AZ ADATVÉDELMI JOG GENERÁCIÓI ÉS EGY MÁSODIK GENERÁCIÓS SZABÁLYOZÁS RÉSZLETES ELEMZÉSE

PhD dolgozat

Írta: Dr. Jóri András

Témavezető: Dr. Balogh Zsolt György egyetemi docens

Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola

Pécs, 2009.

TARTALOM

BEVEZETÉS

A polgári jog és büntetőjog cizellált, évszázadok munkájával csiszolt dogmatikájához mérten az adatvédelmi jog újkeletű, fogalmi rendszere egyszerű, története rövid. Ez a sajátossága alkalmassá teszi arra, hogy dolgozatunk tárgya legyen a maga egészében, hogy ne kelljen a vizsgálódásunk körét valamely meghatározott intézményére szűkíteni. A vizsgálódás fókusza azonban ebben az esetben is kijelölhető: dolgozatunk elsősorban az adatvédelmi jogi szabályozás generációs tagolását kívánja vizsgálni, az e tárgyban született elméleti munkák kritikáját kívánja adni, illetőleg saját generációs felosztást javasol. Ezen elméleti modell bemutatásának illusztrációja (egyben az elmélet gyakorlati próbájára ad lehetőséget) az a széleskörű emipirikus felmérés, amelyet a szerző az európai adatvédelmi jogok egyes intézményeit összevetni szándékozó honlap, a www.dataprotection.eu megalkotása során végzett el. A generációs tagolódás vizsgálata, valamint az EU adatvédelmi irányelve alapján született egyes adatvédelmi szabályozások elemzése reményeink szerint nem csak az adatvédelmi jog jelenlegi állapotáról ad lenyomatot, illetőleg nem csak történeti perspektívába helyezi ezt, hanem lehetővé teszi következtetések levonását az uniós jog érvényesülésének komplex problémájáról is.

A dolgozat célja a fenti elméleti keretek felvázolása után az is, hogy bemutassa a magyar adatvédelmi jog fő intézményeinek érvényesülését a gyakorlatban. Az Alkotmánybíróság által az információs önrendelkezési joggal kapcsolatban kifejtett alkotmányértelmezések, valamint az adatvédelem törvényi szabályozásának adatvédelmi biztosi és bírósági gyakorlata mellett e részben egyes szabályozási javaslatokat is teszünk. A dolgozat e második része nagyban támaszkodik a szerző az Osiris Kiadónál 2005-ben megjelent Adatvédelmi Kézikönyv – Elmélet, történet, kommentár c. művére.

Ezt követően a dolgozat a második generációs szabályozáson túlmutató, új fejleményeket ismerteti: az új törekvések arra irányulnak, hogy az európai jogalkotó az információs társadalom új körülményei között a magánszféra védelmét az adatvédelmi jogon belüli új szabályozási megoldásokkal, vagy akár az adatvédelmi jog keretein túllépő új eszközökkel teremtse meg.

Budapest, 2009. szeptember 9.

A szerző

1. Az adatvédelmi jog kialakulása és az adatvédelmi szabályozás generációs felosztása

1. Magánszféra és magánszféra-védelem

1. Az adatvédelem a magánszféra-védelem sajátos jogi szabályozásban megnyilvánuló módja. Az adatvédelmi jog rendelkezési jogot biztosít az érintettnek minden, személyével összefüggésbe hozható adat felett. Ezzel azt szolgálja, hogy a magánszféra megőrzésének lehetősége fennmaradjon abban a világban, ahol az adatok tömeges felvételének, tárolásának, egyeztetésének lehetősége széles körben rendelkezésre áll. Ebben a helyzetben korábban a jogi szabályozás szempontjából irrelevánsnak (a magántitok körébe nem tartozónak) tekintett tények, adatok jelentősége megnő: míg ezeknek az adatoknak nyilvánosságra kerülése, mások általi megismerése a fejlett adatfeldolgozási technológiák hiányában nem hordozott veszélyt, ma feldolgozásuk, egyeztetésük, társításuk, a felhasználásukkal új adatok előállítása nyomán a magánszféra sérülhet. Az adatvédelmi jog kodifikálása mögött az a megfontolás húzódik, hogy a titokvédelem már nem elegendő: az új közegben a védelemnek minden adatra ki kell terjednie: „az adatvédelmet… el kell szakítani a »személyesség« intimitásként való értelmezésétől”.[1]

Az védelem tárgya tehát új – a *személyes adat* –, ám tulajdonképpeni célja ugyanaz, mint korábban a titokvédelemé vagy a magánszféra, az intimitás védelmét szolgáló bármely, jogon kívüli eszközé. Az adatvédelem mint sajátos jogvédelem tárgyalása előtt ezért meg kell fogalmazni azt, mi is ez a védendő cél, érdek: mit véd – az adatok kezelésére vonatkozó szabályok meghatározásán keresztül – az adatvédelmi jog?

Az adatvédelmi jog célja a *magánszféra védelme*. A személyes adatok védelme az új körülmények között is megvalósíthatja a magánszféra védelmét. Ezek az állítások nézetünk szerint igazak, ám keveset mondanak arról, hogy *mi* is magánszféra, és *miért* kell védeni.

2. A privacy (a továbbiakban – bár tudatában vagyok a magyar szó szűkebb jelentéstartományának – magánszféra) fogalmának számos meghatározási kísérlete létezik. Schoeman szerint a magánszféra fogalma megközelíthető úgy, mint

– olyan igény (claim), jogcím (entitlement) vagy jog (right), amely arra irányul, hogy az egyén meghatározza: mely vele kapcsolatos információk jussanak mások tudomására;

[1] Sólyom 1988a, 55.

– az egyén személyes információi, személyisége intim vonatkozásai feletti ellenőrzés (control), illetve annak meghatározására való képesség, hogy az egyénhez ki fér hozzá (who has sensory access to him);[2]

– állapot, amelyben az egyénhez – a hozzá kapcsolódó információkhoz, életének intim tényeihez, gondolataihoz és testéhez – való hozzáférés korlátozott.[3]

Westin szerint a magánszféra kialakulásának előzményei már az állatvilágban megfigyelhetők. „Szinte minden állat igényt tart az egyedüllétre [individual seclusion] és a kiscsoport intimitására [small-group intimacy]. Ezt rendszerint úgy írják le, mint a territorialitás tendenciáját, amelyben egy szervezet organizmus igényt formál a föld, víz vagy levegő valamely területére, és megvédi azt saját fajtársainak behatolásától".[4] Ehhez kapcsolódóan már az állatvilágban jelen vannak a magánszféra fizikai területét kijelölő mechanizmusok; a két – kapcsolatban nem lévő – egyed meghatározott távolságot tart („személyes távolság", personal distance), míg a fajon belül elkülönülő csoportok között is mérhető a „szociális távolság" (social distance). Ha az egyed rendelkezésére álló terület a kritikus alá csökken, nő az agresszió szintje, és „az átfedő személyes távolságok által lerombolt társas kapcsolatok erősítik a kóros jelenségek minden formáját, ugyanazon betegségeket okozva, mint amelyeket a túlzsúfoltság [overcrowding] okoz az embernél: magas vérnyomást, keringési elégtelenségeket, szívbetegséget".[5]

A magánszféra emberi társadalmakban való megjelenését tekintve Westin antropológiai kutatásokra hivatkozva megállapítja, hogy „a magánszférára vonatkozó kortárs normáink »modern«, »haladó« értékek, amelyek nagyrészt hiányoznak a múlt és jelen primitív társadalmaiból".[6] Westin a magánszféra több olyan vonatkozását különíti el, amelyek minden vizsgált társadalomban élő emberre érvényesülnek. Ezek egyrészt a magánszférával kapcsolatos normák az egyén, a család/háztartás és a nagyobb közösség szintjén; az általa bemutatott eredmények szerint a primitív társadalmakban mindhárom szinten találhatók a magánszférára vonatkozó normák, ám ezek igen nagy változatosságot mutatnak. Külön elemnek tekinti Westin azt, „ahogyan az emberi lények érzékelik egyedüllétüket" – az elkülönüléstől való félelem vezet ahhoz, hogy azt gondolják: soha nincsenek egyedül, a

[2] Vö. Sólyom 1983, 315.: „A magánszféra különböző felfogásainak közös vonása, hogy azt a [fizikai és lelki] területet értik alatta, amelyet az egyén kontrollál, amely tehát mentes a külső beavatkozástól."

[3] Schoeman 1984a, 2. skk.

[4] Westin 1984, 56.

[5] Westin 1984, 58. A szerző a betegségek felsorolásakor H. L. Ratcliffe-re és R. L. Snyderre hivatkozik.

[6] Westin 1984, 59.

szellemek, a természetfölötti erők ott vannak velük. További, általánosan jellemző elem a „kíváncsiság és a megfigyelés" – vagyis az egyén és a társadalom általi beavatkozás a magánszférába. Az önmagáért való kíváncsiság Westin szerint már az állatoknál is megjelenik, a kíváncsiság kielégítésének sajátos formája, a pletyka pedig azért létezik, mert „az emberek tudni akarják, hogy mások – különösen a nagyok és hatalmasok – mit tesznek – ez részben arra szolgál, hogy felmérhessék saját teljesítményüket, vágyaikat, valamint arra, hogy közvetett tapasztalatot nyújtson". A magánszférát fenyegető kíváncsiság mellett minden társadalmat jellemez a megfigyelés is – „bármely rendszernek, amely normákat teremt – miként minden emberi társadalom –, meg kell teremtenie a normák kikényszerítéséhez szükséges mechanizmusokat. Mivel le kell leplezni azokat, akik megsértik a szabályokat és a tabukat, minden társadalomnak megvan a viselkedést figyelő, a normaszegést vizsgáló és a »bűnt« megállapító gépezete."[7] Innen vezet az út addig, amíg „a primitív társadalmak modernné alakulása növeli mind az egyén, mind a családi egységek magánszférájának fizikai és pszichológiai lehetőségeit". A szerző kiemeli a városi élet anonimitásának, a munkahely és a lakóhely tekintetében érvényesülő mobilitásnak, valamint az egyén feletti vallási hatalom gyengülésének a folyamatban játszott szerepét; ám ezzel együtt azt a tendenciát is, amely a bürokrácia megjelenésével, az elidegenedettség által kiváltott kapcsolathiánnyal együtt az orwelli antiutópiát igazoló totális megfigyeléshez vezethet.

3. Minden társadalomban élnek tehát a magánszférával kapcsolatos normák, legyenek azok jogiak vagy jogon kívüliek: a westini széles értelemben idetartoznak a testet elfedő ruhadarabok viselésére vonatkozó szabályok ugyanúgy, mint a családi közösség határait kijelölő normák. Westin utal arra is, hogy a nagycsaládddal szembeállított „atomi" családban az egyén privacyja nagyobb[8] – a kisközösségi autonómia kialakulása pedig híd az egyén magánszférájának elismerése felé.[9] A magánautonómia garanciája kezdetben a tulajdon:[10] „A kapitalizmus kibontakozásával párhuzamosan a tulajdonjog egyre határozottabban az

[7] Westin 1984, 68. skk.

[8] Westin 1984, 63.

[9] „A családon belüli tiszta emberi viszonyok már Hobbesnál is »szabályozatlanok«, és az ő rendszeréhez képest a harmadik utat mutatják a »természetes« harc vagy az alattvalói engedelmesség között. A családi autonómia a személyiségi jogok modern fejlődésében is alapvető szerepet játszik" – Sólyom 1983, 81. (és 77. jegyzet). Majtényi ellentétes következtetésre jut, szerinte a magánszféra kezdeti jelentése a Brandeis-nek tulajdonított „the right to be left alone", ám annak „mai megközelítése egyre inkább túlmutat az individualitáson". Majtényi 2003, 580.

[10] A tulajdon és autonómia összefüggésére Hobbes, Locke és Rousseau társadalomelméletében lásd Sólyom 1983, 80. skk.

autonóm cselekvés garanciájaként funkcionál".[11] A becsület védelme már a római XII táblás törvény injúriájának kiterjesztésével megjelent a klasszikus római jogban,[12] és a középkort átívelő történetét követően máig biztosítja a névjogot és a képmás védelmét a svájci jogban,[13] az Egyesült Államokban pedig a XX. században magába olvasztotta a privacy-védelem.[14]

A kialakuló általános személyiségi jogi védelem[15] elemeként fogalmazódik meg idővel az európai jogokban a „titokszféra" védelme,[16] míg az Egyesült Államokban a right to privacy előbb a korábbi, tulajdonjogi magyarázatot felváltva válik például a képmással kapcsolatos védelmet megalapozó joggá, majd később a személyiségi jogi védelem keretévé, az európai „általános személyiségi jog" megfelelőjévé.[17]

Warren és Brandeis 1890-ben megjelent híres tanulmányukban[18] a „magánszférához való jog" (right to privacy) common law-beli elismerésének indokoltságát a korban megjelenő új találmányok hatásával és az addig ismeretlen „üzleti módszerek" elterjedésével kötik össze: az előbbire példa a fotográfia technológiájának kortárs fejlődése, az utóbbira pedig a sajtó – elsősorban a bulvársajtó – növekvő befolyása. „A pillanatok alatt elkészülő [instant] fotográfiák, a sajtóvállalkozások veszélyeztetik magán- és családi életünk szent birodalmát, és számos mechanikus szerkezet létezik, amelyek elterjedésével igaz lehet a mondás, amely szerint »amit az otthonod mélyén suttogsz, a háztetőkről fogják világgá kürtölni«."[19] Az újságok Warren és Brandeis szerint „ördögi módon" avatkoznak be a magánszférába, „a pletyka már nemcsak a henyék és rosszindulatúak szórakozása, hanem üzletté [trade] vált, amelyet arcátlan módon és szorgalmasan űznek".[20] A pletyka „kínálata megteremti a keresletet", eredménye a „társadalom nívójának csökkenése, erkölcsinek hanyatlása".[21]

---

[11] Sólyom 1983, 123

[12] Sólyom 1983, 133. skk.; de „a római injúriákra […] nem vetíthetjük vissza a modern személyiségi jogok alapját képező »autonómiat«, az egyszeri és megismételhetetlen individualitást, sem az ezek tartalmát még nyíltabban kifejező, a társadalommal szembeállított »magánszférát«". Sólyom 1983, 164.

[13] Sólyom 1983, 129.

[14] Pontosabban: Sólyom 1983, 218. skk.

[15] Kialakulásáról lásd Sólyom 1983, 223. skk.

[16] Balás P. 1941, 652. skk.

[17] Sólyom 1983, 29–44, 203. skk.

[18] Warren–Brandeis 1984.

[19] Warren–Brandeis 1984, 76.

[20] Warren–Brandeis 1984, 76.

[21] A pletyka funkciójával kapcsolatban lásd még Posner kitűnő írását, amelyben a szerző amellett érvel, hogy annak társadalmi hatása kifejezetten pozitív: Posner 1984.

A másik változás, hogy a fényképezés technológiája a korban jelentősen megváltozott, lehetővé téve azt, hogy az érintett akarata ellenére örökítsék meg képmását – korábban ehhez hosszabb ideig kellett egy helyben ülnie. Ez a tény Warren és Brandeis jogi okfejtésében is hangsúlyos: korábban ugyanis a fotografálás céljából tudatosan helyet foglaló alany esetén a „a szerződések joga vagy a titoktartásra vonatkozó jog a megfontoltan eljáró egyén számára elegendő biztosítékot nyújthat képmásának nem megengedhető forgalmazása ellen". Az új helyzetben azonban a védelem biztosabb jogi megalapozására van szükség. A common law bíróságok gyakorlatának áttekintése után Warren és Brandeis megállapítják, hogy a keresett jogok „nem szerződésből vagy meghatározott bizalmi viszonyból [trust] erednek, hanem olyan jogok, amelyek a világ ellenében állnak fenn" (vagyis dologi szerkezetű jogokról van szó), ám „az e jogok védelme során alkalmazott elv nem a magántulajdon elve, hacsak ez utóbbi szót nem egy kiterjesztő, szokatlan értelemben használjuk". Warren és Brandeis szerint a megfelelő megoldás a bírák által korábban is elismert jog, a „magánszféra védelméhez való jog" (right to privacy) új értelmezése. Korábban ezt a jogot a common law-ban naplók, levelek és hasonló, „az irodalom vagy a művészet [writing or arts] médiumán keresztül kifejezett gondolatok, érzések és érzelmek" közzétételének megítélésekor használták a bírák,[22] ám a szerzők szerint ez csak a jog egyik összetevője, „a jognak nem kell új alapelvet megalkotnia, amikor kiterjeszti ezt a védelmet az egyén megjelenésére, szavaira, cselekményeire és személyes viszonyaira, otthonában vagy azon kívül".[23]

4. Warren és Brandeis tehát a nyilvánosság szerkezetének változásával[24] és a korban megjelent technológiák hatásával indokolták a „right to privacy" elismerésének szükségességét. A személyiségvédelem a tulajdonjogi helyett új alapot nyert; a privacy nemcsak a magánszféra, hanem a tágabb értelemben vett autonómia védelmét jelenti, és nem csak a tulajdonosi autonómia védelmét. A privacy története során annak jelentése egyre bővült, már az egyén általános cselekvési szabadságáig terjed,[25] miközben Sólyom szerint

[22] Warren–Brandeis 1984, 79. skk.

[23] Warren–Brandeis 1984, 86.

[24] A nyilvánosság e változásáról lásd még Sólyom 1983, 196. Vajon az internet nyilvánossága nem jelent-e hasonlóan új fejleményt? Az irodalom szerint várható olyan technológiák megjelenése is, amelyek akár az agyműködés külső megfigyelését is lehetővé tehetik: Galántai 2005.

[25] Sólyom 1983, 218.

„riasztó általánosság", „dagályosság" és „filozófiai elnagyoltság" jellemzi.[26] Azonban megjelenése fontos állomása a személyiségi jog fejlődésének: annak a fejlődésnek, amelynek „legfontosabb vonása a védelem függetlenedése a tulajdonosi pozíciótól".[27] A technikai fejlődés kihívásaira válaszolva elismerést nyer a név-, képmás- és hangfelvétel-védelem,[28] törvénybe foglalják – elsőként Svájcban – az általános személyiségi jogot[29].

5. Az általános személyiségi jog körében jelenik meg – részint és ennek keretében nyer elismerést – az egyén „titokszférájának" védelme is. Balás P. Elemér megfogalmazása szerint: „A titokszféra lényege az, hogy bizonyos tények tekintetében a személyiségnek annyira túlnyomó a jelentősége, hogy ezek a tények, illetve megtestesüléseik nem is számítanak a külső világ tárgyai közé jogi szempontból, hanem a személyiség függvényének tekintendők. A titokszféra kialakulása a személyiség életfolyamatának megnyilvánulása az akarat közvetítésével. A külvilághoz tartozó tények egy része is olyan, hogy a személyiség szempontjából nem lehet a külvilághoz számítani mint a személyiség életfolyamatának részét, eszközét."[30] A védelem azonban ekkor még csak a titokszférára terjedt ki.

6. Az általános személyiségi jog átmeneti hanyatlása után a második világháborút követően újból a jogi gondolkodás középpontjába kerül,[31] és a titokszféra személyiségi jogi védelme mellett – a számítástechnika fejlődésére, a tömeges adattárolás és – egyeztetés lehetőségének megjelenésére való reakcióként – megjelenik az egyén titokszférán kívüli tényekkel (adatokkal) kapcsolatos, ám még közvetett jogi védelme az első generációs adatvédelmi törvényekkel: megszületik az adatvédelem. A következő lépés, hogy a német Alkotmánybíróság – az alaptörvény általános személyiségi jogot deklaráló szakaszából levezetve – megfogalmazza az információs önrendelkezési jogot. Az új jog az érintett számára immár rendelkezési jogot biztosít minden olyan adat felett, amely vele kapcsolatba hozható (tekintet nélkül arra, hogy ez az adat a titokszféra része-e vagy sem).

---

[26] Sólyom 1983, 215. Sólyom szerint „erről az ürességről árulkodik egyébként […] a privacy primitív természettudományos »megalapozásának« gyakorisága, amelyben kb. a tulajdon visszavezetése az éhségre ismétlődik meg". Önkritikusan utalhatunk itt Westin tanulmányának fenti ismertetésére is.

[27] Sólyom 1983, 17.

[28] Sólyom 1983, 276.

[29] Sólyom 1983, 296. skk.

[30] Balás P. 1941, 652.

[31] Sólyom 1983, 309. skk.

Az adatvédelem fogalma

1. Az adatvédelem (Datenschutz, data protection) fogalma az 1970-es évektől vált széleskörűen használttá, egy olyan, újfajta védelem megjelölésére, amely a korábbi, a személyek által a személyiségi jogi védelem körében élvezett jogokhoz képest nem csak meghatározott típusú adatok (képmás, hangfelvétel) tekintetében, általában nem az „érzékeny" adatokra korlátozva vagy az adatokkal való visszaélés következményeihez igazodva illeti meg az adatvédelmi jogszabályok szerint (általában) a természetes személyeket. Bár kommentárunk a személyes adat fogalma alapján jól körülírható adatvédelmi jogi szabályok gyakorlati alkalmazását kívánja elősegíteni, mégis hasznos elöljáróban az adatvédelem fogalmának meghatározására tett kísérlet, amelynek során rögzíthető a fogalomnak e mű keretein belül tulajdonított jelentése, valamint a kategória viszonya egyes, gyakran szinonimaként használt fogalmakhoz.[32]

2. Az adatvédelem fogalmát gyakran tárgyalják a *magánszféra védelmének* részeként, vagy éppen ellenkezőleg, azzal szembeállítva, mint amely sajátosan európai (jogi) megoldása egy olyan problémának, amelyre az amerikai alkotmányjogban a „magánélethez való jog" megjelenését indukálta. Álláspontunk szerint a magánszféra védelmének számos – jogi és jogon kívüli – eszköze, módja különböztethető meg, és maga a fogalom jóval jelenségek jóval szélesebb tartományára értelmezhető, mint az adatvédelem – az adatvédelem csak a magánszféra védelmének keretein belül mint a magánszféra-védelem adott társadalmi és technikai körülmények között létrejött jogi eszköze értelmezhető. Nem tekinthetünk el attól sem, hogy a privacy fogalma az amerikai jogi gondolkodásban mára jóval szélesebb értelemben használatos – mint fent arra utaltunk, a múlt század végétől olyan fejlődésen ment át, hogy mára az általános személyiségi jog megfelelőjeként értékelhető .

Ez a védelem létezett az adatvédelem megjelenését megelőzően is: jogon kívüli, természetes korlátok, vagy a jogon kívüli társadalmi normarendszer szolgálta a magánszféra védelmét. Ezek az eszközök az adatvédelem megjelenésével továbbra is alkalmazhatók, illetőleg érvényesülnek. Az adatvédelem mint sajátos jogi védelem megjelenéséhez a magánszféra védelmét biztosító egyes természetes korlátok gyengülése, eltűnése vezetett. Az

[32] A meghatározásra annak ellenére kísérletet teszünk, hogy Mayer–Schönberger szerint „Európában az 1970-es évektől az »adatvédelem« szó bevetté vált az egyén azon joga leírására, hogy rendelkezik saját adatai felett. […] Ám az »adatvédelem« szóhoz társított jelentések ismételten és lényegesen változtak, és a fogalom meghatározásának pontosítására tett kísérletek eredménytelennek, tautológiához vezetőnek bizonyultak" (Mayer–Schönberger 1997, 219.).

utóbbi évek fejleménye azonban, hogy a magánszféra védelmének párhuzamos módjai újra nagyobb jelentőséget kapnak – ezt a jelenséget úgyis leírhatjuk, mint az adatvédelem válságát. Ez a válság egyrészt az adatvédelem mint jogi védelem megújítására irányuló törekvéseket ösztönöz, másrészt azzal a következménnyel jár, hogy az adatvédelmi jogi szabályozás bővül, abban egyre nagyobb terjedelemben jelennek meg a magánszféra védelmét szolgáló egyéb (főképpen technológiai) intézkedések, eszközök (lásd erről alább az adatbiztonság fogalmánál).

Az adatvédelem jellemzője tehát, hogy a magánszféra védelmén belül értelmezhető az alábbiak szerint:

a) az adatvédelem minden esetben a személy magánszférájának *jogi* védelmét jelenti,[33] amely

b) az 1970-es évektől az elektronikai forradalom által egyre általánosabbá váló *automatizált adatfeldolgozás veszélyeire válaszul* jelent meg Európában, és

c) az általa nyújtott jogi védelem tartalma a fogalom megjelenése óta többször is jelentősen *változott,* illetőleg jelenleg is folyamatosan változásban van.

3. Az *információs önrendelkezési jog* az egyén „azon joga, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról”.[34] Az irodalomban igen gyakori az az álláspont, amely az adatvédelmet azonosítja az információs önrendelkezési jogot biztosító szabályokkal.[35] Ez a vélemény álláspontunk szerint nem helytálló – mint alább az adatvédelem történetének tárgyalásakor kifejtjük, az információs önrendelkezési jog koncepciója csak jóval az adatvédelem (tehát a személyek sajátos, személyes adataik kezelésének szabályozásán keresztül érvényesülő jogi védelme) megjelenését követő fejlemény, amelynek megjelenése elsősorban a német alkotmánybíróság 1983-as népszámlálás-ítéletéhez köthető.

Az adatvédelem nem azonosítható az információs önrendelkezési joggal, hiszen a korai adatvédelmi törvények nem biztosítottak az egyénnek rendelkezési jogot személyes adatai

[33] „Az adatvédelem a személy, az ember, más szóval: az adatalany védelmét, nem pedig magának az adatnak a védelmét jelenti” (Majtényi 1997a, 6; Majtényi 2003, 579). „Nem az adatnak van szüksége védelemre, hanem annak az egyénnek, akire az adat vonatkozik” (Mayer–Schönberger 1997, 219). Mayer–Schönberger szerint az adatvédelem fogalmával kapcsolatos ezen ellentmondásra már az első német adatvédelmi biztos, Spiros Simitis felhívta a figyelmet a szövetségi adatvédelmi törvény 1979-ben megjelent kommentárjában.

[34] 15/1991. (IV. 13.) AB határozat.

felett. Az információs önrendelkezési jog megjelenése ugyan az adatvédelem történetében jelentős fejlődési állomás, ám az sem állítható, hogy az adatvédelem fejlődése ne haladhatná meg az információs önrendelkezési jog doktrínájában lefektetett alapelveket. Az irodalomban jelen van az a nézet, amely szerint az információs önrendelkezési jogon alapuló adatvédelem válságba került, s az adatvédelmi szabályozás legújabb generációja valójában már csak névlegesen alapszik az információs önrendelkezési jogon.[36] Az adatvédelem tehát felölel minden olyan szabályozást, amely az egyén személyes adatainak kezelését szabályozva célozza annak védelmét, függetlenül attól, hogy ez a szabályozás biztosítja-e az egyén információs önrendelkezési jogát vagy sem.

4. Míg az adatvédelem a magánszféra-védelem egyik eszköze, s mint ilyen, szükségszerűen a személyre irányul, az *adatbiztonság* tárgya maga az adat. Az adatbiztonság az adat integritásának és bizalmasságának védelmét jelenti, függetlenül az adat információtartalmától és jogi minősülésétől.[37]

Az adatbiztonság megteremtését szolgálhatják technikai, szervezési intézkedések, amelyeket jogi és jogon kívüli normák egyaránt előírhatnak. Adatbiztonsággal kapcsolatos rendelkezéseket számos jogi norma tartalmaz, így jogi formát nyernek például a minősített adatokkal (állami és szolgálati titkokkal) kapcsolatos adatbiztonsági rendelkezések.

Az adatvédelem és adatbiztonság között bonyolult kapcsolatrendszer áll fenn. Ennek két legfontosabb eleme a következő:

a) Az adatvédelmi szabályozás fejlődésének különböző szakaszaiban, eltérő mértékben, de általában tartalmaz adatvédelmet szolgáló adatbiztonsági szabályokat is (amelyek tehát arra adnak előírásokat, hogy a személyes adatok kezelése során a norma címzettja mely technikai, szervezési vagy egyéb intézkedéseket köteles megtenni). Az adatbiztonság tehát a személyes adatok tekintetében az adatvédelmi szabályozás tárgya.

b) Új fejlemény, hogy a magánszféra védelmének eszközei között növekszik az adatbiztonságot szolgáló technológiák szerepe. A számítástechnika fejlődésével a fejlett adatfeldolgozási technológiák olcsón, szinte mindenki számára elérhetővé váltak, a nemzetközi számítógépes hálózatok kialakulása pedig megnyitotta az utat az adatkezelés

---

[35] Lásd például Dietz–Pap 1995, 14. Egy másik szerző nyilvánvalóan téves álláspontja szerint az adatvédelem a közérdekű adatok nyilvánosságával együtt képezi „az információs önrendelkezési jog két elemét" (Dósa 2003, 24.).

[36] Lásd például Mayer–Schönberger 1997.

[37] Székely (1994) szerint „…az adatvédelem az *adatalanyok* védelme, az adatbiztonság maguké az adatoké". A két fogalom a magyar adatvédelmi biztosi gyakorlatban is hasonló értelemben szerepel: ABI 1999, 350.

globalizációja előtt is. Ebben a helyzetben az 1970-es években kialakult adatvédelmi szabályozás mindenképpen reformra szorul, a jövőben a magánszféra védelmében szerepe csökkenhet. A magánszféra védelmét a nyílt hálózati környezetben elsősorban technológiai eszközök szolgálhatják hatékonyan (például az ún. „erős" titkosítás). Ezen eszközök nem jogi védelmet nyújtanak, ám sok esetben – éppen a magánszféra védelmében történő alkalmazásuk tömegessé válása, illetőleg ennek következményei miatt – maguk is a jogi szabályozás tárgyaivá válhatnak. (Az „erős" titkosítás használata például akadályozhatja a nemzetbiztonsági vagy bűnüldözési célból végzett legitim adatgyűjtést, amelynek nyomán a jogalkotó beavatkozása válhat szükségessé annak érdekében, hogy helyreálljon az egyensúly a nemzetbiztonság megőrzéséhez, illetőleg a bűnüldözéshez fűződő érdek és a magánszféra védelme között.) Ez a szabályozás azonban már nem tekinthető adatvédelmi jogi szabályozásnak, bár a magánszféra szempontjából releváns, hiszen akadályozhatja vagy megkönnyítheti a magánszféra védelmét szolgáló technológiák alkalmazását.

Az adatbiztonságot szolgáló technológiák mellett vannak olyanok, amelyek kifejezetten a magánszféra védelmére szolgálnak: ezek a magánszféravédő technológiák (privacy enhancing technologies, PET-ek). A magánszféravédő technológiák lehetnek adatbiztonságot szolgáló technológiák is, ám ezen megoldások célja nem az adattartalom védelme általában, hanem a magánszféra védelme technológiai és szervezési megoldásokkal. A privacy enhancing technologies fogalmát e könyvben magánszféravédő technológiának fordítjuk, és Burkert definícióját követjük, amely szerint a fogalom „az egyén identitását, személyazonosságát védő technikai és szervezeti megoldásokat"[38] jelenti.

A magánszféra technológiai védelmének jogi kereteit azonban gyakran olyan eszközök, módszerek jogi szabályozása is befolyásolja, amelyek nem tekinthetők kizárólag magánszféravédő technológiának (ilyen például az „erős titkosítás", amely bármely adattartalom titkosítására felhasználható).

5. Az *információszabadság* (freedom of Information, FOI)[39] jelentése az, hogy az ún. közérdekű adatok, vagyis – az egyes nemzeti szabályozásokban eltérő módon körülhatárolt – állami vagy közfeladatot ellátó szervek birtokban lévő adatok – meghatározott kivételek

[38] Burkert 1997, 125. Nem tesz különbséget adatbiztonsági és magánszféra-védelmi technológiák között, valamint technológiai megoldásokra szűkíti a fogalmat Banisar 2001, 27.

[39] A továbbiakban az információszabadság kifejezést használjuk, mivel a rövidített megjelölés magyar nyelvi közegben való használatára irányuló kísérletek nem voltak sikeresek: a FOI használata Sólyom szerint is „nehézkes" (Sólyom 1988b, 15) és az a korai irodalomban (Könyves Tóth–Varga 1990) az „információhoz való hozzáférés" rövidítéseként használt IHF is.

mellett – bárki számára hozzáférhető, nyilvános adatnak minősülnek. Az adatvédelem és az információszabadság, a magánszemélyek adatainak jogi szabályozására és az állami adatok nyilvánosságának megteremtésére irányuló törekvések között történetileg is van összefüggés. Az első generációs adatvédelmi törvények – mint alább bemutatjuk – nem közvetlenül a személyes adatok kezelésének szabályozására irányultak, hanem a technológia állam általi alkalmazásának szabályozására. Az igazgatás rendelkezésére álló adattömeg és az azt hatékonyan feldolgozni képes rendszerek nem csupán az egyén magánszféráját fenyegették, hanem magát a hatalommegosztást is: új, „információs hatalommegosztás" megteremtésére volt tehát szükség.[40] Egyes első generációs törvények hozzáférhetővé tették az igazgatás által felhalmozott adattömeget a törvényhozás (és a helyi képviselő-testületek) számára.[41] Az adatvédelmet és az információszabadságot a jogalkotó egyre több államban szabályozza egymásra tekintettel, egy jogszabály keretei között, megteremtve ezzel az átfogó „információszabályozást".[42]

6. A fentiek alapján az *adatvédelem fogalmá*t e könyvben általános értelemben használjuk, amely szerint az olyan jogi védelem, amely az egyének magánszférájának védelmét célozza az egyénnel kapcsolatba hozható adatok (személyes adatok) kezelésére vonatkozó szabályok előírásával; *adatvédelmi jog*nak pedig az ilyen szabályokat tartalmazó jogszabályok összességét tekintjük.

7. A meghatározásunk szerinti adatvédelmi jogi szabályok a magyar jogban elsőként a Ptk.-ban jelentek meg. Az adatvédelem az általános személyiségi jogból „kristályosodott ki". Az alkotmányos védelem és az annak tartalmát konkretizáló adatvédelmi törvény azonban közjogiassá teszi az adatvédelmi jogot. Lábady szerint „a magyar magánjogot maga az Alkotmány »hálózza be« közjogi elvekkel és tételekkel. E folyamattal jelentősen megváltozik a jogágak közötti »szereposztás«. A korábban a polgári jogra háruló feladatok egy jelentős része „átcsúszik" a magánjogba, másrészt a magánjogot is áthatja az Alkotmány egész fogalmi kultúrája és értékrendje, továbbá egyes tételes rendelkezései, ugyanakkor az

[40] A német eredetű kifejezést Sólyom László vezette be a hazai irodalomba: Sólyom 1988b. Lásd még Mayer–Schönberger 199, 228.

[41] Ilyen volt Hessen és Észak-Rajna-Vesztfália adatvédelmi törvénye, valamint az 1974-es osztrák tervezet: Sólyom 1988b, 23. és 18. lábjegyzet; Mayer–Schönberger 1997, 228. és 33. lábjegyzet; Burkert 2002, 184. E sajátos tájékoztatáshoz fűződő jog a két tagállam újonnan elfogadott adatvédelmi törvényeiben is szerepel: lásd az 1999. évi hesseni törvény 38. §-át, Észak-Rajna-Vesztfália 1994. évi adatvédelmi törvényének 36. §-át.

alkotmányjogban is egyre erősebben munkál a magánjog szelleme."[43] Lábady a magánjog „közjogiasodása" fontos fejleményének tartja a „személyiségi jogok magánjogi tiszteletének a megújulását". „A közjognak ez irányú betörése az autonómia viszonyaiba megalapozta a személyhez fűződő jogok függetlenedését a vagyoni jogoktól a magánjogon belül."[44]

Az adatvédelmi jogot az irodalom gyakran – különösen hazánkban – mint a közérdekű adatokhoz való hozzáférés jogát, vagyis az információszabadság ikerjogát tárgyalja: az adatvédelem és az információszabadság a két információs alapjog.[45] A két jog együttes tárgyalását igazolja az, hogy Magyarországon sikeresnek bizonyult az adatvédelmi és az információszabadság-jog együttes kodifikációja, és hazánkat követően több más európai adatvédelmi biztos is kapott az információszabadság-jog érvényesítésével kapcsolatos hatásköröket.[46]

Egy másik felfogás szerint az adatvédelmi és információszabadsággal kapcsolatos joganyag mellett más tárgyakat szabályozó normák, így az ún. titokjog (a minősített adatok [állam- és szolgálati titok] kezelésének szabályai), az elektronikus iratokra vonatkozó jogi szabályozás és az adatbiztonságra vonatkozó jogi rendelkezések együttesen alkotnák az „adatkezelési", „információkezelési" jogot[47] – az információkezelési jog szabályozásának tárgya nem a személyes adat, hanem maga a hordozótól független adat (információ), amelynek kezelését a joganyag egyes területei meghatározott célokból (magánszféra védelme, nemzetbiztonsági érdek stb.) szabályozzák. A koncepció előnye az, hogy az egyes adatkezelők az adatkezelési joggal mint egységesen kodifikált, a különböző szabályozási tárgyakat kifejtő normák egymásra tekintettel kialakított rendszerével szembesülnének, ami megkönnyítené a jogalkalmazást. Nem véletlen, hogy a hazai adatvédelmi törvény

---

[42] Lásd Sólyom 1988, 27. A magyar jogi gondolkodás és jogalkotás úttörő jellegét illusztrálja, hogy ez a gondolat Magyarországon ilyen korán megfogalmazódott. A magyar szabályozás (a kanadai mellett) a külföldi jogirodalomban is elemzés tárgya (például Burkert 2002, 196).

[43] Lábady 2000a, 24.

[44] Lábady 2000a, 26.

[45] Lásd például Majtényi 2003.

[46] Így Nagy-Britanniában, valamint Németország Brandenburg és Berlin tartományaiban.

