön nem nevez meg, ugyanis néhány ország nem találta elfogadhatónak hogy valamely Tagországtól azt kívánják hogy közvetlenül vagy közvetve, területen kívül szerezzen érvényt más Tagországok törvényeinek.

Megjegyzendő, hogy ez a pont kifejezetten megemlíti a személyes adatok re-exportját. E tekintetben a Tagországoknak mindig tudatában kell lenniük annak, hogy segíteniük kell egymás törekvéseit arra, hogy a személyes adatok ne veszítsék el védelmüket azért, mert átkerülnek olyan területre és olyan adatfeldolgozási körülmények közé, ahol az ellenőrzés laza vagy nem is létezik.

Másodszor, az Ajánlás a Tagországokat hallgatólagosan arra biztatja, hogy fontolják meg annak szükségét, hogy adatkezelési szabályokat fogadjanak el olyan különleges körülmények esetére is, amikor külföldi adatokkal vagy más nemzetiségűek adataival kell dolgozni. A szemléltetés kedvéért: előfordulhat olyan helyzet, amikor külföldi állampolgárok adatai olyan célok érdekében válnak hozzáférhetővé, amely az anyaországukat szolgálja (pl. hozzáférés a külföldön élő állampolgárok címeihez).

> *b) „A Tagországoknak minden ésszerű és megfelelő intézkedést meg kell tenniük azért, hogy a személyes adatok határátlépő áramlása, beleértve a Tagországon átmenő forgalmat is, zavartalan és biztonságos legyen."*

Ami az Irányelveket illeti, a személyes adatok nemzetközi áramlásának elősegítése önmagában sem vitán felül álló cél. Ezek jelenlegi mértékű áramlásának megszakítás nélkülinek és biztonságosnak kell lennie, vagyis védettnek az illetéktelen hozzáférés, az adatok elvesztése és hasonló események ellen. Ugyanilyen védelmet kell nyújtani az átmenő adatoknak, tehát azoknak az adatoknak, amelyek egy Tagországon úgy haladnak keresztül, hogy azokat ott nem használják fel, és nem is tárolják ebben az országban történő jövőbeni felhasználás érdekében. Az e pontban említett általános kötelezettséget a számítógépes hálózatok tekintetében a Malaga-Torremolinos-i Nemzetközi Távközlési Egyezmény (1973. október 25.) hátterével együtt kell szemlélni.[55]

> *c) „Egy Tagországnak tartózkodnia kell a közte és egy másik Tagország között határátlépő adatáramlás korlátozásától, kivéve, ha a másik országban ezeket az Irányelveket lényegében még nem alkalmazzák, vagy ha ilyen adatok re-exportja a másik országnak a magánélettel kapcsolatos belföldi törvényeibe ütközik. Egy Tagország korlátozásokat léptethet életbe a személyes adatok bizonyos olyan kategóriáira is, amelyekre nézve a magánélettel kapcsolatos belföldi törvényei az ilyen adatok természetéből következő különleges előírásokat tartalmaznak, vagy amelyekre nézve a másik Tagország azonos értékű védelmet nem biztosít."*

E pont megerősíti a „b" pontnál írottakat a Tagországok közötti kapcsolatok vonatkozásában. A személyes adatok szabad határátlépő áramlásával szembenálló érdekekkel foglalkozik, azokkal, amelyek azonban ezen áramlás korlátozásához jogi alapot adhatnak Tipikusan ilyen példa az, amikor a nemzeti törvényeket úgy akarják megkerülni, hogy az adatokat olyan Tagországban dolgozzák fel, amelyik még lényegében nem fogadta el az Irányelveket. Itt megalkotják az egyenértékű védelem fogalmát, ami olyan védelmet jelent, amely hatásában lényegileg hasonló az exportáló országéhoz, bár nem szükségképpen azonos azzal formájában vagy minden részletében. Itt is külön említést

---

[55] Ezen egyezmény szerint a Nemzetközi Távközlési Unió (ITU) tagjai, beleértve az OECD-tagországokat, megegyeztek többek között abban, hogy biztosítják a nemzetközi távközlés gyors és megszakítás nélküli forgalma érdekében szükséges csatornák és berendezések létesítését a legjobb műszaki feltételek mellett. Ezen túlmenőleg, az ITU tagjai vállalták a nemzetközi forgalmazás titkossága érdekében minden olyan intézkedés megtételét, amely az általuk használt távközlési rendszerekkel összefér. Ami a kivételeket illeti: fenntartották a nemzetközi távközlési szolgálatok felfüggesztésének jogát és azt a jogot is, hogy a nemzetközi forgalmazásról az illetékes hatóságokat értesítsék a belső jogszabályok, valamintazon nemzetközi egyezmények alkalmazása érdekében, amelyeknek az ITU-tagok aláírói. Ezek az előírások mindaddig érvényesek, amíg az adatok a távközlési vonalakon áthaladnak Az Irányelvek, összefüggéseiben, a személyes adatok zavartalan és biztonságos nemzetközi áramlásának kiegészítő biztosítéka.

nyer a személyes adatok re-exportja; ebben az esetben avval a céllal, hogy meg lehessen akadályozni a Tagországok privacy jogszabályainak megkerülésére irányuló kísérleteket. A jogszerű korlátozás harmadik, a különleges személyes adatokra vonatkozó kategóriája e pontban azokat az eseteket fedi le, amelyek a Tagországok fontos érdekeit érintik.

> *d) „A Tagországoknak el kell kerülniük, hogy a magánélet és személyes szabadságok védelme ürügyén olyan törvényeket hozzanak, és olyan politikát és gyakorlatot folytassanak, amely az ilyen védelem követelményeit meghaladó módon akadályokat gördít a személyes adatok határátlépő áramlása elé."*

Az Ajánlás e pontja megkísérel egyensúlyt teremteni a magánélet védelméhez és a személyes adatok szabad határátlépő áramlásához fűződő érdekek között. Elsősorban azok ellen a mesterséges gátak ellen irányul, amelyek nem a magánélet és a személyes szabadságjogok védelmét, hanem másfajta, de nyíltan be nem vallott korlátozási célokat szolgálnak. Ugyanakkor, nem szándékozik korlátozni a Tagországok jogait arra, hogy szabályozzák a személyes adatok határátlépő forgalmát a szabad kereskedelem, a vámtarifák, a foglalkoztatás és a nemzetközi adatforgalom ezekkel kapcsolatos gazdasági feltételei terén.

3.2.1.6. Információcsere és összeférő eljárások

Itt két nagy problémával foglalkozunk, nevezetesen (a) annak szükségességével, hogy az Irányelveket bevezető szabályokról, rendeletekről, határozatokról stb. tájékoztatást lehessen nyerni, és (b) annak szükségességével, hogy fölöslegesen bonyolult és illeszthetetlen eljárási keretek és egyezőségi követelmények ne gördítsenek akadályokat a személyes adatok határátlépő áramlása elé. Az első probléma a magánélet-védelem szabályainak és az adatpolitikának az összetettségéből ered. Gyakori, hogy a (tág értelemben vett) szabályozásnak számos szintje van, és sok fontos szabályt nem lehet tartósan, részletesen törvényileg meghatározni; ezeket meglehetősen nyitottan kell tartani, és az alsóbb szintű döntéshozó testületek mérlegelésére kell bízni.

A második kérdés fontossága, általánosan szólva, arányos a határátlépő személyes adatforgalmat szabályozó nemzeti törvények számával. Már a mai stádiumban is nyilvánvaló szükség van a határátlépő adatáramlás nemzeti jogszabályainak egyeztetésére, beleértve ebbe a szabályok megtartásának ellenőrzésére bevezetett külön intézkedéseket, és ahol ez követelmény, ott az adatkezelő rendszerek működtetésének engedélyeit.

3.2.1.7. Jogrendszerek ütközése

Jelentős figyelmet szentelt a Szakértőcsoport az egymással ellentmondásban lévő jogrendszerek kérdésének és mindenekelőtt annak a kettős kérdésnek hogy meghatározott esetekben mely bíróságok legyenek illetékesek (illetékesség választása), és melyik jogrendszer legyen érvényes e meghatározott esetekre (jogrendszer választása). A különböző stratégiák és javasolt elvek vitája megerősítette azt a nézetet, hogy a jelenlegi stádiumban, ilyen gyors technikai változások küszöbén, és az Irányelvek nem kötelező voltára tekintettel nem szabad megkísérelni speciális, részletes megoldások nyújtását. Bizonyos, hogy mind az elméletileg helytálló szabályozási modell megválasztásával,

mind az önmagukban lehetséges megoldások következményeiről nyert tapasztalatok szükségességével kapcsolatban nehézségek fognak felmerülni.

Ami a jogrendszer megválasztását illeti, a megoldás felé az egyik lehetséges megközelítés egy vagy több összekötő tényező azonosítása, amelyek – legjobb esetben – egy alkalmazható jogot jelölnek meg. Ez a nemzetközi számítógépes hálózatok esetében különösen nehéz, mert az adatok szétszórtsága és gyors mozgása, az adatfeldolgozási tevékenység földrajzilag szétszórt volta miatt számos, szövevényes formában megjelenő összekötő tényező bukkanhat fel, köztük jogi újdonságot jelentő elemek is. Továbbmenve: nem egyértelmű, hogy milyen értéket tulajdonítsunk olyan szabályoknak melyek mechanikus alkalmazása egy bizonyos ország alkalmazható jogának meghatározását eredményezi. Csak egy dolgot említve: az ilyen megoldás helyessége attól függ, hogy hasonlóak-e a jogi fogalmak és szabályszerkezetek, és hogy milyenek a nemzetek vállalt kötelezettségei a személyes adatok védelmének bizonyos normái megtartására. E feltételek hiányában meg lehet kísérelni olyan rugalmasabb elvek megfogalmazását, amelyek feltételezik egy „megfelelő jog" keresését, és amelyek a magánélet és a személyes szabadságjogok hatékony védelmének biztosítása céljához kapcsolódnak Így olyan helyzetben, amikor több jog is alkalmazható volna, olyan megoldás javasolt, hogy az a nemzeti jog részesítendő előnyben, amely a személyes adatoknak a legjobb védelmet nyújtja. Másrészt viszont, úgy is lehet érvelni, hogy az ilyen megoldások túl sok bizonytalanságot hagynak maguk után, nem utolsó sorban azon adatkezelők szemszögéből, akik tudni szeretnék – ahol lehet, előre –, hogy egy nemzetközi adatfeldolgozási rendszer mely ország szabályrendszerének illetékessége alá tartozik majd.

Tekintettel ezekre a nehézségekre, és figyelemmel arra, hogy a jogrendszerek ellentéteit legjobban a személyes és nem személyes adatok átfogó keretében lehet kezelni, a Szakértőcsoport úgy döntött, hogy megelégszik egy olyan nyilatkozattal, amely a vitatott kérdéseket csak jelzi, és javasolja, hogy a Tagországok dolgozzanak megoldásukon.