[47] Szurday Kinga hasonló gondolatot fogalmaz meg, amikor az „információszabályozási törvények" kategóriáját használja. Álláspontja szerint ezek egyrészt általános törvényekből (amelyek „freedom of information" típusú törvények, privacy-törvények és adatvédelmi törvények), másrészt speciális, „az információáramlás adott részterületét" szabályozó törvényekből állnak. Sajnos Szurday nem fejti ki teljesen rendszerét, és végső soron nem értelmezi az „információszabályozási" jogot az adatvédelem és az információszabadság területén kívül. Lásd Szurday 1994.

kodifikációjának kezdetén azt mint „informatikai törvényt” határozták meg,[48] s a jogi gondolkodásban már akkor megjelent az „információszabályozás” gondolata.[49] Az adatvédelem és információszabadság egy jogszabályon belül történő szabályozása mellett a titokjog (az államtitok és szolgálati titok szabályozása) is kapcsolódik ehhez a joganyaghoz: az adatvédelmi biztos meghatározott titokfelügyeleti jogkörökkel rendelkezik, az adatvédelmi törvény háttérjogszabálya az államtitokról és szolgálati titokról szóló törvénynek, stb. Az adatvédelmi jog tehát szemlélhető úgy is, mint egy tágabb – nem csak a személyes adatok védelmét és a közérdekű adatok nyilvánosságát felölelő – „információszabályozás” részterülete.

Az adatvédelmi jog kialakulása és történetének vázlata

1.1. Az adatvédelmi szabályozás generációi

1. Az adatvédelmi jog megjelenése előtti korszak az a kor, amelyre még nem volt jellemző az elektronikus adattároló és –feldolgozó rendszerek tömeges alkalmazása. A személyes adatok összekapcsolásának, feldolgozásának, a személyiséget kiszolgáltatott helyzetbe hozó személyiségprofil megalkotásának az esélye ekkor még csekély volt, mivel az ilyen tevékenység csak igen nagy ráfordítások mellett volt végezhető. A magánszféra totális megsemmisülésétől való félelem azonban már ekkor is élt, ezt jelzik József Attila verssorai 1935-ből:

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

Hasonló félelmet tükröz George Orwell regénye, az *1984*. Louis Brandeis főbíró szerint, „a magánszféra megsértésének a korábbinál kifinomultabb és szélesebb körben ható módszerei váltak az állam számára elérhetővé. A felfedezők és feltalálók tevékenysége

[48] Sólyom 1988a.

[49] Sólyom 1988b, 27.

nyomán a kínpadnál jóval hatékonyabb módszerek állnak rendelkezésre arra, hogy az otthonok mélyén halkan kimondott szavak a bíróság előtt is elhangozzanak".[50] Brandeis már több mint 30 évvel 1928-as véleménye előtt megfogalmazta fent már hivatkozott, Warrennel közös cikkében az új technológiák által hordozott veszélyeket. Azonban „az 1960-as évekig a megfigyelést szolgáló technológiák alacsony technikai színvonalat képviseltek és drágák voltak: a megfigyeltet követni kellett, akár hat személy igénybevételével; 2 főből álló csoportoknak kellett dolgozni három nyolcórás műszakban. Az összegyűjtött anyagot és kapcsolatokat rendszerezni kellett, meg kellett szűrni, és kevés remény volt arra, hogy az adatok gyorsan összevethetők. Még az elektronikus megfigyelés is igen munkaigényes volt. A keletnémet rendőrség például ötszázezer titkos informátorral dolgozott, akik közül tízezren kizárólag a polgárok telefonbeszélgetéseinek lehallgatásával és leírásával foglalkoztak".[51] Az adatfeldolgozás nem volt automatizált, illetőleg a tömeges, ellenőrizetlen megfigyelés túl nagy költségekkel járt, mindez pedig a magánszféra védelmét szolgáló természetes korlátot jelentett. E természetes korlátok dőltek le az 1960-as évek közepétől a számítástechnika adatfeldolgozási célú igénybevételének elterjedésével.

2. Az európai adatvédelmi szabályozás történetének tárgyalása során az irodalom meghatározott szempontok szerint a szabályozás generációit különíti el. Egyesek az adatvédelmi szabályozás három, mások négy generációját írják körül. Mayer-Schönberger szerint az első generációs törvényeket, amelyek az 1970-es évek elején jelentek meg, sajátos technológiai szemlélet jellemzi; a második generációs törvények szabályozása már kevésbé technológiafüggő, és ebben a generációban (az 1970-es évek második felében) az egyén jogai is hangsúlyosabbak a szabályozásban. Felosztása szerint a harmadik generációs adatvédelmi törvények azok, amelyek a német alkotmánybíróság 1983-as népszámlálás-ítéletét követően születtek, s amelyek esetében a szabályozás tükrözi az információs önrendelkezési jog koncepcióját. A negyedik generációs szabályozás – amelyet a szerző a „holisztikus" és „szektorális" kulcsszavakkal jellemez – korrigálja a harmadik generációs törvények

[50] Idézi „An Appraisal of Technologies of Political Control" – az Európai Parlament Scientific and Technological Options Assessment Unit (a továbbiakban: STOA) munkadokumentuma (1998), 4. pont. Az dokumentum vezetői összefoglalója megtalálható az Európai Parlament honlapján: http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm; a teljes szöveg a http://cryptome.org/stoa-atpc.htm címen olvasható.

[51] STOA 4. pont. Az anyag a volt keletnémet titkosszolgálatra (Stasi) utal.

hiányosságait, és új fejleményként ebben az időszakban területspecifikus adatvédelmi szabályozás egészíti ki az általános szabályokat.[52]

Bäumler – aki felosztását elsősorban a német adatvédelmi jog fejlődésére tekintettel fogalmazza meg – nem tesz különbséget a Mayer-Schönberger által első és második generációba sorolt törvények között, hanem ezen szabályokat egy csoportba sorolva azzal jellemzi azokat, hogy generálklauzulákat, elvi tételeket tartalmaztak. A szerző a második generációba sorolja a népszámlálás-ítéletet követő jogalkotás eredményeit (közöttük számos szektorális adatvédelmi normát), a harmadik generációba pedig azon jogszabályokat, amelyeknek egyrészt az irányelvet kell átültetnie a nemzeti jogba, ám alapvetően át is kell alakítaniuk az adatvédelmi jogot, reagálniuk kell az adatfeldolgozási technológia megváltozott jellemzőire.[53] Hasonlóképpen vázolja fel a generációs fejlődést Bizer is – szerinte a legújabb kihívás a jogalkotó előtt az, hogy a klasszikus adatvédelmi jogot kiegészítve „a technikát formáló jogot" (Recht der Technikgestaltung) hozzon létre.[54]

A hazai irodalomban Majtényi az első generációs szabályozás központi jellemzőjének azt tekinti, hogy az a számítógépes (vagy legalább részben automatizált) nyilvántartásokra irányult. A második generációs törvények jellemzője e felosztás szerint, hogy immár az adathordozótól függetlenül von szabályozása alá minden nyilvántartást (így a papíron létezőeket is). A harmadik generáció jellemzője Majtényi szerint, hogy ennek megalkotása során tényező az integráció (az irányelv elfogadása), és a szektorális kihívások.[55]

Álláspontunk szerint a szabályozás történetének generációkkal történő leírása jól használható az európai adatvédelem történetének leírására. A fejlődés három korszakra tagolható:

a) az első adatvédelmi szabályok megjelenésétől az információs önrendelkezési jog kifejtését adó 1983-as német alkotmánybírósági határozatig tart,

b) a második az információs önrendelkezési jog doktrínájának megfogalmazásától tart egészen a harmadik korszak elejéig,

c) a harmadik kezdete az adatvédelmi szabályozás válságára válaszképpen az „új adatvédelem" szabályainak megjelenéséhez köthető (korszakhatárnak az 1997-es német Teledienstedatenschutzgesetz elfogadását tekintjük).

---

[52] Mayer–Schönberger 1997.

[53] Bäumler 1999.

[54] Bizer 1999.

[55] Majtényi 2003. A szektorális szabályozás irányába való elmozdulás jellemzi a szabályozás harmadik generációját Bennett szerint is: Bennett 1997, 114.

1.2. Az első generációs adatvédelmi törvények

1. Az 1960-as évek második felében a fejlődés eljutott odáig, hogy az orwelli antiutópia megvalósulásának lehetősége reálisnak tetszett. A kiteljesedő szociális jóléti állam működtetéséhez a bürokráciának egyre több információra volt szüksége, az óriási információtömeg feldolgozására pedig rendelkezésre állt az új technológia is.[56] A számítógépeket használatba vették a nagy nyilvántartásokkal rendelkező szerzetek – az állam és a legnagyobb vállalatok. Mivel a számítási kapacitás igen drága (és ezzel együtt korlátos) erőforrásnak számított, hamar felmerült az a gondolat is, hogy az adatokat célszerű egyetlen helyen tárolni, s az adatok felhasználását távolról lehetővé tenni a különböző felhasználók számára – így a rendszer üzembe állítása, működtetése és karbantartása is jóval egyszerűbb volt.[57] Az adatbankok összekapcsolásának legegyszerűbb eszköze valamely általánosan használt mesterséges azonosító, amelynek igénye szintén ekkor merül fel az igazgatáson belül.[58] Ezek a fejlemények, az „integrált adatfeldolgozás" koncepciójának megjelenése vezetett Németországban az ún. adatvédelem-vitához (Datenschutzdiskussion),[59] majd az adatvédelmi törvényhozáshoz.

2. *Az első generációs törvények* tehát egy olyan korban születtek, amelyben kevés számú nagy – elsősorban állami – adatkezelő vette alkalmazásba a számítógépeket. Félő volt, hogy az állam a különféle nyilvántartások összekapcsolásával információs túlhatalmat szerez az egyén felett, ezért az első adatvédelmi törvények szövegezői kifejezetten az új technológia kihívásaira reagálva próbálták annak alkalmazását ellenőrizhetővé, transzparenssé tenni. Az első generációs adatvédelmi törvények jellemzőiként az alábbiakat határozhatjuk meg:

a) Ezen törvények elsődleges célja a nagy – elsősorban állami – adatbázisok transzparenciájának megteremtése.

---

[56] A nagy adatbázisok és a szociális jóléti állam kapcsolatáról lásd Mayer–Schönberger 1997, 222.

[57] Svédországban az 1960-as évek második felében született olyan terv, amely szerint egy országos adatbankban kell összekapcsolni az adózással kapcsolatos adatokat, valamint a (már összekapcsolt) népszámlálási és anyakönyvi nyilvántartást. Németországban a helyi, tagállami és szövetségi szintű közigazgatás adatbankjainak összekapcsolását tervezték, valamint tagállami szinten (például Hessenben, Bajorországban) is központosítani kívánták a közigazgatás által végzett adatfeldolgozást (Mayer–Schönberger 1997, 222). A hesseni terv szerint a központosított rendszerben személyenként kb. 70 adatot tároltak volna, méghozzá személyi számon (a „Nagy Hesseni Tervről" lásd Sólyom 1988b, 25). Lásd még erről Bizer 1999, 31.

[58] Bizer 1999, 32.

[59] Bizer 1999, 31.

b) A cél érdekében ezek a törvények még nem biztosítanak rendelkezési jogot az egyénnek az adatai felett: azonban biztosítanak egyes, később a rendelkezési jog részjogosítványaivá váló jogokat, elsősorban a betekintésre és a helyesbítésre irányuló jogot.

c) A szabályozás ezen generációjában jelennek meg az adatbázisok nyilvántartásba vételére illetőleg engedélyezésére vonatkozó kötelezettségek. Hangsúlyozni kell tehát azt, hogy a nyilvántartásba vételi kötelezettség egy kevés nagy adatbázist ismerő környezetben jelent meg.

d) Az első generációs adatvédelmi törvényekkel a jogalkotó kifejezetten a számítógépes adatfeldolgozást kívánta ellenőrzés alá vonni: ezek a törvények tehát a magánszféra-védelem sajátos eszközei voltak az információs forradalom kezdeti időszakában, ám az általunk használt meghatározás szerint nem is tekinthetők adatvédelmi törvénynek abban az értelemben, hogy tárgyuk elsősorban a nyilvántartást szolgáló technológia volt.

e) Jellemző, hogy az első generációs törvények közül egyesek a törvényhozás számára jogot biztosítottak a közigazgatás rendelkezésére álló információkhoz való hozáféréshez. Ez alátámasztja azt, hogy az első generációs törvények közvetlen célja nem a korábban definiált adatvédelem volt, hanem a végrehajtó hatalom információs túlsúlyának visszaszorítása az államon és a társadalmon belül.

1.3. A népszámlálás-ítélet és az adatvédelmi törvények második generációja

1. 1983 decemberében a német alkotmánybíróság az egész világ adatvédelmi jogára kiható döntést hozott, amikor alkotmányellenesnek (az alaptörvénnyel összeegyeztethetetlennek) mondta ki az abban az évben elfogadott népszámlálásról szóló törvény egyes rendelkezéseit. A híressé vált népszámlálás-ítéletben (Volkszählungsurteil) a bíróság úgy foglalt állást, hogy „az alapjog […] biztosítja az egyénnek azt a jogot, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról”.[60]

[60] BVerfGe 65, 1. A szöveg elérhető a http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm címen. Rövidített változatot közöl magyar fordításban *Infofilia,* 1991. Az ügy tárgya az 1983-as népszámlálástörvény, amelyben a jogalkotó népszámlálást rendelt el, s ez kiterjedt az azonosító adatokon kívül a foglalkozással kapcsolatos adatokra („foglalkozásszámlálás”) is; a népszámláshoz kapcsolódott a nem mezőgazdasági vállalkozások, munkahelyek összeírása („munkahelyszámlálás”), valamint a lakóingatlanokkal kapcsolatos épület- és lakásstatisztikai felmérés is. A törvény szerint a felvett adatok meghatározott köre összekapcsolható volt a lakcímnyilvántartással az adattartalom pontosítása céljából. Ezentúl a törvény számos más adattovábbításra is lehetőséget adott – igaz, csak anonimizált adatok vonatkozásában – a szövetségi és

A német alkotmánybíróság az információs önrendelkezési jogot az alaptörvény 2. cikkének (1) bekezdéséből – az 1. cikk (1) bekezdésével együttesen értelmezve – következő általános személyiségi jogból vezette le.[61] Az általános személyiségi jog olyan anyajog, amelynek tartalma a joggyakorlatban „végérvényesen nem konkretizált",[62] ám amelyből időről időre a személyiséget valamely meghatározott módon védő jog kristályosodik ki. A személyiségi jog magában foglalja „az egyénnek az önrendelkezés eszméjéből következő illetékességét arra, hogy alapvetően mikor és milyen mértékben fedi fel személyes életének tényállásait". A bíróság szerint az önrendelkezés a technológia fejlődése nyomán fokozott védelemre szorul: „Azt mindenekelőtt az veszélyezteti, hogy a döntési folyamatokban a korábbi gyakorlattól eltérően nem szükséges a manuálisan összeállított kartotékokhoz és iratokhoz visszanyúlni, mert az automatikus adatfeldolgozás segítségével egy meghatározott személyt érintő, személyes vagy anyagi viszonyaira vonatkozó egyedi adatok {személyes adatok [vö. a szövetségi adatvédelmi törvény 2. § (1) bekezdésével]} műszaki szempontból korlátlanul tárolhatók, és bármikor, a távolságra való tekintet nélkül, másodpercnyi gyorsasággal előkereshetők. Azokat ezen túlmenően – mindenekelőtt integrált információrendszerek kiépítése esetében – más adatállományokkal egy részben vagy messzemenően teljes személyiségképpé lehet összekapcsolni anélkül, hogy az érintett annak helyességét és felhasználását kielégítően ellenőrizhetné". A bíróság szerint mind az egyén önrendelkezési jogára, mind a demokratikus társadalomra veszélyes lehet az a helyzet, „amelyben a polgár nem tudhatja, hogy ki, mit, mikor és milyen alkalomból tud róla. Aki bizonytalan abban, vajon az eltérő magatartásformákat mindig feljegyzik-e, és mint információt tartósan tárolják, felhasználják és továbbítják-e, törekedni fog arra, hogy ilyen magatartásformákkal ne tűnjön ki. Aki számol azzal, hogy egy gyűlésen vagy egy polgári kezdeményezésben való részvételét hatóságilag esetleg nyilvántartásba veszik, és hogy ez számára kockázatos lehet, esetleg le fog mondani megfelelő alapjogai (alaptörvény 8., 9. cikk) gyakorlásáról." Ez indokolja a bíróság szerint az információs önrendelkezési jog mint az

---

tartományi statisztikai hivataloknak egyéb közigazgatási szervek számára (például név nélkül a vallási közösséghez való tartozással kapcsolatos adatok kivételével, ha ez a címzett közigazgatási szerv hatáskörébe tartozó feladat jogszerű ellátásához szükséges, név nélkül tervezési illetőleg környezetvédelmi célokból helyi önkormányzatok számára).

[61] Az alaptörvény 2. cikkének 1. bekezdése szerint: „Mindenkinek joga van személyisége szabad kibontakoztatásához, amennyiben mások jogait nem sérti és az alkotmányos rend és az erkölcsi törvény ellen nem vét." Az 1. cikk 1. bekezdése szerint: „Az emberi méltóság elidegeníthetetlen [unantastbar]. Ennek tisztelete és védelme minden állami szerv kötelezettsége."

általános személyiségi jog által felölelt jog megfogalmazását, amely „biztosítja az egyén illetékességét arra, hogy személyes adatainak kiszolgáltatásáról és felhasználásáról alapvetően maga rendelkezzék".

Az Alkotmánybíróság rögzítette azt is, hogy az információs önrendelkezés joga nem korlátlan. A korlátozás kényszerítő közérdekből (überwiegendes Allgemeininteresse) történhet; a normának eleget kell tennie a normaszabatosság követelményének, tehát azt oly módon kell megfogalmazni, hogy a polgár képes legyen megérteni a korlátozás feltételeit és terjedelmét. A szabályozásban meg kell határozni a célt, és az adatkezelést olyan adatok vonatkozásában lehet előírni, amelyek a célra alkalmasak és szükségesek. További eljárási garanciaként rögzíti a határozat az érintett felvilágosításhoz való jogát és a cél teljesülése esetén az adattörlés kötelezettségét. A bíróság rögzítette azt is, hogy az automatizált adatfeldolgozás összetettsége miatt és a hatékony jogvédelem biztosításának érdekében igen nagy jelentősége van a független adatvédelmi biztosoknak. A határozat ezen túl részletesen tárgyalta az információs önrendelkezési jogból folyó követelményeket a statisztikai célú adatfeldolgozás során.[63]

2. A döntésnek óriási hatása volt mind Németországban, mind külföldön – abban lefektetett elvek jelennek meg a következő években elfogatott német tartományi adatvédelmi törvényekben és még a szövetségi adatvédelmi törvény (BDSG) 1990-es novellájában is. A határozat szelleme érezhető az 1986-os osztrák törvénymódosításban, a norvég, a finn és a holland adatvédelmi szabályozásban is.[64] A népszámlálás-ítéletnek máig ható befolyása volt a magyar adatvédelmi jog alakulására: a magyar adatvédelmi jog ősforrása, a 15/1991. (IV. 13.) AB határozat sokban épít az 1983-as döntésre, amely így közvetett módon a hatályos adatvédelmi jogot (és az adatvédelmi jogi közgondolkodást) is meghatározza.

3. *A második generációs szabályozások*[65] jellemzője Mayer-Schönberger szerint, hogy azok az adatkezelés egész folyamatára vonatkozóan meghatározott jogokat biztosítanak az adatalanyok számára – a jogalkotók felismerték, hogy nem lehetséges az adatalany döntését

---

[62] Lásd a népszámlálás-ítélet indokolását.

[63] Az alkotmánybíróság ezt követően alkotmányellenesnek mondta ki a törvény azon szakaszait, amelyek a népszámlálási adatfelvétel során képződött adatok egyéb célú felhasználását tették lehetővé a közigazgatás számára. A két – statisztika és igazgatási – cél összekapcsolása ugyanis az érvelés szerint áttekinthetetlen helyzetet eredményez a polgár számára, sérti a normavilágosság követelményét, alkalmatlan a célok elérésére, ezáltal alkotmányellenes.

[64] Mayer–Schönberger 1997, 231.

arra szűkíteni, hogy engedélyezi-e adatainak automatizált feldolgozását, vagy sem, mivel a technológia ebben az időben már annyira áthatotta a társadalom szövetét, hogy a nemleges döntés a gyakorlatban óriási költségekkel járt volna az egyén számára. Tipikus jellemzői az e korszakban született szabályozásoknak a marketing- és piackutatási célú adatkezelésekkel kapcsolatos tiltakozási jog, és az elavult adatok törlésével kapcsolatos jog.[66] Tovább erősödött a szabályozás absztrakt jellege, a technológiaspecifikus szabályok háttérbe kerülése. A korszak technológiai változásai – a személyi számítógépek megjelenése, majd azok hálózatokba rendezése – reménytelenné tették volna a technológia szabályozását: a törvényhozó ezért a technológia szabályozása helyett inkább az egyént fegyverezte fel az információs önrendelkezési joggal, amellyel élve az – legalábbis elviekben – minden körülmények között képes volt magát megvédeni. (A technológiaspecifikus szabályozás háttérbe szorulása átmeneti jelenség volt – a harmadik generációs szektorális szabályozások lényege az, hogy a technológia jellegére tekintettel specifikus szabályozással erősítik az információs önrendelkezési jog érvényesítésének lehetőségét valamely adott szektor sajátos körülményei között.) Ebben a korszakban – párhuzamosan az integrált, központosított adatbázisok világának szabályozására kialakított, technológiaközpontú szabályozás visszaszorulásával – leegyszerűsödtek az adatbázisok nyilvántartásba vételi kötelezettségére vonatkozó szabályok is.[67] Érdemes megjegyezni, hogy Mayer-Schönberger szerint ezek a törvények pragmatikus kompromisszumot jelentenek „a hatékony információfeldolgozás ösztönzése és kontrollja között” – vagyis már ebben a korszakban megtörténik a megkövetelt védelmi szint csökkentése a működőképesség érdekében[68].

1.4. Globalizáció: adatvédelmi tárgyú nemzetközi dokumentumok

1. Az első adatvédelmi törvények elfogadása után szükségszerűen merült fel a nemzeti szabályok összahangolásának igénye, hogy azok ne válhassanak az egyre intenzívebb nemzetközi személyesadat-áramlás gátjaivá.

Az adatvédelem globalizálódásának első fejleményeként már 1980-ban megfogalmazták *Nemzetközi Gazdasági és Együttműködési Szervezet (OECD) adatvédelmi irányelveit* (OECD

[65] Mayer–Schönberger felosztása szerint az információs önrendelkezési jog elvi alapján álló szabályozások már az adatvédelmi jogi normák harmadik generációját képviselik. Mayer–Schönberger 1997, 231.

[66] Mayer–Schönberger 1997, 232.

[67] Lásd Mayer–Schönberger példáját az osztrák szabályozással kapcsolatban: Mayer–Schönberger 1997, 231.

[68] Mayer–Schönberger 1997, 231.

irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról).[69] Az OECD-irányelvek különös jelentőségét az adja, hogy a szervezetben az Egyesült Államok is részt vesz, ezért – az ET-egyezménnyel és az EU-irányelvvel ellentétben – az OECD irányelvekben foglaltak Európa és az Egyesült Államok közötti közös nevezőnek tekinthetők. Az OECD-irányelvek elsődleges célja – mint ez a preambulumból kiderül – az adatvédelmi jogszabályok által teremtett esetleges kereskedelmi akadályok, a nemzetközi adatáramlás előtti gátak elhárítása volt. Az OECD-irányelvek között számos olyan is szerepel, amely – az ET-egyezmény közvetítésével – a magyar adatvédelmi jogra is hatással volt, illetőleg hatott az EU adatvédelmi irányelvének megfogalmazóira (az irányelvek tartalmára pedig természetesen befolyással voltak az addig Európában elfogadott adatvédelmi törvények).

Előremutató sajátossága az irányelveknek, hogy azok nemcsak az automatizált, hanem minden olyan adatkezelésre vonatkoznak, amelyek „az adatkezelés módja, vagy az adatok természete, illetőleg azok összefüggései miatt veszélyt jelentenek a magánszférára és az egyéni szabadságokra".

2. Az irányelvek mind a magánszférabeli, mind a közszféra adatkezelésével kapcsolatban (szintén előremutató vonás) ajánlásként fogalmazzák meg az alábbi elveket a tagállamok számára[70]:

– *a korlátozott adatgyűjtés alapelve:* az adatgyűjtés elé korlátokat kell állítani, az adatokat törvényes és tisztességes módon kell felvenni, lehetőség szerint az adatalany tudtával vagy beleegyezésével;

– *az adatminőség alapelve:* az adatok legyenek a felhasználás célja szempontjából relevánsak, és amennyire ez a cél megvalósulásához szükséges, pontosak, teljesek és időszerűek;

– *a cél meghatározásának alapelve:* az adatgyűjtés célját legkésőbb az adatgyűjtéssel egy időben meg kell határozni, és a későbbi felhasználást e célra vagy az ezzel összeegyeztethető és a cél változásakor meghatározott célokra kell korlátozni;

– *a felhasználás korlátozásának alapelve:* az adatokat nem szabad nyilvánosságra hozni, hozzáférhetővé tenni vagy egyébként felhasználni a fenti meghatározottakon kívüli célból, kivéve, ha az adatalany hozzájárul vagy arra törvény felhatalmazást ad;

---

[69] Az irányelvek szövegét lásd: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. Magyar nyelvű áttekintés: http://www.oecd.org/dataoecd/16/9/15590228.pdf. Magyar kivonatos közlés: *Infofilia,* 1992. Lásd még Jay–Hamilton 1999, 5.

[70] Nem szó szerinti fordítás.

– *a biztonság alapelve:* elvárható biztonsági intézkedéseket kell tenni az adatvesztés, az illetéktelen hozzáférés, megsemmisítés, megváltoztatás stb. ellen;

– *a nyíltság alapelve:* alapvetően ennek kell érvényesülnie a személyes adatokkal kapcsolatos gyakorlat és szabályozás terén: meg kell teremteni annak a módját, hogy az adatok léte, természete, az adatfelhasználás célja, az adatkezelő személye és tartózkodási helye megállapítható legyen;

– *a személyes részvétel alapelve:* az egyénnek biztosítani kell azt a jogot, hogy az adatkezelőtől vagy mástól megtudhassa, hogy az kezel-e vele kapcsolatos személyes adatot, hogy ezeket az adatokat megismerhesse (elvárható időn belül, nem aránytalanul magas díjért, számára értelmezhető módon); hogy tájékoztatási kérelme esetén jogorvoslattal éljen; hogy az adatkezeléssel kapcsolatban jogorvoslattal éljen, és ha az sikeres, adatát töröljék, helyesbítsék, módosítsák vagy kiegészítsék;

– *az elszámoltathatóság alapelve:* az adatkezelő elszámoltatható legyen a fenti alapelveknek való megfelelőség érdekében tett intézkedéseivel kapcsolatban.

Az irányelvek érintik a határon átívelő adatáramlás kérdését is: a tagállamok az irányelvek szerint korlátozhatják meghatározott adatfajták továbbítását olyan adatok tekintetében, amelyekre adatvédelmi szabályozásuk ezt előírja, az adatok természetére, és arra tekintettel, hogy a másik tagállam nem biztosítja ezek „azonos védelmét".

3. A következő lépés az *Európa Tanács Adatvédelmi Egyezmény*ének elfogadása volt 1981-ben (Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során). Az egyezmény hatálya kiterjed „a személyes adatok automatizált állományaira" és a „személyes adatok gépi feldolgozására" mind a köz-, mind a magánszférában; a felek azonban nyilatkozatot tehetnek arról, hogy az egyezményt „a személyes adatok nem gépi eszközökkel feldolgozott adatállományaira" is alkalmazzák – ilyen nyilatkozatot tett a Magyar Köztársaság is.

Az adatok minőségéről szóló 5. cikkben az ET-egyezmény az OECD-irányelvekhez nagyon hasonlóan rögzíti, hogy

„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."

Az egyezmény tartalmazza a különleges adatok kezelésének főszabály szerinti tilalmára vonatkozó rendelkezést, az adatbiztonsággal kapcsolatos kötelezettségeket, valamint – szintén az OECD-irányelvek mintájára – az érintett jogairól szóló szabályozást. Az egyezmény határokon átlépő adatáramlásra vonatkozó rendelkezéseit alkalmazni kell „a gépi úton feldolgozott vagy a gépi feldolgozás céljára felvett személyes adatoknak az országhatárokon keresztül – bármely eszközzel – történő továbbításakor". A külföldre irányuló adatáramlást egyik fél sem tilthatja vagy kötheti külön engedélyhez, a magánélet védelmének kizárólagos céljából, ha az egy másik fél területére irányul; ez alól azonban a fél kivételt tehet „meghatározott személyes adatokra vagy személyes adatok meghatározott automatizált állományaira, ezen adatok vagy adatállományok jellege miatt, kivéve, ha a másik Fél szabályozása azonos védelmet nyújt",[71] vagy akkor, ha „a továbbítás saját területéről egy másik Fél területén keresztül egy nem szerződő Fél területére irányul, annak érdekében, hogy megakadályozza, hogy az ilyen továbbítás a Fél e pont elején említett jogszabályainak kijátszását eredményezze". Az ET-egyezmény kihirdetéséről az 1998. évi VI. törvény rendelkezik.

4. Az Európai Bizottság az ET-egyezmény elfogadását követően arra az álláspontra helyezkedett, hogy az egyben megoldja majd az uniós harmonizáció kérdését is: 1981-ben olyan ajánlást fogalmaztak meg, amely a tagállamokat az egyezményhez való csatlakozásra ösztönözte.[72] A jogalkotástól való ódzkodás nem volt alap nélküli: mikor a Bizottság végül észlelte a nemzeti jogok nemkívánatos eltérését, és 1990-ben kezdeményezte az irányelv megalkotását, nyilvánvalóvá vált, hogy a tagállamok erősen megosztottak az adatvédelmi szabályozás kérdésében: Nagy-Britannia határozottan ellenezte az uniós adatvédelmi szabályozást.[73] Az irányelvet végül mégis elfogadták 1995-ben; a tagállamoknak rendelkezéseit 1998-ig kellett implementálniuk.

5. Az irányelv az Európai Közösséget létrehozó szerződés 100a. cikkére alapul, olyan harmonizációs intézkedés, amely a 14. cikkben foglalt cél (az egységes belső piac) megvalósítását szolgálja. Célja azonban mégis kettős, ahogy ezt már a címe is tükrözi: „Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok

[71] Ennek a rendelkezésnek a hatályos magyar joggal kapcsolatos jelentőségéről lásd az Avt. 9. §-hoz fűzött magyarázatot.

[72] Jay–Hamilton 1999, 9.

[73] Jay–Hamilton 1999, 10.

feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról". Az irányelv preambulumában és 1. cikkében is megjelenik a kettős célkitűzés; ez utóbbi („Az irányelv célja" alcímet viselő) rendelkezés szerint:

„(1) A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében.

(2) A tagállamok nem korlátozhatják és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását az (1) bekezdés értelmében biztosított védelemmel kapcsolatos indokok miatt."

Az irányelv szabályozásának igényét a tagállami adatvédelmi szabályozások eltérése, az ebből adódó, az egységes belső piac kialakítását akadályozó hatások váltották ki: ebből egyesek azt a következtetést vonták le, hogy az irányelv *elsődleges* célja a tagállamok közötti szabad adatforgalom biztosítása, az egységes védelmi szint megteremtése.[74] Paradox módon azonban az egységes védelmi szintet úgy kell megteremteni, hogy az nem érintheti az egyes tagállami jogok által biztosított, az irányelv által megkövetelt„l „magasabb" védelmi szintet: erre utal az irányelv preambulumának 10. pontja, amely szerint „mivel a személyes adatok feldolgozására vonatkozó nemzeti jogszabályok célja az alapvető jogok és szabadságok, különösen a magánélet tiszteletben tartásához való jog védelme, amelyet mind az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény 8. cikke, mind a közösségi jog általános alapelvei elismernek; mivel ezért az említett jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez, sőt, magas védelmi szintet kell biztosítson a Közösségen belül". Ezt csak alátámasztja az a fejlemény, hogy a 2000-ben elfogadott Alapjogi Charta 8. cikke alapjogként ismeri el a személyes adatok védelméhez fűződő jogot,[75] és az – magával a chartával együtt – rövidesen részévé vált az Európai Unió Alkotmányának is.

---

[74] Még az irányelv emberi jogi megalapozottságát hangsúlyozó Korff is azt állítja, hogy a szabad adatáramlás biztosításának célja „talán elsődleges", Korff 2002, 6. Bennett szerint az irányelv tartalmát nemcsak az adatvédők 1980-as évek végére kialakuló közössége (policy community), hanem az üzleti érdekeket képviselő, ugyancsak nemzetközi szinten együttműködő csoportok is befolyásolták, „amely érdekek némileg ellentétesek az irányelv céljaival". „Sok a tagállamok rendelkezésére álló eltérésre módot adó rendelkezés, korlátozás, választási lehetőség, amelyek az adatvédelem fontos elemeit a legkisebb közös nevező szintjére csökkenthetik" (Bennett 1997, 106).

[75] „(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. (2) Az ilyen adatokat csak tisztességesen és jóhiszeműen meghatározott célokra az érintett személy hozzájárulása alapján vagy valamilyen

A célok egyenrangúságának vagy a harmonizációs cél elsődlegességének kérdése igen nagy gyakorlati jelentőséggel bír a magyar adatvédelmi jog értékelésekor is. A magyar jog számos szabálya az adatkezelők számára szigorúbb kötelezettségeket állapít meg, mint az irányelv által megkívánt szint. Vajon teljesül-e ebben az esetben a harmonizációs cél? Sérti-e az irányelvet a tagállam, ha szigorúbb adatvédelmi rendelkezéseket állapít meg, mint amelyeket az irányelv előír? Az Európai Bíróság 2003-ban már szembekerült a kérdéssel a Lindqvist-ügyben,[76] és válasza az volt, hogy a tagállami intézkedéseknek mind az irányelv rendelkezéseivel, mind a szabad adatáramlás céljával összhangban kell lenniük, ám a „tagállamot semmi nem akadályozza abban, hogy a 95/46 irányelvet átültető jogszabály hatályát kiterjessze olyan területekre, amelyek nem esnek az irányelv hatálya alá, ha ezt a közösségi jog más rendelkezései nem zárják ki". A magyar szabályozás legtöbb eltérése az irányelvtől vagy igazolható az irányelv által biztosított derogációs lehetőségek valamelyikével, vagy olyan esetekre vonatkozik, amelyek nincsenek az irányelv hatálya alatt: általában tehát az mondható, hogy a magyar szabályozás – a Lindqvist-döntés tükrében – megfelel az irányelv rendelkezéseinek. Megjegyzendő, hogy a Lindqvist-ügyben a Bizottság azt az álláspontot képviselte, hogy a tagállami jog nem biztosíthat magasabb védelmi szintet a személyes adatoknak, mint amelyet az irányelv tartalmaz, és nem állapíthatja meg szélesebb körben e jogszabályok hatályát sem. A Bíróság eltérő értelmezése álláspontunk szerint veszélyezteti a jogközelítés sikerét az adatvédelem terén.

6. Az irányelv rendelkezéseivel kapcsolatban elmondható, hogy azok sok esetben a korábbi dokumentumok megoldásaira építenek (elsősorban az ET-egyezményben foglaltakra), ám egyes esetekben túl is lépnek az ezek által meghatározott kereteken (így például az automatizált egyedi döntés szabályozásával)[77]. Az irányelvet alkalmazni kell a „személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni". Újdonság, hogy a szabályozás a már az OECD-irányelvekben és az ET-egyezményben megjelent, az „adatminőség" körébe sorolt követelményeken (tisztességes, törvényes adatfeldolgozás; célhoz kötöttség; szükségesség stb.) túl rögzíti az „adatfeldolgozás jogszerűvé tételére vonatkozó kritériumokat". Ez azt jelenti, hogy az irányelv taxatív

más, törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy róla gyűjtött adatokat megismerve, és joga van azokat kijavíttatni. (3) Az e szabályok tiszteletben tartását független hatóság ellenőrzi."

[76] C 101/01 (2003).

[77] Dammann–Simitis 1997, 218.

felsorolással határozza meg azokat az eseteket, amelyekben a tagállami jog lehetővé teheti személyes (ezen belül különleges) adatok kezelését. Az irányelv részletesen szabályozza az érintett tájékoztatáshoz és hozzáféréshez fűződő jogát, valamint meghatározott körben tiltakozási jogot is biztosít. A szabályozás tartalmazza az adatbiztonságra vonatkozó követelményeket, és új elemként előírja az adatkezelő számára a felügyelő hatóság „értesítésének" kötelezettségét az adatkezelésről, valamint lefekteti a felügyelő hatóság egyes intézkedéseire vonatkozó kereteket (előzetes ellenőrzés, nyilvántartás), a bírósági jogorvoslatra és szankciókra vonatkozó követelményeket. Szintén újdonság az irányelv „harmadik országokba" irányuló adattovábbításra vonatkozó szabályozásában a „megfelelő védelem" koncepciója: a korábbi „azonos" védelem mechanizmusa helyébe összetettebb rendszer lép: a védelem „megfelelőségének" vizsgálata számos tényezőre kiterjed, és abban szerephez jut a Bizottság.[78] Az irányelv rendelkezéseit nem külön: szövegét teljes egészében közöljük a Függelékben, illetőleg az Avtv. rendelkezéseihez kapcsolódóan is idézzük a releváns szabályokat.

7. Az irányelv nemzetközi hatása igen jelentős volt: az Unió szabályozása befolyásolta Új-Zéland és Hongkong adatvédelmi jogalkotását. Quebec 1993-ban elfogadott, magánszférabeli adatkezelőkre hatályos adatvédelmi szabályozása pedig az irányelv korai tervezetén alapult, s elfogadásának oka az Európa és Quebec közötti adatforgalom üzleti szempontból hátrányos – az EU szabályozása következtében beálló – akadályainak elhárítása volt.[79] Az európai szabályozás befolyása Dél-Amerikában is számottevő, ahol az 1980-as évek végétől megjelenő sajátos, ám az irányelv által megköveteltnél szűkebb körű védelem (a „Habeas Data") mellett (illetőleg helyett) megjelentek az európai mintát követő adatvédelmi törvények – az argentin jogszabály által nyújtott megfelelő védelemről már bizottsági döntés

[78] És bár az irányelv által a külföldre irányuló adattovábbítással kapcsolatban bevezetett „adekvát", „megfelelő" védelem zsinórmértéke megengedőbb, mint a korábbi nemzetközi dokumentumok, az OECD-irányelvek vagy az ET-egyezmény által szabályozott „azonos" védelemé, azonban ennek a követelménynek szigorúan érvényt lehet szerezni. A 25. cikk (4) bekezdése alapján ugyanis a tagállamoknak meg kell akadályozni az adattovábbítást azon országokba, amelyek nem nyújtanak megfelelő védelemet, míg a korábbi dokumentumokban ilyen kötelezettség nem szerepel. Bennett 1997, 109.