3.2.2. Az Európa Tanács *Egyezménye az egyének védelméről a személyes adatok gépi feldolgozása során*[56]

A. Az Európa Tanács Egyezményének legfontosabb hipotézisei:

a) Az Európa Tanács célja a tagjai közötti nagyobb egység elérése, amely elsősorban a jog uralmának, valamint az emberi jogoknak és az alapvető szabadságjogoknak a tiszteletben tartásán alapszik;

b) A mindenkit megillető jogoknak és alapvető szabadságjogoknak, különösen a magánélet tiszteletben tartásához való jognak a védelmét kívánatos kiterjeszteni, a gépi úton feldolgozott személyes adatok[57] védelmére és határokat átlépő adatok szabályozására;

c) Az információszabadság országhatárokra tekintet nélküli elismerése;

---

[56] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981. január 28. (A Magyar Köztársaság megerősítéséről szóló okiratának letétbe helyezése az Európa Tanács főtitkáránál 1997. október 8-án történt meg. Az Egyezményben foglaltakat 1998. február 1. napjától kezdődően kell alkalmazni Magyarországon.)

[57] Az Európa Tanács Egyezményének értelmében *személyes adat:* bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik (adatalany).

d) A magánélet tiszteletben tartásához és az államok közötti szabad információáramláshoz fűződő alapvető érdekek összeegyeztetése szükséges.

B. Az Egyezmény célja

Az Európa Tanács Egyezményének az alapvető célja, hogy minden egyes aláíró tagállam területén minden egyén számára, tekintet nélkül nemzetiségére vagy lakóhelyére, biztosítva legyen, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák a személyes adatainak gépi feldolgozása[58] során (adatvédelem).

C. Az Egyezmény hatálya

Az Egyezmény általános tárgyi hatálya a személyes adatok automatizált állományaira és a személyes adatok gépi feldolgozására terjed ki, függetlenül attól, hogy azt a köz-, vagy a magánszektorban végzik.

Ettől az általános tárgyi hatálytól bármely aláíró fél az Egyezmény aláírásakorvagy a megerősítésről, az elfogadásról, a jóváhagyásról vagy a csatlakozásról szóló okirat letétbe helyezésekor vagy bármely későbbi időpontban az Európa Tanács főtitkáránál nyilatkozattal térhet el. Az eltérés alapvetően két irányú lehet. Egyrészt szűkítő, illetve másrészt kiterjesztő jellegű.

a) Szűkítés. Az Egyezmény 3. Cikkely 2/a pontja tartalmazza a *szűkítés* lehetőségét. Kimondja, hogy a szűkítést óhajtó aláíró fél köteles nyilatkozatot arról, hogy a jelen Egyezményt nem alkalmazza meghatározott személyes adatok automatizált állományaira. A kizárt adatállományra vonatkozó listát is letétbe kell helyezi az ET. Főtitkáránál. Ez a lista azonban nem tartalmazhatja azokat az automatizált adatállományokat,[59] amelyekre hazai jogának adatvédelmi rendelkezései vonatkoznak. Ebből következően ezt a listát új nyilatkozattal módosítja, ha hazai jogának adatvédelmi rendelkezéseit személyes adatok további automatizált állományára terjeszti ki.

Abban az esetben, ha bármelyik aláíró Fél, amely a 2/*a* pont alapján nyilatkozatával a személyes adatok meghatározott állományát kizárta, nem igényelheti a jelen Egyezmény alkalmazását ezekre az adatokra attól a Féltől, amely ezeket nem zárta ki.

b) Kiterjesztés. Az Egyezmény 3. Cikkely 2/b és 2/c pontjai tartalmazzák a *kiterjesztés* lehetőségét. A kiterjesztés egyrészt a személyi hatályra – nem természetes személyek adatvédelmére – vonatkozik. Kimondja, hogy az Egyezmény előírásai alkalmazhatók személyek csoportjaira, egyesületekre, alapítványokra, társaságokra, vállalatokra és minden más, közvetlenül vagy közvetve egyénekből álló szervezetekre vonatkozó információkra is, függetlenül attól, hogy ezek a szervezetek jogi személyiséggel rendelkeznek-e. A kiterjesztés másik aspektusa az Egyezmény tárgyi hatályát érintheti, ugyanis az Egyezményt az adott tagállam alkalmazhatja a személyes adatok nem gépi eszközökkel feldolgozott állományaira is.

---

[58] *Gépi feldolgozás* a következő műveleteket tartalmazza, ha azokat részben vagy egészben automatizált eszközökkel hajtják végre: az adatok tárolása, az adatokkal végzett logikai vagy aritmetikai műveletek, az adatok megváltoztatása, törlése, visszakeresése és terjesztése.

[59] Az Egyezmény alapján *automatizált adatállomány alatt értjük az* automatikus feldolgozásra kerülő adatok sorát.

További megszorítást jelent, hogy bármely állam, amely a jelen Egyezmény hatályát a 2/*b* vagy 2/*c* pont alapján tett nyilatkozattal kiterjesztette, az említett nyilatkozatban jelezheti, hogy ezek a kiterjesztések csak a személyes adatok meghatározott állományaira vonatkoznak. Ezzel egyidejűleg ezeknek a listáját letétbe kell helyezni.

Ugyanakkor, az a Fél, amely a 2/*b* vagy 2/*c* pont alapján nem tett kiterjesztést, nem igényelheti az Egyezmény ezen pontjainak alkalmazását attól a Féltől, amely ilyen kiterjesztéseket tett.

D. Az adatvédelem alapelvei az ET Egyezményében

1. Az adatok minőségének elve

A személyes adatokra vonatkozó követelmények a gépi feldolgozás során:

a) az adatokat csak tisztességesen és törvényesen szabad megszerezni és feldolgozni;
b) az adatokat csak meghatározott és törvényes célra szabad tárolni, és attól eltérő módon nem szabad felhasználni;
c) az adatoknak tárolásuk céljával arányban kell állniuk, és meg kell felelniük e célnak, azon nem terjeszkedhetnek túl;
d) az adatoknak pontosaknak és ha szükséges időszerűeknek kell lenniük;
e) az adatok tárolási módjának olyannak kell lennie, amely az adatalany azonosítását csak a tárolás céljához szükséges ideig teszi lehetővé.

Ettől az alapelvtől csak akkor lehet eltérni, ha erről az adott Fél törvénye rendelkezik, és a szükséges intézkedésekre egy demokratikus társadalomban: *a)* az állam biztonsága, a közbiztonság, az állam pénzügyi érdekének a védelme vagy a bűncselekmények megelőzése érdekében és/vagy *b)* az adatalany vagy mások jogainak vagy szabadságjogainak védelme érdekében kerül sor.

2. A különleges adatok speciális védelmének elve

Nem lehet gépi úton feldolgozni a faji eredetre, a politikai véleményre, a vallásos vagy más meggyőződésre, valamint az egészségre, a szexuális életre vonatkozó személyes adatokat, kivéve, ha a hazai jog megfelelő biztosítékokat nyújt. Ez vonatkozik a büntető ítéletekkel kapcsolatos személyes adatokra is.

Ettől az alapelvtől csak akkor lehet eltérni, ha erről az adott Fél törvénye rendelkezik, és a szükséges intézkedésekre egy demokratikus társadalomban: *a)* az állam biztonsága, a közbiztonság, az állam pénzügyi érdekének a védelme vagy a bűncselekmények megelőzése érdekében és/vagy *b)* az adatalany vagy mások jogainak vagy szabadságjogainak védelme érdekében kerül sor.

3. Az adatbiztonság elve

Megfelelő biztonsági intézkedéseket kell tenni az automatizált adatállományokban tárolt személyes adatok védelme érdekében a véletlen vagy jogtalan megsemmisítés, vagy véletlen elvesztés, valamint a jogtalan hozzáférés, megváltoztatás vagy terjesztés megakadályozására.

E. Az adatalanyt védő további garanciák

Mindenkinek joga van arra, hogy *a)* tudomást szerezzen a személyes adatok automatizált állományáról, annak fő céljairól, valamint az adatállományt kezelő személyéről és szokásos lakhelyéről vagy székhelyéről; *b)* ésszerű időközönként és túlzott késedelem vagy költség nélkül értesüljön arról, hogy egy automatizált adatállományban személyes adatait tárolják-e, és ezekről az adatokról számára érthető formában tájékoztassák; *c)* indokolt esetben ezeket az adatokat helyesbíttethesse vagy töröltethesse, ha ezen adatok feldolgozása ellentétes az ET Egyezményében foglalt alapelveket érvényesítő hazai jog rendelkezéseivel; *d)* jogorvoslattal élhessen, ha a tájékoztatási vagy indokolt esetben közlési, helyesbítési, illetve törlési kérelmét nem teljesítik.

Ettől a ponttól csak akkor lehet eltérni, ha erről az adott Fél törvénye rendelkezik, és a szükséges intézkedésekre egy demokratikus társadalomban: *a)* az állam biztonsága, a közbiztonság, az állam pénzügyi érdekének a védelme vagy a bűncselekmények megelőzése érdekében és/vagy *b)* az adatalany vagy mások jogainak vagy szabadságjogainak védelme érdekében kerül sor.

Továbbá, a garanciális jogok gyakorlásának korlátozását törvény elrendelheti, személyes adatok statisztikai vagy tudományos kutatási célra használt automatizált állományai esetén, ha ezzel az adatalany magánélete nyilvánvalóan nem kerül veszélybe.

F. Szankciók és jogorvoslatok

Az adatvédelmi alapelveket érvényesítő hazai jog rendelkezéseinek megsértése esetén a tagállamok belső jogrendszerbeli szankciókat és jogorvoslatokat állapítanak meg.

G. Fokozott védelem

Az Egyezmény kimondja, hogy egyetlen aláíró államot sem lehet korlátozni vagy befolyásolni abban, hogy az adatalanyt a nemzetközi Egyezményben meghatározottaknál fokozottabb védelemben részesítse.

3.2.3. Az EU szabályozása

Az Európai Unió – felismerve az egyes államok szabályozásának hiányosságait és az államok védelmi rendszerei között meglévő eltéréseket – elfogadott két irányelvet, amelyben az EU polgárainak adatvédelméről rendelkeztek. Ezek az Európai Telekommunikációs Irányelv[60] és az Európai Adatvédelmi Irányelv.[61] Ez az irányelv iránymutatásul szolgált a tagállamok jogalkotói számára. Az irányelv értelmében és szellemében minden tagállamnak 1998 októberéig el kellett fogadnia az irányelv rendelkezéseit végrehajtó (kiegészítő) saját belső normáit. Az irányelv hatálya az EU-n belül áramló az EU-s polgárokra vonatkozó személyes információ védelmén kívül kiterjed az uniós polgárok személyes adatainak EU-n kívül történő kezelésére, átvitelére is. Ez a rendelkezés alapvetően megtermékenyítőleg hatott az EU-n kívüli országokra abban a tekin-

[60] European Telecommunications Directive.
[61] European Data Protection Directive.

tetben, hogy a magánszféra védelmét szolgáló jogi normákat fogadjanak el. Egyre több ilyen országgal találkozhatunk.