[79] Bennett 1997, 110. A szerző azt is megállapítja: „Az irányelv befolyásolja az EU-tagságra törekvő országok adatvédelmi politikáját is: 1992-ben például Magyarország volt az első állam Kelet-Európában, amely jogszabályt alkotott és adatvédelmi biztosi intézményt állított fel." Ha ez első tervezetek esetleg befolyásolták is a magyar szabályozás előkészítőit, a magyar szabályozás lényegesen előremutatóbb volt 1992-ben, mint amely a végül 1995-ben elfogadott irányelvből következne.

is született.[80] Az irányelv elfogadása ösztönözte a kanadai adatvédelmi szabványosítási törekvéseket is.[81] Az irodalomban megszületett a magánszféra-védelem szabályozásával kapcsolatos konvergencia gondolata:[82] e koncepció szerint az 1990-es években egyrészt az uralkodó technológia sajátosságai, a globális adatáramlás, másrészt pedig az irányelv elfogadása oda vezet, hogy az államok világszerte hasonló adatvédelmi politikát kezdenek követni (policy harmonization) – egy jelentős kivétellel, s ez az Egyesült Államok.[83]

8. Bennett szerint az amerikai fél részéről az 1970-es és 1980-as évek folyamán gyakran hangoztatott érv, amely szerint az adatvédelmi szabályozás a kontinentális jogra jellemző megoldás, s az „angolszász rendszer szűkebb szabályozási rezsimet feltételez, és ez az egyénre nagyobb felelősséget telepít abban, hogy bizonyítsa a kárt, és igényét bíróságon érvényesítse", sokat veszített erejéből azzal, hogy 1984-ben megszületett a brit, majd 1983-ban az új-zélandi adatvédelmi törvény.[84] Az állami szféra adatkezelését az Egyesült Államokban az 1974-es Privacy Act szabályozza; hasonló jogszabályokat fogadtak el tagállami szinten is. A magánszektorra vonatkozó szabályozás azonban töredékes, „szövetségi és tagállami rendelkezések hiányos hálója", és a megfelelő felügyelő hatóság is hiányzik.[85] Az Európai Unió hosszas tárgyalások után csak feltételesen (az ún. Safe Harbour Privacy-alapelvek keretében történő adatkezelések vonatkozásában) fogadta el „megfelelőnek" az Egyesült Államok által nyújtott védelmi szintet. A fent már tárgyalt, az általános személyiségi jog szerepét átvett privacyvel kapcsolatos joggyakorlat és az Egyesült Államokban kedvelt, gyakran magánszféravédő technológiákra építő önszabályozási rendszerek (lásd alább) tehát Európa szerint mégsem biztosítják az adatvédelem kielégítő szintjét. Az EU adatvédelmi irányelve alapján működő munkabizottság szerint:

„Az Egyesült Államok adatvédelemre és magánszféra-védelemre vonatkozó szabályozása a szövetségi és tagállami szabályozásipari önszabályozással kiegészített bonyolult szövete. A utóbbi hónapokban jelentős erőfeszítések történtek annak érdekében, hogy az ipari önszabályozás hitelét növeljék és gyakorlati érvényesülését elősegítsék,

[80] A „habeas data" szabályozása országonként eltér, ám általában biztosítja a hozzáférés, helyesbítés, törlés jogát és a célhoz kötöttség követelményét – nem alkalmas azonban például a külföldre irányuló adattovábbítás kontrolljára. Lásd Guadamuz 2000.

[81] Bennett 1997, 110.

[82] Lásd elsősorban Bennett 1992; Bennett 1997.

[83] Bennett megfogalmazása szerint ez az „American exceptionalism": Bennett 1997, 113.

[84] Bennett 1997, 112.

[85] Bennett 1997, 113.

különösen az internet és az elektronikus kereskedelem tekintetében. Mindennek ellenére a munkabizottság álláspontja az, hogy a szűkre szabott hatályú szektorális jogszabályok hálója és az önkéntesen követendő iparági önszabályozás jelenleg nem nyújt minden esetben megfelelő [adequate] védelmet az Európai Unióból továbbított adatok számára."[86]

9. A „megfelelő" védelemről folytatott hosszas tárgyalások után – melyek közben született a fent idézett értékelés is – EU Bizottsága és az Egyesült Államok képviselői 2000-ben jutottak eredményre. A megegyezés szerint az amerikai Kereskedelmi Minisztérium bábáskodása alatt elindul az a program, amelynek keretében egyes, az EU-irányelvnek megfelelő normák betartását vállaló amerikai cégeket az EU elismer olyannak, mintha az azokhoz történő adattovábbítás „megfelelő" védelemmel rendelkező állam területére történne. Az EU és az Egyesült Államok között e tárgyban született megállapodás az ún. Safe Harbour Agreement. A programhoz csatlakozó szervezeteknél biztosított védelmi szintet az Unió elfogadja az irányelv értelmezésében „megfelelőnek"; a csatlakozó szervezetnek meg kell felelnie bizonyos alapelveknek (Safe Harbour Principles); az alapelvek megtartását amerikai hatóságok (főszabály szerint a Federal Trade Commission) ellenőrzik.

10. Az irányelv a „megfelelő védelem" koncepcióján keresztül sokak szerint hatékonyan befolyásolta a nemzetközi adatvédelmi szabályozást – erre utalnak a fenti példák is. Ugyanakkor nem lehet eltekinteni azoktól a fejleményektől sem, amelyek ellentétes tendenciává állnak össze: a 2001. szeptember 11-ét követő terrorellenes harc jegyében jelenleg inkább az Egyesült Államok exportálja adatvédelmi politikáját Európába. Ez alapvetően a terrorellenes harc hatékonyságát korlátozó magánszféra-védelem szintjének csökkentésére irányul. Öt európai állam biometrikus azonosítókat tartalmazó útlevél kibocsátásáról döntött, miután az Egyesült Államok kilátásba helyezte a vízumkötelezettség bevezetését azon országok részére, amelyek nem vezetik be az új típusú okmányt.[87] Az Egyesült Államokba tartó repülőgépek utasainak adatszolgáltatásával kapcsolatban – amelynek célországa egy megfelelő védelmi szintet főszabály szerint nem biztosító állam! – a magyar adatvédelmi biztos is állást foglalt – majd az Unió megfelelőnek ismerte el az ilyen módon továbbított adatok védelmét. Az irányelv vélt extraterritoriális hatása helyébe tehát valóságos, ellentétes, irányú befolyás lépett. Ám az adatvédelem válsága nem 2001. szeptember 11-én kezdődött.[88]

---

[86] Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, 1999. január 26.

[87] *Öt nagy EU-ország megegyezett – biometrikus útlevél 2006-tól* (euro.hu 2004. október 21.).

[88] Mivel Magyarországon az ún. „privacy-szkeptikusok" – vagyis az adatvédelem, az adatvédelmi jog hasznát és

értemét megkérdőjelezők – véleménye szinte teljesen ismeretlen, az alábbiakban bemutatunk egy ilyen álláspontot Louis Bergkamp tanulmánya alapján (Bergkamp 2002). Bergkamp szerint megkérdőjelezhető az, hogy az EU adatvédelmi joga annak jelenlegi formájában szükséges és kívánatos lenne az információs társadalom körülményei között, s amellett érvel, hogy az adatvédelem korlátozza a fogyasztói választás lehetőségét és a fogyasztó szabadságát, s azt eredményezi, hogy a fogyasztók elavult, alacsonyabb minőségű termékekhez és szolgáltatásokhoz jutnak hozzá magasabb árakon. Bergkamp azt állítja, hogy bár a közvélekedés szerint az EU adatvédelmi rendszere szükséges az egyének védelméhez a személyes adatok nem helyénvaló felhasználása és a magánszférát fenyegető „növekvő" veszély ellen, holott „ezen kockázatokról és a szabályozás hatásairól empirikus adatok nem állnak rendelkezésre". A szerző szerint ráadásul a szegényeket az adatvédelmi előírásokból származó káros hatások aránytalanul sújtják, mivel bizonyos esetekben éppen amiatt nem képesek hozzájutni meghatározott árukhoz vagy szolgáltatásokhoz. Álláspontja szerint az EU adatvédelmi joga továbbá ösztönzi a csalást (fraud) és az őszintétlenséget (dishonesty), ezen felül korlátozza a versenyt és a WTO jogával ellentétesen kereskedelmi akadályokat képez. Az európai ipar csak amiatt képes a túlélésre emellett a szabályozás mellett, mert a végrehajtás különlegesen megengedő. „Az adatvédelem, ahogy az EU azt értelmezi, tévedés. [..] Érzelmi, és nem racionális válasz a növekvő adatforgalommal kapcsolatos rossz érzésekre."

A privacy-szkeptikusoktól megszokott társadalmi költség-haszon elemzésen túl Bergkamp jogi érveléssel is él. Álláspontja szerint a személyes adatok védelméhez fűződő jog gyakorta háttérbe szorítja Európában a véleményszabadsághoz fűződő jogot; az Egyesült Államokban azonban általában a véleményszabadsághoz fűződő jogot helyezik előtérbe. Ez a magyarázata annak, hogy az USA adatvédelmi joga csökevényes és inkoherens; az EU adatvédelmi joga azonban nyilvánvalóan visszaszorítja a véleményszabadságot az információszabadságot. Az adatvédelmi irányelv ugyan felhatalmazza a tagállamok kormányait, hogy kivételeket állapítsanak meg „újságírói" és „irodalmi" szempontokra tekintettel, ám a kereskedelmi szólásszabadság érdekében tett kivételre az irányelv nem ad lehetőséget.

A szerző szerint arra sincs bizonyíték, hogy a magánszektor általi adatvédelmi jogsérelem valós kárt okozott volna. Az okozott károk vagy elhanyagolható nagyságúak (például a kéretlen elektronikus üzenetek letöltésével együtt járó minimális kár), vagy hipotetikusak – az ismert valós sérelmeket mind államok okozták.

A magánszféra-védelem lehetővé teszi az egyén számára, hogy „definiálja önmagát, vagyis meghatározza, hogy milyen arcot mutat más személyek irányába". Ez az információs önrendelkezés, amelyen az EU adatvédelmi joga alapszik. A szerző kritikája szerint ez a jog maga is korlátozza az önrendelkezést. Ami még fontosabb: azzal, hogy lehetővé tesszük az embereknek, hogy megválasszák, mely arcukat mutatják a világnak, lehetővé teszi azt is, hogy másokat gazdasági vagy versenyelőnytől fosszon meg, illetve a maguk helyzetét mások költségére javíthassák.

A tanulmány számos túlzó és leegyszerűsítő állítása – valamint Posnerhez képest felületes volta – ellenére alkalmas arra, hogy érzékeltesse a „privacy-szkeptikusok" álláspontját. Magyarországon ma csak elméleti vitát lehet folytatni arról, hogy a jelen formájában szükség van-e az adatvédelmi jogra, hiszen annak léte és az EU adatvédelmi irányelvével történő összehangolása az országgal szemben követelmény. A joganyag „működésbe hozatala", a sokszor jogosan bírált hiányos szankciórendszer átalakítása, valamint az adatkezelők tájékoztatása és a részükre az adatvédelmi jog betartásához nyújtott segítség nyújtása azonban további erőfeszítést igényel: ennek hiányában az adatvédelmi jog puszta „írott malaszt" marad, rosszabb esetben diszfunkcionálisan működik, és válságba kerül – ebben az esetben Európában is többségbe kerülhetnek a Bergkamphoz hasonló „privacy-

1.5. Válság? A második generációs adatvédelmi szabályozás kritikája

1. Az információs önrendelkezési jog megfogalmazása óriási lépés az adatvédelem történetében, ám nem az utolsó lépés. A döntés Németországban először sokkot váltott ki az igazgatáson belül, majd megindult a jogalkotási dömping. Bäumler szerint a szektorális jogalkotás során – amely elsősorban a bűnüldözési és nemzetbiztonsági tevékenységet (Sicherheitsbereich) érintő szabályok módosítására terjedt ki – az igazgatás elérte azt, hogy az elfogadott törvények „elismerték" a már kiépített informatikai rendszerek létét, „a status quo törvényi szabályozása nagyobb engedmények nélkül sikerült".[89] Igen érdekes (különösen magyar nézőpontból) Bäumler összefoglalója a népszámlálás-ítéletet követő évekről:

„Azonban miközben az adatvédelem …győzelmet aratott győzelem után, növekvő mértékben igazolódtak azok a »népszámlálás-eufória« csúcsa idején különösnek ható előrejelzések, amelyek szerint történetének legmélyebb válsága felé halad. […] Az adatvédelem tartalmi kérdéseit egyre inkább kiszorították a jogalapra vonatkozó [kényelmesen feltehető, és a másik oldal számára oly kellemetlen] kérdések. Könnyű sikereket lehetett elérni addig, amíg a jogalapok mindenütt hiányoztak. Ám az ár hosszú távon magasnak bizonyult: az adatvédők a hiányzó jogalapokra történő makacs hivatkozással akadályoztak meg olyan törekvéseket, amelyek szándékuk szerint a lehető legértelmesebbek voltak. Amint azonban rendelkezésre állt a jogalap, sok polgár megütközéssel tapasztalta, hogy az igazgatás helyzete jogilag számukra elfogadhatatlanként feltűnő esetekben is tökéletesen be volt biztosítva. Miközben az adatvédők mindent akadályoztak, a polgárok pedig az adatvédelem hatástalanságát tapasztalták, két malom között őrlődve az adatvédelem tekintélye és imázsa sérült, és máig nem állt helyre."

Az információs önrendelkezési jogon alapuló adatvédelem „fogatlan papírtigrisnek", a felső középosztály játékszerének bizonyult.[90] Mayer-Schönberger érzékletesen írja le azt a helyzetet, amelyben az információs önrendelkezési joggal élve az egyén hozzájárulása a személyes adatok kezelésének legfontosabb jogalapja – a gazdasági erőfölényben, jobb alkupozícióban lévő adatkezelőkkel szemben az adatalany általában meg is adja a hozzájárulást, azaz valójában az adatvédelem nem érvényesül a magánszférát védő

---

szkeptikusok".

Az európai típusú adatvédelmi szabályozással szembeni érvrendszer koherens kifejtésére lásd még Posner 1984.

[89] Bäumler 1999, 3.

[90] Mayer–Schönberger 1997, 232.

mechanizmusként. „…A többség rutinszerűen és nem is tudatosan szerződésben mondott le információs önrendelkezési jogáról valamely üzleti megállapodás során, ráadásul maga a jog még csak nem is volt tényező az alkufolyamatban. Ám mivel – ha komolyan vesszük az információs önrendelkezési jogot – a hozzájárulásnak elegendő alapnak kell lennie az információ kezeléséhez, az információs önrendelkezési jognak az ilyen szerződésekkel történő leértékelése a jog szerint érvényes…" Az információs önrendelkezés joga ilyen körülmények között „a kisebbség privilégiuma marad, azoké, akik gazdaságilag és szociálisan megengedhetik maguknak, hogy éljenek jogaikkal – ám amire a szándék irányult, vagyis annak széles körű biztosítása, hogy az egyén saját maga formálhassa a róla információkból összeálló képet, a politikai retorika szintjén maradt".[91]

2. Lehetséges tehát, hogy a helyzet mégsem jobb, mint az Egyesült Államokban? Schwartz az internetes adatkezelésekkel kapcsolatos magánszféra-védelem tekintetében vizsgálja az Egyesült Államokban felmerült alternatívákat: ezek a piac által kínált megoldások, az ipari önszabályozás, valamint a jogi szabályozás. Schwartz szerint a legnépszerűbb az ipari önszabályozás, ám ő maga a jogi szabályozás szükségessége mellett érvel.[92] Ennek oka, hogy a magánszféra-védelem piaci „garanciái" valójában nem léteznek a cybertérben (sem). Schwartz szerint az adatalanyok nagy része nincs tudatában a személyes adatait illető felhasználási módoknak, ezen adatok piaci értékének, ezért nem is alkuképes az adatok felhasználását illető megállapodások megkötése során, amelyek így az adatkezelők érdekeit tükrözik („knowledge gap"). A másik ok a hozzájárulás gyakorlásának körülményeivel kapcsolatos – mivel annak gyakorlása a legtöbb esetben nem alapul megfelelő információkon (tehát nem „tájékozott" beleegyezésről van szó), továbbá számos esetben az önkéntesség is kérdéses (például bizonyos weboldalak megtekintésének lehetőségét az üzemeltető az adatvédelmi szabályok [policy] elfogadásához köti – „consent fallacy"), ezért a piac önmagában nem képes a magánszféra megfelelő védelmére (Schwartz rendszerében a „tisztességes információkezelés elveinek" [fair information practices] érvényesítésére).[93] Bár nyilvánvaló, hogy az európai polgár kedvezőbb helyzetben van – az adatkezelőket köti az

[91] Mayer–Schönberger 1997, 232. A „hozzájárulás-humbug" (consent fallacy) jelenségét elemzi az Egyesült Államokban a cybertérben működő vállalkozások adatkezelési modelljeit elemzve Schwartz 2002. Egyes weboldalak a belépéshez szabják feltételül a hozzájárulást, mások olyan adatvédelmi politikát (privacy policy) fogalmaznak meg, amelyek az oldal látogatását az adatkezeléshez történő hozzájárulásnak tekintik. Ez a hozzájárulás azonban a gyakorlatban a legtöbbször nem informált és nem önkéntes (Schwartz 2002, 73).

[92] Schwartz 2002, 70.

[93] Schwartz 2002, 71–73.

adatvédelmi jog számos alapelve, a célhoz kötöttség, a szükségesség stb. – az alapvető probléma, a consent fallacy, az információs önrendelkezési jogra építő rendszerek esetében is fennmarad.

Mindez igen jól érzékelhető a tipikusan második generációs szabályozásnak tekinthető magyar adatvédelmi törvénnyel kapcsolatos jogalkalmazási problémákat elemezve. Az ügyek vizsgálata igen gyakran a jogalapok formális vizsgálatában merül ki;[94] a hozzájáruláson alapuló adatkezelések esetén, főképp az üzleti forgalomban, a jogalkalmazó kényszermegoldásokkal, bonyolult és gyakran téves jogértelmezéssel próbálja segíteni az információs önrendelkezési jogának értéktelenségét tapasztaló, a nagy adatkezelő szervezeteknek kiszolgáltatott egyént.

3. Az információs önrendelkezési jogon alapuló második generációs szabályozás hatékony érvényesülését nem csak a rendelkezési jog alanyának az adatkezelőkkel szembeni gyenge pozíciója akadályozta. Az 1990-es években kiteljesedett az a korábbi tendencia, amely a centalizált adatbankok világától a hálózatba kötött mikroszámítógépek korszakáig vezetett. A nemzetközi számítógépes hálózat, az internet tömeges alkalmazása, az egyre olcsóbb számítógépek, az egyre nagyobb tárolókapacitású digitális adathordozók megjelenése oda vezetett, hogy a hétköznapi életet is áthatotta a mindenütt jelen lévő elektronizált adafeldolgozás és -tárolás, ezzel a magánszféra-védelemnek gyökeresen új közegben kell hatékonyan érvényesülnie.

A centralizált adatbankok szabályozására az adatvédelem megfelelő eszköz volt. Az új körülmények között azonban a technológia már számos esetben megkerülte a jogi szabályozást; annak érvényesítése egyre nehezebbé vált.[95] Az adatvédelem mint a magánszféra-védelem új és hatékony módja a múlté volt: az anakronisztikus szabályok merev

[94] Például követeléskezelő cég nem vehető igénybe követelés behajtására, ám ügyvéd – a létező törvényi felhatalmazás miatt – igen (ABI 2001, 146); a jogalapok vizsgálatával kapcsolatos megállapításokról lásd például a ABI 2001, 276; ABI 2002, 23 stb.

[95] Hasonló folyamat ment végbe a szólásszabadságra vonatkozó jogi szabályozással kapcsolatban, ahol szintén az új technológia egyik jellemzője – annak nemzetközi jellege – teszi kétségessé a jogi normák hatályosulását: egy híressé vált megfogalmazás szerint „az internet hibaként értelmezi a cenzúrát, és létrehozza a kerülőutakat". John Gilmore megfogalmazását idézi Gelman 1998, 22. Nem véletlen, hogy a jogi szabályozás fogyatékosságai (az adatvédelmi jog érvényesíthetőségével kapcsolatos kétségek, illetőleg az amerikai Communications Decency Act alkotmányosságával kapcsolatos, 1996-tól kibontakozó vita) a két területen hasonló, a szabályozást szolgáló technológiák fejlesztéséhez vezettek: ilyen a Platform for Internet Content Selection (PICS) és a Platform for Privacy Preferences (P3P). A szólásszabadsággal kapcsolatos korai esetekre lásd Jóri 1998; a technológia által szabályozásra és a technológia alakításának jogi lehetőségeire mindkét területen lásd Lessig 1999.

alkalmazása csak a Bäumler által leírt presztízsveszteséget erősítette. A magánszféra-védelem hatékony védelmére új, jogon kívüli eszközök jelentek meg, amelyek azonban maguk is jogi szabályozás tárgyává váltak.

Az alábbiakban két olyan példát mutatunk be, amelyek a magánszféra szinte szükségszerű „összeszűkülését" illusztrálják az új körülmények között.

4. A *cégnyilvántartás* arra szolgál, hogy a hitelezők érdekeinek védelme, a forgalom biztonsága érdekében megismerhetők legyenek a cégek adatai (cégnyilvánosság), közöttük a cégben tagként, cégjegyzésre jogosultként, vezető tisztségviselőként vagy felügyelőbizottsági tagként szereplő természetes személyek adatai is. Az érintett személyek ebben az esetben természetesen nem hivatkozhatnak a személyes adatok védelméhez fűződő alkotmányos jogukra, hogy a betekintést megakadályozzák. A keresés – általában – csak a cég „irányából" célhoz kötött, s ezáltal jogszerű.[96]

Az elektronikus adatkezelés lehetősége azonban a gyakorlatban igen megnehezíti ennek az előírásnak az érvényesítését. A cégjegyzék adatainak felhasználásával készült, CD-ROM-on forgalmazott nyilvántartások közül ismereteink szerint jelenleg is van olyan, amely lehetőséget ad arra, hogy ún. „teljes szövegű keresést" végezzünk: ezen keresési mód segítségével a felhasználó a nyilvántartás összes mezőjében keresheti a megadott karaktersort. A keresés könnyen végezhető úgy, hogy eredményül a megadott személy érdekeltségeit kapjuk. Ez azonban már az eredeti céltól eltérő adatkezelést eredményez. Az adatok ilyen lekérdezésével olyan következtetésekre juthatunk, amelyek levonására a hagyományos cégnyilvántartás használatával csak a törvény által meghatározott személyeknek lenne módjuk. Az adatvédelmi hatóságok természetesen javasolhatják, hogy a CD-ROM-ok forgalmazói fordítsanak figyelmet az ilyen keresőfunkciók mellőzésére, ám a szoftver minimális módosításával ezek a lehetőségek házilag is megteremthetők. Megtiltható az ilyen CD-k forgalmazása, ám a megfelelő berendezésekkel nem jelent nehézséget a hivatalos lap példányaiban megjelent adatokat elektronikus formába átvinni, s így a keresés lehetősége ismét megteremthető. A technológia tehát ebben az esetben oly módon alakít át egy hagyományos intézményt – a cégnyilvánosságot –, hogy az a személyes adatok védelmét immár a szükséges mértéknél jobban korlátozza, s jelenleg nem látni olyan megoldást, amellyel a technológia fejlődésének ez a nem szándékolt következménye kiküszöbölhető lenne.

5. A második példa a büntetőjogban ismert *mentesítés* intézményével kapcsolatos. A büntetőjog szerint a mentesítés következményeképp az elítéltet nem terhelik az elítéléshez fűzött hátrányos jogkövetkezmények.[97]

A mentesítés intézménye mögött az a megfontolás húzódik, hogy az elkövetőnek meg kell adni a társadalomba történő visszailleszkedés lehetőségét, és azt az emberképet tükrözi, amely képesnek tartja az elkövetőt a reintegrációra.[98] Ugyanakkor a folyamatos jelenben létező események és adatok nyomait egy hatalmas, kereshető adatbázisba gyűjtő nemzetközi számítógépes hálózat működése nyomán a mentesítés intézménye a jövőben nehezen érvényesülhet. A hatályos büntető eljárásjog szerint ugyanis a tárgyaláson hozott határozat rendelkező részét abban az esetben is nyilvánosan hirdeti ki a bíróság, ha a tárgyalásról a nyilvánosságot kizárta".[99] A helyi újság természetesen tudósíthat, majd e tudósítás a lap elektronikus archívumába is bekerülhet – s onnan akár évtizedek múlva is előhívható. Az interneten az adatok halmozódnak: bár a jelenlegi szabvány (IPv4) helyébe fokozatosan újabb lép (IPv6)[100], a korábbi szabványok szerint létező Internetet az új mintegy „magába olvasztja" majd – vagyis e hatalmas adatbázis adattartalma megmarad. Vajon miképp biztosítható, hogy bármely munkatársat kereső munkáltató ne használja rendszeresen az internet keresőgépeit arra, hogy a jelentkezők közül kiszűrje a rovott múltúakat? A mentesítés intézménye könnyen kiüresedhet: igen szofisztikált jogi szabályozásra van szükség ahhoz, hogy az ilyen esetekben az egyént megillető jogok valóban érvényesüljenek. A „feledés" többé nem létezik, az adategyeztetés előtt álló gátak megszűnnek. Minden olyan információ, amely valaha nyilvánosságra került az interneten, társítható bármely további ilyen információval. Már léteznek olyan projektek is, amelyek célul tűzték ki az internet meghatározott időtartamonként rögzített teljes adattartalmának rögzítését, és olyan technológia biztosítását, amely nemcsak a mindenkor elérhető, hanem a múlt adott időpontjában vagy időtartamában elérhető adattartalomban teszi lehetővé a keresést.[101] Vajon a sajtóhelyreigazításra vonatkozó jogi

---

[96] Tükrözi ezt a magyar szabályozás is. A cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény (Ctv.) vonatkozó rendelkezései a csoportosított cégadatok igénylése során rögzítik a célhoz kötött adatkezelés érvényesítéséhez szükséges feltételeket (14. §)

[97] A magyar szabályozás szerint „a mentesítés folytán az elítélt mentesül azon hátrányos következmények alól, amelyeket az elítéléshez jogszabály fűz", a továbbiakban büntetlen előéletűnek minősül, s nem tartozik számot adni az adott elítéltetésről (Btk. 100. §).

[98] Az intézményről részletesen lásd: Bárd–Gellér–Ligeti–Margitán–Wiener A. 2002, 240.

[99] 1998. évi XIX. tv. 239. § (2) bekezdés

[100] Az IPv6-ról lásd az internet Society weblapját: http://www.isoc.org/briefings/006/.

[101] Lásd http://www.archive.org.

szabályok érvényesítése a megoldás?[102] Vagy az adatok törlésének az adatvédelmi szabályozás által biztosított joga? Aligha. A mentesítés célja ugyanis éppen a „tiszta lap" biztosítása az elítélt számára, olyan helyzet megteremtése, amelyben nem kell elszámolnia múltjával, a fenti jogi eszközök alkalmazása pedig éppen elszámolásra kényszerít. Ha az érintett nem ugyanabban a kisközösségben élt cselekménye elkövetésekor és büntetése letöltése után is, a mentesítés intézményének megalkotásakor fennállt körülmények között az elítélt számíthatott arra, hogy valóban új életet kezdhet. A magánszféra azonban a korlátlan jelenidőt biztosító, mindenki számára elérhető hálózat miatt leszűkült: a megoldást talán olyan jogi szabályozás jelenthetné, amely megkülönbözteti a valódi jelen idejű, múlékony nyilvánosságot (a tárgyalás nyilvánosságát, sőt akár a gyors adategyeztetést nehezítő, papíralapú médiumokban biztosított nyilvánosságot) a nyilvánosság olyan formáitól, amelyek emberi léptékben örökké elérhetővé teszik az egyébként feledésre ítélt információt.

6. A mindent átható technológia tehát összeszűkíti a magánszférát; az adatvédelem, a magánszféra jogi védelme mellett új – a technológiára alapozó – védelmi módok is megjelennek, a második generációs adatvédelmi szabályozás pedig reformra szorul: intézményei az új közegben egyes esetekben kifejezetten diszfunkcionálisan működnek. E szabályok anakronizmusára jó példa *az adatvédelmi nyilvántartásba történő bejelentkezési kötelezettség*. Ez a kötelezettség az adatvédelmi szabályozás korai szakaszában megjelent: az adatbankok bejelentésének, sőt engedélyeztetésének kötelezettsége a nagy, centralizált adatbázisok korában az adatvédelem működésének alapvető feltétele volt. Az adatvédelmi nyilvántartások szabályozása azonban idővel – alkalmazkodva a körülményekhez – változott, a szabályozások egyre több kivételi kört ismertek el. Az elektronikus környezetben végzett adatkezelés mindennapivá válása azonban még ezeket a megengedőbb szabályokat is anakronisztikussá teheti.

Az internet számítógépes hálózat legnépszerűbb alkalmazása a World Wide Web, amely lehetővé teszi, hogy a felhasználók szöveges, képes, hangos információt egy egységes felületen hívjanak le távoli számítógépekről (szerverekről). A böngészés során e távoli számítógépeken azonban az esetek nagy részében megmarad a felhasználó számítógépének (kliens) nyoma: a szerveren ugyanis egy állományban (logfile) rögzül, hogy mely (az internet-protokoll szerinti IP-címmel azonosított) számítógép mely állományt mely időpontban hívott le. A logfile-elemzés igen fontos a rendszer biztonságán őrködő rendszergazda számára,[103] de

[102] Vö. a BH 1988. 98 sz. jogesettel.

[103] Lásd például: Pulay–Sziklássy–Tóth–Udvaros 1997, 4. fejezet.

a weblap látogatottságának mérésére, cookie-k alkalmazásával valamely látogató visszatérésének jelzésére, sőt regisztrációs űrlap alkalmazása mellett egy adott, ismert személy látogatási szokásainak felmérésére is alkalmas. Ez utóbbi esetben nyilvánvaló, hogy személyes adatok kezeléséről van szó, az érintettet tájékoztatni kell, s meg kell tartani a személyes adatok védelmére vonatkozó jogszabályi előírásokat. Kérdés mármost, hogy a webszerveren logfile-ban tárolt IP-címek személyes adatnak minősülnek-e abban az esetben, ha további azonosító mechanizmusok nincsenek, a felhasználó csupán egy statikus weblapot tekint meg, s gépének csupán az IP-címe rögzül a szerver naplófájljában?

Az IP-cím – ha meghatározott természetes személlyel kapcsolatba hozható – mind a magyar, mind az EU-tagállamokban uralkodónak tekinthető jogalkalmazói gyakorlat szerint személyes adatnak minősül. Ezen álláspontot elfogadva felmerül a kérdés: szükség van-e ebben az esetben az ilyen naplófájlok – amelyek, hangsúlyozzuk, a webszerverek igen nagy hányadán léteznek, s amelyek rögzítése a rendszerbiztonság fenntartása miatt indokolt – bejelentésére az adatvédelmi nyilvántartásba az alkalmazandó adatvédelmi jog alapján? Ez esetben az adatkezelő szerverüzemeltetők széles körére ró a jogalkotó olyan kötelezettséget, amely álláspontunk szerint nem méltányos: az internet infrastruktúrájában tömegével keletkező forgalmi adatok és a valóban az érintett személlyel kapcsolatba hozható, s ezáltal „érzékenyebb” adatok megkülönböztetése a jogalkotás során mindenképpen indokolt.

Az új technológia által meghatározott közegben tehát a magánszféra összeszűkül, sőt, az az informatikai ipar egyik csúcsvezetőjének hírhedt mondása szerint már meg is szűnt.[104] Az adatvédelmi törvények egyes rendelkezései nem érvényesülnek, míg mások felesleges terheket rónak az adatkezelőkre, amelyek e szabályokat tömegesen ignorálják (lásd erre a magyar adatvédelmi nyilvántartás ún. „elutasított kérelmek nyilvántartására” vonatkozó szabályozását). Mi a kiút? Újszerű jogi szabályozás? A már évtizedek óta az irodalom kedvelt témái közé tartozó, ám áttörő eredményt mindeddig nem produkáló magánszféravédő technológiák alkalmazása? Vagy mindez együtt?

Az e kérdésre született válaszkísérleteket a dolgozat 3. részében összegezzük; ezt megelőzően azonban részletes elemzés alá vonjuk egy, az információs önrendelkezési jog elméletén alapuló második generációs szabályozás, a magyar adatvédelmi jog rendelkezéseit.

[104] „Már most sincs magánszférájuk. Lépjenek túl ezen” („You already have zero privacy – get over it”) – fogalmazott Scott McNealy, a Sun Microsystems elnök-vezérigazgatója 1999-ben. Idézi Schwartz 2002, 77. Az eredeti hír: http://www.wired.com/news/politics/0,1283,17538,00.html.

2. EGY MÁSODIK GENERÁCIÓS SZABÁLYOZÁS RÉSZLETES ELEMZÉSE: A MAGYAR ADATVÉDELMI JOG DE LEGE LATA ÉS DE LEGE FERENDA

1. Szabályozási környezet: az Alkotmány és az alkotmánybírósági gyakorlat

1.6. A magánszféra-jogok az Alkotmányban

1. A magánszférához való jogot (a magánélet szabadságához való jogot)[105] az Alkotmánybíróság az Alkotmány 54. §-ában megfogalmazott emberi méltósághoz való jogból mint általános személyiségi jogból vezeti le[106]. A magánszféra lényegi fogalmi eleme az AB szerint, hogy „az érintett akarata ellenére mások oda ne hatolhassanak be, illetőleg be se tekinthessenek"[107]. A magánszférához való joggal ellentétes az AB szerint pl., ha „valakivel szemben kellő alap nélkül alkalmaznak hatósági kényszert, s ezáltal az állam indok nélkül avatkozik be a magánszféra körébe tartozó viszonyokba."[108] A magánszférához való jog lényeges tartalmát korlátozza az olyan szabályozás, amely a közalkalmazottak számára előírja, hogy azok a munkahelyen kívül is a közalkalmazotti jogviszonyhoz méltó magatartást kötelesek tanúsítani és ezeket a magatartás-szabályokat munkaviszonyon belüli hátrányokkal - fegyelmi büntetéssel – szankcionálja[109].

2. Az 59. § (1) bekezdésében felsorolt jogok olyan nevesített alapjogok, amelyek a magánszféra meghatározott elemeinek (jóhírnév, magánlakás, magántitok) védelmére irányulnak, illetőleg a magánszféra védelmét sajátos módon (a nem feltétlenül a magánszférába sorolható, akár nyilvános adatokkal kapcsolatos egyes követelmények érvényesítésén keresztül) biztosítják. Számos korlátozás megítélésekor az AB párhuzamosan hivatkozik az 54. §-ban foglalt emberi méltósághoz fűződő alapjog egy elemét képező magánszférához való jogra és az 59. § (1) bekezdésében foglalt valamely nevesített jogra: így pl. a közjegyzői végrehajtási záradék intézményének kellő garanciák nélküli szabályozása

[105] 56/1994. (XI. 10.) AB határozat, ABH 1994, 312, 312

[106] Az AB gyakorlatában a magánszférához való jog mint az általános személyiségi jog egyik megnevezése, másképp egy aspektusa első említése: 8/1990. (IV. 23.) AB határozat (ABH 1990, 42, 44); máshol a magánszférához való jog az emberi méltósághoz való jog egyik eleme: „[A]z emberi méltósághoz való jog korántsem csupán a jó hírnévhez való jogot foglalja magában, hanem egyebek között a magánszféra védelméhez fűződő jogot is." (46/1991 (IX. 10.) AB határozat, ABH 1991, 184, 187)

[107] Elektronikus úton történő megfigyeléssel kapcsolatban: 36/2005. (X. 5.) AB határozat, ABH 2005, 390, 400

[108] 46/1991 (IX. 10.) AB határozat, ABH 1991, 184, 187

nem csak a magánlakás sérthetetlenségéhez fűződő, az 59. § (1) bekezdésében nevesített alapjogot sérti, hanem a magánszférához való jogot is[110]. Egyes esetekben vitás lehet, hogy valamely tényállást az AB (kizárólag) az 54. §-ban foglalt jog, vagy (ezzel párhuzamosan) valamely nevesített jog alapján ítéljen meg. Ilyen eset pl. a kamerák vagy hangfelvevő eszközök segítségével végzett megfigyelés, amely lehetséges oly módon, hogy a megfigyelés eredményét nem rögzítik, illetőleg úgy is, hogy az eredményt felveszik és tárolják. A testület a témával foglalkozó első, 2002-ben született határozata a két mozzanatot nem különíti el, és mind a magát a megfigyelést, mind az adatok tárolását, további kezelését mint az 59. § (1) bekezdésében meghatározott személyes adatok védelméhez fűződő jog korlátozását értékeli[111]; Harmathy Attila párhuzamos indokolásában azonban már ekkor kifejti, hogy, a fényképfelvétel vagy hangfelvétel kezelését előíró jogszabályok vizsgálatakor az Alkotmány 54. § (1) bekezdésében foglalt emberi méltósághoz fűződő jogot kell alapul venni[112]. 2005-ben már az AB többsége is úgy foglal állást, hogy „az Alkotmány 54. § (1) bekezdésében deklarált emberi méltósághoz való jog lényeges tartalmát érinti az, ha az elektronikus megfigyelőrendszer alkalmazását lehetővé tevő szabályozás figyelmen kívül hagyja a magánszféra tiszteletét és védelmét”[113], és csak a rendszer alkalmazásával nyert adatok további kezelésének elbírálásakor hívja fel az Alkotmány 59. § (1) bekezdését[114].

3. Az AB gyakorlatából kiolvasható két álláspont az Avtv. alkalmazásának kontextusában úgy vethető fel, hogy az Avtv. szerinti adatkezelés történik-e rögzítés nélküli megfigyelés esetén, s így az ilyen tevékenysége az Avtv. hatálya alá tartozik-e. Az adatvédelmi biztos mind csak megfigyelést szolgáló, mind a megfigyelt képet rögzítő rendszerek esetében több esetben állást foglalt; ám gyakorlata a kérdésben ellentmondásokkal terhelt[115]. Az az értelmezés, hogy a megfigyelőkamerák működtetése, a szóbeli adattovábbítás stb. nem tartoznak az adatvédelmi jog hatálya alá, kizárná az adatvédelmi biztos fellépésének lehetőségét, számos esetben lerontaná az adatvédelmi jog által biztosított garanciákat. Az ezzel ellentétes interpretáció – bár módot ad a biztosnak a fellépésre a fentiekhez hasonló

---

[109] 56/1994. (XI. 10.) AB határozat, ABH 1994, 312

110 46/1991 (IX. 10.) AB határozat, ABH 1991, 184, 187

[111] 35/2002. (VII. 19.) AB határozat, ABH 2002, 199, 206

[112] ABH 2002, 199, 217. Harmathy érvelése a személyes adat fogalmának értelmezéséhez is kapcsolódik; lásd erről még alább az adat fogalmának tárgyalásakor.

[113] 36/2005. (X. 5.) AB határozat, ABH 2005, 390, 400

[114] 36/2005. (X. 5.) AB határozat ABH 2005, 390, 403-404; az adatok tárolási idejének az indokoltnál hosszabb tárolásával kapcsolatban ebben az esetben is megállapítja az 54. § sérelmét is (ABH 2005, 390, 406).

esetekben – annak ellenzői szerint abszurd következményekkel járhat: adatkezelésnek minősülne ebben az esetben bármely személyes adat érzékelése is (például utcán álló gépjármű rendszámának leolvasása, az aktuális pletyka meghallgatása). Nézetünk szerint ilyen esetekben az Avtv. által meghatározott adatkezelés megvalósul[116].

Ebből az értelmezésből természetesen nem következik az, hogy a rögzítés nélküli megfigyelés esetén is megállapítható – az Alkotmány 54. § (1) bekezdése által védett emberi méltóság, illetőleg magánszféra korlátozása mellett – az 59. § (1) bekezdése szerinti információs önrendelkezési jog korlátozása is, hiszen ennek további feltétele, hogy az AB mind az Alkotmányban foglalt személyes adat fogalmát (mind azt, hogy az azon végzett cselekmények mely köre korlátozza a személyes adatok védelméhez fűződő jogot) úgy értelmezze, ahogyan azt a törvényhozó az Avtv-ben meghatározta.

4. A jóhírnévhez való jog az 59. § (1) bekezdésében foglalt jogok közül az Alkotmánybíróság által legkevésbé kibontott, inkább mindenkor a 61. § által biztosított véleményszabadság külső korlátjaként értelmezett jog.

Míg a jóhírnév védelmét az Alkotmány 59. § (1) bekezdése nevesíti[117], az AB az emberi méltóság anyajogából (54. §) vezeti le a becsület alapjogi védelmét[118]. „Bár emberi méltósága csak a hatóságot képviselő hivatalos személynek lehet, a társadalom kedvező értékítéletére, megbecsülésére azonban maga a hatóság is igényt tarthat."[119] A jó hírnév védelme az Alkotmány szövege szerint „mindenkit" megillet, így a hatóság vagy hivatalos személy becsületének vagy jó hírnevének büntetőjogi védelme sem ellentétes az Alkotmánnyal, ám az alkotmányosan védett véleménynyilvánítás köre a közhatalmat gyakorló személyekkel és intézményekkel, valamint a közszereplő politikusokkal kapcsolatos véleménynyilvánítást tekintve tágabb legyen, mint más személyeknél[120].

---

[115] A vonatkozó adatvédelmi biztosi gyakorlatra lásd Jóri 2005, 148.

[116] Ezt támasztja alá az Avtv. 1. § 9. pontja szövegének – amely adatkezelésnek minősít az adatokon végzett „bármely műveletet" - nyelvtani értelmezése, továbbá a 95/46/EK irányelv 2. cikk b) pontjában foglalt meghatározás, amellyel az Avtv. meghatározását összhangban kell értelmezni. Lásd erre részletesen: Jóri 2005, 147-149.

[117] „Az Alkotmánybíróság ugyancsak az emberi méltósághoz való jog egyik - az Alkotmányban nevesített - elemeként kezeli a jó hírnévhez való jogot." (43/2004. (XI. 17.) AB határozat, ABH 2005, 390, 406.)

[118] 36/1994. (VI. 24.) AB határozat (ABH 1994, 219, 229.)

[119] 36/1994. (VI. 24.) AB határozat (ABH 1994, 219, 229.)

[120] 36/1994. (VI. 24.) AB határozat

A jó hírnév mint külső korlát érvényesül mind az értékítéletben megnyilvánuló véleménynyilvánítási szabadság[121], mind a tényállítások, akár „a becsületsértésre alkalmas, valóságnak megfelelő tények, információk" közlése esetén[122]. Ez utóbbi esetben a jóhírnév védelme indokolhatja – az emberi méltóság és a becsület alkotmányos oltalma mellett – a tudatosan valótlan tartalmú tényállítások kizárását a véleménynyilvánítási szabadság köréből[123]. Ez a külső korlát a véleménynyilvánítási szabadság részét képező parlamenti szólásszabadság esetén is érvényesül, ha a közhatalmat nem gyakorló illetőleg közszereplőnek nem minősülő személyek jó hírneve sérül, ám csak szűkebb körben abban az esetben, ha közhatalmat gyakorló személyek vagy közszereplő politikusokról van szó[124].

5. A magánlakás sérthetetlenségéhez való jog „az emberi méltósághoz való jog, mint általános személyiségi jog alkotó eleme, olyan az Alkotmányban nevesítetten biztosított jog, amely a magánszféra egyik jelentős összetevőjének sérthetetlenségét alapozza meg"[125], Az AB a magánlakás sérthetetlenségéhez való alapjogot – az Egyezmény 8. cikkével összhangban - negatív jellegű alapjogként, védelmi jogként értelmezeti a védett tárgykörben a kívül állók bizonyos zavaró, beavatkozó, sértő megnyilvánulásaitól való mentességre és a mentesség állami védelmére jogosít."[126] A alapjogi védelem terjedelmét meghatározó magánlakás-fogalom körülhatárolásához támpont, hogy az AB a védelem „irányultságának és tárgykörét" kifejező rendelkezésként hívja fel a Btk. magánlaksértés tényállását, amelynek elkövetési tárgya a lakás, egyéb helyiségébe, és az ezekhez tartozó bekerített hely, valamint a magánlakás sérthetetlenségéhez fűződő alapjog korlátozásának tekinti a büntető eljárásjog

[121] Az értékítéletre, az egyén személyes véleményére a véleménynyilvánítási szabadság minden esetben kiterjed, függetlenül attól, hogy az értékes vagy értéktelen, igaz vagy hamis, érzelmen vagy észérveken alapul. A szintén alkotmányos oltalom alatt álló emberi méltóság, becsület, jó hírnév azonban az értékítéletben megnyilvánuló véleménynyilvánítási szabadság külső korlátja lehet, és ezek védelmében a büntetőjogi felelősség érvényesítése sem tekinthető - általánosságban - aránytalannak, így alkotmányellenesnek". (ABH 1994, 219, 230.)

[122] 36/1994. (VI. 24.) AB határozat

[123] Ám más a határ, ha a véleménynyilvánítás szabadsága nem ezen alapjogokkal, hanem pl. a köznyugalommal mint alkotmányos értékkel kerül kollízióba: lásd a 18/2000. (VI. 16.) AB határozatot

[124] 34/2004. (IX. 28.) AB határozat

[125] 1115/B/1995. AB határozat, ABH 1996, 551, 552

[126] 1115/B/1995. AB határozat. A jog alkotmányos korlátozására a határozat indokolása az (akkor hatályos) Be. ház, lakás, egyéb helyiség vagy azokhoz tartozó bekerített hely, továbbá jármű hatósági átkutatására vonatkozó szabályait említi példaként, ABH 1996, 551, 552

azon rendelkezéseit, amelyek „ház, lakás, egyéb helyiség vagy azokhoz tartozó bekerített hely, továbbá jármű hatósági átkutatásának eljárási feltételeit és rendjét állapítják meg”[127].
Az AB szerint „ez az alapjog egyaránt kapcsolódhat a tulajdonos, a birtokos és más jogos lakáshasználó, így pl. a lakásbérlő, a társbérlő, az albérlő stb. valamely konkrét lakást érintő jogához.”[128] A magánlakás védelme mindenkit megillet, és mint az AB – az Emberi Jogok Európai Bíróságának gyakorlatát követve[129] – állást foglalt, az kiterjed a hivatás gyakorlását szolgáló helyiségekre, a gépjárműre, lakásra is[130]. Az AB értelmezése azt jelenti, hogy Alkotmányból következő magánlakás-fogalom – bár azok elemeit a fentiek szerint magában foglalja – nem szűkíthető le a Btk. magánlaksértés elnevezésű tényállásában, a polgári törvénykönyv személyiségi jogi fejezetében, vagy a rendőrségről szóló törvényben használt fogalomra[131]. Nem a magánlakás sérthetetlenségéhez fűződő jog, hanem az Alkotmány 54. §

[127] 1115/B/1995. AB határozat, ABH 1996, 551, 553. Az AB a határozat idején hatályos büntetőeljárási kódex (1973. évi I. törvény) szabályozására hivatkozik. Kühne a német irodalom alapján a fogalmat egy szubjektív (lakásra rendeltetés) és egy objektív (felismerhetőség) elemmel határozza meg oly módon, hogy abban közterületen elhelyezett telefonfülkék, padok, stb. is beletartozhatnak, lásd Kühne 2006, 569.

[128] 1115/B/1995. AB határozat, ABH 1996, 551, 552

[129] Niemietz v. Germany (Publications of the European Court of Human Rights, Series A.No. 251.)

[130] 26/2004. (VII. 7.) AB határozat ABH 2004, 398, 417

[131] A Btk. 176. § (1) bekezdése szerint „aki másnak a lakásába, egyéb helyiségébe vagy ezekhez tartozó bekerített helyre erőszakkal, fenyegetéssel, hivatalos eljárás színlelésével bemegy, vagy ott bent marad, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő”; a bírósági gyakorlat szerint nem valósul meg magánlaksértés abban az esetben, ha nem lakás céljára szolgáló helyiségbe történik a behatolás, mert ezek a helyiségek a házijog körén kívül esnek (lásd BH 1994.523). Szélesebb körben érvényesül a polgári jogi védelem: a Ptk. 82. §-a szerint [a] törvény védi a magánlakáshoz és a jogi személy céljaira szolgáló helyiségekhez fűződő jogot”. A rendőrségről szóló 1994. évi XXXIV. törvény alkalmazásában a magánlakás „a lakás (üdülő, nyaraló vagy a lakás céljára használt egyéb helyiség, létesítmény, tárgy), az ahhoz tartozó nem lakás céljára szolgáló helyiség, létesítmény, bekerített terület” (97. § (1) bekezdés c) pont). Az AB többsége szerint e törvényi meghatározás nincs összefüggésben a magánlakás sérthetetlenségéhez fűződő alkotmányos alapjoggal (44/2004. (XI. 23. AB határozat, ABH 2004, 618, 653), ám két különvéleményt fogalmazó bíró is ezzel ellentétesen foglalt állást. Holló András különvéleménye szerint „[h]a a magánlakás törvényi fogalma nem, vagy nem egyértelműen fogja át az alkotmányos alapjog védelmi körét, a definíció a magánlakás sérthetetlenségéhez való jog alkotmányellenes korlátozását eredményezi” (ABH 2004, 618, 668); Tersztyánszkyné Vasadi Éva úgy foglal állást, hogy „a magánlakás fogalmát az Rtv-nek az Alkotmányból következő magánlakás-fogalommal egyezően kell megállapítania”, s mivel az Rtv. meghatározása nem öleli fel a csupán hivatás gyakorlására szolgáló helyiségeket, az sérti a magánlakás sérthetetlenségéhez fűződő jogot (ABH 2004, 618, 671).

bekezdésében biztosított magánszférához való jog korlátozását valósítja meg az egyéb, nem magánlakásnak minősülő területen, ám intim helyzetben történő megfigyelés[132].

6 . A magánlakás sérthetetlenségéhez fűződő alapjog – más alapjogokhoz hasonlóan – csak az Alkotmány 8. § (2) bekezdésében meghatározottak szerint korlátozható[133]. Az AB alkotmányos korlátozásnak minősítette - a bíróságnak az igazságszolgáltatással kapcsolatos alkotmányos feladatainak végrehajtása mint alkotmány cél érdekében – a magánlakás sérthetetlenségéhez fűződő alapjog korlátozását a szemle karhatalom igénybevételével történő lebonyolítását[134]; szintén a magánlakás sérthetetlenségéhez fűződő jog alkotmányos korlátozását jelenti a rendőrségi törvény azon rendelkezése, amely szerint a rendőr bűncselekmény elkövetésének megakadályozása, megszakítása, vagy a bűncselekmény elkövetőjének vagy gyanúsítottjának elfogása és előállítása céljából beléphet vagy behatolhat bebocsátás és hatósági határozat nélkül magánlakásba[135].

Alkotmányosnak minősülnek a rendőrségi törvény azon előírásai is, amelyek a rendkívüli vagy tisztázatlan okból bekövetkezett haláleset vizsgálata céljából vizsgálat (szemle, hatósági boncolás) esetén[136] teszik lehetővé a magánlakásba történő belépést, amelyek– az állam életvédelmi kötelezettsége, mint alkotmányos cél érdekében – védett személyek védelme érdekében adnak bebocsátás és hatósági határozat nélkül belépésre és egyes intézkedésekre (ellenőrzés, helyszín megfigyelése és biztosítása) a rendőrség számára[137], valamint amelyek – a büntetőjogi igény érvényesítése és a közbiztonság védelme mint alkotmányos célok érdekében – az előállítás foganatosítása céljából biztosítanak – jól körülírt esetekben – lehetőséget a magánlakásba történő belépésre[138].

---

[132] „A részben értelmezési problémát felvető, részben pedig hiányos szabályozás alkalmatlan arra, hogy a magánszféra különösen érzékeny területeit (intim helyzeteket: pl. próbafülkében, mosdóban, öltözőben, illemhelyen való tartózkodást) a megfigyelés alól teljes egészében kivonja.” 36/2005. (X. 5.) AB határozat, ABH 2005, 390, 401.

[133] Pl. 44/2004. (IX. 23.) AB határozat, ABH 2004, 618

[134] 392/B/1998. AB határozat, (ABK 2004. január 2., 3.)

[135] Ebben az esetben a korlátozás szükségességi eleme (az alkotmányos cél) a büntetőjogi igény késedelem nélküli teljesítéséhez fűződő állami kötelezettség, míg az arányosságot a rendőrségi törvény azon rendelkezése biztosítja, amely szerint a magánlakásban tartózkodás csak a feladat végrehajtásához szükséges ideig tarthat (44/2004. (XI. 23.) AB határozat, ABH 2004, 618, 650)

[136] 44/2004. (XI. 23.) AB határozat, ABH 2004, 618, 650

[137] 44/2004. (XI. 23.) AB határozat, ABH 2004, 618, 651

[138] 44/2004. (XI. 23.) AB határozat, ABH 2004, 618, 652

A magánlakás sérthetetlenségéhez fűződő jog alkotmányosan csak az Alkotmánybíróság alapjogi tesztjét kielégítő módon korlátozható[139]. A magánlakás sérthetetlensége némely esetben elválaszthatatlanul összefonódik a magántitokhoz és személyes adatokhoz fűződő joggal, s azok sérelmét az AB együttesen állapítja meg[140].

1.7. A magántitok és a személyes adatok védelméhez való jog

1.7.1. A magántitok fogalma, a magántitok és a személyes adat viszonya

1. A magántitok jogi védelmének kialakulása időben megelőzi a személyes adatok védelmének megjelenését, és a szabályozás tárgya is adatok, tények egy szűkebb csoportja (a magánszemély magántitka mindenkor egyben személyes adatnak is minősül).
A titok esetében fogalmi elem az, hogy a szóban forgó tény a nyilvánosságtól elzárt legyen, és a nyilvánosság kizárásához a jogosultnak valamely érdeke fűződjön,

---

[139] A magánlakás sérthetetlenségéhez fűződő jog alkotmányellenes korlátozására lásd: 46/1991. (IX. 10) AB határozat (ABH 1991, 184): a végrehajtási záradékolás adott módon való szabályozása „megfelelő garanciák" hiányában alkotmányellenes; 26/1994. AB határozat: az adózás rendjéről szóló törvényben az átvizsgálás intézményével kapcsolatban, amely „aránytalan", s nélkülözi a megfelelő garanciákat)

[140] Így hatósági tanú alkalmazása esetén az „szükségképpen betekintést nyer a nyomozási cselekményekkel érintett személyek magánéletébe - akár annak rendkívül intim részleteibe is (pl. házkutatás, motozás) -, olyan információk birtokába jut, amely az érintettek Alkotmány által védett magánszférája, magántitkainak, személyes adatainak körébe tartoznak, s amelyek illetéktelen személyek tudomására jutása, nyilvánosságra kerülése az érintetteknek az Alkotmány 54. § (1) bekezdésében, valamint 59. § (1) bekezdésében szabályozott alapvető jogainak sérelmét eredményezi. Az Alkotmánybíróság álláspontja szerint a magánszférához való jog sérelmét jelenti az is, ha valaki akarata ellenére, belegyezése nélkül köteles tűrni azt, hogy számára idegen személy a magánéletébe betekintést nyerjen, tanúja legyen a személyét érintő kényszercselekményeknek, a magántitkai, személyes adatai körébe tartozó információkhoz jusson. Így a büntetőeljárási jognak nemcsak az alkotmányos alapjogoknak a nyomozó hatóság által történő korlátozása tekintetében kell biztosítani a az alapjogok védelmének garanciáit, hanem az eljárásba az eljáró hatóság által bevont, közhatalommal nem rendelkező közreműködők tekintetében is megfelelő jogi biztosítékokkal kell körülbástyáznia a nyomozási cselekményekkel érintettek magánszférához való jogát". Az AB szerint Mindezeket figyelembe véve az Alkotmánybíróság hivatalból eljárva megállapította, hogy alkotmányellenes helyzet keletkezett annak következtében, hogy a büntetőeljárásról szóló Be. a hatósági tanú alkalmazásával kapcsolatosan nem állapította meg az Alkotmány 54. § (1) bekezdésében, valamint 59. § (1) bekezdésében szabályozott alapvető jogok védelmének garanciális szabályait. (43/2004 (XI. 17.) AB határozat). Hasonlóan az „59. § (1) bekezdésében biztosított alkotmányos jogok" sérelmére hivatkozva semmisített meg az AB – csomagátvizsgálásról szóló - jogszabályt a 2/2007. (I. 24.) AB határozattal.

E két elem jelenik meg az irodalomban: Balás P. szerint a titokszférába tartozik „minden tény, mely tényleg nem közismert és nem közészlelhető s a személy maga sem akarja, hogy ilyen legyen”[141], és a bírói gyakorlatban is („[m]agántitok minden olyan bizalmas, - csak szűk körben, illetve beavatottak előtt ismert személyi, családi, vagyoni helyzetre, egészségi állapotra, szokásokra vonatkozó tény vagy adat, amelynek nyilvánosságra hozatala a sértettre érdeksérelemmel jár” (BH 2004.170)).

A titokra vonatkozó szabályozás olyan eseteiben, ahol a titkossághoz fűződő érdekkel szemben egyes esetekben a nyilvánossághoz fűződő érdek is állami elismerést nyerhet, további elemként jelenik meg a titkosság fenntartásához szükséges intézkedések megtétele: így a Ptk. 81. § (2) bekezdése szerint „[ü]zleti titok a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette”. Ahol a nyilvánossághoz fűződő érdek különösen erős – így az államtitok és szolgálati titok esetén – a szabályozás további, a titokként minősüléshez szükséges formai-eljárási követelményeket állít fel, lásd az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény minősítésre vonatkozó rendelkezéseit (7. és köv. §§).

2. A személyes adat jogi védelme olyan adatokra is kiterjed, amelyek esetén a fenti feltételek nem állnak fenn. Így személyes adatként jogi szabályozás tárgyává lehet olyan adat, amelynek nyilvánosságra kerülése önmaga nem sérti az érintett érdekeit. Az érdeksérelem az adatok informatikai eszközök alkalmazásával történő feldolgozásával, összekapcsolásával, értékelésével állhat elő; így a magánszféra védelme érdekében a jog elismeri az egyén rendelkezési jogosultságát olyan adatok felett is, amelyek nem titkosak[142].

---

[141] Balás P. 1941, 652.

[142] Az információs önrendelkezési jogot lefektető alkotmánybírósági határozatok egyértelműen emiatt adnak teret az újszerű alapjogi védelemnek (15/1991. (IV. 13.) AB határozat, ABH 1991, 39; BVerfGE 65,1). Ugyanakkor az egyes elfogadott adatvédelmi szabályok nem minden esetben különböztethetők meg ilyen élesen a hagyományos titokvédelmi rendelkezésektől. Az osztrák adatvédelmi törvény az adatvédelemhez való alapjog legfőbb elemét kifejezetten a titokvédelem mintájára határozza meg: „[m]indenki igényelheti – különösen magán- és családi élete tekintetében – az őt érintő személyes adatok titokban tartását, ha ehhez védendő érdek fűződik. Ilyen érdek fennállása kizárt, ha az adatok azok általános elérhetősége vagy az érintetthez történő kapcsolat visszaállíthatóságának hiánya miatt a titokban tartáshoz fűződő igényt megalapozására nem alkalmasak”. (Datenschutzgesetz 2000, 1. § (1)) - ám az osztrák adatvédelmi jog is biztosít egyes jogokat már nyilvánosságra került adatok vonatkozásában is (lásd pl. a törvény 8. § (2) bekezdését).

3. Az Alkotmánybíróság már a 2/1990. (II. 18.) AB határozattól kezdve az 59. § (1) bekezdésének „a magántitok és a személyes adatok védelme" fordulatát használja olyan esetekben is, amelyekben a határozat tárgya egyértelműen csak a személyes adatok védelméhez fűződő jog, és nem tisztázott, hogy ezekben az esetekben az AB azonosítja-e a magántitkot és személyes adatokat[143]. A pontos megkülönböztetés hiányának oka nyilvánvalóan az, hogy a személyes adatok védelme az AB gyakorlatában rendszerint – a titoknak minősülő tények személyes adatkénti minősülése miatt – magába olvasztja a magántitok-védelmet[144].

4. A magántitokhoz fűződő jog önmagában két vonatkozásban nyert jelentőséget az Alkotmánybíróság gyakorlatában. Az első, hogy az Alkotmánybíróság rögzítette: az 59. § (1) bekezdése – mint a magántitokhoz való jog alapvető részét – védi a levéltitkot is[145].
A második, hogy az AB szerint az 59. § alkalmazásában a magántitok fogalma alá tartozik az üzleti titok is[146]. Ez utóbbi tény jelentőséget nyerhet atekintetben, hogy az 59. § (1) bekezdésében meghatározott jog milyen tartalommal – az információs önrendelkezési jog teljességével, vagy meghatározott titkokra vonatkozó védelmi jellegű jogként – illeti meg a jogi személyeket és a jogi személyiség nélküli szervezeteket.

1.7.2. Az információs önrendelkezési jog és garanciái

[143] Lásd erre: Majtényi 2006, 168. Majtényi rámutat arra is, hogy Sólyom különvéleményében kerüli a magántitok és a személyes adat fogalmának együttes használatát, és „a személyes adatok védelméhez való jogról" ír (uo.)

[144] A német alaptörvény 10. szakasza, amely a levél-, postai és távközlési titok sérthetetlenségéről rendelkezik, lex specialis az információs önrendelkezési jog védelméhez képest (Pagenknopf 2006, 492.)

[145] 634/B/1991 AB határozat (ABH 1993, 558) A levéltitok védelmének tartalmát az AB nem bontotta ki; a hatályos Btk. a levéltitok megsértése tényállásban nem csak a szűk értelemben vett levéltitok megsértését (közlést tartalmazó zárt küldemény megismerés céljából történő felbontása, stb.), hanem a távközlési titok megsértését (távközlési berendezés útján továbbított küldemény kifürkészését) is szankcionálja.

[146] „Az Alkotmány 59. § (1) bekezdése a magántitok védelméhez való jogról szól. Az Alkotmány 59. §-a alkalmazásában az üzleti titok is a magántitok fogalma alá tartozik. Az üzleti titok védelmének elvét számos törvény tartalmazza, ezek a törvények az üzleti titkot részben eltérő rendelkezésekkel védik. Az üzleti titok megsértését jelentheti általában, ha az üzleti titkot jogosulatlanul szerzik meg, használják fel vagy hozzák nyilvánosságra." 26/2004. (VII. 7.) AB határozat, ABH 2004, 398, 420

1. Az Alkotmánybíróság a személyes adatok védelméhez fűződő jogot információs önrendelkezési jogként értelmezi: „E jog tartalma az, hogy mindenki maga rendelkezik magántitkainak és személyes adatainak feltárásáról és felhasználásáról." (20/1990. (X. 4.) AB határozat)[147]. Maga az információs önrendelkezési jog kifejezés először a német Alkotmánybíróság ún. népszámlálásdöntésével párhuzamba állítható, az egységes személyi szám alkotmányellenességét kimondó kulcshatározatában, a 15/1991. (IV. 13.) AB határozatban szerepel[148].

A döntés indokolása szerint: „Az Alkotmánybíróság – a 20/1990. AB határozat szerinti eddigi gyakorlatát folytatva – a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként."[149] A testület ebben a határozatban már részletesebben fejti ki az információs önrendelkezési jog tartalmát, amelynek lényege, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Általános követelményként rögzítette a bíróság, hogy személyes adatot felvenni és felhasználni csak az érintett beleegyezésével[150] szabad. Csak kivételes az az eset, amelyben személyes adat kötelező kezelését törvény rendeli el: „Az

[147] ABH 1990, 69, 70. Hangsúlyozni kell azonban, hogy az AB gyakorlatán kívül a két fogalom nem feleltethető meg egymásnak teljes egészében: az információs önrendelkezési jog koncepciója csak jóval az adatvédelem (tehát az egyén magánszférájának sajátos, személyes adatai kezelésének szabályozásán keresztül érvényesülő jogi védelme) megjelenését követő fejlemény, amelynek megjelenése a német alkotmánybíróság 1983-as népszámlálás-ítéletéhez köthető, s az jellemzően az adatvédelmi szabályozások ún. második generációját jellemzi. (A népszámlás-ítélet hatása a 15/1991. (IV. 13.) AB határozatra annak szövegéből is egyértelműen kitűnik, illetőleg maga az információs önrendelkezési jog is „tükörfordítása a német [informationelle Selbstbestimmung] kifejezésnek" (Sólyom 2005., 181.)

[148] ABH 1991, 39, 40

[149] Kiemelés az eredetiben.

[150] A hozzájárulás fogalmának speciális adatvédelmi jog meghatározását adja az Avtv. (2. § 6 pont), ennek elemzésére lásd Jóri 2005, 136-141..; az AB gyakorlata szerint „az a törvényi feltétel, miszerint az érintett személynek az alapjogi korlátozáshoz ráutaló magatartással történő hozzájárulása akár ahhoz is elegendő, hogy őt intim helyzetben megfigyeljék, sérti az emberi méltósághoz való alkotmányos alapjogot". 36/2005. (X. 5.) AB határozat, ABH 2005, 390, 401, ill. lásd Kukorelli István és Kiss László bírák különvéleményét a 35/2002. (VII. 19.) AB határozathoz: „Abból, hogy előzetesen tájékoztatni kell a résztvevőket a kamerázásról, nem következik, hogy minden résztvevő önként beleegyezik a megfigyelésbe, mivel a megfigyelést törvény írja elő, és a nézők nincsenek abban a helyzetben, hogy egyenrangú félként megegyezzenek a feltételekről. A határozat tehát helyesen indul ki abból, hogy a volenti non fit iniuria elv nem alkalmazható, és alapjog-korlátozásnak kell tekinteni a szabályozást." (ABH 2002, 199, 226)

ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek."

Az adatkezelésnek átláthatónak kell lennie: „mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát". Az átlátható adatkezelés követelményéből közvetlenül következő tájékoztatáshoz fűződő jog mellett az információs önrendelkezési jog eleme a helyesbítéshez való jog, a törléshez való jog, valamint a jogok érvényesítéséhez szükséges előfeltételek biztosítása, így pl. az adatok továbbításáról szóló nyilvántartás vezetése.

2. Az információs önrendelkezési jog két legfontosabb garanciája a célhoz kötöttség és az adatok továbbításának és nyilvánosságra hozatalának korlátozása. Ezeket az információs önrendelkezési jog korlátozását megvalósító szabályokkal kapcsolatos speciális követelményeknek tekintjük, így alább - az AB általánosan alkalmazott alapjogi tesztjének az 59. § vonatkozásában történő alkalmazásának bemutatását követően – tárgyaljuk.

Az információs önrendelkezési jog áthatja a magyar adatvédelmi jogi szabályozást: az Avtv. adatkezelés jogalapjára vonatkozó szabályozása, a célhoz kötöttség elvének – szükségesség elvével együttesen - törvényi szinten történő rögzítése, az átlátható adatkezelést szolgáló, az adatalany számára biztosított jogok, illetőleg az adatminőséggel kapcsolatos követelmények az információs önrendelkezési jogot szolgálják, annak gyakorlásának kereteit határozzák meg. Az univerzális, általános célú személyi szám lényegénél fogva ellentétes az információs önrendelkezési joggal. Lásd ennek részletes tárgyalását alább.

1.7.3. Az információs önrendelkezési jog korlátozásának általános feltételei

1. Az Alkotmánybíróság gyakorlata szerint az információs önrendelkezési jogként értelmezett személyes adatok védelméhez fűződő jog alkotmányos alapjog, azonban nem abszolút jog: törvény azt korlátozhatja; a korlátozás azonban csak akkor alkotmányos, ha eleget tesz az Alkotmányban meghatározott követelményeknek[151].

A személyes adat kezelését elrendelő törvény minden esetben korlátozza az Alkotmány 59. § (1) bekezdésében rögzített személyes adatok védelméhez fűződő alapjogot. Az Alkotmány 8. § (2) bekezdése szerint: „A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg […]"

[151] 2/1990. (II. 18.) AB határozat (ABH 1990, 18), 15/1991. (IV. 13.) AB határozat (ABH 1991, 39, 41)

2. Az alkotmányos alapjogok korlátozásának az Alkotmánybíróság gyakorlata szerint formai és tartalmi követelményei vannak. A formai feltételek egy része a jogalkotási eljárással, az elfogadott jogszabály érthetőségével stb. kapcsolatos (ezek összefoglalva a jogbiztonsággal kapcsolatos követelmények),[152] más része pedig a jogkorlátozó norma jogforrási szintjével. Az alapjogot korlátozó norma tartalmi alkotmányosságának megítélése során az Alkotmánybíróság a korlátozás szükségességét[153] és arányosságát vizsgálja.

Az Avtv. 3. § (1) bekezdésének szabálya azt írja elő a normaalkotó számára, hogy – törvényi felhatalmazás alapján alkotott önkormányzati rendelet[154] kivételével – az adatkezelést csak törvényben rendelhet el.

Az Alkotmány 35. § (2) bekezdése szerint „a Kormány a maga feladatkörében rendeleteket bocsát ki […] A Kormány rendelete […] törvénnyel nem lehet ellentétes." Az Alkotmány 37. § (3) bekezdése szerint: „A Kormány tagjai feladatuk ellátása körében rendeleteket adhatnak ki. Ezek azonban törvénnyel vagy a Kormány rendeletével és határozatával nem lehetnek ellentétesek." A jogalkotásról szóló 1987. évi XI. törvény 1. § (2) bekezdése szerint: „[…] az

[152] Halmai-Tóth 2003a, 118.

[153] Pl. Célzott vagy ígért gazdasági növekedés, tartós gazdasági növekedés feltételeinek kibontakoztatása illetőleg az ehhez fűződő közérdek az információs önrendelkezési jog korlátozásnak nem elegendő alkotmányos indoka (46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 224). Ugyanakkor igen korán megjelent – bár nem vált egy ellenkező tendencia kiindulópontjává – egy olyan határozat, amely relativizálta az információs önrendelkezési jogot. A kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény (az ún. direktmarketing-törvény) számos, az információs önrendelkezési jogra vonatkozó korlátozó rendelkezést tartalmaz: a direktmarketing-tevékenységet végző cégek meghatározott feltételek mellett felhasználhatják a hasonló tevékenységet végző más társaságok adatbázisait, volt ügyfeleik adatait, nyilvános adatbázisok tartalmát, valamint adatokat igényelhetnek a központi népesség-nyilvántartásból. Az az állampolgár, aki nem kívánja, hogy adatait ezen direktmarketing-célokra felhasználják, erre irányuló nyilatkozattal kérheti adatainak letiltását (ún. opt-out modell). Álláspontunk szerint nincs olyan alkotmányos cél, amely az adott esetben indokolja az információs önrendelkezési jog korlátozását: a jogalkotó álláspontunk szerint egy gazdasági szektor érdekét helyezte az adatalanyok joga elé, amikor elfogadta Magyarországon az opt-out modellt. Az Alkotmánybíróság álláspontja szerint azonban a szabályozás alkotmányos, mivel az rögzíti az adatkezelés célját, valamint „az Avtv-vel összhangban állapítj[a] meg a személyes adatokkal való rendelkezés jogának korlátozását". A határozat azonban nem tér ki arra, hogy a törvény direktmarketing célú adatkezeléseket lehetővé tévő szabályai, az ezek által megvalósuló alapjogkorlátozás mely másik alkotmányos jog, illetőleg alkotmányos cél érvényesítéséhez szükséges (876/B/1996.).

[154] Törvényi felhatalmazáson alapuló önkormányzati rendeletben szabályozott adatkezelés alkotmányosságának kimondására lásd pl. a 57/2003. (XI. 21.) AB határozatot.

alacsonyabb szintű jogszabály nem lehet ellentétes a magasabb szintű jogszabállyal". Személyes adat kezelésének kormányrendeletben, miniszteri rendeletben, illetőleg nem törvényi felhatalmazás alapján alkotott önkormányzati rendeletben foglalt elrendelése tehát – mivel az Avtv. 3. § (1) bekezdésébe ütközik – formailag alkotmányellenes[155]. Már a 15/1991. (IV. 13.) AB határozat rögzíti, hogy a kezelt adatok körének rendeletben történő meghatározására vonatkozó felhatalmazás is alkotmányellenes[156]. Az AB szerint azonban az alkotmányos jogok „csupán távolról, közvetetten érintő, technikai és nem korlátozó jellegű" szabályozása rendeleti szinten is történhet[157]. Ugyanakkor az AB szerint személyes adatok kezelése csak akkor rendelhető el, „ha az adatkezelés lehetővé tételével egyidejűleg meghatározza az adatkezelés pontos feltételeit, azaz az Alkotmány 59. § (1) bekezdésben garantált személyes adatokhoz való alapjog korlátozásának konkrét részletszabályait."[158] Fokozott figyelemmel kell lenni arra is, hogy az Avtv. 3. § (3) bekezdése kötelező adatkezelés esetén megkívánja az adatkezelés egyes részleteinek (cél, „az adatkezelés feltételei", a kezelendő adatok köre és megismerhetősége, az adatkezelés időtartama, az adatkezelő személye) az adatkezelést elrendelő törvényben vagy önkormányzati rendeletben történő szabályozását, így ezen attributumok az Alkotmány 35. § (2) bekezdésének vagy 37. § (3)

[155] Az Alkotmánybíróság formai okból nyilvánította alkotmányellenesnek a személyes adatok védelméhez fűződő jog korlátozását előíró miniszteri rendeleti (11/1990. (V. 1.) AB határozat, ABH 1990, 156, 29/1994. (V. 20.) AB határozat, ABH 1994, 148, 27/2002. (VI. 28.) AB határozat, ABH 2002, 143, 38/2003. (VI. 26.) AB határozat,), kormányrendeleti (12/1996. (III. 22.) AB határozat, 59/1998. (XII. 11.) AB határozat, 25/2002. (VI. 21.) AB határozat) szintű szabályozást, illetőleg egyes adatkezelések országgyűlési határozatban (50/2003. (XI. 5.) AB határozat), belső utasításban (47/2003. (X. 27.) AB határozat) történő előírását.

[156] Az Avtv. 2003-as novellájával ez a szabály törvényi rendelkezéssé vált: „kötelező adatkezelés esetén […] a kezelendő adatok körét […] az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg" (Avtv. 3. § (3) bekezdése)

[157] 64/1991. (XII. 17.) AB határozat. Így az Alkotmánybíróság szerint alkotmányos az a rendeleti szintű szabályozás, amely névkitűző viselését tette kötelezővé egyes személyek számára olyan esetben, amikor a névkitűzőn szereplő adatok nyilvánosságát törvény mondja ki (54/2000. (XII. 18.) AB határozat). Az 56/2000. (XII. 19.) AB határozatban az Alkotmánybíróság az akkor hatályos egészségügyről szóló törvény végrehajtásáról szóló MT rendelet azon szabályainak alkotmányosságát vizsgálta, amelyek előírták, hogy vélelmezni kell a beteg hozzájárulását egészségügyi dokumentációja átadásához – más esetek mellett – akkor, ha az általa választott háziorvos feladatait annak körzetében (rendelőjében) időlegesen vagy véglegesen más háziorvos látja el. Az AB szerint az az előírás, amely a hozzájárulást a helyettesítő orvosnak történő továbbítás esetén vélelmezi, alkotmányos. Az érvelés szerint ebben az esetben a vizsgált rendelkezés „nem minősül az egészségügyi állapottal összefüggő adatok továbbítását előíró rendeleti szabálynak", mivel az csak az Eüatv.-ben, tehát törvényi szinten megfogalmazott szabályok „meghatározott esetben való alkalmazását fogalmazza meg".

bekezdésének sérelme nélkül nem szabályozhatók kormányrendeletben vagy miniszteri rendeletben.