Az említett két irányelv széleskörűen védi az EU-s polgárok személyes adatait. A két irányelv nem egyszerűen megismétli a korábban elfogadott adatvédelmi jogi normákat, hanem azokon túlmenve új típusú védelmet alapít. Az Adatvédelmi irányelv harmonizációs mintául szolgál az EU tagállamai számára.[62] A Telekommunikációs irányelv[63] speciális védelmi standardokat állít fel a telefon, digitális televíziózás, a mobilhálózatok és más telekommunikációs rendszer vonatkozásában. A telekommunikációs irányelv elsősorban a szolgáltatókra vonatkozó kötelezettségeket ír elő. Ezek lényege, hogy a felhasználók kommunikációjában lévő személyiségi jogi elemeket védjék. Az új szabályozásnak olyan kérdéseket kell lefednie, amelyek eddig nem kerültek a jogi szabályozás hatáskörébe. Az adatokhoz való hozzáférés értékesítése és a marketing célú felhasználás szigorúan tilalmazott magatartás. A különböző kommunikációs információ szolgáltatások által összegyűjtött adatokat csak addig lehet tárolni, amíg a címzett egyszer lekéri. Ezt követően meg kell azokat semmisíteni. A fent említett EU-s irányelvekben számos alapelvi jelentőségű szabály található. Például az egyénnek joga van arra, hogy ellentételezés és indoklás nélkül kitérjen az ún. direkt marketing célból küldött szóróanyagok megválaszolása, illetve a programban való részvétel elől.

Az adatvédelmi irányelv különös figyelmet fordít az ún. érzékeny személyes adatok – például egészségügyi vagy az egyén pénzügyi helyzetére vonatkozó információk – védelmére. A jövőben az ilyen típusú adatok kereskedelmi vagy kormányzati célú felhasználásra csak az érintett személy kifejezett és egyértelmű beleegyezése esetén kerülhet sor.

Az európai modell központi elve az „kikényszeríthetőség". Az EU álláspontja szerint az adatok alanyait jogok illetik meg, amely jogokat kifejezett és egyértelmű jogi szabályozás keretei között kell megfogalmazni. Ezen kívül létezik egy olyan személy (adatvédelmi biztos) vagy szerv, akinek az a feladata, hogy a védelemre jogosult személy nevében eljárjon, illetve a vonatkozó normáknak érvényt szerezzen. Ugyancsak elvárás az EU részéről, hogy azokban az országokban (3. állam), akikkel üzleti kapcsolatban állnak hasonló szintű védelemben részesüljenek a személyes adatok.

Az irányelv előírja a tagállamok számára, hogy azokat az adatokat is védelemben kell részesíteni, amelyeket másik – Európán kívüli – országba exportálják, illetve ott dolgozzák fel azokat. Az irányelv ezen cikkelyének hatására az EU-n kívüli államokban – akik továbbra is fenn szeretnék tartani a kapcsolatot az EU-s országokkal – is megindult a személyiségi jogok védelmét szolgáló jogi szabályozás kialakítása, illetve fejlesztése, mivel ennek hiányában megbénulhat az EU-val az információáramlás.

---

[62] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (http://www.odpr.org/restofit/Legislation/Directive/Directive_Contents.html)

[63] Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997. (http://www2.echo.lu/legal/en/dataprot/protection.html)

3.2.3.1. A 95/46/EK Irányelv rendelkezéseinek részletes bemutatása

Az Európai Parlament és a Tanács 1995. október 24-én fogadta el a 95/46/EK Irányelvet, amely „A személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról" rendelkezik.

A Közösségnek a Római Szerződésben megállapított, és az Európai Unióról szóló szerződés által módosított célkitűzései között szerepel a tagállamok közötti egyre szorosabb unió megteremtése, továbbá a Közösség gazdasági és társadalmi fejlődésének biztosítása, valamint az emberi jogok és alapvető szabadságjogok védelméről szóló európai egyezményben elismert alapvető jogok garantálása. Ennek értelmében nemzetiségtől és lakóhelytől függetlenül tiszteletben kell tartani a személyek alapvető jogait és szabadságjogait, különösen a magántitokhoz való jogukat, és hozzá kell járulniuk a gazdasági és társadalmi fejlődéshez, a kereskedelem kiterjedéséhez, valamint az egyének jólétéhez. Egy olyan belső piac kialakítása és működése, amelyben a RSz. 7a. cikkének megfelelően biztosított az áruk, a személyek, a szolgáltatások és a tőke szabad mozgása, nem csak azt kívánja meg, hogy a személyes adatok szabadon áramolhassanak egyik tagállamból a másikba, hanem azt is, hogy az egyének alapvető jogai biztosítottak legyenek. Megfigyelhető, hogy a Közösségben a gazdasági és társadalmi tevékenység számos területén egyre többször folyamodnak a személyes adatok kezeléséhez; mivel az informatika terén elért haladás az ilyen adatok kezelését és cseréjét lényegesen megkönnyíti.

A RSz. 7a. cikke értelmében a belső piac kialakításából és működéséből eredő gazdasági és társadalmi integráció szükségszerűen a személyes adatok határokon keresztüli áramlásának lényeges növekedéséhez vezetett – és ez a tendencia a jövőben még tovább fog erősödni – mindazok között, akik a tagállamokban magán- vagy állami szinten gazdasági vagy társadalmi tevékenységben vesznek részt. Mi az alapvető oka ennek a növekedésnek: *a)* a személyes adatok cseréje a különböző tagállamokban lévő vállalkozások között emelkedő tendenciát mutat; *b)* a különböző tagállamok nemzeti hatóságai a közösségi jog értelmében kötelesek olyan mértékben együttműködni és személyes adatokat cserélni, ami lehetővé teszi számukra feladataik ellátását, vagy a fellépést egy másik tagállam hatósága nevében a belső piac által képezett belső határok nélküli térség keretében és *c)* ezenfelül a növekvő tudományos és műszaki együttműködés és az új telekommunikációs hálózatok összehangolt bevezetése.

Ugyanakkor problémaként merül fel, hogy az egyes tagállamokban végzett személyesadat-kezelés terén az egyének jogai és szabadságjogai, különösen a magántitokhoz való jog védelmének szintjei közötti eltérések akadályozhatják az ilyen adatok egyik tagállamból a másikba történő továbbítását. Ebbol eredően ezek az eltérések akadályt jelentenek számos közösségi szintű gazdasági tevékenység elvégzésében, torzítják a versenyt, és hátráltatják a hatóságokat a közösségi jog szerinti feladataik teljesítésében. A védelmi szintek közötti ezen eltérések a nemzeti törvényi, rendeleti és közigazgatási rendelkezések sokféleségének tulajdoníthatók.

Fontos elofeltétel a személyes adatok áramlása elotti akadályok elhárítása érdekében, hogy az egyének jogai és szabadságjogai védelmének szintje az ilyen adatok kezelése terén minden tagállamban azonos legyen. Mivel ez a célkitűzés alapvető fontosságú az egységes belso piac megteremtése szempontjából, de a tagállamok ezt egyedül nem tudják megvalósítani – foként a tagállamok vonatkozó jogszabályai között jelenleg fennálló eltérések miatt –, ezért össze kell hangolni a tagállamok jogszabályait annak érdekében, hogy biztosított legyen a személyes adatok határokon keresztül történő

áramlásának a RSz. 7a. cikkében meghatározott belső piac céljának megfelelő következetes szabályozása. Ezért szükséges az említett tagállami jogszabályok közelítését célzó közösségi fellépés.

Tagadhatatlan, hogy az egységesítés a fő vonal, de ezzel egyidejűleg létezik egy másik trend is. Ez utóbbin belül a tagállamok sok esetben az egyének jogai és szabadságjogai, különösen a magántitokhoz való jog védelmére hivatkozva igyekeznek akadályt gördíteni az adatvédelem harmonizációja felé. Sok tagállam megnyugvással vette tudomásul, hogy a Közösségi szintű szabályozás irányelv formájában történik, mivel ebből joggal lehet feltételezni, hogy a tagállamoknak marad annyi mozgástere, amelyet az irányelv végrehajtása során az üzleti és szociális partnerek céljaiknak megfelelően használhatnak. Ugyanakkor az irányelvvel történő szabályozás negatív hatása lehet, hogy az említett tagállami mozgástér keretein belül, és a közösségi joggal összhangban különbségek merülhetnek fel ezen irányelv végrehajtása során, ami negatív hatással lehet akár egy tagállamon belüli, akár a Közösségen belüli adatáramlásra.

A. Az irányelv célkitűzése

A személyes adatok kezelésére vonatkozó tagállami szintű jogszabályok célja az alapvető jogok és szabadságjogok, különösen a magántitokhoz való jog védelme. Ezt a premisszát mind az emberi jogok és alapvető szabadságjogok védelméről szóló európai egyezmény 8. cikke, mind a közösségi jog általános alapelvei elismerik. Ezért az említett belső jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez, sőt, magas védelmi szintet kell biztosítson a Közösségen belül. Az EK Irányelve kiegészíti az Európa Tanács 1981. január 28-i, az egyéneknek a személyes adataik gépi feldolgozása során való védelméről szóló egyezményében foglaltakat.

B. Az irányelv tárgyi hatálya

Az irányelvet az olyan személyes adatok részben vagy egészben automatizált eszközök által, illetve nem elektronikus eszközökkel történő kezelésére nézve kell alkalmazni, amelyek valamely nyilvántartási rendszer részét képezik, vagy azokat egy nyilvántartási rendszer részének szánják. Az irányelv értelmében az egyének védelme tehát a gépi adatkezelésre éppúgy vonatkozik, mint a kézi adatkezelésre. A személyiségi jogok védelme nem függhet az alkalmazott módszerektől, mivel ez megkerüléshez vezethetne. Ugyanakkor az irányelv a kézi adatkezelés tekintetében csak a nyilvántartási rendszerre terjed ki, a nem rendszerezett iratokra nem.

Ugyanakkor nem terjed ki az irányelv tárgyi hatálya az alábbi személyesadat-kezelésekre:

a) a közösségi jog hatályán kívül eső tevékenységek (pl. az Európai Unióról szóló szerződés V. és VI. címei);
b) a közbiztonságra, a védelemre, az állambiztonságra (beleértve az ország gazdasági jólétét is, ha az feldolgozási művelet állambiztonsági ügyre vonatkozik);
c) a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek;
d) a természetes személy által tisztán magáncélból, vagy otthoni tevékenység keretében végzett adatfeldolgozás.

Ugyancsak kizárt az Irányelv tárgyi hatálya alól a természetes személyek által végzett adatkezelést, amennyiben azt kizárólag személyes vagy házi használatra, például levelezés, vagy címjegyzékek vezetése során végzik.

A jogi személyek védelmére vonatkozó jogalkotás nem tartozik az EK irányelv hatálya alá.

Az újságírás, az irodalmi, vagy muvészi kifejezés céljából végzett hang-, vagy képadatok kezelését tekintve, különösen audiovizuális téren az irányelv alapelveit korlátozott módon kell alkalmazni (lásd 9. Cikkely).

Annak biztosítása érdekében, hogy az egyéneket ne lehessen megfosztani attól a védelemtol, amelyre az irányelv értelmében jogosultak, a Közösség területén végzett minden személyesadat-kezelési tevékenységet a tagállamok valamelyikének jogszabályai szerint kell végrehajtani. Következésképpen, a valamely tagállamban letelepedett adatkezelő felelőssége mellett végzett adatkezelésre ennek a tagállamnak a jogszabályai vonatkoznak. A valamely tagállamban való letelepedés magában foglalja a tevékenység tartós jellegű, tényleges gyakorlását. A letelepedés jogi formája – legyen akár egyszerűen fióktelep, akár jogi személyiséggel rendelkező leányvállalat – e tekintetben nem meghatározó tényező. Elofordul, hogy egy adatkezelő akár több tagállamban is letelepedett, főként leányvállalatok révén. Ilyenkor, a nemzeti szabályozás megkerülésének kizárása érdekében gondoskodnia kell arról, hogy minden egyes létesítménye megfeleljen a tevékenységére alkalmazandó nemzeti jogszabályok által meghatározott kötelezettségeknek.

Az is előfordul, hogy az adatkezelést valamely harmadik országban letelepedett személy végzi. Ez a tény önmagában nem gátolhatja az egyéneknek az Irányelvben elrendelt védelmét. Ilyen esetekben az adatkezelésre annak a tagállamnak a jogszabályai irányadóak, amelyben az alkalmazott eszközök találhatók, továbbá garanciákat kell találni arra, hogy EK Irányelvben meghatározott jogok és kötelezettségek a gyakorlatban is érvényesüljenek.

A tagállamok az egyének védelmének megvalósításáról gondoskodhatnak a) általános jogszabály keretében, vagy b) ágazati jogszabályokban (mint például a statisztikai intézetekre vonatkozó szabályozás).

C. Az irányelv alapelvei

Az irányelv csak alapvető elveket határoz meg – elsősorban az adatminőségre és az adatkezelésre vonatkozó elvek formájában – és ezek keretein belül minden tagállam saját hatáskörében dolgozza ki, hogy a személyes adatok kezelése milyen feltételek mellett jogszerű.

A védelem elveit minden azonosított vagy azonosítható személyre vonatkozó információ esetében alkalmazni kell. Annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására. A védelem elvei nem alkalmazhatók az olyan módon anonimmá tett adatokra, ahol az érintett a továbbiakban nem azonosítható.

1. Az alkalmazandó nemzeti jog elve

A személyes adatok kezelésére minden tagállam az irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza.

2. Az adatok minoségére vonatkozó elvek:

a) Tisztességes és törvényes adatkezelés;
b) Csak meghatározott, egyértelmű és törvényes célból lehet adatgyűjtést folytatni,és az adatok további kezelése sem végezhető e célokkal összeférhetetlen módon;[64]
c) Összegyűjtésük és/vagy további kezelésük célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek kell legyenek;
d) Pontosak, és ha szükséges, időszerűek kell legyenek; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy a pontatlan vagy hiányos adatok, tekintettel összegyűjtésük vagy további kezelésük céljaira, törlésre vagy kiigazításra kerüljenek;
e) Tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok összegyűjtése vagy további kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.[65]

3. Az adatkezelés jogszerűvé tételére vonatkozó kritériumok

A személyes adatok csak abban az esetben kezelhetőek, ha: *a)* az érintett ahhoz egyértelmű hozzájárulását adta; vagy *b)* az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; vagy *c)* az adatkezelés az adatkezelőre vonatkozó jogi kötelezettségnek való megfeleléshez szükséges; vagy *d)* kezelésük az érintett alapvető érdekei védelméhez szükséges; vagy *e)* az adatkezelés közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges, vagy *f)* a feldolgozásra az adatkezelő, vagy az adatokról tudomást szerző harmadik fél, vagy felek által felmutatott jogszerű érdekek szempontjából van szükség, kivéve, ha ezeknél az érdekeknél magasabb rendűek az egyén alapvető szabadságjogai.

Különleges adatkategóriák kezelése: Az irányelv értelmében a tagállamok szabályozása megtilthatja az olyan személyes adatok kezelését, amelyek betekintést engednek a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy filozófiai meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkozó kérdésekbe. Nem lehet alkalmazni ezt a megszorítást abban az esetben, ha: *a)* az érintett kifejezett hozzájárulását adta az említett adatok kezeléséhez, kivéve, ha a közösségi intézmény vagy szerv belső szabályai eltérően rendelkeznek; *b)* az adatkezelés az adatkezelő bizonyos jogai és kötelezettségei betartása érdekében szükséges a foglalkoztatási jogszabályok területén, amennyiben a megfelelő biztosítékokról rendel-

[64] A személyes adatok további kezelése történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat.

[65] A tagállamok állapítják meg a személyes adatok történelmi, statisztikai vagy tudományos célból, hosszabb ideig történő tárolásának megfelelő garanciáit.

kező nemzeti jogszabályok ezt lehetővé teszik, illetve *c)* az adatkezelés az érintett vagy más személy alapvető érdekeinek védelméhez szükséges abban az esetben, ha az érintett fizikailag vagy jogilag képtelen a hozzájárulását adni, illetve *d)* az adatkezelés valamely alapítvány, egyesület vagy nonprofit szervezet megfelelő biztosítékok mellett végzett törvényes tevékenysége keretében történik, politikai, filozófiai, vallási vagy szakszervezeti céllal, azzal a feltétellel, hogy a kezelés kizárólag az ilyen szerv tagjaira, vagy olyan személyekre vonatkozik, akik azzal rendszeres kapcsolatban állnak a szerv céljainak megfelelően, és az adatok nem adhatók ki harmadik fél részére az érintettek hozzájárulása nélkül, illetve *e)* az adatkezelés olyan adatokra vonatkozik, amelyeket az érintett köztudottan nyilvánosságra hozott, vagy amelyek jogi követelések megállapításához, gyakorlásához vagy védelméhez szükségesek.

Nem tiltható meg a személyes adatok kezelése akkor sem, ha az adatok kezelése megelőzési célú gyógyszer, orvosi diagnózis, gondozás vagy kezelés alkalmazása vagy egészségügyi szolgáltatások igazgatása céljából szükséges, és ha az adatokat szakmai titoktartási kötelezettség alá eső egészségügyi szakember vagy azzal egyenértékű titoktartási kötelezettség alá eső más személy kezeli.

A tagállamok határozzák meg a nemzeti azonosító számok és egyéb általános jellegű azonosító jelek kezelésének feltételeit.

4. A tájékoztatáshoz való jog

Az adatkezelőnek vagy képviselőjének legalább az alábbiakról tájékoztatnia kell az érintettet, akitől a rá vonatkozó adatokat gyűjtik, kivéve ha az érintett már rendelkezik ezen információkkal:

a) az adatkezelő, vagy ha van ilyen, képviselőjének személye;
b) az adatkezelés célja, amelyre az adatokat szánják;
c) minden olyan további adatot, mint például:
- az adatok címzettjei, illetve a címzettek kategóriái,
- hogy a kérdések megválaszolása kötelező vagy önkéntes, továbbá a válaszadás elmulasztásának lehetséges következményei,
- betekintési jog és az érintettre vonatkozó adatok kiigazításához való jog, amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatkezelés biztosításához szükségesek.

Abban az esetben, ha az adatokat nem az érintettől szerezték be, a tagállamoknak rendelkezniük kell arról, hogy az adatkezelő vagy képviselője a személyes adatok felvételének elvállalásakor, illetve, ha az adatokat harmadik személyhez szándékoznak továbbítani, legkésőbb az adatok első nyilvánosságra hozatalakor köteles az érintettel legalább az alábbi információkat közölni, kivéve, ha az érintett már rendelkezik ezekkel az információkkal:

a) az adatkezelő, vagy ha van ilyen, képviselőjének személye;
b) az adatkezelés célja;
c) bármely egyéb információ, mint például:
- az érintett adatok kategóriái,
- az adatok címzettjei vagy a címzettek kategóriái,

– betekintési jog és az érintettre vonatkozó adatok kiigazításához való jog, amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatkezelés biztosításához szükségesek.

Ez a rendelkezés nem alkalmazható, különösen a statisztikai célú vagy történelmi, vagy tudományos célú adatkezelés esetében, ha a kérdéses információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel, illetve ha a nyilvántartást vagy a nyilvánosságra hozatalt jogszabály kifejezetten előírja. Ezekben az esetekben a tagállamoknak garantálniuk kell a megfelelő biztosítékokat.

5. Az adatkezelés titkossága

Bármely, az adatkezelő vagy az adatfeldolgozó meghatalmazásával eljáró személy, beleértve magát az adatfeldolgozót is, aki a személyes adatokhoz hozzáféréssel rendelkezik, kizárólag az adatkezelő utasítása alapján kezelheti ezeket az adatokat, kivéve, ha erre őt jogszabály kötelezi.

6. Az adatkezelés biztonsága

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő műszaki és szervezeti intézkedéseket a személyes adatok véletlen vagy jogszerűtlen megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a kezelés közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen.

Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatkezelés által jelentett kockázatoknak és a védendő adatok jellegének.

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő – amennyiben az adatkezelés az ő nevében történik – köteles olyan adatfeldolgozót választani, aki a műszaki biztonsági intézkedések és az elvégzendő adatkezelésre vonatkozó szervezeti intézkedések tekintetében megfelelő garanciákat nyújt, továbbá köteles biztosítani az említett intézkedések teljesítését.

D. A felügyeleti hatóság értesítésére vonatkozó kötelezettség

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő vagy annak képviselője, ha van ilyen, értesítse a tagállam felügyeleti hatóságot akár egyetlen, akár több, összefüggő célt szolgáló, részben vagy egészen gépi úton történő adatkezelési művelet vagy műveletsorozat elvégzését megelőzően.

A tagállamok rendelkezhetnek arról, hogy az értesítési kötelezettség ne vonatkozzon arra az adatkezelésre, amelynek kizárólagos célja egy olyan nyilvántartás vezetése, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll.

E. Mentességek és korlátozások

A tagállamok jogi intézkedéseket fogadhatnak el az adatok minőségére [6. cikk (1) bek.], az érintett tájékoztatására (10. cikk), a más személytől beszerzett adatokról történő tájékoztatásra [11. cikk (1) bek.], valamint az adatkezelési műveletek nyilvánosságának biztosítására (21. cikk) vonatkozó jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás az alábbiak biztosításához szükséges: *a)* nemzetbiztonság; *b)* honvédelem; *c)* közbiztonság; *d)* bűncselekmények vagy a szabályozott foglalkozások szakmai etikája megsértésének megelőzése, nyomozása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása, *e)* valamely tagállam vagy az Európai Unió fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket; *f)* a c), d) és e) pontban említett esetekben esetlegesen a közhatalom gyakorlásához kapcsolódó ellenorzési, felügyeleti és szabályozási tevékenység és *g)* az érintett, vagy mások jogainak és szabadságjogainak védelme.