3. Az Alkotmánybíróság állandó gyakorlata szerint a személyes adatok védelméhez fűződő jog minden korlátozásának „meg kell felelnie az alapjogi korlátozás mindenkori alkotmányos feltételeinek, azaz az Alkotmány 8. § (2) bekezdésében foglalt követelményeknek. Ez azt jelenti, hogy az információs önrendelkezési jogot, az Alkotmány 59. § (1) bekezdésében biztosított szabadságjogot mint alapjogot csak elkerülhetetlen esetben lehet alkotmányosan korlátozni, akkor ha a korlátozás elkerülhetetlenül szükséges és az a korlátozással elérni kívánt célhoz képest arányos."[159] Az AB a személyes adatok védelméhez kapcsolódóan rögzítette először azt a követelményt, hogy a korlátozás során a jogalkotónak a cél eléréséhez alkalmas legenyhébb eszközt kell választania[160].

A személyes adatok védelméhez fűződő jog korlátozása kapcsán az AB többször kimondta, hogy (ha az nem az Alkotmányban van szabályozva) közérdek önmagában nem indokolhat alapjog-korlátozást[161]. Így az Avtv. 3. § (4) bekezdésében foglalt rendelkezés ellenére – amely szerint „[t]örvény közérdekből – az adatok körének kifejezett megjelölésével – elrendelheti a személyes adat nyilvánosságra hozatalát". A nyilvánosságra hozatal „elrendelésének" valós korlátait nem az Avtv. határozza meg, hanem az Alkotmánybíróság alapjogi korlátozások vizsgálatakor alkalmazott tesztje.

---

[158] 65/2002. (XII. 3.) AB határozat, ABH 2002, 357, 363

[159] 46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 223

[160] 20/1990. (X. 4.) AB határozat, ABH 1990. 69, 71.] Lásd azonban az AB állásfoglalását a névkitűző viselésének, mint a hivatalos közeg egyediesítésének vizsgálatával kapcsolatban: „A megfelelőbbnek, célszerűbbnek tekintett módszer kiválasztása a jogalkotó hatáskörébe tartozik. Az alkotmányos célnak egyaránt megfelelő módszerek közötti választás nem alkotmányossági kérdés" (54/2000. (XII. 18.) AB határozat.)

161 Lásd pl. „a közérdek fennállásának és alkotmányos indokának a vizsgálatánál is a szükségesség-arányosság ismérveit alkalmazza", (46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 224), vagy 60/1994. (XII. 24.) AB határozat. Az AB néhol mégis bevonja a közérdeket a személyes adatok védelmét illető korlátozás alkotmányosságának indokolásába, lásd pl. a 26/2004 (VII. 7.) AB határozatot: „A jelen eseten nyilvánvaló, hogy a nyilvánosságra hozatal elrendelését előíró szabály a vizsgált törvény alapján alkotmányos kötelezettségen alapul, közérdekből történik és mások jogainak megóvása a célja" (ABH 2004, 398, 416).

1.7.4. Az információs önrendelkezési jog sajátos garanciái: célhoz kötöttség, az adattovábbítás és az adatok nyilvánosságra hozatalának korlátozása

1. Az információs önrendelkezési jog érvényesülésének két legfőbb garanciája a célhozkötöttség, valamint az adattovábbítás és az adatok nyilvánosságra hozatalának korlátozása. Ezeknek a garanciáknak mindenkor együttesen kell érvényesülnie, nem vagylagos feltételei valamely adatkezelés elrendelésének[162]. A célhozkötöttség elve az Alkotmánybíróság alapjogi tesztje szükségességi elemének konkretizálása az 59. § (1) bekezdésére[163].

A célhozkötöttség jelentése az Alkotmánybíróság gyakorlatában az, hogy személyes „adat kezelése mindenkor csak előzetesen lefektetett, meghatározott, jogszerű, bejelentett és „közhitelűen rögzített" célra szabad[164]. Az adatkezelésnek annak minden szakaszában – az adat felvételétől annak törléséig- meg kell felelnie a célnak. A 15/1991. (IV. 13.) AB határozat szerint az adatkezelés „célját úgy kell az érintettel közölni, hogy az megítélhesse az adatfeldolgozás hatását jogaira, és megalapozottan dönthessen az adat kiadásáról; továbbá, hogy a céltól eltérő felhasználás esetén élhessen jogaival. Ugyanezért az adatfeldolgozás céljának megváltozásáról is értesíteni kell az érintettet. Az érintett beleegyezése nélkül az új célú feldolgozás [kezelés] csak akkor jogszerű, ha azt meghatározott adatra és feldolgozóra [adatkezelőre] nézve törvény kifejezetten megengedi"[165]. Az Alkotmánybíróság gyakorlata rögzíti azt a követelményt is, hogy az adatkezelési célnak pontosan meghatározottnak kell lennie[166], ám egyes esetekben mégis elfogad olyan általános célmeghatározásokat, amely

[162] 15/1991. (IV. 13.) AB határozat, ABH 1991, 39, 43

[163] 65/2002. (XII. 3.) AB határozat, ABH 2002, 357, 362)

[164] 15/1991. (IV. 13.) AB határozat, ABH 1991, 39, 41

[165] 15/1991. (IV. 13.) AB határozat, ABH 1991, 39, 41

[166] Lásd pl. a 65/2002. (XII. 3.) AB határozatot, amely alkotmányellenesnek minősítette az Eüatv. rendelkezését, amely egészségügyi adatnak minősítette a szexuális szokásokkal kapcsolatos adatokat abban az esetben, ha a törvény által felállított négy adatkezelési cél valamelyike fennállt. Az Alkotmánybíróság szerint a „meghatározott célok együttesen aránytalanul széles, pontosan meg nem határozott körben teszik lehetővé a szexuális szokásokra vonatkozó adatok kezelését. A szexuális szokásokra vonatkozó különleges adatok kezelése céljának túl tág meghatározása pedig nem felel meg az alapjog-korlátozással szemben támasztott szükségességi mércének." Az AB szerint: „ A különleges személyes adatoknak minősülő, szexuális szokásokkal összefüggő adatok kezelésével szemben követelményként érvényesül, hogy az adatkezelésnek konkrét célhoz kötöttnek kell lennie. Az adatkezelési cél túlságosan tág módon történő meghatározása, azaz ha nincs összefüggésben az adatkezelés a megjelölt céllal, továbbá, ha arra bizonytalan esetkörben kerül sor, illetve arra nem a szükséges

szerint valamely adatkezelésre pl. „mások jogainak és biztonságának védelme érdekében” van szükség[167]. Távoli, elvont veszély elhárítása nem jelent olyan célt, amely igazolhatná a készletre történő adatgyűjtést[168].

2. A célhoz kötöttség elvéhez kapcsolódik, abból következik, hogy a meghatározott cél nélküli, »készletre«, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes.” Lényeges, hogy a célhozkötöttség nem teremthető meg olyan szabályozással, amely a meghatározott cél nélkül gyűjtött és tárolt adatok lekérdezését, az azokhoz való hozzáférést köti célhoz: „Nem konstruálható meg tehát alkotmányosan olyan megoldás, hogy egy meghatározott cél nélküli, központi integrált adatbankra nézve az adatvédelemhez való alkotmányos jog egyik konstitutív elemét, a célhozkötöttséget csakis a lekérdezőkre tartsuk érvényesnek.” Ez következik abból, hogy az AB a célhozkötöttséget és az adattovábbítás korlátozását az adatvédelem konjunktív garanciáinak tekinti, ilyen esetben pedig a felvétel/tárolás során az egyik garanciális elem, a célhoz kötöttség hiányzik[169].

---

mértékre korlátozott személyi kör jogosult, akkor az adatkezelés meghatározott cél nélkül, illetve korlátlan módon válik lehetővé.”

[167] 9/2007. (III. 7.) AB határozat, ABH 2007, 177, 199. Az indítványozó szerint alkotmányellenes az a szabályozás, amely a lőfegyverek engedélyezési eljárásában lehetővé teszi a bűnügyi nyilvántartásban található adatok kezelését, mert a nyilvántartást szabályozó törvény szerint – amely szerint annak célja „a büntetett, illetve a büntetlen előélet tényének megállapítása bűnüldözési, igazságszolgáltatási és nemzetbiztonsági érdekből, valamint az érintett jogai gyakorlásának biztosítása, illetőleg mások jogainak és biztonságának védelme érdekében” – nem szerepelteti az adatkezelési célok között a fegyvertartási engedélyezési eljárást. Az AB szerint „Az idézett előírás nevesített formában valóban nem tartalmaz a lőfegyverekkel kapcsolatos rendelkezést, de amiatt, hogy a lőfegyver természeténél fogva veszélyes, a biztonsági szempontú célmeghatározás relevánsnak tekintendő. A „mások biztonságának védelme” fordulat tehát magában foglalja az állam életvédelmi kötelezettsége teljesítéséből fakadó és az Alkotmány 8. § (1) bekezdésén alapuló korlátozást, ami a lőfegyverek engedélyezési eljárásában - a jogszerű feltétel megléte esetén - a kérelem elutasításában manifesztálódik.”

[168] 35/2002. (VII. 19.) AB határozat (ABH 2002, 199, 208), ill. az erre utaló 36/2005. (X. 5.) AB határozat: „Az Alkotmánybíróság álláspontja szerint […] csak a tényleges és a közvetlen, s nem az eshetőleges veszély értelmezhető a célhozkötöttség követelményét kielégítő alkotmányos ismérvként.” (ABH 2005, 390, 397)

[169] Ennek az érvelésnek azért nagy a jelentősége, mert a készletre történő adatgyűjtés majd célhoz kötött lekérdezés modell – amelyen már a korai, az adatvédelem kiváltó okát jelentő német kísérletek is alapultak – azóta is több esetben felbukkant az állami nyilvántartások vonatkozásában (lásd alább a főszövegben a KATOR-projekt ismertetését). Ráadásul ezen értelmezés megkérdőjelezi olyan új technológiák, eljárások alkalmazását, amelyek lényege, hogy már rendelkezésre álló adatok elemzésével állapítanak meg új összefüggéseket, tendenciákat (adatbányászat), pl. a terrorizmusellenes küzdelem céljából. Hasonló – és várhatóan Magyarországon is felmerülő - kérdést vet fel pl. a nyomozási célú tömeges adategyeztetés (Rasterfahndung),

3. Az Avtv. a célhoz kötöttség elvéhez kapcsolva szabályozza azt a követelményt is, hogy „csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig" (5. § (2) bekezdése). Ez az elv (javasolt elnevezésünkkel a „szükségesség elve") nézetünk szerint nem a célhoz kötöttség követelményének része, abból nem is következik[170]. Ez a követelmény az AB gyakorlatában az alkotmányos cél, illetőleg a szükségesség követelményét az információs önrendelkezési jog vonatkozásában konkretizáló célhoz kötöttségtől eltérően - a jogkorlátozás arányosságának (és a korlátozás legenyhébb eszköze választásának) vizsgálataként jelenik meg; máshol az Avtv. e rendelkezését mint az információs önrendelkezési jog tartalmából következő elvet hívja fel az Alkotmánybíróság[171]. A célhozkötöttség elve, mint az információs önrendelkezési jog garanciája, nem érvényesül közérdekű adatok kezelése esetén[172]. E tétel azonban értelmezési kérdéshez vezet, mivel egyes döntéseiben az AB meghatározott személyes adatok „közérdekűvé válását" mondta ki, később pedig azt, hogy az ilyen adatok a közérdekű adatok jogi sorsát osztják.[173] Kérdés tehát,

---

amelyet a német alkotmánybíróság csak abban az esetben tart alkotmányosnak, ha különösen védendő jogi tárgyat érintő konkrét veszély áll fenn (Murswiek 2006, 138, BVerfG, 1 BvR 518/02 vom 4.4.2006).

[170] Lásd Jóri 2005, 217-224..

[171] És annak alapján megállapítja két személyazonosító jelrendszer párhuzamos használatának alkotmányellenességét: 29/1994. (V. 20.) AB határozat (ABH 1994, 148, 157)

[172] Az Alkotmánybíróság egy, a közérdekű adatok felhasználását „csak a köz érdekében" lehetővé tévő önkormányzati rendelet vizsgálata során kimondta: „Az Avtv. nem tartalmaz olyan korlátozó rendelkezést, amely a közérdekű adatok megismerését célhoz kötötté teszi. Ezáltal a szabályozás megengedi azt is, hogy a kérelmező ne csupán közérdekből, hanem például saját jogos érdekei érvényesítése vagy csoportérdek megvalósítása céljából kezdeményezze a közérdekű adat megismerését. Az Avtv. szerint a közérdekű adatot kezelő szerv nem jogosult az adatkérés céljának vizsgálatára sem. […] Az Alkotmány 61. § (1) bekezdése nemcsak a közérdekű adatok megismeréséhez, hanem ezeknek az adatoknak a terjesztéséhez való jogot is biztosítja. A közérdekű adatok terjesztése egyaránt jelentheti az adatok köz-, illetve magáncélú megismertetését és felhasználását."

[173] Ezek az adatok a 44/1994. (XI. 23) AB határozat szerint ugyan nem közérdekű, hanem – az Avtv. terminológiájának egyébként megfelelően – közérdekből nyilvános adatok. „A személyes adat nyilvánosságra hozatalát a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 3. § (4) bekezdése szerint törvény közérdekből elrendelheti. Ekkor a személyes adat közérdekből nyilvános adattá válik és a »közérdekű adatokéhoz hasonló jogi elbírálás alá esik, amelynek a szabályait az adatvédelmi törvény III. fejezete tartalmazza«" [44/1994. (XI. 23) AB határozat, ABH 1994, 354]. Ám a döntés a személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog egymáshoz való viszonyát az átvilágítás kontextusában meghatározó, egyes személyek jogállamisággal ellentétes tevékenységének tényét (tehát személyes adatot) közérdekű adatnak minősítő 60/1994. (XII. 24.) AB határozatra

hogy az AB által „közérdekűnek” minősített személyes adatok esetén érvényesül-e a célhozkötöttség elve. Ezekben az esetekben az AB a közérdekű adat fogalmát nem az Avtv. szerinti értelemben használta, hanem az Alkotmány 61. § (1) bekezdése szerinti – adott esetben reflektált módon az Avtv. meghatározásától eltérő, annál szélesebb, a személyes adatokat is magában foglaló – „nyilvános” értelemben[174]. Mivel az AB a szóban forgó személyes adatok nyilvánosságáról foglal állást, a határozatból nem olvasható ki az, hogy az adatok személyes adat volta adott esetben megszűnne, és elenyésznének a személyes adatok kezelésére vonatkozó követelmények, s azok legfontosabbika, a célhoz kötöttség[175].

4. A célhoz kötöttség elvéből következik az univerzális, általánosan használt személyazonosító kód alkotmányellenessége, és az osztott információs rendszerek követelménye. Ezeket alább részletesen tárgyaljuk.

---

utal. Ebben a határozatban azonban az AB rögzíti: „Az Alkotmánybíróság ebben a határozatában […] a »közérdekű adat« fogalmát az Alkotmány 61. § (1) bekezdésére vonatkoztatja, s nem abban az értelemben használja, ahogy azt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 2. § 3. pontja meghatározza, illetve ahogy arról az Avtv. 19. § (3) bekezdése rendelkezik. A vizsgált törvény az Avtv.-től függetlenül, az Alkotmány 61. §-ra tekintettel elrendeli bizonyos személyes adatok nyilvánosságra hozatalát.” (ABH 1994, 342, 352) (Korai, a cégnyilvántartás teljes adattartalmát, tehát személyes adatokat még az Avtv. elfogadása előtt közérdekűnek minősítő döntés: 11/1990. (V.1.) AB határozat, ABH 1990, 156, 158.) Az AB e határozataiból tehát nem olvasható ki, hogy adott esetben az adat személyes adatkénti minősülése megszűnne. Ezért helytelen nézetünk szerint Bártfai Zsolt a fenti határozatokon alapuló azon nézete, amely szerint a nyilvánosságra hozatal után „a[…] határozatok szerint – a személyes adat közérdekből nyilvános adatnak minősül és a közérdekű adat jogi sorsát osztja, nincs szükség tehát külön érdekeltség, cél stb. igazolására a további „adatkezeléshez”” (Jóri – Bártfai 2005, Jóri 2005, 216.) A 60/1994. (XII. 24.) AB határozatot elemzi és az érvelés dogmatikai tisztaságát bírálja Majtényi 2006, 174-175, a 30/1997 AB határozatról uo. 194.

[174] 60/1994. (XII. 24.) AB határozat, ABH 1994, 342, 352

[175] Ezzel összhangban a magyar jogban a törvényalkotó több esetben olyan szabályozással él, amely a célhoz kötöttség követelményét nyilvános adatbázisokban található személyes adatokkal kapcsolatban is érvényesítendőnek rendeli: lásd a Ctv. szabályozását. A kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény szerint például a tudományos kutató, piac- és közvélemény-kutató, valamint közvetlen üzletszerző szerv a jogszerűen nyilvánosságra hozatal céljából készített és nyilvánosságra hozott adatállományban, név- és címjegyzékben, valamint kiadványban – így különösen telefonkönyv, szaknévsor, statisztikai névjegyzék – szereplő adatot akkor gyűjthet a törvényi felhatalmazás alapján (az érintett hozzájárulása nélkül), „ha az adatgyűjtéskor vagy az adategyeztetéskor az érintettet tájékoztatták az eredetitől eltérő célra történő adatfelhasználás lehetőségéről, illetőleg a letiltás jogáról” [1995. évi CXIX. törvény 3. § (1) bekezdés b) pontja]. Az adatvédelmi biztos gyakorlata a kérdésben ellentmondásos (Jóri 2005, 212-214)

5. A másik garancia az adattovábbítás és az adatok nyilvánosságra hozatalának korlátozása. Ennek tartalma az AB szerint az, hogy az érintetten (adatalanyon) illetve az eredeti adatkezelőn kívüli személy számára csak abban az esetben lehet személyes adatot továbbítani, ha „minden egyes adat vonatkozásában az adattovábbítást megengedő összes feltétel teljesült", vagyis érvényesül a célhoz kötöttség követelménye, valamint az adattovábbítás címzettje „konkrét törvényi felhatalmazással" rendelkezik az adatkezelésre, vagy ehhez megszerezte az érintett hozzájárulását[176]. Az információs önrendelkezés jogát korlátozó szabályozással szemben alkotmányossági követelmény, hogy az adat útja az érintett számára követhető legyen, így lehetősége legyen a jogérvényesítésre[177], és az adatkezelés pontos feltételei, részletszabályai meghatározottak legyenek[178].

Az AB gyakorlata szerint mind a két követelmény – a célhoz kötöttség és az adattovábbítás/nyilvánosságra hozatal korlátozása – is érvényesül mind „államigazgatási szervek közötti", mind azokon belüli adattovábbítás esetén[179].

---

[176] 15/1991. (IV. 13.) AB határozat, ABH 1991, 39, 41

[177] „Bármilyen jogszabály, amely – az alkalmazott eljárásra tekintet nélkül – személyes adat felvételéről, gyűjtéséről, tárolásáról, rendezéséről, továbbításáról, nyilvánosságra hozásáról, megváltoztatásáról, a további felhasználás megakadályozásáról, az adatból új információ előállításáról, vagy akármilyen más módon történő felhasználásáról (a továbbiakban: a személyes adat feldolgozásáról) rendelkezik, csak akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra nézve, hogy az érintett személy az adat útját a feldolgozás során követni, és jogait érvényesíteni tudja. Az erre szolgáló jogintézményeknek tehát biztosítaniuk kell az érintett beleegyezését a feldolgozásba, illetve pontos garanciákat kell tartalmazniuk azokra a kivételes esetekre nézve, amikor az adatfeldolgozás az érintett beleegyezése (esetleg tudta) nélkül történhet. E garanciális jogintézményeknek – az ellenőrizhetőség érdekében is – objektív korlátok közé kell szorítaniuk az adat útját." [15/1991 (IV. 13.) AB határozat] „Az Avtv. 8. § (1) bekezdése pedig úgy rendelkezik, hogy az adatok csak akkor továbbíthatók, valamint a különböző adatkezelések csak akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy külön törvény azt megengedi, feltéve, ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. A támadott törvényi felhatalmazás ez utóbbi feltételnek, garanciális követelménynek nem felel meg, mert lehetővé teszi az adatállományok olyan összekapcsolását, ahol az adat útja már nem követhető, ezzel pedig az adatalany alkotmányos jogérvényesítését akadályozza. Az adattovábbításra és adatszolgáltatásra vonatkozó törvényi rendelkezés csak akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra nézve, hogy az érintett személy az adata útját követni tudja és jogainak érvényesítésére lehetősége van" (46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 226)

[178] 65/2002. (XII. 3.) AB határozat, ABH 2002, 357, 363

[179] 15/1991. (IV. 13.) AB határozat (ABH 1991, 39, 42), ill. az adatkezelés célhozkötöttségének követelményére az adatvédelmi biztos gyakorlatában lásd Jóri 2005, 214.

Az információs önrendelkezési jog tartalmának főbb, az AB határozataiból kiolvasható elemein túl tendencia, hogy az AB határozataiban az Avtv. által használt fogalmakra, illetőleg az Avtv. egyes rendelkezéseinek sérelmére is hivatkozik, így az Avtv. rendelkezéseiben foglalt szabályokat az információs önrendelkezési jogból közvetlenül következő elvárásokként tételezi. (lásd pl. az Avtv. 5. § (2) bekezdésében foglalt rendelkezés példáját) Hasonlóan sérti az AB szerint az Alkotmányt az Avtv. 10. §-ában megfogalmazott, az adatok biztonságára, az adat- és titokvédelmi szabályok érvényre juttatásához szükséges technikai, szervezési intézkedések megtételére, a megfelelő eljárási szabályok kialakítására vonatkozó szabályokat az a szabályozás, amely szociális segélynek közterületen történő kifizetését írja elő[180].

1.7.5. Az osztott információs rendszerek elve

1. A célhoz kötöttség elvéből következik az is, hogy az Alkotmánybíróság szerint az univerzális, általános célú személyazonosító kód (minden állampolgárnak és országlakosnak ugyanazon elv szerint kiosztott személyi szám) ellentétes az információs önrendelkezési joggal. A 15/1991. (IV. 13.) AB határozat középpontjában egy azonosító kód, az általánosan használt személyi szám megítélése állt; e határozat központi eleme, s egyben ebben a határozatban jelenik meg először Magyarországon a *„célhozkötött, osztott információs rendszerek" követelménye*.[181] Az AB szerint az Alkotmánnyal csak „a meghatározott célú

[180] 55/2007. (IX. 26.) AB határozat: „Az Alkotmánybíróság a vizsgált jogszabállyal összefüggésben felhívja a figyelmet arra, hogy a szociális segélynek közterületen történő kifizetése sérti az Alkotmány 54. § (1) bekezdésében foglalt emberi méltósághoz való jogot, sérti az Alkotmány 59. § (1) bekezdésébe foglalt, a személyes adatok védelméhez való alkotmányos jogot, az Avtv. 10. §-ában meghatározott kötelezettségek önkormányzati megsértését eredményezi, a végrehajtás módja is meg kell feleljen az alkotmányos követelményeknek."

[181] Az AB szerint a megsemmisített szabályozás legfőbb fogyatékossága az volt, hogy az „nem tartalmaz[ott] a személyi szám használatára vonatkozó semmiféle korlátozást vagy feltételt."; a bírák elismerték az általános személyazonosító kód használatának egyes előnyeit: az ilyen kód segítségével „az adatok könnyen hozzáférhetőek, valamint kölcsönösen ellenőrizhetőek lesznek", és további előny, hogy a kódok „költséget és időt takarítanak meg az érintett adatalanyok számára, mert elkerülhetővé teszik az ismételt adatszolgáltatást". A testület szerint azonban az egységes személyazonosító kód használata az előnyöket meghaladó adatvédelmi kockázatokat vet fel: „A személyi szám különösen veszélyes a személyiségi jogokra." Ennek oka, hogy „a személyi szám elterjedt használata esetén a magánszféra megszűnik, mert a legtávolabb eső különböző célú nyilvántartásokból összehozott adatokból előállítható az ún. személyiségprofil, az érintett tetszőlegesen széles tevékenységi körére kiterjedő és intimszférájába is behatoló művi kép, amely ugyanakkor az adatok kontextusból

adat[kezelésre] korlátozott használatú azonosító szám egyeztethető össze. Sem az „állami szféra," sem az államigazgatás egésze nem tekinthető olyan egységnek, amelyen belül egyetlen egységes személyazonosító kódot lehetne bevezetni vagy használni."[182] A célhoz

---

kiragadott volta miatt nagy valószínűséggel torz is." A bíróság mindezek alapján megállapította, hogy „A személyi szám logikája […] ellentétes az adatvédelemhez való jog konstitutív elemeivel: a célhozkötött, osztott információs rendszerek elvével, és azzal a főszabállyal, hogy az adatot az érintettől, annak tudtával és beleegyezésével kell felvenni. Ha az adatvédelem elveit következetesen alkalmazzuk, a személyi szám értelmét veszti, mert „előnyeit" nem lehet kihasználni." Az AB már a határozatban elébe ment a várható bírálatoknak: „Személyes adatokat természetesen össze lehet kapcsolni névvel, és szükség szerint kiegészítő azonosítók segítségével, mint pl. az anya neve, vagy lakcím. A mai számítógép kapacitások mellett ezek terjedelme sem jelent különösebb problémát. A „természetes" adatok azonban változhatnak (pl. a név férjhezmenéssel vagy névváltoztatással), s előfordulhat, hogy a megkülönböztetéshez további adatok szükségesek; továbbá változó adatok esetén (mint a lakcím) az adatok követése és karbantartása szükséges. Az ezzel járó nehézségek és kiadások jelentős tételként jönnek számba az adatfeldolgozás költség/haszon elemzésénél, s minthogy természetes fékjét képezik az indokolatlan adatgyűjtésnek, amire a kéznél lévő személyi szám késztet." A cél tehát természetes fék beépítése volt: a bíróság ennek érdekében mondta az univerzális személyi szám alkotmányellenességét.

[182] A személyi szám-határozat nyomán megszülető Avtv. kifejezetten rögzíti az osztott információs rendszerek követelményét: 7. §-ának (2) bekezdése szerint „Korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos." Miután az AB az általános személyi szám alkalmazását időben 1999. december 31-ig kiterjesztő szabályozást megsemmisítette (46/1995. (VI. 30.) AB határozat, ABH 1995, 219), megszületett az azonosító kódok használatát részletesen a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény (a továbbiakban: Szaz. tv.). A Szaz. tv. szerint a polgárt „természetes személyazonosító adataival, vagy az azokból kiválasztott, az adatkezelés célja szerint szükséges és megfelelő mértékű adattal kell azonosítani", ugyanakkor a természetes személyazonosító adatokkal történő azonosítás „kiegészítésére vagy helyettesítésére" az adatkezelő azonosító kódot is használhat [Szaz. tv. 4. § (1)–(2) bekezdése].

A Szaz. tv. meghatározása szerint: „Az azonosító kód olyan, matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely a polgárt az adatkezelés során egyértelműen azonosítja." Az azonosító kódot maga törvény minősíti személyes adatnak (5. § (2) bekezdés). A törvény szerint az adózással kapcsolatos nyilvántartás azonosító kódja az adóazonosító jel, az egészségügyi, szociális és a társadalombiztosítási és a magánnyugdíj rendszerrel kapcsolatos nyilvántartások azonosító kódja a társadalombiztosítási azonosító jel (tajszám), a személyiadat- és lakcímnyilvántartás azonosító kódja pedig a személyi azonosító (Szaz. tv. 6. §). A törvény szerint az azonosító kódokat az adatkezelő „az érintettel, illetve más adatkezelővel való, meghatározott célú kapcsolattartása során csak azt az azonosító kódot használhatja, amelyre a feladatot meghatározó törvény őt felhatalmazza"; más adatkezelő számára az azonosító kód használata csak az érintett („polgár") előzetes írásbeli hozzájárulásával lehetséges; „a polgárt a hozzájárulás megadása, megtagadása, illetve visszavonása miatt hátrány nem érheti, a hozzájárulás megadásáért bármilyen előny kilátásba helyezése tilos". A párhuzamosan törvényi felhatalmazás alapján több azonosító kódot kezelő adatkezelő a különböző azonosító kódokat tartalmazó

kötöttség elve csak meghatározott célra használt azonosító kód használatát teszi lehetővé, és „[a]z ilyen korlátozott használatú „személyi számot" bevezető törvénynek szabályozási és ellenőrzési garanciákat kell tartalmaznia arra, hogy ezt a számot más összefüggésben ne használhassák."

2. Az Alkotmánybíróság gyakorlata az ágazatspecifikus azonosítók kialakult rendszerének alkotmányosságának (illetőleg egy eseteleges általánosan használt azonosító alkotmányellenességének) tekintetében töretlen, a személyiszám-határozatot tartja irányadónak. Legutóbb a 26/2004. (VII. 7.) AB határozatban foglalt állást hasonló kérdésben, s a korábbi gyakorlatra hivatkozva kimondta, hogy „a határozott cél nélküli, s definiált célok hiányában a különböző felhasználási célok szerint nem osztható, bármely adatot előre meg nem határozható felhasználói körök számára rendelkezésre bocsátó, „készletre" való adatfeldolgozás alkotmányellenes."[183]

3. Az osztott információs rendszerek elvét azóta számos esetben érte kihívás. E kihívások egyik csoportja olyan integrált adatbázisok létrehozására irányult, amelyek az AB által már a személyiszám-határozatban alkotmányellenesnek minősített megoldáson alapultak volna, amely a célhozkötöttséget csak az adatbázisból történő lekérdezés fázisában

---

nyilvántartásokat elkülönítetten köteles vezetni. (Szaz. tv. 7. §). A törvény részletesen meghatározza az adóazonosító jel, a TAJ-szám és a személyazonosító jel kezelésének szabályait, valamint az azonosító kódokat alkalmazó alrendszerek együttműködését és annak korlátait. Lényeges, hogy a Szaz. tv. hatálya nem terjed ki a kizárólag belső azonosításra szolgáló technikai kódokra [Szaz. tv. 2. § (2) bekezdése]. Sólyom László szerint [a Szaz. tv. elfogadásakor] „…a kevés karakterből álló numerikus azonosító eredeti előnyei a műszaki fejlődés következtében érdektelenné váltak; így a személyi számból az elvi kérdések maradtak fenn". SÓLYOM (21. lj.) 182. o.

Figyelemre méltó az Alkotmánybíróság 58/2001. (XII. 7.) számú – nem adatvédelmi tárgyú – határozata az *azonosíthatóság* tekintetében. A határozat szerint az azonosítást segítő, a személyt jellemző legfőbb attribútum a név: „a saját név a személy identitásának egyik – mégpedig alapvető – meghatározója, amely azonosítását, egyúttal másoktól való megkülönböztetését is szolgálja, ezért a személy individualitásának, egyedi, helyettesíthetetlen voltának is az egyik kifejezője. „A saját névhez való jog tehát az önazonossághoz való jog alapvető eleme, így olyan alapvető jog, amely a születéssel keletkezik, az állam által elvonhatatlan és – lényeges tartalmát tekintve – korlátozhatatlan." Álláspontunk szerint a határozat azért érdekes, mert elképzelhető olyan érvelés, amely a személyiszám-határozatban adatvédelmi alapon alkotmányellenesnek kimondott általánosan alkalmazandó személyi szám alkotmányellenességét a névjog mint az önrendelkezési jog elemének sérelmével összefüggésben állapítja meg (s így nem ad alapot azon kritikáknak, amelyek a technológia fejlődésével a határozat érvelését meghaladottnak tekintik). Szintén alapozható a névjogra a Szaz. tv. természetes azonosítók előnyben részesítését előíró rendelkezése.

[183] 26/2004. (VII. 7.) AB határozat, ABH 2004, 398, 423

biztosítja.[184] Ezek a kezdeményezések az adatvédelmi biztos fellépésének eredményeképpen jogszabályi formát nem öltöttek, így az AB azok kapcsán nem foglalt állást.

Az elektronikus közigazgatás megteremtésének igényével együtt gyakran vetődik fel az a kérdést, hogy sérti-e az osztott információs rendszerek követelményét az, ha a Szaz. tv. által szabályozott azonosítók elkülönített kezelését technológiai eszközökkel biztosítaná a jogalkotó oly módon, hogy azok egy hordozón (például kártyán) vannak jelen. Az Igazságügyi Minisztérium 2003. áprilisában előterjesztett, majd utóbb visszavont, egy, az Avtv. átfogó módosítására irányuló törvényjavaslatot (T/3735). Az Avtv. átfogó módosításán túl a javaslat módosította volna a Szaz. tv.-t is a következő rendelkezés beillesztésével: „A polgár részére - kérelmére - megfelelő biztonsági rendszerrel ellátott azonosító kártya is kiadható, amely természetes személyazonosító adatait és azonosító kódjait tartalmazza. Az azonosító kártyát úgy kell kialakítani, hogy adattartalmából az adatkezelő csak azokat az adatokat és azonosító kódokat ismerhesse meg, amelyek kezelésére jogosult." Az adatvédelmi biztos fellépése nyomán az előterjesztők „valószínűleg csak átmenetileg" elálltak a három azonosító kártya adatait tartalmazó új kártya bevezetésének tervétől.[185]

4. Meglehet, hogy jelentősége lesz e kérdés eldöntésében annak a tendenciának, amelyet a 2007. évi CI. törvény szabályozási megoldása tükröz. Ez a szabályozás úgy rendelkezik, hogy egy kriptográfiai megoldásokkal a személyes adatok úgy módosíthatók, hogy azok *ex lege* nem személyes adatok. Ha a jogalkotó hasonló szabályozással élne egyes azonosító kódok kezelésével és kriptográfiai eszközökkel történő elkülönítésével kapcsolatban, akkor az AB-nek értelmeznie kellene az osztott információs rendszerek elvét az

[184] Ilyen volt az 1997-es Központi Adategyeztetés és Továbbítás Országos Rendszere (KATOR) tervezet. ellen. A projekt nem jutott el addig, hogy azt jogi szabályozásba öntsék, s így az alkotmánybírósági kontrollig sem, az adatvédelmi biztos azonban megállapította, hogy „[a] tervezett rendszer az adatvédelem nemzetközileg elfogadott elveit (például az adatkezelések célhoz kötöttségének elvét, vagy az osztott információrendszerekre vonatkozó követelményeket) figyelmen kívül hagyja, és olyan rendszer létrehozását célozza meg, amely beleillik az állampolgárok totális ellenőrzését szolgáló egyéb - az elmúlt hónapokban felszínre került - kormányzati törekvések sorába. A nemzetközi gyakorlatban kevés példát lehet arra találni, hogy az eltérő céllal létrehozott és működtetett adatbázisokat olyan módon kapcsolják össze, ahogyan azt a jelentés javasolja. A személyiségi jogok javaslatból kiolvasható korlátozását ezért is elfogadhatatlannak tartom. E terv megvalósulása oly mértékben sértené az állampolgárok információs önrendelkezési jogát, melyre nincs alkotmányos indok. Az adatbázisok összekapcsolásának tervezett módja véleményem szerint akkor sem fogadható el, ha azt korszerű számítástechnikai módszerek alkalmazásával, »virtuális adatbázis« és »központi index« használatával kívánják megoldani, vagy ha az »egy személy - egy hely - egy időpont« elv érvényesítésével azt a hamis illúziót kívánják kelteni, hogy ez a központosított nyilvántartás az állampolgárok érdekét szolgálja." (Ügyszám: 72/K/1997)

információs társadalom körülményei között, illetőleg állást kellene foglalnia a személyes adat relatív vagy abszolút fogalmának elismerése mellett.

A törvényi szint: a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény főbb rendelkezéseinek elemzése, törvénymódosítási javaslatok

1.8. A törvény hatálya

1.8.1. Értelmezési kérdések a törvény hatályával kapcsolatban

1. Az Avtv. 1/A. § (1) bekezdése szerint „e törvény hatálya a Magyar Köztársaság területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz."

2. A törvény hatályának meghatározása az Avtv. eredeti szövegében nem szerepelt, az 1/A §-t a törvény 2003. évi novellája (a 2003. évi XLVIII. törvény) illesztette a normaszövegbe. A miniszteri indokolás szerint: „Az adatvédelmi törvény jelenleg nem tartalmaz kifejezett rendelkezést a hatályát illetően, arra az általános joghatósági elvek érvényesülnek, illetve csak az egyes konkrét szabályokból lehet következtetni a hatályra. Ez az unióba történő belépésünk után értelmezési problémákat vet fel, különös tekintettel a külföldi és a magyar adatkezelők és adatfeldolgozók egymáshoz való viszonyára, illetve a külföldre irányuló adatkezelésekre." Igen fontos, hogy ezt a rendelkezést a 4/A. § (6) bekezdésében foglaltakkal együttesen kell értelmezni, amely kivételt állapít meg arra az esetre, ha az Európai Unió területén kívül személyes adatok kezelését folytató adatkezelő az adatfeldolgozással a Magyar Köztársaság területén székhellyel, telephellyel (fióktelepel) vagy lakóhellyel (tartózkodási hellyel) rendelkező adatfeldolgozót bíz meg, vagy itt lévő eszközt használ fel, *és ez az eszköz csak az Európai Unió területén átmenő adatforgalom célját szolgálja*.

3. Az 1/A. § szerint tehát a „törvény a Magyar Köztársaság területén folytatott minden olyan adatkezelésre [..] kiterjed, amely természetes személy adataira vonatkozik, valamint

[185] ABI 2004, 43.

amely közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz". A rendelkezés hibája, hogy a törvény hatályának meghatározását az „adatkezelés" fogalmára építi. Ennek meghatározása szerint (1. § 9. pontja): „*adatkezelés:* az alkalmazott eljárástól függetlenül a *személyes adatokon* végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása". Mivel a definícióból következően az adatkezelés fogalma a törvény alkalmazása során csak személyes adatra értelmezett, amely fogalmilag (a közérdekű adat 2. § 4. pontjában foglalt meghatározásából következően) nem lehet közérdekű adat, a hatály meghatározása csak jogalkalmazói jogértelmezéssel lehetséges. Megjegyzendő, hogy a probléma nem csupán elméleti jellegű: nem kizárt az, hogy valamely közérdekű adatokat birtokló, a 19. §-ában meghatározott körbe tartozó szerv vagy személy működhet külföldön is, illetőleg közérdekű adatokat tartalmazó adatbázisát külföldön tárolja/dolgozza fel.[186] Ezekben az esetekben az Avtv. jelenlegi szövege álláspontunk szerint indokolatlanul zárja ki a törvény hatályát.[187]

A tárgyi hatállyal kapcsolatos további kérdés, hogy az adatvédelmi jog alapfogalma, a számos interpretáció és vita tárgyát képező „személyes adat" helyett miért használja a jogalkotó a „természetes személy adatai" meghatározást – remélhető, hogy ez a megoldás nem vezet majd gyakorlati jogalkalmazási problémákhoz.

4. Az 1/A. (1) bekezdése meghatározza a törvény területi hatályát is. Az adatkezelés körében számos esetben a gyakorlatban is felmerült értelmezési kérdés az, hogy nemzetközi távközlési vagy informatikai rendszerek felhasználásával végzett adatkezelés kapcsán mikor történik az adatkezelés a Magyar Köztársaság területén – ráadásul a rendelkezés nincs összhangban az irányelv vonatkozó szabályával (lásd erre vonatkozóan alább).

További értelmezési kérdést vet fel az, ha *magyar adatkezelő külföldi adatfeldolgozót, vagy külföldi adatkezelő magyar adatfeldolgozót vesz igénybe.*

Az első kérdés, hogy amennyiben magyar adatkezelő külföldön végeztet az Avtv. szerinti adatfeldolgozást, akkor alkalmazni kell-e ezen adatfeldolgozási tevékenység során az

[186] Mivel a miniszteri indokolás az irányelvre utal, így feltételezhető, hogy a jogszabály-előkészítő célja a személyes adatokra vonatkozó szabály átvétele volt, és később, kellő előkészítés nélkül vonta e szabály körébe a közérdekű adatokkal kapcsolatos „adatkezelést" is.

[187] A 12/2004. (IV. 7.) AB határozat indokolásában – az Avtv. 19. § (3) bekezdésében foglalt „kezelésében lévő" fordulathoz kapcsolódva – az Alkotmánybíróság is közérdekű adatok vonatkozásában támaszkodik az adatkezelés meghatározására.

Avtv. rendelkezéseit. (Az Avtv. az uniós tagállamoknál több esetben szigorúbb követelményeket állapít meg az adatfeldolgozási tevékenységgel kapcsolatban – lásd erről a 4/A §-hoz fűzött kommentárt.) Ha a külföldi adatfeldolgozó tevékenységére nem kell a magyar törvény e sajátos rendelkezéseit alkalmazni, akkor az adatkezelés egésze megengedőbb jogi környezetbe kerül. Ha a külföldi adatfeldolgozás során alkalmazni kell az Avtv. rendelkezéseit is, akkor ezt a körülményt figyelembe kell venni az adatfeldolgozási szerződés megkötésekor.

Álláspontunk szerint a törvény rendelkezéseit alkalmazni kell abban az esetben is, ha a Magyar Köztársaság területén végzett adatkezeléshez külföldön végzett adatfeldolgozás kapcsolódik. Ezt az értelmezést az alábbiak támasztják alá:

a) Az 1/A. § (1) bekezdése szerint „e törvény hatálya a Magyar Köztársaság területén folytatott minden [..] adatkezelésre és adatfeldolgozásra kiterjed [..]". Álláspontom szerint az adatkezelés abban az esetben is a Magyar Köztársaság területén történik, ha egyes adatfeldolgozási műveleteket külföldön hajtanak végre. A 2. § 15. pontja szerint az adatfeldolgozás „az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése". Az adatfeldolgozás folyamata a hazai szabályozás rendszerében tulajdonképpen az adatkezelés keretében is szemlélhető, s így lehet érvelni amellett, hogy bár az adatfeldolgozás maga külföldön történik, mivel az egy, a Magyar Köztársaság területén végzett adatkezelés része, ezért az 1/A. § (1) bekezdése alapján a törvény hatálya alá esik. (Ez az érvelés egyébként épít arra az álláspontom szerint rossz megoldásra, amellyel a magyar szabályozás különbséget tesz adatkezelés és adatfeldolgozás között – lásd ezzel kapcsolatban a 2. § vonatkozó részeihez fűzött kommentárokat.)

b) Az Avtv. számos esetben az adatkezelő kötelezettségeként szabályozza az adatfeldolgozásra vonatkozó szabályozásnak történő megfelelést. A 4/A. § (1) bekezdése szerint: „Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel." A 4/A. § (3) bekezdése szerint az adatfeldolgozó „a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni". A 4/A. § (4) bekezdése és (5) bekezdése esetében a címzett szintén az adatkezelő: ezen rendelkezések azt szabályozzák, hogy meghatározott vállalkozásoknak nem adható megbízás adatkezelési tevékenységre (ez egyike azon rendelkezéseknek, amelyek esetében az Avtv. a tagállami adatvédelmi törvények többségéhez képest szigorúan szabályoz), az (5) bekezdés pedig az adatfeldolgozási szerződés tartalmára vonatkozóan ad szabályozást. Álláspontunk szerint

ezekből a rendelkezésekből az következik, hogy a Magyar Köztársaság területén végzett adatkezeléssel kapcsolatos bármely adatfeldolgozási szerződést az adatkezelő és az adatfeldolgozó csak az Avtv.-ben meghatározott keretek között köthet, azaz a szerződésben külföldön végzett adatfeldolgozás esetében is mindenkor ki kell kötni az Avtv. szabályainak való megfelelést.

c) Az irányelv preambulumának 18. szakasza szerint „mivel annak biztosítása érdekében, hogy az egyéneket ne lehessen megfosztani attól a védelemtől, amelyre az irányelv értelmében jogosultak, a Közösség területén végzett minden személyesadat-feldolgozási tevékenységet a tagállamok valamelyikének jogszabályai szerint kell végrehajtani; mivel ezzel összefüggésben, a valamely tagállamban letelepedett adatkezelő felelőssége mellett végzett adatfeldolgozásra ennek a tagállamnak a jogszabályai vonatkoznak". Az irányelv tehát azon tagállam jogát rendeli alkalmazni, amelyben az adatkezelő „letelepedett" (erről lásd alább) *minden olyan adatfeldolgozásra, amelyet az adatkezelő felelőssége mellett végeznek.*[188] Az irányelv fogalomrendszerében „adatfeldolgozásnak" fordított fogalom (data processing) magában foglal bármely adatkezelési/adatfeldolgozási műveletet (vagyis az irányelv fogalomrendszerében az „adatfeldolgozás" fogalma ismeretlen, tevékenységként csak a „data processing" van meghatározva: lásd erről alább a vonatkozó fogalmakhoz fűzött kommentárokat). Az irányelv preambulumában kifejtett szabályozási cél tehát az, hogy az adott tagállam joga (amelyben az adatkezelő letelepedett) legyen alkalmazandó minden olyan esetben, amelyben az „adatfeldolgozást" az adatkezelő felelőssége mellett végzik – vagyis az Avtv. fogalomrendszerét használva, *minden az adatkezelő által végzett adatkezelésre és végeztetett adatfeldolgozásra.*

Az 1/A. § (1) bekezdése szerint az Avtv. hatálya a Magyar Köztársaság területén végzett valamennyi adatfeldolgozásra is kiterjed, így azon adatfeldolgozásokra is, amelyek esetén az adatkezelő külföldi. Álláspontunk szerint ilyen esetben is alkalmazni kell az Avtv.-nek az adatfeldolgozásra vonatkozó sajátos szabályait, mindamellett a fenti *c)* pont szerint az irányelvnek megfelelő EU-tagállami szabályozások ebben az esetben az adatkezelő letelepedésének helye szerinti jog alkalmazását írják elő (lásd erről részletesebben alább).

A fentiekkel kapcsolatban megjegyzendő még, hogy az irányelv 17. szakaszának (3) bekezdése alapján az adatfeldolgozó letelepedésének helye szerinti adatvédelmi jogot is

[188] Az angol szövegben: „processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State".

alkalmazni kell a 17. szakasz (1) bekezdésében meghatározott kérdésekre (adatbiztonság). Lásd ezzel kapcsolatban alább a 4/A. § (1) bekezdéséhez fűzött magyarázatot.

1.8.2. Az adatvédelmi biztos vonatkozó gyakorlata

1. Az adatvédelmi biztosi gyakorlatban több állásfoglalás is található a törvény hatályával kapcsolatban.

Egy ügyben a panaszos egy amerikai cég weboldalán igényelt reklámanyagot személyes adatainak megadásával, amelyet az – az érintett tájékoztatása, illetőleg hozzájárulása nélkül – a cég magyar partnerének továbbított. A biztos szerint a magyar cég által végzett adatkezelés jogellenes, ám állásfoglalásában azt nem mondta ki, hogy az lenne az amerikai cég által végzett adattovábbítás is.[189]

Több ízben állást foglalt a biztos diplomáciai testületek, azok tagjai által végzett adatkezelésekkel kapcsolatban. Így például megállapította, hogy a stockholmi magyar nagykövetség külföldre továbbított adatot, amikor azokat egy svéd állampolgárnak átadta[190] – a magyar nagykövetségek adatkezelésére tehát a biztos szerint a magyar adatvédelmi jogot kell alkalmazni.[191] A Magyarországon működő nagykövetségek adatkezelésére – mint azt Egyesült Államok budapesti nagykövetsége által a vízumigénylés során végzett adatkezelés ellen irányuló panasz kapcsán kifejtette – a magyar adatvédelmi jog nem alkalmazható.[192]

Más esetben a biztos egy külföldön nyilvántartásba vett egyetem adatkezelésével kapcsolatban mutatott rá arra, hogy „[…] az, hogy az adatkezelőt nem Magyarországon vették nyilvántartásba, vagy székhelye nem Magyarországon van, nem bír jelentőséggel. Az adatkezelés a magyar jog szabályainak kell megfeleljen”.[193]

Vitatható az a korai jogesetben kifejtett nézet, amely szerint „a [magyarországi levéltárban kutatásokat folytató] kutató már a jegyzeteléskor is külföldi adatkezelőnek tekinthető [..]”,[194] vagyis a számára történő adattovábbítás külföldre irányuló továbbításnak minősülne. Az eset azért említendő, mert az irányelv helyes alkalmazása esetében hasonló tényállás – EGT-tagállamban letelepedett adatkezelő Magyarország területén végzett, eseti

[189] ABI 1999, 98.

[190] ABI 2000, 151.

[191] Hasonlóan egy másik nagykövetségre: ABI 2000, 153.

[192] ABI 2000, 152.

[193] ABI 2001, 242.

[194] ABI 1997, 242.

adatkezelése – valóban nem a magyar adatvédelmi jog lenne alkalmazandó (lásd részletesebben alább).

A biztos egyik beszámolójában rögzíti azt is, hogy a nemzetközi magánjogról szóló 1979. évi 13. tvr. szerint a magyar adatvédelmi jog külföldi adatkezelésekkel kapcsolatban is „szerepet kaphat".[195]

1.8.3. Az irányelv vonatkozó rendelkezései

Az irányelv 4. cikke szerint:

„(1) A személyes adatok feldolgozására minden tagállam az ezen irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza, amennyiben:

a) az adatkezelést az adatkezelő olyan szervezete [establishment, Niederlassung] tevékenységének keretében végzik, amely a tagállam területén telepedett le; amennyiben ugyanaz az adatkezelő több szervezete több tagállam területén is letelepedett, meg kell tennie a szükséges intézkedéseket annak biztosítása érdekében, hogy szervezeteinek mindegyike megfeleljen az alkalmazandó nemzeti jog által megállapított kötelezettségeknek;[196]

b) az adatkezelő nem valamely tagállam területén telepedett le, hanem olyan helyen, amelynek nemzeti joga – a nemzetközi közjog értelmében – alkalmazandó;

c) az adatkezelő nem telepedett le a Közösség területén, és a személyes adatok feldolgozása céljából gépi vagy más olyan eszközt alkalmaz, amely a fenti tagállam területén található, kivéve, ha ezt az eszközt kizárólag a Közösség területén átmenő adatforgalom céljára használják.

(2) Az (1) bekezdés *c)* pontjában említett körülmények esetén az adatkezelőnek – az ellene indítható jogi keresetek sérelme nélkül – ki kell jelölnie egy, az adott tagállam területén letelepedett képviselőt."

2. Az irányelv és az Avtv. szabályozása ebben az esetben olyan módon tér el egymástól, amely jogalkalmazási problémákhoz is vezethet. Az irányelv megfogalmazói

---

[195] ABI 2001, 163. Lásd az 1979. évi 13. tvr. 10. skk. §-ait, valamint Mádl–Vékás 1997, 147. skk.

[196] Az *a)* pont első fordulata a szerző fordítása. A hivatalos fordítás hibás: „az adatfeldolgozást a tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzik". Az irányelv azonban nem ahhoz fűzi a tagállami jog alkalmazását, hogy „az adatkezelést a tagállam területén […] végzik", hanem ahhoz, hogy az adatkezelőnek az adott tagállam területén letelepedett szervezete tevékenységének keretében végzik. Az angol szöveg szerint „the processing is carried out int he context of the activities of an establishment of the controller on the territory of the Member State"; a német szöveg szerint „[Daten] die im Rahmen der Tätigkeiten einer

tudatosan nem az adat vagy az adatkezelés helyére építve határozták meg annak területi hatályát, mert ez adatbázisok, adathálózatok esetén a szabályozást nehezen alkalmazhatóvá tenné.[197] Az irányelv alapján a nemzeti jog főszabály szerint akkor alkalmazandó, ha az adatkezelés az adatkezelőnek a tagállamban letelepedett [a jogi formától függetlenül tartósan tevékenységet gyakorló – lásd az irányelv preambulumának (19) bekezdését] szervezete tevékenysége keretében történik. Lehetséges, hogy ez a szervezet másik tagállamban végez adatkezelést (tipikusan ilyenek a magyar jogalkotó által „adatfeldolgozásként" meghatározott esetek) – *ám tevékenységére a letelepedés helye szerinti adatvédelmi jogot kell alkalmazni.*[198]

A magyar jogalkotó ezzel szemben minden Magyarországon végzett adatkezelésre vagy adatfeldolgozásra kiterjeszti a törvény területi hatályát. Ez – az adatkezelés és adatfeldolgozás fogalmának elhatárolhatatlanságával együtt (lásd alább a 2. § vonatkozó pontjaihoz fűzött kommentárokat) – azzal az eredménnyel jár, hogy irányelvnek megfelelően megalkotott adatvédelmi jogszabályok alapján működő tagállami adatkezelők egyes Magyarország területén végzett adatkezeléseire és adatfeldolgozásaira – amelyek az adott tagállamban letelepedett szervezet tevékenységi körébe illeszkedve mennek végbe – *párhuzamosan kell alkalmazni az irányelvnek megfelelő tagállami jogot és a magyar adatvédelmi jogot*.

Míg tehát az Avtv. 1/A. § (1) bekezdése „a Magyar Köztársaság területén folytatott" adatkezeléseket és adatfeldolgozásokat vonja a törvény hatálya alá, az irányelv 4. cikkének 1. *a)* pontja szerint a tagállami jog akkor terjed ki az adatkezelésre („adatfeldolgozásra"), ha „az adatfeldolgozást a tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzik" („the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State"). E rendelkezéshez kapcsolódik az irányelv preambulumának (19) bekezdése, amely szerint „mivel a valamely tagállamban való letelepedés magában foglalja a tevékenység tényleges gyakorlását tartós jelleggel; mivel e letelepedés – legyen akár egyszerűen fióktelep, akár jogi személyiséggel rendelkező leányvállalat – jogi formája e tekintetben nem meghatározó tényező; mivel ha egy adatkezelő több tagállamban is letelepedett, főként leányvállalatok révén, a nemzeti szabályozás megkerülésének kizárása érdekében gondoskodnia kell arról, hogy minden egyes

---

Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt".

[197] Lásd az irányelv vonatkozó szakaszának indokolását. Közli Dammann–Simitis 1997, 126.

[198] Hasonlóan Jay–Hamilton 1999, 41; Dammann–Simitis 1997, 128.

szervezete megfeleljen a tevékenységére alkalmazandó nemzeti jogszabályok által meghatározott kötelezettségeknek".

Például egy németországi (vagy bármely más EU-tagállamban letelepedett) vállalkozás egyszeri, Magyarországon végzett adatkezelésére (például adatfelvétel) az irányelv szabályozása szerint a német adatvédelmi jog (illetve az adott tagállam adatvédelmi joga) hatályos. Az irányelv 4. cikk (1) bekezdés *c)* pontja és (2) bekezdése – amelyet a hazai jogalkotó a 4/A. § (6) bekezdésével kívánt implementálni – éppen erre tekintettel rendezi azt a helyzetet, amelyben olyan adatkezelő végez valamely adatkezelési cselekményt valamely tagállamban, amely egyik tagállam területén sem letelepedett (tehát tevékenysége egyébként egyáltalán nem esne az irányelv hatálya alá).[199] Az irányelv szabályozása szerint csak ebben az esetben releváns az adatkezelés (data processing) helye, pontosabban az adatkezelést szolgáló berendezés elhelyezkedése a hatály megállapítása szempontjából. Ezzel szemben az Avtv. szabályozása a hatály meghatározásakor általában az adatkezelés helyéből indul ki, így rendelkezése szerint akár egyszeri adatkezelési művelet esetén is a magyar adatvédelmi jog hatályos. Ez a probléma kapcsolatban van az adatkezelés/adatfeldolgozás fogalmai körül az Avtv. szabályozásában érezhető zavarral, hiszen a jogalkotó az irányelv egy, bármely adatkezelési („adatfeldolgozási") műveletre (processing) vonatkozó rendelkezését [4. cikk (1) bekezdés *c)* pontja és (2) bekezdése] a hazai, szűkebb körű adatfeldolgozás intézményére értelmezett módon vette át, álláspontunk szerint hibásan.

3. Az Avtv. területi hatályával kapcsolatban ki kell emelni még az irányelv preambulumának 20. bekezdését, amely szerint „[..] ez az irányelv nem érinti a büntetőügyekben alkalmazandó territorialitási szabályokat".

1.8.4. Automatizált és manuális adatkezelés

1. Az Avtv. 1/A § (2) bekezdése szerint „e törvényt a teljesen vagy részben automatizált eszközzel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell." A rendelkezés – az 1/A. § egészéhez hasonlóan – az Avtv. 2003. évi novellájával került a törvényszövegbe. A módosításhoz fűzött miniszteri

[199] Lásd Jay–Hamilton 1999, 42.

indokolás szerint ez a szabály „a hatályos törvényből már eddig is következő", amelynek azonban kifejezett rögzítése „indokolt".[200]

2. Az 1/A. § (2) bekezdésében – az (1) bekezdéshez hasonlóan – a törvényalkotó az adatkezelés és az adatfeldolgozás fogalmát használja, amely a 2. § 9. pontja alapján csak személyes adatok vonatkozásában értelmezhető. Mivel a rendelkezésnek normatív tartalma valójában nincs (a törvény hatálya e bekezdés hiányában is megegyezne azzal, amit e szabály rögzít), ezért e körülmény várhatóan nem vezet majd gyakorlati jogalkalmazási problémákhoz.

Az Avtv. sajátossága, hogy tárgyi hatálya minden adatkezelésre és adatfeldolgozásra kiterjed, tekintet nélkül nemcsak arra, hogy azt automatizált vagy manuális módon végzik, hanem arra is, hogy a szóban forgó adatkezelés tárgya valamely nyilvántartás (adatbázis), vagy csupán egyetlen adat.

3. A magyar jogalkotó szélesebb körben állapította meg a törvény tárgyi hatályát, mint ahogyan azt az irányelv 3. cikk (1) bekezdése megkívánná: „Ezen irányelvet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni." A személyesadat-nyilvántartó rendszer fogalmát a novellával a magyar jogalkotó is átvette (lásd a 2. § 17. pontjához fűzött kommentárt), ám más összefüggésben.

Az irányelv preambulumából is kitűnően a fenti rendelkezés célja az, hogy a nem gépesített, manuális módon kezelt állományok közül a nem strukturált irat- és adatállományok ne tartozzanak annak tárgyi hatálya alá (vagyis másik megközelítéssel: az automatizált adatkezelés tárgyát képező állományok mellett csak a strukturált, vagyis rendezett, áttekinthető, manuálisan kezelt állományok kerüljenek az adatvédelmi rendelkezések hatálya alá, amelyek esetén fennáll a magánszféra sérelmének a veszélye: épp az automatizált

[200] Érdemes megjegyezni azt, hogy a jogszabály-előkészítő egy olyan szabály rögzítését látta ebben az esetben indokoltnak, amely kifejezetten utal arra, hogy a magyar adatvédelmi törvény – a szerzők által alkalmazott korszakolástól függően – az első vagy második generációs törvények közé tartozik, szabályait mára túlhaladta az idő. Bäumler a német adatvédelmi törvények generációit elemezve így fogalmaz: „Az adatvédelmi törvények első generációja azonban lényegében csak mellékesen foglalkozott az adatkezelés technológiájával. A valódi témájuk az volt, hogy ki, milyen feltételekkel, kiről, mennyi ideig és mely személyes adatokat kezelhet, függetlenül attól, hogy használnak-e egyáltalán, s ha igen, mely technológiát. A manuális nyilvántartások ugyanazon megítélés alá estek, mint az automatizáltak…" Bäumler 1999, 6.

adatkezelés szintjét el nem érő, de ahhoz hasonló rendezési, válogatási, hozzáférési lehetőségek miatt). A tagállamok adatvédelmi jogai hasonló célból használják a fogalmat.[201] Az Avtv. rendszerében a nyilvántartó rendszer fogalma azonban csak az adatvédelmi biztos előzetes ellenőrzési jogkörével kapcsolatban kap szerepet.[202]

A tárgyi hatálynak az irányelvnél szélesebb meghatározása – az Európai Bíróság által a Lindqvist-ügyben kifejtett értelmezésére is tekintettel – nem sérti az irányelvet [lásd erre az 1. § (1) bekezdéséhez fűzött magyarázatot].

1.8.5. Kizárólag magáncélt szolgáló adatkezelés

1. Az Avtv. 1/A § (3) bekezdése szerint „nem kell alkalmaznia e törvény rendelkezéseit a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire."A jogalkotó az Avtv. 2003. évi novellájával vette át az irányelv 3. cikk (2) bekezdésében foglalt kivételt. Az Avtv. hatálybalépésétől 2004. január 1-jéig a törvény rendelkezéseit a természetes személy által végzett, kizárólagosan saját személyes céljaira szolgáló adatkezelésekre is alkalmazni kellett.

A hatályos rendelkezésben szereplő „saját személyes céljait" fordulat értelmezése még a jogalkalmazóra vár. Az irányelv és a tagállami jog hasonló rendelkezéseit elemző irodalom szerint ilyennek minősülhetnek a személyes telefonregiszterek, a hozzátartozók születésnapjára vonatkozó feljegyzések, a magánszemélyek által folytatott levelezés;[203] abban az esetben, ha a magánszemély otthoni számítógépén munkájával kapcsolatos adatokat kezel, az adatkezelés nem tartozik a kivétel hatálya alá;[204] nem alkalmazható a kivétel abban az esetben sem, ha az adatot meghatározhatatlan számú személy ismeri meg (vagyis az nyilvánosságra kerül).[205]

2. A novella hatálybalépését megelőzően számos olyan panasz érkezett az adatvédelmi biztoshoz, amelyek magánszemély adatkezelők által végzett adatkezelések ellen irányultak.

---

[201] Lásd például a „relevant filing system" fogalmát az 1998-as brit adatvédelmi törvényben, a „nich automatisierten Datei" fogalmát a német szövetségi adatvédelmi törvényben stb.

[202] Az a tény, hogy a jogalkotó a novellálás során is fenntartotta az Avtv.-nek az irányelvnél szélesebb tárgyi hatályát, álláspontunk szerint nem kifogásolható. Az Avtv. szabályozásának alapvető hibája véleményünk szerint az, hogy az irányelv által megállapított hatályon belül, tehát az EU harmonizációs normája által érintett szabályozás körében hat számos esetben a kívánatos egységes védelmi szint megteremtésével szemben.

[203] Dammann–Simitis 1997, 123. skk.

[204] Dohr–Pollirer–Weiss 2004, 280.

Ezekben az esetekben a nyomozati jogkör hiánya, a bizonyítás nehézségei, általában a két magánszemély közti viták eldöntésére rendelkezésére álló eszközök hiánya miatt a biztos sokszor nem tudott eljárni.[206]

Egyes esetekben azonban olyan ügyekben is vizsgálatot indított, amelyek tárgya – a „személyes cél" értelmezésétől függően – a hatályos szabályozás szerint már a tárgyi hatály alóli kivételi körbe tartozhat: így például amikor az érintettet szomszédja rendszeresen lefényképezte.[207]

Más esetekben – nézetünk szerint – nyilvánvaló a magánszemély adatkezelő által végzett adatkezelés társadalomra veszélyessége. Ilyen például az az eset, amelyben az üzlettulajdonos közszemlére tette annak a személynek a nevét, akinek kezdeményezésére az üzlet nyitvatartását korlátozták;[208] még nyilvánvalóbb ez abban az esetben, amelyben rendőr kért le magáncélból adatokat a munkakörével kapcsolatban rendelkezésére álló adatbázisokból.[209] Az első esetben álláspontunk szerint a „kizárólag saját célból" végzett adatkezelésen kívüli tevékenységről van szó. A második esethez hasonló tényállás megítélése során a jogalkalmazó helyzete nehezebb, hiszen az adatkérés történhet kizárólag magáncélra, s ebben az esetben az beleillik az 1/A. (3) bekezdése alatt szabályozott kivételi körbe. (A jogalkalmazó hasonló esetben várhatóan a hivatalos személyként történő adatkezelés miatt nem állapítja meg majd a kivételt, ám ez a megoldás dogmatikailag nem helyes, hiszen míg a rendőr szabályszerűen jár el az adatkezelés során, addig adatkezelőnek a rendőrség minősül [lásd erre alább a 2. § 8. pontjához fűzött kommentárt], ám a magáncélú adatkérés során az adatkezelő már a rendőr mint magánszemély.)

3. Az irányelv 3. cikke (2) bekezdésének második francia bekezdése szerint az irányelv nem alkalmazandó „a természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett adatfeldolgozásra".

A jogalkotó e rendelkezéssel indokolta a 1. § (3) bekezdésében foglalt kivétel felvételét az Avt. 2003. évi módosításakor. Megjegyzendő, hogy az Európai Bíróság Lindqvist-ügyben kifejtett értelmezése alapján a tagállam abban az esetben sem sérti az irányelv rendelkezéseit, ha a személyes adatokra vonatkozó szabályozás hatályát az

---

[205] Dammann–Simitis 1997, 124. Lásd ilyen esetre a magyar adatvédelmi biztosi gyakorlatban: ABI 2001, 285.

[206] Lásd erre ABI 1998, 119.

[207] ABI 1999, 123.

[208] ABI 2001, 285.

[209] ABI 2001, 280.

irányelvnél szélesebb körben állapítja meg.[210] A fenti példák nyomán – bár a kivétel életszerű, s a magánszemély általi adatkezelések esetén a törvény rendelkezései a gyakorlatban egyébként is nehezen volnának érvényesíthetők – felvethető, hogy az adatkezelő személye és az adatkezelés célja önmagában vezethet-e olyan helyzethez, hogy az érintett információs önrendelkezési joga az adott esetben ellenőrzés nélkül korlátozható.

4. Az irányelv 3. cikkének (2) bekezdése szerint annak tárgyi hatálya nem terjed ki „a közösségi jog hatályán kívül eső tevékenységek, mint például az Európai Unióról szóló szerződés V. és VI. címeiben megállapítottak, valamint a közbiztonsággal, a védelemmel, az nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási művelet nemzetbiztonsági ügyre vonatkozik), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletekre". Az irányelv rendelkezéseit tehát ezen adatkezelések vonatkozásában nem kell átvenni, vagyis az irányelv által meghatározott egységes védelmi szintnek ezeken a területeken nem kell érvényesülnie. Az Avtv. hatálya ezekre az adatkezelésekre is kiterjed.

Az irányelv 9. cikke szerint (A személyes adatok feldolgozása és a szólásszabadság): „A tagállamok e fejezet, a IV. és a VI. fejezet rendelkezései alóli felmentésről, illetve eltérésről kizárólag a személyes adatoknak újságírás, vagy irodalmi, illetve művészi kifejezés céljából történő feldolgozása esetén rendelkezhetnek, amennyiben azok a magánélet tiszteletben tartásához való jognak a szólásszabadságra vonatkozó szabályokkal való összeegyeztetéséhez szükségesek." (A hivatkozott fejezetek a személyes adatok feldolgozására vonatkozó általános szabályokról, az érintett tájékoztatásáról, a mentességekről és korlátozásokról szólnak.) A sajtóról szóló 1986. évi II. törvény 3. § (1) bekezdése szerint „a sajtószabadság gyakorlása nem valósíthat meg bűncselekményt vagy bűncselekmény elkövetésére való felhívást, nem sértheti a közerkölcsöt, valamint nem járhat mások személyhez fűződő jogainak sérelmével".

Az Avtv. 3. § (1) bekezdésének és a sajtótörvény rendelkezéseinek értelmezéséből az a következtetés adódik, hogy személyes adat sajtó útján történő nyilvánosságra hozatala jogellenes adatkezelést valósít meg. Ezen értelmezés elfogadása esetén tulajdonképpen a tényfeltáró újságírás egésze jogellenesnek minősül.[211] Megfontolandó ezért a törvény tárgyi hatályának, esetleg más szabályainak olyan irányú módosítása, amely az irányelv megszabta

[210] Lásd ilyen szabályozásra például az osztrák adatvédelmi törvény (DSG 2000) 45. §-át.

[211] Lásd erre például ABI 2004, 113: az érintett adatainak közlése *A 100 leggazdagabb magyar* című kiadványban hozzájárulása nélkül jogellenes. „Értelmezésünk szerint ún. tényfeltáró újságíró nincs, mert valaki vagy olyasmit közöl, ami jogszerű, vagy fél lábbal a börtönben van" – mondja Péterfalvi Attila (Babus 2004).

határok között eltérést biztosít a törvény rendelkezéseitől, s ezáltal rendezi a tényfeltáró újságírás adatvédelmi jogi helyzetét.

1.9. Alapfogalmak: a személyes adat, a közérdekű adat és a közérdekből nyilvános adat fogalma, és ezek viszonya

1.9.1. A személyes adat

1. Az Avtv. 2. § 1. pontja szerint a törvény alkalmazása során „*személyes adat:* bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet". A személyes adat fogalma az Avtv. legfontosabb meghatározása: annak elbírálásakor, hogy valamely cselekményre kiterjed-e törvény hatálya, minden esetben alapkérdés az, hogy a szóban forgó művelet tárgyát képező adatok személyes adatnak minősülnek-e. A személyes adat fogalmával kapcsolatos főbb értelmezési kérdések az alábbiak:

2. Bár a fogalom nyelvtani értelmezéséből ez nem következik, az Avtv. szerint személyes adatnak csak az *élő* természetes személlyel kapcsolatba hozható adat minősülhet. Az Avtv. indokolása szerint „az információs önrendelkezési jog szükségképpen az adattal érintett élő személyt illeti meg. A meghalt személy adatainak védelméről, illetőleg a velük való rendelkezésről – az adattal vagy az adatkezeléssel összefüggő – külön jogszabályok szólnak (például Ptk., levéltári, anyakönyvi jogszabályok)."

Az elhunytakkal kapcsolatba hozható adatokra vonatkozó szabályozást tartalmaz az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüatv.) is. Mint szektorális adatvédelmi törvényt azt nemcsak az elő természetes személyekkel kapcsolatba hozható adatokra, hanem az Eüatv. által meghatározott érintettel összefüggésbe hozható egészségügyi és személyazonosító adatokra is alkalmazni kell. Az Eüatv. 2. § *b)* pontja szerint a törvény hatálya kiterjed „minden, az egészségügyi ellátóhálózattal, valamint az egyéb adatkezelő szervvel kapcsolatba került vagy kerülő, illetve annak szolgáltatásait igénybe vevő természetes személyre,

függetlenül attól, hogy beteg-e vagy egészséges" (a törvény ezt a személyt nevezi „érintettnek").

Az Eüatv. nem használja a személyes adat fogalmát, helyette az egészségügyi adat és a személyazonosító adat fogalmát határozza meg. Az Eüatv. 3. § *a)* pontja szerint egészségügyi adat „az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (például magatartás, környezet, foglalkozás)"; az egészségügyi adat tehát élő vagy elhunyt természetes személyhez is kapcsolódhat. Az Eüatv. 3. § *b)* pontja szerint „személyazonosító adat: a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, a társadalombiztosítási azonosító jel (a továbbiakban: taj-szám) együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett azonosítására".

Az Eüatv. a fenti, az Avtv.-től eltérő hatály miatt arról is rendelkezik, hogy meghatározott esetben ki gyakorolhatja az érintett életében, illetve a halál beállta után a törvényben szabályozott adatkörökhöz kapcsolódóan az érintettnek biztosított jogokat. Eüatv. 7. § (5) bekezdése szerint a törvény által az egészségügyi és személyazonosító adatokkal, valamint az orvosi dokumentációval kapcsolatban biztosított betekintési és másolatkészítési jog gyakorlására „[a] beteg életében, illetőleg halálát követően az érintett házastársa, egyeneságbeli rokona, testvére, valamint élettársa – írásbeli kérelme alapján – akkor is jogosult…, ha

a) az egészségügyi adatra,

aa) a házastárs, az egyeneságbeli rokon, a testvér, illetve az élettárs, valamint leszármazóik életét, egészségét befolyásoló ok feltárása, illetve

ab) az *aa)* pont szerinti személyek egészségügyi ellátása céljából

van szükség, és

b) az egészségügyi adat más módon való megismerése, illetve az arra való következtetés nem lehetséges." Az Eüatv. 7. § (6) bekezdése szerint „csak azoknak az egészségügyi adatoknak a megismerése lehetséges, amelyek az (5) bekezdés *a)* pontja szerinti okkal közvetlenül összefüggésbe hozhatóak".

Az Eüatv. 7. § (7) bekezdése további betekintési jogosultságot biztosít az érintetten kívüli személyeknek: „Az érintett halála esetén törvényes képviselője, közeli hozzátartozója, valamint örököse – írásos kérelme alapján – jogosult a halál okával összefüggő vagy

összefüggésbe hozható, továbbá a halál bekövetkezését megelőző gyógykezeléssel kapcsolatos egészségügyi adatokat megismerni, az orvosi dokumentációba betekinteni, valamint azokról – saját költségére – másolatot kapni."

3. Az Avtv. 1/A. § (1) bekezdésnek a hatályt illető meghatározásából és a személyes adat fogalmának a 2. § 1. pontjában szereplő meghatározásából egyértelműen az következik, hogy személyes adatnak csak *természetes személlyel* összefüggésbe hozható adat minősülhet, vagyis *szervezetek adatai nem*. Ez egyértelműen következett a 2004. január 1-je előtt hatályban volt meghatározásból is, amely a személyes adatkénti minősüléshez szintén a „meghatározott természetes személy"-hez köthetőséget követelte meg.

Figyelemre méltó, hogy az Avtv. korai tervezetei még kifejezetten kiterjesztették volna a védelmet a jogi személyekre és jogi személyiséggel nem rendelkező szervezetekre is.[212] Az adatvédelem és a szervezetek adatainak védelmének viszonyára lásd részletesebben alább az Alkotmánybíróság gyakorlatával kapcsolatos részt.

4. Sem az adatvédelmi törvény, sem annak miniszteri indokolása nem ad iránymutatást arra, vajon mely természetes személy tekinthető *„meghatározott"-nak (azonosítottnak vagy azonosíthatónak)*. A „meghatározott" fogalom jelentését az adatvédelmi biztosi gyakorlat sem bontotta ki. Az Európa Tanácsnak az egyének védelméről a személyes adatok gépi feldolgozása során című egyezménye (kihirdette az 1998. évi VI. törvény) – amelyre az Avtv. miniszteri indokolása mint „nemzetközi mércére" hivatkozik – szerint „személyes adat: bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik". A vonatkozó irodalom szerint „azonosíthatónak az a személy tekinthető, akinek különálló identitása felismerhető, de személye nem ismert. […] Javasoljuk azt a meghatározást, amely szerint valaki azonosítható, ha elég információ áll rendelkezésre, hogy elkülönült létezésének, egyénként való létének tényét tükrözze, és akkor válik azonosítottá, ha elég információ áll rendelkezésre, a vele történő kapcsolatfelvételhez vagy a másoktól való valamilyen módon történő megkülönböztetéséhez, felismeréséhez."[213]

5. A meghatározás szerint a természetes személlyel *„kapcsolatba hozható"* adat minősül személyes adatnak. Az adatvédelmi jogban a személy és az adat közötti kapcsolat megállapíthatóságának értelmezése alapvető fontosságú a tekintetben, hogy mely adatkört minősíthetünk személyes adatnak, s így adott esetben megállapítható-e a törvény hatálya, vagy nem.

[212] Sólyom 1988a, 59.

[213] Jay–Hamilton 1999, 29.

A kapcsolatba hozhatóság megítélésével kapcsolatban felmerülő alapvető értelmezési kérdés az, hogy kielégíti-e ezt a követelményt az az adat, amely a meghatározott természetes személyhez csak több lépésben, sőt, akár több adatkezelő közreműködésével kapcsolható. Egyes uniós tagállami jogok a személyes adatkénti minősüléshez azt követelik meg, hogy a személy és az adat között a kapcsolat meghatározott adatkezelő által legyen helyreállítható (a személyes adat ún. „relatív" fogalma).[214]

A két értelmezés nyomán jelentősen különbözik a személyesnek minősülő adatok köre; a relatív értelmezés elfogadása esetén az adatvédelmi szabályozást jóval kevesebb adatra kell alkalmazni. A különbséget az alábbi példával szemléltetjük:

A számítógépeket az interneten egy négybájtnyi azonosító, az ún. IP-cím azonosítja. Az IP cím négy, 0–255 közötti értékű, ponttal elválasztott számból áll; például 157.181.2.1.