F. Az érintett kifogásolási joga

A tagállamoknak biztosítaniuk kell az érintettnek, hogy *a)* sajátos helyzetével kapcsolatos lényeges jogos érdekből bármikor kifogást emelhessen a rá vonatkozó adatok kezelése ellen. Jogos kifogás esetén az adatkezelő által kezdeményezett adatkezelés a továbbiakban nem terjedhet ki a szóban forgó adatokra és *b)* kérelemre és térítésmentesen kifogást emelhessen az olyan, rá vonatkozó személyes adatok kezelése ellen, amelyekkel kapcsolatban az adatkezelő előre jelzi, hogy feldolgozásuk célja direkt marketing, illetve hogy tájékoztassák személyes adatainak harmadik személyeknek első alkalommal történő tudomására hozása, vagy a nevükben direkt marketing céljára történő felhasználás előtt, valamint számukra az ilyen nyilvánosságra hozatal vagy felhasználás elleni kifogás jogát kifejezetten biztosítani.

G. Automatizált egyéni döntések

Az irányelv értelmében a tagállamok kötelessége, hogy minden személynek biztosítsa a jogot arra, hogy ne terjedhessen ki rájuk olyan határozat hatálya, amely rájuk nézve jogi hatással járna, vagy őket jelentős mértékben érintené, és amelynek alapja kizárólag gépi adatkezelés, amelynek célja a rá vonatkozó egyes olyan személyes szempontok kiértékelése, mint például a munkahelyi teljesítmény, a hitelképesség, a megbízhatóság, az életvitel stb.

Ugyanakkor a tagállamok úgy is rendelkezhetnek, hogy az említett határozat hatálya kiterjedhet a személyre, amennyiben a határozatot:

a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve, hogy az érintett által a szerződés megkötése vagy teljesítése iránt benyújtott kérelmet teljesítették, vagy jogos érdekének biztosítására megfelelő biztosítékok állnak rendelkezésre, mint például a véleményének kinyilvánítását lehetővé tevő intézkedések; vagy
b) olyan jogszabály teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja.

H. Felelősség

Mindenki, aki törvénytelen adatkezelési művelet vagy az adatvédelmi irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett károkért. Az adatkezelő részben vagy egészben mentesül e felelősség alól, ha bizonyítja, hogy a kárt okozó eseményért nem felelős.

I. A személyes adatok harmadik országokba irányuló továbbítása

A tagállamoknak rendelkezniük kell arról, hogy a feldolgozásra kerülő vagy továbbítás után feldolgozásra szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül az adott harmadik ország megfelelő védelmi szintet tud biztosítani.

A fenti tilalomtól eltérően, és amennyiben az adott esetre vonatkozó belföldi jogszabályok másképp nem rendelkeznek, a tagállamok rendelkeznek arról, hogy a személyes adatok olyan harmadik országba irányuló továbbítása vagy továbbítás-sorozata, amely nem biztosít megfelelő szintű védelmet, csak a következő feltételek mellett történhet:

a) az érintett egyértelműen hozzájárulását adta a tervezett továbbításhoz; vagy
b) a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; vagy
c) a továbbítás az adatkezelő és valamely harmadik fél közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; vagy
d) a továbbítás fontos közérdekből vagy jogi követelések létrejötte, érvényesítése vagy védelme miatt szükséges, illetve azt jogszabály írja elő; vagy
e) a továbbítás az érintett alapvető érdekeinek védelme miatt szükséges; vagy
f) a továbbítást olyan nyilvántartásból végzik, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, amennyiben a jogszabályok által a betekintésre megállapított feltételek az adott esetben teljesülnek.

J. Az adatvédelem intézményrendszere

1. A tagállamokban működő felügyeleti hatóság

Minden tagállamnak létre kell hoznia egy felügyeleti hatóságot, amelynek feladata az adatvédelmi irányelvből a tagállam által elfogadott nemzeti rendelkezéseknek a területén történő alkalmazásának az ellenőrzése. E hatóságok a rájuk ruházott feladatok gyakorlásában teljes függetlenségben járnak el.

A hatóságok különösen a következő jogosultságokkal rendelkeznek:

a) nyomozati jog (pl. az adatkezelési műveletek tárgyát képező adatokhoz való hozzáférés joga, továbbá a felügyeleti feladatok ellátásához szükséges adatok gyűjtésének joga),

b) tényleges beavatkozási jogosultság (pl. az adatok zárolásának, törlésének vagy megsemmisítésének elrendelése, az adatkezelés átmeneti vagy végleges tilalmának megállapítása, az adatkezelő figyelmeztetése vagy megrovása, illetve az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése stb).

c) bírósági eljárásban való részvétel joga (az irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén, továbbá e jogsértések igazságügyi szervek elé terjesztésének joga).

A felügyeleti hatóság kifogásolható határozatai bíróság előtt megtámadhatók.

A felügyeleti hatóságok foglalkoznak a személyes adatok kezelése vonatkozásában az egyének jogainak vagy szabadságjogainak védelmével kapcsolatos, bármely személy vagy az őt képviselő szervezet által benyújtott kérelmekkel. A kérelem elbírálásáról az érintett személyt értesíteni kell.

A felügyeleti hatóságoknak foglalkozniuk kell különösen az adatkezelés törvényességének ellenőrzésére irányuló, bármely személy által benyújtott kérelemmel, amennyiben az ezen irányelv 13. cikkének értelmében elfogadott nemzeti rendelkezések alkalmazhatóak. Az érintett személyt mindenképpen értesíteni kell, ha az ellenőrzés megtörtént.

2. A személyes adatkezelés vonatkozásában az egyének védelmével foglalkozó munkacsoport

Az adatvédelem intézményrendszerének egy másik megjelenési formája az egyének védelmével foglalkozó munkacsoport. A munkacsoport tanácsadói státuszban működik és függetlenül jár el. A munkacsoport az egyes tagállamok által kijelölt felügyeleti hatóság vagy hatóságok képviselőjéből, a közösségi intézmények és szervek nevében létrehozott hatóság vagy hatóságok képviselőjéből, továbbá a Bizottság egy képviselőjéből áll. A munkacsoport minden egyes tagját az az intézmény, hatóság, vagy hatóságok jelöli vagy jelölik ki, amelyet, illetve amelyeket képvisel. Ha a tagállam több felügyeleti hatóságot jelöl ki, ezek közös képviselőt állítanak. Ugyanez vonatkozik a közösségi intézmények és szervek nevében létrehozott hatóságokra is.

A munkacsoport hatásköre:

a) megvizsgál minden, az irányelv értelmében elfogadott nemzeti intézkedések alkalmazása körébe tartozó kérdést azok egységes alkalmazása érdekében;

b) véleményt nyilvánít a Bizottságnak a Közösség és a harmadik országok védelmi szintjéről;

c) tanácsot ad a Bizottságnak az adatvédelmi irányelv javasolt módosításaira;

d) véleményt nyilvánít a közösségi szinten kidolgozott eljárási szabályzatokról.

A munkacsoport saját kezdeményezésére ajánlásokat tehet bármely kérdésben, amely a személyes adatok közösségen belüli kezelése tekintetében a személyek védelmével kapcsolatos. A munkacsoport véleményeit és ajánlásait továbbítani kell a Bizottsághoz, valamint a 31. cikkben említett bizottsághoz.

3. A közösségi szintű intézményi védelem: A bizottság

A Bizottságot a tagállamok képviselőibol álló bizottság segíti, amelynek elnöke a Bizottság képviselője. A Bizottság képviselője tervezetet nyújt be a bizottságnak a meghozandó intézkedésekről. A bizottság véleményt nyilvánít a tervezetről az elnök által az ügy sürgősségének megfelelően megállapított határidőn belül.

3.3. A személyiségi jogok védelme – különös tekintettel az adatvédelemre – néhány skandináv államban, különös tekintettel az EU-s adatvédelmi irányelv rendelkezéseire

A skandináv országokon belül a legszisztematikusabb és legkidolgozottabb – a személyiségi jogok (magánszféra) védelmére vonatkozó – jogelvekkel a norvég „privacy interest model", vagy mászóval a norvég magánszféra jogi védelmének az elmélete (theory of privacy protection – personvern) rendelkezik. A modell lényege a következő: *a)* statikus elem: a rendszer számbaveszi az alapvető emberi jogokat, illetve az ezeket tartalmazó dokumentumokat (pl. Human Rights Convention of the European Council) és *b)* dinamikus elem: egyenként megvizsgálja, hogy a kérdéses magatartás, mulasztás, stb. vajon a rögzített emberi jogok keretei közé esik vagy sem. Ennek a megoldásnak az elvi alapja, hogy minden egyes ember magánszféráját megilleti valamilyen szintű jogi védelem.

Ez a „privacy-odell" döntésorientált (decision orientated). A személyes adatok szolgálnak alapul ahhoz, hogy a munkáltató képes legyen meghozni a döntését. A rendszer lényege, hogy a konkrét szituációktól függően, illetve az adott viszony keretei között mérlegelve hozza meg az arra jogosult a döntését. Az érdekek pontos és körültekintő mérlegelését követően dönthető el, hogy az adott információ milyen viszony, illetve helyzet keretében szolgáltatható ki. Az adott munkavállalóról rendelkezésre álló személyes adat lesz az alapja a vele összefüggésben meghozott döntés alapja.

A modell a különböző egyéni és közérdek érvényesítésére szolgál.

A. Az egyéni érdekek leggyakrabban az alábbi három formában jelennek meg: *a)* az információk bizalmas kezelése (confidentiality) – az egyén érdeke ahhoz fűződik, hogy ellenőrizhesse a rá vonatkozó adatok gyűjtését és felhasználását; ugyanakkor ez nem jelent teljes mértékű kontrollt, hanem alapvetően azt kívánja elérni, hogy ne lehessen beleegyezés nélkül adatot gyűjteni és felhasználni; *b)* a döntéshez leginkább megfelelő adat szolgáltatása – adekvátság: ezen belül további két kérdést kell megvizsgálni: *ba)* relevancia (A kért, illetve szolgáltatott információnak az adott kérdés eldöntéséhez relevánsnak kell lennie. A nem releváns adatokat nem lehet kérni, illetve nem kell szolgáltatni. Példálózó jelleggel megemlítünk néhány esetet, amikor nem releváns az adat: már túlságosan elavult, vagy az adott kérdéshez nem kapcsolódik igazán; például a legtöbb esetben a politikai, vallási hovatartozás vagy a nemhez kapcsolódó kérdések irrelevánsak. Ez utóbbi példa jól szemlélteti a személyiségi jogok védelme és a diszkrimináció ellenes jogalkotás közeli kapcsolatát.); *bb)* a megfelelőség (adekvátság) elve, vagyis a szolgáltatott adatnak mindenkor korrektnek kell lennie. Önmagában egy helyesen szolgáltatott adat is lehet nem megfelelő, ha a többi releváns – de a másik fél által nem ismert – tényt nem közöljük. Ezért a megfelelőség (adekvátság) elvét a jóhiszemű együttműködés elvével kell összekapcsolni. *c)* A harmadik egyéni érdek, ami megjelenik: a személyhez kötöttség (access), vagyis a szolgáltatott adat az illető személyre vonatkoz-

zon. Magától értetődik, hogy a fent említett érdekek egymással nagyon szoros összefüggést mutatnak.