Az Internet fejlődésének korai szakaszában igen elterjedt (és még ma sem teljesen ismeretlen) az ún. dial-up internetkapcsolat, amikor is a felhasználó – modem segítségével – telefonvonalon éri el az internetszolgáltatót, oly módon, hogy ha kapcsolódni kíván az internetre, akkor hívást kezdeményez, majd a szolgáltató a rendelkezésére álló IP-cím-tartományból a kapcsolat idejére a felhasználó gépéhez rendel egyet. A felhasználó gépét a kapcsolat alatt ezen IP-cím azonosítja a hálózaton. A kapcsolat bontása után azonban a szolgáltató egy másik felhasználónak is „kioszthatja" az IP-címet, illetve a szóban forgó felhasználó újbóli kapcsolat létesítése esetén szintén véletlenszerűen „kap" IP-címet a szolgáltató rendelkezésére álló tartományból. A felhasználót tehát minden egyes kapcsolat alatt más IP-cím (ún. dinamikus IP-cím) azonosítja (vagy mégis ugyanaz, akkor az a véletlennek köszönhető). Ezen IP-címek az interneten elérhető ún. whois-adatbázisok alapján az internetszolgáltatóhoz köthetők. A dinamikus IP-cím-kiosztás mellett vannak felhasználók, akik ún. fix IP-címet használnak: gépüket állandóan ugyanaz a cím azonosítja – ez az állapot tipikus azokban az esetekben, amelyeknél a számítógép kapcsolata a hálózattal állandó (kábeltelevíziós, bérelt vonali internetkapcsolat esetén).

Példánk az ún. dinamikus IP-címmel kapcsolatos. Tegyük fel, hogy dinamikus IP-cím segítségével kapcsolódunk az internethez. Böngészés közben valójában az történik, hogy az általunk megtekintett weboldalt letöltjük számítógépünkre, ahol a böngészőprogram meghatározott szabályok szerint megjeleníti azt. Történik azonban még valami, ami adatvédelmi jogi szempontból releváns: a webszerver – vagyis az a számítógép, amely a

[214] Ilyen például a brit jog; lásd erről a kérdésről részletesebben a 2. fejezetet. A „relatív" jelzőt ebben az összefüggésben Douwe Korff (2002) nyomán használjuk.

weboldalt tárolja, amelyről az oldalt saját gépünkre lehívtuk – az esetek többségében naplófájlban rögzíti azon gép IP-címet, amelyre valamely oldalt lehívták (ez az ún. kliensgép, az adott esetben az általunk használt gép). Ezen a webszerveren tehát egy, az oldalakat lehívó gépek IP-címeiből, a lehívás időpontjából és a lehívott oldalból álló naplófájl található, amely a mi látogatásunk során is egy újabb bejegyzéssel bővült. Az adatvédelmi jogi kérdés az adott esetben az, hogy vajon ezen naplófájl tartalmaz-e személyes adatokat, vagyis kiterjed-e az abban található (egyes) adatokra az Avtv. hatálya.

Ha minden olyan adatot személyes adatnak tekintünk, amely meghatározott természetes személyhez akár több lépésben, akár több adatkezelő közreműködésével kapcsolható, akkor azt kell vizsgálnunk, így van-e ez az adott esetben.

Tegyük fel, hogy a böngészést követő napon valamely harmadik személy – például nyomozó hatóság, nemzetbiztonsági szolgálat stb. – a szükséges engedélyek birtokában megkísérli megállapítani azt, hogy az adott időpontban ki volt az a személy, aki az oldalt megtekintette. A naplófájlban rögzült az IP-cím, az időpont, és a lekért oldalra vonatkozó adat. Az IP-címből megállapítható az az internetszolgáltató, amelynek rendszerét a felhasználó az elérés során használta, tehát amelynek nagy valószínűséggel ügyfele – hiszen az IP-cím az ezen szolgáltató számára kiosztott tartományba tartozik. A következő lépés tehát az internetszolgáltató megkeresése. Tegyük fel, hogy ez a szolgáltató szintén naplófájlban tárolja azt az adatot, hogy adott IP-cím adott időpontban mely azonosítóval bejelentkező felhasználó számítógépéhez volt rendelve – ilyen naplófájl képzésére például a számlázás miatt lehet szükség. Így a hatóság már egy lépéssel közelebb jutott a felhasználó személyéhez, hiszen ismeri a felhasználói azonosítót. Lehetséges azonban, hogy az azonosító egy céghez tartozik, például egy háromtagú betéti társasághoz. Ebben az esetben a hírközlési szolgáltatónál rendelkezésre állhatnak azok a naplófájlok, amelyek a három tag telefonforgalmára vonatkoznak, s az ún. hívásrekordok tartalmazzák azt az adatot is, hogy az előfizető adott időpontban mely számot hívta. Ha a társaság valamelyik tagjának híváslistájában megtalálható az internetszolgáltató modemes előfizetők által használt száma, akkor – további feltételek teljesülése esetén, például az adott személy egyedül él, tanúk bizonyítják, hogy az adott időpontban használta a számítógépet – lehetséges, hogy a láncszemek elvezetnek egy meghatározott felhasználóhoz, aki az adott időpontban az oldalt megtekintette. Mindez így van egészen addig, amíg valamely naplófájlt nem törlik, ily módon megszakítva a személy és az adat között helyreállítható kapcsolatot.

Személyes adatnak tekintsük-e mindezek alapján a dinamikusan kiosztott IP-címet? Ha elfogadjuk azt az értelmezést, amely szerint a több lépésben, akár több adatkezelő által

felépíthető kapcsolat is elegendő a személyes adatkénti minősüléshez, akkor ez az adat személyes adat (bár példánkban egy omnipotens külső adatkezelő létét feltételeztük, aki a kapcsolatot létrehozza, az természetesen a szolgáltatók együttműködésével is felépíthető; a példában mindkét esetben eltekintünk a hatályos jogi szabályozás tárgyalásától, bár a nyomozó hatóságoknak illetve a nemzetbizonsági szolgálatoknak a hatályos jog szerint is módjuk van ilyen adatkezelésre). A „relatív" értelmezés elfogadása esetén azonban következtetésünk ellentétes lenne: mivel az IP-cím a webszerver üzemeltetőjének áll rendelkezésére (személyes adatkénti minősülés esetén ez a szervezet lenne az adatkezelő), s számára nem lehetséges az adat meghatározott természetes személyhez rendelése, ezért az adat nem személyes adat. A példa megvilágítja azt is, hogy a relatív értelmezés elfogadása azzal a veszéllyel jár, hogy olyan adatok kerülnek az adatvédelmi szabályozás hatályán kívülre, amelyek kezelése mégis érintheti az egyén jogait; ugyanakkor az ellenkező értelmezésből, amely szerint valamely adat közvetett kapcsolat esetén is személyes adatnak minősül, az adatkezelők igen széles körére kiterjedően következik számos adatvédelmi jogi kötelezettség (például az illusztrációként feltételezett esetben a webszerver-üzemeltetőknek minden olyan naplófájlt be kellene jelenteniük az adatvédelmi nyilvántartásba, amelyek meghatározott természetes személyhez köthető IP-címeket tartalmaznak).

Az ún. relatív értelmezés hívei számára az Avtv. miniszteri indokolása szolgáltat egy érvet. Az indokolás szerint „a [személyes adatra vonatkozó] meghatározás értelmezése szerint azok az adatok is személyes adatnak tekintendők, amelyek önmagukban ugyan nem, de *az adatkezelő birtokában lévő egyéb személyes adatokkal összevetve* az érintettel kapcsolatba hozhatók". (Kiemelés tőlem – *J. A.*) Kétséges azonban, hogy az indokolás idézett mondata kizárja, hogy a *más adatkezelő* birtokában lévő adatok segítségével visszaállítható kapcsolat esetén az adat személyes adatnak minősüljön, különös tekintettel az Avtv. 2. § 1. pontjának már hivatkozott második mondatára.

A kérdésben uralkodó jogalkalmazói álláspont közvetett kapcsolat esetén is elismeri a személyes adatkénti minősülést, ám ezzel ellentétes állásfoglalások is születtek (lásd alább).

6. A „kapcsolatba hozható" fordulat értelmezésével kapcsolatos alesetnek tekinthető *a kódolt adatok megítélésének kérdése*. Ebben az esetben arról kell állást foglalni, hogy a valamely személy vagy szervezet birtokában lévő olyan kódolt adat, amelynek adattartamához az adott személy vagy szervezet – a dekódolásra szolgáló kulcs ismerete nélkül – egyáltalán nem fér hozzá, vagy az adatot a kulcs ismerete nélkül nem képes természetes személyhez kötni, személyes adatnak minősül-e. A problémát az alábbi két esettel szemléltethetjük:

a) A 2003-as, nagy sajtóvisszhangot kapott ún. adatmentésügy tárgya az volt, hogy a pénzügyminiszter a minisztérium felügyelete alá tartozó egyes szervek, így az Adó- és Pénzügyi Ellenőrzési Hivatal teljes adatállományának átadását kérte abból a célból, hogy az adatállományok másolati példányát a Pénzügyminisztériumban tárolják. Jelen gondolatmenet szempontjából nem releváns az, hogy adott esetben volt-e meghatározott célja, illetőleg jogalapja az adattovábbításnak.[215] Érdekes viszont az az ügyben érintett hatóságok részéről több esetben elhangzott érvelés, amely szerint a szóban forgó adatbázisokat csak az adott hatóság egyedi fejlesztésű informatikai rendszerében lehet olvasni. Az állítás valóságának megítélése természetesen informatikai szakkérdés, ám ha feltesszük annak valódiságát, eljutunk egy adatvédelmi jogi problémához: személyes adatnak minősülnek-e ebben az esetben az adatok annál a szervnél, amelynél azok – formátumuk miatt – nem értelmezhetők, csak kódolt formában állnak rendelkezésre?

b) Hasonló kérdést vet fel egyes olyan algoritmusok alkalmazása, amelyek megőrzik az adat egyediségét, ám megakadályozzák azt, hogy az az algoritmus alkalmazása után is meghatározott természetes személyhez legyen köthető. Ilyenek az ún. lenyomatképző eljárások. Ezen eljárások valamely karaktersorozatból arra egyértelműen jellemző, meghatározott hosszúságú bitsorozatot állítanak elő. A lenyomatképző eljárások tulajdonsága az, hogy a képzett lenyomat egyértelműen származtatható az adott karaktersorozatból, a képzett lenyomatból a gyakorlatban nem lehetséges a karaktersorozat meghatározása vagy annak tartalmára történő következtetés, valamint az, hogy a képzett lenyomat alapján a gyakorlatban nem lehetséges olyan karaktersorozat utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat adódik.[216] Ezen eljárások ún. hash-függvények alkalmazásán alapulnak, amilyen például az MD5.[217]

Tegyük fel, hogy valamely – például elemzési – célokra egy másik adatkezelőnek (akár más országban működő adatkezelőnek) kívánjuk továbbítani ügyfeleink személyes adatait, például számlaforgalmát, a fogyasztói szokásaira vonatkozó adatokat. Az ügyfél meghatározott azonosító adataira a lenyomatképző eljárást alkalmazva olyan bitsorozatot kapunk, amelyből ezek az azonosító adatok nem állíthatók vissza; ezen azonosítóval együtt továbbíthatjuk a másik adatkezelőnek. Mivel a lenyomatképző eljárást a későbbiekben is

[215] Az adatvédelmi biztos az üggyel kapcsolatban 2003. március 26-án kiadott tájékoztatóját lásd a http://abiweb.obh.hu/abi/aktualis/127k0315.htm weboldalon.

[216] Az elektronikus aláírás technológiájában is központi szerepet játszó lenyomatképző eljárásokról lásd Almási 2002, 69.

[217] Az MD5 leírását lásd Rivest 1992.

alkalmazhatjuk, ezért mód van arra, hogy az utólag képződött számlaforgalmi adatokat is továbbítsuk, miután az érintett azonosító adataira újra alkalmaztuk a lenyomatképző eljárást.

Miben tér el a lenyomatképző eljárás alkalmazása attól, mint ha más, egyszerűbb azonosító kód segítségével oldanánk meg az utólagos adategyeztetést, illetve próbálnánk meg kizárni a továbbított adatok személyes adatkénti minősülését? Annyiban, hogy a képzett lenyomat nem utal vissza az azonosító adatokra, vagyis a hozzárendelés egyirányú. Ezáltal az adatkezelő az egyszerű azonosító kód használatához képest nagyobb eséllyel hivatkozhat arra, hogy mivel az adatok a lenyomatképzés után – a lenyomatképző algoritmus tulajdonságaiból következően – már nem köthetők az érintett természetes személyhez, ezért nem személyes adatok.

Ugyanakkor megjegyzendő, hogy a kapcsolat helyreállítása ebben az esetben sem kizárt, amennyiben az eredeti azonosító adatok rendelkezésre állnak. Tegyük fel, hogy a bűnüldöző hatóság célja az adott fogyasztói szokásokkal rendelkező személy azonosítása. A hatóság rendelkezésére áll a képzett lenyomat. Az adatokat továbbító társaságot megkeresve lehetséges az összes ügyfél meghatározott azonosító adataira alkalmazni a lenyomatképző eljárást. Mivel a képzett lenyomat egyértelműen származtatható az eredeti karaktersorozatból, az eljárás nyomán újra megkapjuk a többi között a rendelkezésre álló lenyomatot is. Ezek után csak ki kell választani azon eredeti azonosító adatokat, amelyekre az eljárást alkalmazva a rendelkezésünkre álló lenyomat adódott.

c) Hasonló kérdést vethetnek fel esetleg egyes chipkártyás alkalmazások is: tegyük fel például, hogy valamely természetes személy adatait tartalmazó személyes adatok képezik a kártya adattartamát, de az adott szerv – például adóhatóság – csak a kártya adattartamának meghatározott részéhez fér hozzá – vajon személyes adatnak minősül-e ebben az esetben a fizikailag birtokába került kártyán található többi, ám számára elérhetetlen adat? Ez a kérdés igen fontos lehet például annak megítélésekor, hogy egyes chipkártyára épülő elektronikus kormányzati alkalmazások esetén miképp érvényesíthető az osztott információs rendszerek elve – elegendők-e a kriptográfiai eszközök annak biztosítására, hogy a meghatározott ágazati azonosító kódhoz csak a jogosult alrendszerbe tartozó szervezetek férjenek hozzá, vagy a kártyák fizikai elkülönítése szükséges? Általánosabban feltéve a kérdést: a kódolás a magánszféra-védelem új eszköze-e, amely az információs önrendelkezés lehetőségeit növeli, vagy ragaszkodnunk kell a hagyományos garanciákhoz?[218]

[218] Burkert a magánszféravédő technológiák korlátai kapcsán tárgyalja a kérdést, s egyértelműen úgy foglal állást, hogy példája szerint (amelyben a bankkártya birtokosának azonosító adatait – nevét és lakcímét –

A kódolt adatok személyes adatkénti minősülésének értelmezése során ugyanazok a kérdések merülnek fel, mint az előző pontban. A lenyomatképző eljárások kapcsán rámutattunk arra, hogy ebben az esetben is lehetséges az adatok és az érintett személy közötti kapcsolat visszaállítása – ez minden kódolt adat esetében lehetséges, amennyiben a kód valamely személy számára rendelkezésre áll. Ha a személyes adat fogalmának relatív értelmezését elvetjük, akkor abból az következik, hogy a kódolt adatok a dekódolás lehetőségének fennállásáig személyes adatnak minősülnek.

7. Végül értelmezési problémát jelent az is, hogy mi minősül a törvény alkalmazásában *„adatnak", „következtetésnek"*. Az adat meghatározása az Avtv.-ben nem szerepel. A jogirodalomban megjelenő értelmezés szerint az adat „tények és elképzelések nem értelmezett, de értelmezhető formában való közlése, formailag befogadható, de szemantikailag nem értelmezett közlés".[219] Egy másik értelmezés szerint az adat „rögzített, tárgyiasult információ". A két értelmezésből eltérő jogi értékelés következhet például abban az esetben, ha valamely személy szóban hoz egy másik személy tudomására személyes adatot; az utóbbi értelmezés szerint ebben az esetben nem történne adattovábbítás. Ezzel kapcsolatban megjegyzendő, hogy egy, tárgyát tekintve hasonló (meghatározott jellemzőkkel bíró adatok kezelésének szabályairól szóló) jogszabály, az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény (Ttv.) értelmező rendelkezésben kifejezetten kimondja, hogy a hatálya alá tartozó (minősített) adatnak tekintendő „a szóban közölt államtitkot vagy szolgálati titkot képező információ" is.[220] A gyakorlatban az adatvédelmi biztosi gyakorlat szerint a szóban közölt, meghatározott természetes személlyel kapcsolatba hozható adat is személyes adatnak minősül.

Ez a kérdés jelentőséghez jut akkor, amikor abban a kérdésben foglalunk állást, vajon adatkezelésnek minősül-e valamely személyes információ szóbeli továbbítása, a csupán megfigyelést (de nem rögzítést) végző kamera üzemeltetése stb. Ha az adat rögzített, tárgyiasult információ, akkor ezek a cselekmények kívül esnek az adatvédelmi jog hatályán. Ha a személyes adat valamely *információ,* akkor ezek a tevékenységek – az adatkezelés fogalmának értelmezésétől függően – vagy az adatvédelmi jog hatálya alá esnek, vagy nem.

---

elkülönítve és titkosítva tárolják) a bankkártyaszám személyes adatnak minősül. A kérdés azért jelent korlátot ezen technológiák fejlesztése szempontjából, mert előre nem lehet megjósolni, hogy maga a rendszer – vagy azon nem magánszféravédő rendszerek, amelyekkel együttműködik – nem generál-e olyan addicionális információt, amely elegendő a kapcsolat helyreállításához személy és adat között. Lásd Burkert 1997, 132.

[219] Balogh 1998, 17.

[220] Lásd Ttv. 2. § (1) bekezdés 2. *b)* pontja.

Álláspontunk szerint a személyes adat nemcsak tárgyiasult, rögzített információ, hanem maga a személyhez kötődő információ, annak formájától, az adathordozótól függetlenül. (A megfigyelési céllal üzemeltetett kamerák adatvédelmi jogi megítéléséről lásd még az adatkezelés fogalmához fűzött kommentárt.)

Az alábbiakban részletesen tárgyaljuk, hogy az egyes jogalkalmazók gyakorlatában mely értelmezést nyert az „adat", a „következtetés" fogalma. Előre kell bocsátani azt, hogy egyes adatok *ex lege* személyes adatok. A törvény erejénél fogva személyes adat az azonosító kód, vagyis az „olyan, matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely a polgárt az adatkezelés során egyértelműen azonosítja".[221]

1.9.2. A személyes adat fogalma az adatvédelmi biztos gyakorlatában

1. Az adatvédelmi biztosi gyakorlat következetes abban, hogy Avtv. hatályát csak az élő természetes személyekkel kapcsolatban állapítja meg. „A magyar szabályozás ugyanis a személyes adatok védelmét nem hagyományos védelmi jogként, hanem aktív jogként, az információs önrendelkezés jogaként értelmezi. Önrendelkezése csak élő személynek lehet, így a szorosan vett adatvédelmi jog is csak élő személyekre vonatkoztatható. „A magyar adatvédelmi jog csak élő személyekre vonatkozik, ugyanakkor azonban a személyiséget a halál után a kegyeleti jog védi, mely többek között a levéltári törvénynek a személyes adatokat tartalmazó iratok kutathatóságáról szóló szabályaiban tükröződik."[222] „A személyes adatok védelme a magyar jogrendszerben az élő természetes személyeket illeti meg, a szervezeteket nem."[223]

Az elhunyt természetes személyek adatainak kezelésével kapcsolatban azonban felmerülhet azonban más, élő személyek adatainak kezelése is, amely már az Avtv. hatálya alatt áll: „amennyiben a túlélő családtagok, hozzátartozók nem ismertek, vagy hozzájárulásuk beszerzése aránytalan fáradságot jelentene, a fakszimilében leközölt dokumentumok esetén olyan képkivágást vagy más foto- vagy nyomdatechnikai megoldást alkalmazzanak, ami az

[221] A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 5. § (1)–(2) bekezdése.

[222] Állásfoglalás: a második világháborúban elesett katonák adatai a személyes adatok védelme mellett publikálhatóak (475/K/1998), ABI 1999, 314. o.

[223] Az egyes fontos tisztségeket betöltő személyek ellenőrzéséről és a Történeti Hivatalról szóló 1994. évi XXIII. törvény alapján az információs önrendelkezési jog és az információszabadság érvényesülésével kapcsolatban lefolytatott vizsgálat eredményét összegző ajánlás (225/K/1999), ABI 2000, 303. o.

otthonról írt levél feladóinak, illetve a frontról írt levelek, tábori levelezőlapok címzettjeinek azonosíthatóságát nem teszik lehetővé".[224] „Emellett azt is figyelembe kell venni, hogy a szóban forgó dokumentumokban nemcsak az abban nevesített személyekre, hanem azonosítható hozzátartozóikra, családjukra, túlélő rokonaikra, leszármazottaikra is vonatkozó adatok találhatók, illetve következtetések vonhatók le."[225]

A halál bekövetkezésének pillanatában tehát az adatvédelmi jog hatálya megszűnik, „ugyanakkor a személyiség és a »személyesség« nem szűnik meg azonnal, s védelmét egyfajta – a Polgári Törvénykönyv által elismert – kegyeleti jogi »csóva« van hivatva átvenni, amely az idő múlásával fokozatosan elenyészik"[226]. Az adatvédelmi biztos egy drámai esetben – amelynek során egy labdarúgó a pályán vesztett életét – azért marasztalt el közleményben egy bulvárlapot, mert „a címoldalán közzétette a szerencsétlenül járt sportoló haláltusája közben készült fényképét, megsértve ezzel emberi méltóságát, képmása és személyes adatai védelméhez fűződő jogát".[227]

2. Az adatvédelmi biztosi gyakorlat töretlen abban is, hogy a személyes adatokkal kapcsolatos védelem csak *természetes személyeket* illet meg: „A megfigyelések közvetlen alanyai nem csupán személyek [ti. természetes személyek], hanem szervezetek is voltak. A személyes adatok védelme a magyar jogrendszerben az élő természetes személyeket illeti meg, a szervezeteket nem."[228]

---

[224] Állásfoglalás: a második világháborúban elesett katonák adatai a személyes adatok védelme mellett publikálhatóak (475/K/1998), ABI 1999, 315. o. Az adott ügy szempontjából igen lényegesek a levéltári törvény rendelkezései is.

[225] Ajánlás a náci korszak zsidóüldözéseivel kapcsolatos, személyes adatokat tartalmazó iratok mikrofilmre viteléről és a jeruzsálemi Yad Vashem Archívumba továbbításáról (33/A/1995), ABI 1997, 237.

[226] Ajánlás a náci korszak zsidóüldözéseivel kapcsolatos, személyes adatokat tartalmazó iratok mikrofilmre viteléről és a jeruzsálemi Yad Vashem Archívumba továbbításáról (33/A/1995), ABI 1997, 237.

[227] Közlemény, 2004. január 28., lásd http://abiweb.obh.hu/abi/aktualis/blikk_kozl.htm. Az adatvédelmi biztos sajtónyilatkozataiból kiderül, hogy a közleményben olvasható, a személyes adatok védelméhez fűződő jogra történő utalás magyarázata az, hogy álláspontja szerint a halál beálltáig hozzájárulás kellett volna a kép közléséhez: „A *Blikk*ben közölt kép megsérthette Fehér Miklós személyes adataihoz fűződő jogát, azzal, hogy őt ilyen helyzetben ábrázolta, ehhez ugyanis – mivel a készítés időpontjában még életben volt – személyes hozzájárulása szükségeltetett volna. A fotóból egészségi állapotára lehet következtetni, ami ráadásul különleges adatnak minősül, fejtegette Péterfalvi." Lásd Csepregi J. Botond: Az adatvédelmi biztos a *Blikk* címlapját kifogásolja – Semmi nem indokolja a haláltusák ábrázolását. http://index.hu/sport/040127blikk/.

[228] Az egyes fontos tisztségeket betöltő személyek ellenőrzéséről és a Történeti Hivatalról szóló 1994. évi XXIII. törvény alapján az információs önrendelkezési jog és az információszabadság érvényesülésével kapcsolatban

A biztosi gyakorlat szerint adatvédelmi jogi szempontból természetes személynek minősül az egyéni vállalkozó is: az egyéni vállalkozóval kapcsolatba hozható adat személyes adat.[229]

3. Az adatvédelmi biztos több esetben értelmezte azt, hogy mely esetekben állapítható meg a személy és az adat közötti kapcsolat („kapcsolatba hozhatóság"). Gyakorlatában az az értelmezés tekinthető uralkodónak, amely szerint az adat közvetett, akár több lépcsőben, több adatkezelő által felépíthető kapcsolat esetében is személyes adatnak minősül: „a magyar adatvédelmi törvény definíciója szerint […] minden olyan adat személyes adat, amely természetes személlyel kapcsolatba hozható. Az ilyen adat személyes adat tekintet nélkül arra, hogy a kapcsolat csak több lépésben építhető fel, illetve arra, hogy a kapcsolat megteremtésére valamely adatkezelő önmagában nem képes."[230] Ezt az álláspontot az adatvédelmi biztos éppen a – fenti példa tárgyául szolgáló – IP-cím vonatkozásában fejtette ki.

A jelenlegi adatvédelmi biztos egy országgyűlési vizsgálóbizottság előtt (az ún. APEH-adatmentés-ügy kapcsán: az ügy ismertetését lásd alább, a kódolt adatok problémájának tárgyalásánál) megerősítette, hogy az adatvédelmi biztosi gyakorlat szerint a közvetett kapcsolat is elegendő a személyes adatként történő minősüléshez.[231] Ezt az

---

lefolytatott vizsgálat eredményét összegző adatvédelmi biztosi ajánlás (225/K/1999), ABI 2000, 309. A jogirodalomban lásd Trócsányi 2004, 81.

[229] Például ABI 1997, 61; ABI 2000, 265; ABI 2001, 77; ABI 2002, 108 stb.

[230] Állásfoglalás: internetezés az iskolában, a szolgáltatók és a felhasználók jogai, ABI 2000, 286.

[231] „Dr. Wiener György (MSZP): „A következő kérdésem már jogkérdés lenne. A magyar adatvédelmi jogi szakirodalomban és az adatvédelmi biztosok gyakorlatában is felmerült az a probléma, hogy a személyes adat fogalma esetében közvetettségnek kell fennállnia, tehát szigorúbb értelmezést veszünk alapul, vagy csupán a közvetlenség esetében minősíthető valamely adat személyesnek?

Tehát személyes adatnak minősül-e valamely személy birtokában lévő, ám számára elérhetetlen módon kódolt vagy más okból számára nem azonosítható adat? Meg kell jegyeznem, hogy a ma még hatályos adatvédelmi törvény szerintem nem teljesen egyértelműen foglal állást ebben a kérdésben, a módosított törvény már egyértelműen kimondja, hogy közvetettség esetében is az adat személyes adatnak minősül, a ma hatályos definícióban is van egy olyan mondat a helyreállíthatósággal kapcsolatosan, amely arra utal, hogy inkább a közvetettséget veszi alapul a magyar adatvédelmi törvény, ám a bírói gyakorlat sem egységes ebben. Mi az ön álláspontja ebben a kérdésben?

Dr. Péterfalvi Attila adatvédelmi biztos: *Az adatvédelmi biztos eddigi gyakorlata – és itt az elmúlt nyolc évre egyértelműen utalhatnék – a közvetettség mellett áll ki.* Tehát akkor is, hogy ha azonosítható vagy helyreállítható ez a kapcsolat." (Lásd az Országgyűlés kormányzati szerveknél, illetve a kormány felügyelete alá tartozó szerveknél, különös tekintettel az Adó- és Pénzügyi Ellenőrzési Hivatalnál elrendelt adatmásolással, esetleges

értelmezést erősíti az Avtv. 2. § 1. pontja második mondatának nyelvtani értelmezése is: „A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható”-törvényszöveg nem tartalmaz utalást arra, hogy a kapcsolatnak meghatározott adatkezelő által kellene helyreállíthatónak lennie.

Az uralkodó értelmezés mellett azonban egyes adatvédelmi biztosi állásfoglalásokban ellenkező interpretáció is megjelenik – ezen állásfoglalások többsége a jármű hatósági jelzésének (rendszámának) személyes adatkénti minősülésével foglalkozik. Egy ezzel kapcsolatos ügyben az adatvédelmi biztos azon álláspontját fejtette ki, hogy az autópálya-kezelő által rögzített, az elhaladó személygépkocsik hatósági jelzését (rendszámát) tartalmazó adatbázis nem tartalmaz személyes adatokat: „Ha pedig azoknak az adatait, akik jogszerűen használták az autópályát, törlik, mielőtt még bármiféle adatkérés történne a BM KH-ból, valójában személyes adatok kezelésére nem is kerül sor, mivel a rögzített adatok az adatkezelőnél [..] nem is hozhatók kapcsolatba az érintettekkel.”.[232] „A járművek hatósági jelzései – a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) szerint – *a BM Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal*ban személyes adatnak minősülnek”[233] (vagyis az autópálya-kezelőnél nem minősülnek annak – kiemelés tőlem – *J. A.*). Az értelmezés nem következetes, mivel ugyanazon ügy kapcsán a biztos olyan érvelést is kifejtett, amely szerint a hatósági jelzés továbbítása a BM Központi Hivatalának személyes adatok továbbítása lenne[234] (ami ellentmond annak, hogy az értelmezés szerint az autópálya-kezelő birtokában a forgalmi rendszámok *nem* személyes adatok, tehát azoknak az autópálya-kezelő általi továbbítása nem esik az Avtv. hatálya alá). A relatív értelmezés a rendszám mint személyes adat minősítése során más esetben is megjelenik az adatvédelmi biztos érvelésében.[235] Az idézett esettel

---

jogosulatlan adatkezeléssel, adatátadással, illetve az APEH informatikai rendszerének megismerésével, valamint az APEH által különböző adóalanyok felé történő információkéréssel összefüggő tevékenységek körülményeit vizsgáló bizottságának 2003. november 18-én tartott ülésének jegyzőkönyvét [kiemelés tőlem – *J. A.*].)

[232] 40/H/2002–11 sz. ügyirat (nem publikált).

[233] 40/H/2002–14 sz. ügyirat (nem publikált).

[234] 40/H/2002–14. sz. ügyirat (nem publikált).

[235] Lásd erre például azt az állásfoglalást, amelynek tárgya, hogy jogszerű-e a benzinkutaknál a fizetés nélkül elhajtó gépjárművek típusát, színét és rendszámát tartalmazó nyilvántartás vezetése. Az állásfoglalás idézi a személyes adat törvényi meghatározását, majd rögzíti, hogy „[a] fenti definícióból következően az érintetteknek nemcsak az ún. természetes személyazonosító adatai [..] minősülhetnek személyes adatnak, hanem minden olyan adat, amely az érintettek beazonosítására alkalmas lehet. Ennek megfelelően amennyiben a kezelt adatok alapján az adatkezelőnek lehetősége van arra, hogy az adatból egy meghatározott természetes személyt

kapcsolatban megjegyzendő, hogy a rendszámadatok – hasonlóan a fent tárgyalt, meghatározott személyhez köthető IP-címekhez – az európai jogalkalmazói gyakorlatban uralkodó álláspont szerint személyes adatoknak minősülnek.[236]

4. A fentiekkel összhangban foglalt állást az adatvédelmi biztos a *kódolt adatok* minősülésével kapcsolatban. A fenti példaként idézett APEH-adatmentés-ügyben kifejtette, hogy az adatok annál az adatkezelőnél is személyes adatnak minősülnek, amelynek informatikai rendszere nem alkalmas azok értelmezésére: „a szóban forgó adatkezelések annak ellenére is jogellenesek, hogy a Pénzügyminisztériumban tárolt adatokhoz »csak [az] adatot szolgáltató intézmények informatikai rendszerében […] lehet hozzáférni «".[237]

5. Az adatvédelmi biztos gyakorlata során – még mielőtt az adatkezelés fogalmának a 2003. évi novella által bevezetett változásából ez egyértelmű lett volna – szélesen, az irányelvnek megfelelően értelmezte az „adat" fogalmát a személyes adat meghatározásával összefüggésben (megszorító értelmezésre lásd alább az Alkotmánybíróság gyakorlatáról írottaknál Harmathy Attila interpretációját). Az adatvédelmi biztos szerint személyes adatnak minősülnek például a következők:

– név;[238] születési adatok, lakcím, foglalkozás, beosztás, munkahely;[239]

– „életrajzi adatok";[240]

---

beazonosíthasson, az adat személyes adatnak minősül." Ez a megfogalmazás mintha a relatív értelmezésre utalna, ám az állásfoglalás végül személyes adatnak minősíti a szóban forgó adatokat, és kimondja, hogy „..az Avtv.-ben megadott definíció értelmében a személyes adat minőségének megállapításához nem szükséges, hogy az adatkezelő az érintett személyt ténylegesen beazonosítsa, az Avtv.-ben meghatározott törvényi vélelem [sic!] érvényesüléséhez elegendő a beazonosíthatóság lehetőségének fennállása is". Lásd ABI 2001, 276. Más esetben a biztos mintha mégis a relatív értelmezést fogadná el: „miután a számlán a forgalmi rendszám névvel és lakcímmel együtt kerül rögzítésre (ettől személyes adat)" – fogalmaz egy, a MOL Rt. készpénzfizetési számlák kiállításával kapcsolatban követett gyakorlatát kifogásoló állásfoglalásában (ABI 1999, 320); az igazolvány sorszáma nem nem minősül személyes adatnak „mindaddig, amíg egy természetes személlyel összefüggésbe nem hozható[...]" – ha a külső szemlélő számára csak a sorszám válik megismerhetővé, „ez nem jelenti a személyes adatok védelméhez fűződő jog sérelmét, hiszen ezen adatok alapján nem állapítható meg a […] személy kiléte" (ABI 2005, 69).

[236] „Némely esetben egy tárgy és annak tulajdonosa vagy üzembentartója (registered keeper) között a kapcsolat olyan szoros, hogy a tárgyra vonatkozó adatot változatlanul a személyre vonatkozó adatnak tekintik: így mindenhol személyes adatként kezelik az autók rendszámtábláján szereplő adatokat és a meghatározott személyi számítógéphez köthető IP-címeket." Korff 2002, 17.

[237] ABI 2004, 41.

[238] ABI 1998, 247.

[239] ABI 1997, 187; ABI 2000, 190; ABI 2000, 23.

– biometrikus azonosítók, vagyis mérhető testi jellemzők, így az ujjlenyomat, a retina és az írisz képe, a kéz geometriája, a hang és az arc jellemzői;[241]

– a „vagyonra vonatkozó adatok”,[242]

– kereset, havi jövedelem,[243]

– a nyugdíj összege;[244]

– a bankszámla egyenlegére, forgalmára vonatkozó adatok, általában a magánszeméllyel kapcsolatba hozható banktitok;[245]

– az érintett tulajdonában/érdekeltségében lévő cég neve, tevékenységi köre, valamint az a tény/állítás, hogy az érintett Magyarország száz leggazdagabb embere közé tartozik;[246]

– családi állapot, kiskorú gyermekek vagy eltartott személyek száma;[247]

– képmás, az érintett azonosítására alkalmas képrészlet, hangfelvétel,[248]

– a beszélgetés során elhangzó kijelentés, megjegyzés, vélemény,[249]

– a tanúvallomás,[250]

– a képfelvevő, -rögzítő berendezések által felvett és tárolt felvételek;[251]

– a természetes személy által olvasott művek, a természetes személy olvasási szokásai[252];

– meghatározott személy által bonyolított telefonhívások listája, mind a telefon birtokosa, mint a másik fél vonatkozásában;[253]

– meghatározott természetes személlyel kapcsolatba hozható e-mail cím, webcím és weboldal (!);[254]

---

[240] ABI 1999, 323.

[241] ABI 2001, 249.

[242] ABI 1998, 224.

[243] ABI 2000, 190.

[244] ABI 2001, 70.

[245] ABI 1998, 220 és 224.

[246] ABI 2003, 268.

[247] ABI 2000, 190.

[248] ABI 1997, 173; ABI 2000, 201 és 209; ABI 2002, 288; ABI 2002, 314.

[249] ABI 2002, 263.

[250] ABI 2003, 246.

[251] ABI 2001, 217.

[252] ABI 1998, 277.

[253] ABI 1999, 256; ABI 2001, 269; ABI 2002, 284. A híváslisták személyes adatkénti minősülésével kapcsolatban lásd még alább a bírósági gyakorlattal kapcsolatban írtakat.

– a számítógépet az interneten azonosító IP-cím, amennyiben az meghatározott természetes személlyel kapcsolatba hozható;[255]

– az, hogy az érintett milyen oldalakat és milyen gyakorisággal tekint meg az interneten;[256]

– grafológiai vizsgálat eredményeképp előálló véleményben szereplő következtetések,[257]illetőleg maga a grafológiai és személyiségvizsgálat nyomán előálló szakvélemény;[258]

– az adósminősítési eljárás során nyert megállapítások;[259]

– a bizonyítvány tartalma;[260]

– az esküokmányban szereplő „Isten engem úgy segéljen!" fordulat;[261] az a tény, hogy az érintett közérdekű bejelentést tett;[262] egy perrel kapcsolatban „egy adott ténnyel, körülménnyel kapcsolatos állítások, illetve azok cáfolatai és az ezeket igazoló különböző bizonyítékok együttesen";[263]

– szakmai szervezet etikai bizottságának egy taggal kapcsolatos elmarasztaló állásfoglalása;[264]

– természetes személy által egy vizsgateszten bármely kérdésre adott válasz, illetve az íráskép;[265]

– az orvos által kapott hálapénz összege.[266]

Az adatvédelmi biztosi gyakorlatban jelentőséghez jutott az is, hogy az Avtv. meghatározása alapján a *„következtetés"* is adatnak minősülhet. A származásuk, etnikai

---

[254] ABI 1999, 329, a honlap címe tekintetében hasonlóan ABI 2001, 293; az e-mail cím tekintetében hasonlóan ABI 2002, 111, 2005, 308, stb.

[255] ABI 1999, 332, ABI 2000, 286.

[256] ABI 2002, 95.

[257] ABI 2000, 247.

[258] ABI 2005, 281

[259] ABI 2000, 213.