B. A közérdek megjelenése. *a)* A társadalom tagjaiban megfogalmazódik az igény arra, hogy kontrollálhassák a rájuk irányuló megfigyelés szintjét (controlling the surveillance level in society). *b)* Életerős társadalom létrehozása (robust society). Ez magában foglalja azon gyengeségek kiküszöbölését, amelyek az információs társadalomban – a különböző adatbankok létrehozásakor, vagy hálózatok, illetve információs sztrádák kiépítésekor – fordulhatnak elő. *c)* A harmadik érdek, egy jóindulatú, jóakaratú igazgatás kiépítése. A privát szférában ennek a megtestesítője a közigazgatás, míg a munka világában ezt az igazgatási funkciót a munkáltató látja el és ezért vele szemben kell törekedni a munkavállalók védelmére.

Mint ahogy azt a magánérdek vonatkozásában jeleztük, a magánérdekekhez hasonlóan a közérdek egyes megtestesítői is egymással szoros kölcsönhatásban vannak, sőt az is bátran kijelenthető, hogy a magánérdek és a közérdek is kölcsönös egymásra hatásban állnak egymással. Ugyanakkor a jogalkotás vagy döntéshozatalkor megfigyelhető, hogy az egyes elvek között ésszerű és kompromisszumra hajló engedményeket kell tenni.

A munkavégzéssel kapcsolatos személyiségi jogok fejlődését vizsgálva megállapítható, hogy ebben meghatározó szerepe van – különösen a skandináv országokban – a kollektív szerződésnek. Történelmileg teljesen nyilvánvaló volt, hogy a munkáltató saját kiváltságának tartotta a munkavégzés feltételeinek – beleértve a kollektív szerződés végrehajtását is – a teljes körű kontrollját. Ez természetesen nem volt ennyire magától értetődő a munkavállalók számára. Ezért e vonatkozásban számos összetűzésre és érdekellentétre került sor. A munkáltatók korlátlan ellenőrzési és megfigyelési jogát is magában a kollektív szerződésben rögzítették. A nagy kérdés természetesen az volt, hogy milyen elvek figyelembe vételével határozzák a határvonalakat: mi az ami még megengedett és mi az ami már nem. Ezt nevezték az „arányos akciók kívánalmának" (requirement of proportionate actions), amely elv az objektíve indokolható megfigyelést tartotta jogszerűnek (reasonable objectives of surveillance). Ugyanakkor sem a jogalkotás, sem a bírói gyakorlat, sem pedig a kollektív szerződéskötési gyakorlat nem feltétlenül ismeri el ezt az elvet: kimondják, hogy a munkáltató megfigyeléshez és az ellenőrzéshez való joga nem legitimizál minden egyes munkáltatói magatartást. Vagyis nem jelenti azt, hogy minden a munkáltató által szükségesnek tartott akció egyidejűleg automatikusan jogszerű is lesz. Milyen elvek sietnek a munkavállalók segítségére:*a)* arányos magatartás (proportionate measures); *b)* adekvát magatartás (adequate measures); c) megfelelő munkaerőpiaci standardok, amelyek képesek felvenni a harcot a munkáltatói túlerővel szemben (good labour market standards) stb.

Alapvetően a fentiekben tárgyalt szempontok különböző konstellációja alakítja napjaink magánélet, illetve ezen belül az adatvédelemre vonatkozó normatív szabályozásának főbb vonalait.[66]

Finnország: A munkáltató megfigyeléshez való joga a munkaszerződés és az új munkaszerződésről rendelkező törvény[67] figyelembe vételével határozható meg. A jogszabály nem tartalmaz erre vonatkozó részletes előírásokat. Figyelembe véve a hagyomá-

[66] ANDERS VON KOSKULL: Employment Privacy Protection – Scandinavian Comparative Perspectives; in. *Stability and Change in Nordic Labour Law*, ed. Peter Wahlgren, Scandinavian Studies in Law Volume 43, Stockholm Institute for Scandinavian Law, Stockholm 2002, pp.335–339.

[67] 2001. évi 55. sz. törvény (2001. július 1-én lépett hatályba.).

nyokat, nem jogi normában szabályozott elv, hogy a megfigyelésnek korrektnek kell lenni és csak odáig terjedhet, ameddig a munkáltató objektíve igazolható érdekeit szolgálja. Másszóval: nem lehet rosszhiszeműen visszaélni ezzel a lehetőséggel.

Azt is meg kell említeni, hogy Svédországban 2002. március 5-én terjesztettek elő megvitatásra egy tanulmányt, amely a leendő munkavállalói személyiségi jogok védelmét szolgáló speciális törvény alapja lehet. Az ebben a tervezetben szereplő kérdések és célkitűzések hasonlítanak a fent említett finn törvényhez. Ugyanakkor e kérdésben is fontos szerepet szán a szociális partnereknek, hogy a kollektív szerződésekben határozzák meg a jogviszony alanyait megillető jogokat és terhelő kötelezettségeket.

Finnországban az EU-s irányelv végrehajtására elfogadtak egy törvényt a munkavállaló személyiségi jogainak a védelméről[68] (Act on Protection of Privacy in Working Life). A törvény bevezető rendelkezései között megemlíti, hogy a finn szabályozásnak túl kell lépnie az EU-s irányelv előírásait. A kiindulási pont az volt, hogy az általános adatvédelmi törvény nem képes teljes mértékben megfelelni a munkaerőpiac résztvevői elvárásainak. A kettő közötti kapcsolat: a munkavállalók személyiségi jogait védő törvényt kell elsősorban alkalmazni és ha az általános adatvédelmi törvénnyel konkurenciába kerülne, akkor a speciális szabály megelőzi az általános szabályt, vagyis a munkavállalók személyiségi jogait védő törvényt kell először alkalmazni. Jelenleg a finn munkavállalók személyiségi jogait védő törvény egyedülálló szabályozás az EU-ban, mivel nincs olyan másik tagállam, amelyben ilyen széles körben védenék a munkavállalók személyiségi jogait. Minden bizonnyal a jövőben a többi tagállam is követi a jó példát. Ugyanakkor azt is meg kell jegyezni, hogy a finn törvény a címében jelzett kérdéskörnél szűkebb tárgyi hatállyal rendelkezik. A törvény a következő fontosabb kérdésekről rendelkezik: a munkavállalóról történő adatgyűjtés; személyiségi és értékelési teszt; egészségügyi – beleértve alkohol és drog – vizsgálat és genetikai teszt; a munkavállalók tevékenységének technikai eszközökkel történő megfigyelése, ezen belül az e-mail és egyéb telekommunikációs eszközök használatának az ellenőrzése.

Azt már korábban említettük, hogy a törvény általában konkrét anyagi jogi normákat nem ír elő az egyes jogintézmények működésére nem határozza meg konkrétan, hogy a munkáltató mit tehet és mit nem stb. A törvényben szereplő szabályok sokkal inkább a munkáltató elvárható és megengedhető viselkedését behatároló minőségi standardok és eljárási szabályok. Például, rendelkezik arról, hogy milyen forrásokból szerezhetők be a munkavállalókra vonatkozó adatok, de nincs utalás a megfigyelés technikájára. Csak az információra és a megállapodásra vonatkozó szabályokat találjuk meg.[69]

A finn példán kívül az EU-ban még több helyen is megjelenik az a törekvés, hogy a munkavállalók személyiségi jogait és méltóságát védjék. Például a Data Protection Working Party Opinion 8/2001 29. cikkelye, amely a foglalkoztatással összefüggő személyes adatok feldolgozásáról szól (Brüsszel, 2001. szeptember 13.), vagy a Social Policy Agenda of the Commission (COM2000/379 final, 28.6.2000), amely az alapvető szociális jogok tiszteletben tartásáról és fejlesztéséről szól, mert ez kulcsfontosságú tényező egy igazságos társadalom felépítéséhez, amelyben tisztelik az emberi méltóságot, beleértve a munkavállalók személyiségi jogainak a védelmét is.

[68] 2001. évi 477. sz. törvény (2001. október 1.).
[69] ANDERS VON KOSKULL, 2002, pp.344–346.

3.3. A személyes adat védelemről rendelkező 95/46/EC irányelvének gyakorlati összefüggései

A személyes adatok védelmére vonatkozó jogi szabályozás számos vonatkozásban érinti a munkavállalók megfigyelését. Attól a perctől kezdve, hogy a személyes adatok beszerzésre és felhasználásra kerülnek a személyes adatok védelmét szolgáló jogszabályokat – beleértve az EU-s irányelvet is – alkalmazni kell. Az irányelv rendelkezéseinek a végrehajtása nem minden esetben egyértelmű. Például, a manuális adatfeldolgozás (manual processing of personal data) kérdése; vagy a 2 (c) cikkely értelmében rendszerezett adatállománynak (structured set of data) teinthető-e a titkár/nő asztalán heverő írásban benyújtott pályázat; vagy ahhoz, hogy személyes adatgyűjtő rendszerről (personal data filing system) beszéljünk szükség van-e több személy adataira. Ugyancsak jogalkalmazási problémát vet fel a személyes adatok védelmére vonatkozó 96/46/EGK irányelv és a telekommunikációs szektorban a személyiségi jogok védelmét szabályozó 97/66/EGK irányelv kapcsolata. Jelenleg ez a kérdés az EU szintjén sem került kellőképpen tárgyalásra.[70]

Az Európai Unió Adatvédelemmel foglalkozó biztosa (Data Protection Comissioner) az információs technológia és telekommunikáció munkahelyi alkalmazásából eredő problémák kiküszöbölése érdekében számos ajánlást fogalmazott meg. Ezek a problémák túlnyomó többségében a munkahelyeken a munkavállalóra vonatkozó adatok védelmére vonatkoznak. A munkaviszony létesítése és fennállása során – kölcsönösen – számos információ jut a szerződő felek tudomására. Ezen információk védelméhez mindkét félnek nyomós indoka fűződik. A közelmúltban bekövetkező robbanásszerű információs robbanás megsokszorozta a lehetőségét és a ténylegesen összegyűjtött adatok számát. Leegyszerűsödtek az eljárások, az adatfeldolgozás gyorsabbá vált. Ugyanakkor ezt a felgyorsult folyamatot nem követte ugyanilyen sebességgel a munkavállalók adatainak, illetve az ehhez kapcsolódó személyiségi jogoknak a védelme.

Ugyanakkor kialakult néhány új gyakorlat. Lehetséges a munkavállalók tevékenységének – különböző szempontok és célok szerinti – folyamatos megfigyelése és a róluk történő adatok gyűjtése, még akkor is, ha erről ők nem is tudnak. Az ilyen jellegű megfigyelések gyakorlata egyre szélesebb körben terjed és – bizonyos megszorítások között – egyre inkább elfogadottá válik. Milyen indokok állnak ennek a hátterében: *a)* az ilyen jellegű megfigyeléseket elsősorban a munkavállalók biztonsága indokolja, továbbá *b)* a megfigyelések tapasztalatainak elemzése után a munkavégzés hatékonyságát és ennek eredményeként a termelékenységet (ergonómiai szempontok) lehet növelni, *c)* hatalmas információbázis gyűjthető a munkavállalók viselkedéséről, személyiségéről és tevékenységéről.

Ezzel a pozitív megközelítéssel szemben a munkavállalókról összegyűjtött és a munkáltató vagy esetleg külső harmadik személy számára rendelkezésre álló hatalmas információmennyiség sebezhetővé teszi a munkavállalót és sértheti a személyiségi jogait. Ezért van szükség a személyes adatok jogi védelmére.

Felmerülhet a kérdés, hogy mit értünk munkahely alatt. A vonatkozó EU-s megközelítés értelmében a munkahelyet kiterjesztően kell értelmezni: minden olyan lehetséges hely munkahelynek minősül, ahol a munkavállaló – munkáltatói utasításra – a munka-

[70] Erre a megállapításra egy 2001. október 4–5 között, Frank professzor elnökletével lezajlott jogi szakértőkből álló kerekasztal konferencia résztvevői jutottak.

végzési tevékenységét folytatja. Ez lehet a munkáltató telephelye, a munkavállaló gépkocsija vagy esetleg a saját lakása (kiváló példa lehet erre az egyre jobban terjedő telemunka típusú munkavégzés).

A munkavállalók személyiségi jogainak védelmét szolgáló jogi normák alulreprezentáltak az egyes országok munkajogi szabályozásában. Ezért fontos szerephez jutnak a nemzetközi és az EU-s normák. Segítik a jogalkotókat, de egyidejűleg segítenek a munkáltatóknak is abban, hogy kialakuljon egy kulturált munkavégzési környezet.

3.4. Ajánlások az EU irányelv alkalmazásához és a továbbfejlesztéséhez

a) A munkavállalók képviselőinek bevonása – A munkavállalók képviselőit teljes körűen tájékoztatni kell minden bevezetendő olyan új információs rendszerről,amelynek a rendeltetése, hogy a munkavállalókat megfigyelje, róluk információkat gyűjtsön. A munkavállalói képviselőknek biztosítani kell, hogy bármikor meggyőződhessenek arról, hogy a munkahelyi belső szabályok rendelkeznek a munkavállalók személyiségi jogainak a védelméről. Rendszeres információcserét és tárgyalásokat kell folytatni annak érdekében, hogy olyan új információs technológiák kerüljenek bevezetésre, amelyek lehetővé teszik a munkavállalók személyiségi jogainak a védelmét. A munkahelyen működő információs rendszerekben jelentős változást csak a munkavállalók képviselőinek egyetértésével lehessen bevezetni.

b) A munkavállalók tájékoztatása – Az olyan munkahelyeken, ahol adatgyűjtés, illetve megfigyelés miatt elektronikus rendszereket (számítógéphálózat, audió-video rendszer, stb) alkalmaznak a munkavállalókat előre tájékoztatni kell az adatgyűjtés (megfigyelés) céljáról, a gyűjtött adatok felhasználásának módjáról és céljáról, az alkalmazott módszerről (technikáról, rendszerről), a gyűjtött adatok jellegéről, azon személyek köréről, akik ezekhez az adatokhoz hozzáférhetnek és annak a lehetőségéről, hogy miként eszközölhetnek helyesbítést a rendszer által gyűjtött adatokban, ha azok hibásak. A betekintéshez és az esetleges hiba esetén a kijavításhoz való jogot egy jól behatárolható időszakon belül kell biztosítani.

c) A munkáltatónak informálnia kell a munkavállalóját a munkahelyen alkalmazott információs-rendszer megjelenési formáiról (pl. e-mail vagy hangposta stb) felhasználási rendjéről. Ugyancsak informálnia kell a munkavállalót az összegyűjtött adatok felhasználásának elveiről, céljáról és módszeréről.

d) A munkáltatónak tiszteletben kell tartania a munkavállaló személyiségi jogait. Létezik a munkavállaló személyiségi jogaival kapcsolatos legitim elvárási szint, amit tiszteletben kell tartani. Az elvárási szint megítélése minden esetben az adott munkahely sajátosságainak megfelelően alakul. Az elvárási szint magasabb lesz egy zárt munkahelyen, mint egy nyitott munkahelyen.

e) Szükséges és indokolt adatgyűjtés – A munkahelyeken csak jogszerűen lehet adatot gyűjteni és felhasználni. Az adatok felhasználásának mindig korrektnek kell lennie és soha nem sértheti a munkavállalók emberi méltóságát. Az adatgyűjtésnek szükségesnek, arányosnak és adekvátnak kell lennie, amelyet a jóhiszeműség és a a szakmai szükségszerűség vezérel. Az adatokat csak olyan mértékig és időtartamig lehet gyűjteni, amely az elérendő cél megvalósítása érdekében indokolható.

f) Személyhez köthető anyagok gyűjtése – Az adatgyűjtés során a munkáltatónak minden esetben ügyelnie kell arra, hogy tartózkodjon az olyan jellegű információk, adatok gyűjtésétől, amelyek nem kapcsolódnak közvetlenül a munkavégzéshez. Nem kapcsolódnak közvetlenül a munkavégzéshez azok az adatok, amelyek például a a munkavállaló személyes viselkedésére, személyiségjegyeire, vagy a munkahelyen belüli, illetve kívüli személyes kapcsolataira vonatkoznak.

g) A személyes adatok felhasználása a munkavállalóval szemben – A különböző módszerek segítségével összegyűjtött adatok nem használhatók fel a munkavállalókkal szemben. A munkavállalóról rendelkezésre álló adat csak abban az esetben használható fel vele szemben, ha a neki már korábban lehetősége volt arra, hogy ezeket az adatokat megismerje és alkalmazhassa őket.

h) A munkavállalók rejtett megfigyelésének a tilalma – Csak kivételes esetben indokolható az olyan adatgyűjtés, illetve felhasználás, amelyről az érintett munkavállalónak nincs előzetes tudomása, illetve amely eltér az előre jelzett célkitűzéstől. Az információt az érintett személy előzetes és írásbeli belegyezésével lehet jogszerűen gyűjteni, illetve felhasználni. Ennek az írásbeli nyilatkozatnak a következő kérdéseket kell tartalmaznia:

– az okok és célok megjelölése;

– az összegyűjtendő információ természetére vonatkozó kitételek.

Megjegyezzük, hogy az adatgyűjtésről, illetve felhasználásról nemcsak magát a munkavállalót, hanem a munkavállaló érdekképviseleteket is tájékoztatni kell.

i) Megfigyeléstől mentes övezet kijelölése – A munkáltatónak garantálnia kell azt, hogy létezik a munkahelyen belül egy olyan térség, ahol a személyiségi jogai semmilyen adatszerzéssel nem kerülnek veszélybe. Világosabban fogalmazva ez annyit jelent, hogy van a munkahelyen belül egy olyan tér (szoba, folyosó, stb), ahol a munkavállaló szabadon – a megfigyelés veszélye nélkül – beszélgethet a munkatársaival.

Záró megjegyzések

Az 1970-es évek a személyes adatok gyűjtésével és felhasználásával kapcsolatos intenzív magánélet-védelmi kutatás és jogalkotás kezdeti időszaka volt. A dolgozatban utalunk arra, hogy ez nem teljesen előzmények nélküli munka volt. Számos hivatalos jelentés tanúsítja, hogy e problémát politikai szinten is komolyan veszik, de ezzel egyidejűleg azt is, hogy az egymásnak ellentmondó érdekek kiegyensúlyozása kényes feladat, és aligha oldható fel egyszer s mindenkorra. A közvélemény hajlik arra, hogy leginkább a számítógépes adatfeldolgozás következményeire és az abban rejlő kockázatra összpontosítson. Ezzel párhuzamosan az egyes országok jogalkotói is azt választották, hogy kizárólag számítógépekre és számítógépekkel támogatott tevékenységekre vonatkozó jogszabályokat alkottak. Ezzel szemben, más országok a magánélet védelmének általánosabb megközelítését választották, függetlenül az alkalmazott adatfeldolgozási módszertől. A magánszféra védelmére vonatkozó normatív szabályozás olyan, az egyént védő biztosítékokat jelent, amelyek megelőzik a magánélet klasszikus értelemben vett megsértését, mint pl. intim személyes adatok nyilvánosságra hozatalát vagy az azokkal való visszaélést. Ugyanakkor felszínre kerültek a magánszféra védelméhez többékevésbé közvetlenül kapcsolódó egyéb védelmi igények is, mint például: *a)* a nyilvántar-

tók azon kötelessége, hogy a közvéleményt az adatkezeléssel kapcsolatos tevékenységről tájékoztassák; *b)* továbbá az adatalanyok joga arra, hogy a rájuk vonatkozó adatokat kiegészíthessék vagy módosíthassák Általánosságban szólva, törekvés tapasztalható a magánélet hagyományos értelmezésének(a „békén hagyatáshoz" való jog) bővítésére, és az érdekek szintézisének összetettebb értelmezésére, amelyet már inkább „magánélet és személyes szabadságok"-nak kellene nevezni.

Az automatizált adatkezelés jogi problémái terén a magánélet és a személyes szabadságjogok védelme talán a legvitatottabb kérdés. Annak hogy ez a kérdés ilyen széles körben kelt figyelmet, elsődleges oka a számítógépek mindenhol elterjedt használata a személyes adatok feldolgozásában, a tárolás, az összehasonlítás, az összekapcsolás, a kiválasztás és a hozzáférés jelentősen megnövekedett lehetőségei, valamint a számítógépek és a távközlési technikák kombinációja, amely lehetővé teszi, hogy személyes adatokhoz földrajzilag szétszórt felhasználók ezrei férhessenek hozzá egyidejűleg, és amely ugyancsak megvalósíthatóvá teszi az adatgyűjtés központosítását és komplex országos és nemzetközi adathálózatok létrehozását. Egyes problémák különösen sürgős figyelmet kívánnak, például azok, amelyek a nemzetközi adathálózatok megjelenésével, valamint azzal az igénnyel kapcsolatosak, hogy egyensúly jöjjön létre egyfelől a magánélet, másfelől az információszabadság egymással versengő érdekei között annak érdekében, hogy a modern adatfeldolgozás lehetőségeit a kívánatos mértékig ki lehessen használni.

Fontos kiemelnünk, hogy a magánszféra – ezen belül is a munkavállalók magánszférájának – védelme nemcsak a belső (nemzeti) jogokban, hanem a nemzetközi normaalkotás szintjén is megjelent. Ezek utóbbiak közül a leginkább mértékadó szervek normáival – Európa Tanács, OECD és Európai Közösség – részletesen is foglalkoztunk a dolgozatban. A globalizált gazdaságban valószínűsíthető, hogy az államok feletti normaalkotás szerepe a jövőben is tovább növekszik.

Felhasznált irodalom

Beddard, Dr. Ralph: Human Rights and Europe, Third Edition, Cambridge, Grotius Publications Limited, 1993.

Berkeley Journal of Employment and Labor Law, Vol.17(1), 1996.

Berkeley Journal of Employment and Labor Law Vol.19(1), 1998.

Bowers, John: Employment Law, Blackstone Press Limited, 1997.

Brearley, Kate: Employment Covenants and Confidential Information: Law, Practice and Technique London, 1993.

Doherty, Robert E.: Industrial and Labor Relations Terms: a Glossary ILR Press, New York State School of Industrial and Labor Relations Cornell University, Ithaca, NY 1979., 1989.

Duston,Robert L.; Russel, Karen S.; Shepard, Michael: Workplace Privacy Washington D.C.,1989.

Employee Relations Law Journal Vol. 24(1), Summer 1998.

Employee Relations Law Journal, Vol.24(3) Winter 1998.

European Journal of Law and Economics, Kluwer Academic Publishers, 1999.

European Union Review, IDS Employment Europe 458 Febr. 2000.

Finkin, Matthew W.: Privacy in Employment Law, Washington, D.C.
Gold, Michael, Evan: An Introduction to the Law of Employment Discrimination ILR Bulletin 68, ILR Press, 1993. New York State School of Industrial and Labor Relations Cornell University.
Hayden, Trudy; Hendriks, Evan; Novik, Jack D.: Your Right to Privacy, Southern Illinois Univ. Press, Carbondale, 1990.
IDS Employment Europe 457 January 2000.
International Encyclopedia of Comparative Law Volume XV. Chapter 15, 1997.
Journal of Individual Employment Rights, Vol.5(3) 235–249, 1996–97.
Journal of Individual Employment Rights,Vol.6(2) 103–117, 1997–98.
Journal of Individual Employment Rights,Vol.6(3) 179–191, 1997–98.
Journal of Individual Employment Rights,Vol.6(3) 193–199, 1997–98.
Journal of Individual Employment Rights,Vol.7(3) 215–226, 1998–99.
Journal of Individual Employment Rights,Vol. 8(2) 125–142, 1999–2000.
Legal Issues of European Intergration 1996/1, Kluwer Law International.
Legal issues of European integration 1992/1, Kluwer Law and Taxation Publishers.
McWhirter, Darien A.: Your Rights at Work c. Könyvből részlet (The Rights to Privacy), John Wiley and Sons, Inc., 1993.
Neal,Alan C.: European Labour Law and Social Policy (Cases and Materials) Kluwer Law International,1999.
Palmer, Camilla: Discrimination at Work – the Law on Sex and Race Discrimination Second edition, Legal Action Group, 1992.
Randall, Nicholas; Smith, Ian: A Guide to the Employment Relations Act 1999, London, 1999.
The Labor Lawyer 107, 1997.
Transfer European Review of Labour and Research, Vol. 1–2. Spring–Summer, 1999.
Transfer European Review of Labour and Research, Vol. 5(3) Autumn, 1999.
Wacks, Raymond: Personal Information, Privacy and the Law, Oxford,1989.
Wahlgren, Peter ed.: Stability and Change in Nordic Labour Law; Scandinavian Studies in Law, Volume 43; Stockholm Institute for Scandinavian Law, Stockholm 2002
Whincup, Michael: Modern Employment Law – A Guide to Job Security and Safety Ninth edition Butterworth and Heinemann, 1997.
Wright, Becky A.: Employee Benefit Plans: A Glossary of Terms Brookfield, Wisconsin 1984.

JÓZSEF HAJDÚ

THE PROTECTION OF WORKER'S PRIVACY, WITH SPECIAL ATTENTION TO DATA PRIVACY

(Summary)

Privacy has become one of the most important human rights issues of the modern age. At a time when computer based technology gives government and private sector organisations the ability to conduct mass surveillance of populations, privacy has become a crucial safeguard for individual rights. According to opinion polls, concern over privacy violation is now greater than at any time in recent history. Uniformally, populations throughout the world report their distress about encroachment on privacy, prompting an unprecedented number of nations to pass laws which specifically protect the privacy of their citizens.

The basis for this legal activity rests on a growing understanding that privacy is a fundamental right. Privacy is a process which underpins human dignity and other key values such as freedom of association and freedom of speech. These rights are established squarely in international covenents, and protected specifically in the constitutions of many nations. The increasing sophication of information technology, with its capacity to collect, analyse and disseminate information on individuals, has introduced a sense of urgency to the demand for legislation.

New developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system.

As the pages of this report make clear, rapid advances in the development of powerful technology, in conjunction with the demand for greater management efficiency, are promoting a seamless web of surveillance throughout the workplace. At the same time, inadequate laws and regulations are failing to check an expanding pattern of abuses.

Employees in nearly all sectors are vulnerable to comprehensive surveillance by managers. Legal protections are generally lax in such circumstances because surveillance is frequently imposed as a condition of employment. The changing structure and nature of the workplace has facilitated an increasing level of surveillance.

The technology being used to monitor employees is extremely powerful, and extends to every aspect of a workers life. Miniature cameras monitor behaviour. "Smart" ID badges track an employees movement around a building. Telephone Management Systems (TMS) analyse the pattern of telephone use and the destination of calls. Psychological tests general intelligence tests, aptitude tests, performance tests, vocational interest tests, personality tests and honesty tests – many of which are electronically assessed – raise a great many issues of privacy, control and fairness. Surveillance and monitoring have become design components of modern information systems and the modern work environment.

The use of this technology is often justified on the grounds of health and safety, customer relations or legal obligation. The real purpose of most surveillance, however, is for performance monitoring, personnel surveillance, or outright discrimination. Even in workplaces staffed by highly skilled information technology specialists, bosses demand the right to spy on every detail of a worker's performance. Modern networked systems can interrogate computers to determine which software in being run, how often, and in what manner. A comprehensive audit trail gives managers a profile of each user, and a panorama of how the workers are interacting with their machines.

In this article we deal with the basic questions of privacy: definitions, structure of regulations (international and national norms or even soft-laws), basic theory of worker's privacy. The second part of the article introduce the most important and influencial international norms of data privacy: the norms of OECD, Council of Europe and European Community.

Nyomás és kötés: OFFICINA Press Kft.
6721 Szeged, Vadász u. 2/B 2002-457

A SZEGEDI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK E SOROZATBAN ÚJABBAN MEGJELENT KIADVÁNYAI

Tomus LXI.

Fasc. 23. *Tóth* Károly: A magyar választási eljárás néhány kérdése az Országos Választási Bizottság gyakorlatában (Szeged, 2002.) 373–389. p.

Fasc. 24. *Tóth* Lajos: Agrárviszonyok 1957 és 1967 között a jogi szabályozás tükrében (Szeged, 2002.) 391–406. p.

Fasc. 25. *Trócsányi* László: Az európai integráció jövője egy nagykövet szemszögéből (Szeged, 2002.) 407–418. p.

Fasc. 26. *Valki* László: A 2001. szeptember 11-i terrortámadás és az önvédelem joga (Szeged, 2002.) 419–429. p.

Nagy Károly publikációinak jegyzéke. 431–433. p.

Tomus LXII.

Fasc. 1. *Bató* Szilvia: Büntetőjogi szankciórendszer a reformkorban (Szeged, 2002.) 36 p.

Fasc. 2. *Bobvos* Pál: A szövetkezeti vagyon szabályozása az új szövetkezeti törvényben, különös tekintettel a fel nem osztható vagyonra (Szeged, 2002.) 16 p.

Fasc. 3. *Fantoly* Zsanett: Societas delinquere non potest ...? (Szeged, 2002.) 14 p.

Fasc. 4. *Gellén* Klára: Az akarat szerepe a szerződéskötés során, különös tekintettel a színlelésre (Szeged, 2002.) 39 p.

Fasc. 5. *Gémes* Gábor: A munkaügyi ellenőrzés gyakorlati kérdései a jogi szabályozás tükrében (Szeged, 2002.) 16 p.

Fasc. 6. *Görög* Márta: Összehasonlító utazási jog a német, svájci és magyar utazási jog tükrében (Szeged, 2002.) 52 p.

Fasc. 7. *Hajdú* József: A munkavállalók magánszférájának védelme, különös tekintettel az adatvédelemre (Szeged, 2002.) 54 p.

Fasc. 8. *Heka* László: A horvát Sabor (Szábor) jogtörténeti szerepe (Szeged, 2002.) 43 p.

Fasc. 9. *Juhász* Zsuzsanna: A hazai büntetés-végrehajtási jog és az Európai Börtönszabályok ajánlásai (Szeged, 2002.) 36 p.

Fasc. 10. *Juhászné Zvolenszki* Anikó: A felülvizsgálati eljárás szabályainak koncepcionális változásai (Szeged, 2002.) 30 p.

Fasc. 11. *Kampler* Béla: Eladósodás és pénzügyi önállóság a települési önkormányzatoknál (Szeged, 2002.) 26 p.

Fasc. 12. *Kiss* Barnabás: Az egyenjogúság problémája a magyar közjog (államjog) II. világháború utáni fejlődésében a rendszerváltásig (Szeged, 2002.) 28 p.

Fasc. 13. *Kovács* Judit: A magánvád szabályozásának hazai története az 1973. évi I. törvény megjelenéséig (Szeged, 2002.) 38 p.

Fasc. 14. *Köblös* Adél: Joghatósági szabályok Európában és Magyarországon (Szeged, 2002.) 63 p.

Fasc. 15. Tekla *Papp*: About the Japanese Company Law (Szeged, 2002.) 38 p.

Fasc. 16. *Révész* Béla: A proletárdiktatúra államvédelmi funkcióinak változásai az első Nagy Imre-kormány idején (Szeged, 2002.) 90 p.

Fasc. 17. *Ruszoly* József: Az országgyűlési népképviselet kezdetei Bihar vármegyében (Két tanulmány) (Szeged, 2002.) 75 p.

Fasc. 18. *Szondi* Ildikó – *Kovács* Péter – *Idovika* Bettina: A családok helyzete Szeged város lakótelepein (Szeged, 2002.) 30 p.

Fasc. 19. Moritz *Weiß:* Rechtliche Behandlung von intelligenten Shopping Agenten im Internet (Szeged, 2002.) 32 p.