[260] ABI 2002, 239.

[261] „Az olyan esküokmányban, amely az eskütevő választásának megfelelően tartalmazza az »Isten engem úgy segéljen!« mondatot, különleges adat szerepel, mert általánosságban alkalmas lehet az érintett lelkiismereti meggyőződésére vonatkozó következtetés levonására is" (ABI 2002, 305).

[262] ABI 2001, 224.

[263] ABI 2003, 304.

[264] ABI 2000, 270.

[265] ABI 2003, 169 és 171.

[266] ABI 2005, 274.

azonosságuk miatt menekültté vált személyek neve nem különleges adat, hiába ad módot különleges adatra történő következtetésre.[267] E következtetés azonban már különleges adat; annak adatként történő kezelésére már a törvény által a különleges adatokra előírt szigorúbb szabályokat kell alkalmazni.

A közelmúltban az adat fogalmának megszorító értelmezése nyert teret az adatvédelmi biztosi gyakorlatban – erről lásd részletesen alább a 2. § 4. pontjához fűzött magyarázatot.

1.9.3. A személyes adat fogalma az Alkotmánybíróság gyakorlatában

1. A személyes adat fogalmával kapcsolatos alkotmánybírósági értelmezések közül előbb azokat tárgyaljuk, amelyek tárgya *a szervezetek adataira vonatkozó jogi védelem*.

Tény, hogy az Avtv. hatálya nem terjed ki a jogi személyekre és a jogi személyiség nélküli szervezetekre. Nem helytálló azonban az a megállapítás, hogy a „személyes adatok védelme" nem terjed ki ezekre a jogalanyokra. A 34/1994. (VI. 24.) AB határozatban az Alkotmánybíróság úgy foglalt állást, hogy „a természetes személyekkel kapcsolatba hozható adatok védelmére irányadó rendelkezéseket" alkalmazni kell szervezetekre is.[268]

Az érvelés egyrészt az Európa Tanács (ET) 1981-es adatvédelmi egyezményére, másrészt a Ptk. 75. § (2) bekezdésére és 81. §-ára épül: „az Alkotmánybíróságnak azt is vizsgálnia kellett, hogy a természetes személyekkel kapcsolatba hozható adatok védelmére irányadó rendelkezések mennyiben alkalmazandók a jogi személyekre vonatkozó adatok feltárására és felhasználására. Az Alkotmánybíróság állandó gyakorlata szerint [21/1990. (X. 4.) AB határozat (ABH 1990., 77.); 7/1991. (II. 28.) AB határozat (ABH 1991., 25.), 28/1991. (VI. 3.) AB határozat (ABH 1991., 114.)] az alapjogok rendszerint a jogi személyekre is vonatkoznak, így az alapjogok alkotmányos védelmét általában a jogi személyek is érvényesíthetik. Az Európa Tanács 1981-ben kelt és 1985-ben hatályba lépett adatvédelmi egyezményének (No 108.) 3. cikk 2. pont *b)* alpontjában foglalt értelmező szabálya szerint az egyezményt alkalmazni kell személycsoportokra, társaságokra, alapítványokra, egyesületekre, testületekre és minden más, közvetlenül vagy közvetve személyekből álló szervezetre is. A Polgári Törvénykönyvről szóló 1959. évi IV. törvény 75. § (2) bekezdése úgy rendelkezik, hogy a személyhez fűződő jogok védelmére vonatkozó szabályokat a jogi személyekre is alkalmazni kell, kivéve, ha a védelem – jellegénél fogva – csak a magánszemélyeket illeti

[267] ABI 2000, 251.

[268] Lásd előzményként a 34/1992. (VI. 1.) AB határozatot.

meg. A törvény 81. §-a pedig kimondja, hogy személyhez fűződő jogot sért az is, aki üzemi vagy üzleti titok birtokába jut, és azt jogosulatlanul nyilvánosságra hozza, vagy azzal egyéb módon visszaél."

Az ET adatvédelmi egyezményét azóta kihirdette az 1998. évi VI. törvény.[269] Megjegyzendő, hogy az AB határozatában hivatkozott rendelkezés nem az ET-egyezmény „személyes adat"-ra vonatkozó meghatározása: az az egyezmény 2. cikk *a)* pontjában található, s ahogy már idéztük, szövege szerint „személyes adat: bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik (adatalany)".

Az egyezménynek az AB által hivatkozott 3. cikk 2. pont *b)* pontja arról rendelkezik, hogy a bármely állam nyilatkozatot tehet az Európa Tanács főtitkáránál arról, hogy „a jelen egyezményt alkalmazza 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 Magyar Köztársaság nem tett ilyen nyilatkozatot.[270] Az ET-egyezményre történő hivatkozás tehát az adott összefüggésben téves.

A Ptk. 75. § (2) bekezdésére és 81. §-ára történő hivatkozást vizsgálva kérdés, hogy az Alkotmánybíróság értelmezéséből következik-e az, hogy a 75. § (2) bekezdéséből következő védelmet a testület úgy értelmezi, mint amelyet a 81. § valósít meg. Vajon csak az üzleti titokra[271] vonatkozó szabályok juttatják érvényre a jogi személyek és jogi személyiség nélküli szervezetek adatainak védelméhez fűződő jogot? Álláspontunk szerint nem ez a helyes értelmezés. A 75. § (2) bekezdéséből az következik, hogy ha a védelem – jellegénél fogva – nem csak magánszemélyeket illethet meg, a személyhez fűződő jogokra vonatkozó minden szabályt alkalmazni kell jogi személyekre is. A bírói gyakorlat a 75. § (2) bekezdésének kiterjesztő értelmezésével a védelem körét úgy tágította, hogy az kiterjed a jogi személyiség

[269] Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény.

[270] Lásd http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=8&DF=&CL=ENG&VL=1, 2004. április 4-i állapot szerint. A Magyar Köztársaság csak a 3. cikk 2. pont *c)* pontja szerint nyilatkozott a főtitkárnál arról, hogy az egyezményt alkalmazza a személyes adatok nem gépi eszközökkel feldolgozott állományaira is, illetve a 13. cikk 2. *a)* pontja szerint az Igazságügyi Minisztériumot nevezte meg, mint amely részt vesz az egyezmény alkalmazása során a felek közötti kölcsönös segítségnyújtásban. A 3. cikk 2. *b)* pont szerinti nyilatkozatot a felek közül Ausztria, Norvégia, Olaszország és Svájc tett.

[271] Az üzemi titok fogalma a 81. § 2003. június 9-én hatályba lépett módosításával eltűnt a Ptk.-ból.

nélküli szervezetekre is.[272] A Ptk. 83. § (1) bekezdése szerint: „A számítógéppel vagy más módon történő adatkezelés és adatfeldolgozás a személyhez fűződő jogokat nem sértheti". Álláspontunk szerint a Ptk. 75. § (2) bekezdésének és 83. §-ának együttes értelmezéséből az következik, hogy a 83. §-ban meghatározott védelem, illetve az ott rögzített jogok jogi személyeket és jogi személyiség nélküli szervezeteket is megilletnek. Ennek legjelentősebb következménye, hogy a Ptk. 83. § (2) bekezdése alapján, amely szerint „[a] nyilvántartott adatokról tájékoztatást – az érintett személyen kívül – csak az arra jogosult szervnek vagy személynek lehet adni", a szervezetekkel kapcsolatos adatokról történő tájékoztatás is jogilag szabályozott. További értelmezési kérdést vet fel a Ptk. 83. § (3) bekezdésében rögzített helyesbítési jog, amely szerint „ha a nyilvántartásban szereplő valamely tény vagy adat nem felel meg a valóságnak, az érintett személy a valótlan tény vagy adat helyesbítését külön jogszabályban meghatározott módon követelheti", ahol az utalás az egyes eljárásjogi és a nyilvántartásokra vonatkozó külön jogszabályok mellett az Avtv. szabályaira is vonatkozhat. A Ptk. 75. § (2) bekezdéséből következően ebben az esetben is lehetséges olyan értelmezés, amely szerint a helyesbítési jog a szervezetet mint adatalanyt is megilleti, amely jogát ebben az esetben annak ellenére gyakorolhatja az Avtv. szerint, hogy annak hatálya csak a természetes személlyel összefüggésbe hozható adatokra terjed ki.

Álláspontunk szerint tehát, miként azt az Alkotmánybíróság is megállapította, a Ptk.-ban rögzített, a személyhez fűződő jogokra vonatkozó szabályokat, így az üzleti titok védelmére vonatkozó 81. §-ban írtak, valamint a 83. §-ban rögzített, kifejezetten adatvédelmi jellegű szabályok jogi személy és jogi személyiség nélküli gazdasági társaság adatalanyok esetén is alkalmazandók; az Avtv.-ben rögzített szabályokat azonban kizárólag a természetes személyekkel összefüggésbe hozható adatok kezelése esetén kell figyelembe venni[273].

---

[272] „A gyakorlat a törvény előírásait tovább tágította azzal, hogy személyiségi jogvédelmet biztosít minden olyan nem természetes személynek is, amely jogi személyiséggel ugyan nem rendelkezik, de önálló jogalanyként vesz részt a társadalom életében. Ennek megfelelően alkalmazza a vonatkozó rendelkezéseket például a saját név alatt jogszerzésre jogosult és kötelezettségvállalásra is képes jogi személyiséggel nem bíró gazdasági társaságok vonatkozásában (betéti társaság, közkereseti társaság)." Gellért 2004.

[273] A kérdés összefüggésben áll a közérdekű adat és a közérdekből nyilvános adat fogalmának értelmezésével is. Az adatvédelmi biztos gyakorlatában újabban megjelent értelmezés szerint „Közfeladatot ellátó szervnek, személynek nem minősülő természetes személyre, jogi személyre, illetve jogi személyiség nélküli szervezetre vonatkozóan törvénynek kell kimondania valamely adat nyilvánosságát, megjelölve a nyilvánosságra hozandó adatkört is" (ABI 2005, 542). A közérdekből nyilvános adat fogalmának bevezetése nyomán tehát a biztos olyan értelmezést látszik magáévá tenni, amely szerint a szervezeti adatok nyilvánosságához – hasonlóan a személyes adatokéhoz – kifejezett törvényi rendelkezés szükséges. Más megfogalmazásban: az ezekben az ügyekben

2. Figyelemre méltó az Alkotmánybíróság 58/2001. (XII. 7.) számú – nem adatvédelmi tárgyú – határozata az *azonosíthatóság* tekintetében. A határozat szerint az azonosítást segítő, a személyt jellemző legfőbb attribútum a név: „a saját név a személy identitásának egyik – mégpedig alapvető – meghatározója, amely azonosítását, egyúttal másoktól való megkülönböztetését is szolgálja, ezért a személy individualitásának, egyedi, helyettesíthetetlen voltának is az egyik kifejezője. „A saját névhez való jog tehát az önazonossághoz való jog alapvető eleme, így olyan alapvető jog, amely a születéssel keletkezik, az állam által elvonhatatlan és – lényeges tartalmát tekintve – korlátozhatatlan." Ez természetesen nem jelenti azt, hogy a meghatározott nevű természetes személyhez társítható adat személyes adat az Avtv. 2. § (1) bekezdésének értelmében, ám azt igen, hogy a név megismerésének lehetősége az azonosíthatóság feltétele.

3. Az Alkotmánybíróság gyakorlatában megjelenő másik értelmezési probléma az, hogy mennyire széles körben értelmezhető az Avtv. által a személyes adat meghatározása során használt „*adat"* fogalma. Egy Harmathy Attila alkotmánybíró által megfogalmazott párhuzamos indokolásban jelenik meg az a nézet, amely szerint az Avtv. 2. § 1. pontjában használt „adat" szűkebb értelemmel bír, mint amely a fenti ismertetett jogalkalmazói gyakorlatból kibontakozni látszik. Ezen álláspont szerint „a szabály [az Avtv. 2. § 1. pont] adatot jelöl meg; a fénykép, a hangfelvétel azonban kifejezett jogszabályi előírás nélkül nem tartozik az adatok közé". Az 1998. évi VI. törvénnyel kihirdetett 1981. évi ET-egyezmény meghatározását vizsgálva Harmathy elismeri, hogy az szélesebb körű („bármely információ" személyes adat, amely azonosított egyénre vonatkozik), ám úgy foglal állást, hogy „az egyezménynek ebből a rendelkezéséből sem következik azonban, hogy a fényképekre, hangfelvételekre, ujjlenyomatokra mindenben azonos szabályokat kell alkalmazni, mint az adatokra (például név, lakcím)".[274] Az Avtv. 2003. évi novellájának hatálybalépését követően ennek az értelmezésnek nem marad tere, hiszen – az adatkezelés fogalmán keresztül – az kifejezetten a törvény hatálya alá vonja a „fénykép-, hang- vagy képfelvétel készítését", és „a

---

kifejtett értelmezés arra vezet, hogy az védelem nem csak a szervezetek egyes kitüntetett adataira (pl. az üzleti titkokra) terjed ki, hanem a szervezet minden adatára. Álláspontunk szerint ez az értelmezés nem helyes, ellentmond a közérdekű adat és közérdekből nyilvános adat törvényi meghatározásának.

[274] Ez az értelmezés része annak a nézetnek, amely szerint fényképfelvétel és hangfelvétel kezelését előíró jogszabály alkotmányosságának vizsgálata során nem az Alkotmány 59. § (1) bekezdésében meghatározott személyes adatok védelméhez fűződő jogot, hanem az 54. § (1) bekezdésében rögzített – az általános személyiségi jog megfogalmazásának tekintendő emberi méltósághoz fűződő – jogot kell alapul venni [35/2002. (VII. 19.) AB határozat, Harmathy Attila párhuzamos indokolása].

személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítését" is. Az, hogy az „adat" az Avtv. alkalmazásában a fenti jogalkalmazói gyakorlat által tükrözött szélesebb körű fogalmat jelenti, abból is következik, hogy az Avtv. az irányelvet építi be a magyar jogba, amely esetében ez az értelmezés egyértelmű.[275] Az Avtv. meghatározása tehát nem értelmezhető szűkebben pusztán annak alapján, hogy az „adat" szót használja az „információ" szó helyett – ennek mind az „adatkezelés" fogalmának meghatározásából, valamint a 2003. évi novella indokolásából kitűnő jogalkotói cél, mind az ellentmond, hogy az Avtv.-t az irányelvvel összhangban kell értelmezni.

Az AB többsége azonban az adott esetben a személyes adatok védelméhez fűződő jog korlátozásaként értékelte a videofelvételek készítését az érintettekről, így – közvetve – helyt adott a „szélesebb" értelmezésnek.[276]

1.9.4. A személyes adat fogalma a bírói gyakorlatban

A kapcsolatba hozhatóság problémája merült fel a Legfelsőbb Bíróság a BH 2001/269. számon közzétett eseti döntésének alapjául szolgáló ügyben is. A felperesi kereseti kérelem arra irányult, hogy „a bíróság állapítsa meg: az alperes üzletszabályzatának az az általános szerződési feltétele, amely szerint a részletes számla közléséért az előfizető díjat tartozik fizetni, jogszabályba ütközik, s ezért az semmis". A felperesi érvelés szerint a részletes számlán feltüntetett adatok a felperes – az előfizető – személyével kapcsolatba hozható adatok, s „ezekből az adatokból a felperesre vonatkozó következtetések sora levonható".

A felperes érvelésében az 1998. évi VI. törvénnyel kihirdetett ET-egyezmény rendelkezéseinek megsértésére is hivatkozott. A Legfelsőbb Bíróság azonban a felülvizsgálati kérelmet elutasította. A döntés szerint: „Helyesen mutatott rá a jogerős ítélet arra, hogy meghatározott természetes személlyel kapcsolatba hozható adatnak minősül a természetes személy lakáscíme, telefonszáma. Az az adat azonban, hogy az előfizető telefonvonaláról mikor, mely telefonszám hívásával és milyen időtartamban került sor telefonbeszélgetésre, meghatározott természetes személlyel már nem hozható *közvetlenül* összefüggésbe. A telefonbeszélgetések időtartama, irányultsága alapján meghatározott természetes személyre

[275] Dammann–Simitis 1997, 110.

[276] Az AB egyes határozataiban magától értetődően nyilvánította személyes adatnak a nevet [54/2000 (XII. 18.) AB határozat], a vagyonra vonatkozó adatokat [20/1990. (II. 18.) AB határozat, 21/1993. (IV. 2.) AB határozat, 30/1997. (IV. 29.) AB határozat].

következtetés sem vonható le. Ezért a hívásrészletezés adatai nem minősülnek olyan személyes adatnak, amelyekről az adatkezelőnek ingyenesen kellene az érintett részére tájékoztatást adnia. E megállapítás nincs ellentétben az Európa Tanács tagjai által megkötött és az 1998. évi VI. törvénnyel Magyarországon is kihirdetett, »Az egyének védelméről a személyes adatok gépi feldolgozása során« címmel létrejött egyezmény rendelkezéseivel sem." [Kiemelés tőlem – *J. A.*] Az eseti döntésből kiolvasható értelmezés alapján közvetlen kapcsolat esetén az adat személyes adat, ám közvetett kapcsolat esetén nem az.

A döntés tárgyával kapcsolatban megjegyzendő, hogy az adatvédelmi biztos a híváslistát többször személyes adatnak minősítette. Ilyen volt például az az eset, amikor a biztos önkormányzati képviselők hívásairól generált listák szabályozatlan kezelését kifogásolta.[277] Ebben az esetben azonban a hívó félnek PIN-kóddal kellett magát azonosítania, így a hívó személye és a híváslista közötti kapcsolat szorosabb volt – bár, mint az kiderült az ügy vizsgálata során, „előfordult olyan eset, amikor valaki visszaélt más kódjával, számlájára hívást kezdeményezett".[278] Egy másik esetben a biztos úgy foglalt állást, hogy a mobiltelefonról intézett és az arra érkező hívások listája személyes adat, „mégpedig legalább két személy adata: azé, akié a telefon, és azé is, akivel ő a beszélgetést folytatta".[279] Ebben az esetben a személy és az adat közötti kapcsolat valóban szorosabb, hiszen a mobiltelefonra általában jellemzőbb a személyes használat, mint a vezetékes telefonra. Az a megállapítás azonban, hogy a másik fél hívószáma is minden esetben (tehát az azonosíthatóságot illető további feltételekre tekintet nélkül, így attól függetlenül, hogy a másik fél telefonszáma mobiltelefonszám-e, illetve egyébként egyértelműen azonosítható-e a másik számot használó személy) személyes adat, ellentmond a Legfelsőbb Bíróság döntésében foglalt megállapításnak. Egy további adatvédelmi biztosi állásfoglalás feltétel nélkül minősíti személyes adatnak az előfizető által egy adott időpontban hívott számok listáját.[280]

A joggyakorlat tehát ellentmondásos – a fenti bírósági határozat arra is illusztrációként szolgálhat, hogy az adatvédelmi biztosi gyakorlatban kialakult értelmezés még az adatvédelmi jog alapfogalmainak értelmezése terén sem feltétlenül áll összhangban a – sajnos meglehetősen szűk körű – bírósági gyakorlattal. Álláspontunk szerint a személyes adat fogalmának értelmezésekor az adatkezelők abban az esetben járnak el helyesen, ha a jogi kockázat kizárása érdekében a fogalomnak az adatvédelmi biztosi gyakorlatban uralkodó

[277] ABI 1999, 254 (803/A/1997, 387/A/1998.)

[278] ABI 1999, 254

[279] ABI 2001, 269 (533/A/1999.)

[280] ABI 2002, 284 (410/K/2001.)

interpretációját fogadják el, vagyis az érintettel akár közvetett úton, több adatkezelő által kapcsolatba hozható adatokra is alkalmazzák az Avtv. rendelkezéseit.[281]

1.9.5. Az irányelv vonatkozó rendelkezései

Az irányelv 2. cikk *a)* pontja szerint „»személyes adat« az azonosított vagy azonosítható természetes személyre (»érintettre«) vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén".

E definíció nem tér el lényegesen az Avtv. – épp az irányelvre tekintettel – módosított 2. § 1. pontjától. A „közvetlen vagy közvetett módon azonosítható" fordulat arra utal, hogy nem felelne meg az irányelvnek az a tagállami jogalkotó, amely kizárólag az adatkezelő általi azonosíthatóság esetén minősítené az adatot személyes adatnak.[282]

Érdekes e tekintetben még az irányelv preambulumának (26) bekezdése, amely a következő:

„mivel a védelem elveit minden azonosított vagy azonosítható személyre vonatkozó információ esetében alkalmazni kell; mivel 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; mivel a védelem elvei nem alkalmazhatók az olyan módon anonimmá tett adatokra, ahol az érintett a továbbiakban nem azonosítható; mivel a 27. cikk szerinti eljárási szabályzat hasznos eszköz lehet útmutatásként ahhoz, hogy hogyan kell az adatokat anonimmá tenni, és olyan formában megőrizni, amelyben a szóban forgó adatok azonosítása a továbbiakban már nem lehetséges".

---

[281] További, az adat fogalmával kapcsolatos bírósági határozat például BH 2002/234: a feljelentésben meghatározott személyről tett nyilatkozat a feljelentett személyes adatait tartalmazza.

[282] Az 1998. évi brit törvény szerint *személyes adatok azok az adatok, amelyek olyan élő személyre vonatkoznak, aki azonosítható ezen adatok, vagy ezen adatokból és más olyan információ segítségével, amely az adatkezelő birtokában van, illetve valószínűleg az adatkezelő birtokába kerül.* A brit törvény az azonosított személyekre vonatkozó adatok mellett csak azon személyekre vonatkozó adatokat minősíti személyes adatnak, amelyek az *adatkezelő által* azonosíthatók. Az irodalom szerint „egyáltalán nem világos, hogy mi az oka e korlátozásnak az irányelv tekintetében – ez bizonyos nehézségeket okozhat". Jay–Hamilton 1999, 30.

A preambulum szerint az azonosíthatóság megítélésekor az is szerepet játszik, hogy az alkalmazott módszert „valószínűleg", „ésszerűen elvárható valószínűséggel"[283] felhasználna-e az adatkezelő vagy más személy a kapcsolat megteremtéséhez; lehetőség van tehát arra, hogy a jogalkalmazó olyan esetekben, amelyekben a kapcsolat megteremtésének lehetősége elméleti, csekély valószínűségű, irányelvkonform értelmezéssel zárja ki az Avtv. hatályának megállapíthatóságát.

1.9.6. Szabályozási javaslat

1. Az Avtv. várható módosításának előzményeképpen megalkotott koncepció 2004. decemberi állapot szerint bevezette volna az „adat" fogalmának meghatározását a törvénybe, a következők szerint: „adat: bármilyen információ függetlenül annak rögzítése, tárolása vagy továbbítása módjától, önálló vagy gyűjteményes jellegétől". Ez a módosítás végül nem került be a törvénybe, a jogalkotó az „adat" fogalmát csak a közérdekű adat meghatározásának keretében pontosította (lásd alább a 2. § 4. pontjához fűzött magyarázatot). A választott megoldás szerencsés, mivel a személyes adatok tekintetében nem korlátozza a jogalkalmazót az Irányelvhez illeszkedő értelmezésben, míg a közérdekű adatok vonatkozásában – vonatkozó uniós jogszabály hiányában – az adat fogalmának jogalkotói értelmezésével biztosítja a széleskörű nyilvánosságot.

2. A kapcsolatba hozhatóság, a személyes adatkénti minőség megállapíthatóságára vonatkozóan figyelemre méltó az osztrák adatvédelmi jog szabályozási megoldása. A szabályozásnak el kell kerülnie, hogy – a személyes adatkénti minősülés kizárásával – megkerülhetőek legyenek a törvény rendelkezései, ám biztosítania kell azt is, hogy távoli összefüggés esetén ne háruljanak indokolatlan kötelezettségek az adatkezelőkre. Az osztrák jogalkotó ezt az „indirekt személyes adat" fogalmának bevezetésével biztosítja. Az indirekt személyes adat olyan adat, amely ugyan kapcsolatba hozható az érintettel, ám az adott adatkezelő (vagy más alany) a kapcsolatot jogszerű eszközökkel nem képes megteremteni.[284] A törvény az indirekt személyes adatok kezelésére számos esetben az általánosnál megengedőbb szabályokat tartalmaz (például a harmadik országba történő továbbítás, a bejelentési kötelezettség, az érintett jogainak biztosítása stb. tekintetében).

[283] Az angol szövegben „the means likely reasonably to be used", a német szövegben „alle Mittel […] die vernünftigerweise […] eingesetzt werden könnten".

[284] Lásd az osztrák adatvédelmi törvény 4. § 1. pontját.

Az indirekt (közvetett) személyes adat fogalma álláspontunk szerint könnyen illeszthető lenne az Avtv. fogalomrendszeréhez is. Az ilyen adatok kezelésére vonatkozó egyes különös szabályok megállapításával a jogalkotó nagyban segíthetné a jogalkalmazás egységességét.

1.9.7. A közérdekű adat

1. Az Avtv. 2. § 4. pontjában foglalt meghatározás szerint „*közérdekű adat:* az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől" A közérdekű adat fogalmával kapcsolatban értelmezési kérdésként merül fel, hogy *mely szervek, személyek* kezelésében lévő adatok minősülnek ilyen adatnak, vagyis a miképpen határolható körül az „állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szervek vagy személyek" köre. Erre vonatkozóan lásd alább az adatvédelmi biztosi gyakorlatot.

2. Közérdekű adatnak az Avtv. hatálybalépésétől a 2003-as ún. „üvegzseb"-program keretében elfogadott módosításig csak azon adat minősült, amely a szerv vagy személy *kezelésében volt*. Az adatvédelmi biztos gyakorlatában is egyértelmű volt az az értelmezés, hogy a közfeladatot ellátó szerv a *rendelkezésére álló* adatokat köteles szolgáltatni.[285]

A szerv nem kötelezhető „az adatok kivonatolására, összesítésére, feldolgozására, aggregátumok készítésére – ha az nem tartozik az adatkezelő alapfeladatához vagy nem áll eleve rendelkezésére".[286]

A hatályos – immár a 2003. évi novella által megállapított – meghatározás már nem kizárólag a birtokos, az „adatkezelő" személyéhez köti a közérdekűadat-minőséget, hanem az megállapítható akkor is, ha az adat ilyen szerv vagy személy tevékenységére vonatkozik. Mivel a 19. § változatlanul csak a korábban meghatározott alanyi kör számára írja elő a közérdekű adatok nyilvánosságra hozatalának kötelezettségét, ezért álláspontunk szerint a meghatározás változása nem érdemi.

---

[285] ABI 2001, 144.

[286] 862/A/2004, idézi a 453/K/1997. ügyben született állásfoglalást.

Újabban értelmezési kérdésként merült fel az, hogy a „szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó" fordulat esetén a „valamint" szó a két feltétel között „és" vagy „vagy" relációt jelez. Álláspontunk szerint a helyes értelmezés az utóbbi – lásd erre vonatkozóan alább az adatvédelmi biztosi gyakorlat bemutatását. Ehhez kapcsolódóan kell megválaszolnia a jogalkalmazónak azt a kérdést is, hogy a közérdekből nyilvános adat fogalmának bevezetését követően is fennáll-e az a korábbi helyzet, hogy minden, a meghatározott szervek kezelésében lévő adat közérdekű adatnak minősül, vagy az új fogalomrendszer szerint lehetséges az, hogy egyes közfeladatot ellátó szervek kezelésében lévő – nem személyes – adatok nem minősülnek közérdekű adatnak. Álláspontunk szerint a a közérdekű adat meghatározásából, és abból, hogy a közérdekből nyilvános adat definíciója erre a meghatározásra épít, az következik, hogy a korábban követett értelmezési gyakorlat feladása nem egyeztethető össze az Avtv. hatályos rendelkezéseivel sem. (Lásd erről részletesebben alább az adatvédelmi biztosi gyakorlatról írtakat.

3. A közérdekű adat fogalmának meghatározása szerint ezen adatkörbe tartozik minden olyan adat, amely a fent tárgyalt alanyi kör kezelésében van, illetőleg annak tevékenységére vonatkozik, kivéve az Avtv. 2. § (1) bekezdésében meghatározott személyes adatokat. A meghatározásból következően *valamely adat* – az Avtv. alkalmazásában – *nem lehet egyszerre személyes adat és közérdekű adat*. A fogalom értelmezésével kapcsolatban a jogalkalmazói gyakorlatban tapasztalható zavarok több forrásra vezethetők vissza:

– A személyes adat Avtv. által meghatározott fogalma alapján a személy és az adat közötti igen távoli összefüggés esetén is megállapítható a személyes adatként minősülés, ezáltal a közfeladatot ellátó szerv vagy személy birtokában lévő vagy rá vonatkozó adatok igen széles köre „kiüresítheti" a közérdekű adatkört.

– Az Avtv. 19. § (4) bekezdése szerint: „Az (1) bekezdésben említett szervek hatáskörében eljáró személynek a feladatkörével összefüggő személyes adata a közérdekű adat megismerését nem korlátozza." A jogalkalmazás során igen sok esetben mosódik össze az eljáró személy személyes adata és a megismerendő közérdekű adat. A 19. § (4) bekezdésének alkalmazásában soha nem lehet személyes adat az az adat, amelynek megismerése a cél.

– Az Alkotmánybíróság gyakorlatában teret nyert az a fogalomhasználat, amely a közérdekű adat fogalmát „nyilvános adat" értelemben használja (például meghatározott személyes adatok „közérdekűvé válásáról", „közérdekűvé tételéről" szól), ily módon eltérve az Alkotmány által biztosított személyes adatok védelméhez fűződő jog és közérdekű adatok megismeréséhez fűződő jog gyakorlásának kereteit meghatározó Avtv. fogalomrendszerétől;

mindez pedig egyes esetekben az adatvédelmi biztosi ajánlások és állásfoglalások szövegezésében is tükröződik.Újabb fejlemény, hogy az Alkotmánybíróság szerint a közérdekből nyilvános adat fogalmát is felhasználja a fentihez hasonló értelmezés során: „A személyes adat nyilvánosságra hozatalát [az Avtv.] 3. § (4) bekezdése szerint törvény közérdekből elrendelheti. Ekkor a személyes adat közérdekből nyilvános adattá válik és a »közérdekű adatokéhoz hasonló jogi elbírálás alá esik, amelynek a szabályait az adatvédelmi törvény III. fejezete tartalmazza" [44/2004. (XI. 23.) AB határozat]. Részletesebben lásd alább a jogalkalmazó szervek gyakorlatát. (A közérdekű adatokra vonatkozó szabályozás és egyes törvény által meghatározott titkok kezelésének szabályai közötti konfliktusokról lásd a 19. §-hoz fűzött magyarázatot.)

4. Lényeges értelmezési kérdés, hogy a törvény által meghatározott szervek és személyek kezelésében lévő minden adat közérdekű adat-e (a személyes adatok kivételével), vagy csak az e szervek tevékenységére vonatkozó adatok minősülnek közérdekű adatnak (így a személyes adatokon kívül nem minősülnek annak például a szerv kezelésébe került üzleti titkok stb. sem). Az előbbi értelmezés szerint az Avtv. által meghatározott szerv kezelésében lévő – személyes adatnak nem minősülő – minden adat közérdekű adat; ám ezek közül egyes adatok – például az üzleti titoknak minősülő adatok – nyilvánosságát külön törvény korlátozza, vagyis ezek nem nyilvános közérdekű adatok (ez az értelmezés volt uralkodó a korai adatvédelmi biztosi gyakorlatban). Az utóbbi interpretáció szerint a közérdekű adatok köre szűkebb, és a személyes adatokon kívül számos, a meghatározott szerv kezelésében lévő adat nem közérdekű adat (a közelmúltban az adatvédelmi biztos több esetben így foglalt állást).

5. A 2005. évi XIX. törvény a meghatározásban korábban szereplő „adat" fogalom helyébe a „bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől" szöveget illesztette. A módosítás előzménye az volt, hogy egy bíróság jogértelmezése szerint nem minősült adatnak – így közérdekű adatnak - az Alkotmánybíróságnak címzett, jogi érvelést tartalmazó indítvány (lásd alább a 3. pontban.) A korrekció nyomán várhatóan kevesebb tere lesz azon jogértelmezéseknek, amelyek az „adat" fogalmára építve zárnak ki egyes tartalmakat a közérdekű adatkörből.

1.9.8. Az adatvédelmi biztos közérdekű adatokkal kapcsolatos gyakorlata

1. Az „állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy” fogalmának értelmezéséhez az alábbi adatvédelmi biztosi állásfoglalások nyújtanak támpontot. Az adatvédelmi biztos szerint annak megállapíthatóságát, hogy az adott szerv állami vagy helyi önkormányzati feladatot ellátó szervnek minősül-e, „a hatásköri és illetékességi szabályok biztosítják, illetve az, hogy az állam vagy az önkormányzat a feladata ellátására valamilyen szervezetet hoz létre vagy szerződéssel a feladat ellátását másnak átengedi”. A „jogszabályban meghatározott egyéb közfeladatot ellátó szerv” tekintetében a biztos kifejtette, hogy „a jogszabálynak egyszerre kell megjelölnie a közfeladatot és azt ellátó szervet is, mégpedig úgy, hogy a jogszabályból magából a szerv is azonosítható legyen legalább olyan speciális kritérium(ok) megadásával, amely(ek) az azonos vagy hasonló szervezeti formában működő vagy tevékenységet végző más szervezetektől megkülönbözteti(k). Önmagában a szervezeti formára vagy a végzett tevékenységre utalás nem elegendő.”[287]

Az adatvédelmi biztos szerint közfeladatot lát el

– az Országos Rádió és Televízió Testület;[288]

– közfeladatot ellátó szerv az ELMÜ Rt.;

– közfeladatot ellátó szervnek minősül a Magyar Televízió Rt., mivel közszolgálati műsorszolgáltatóként jogszabályban – az 1996. évi I. törvényben – meghatározott közfeladatot lát el;[289]

– közfeladatot lát el az Állami Privatizációs és Vagyonkezelő Rt.[290]

Közérdekű adat az Országgyűlés bizottságainak ülésén készült jegyzőkönyv is.[291]

Nem közfeladatot ellátó szerv a szakszervezet, mivel nem rendelkezik közhatalmi jogosítványokkal és nem kezel költségvetési pénzeket.[292] Nem tartozik az alanyi körbe a kereskedelmi bank, akkor sem, ha az adófizetők pénzéből konszolidálták, mivel nem lát el állami vagy helyi önkormányzati, illetőleg jogszabályban meghatározott egyéb közfeladatot.[293] Nem tekinthető közfeladatot ellátó szervnek a Tartalékgazdálkodási Közhasznú Társaság; azonban a rá vonatkozó, igényelt adatkört az adatigénylő tulajdonosi

[287] Lásd a 1409/A/2004. ügyet. (Az esetre Bárfai Zsolt hívta fel a figyelmemet.)

[288] ABI 2000, 356.

[289] ABI 1998, 135; ABI 2000, 120; ABI 2000, 374.

[290] ABI 1999, 141.

[291] ABI 2000, 358.

[292] ABI 1999, 129.

[293] ABI 2000, 119; ABI 2000, 367.

jogokat gyakorló minisztériumtól és Kincstári Vagyoni Igazgatóságtól mint közérdekű adatokat kérheti.[294]

Az adatvédelmi biztosi gyakorlat szerint lehetséges az is, hogy valamely szerv csak meghatározott feladatok tekintetében minősül közfeladatot ellátó szervnek, s így a kezelésében lévő adatok csak e körben minősülnek közérdekű adatnak.[295]

2. Az adatvédelmi biztosi gyakorlat is alátámasztja azt, hogy a közfeladatot ellátó szerv vagy személy csak a *rendelkezésére álló* adatot köteles szolgáltatni, nem kötelezhető adat előállítására.

A biztos szerint az, hogy mi az MTV Rt. adóssága kialakulásának oka, illetőleg az MTV Rt. tesz-e különbséget hitelezői, illetőleg azok csoportjai között a kifizetések határidejében, csak akkor lehet közérdekű adat iránti kérelem tárgya, ha az MTV Rt. birtokában erre vonatkozó „irat" van.[296]

3. Az utóbbi idők adatvédelmi gyakorlatában merült fel az az értelmezési kérdés, hogy a közérdekű adat meghatározásában szereplő két, közérdekű adatkénti minősüléshez szükséges feltétel (amely szerint közérdekű adat a „szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó" adat) között „és" vagy „vagy" reláció áll fenn. Az adatvédelmi biztos szakirodalomban kifejtett nézete szerint: „Zavaró, hogy »a kezelésében lévő, tevékenységére vonatkozó« adatokról többen azt hiszik, hogy amely adat a közfeladatot ellátó szerv kezelésében, birtokában van, az közérdekűvé válik, legfeljebb csak nem nyilvános. Az én álláspontom szerint ezek az adatok nem válnak közérdekű adattá pusztán azért, mert közfeladatot ellátó szerv döntési kompetenciájába kerülnek. Az e szervek tevékenységére vonatkozó adatok közérdekűek, tehát az, hogy milyen ügyeket látnak el, mennyi ügyet, de az egyes ügyek tartalma nem."[297] Ennek nyomán az újabb keletű adatvédelmi biztosi értelmezés szerint nem minősül közérdekű adatnak az egyes hatósági döntések (azok személyes adatokon kívüli) tartalma, a jogszabályok szövege stb.[298]

---

[294] ABI 2000, 365.

[295] Lásd a 1409/A/2004. ügyben kifejtett értelmezést: „Tipikus példák […] az alapítványok, egyházak által fenntartott közoktatási és egészségügyi intézmények, amelyek az állammal, önkormányzattal kötött szerződés keretében látják el az állami, önkormányzati feladatokat. E magánszervezetek azonban csak az ellátott közfeladat tekintetében minősülnek közfeladatot ellátó szervnek, nem pedig egész tevékenységük tekintetében."

[296] ABI 2000, 383. A „kezelésében lévő" fordulat értelmezésére lásd még ABI 1999, 134.

[297] Szabó Máté 2004c, 43.

[298] Szabó Máté 2004c, 42–43.

Hasonló az adatvédelmi biztosi gyakorlatban újabban megjelent azon értelmezés, amely szerint: „A jogi személyek, jogi személyiség nélküli szervezetek adatai nem válnak […] közérdekű adattá pusztán amiatt, mert bekerülnek egy közfeladatot ellátó szerv kezelésébe. Közfeladatot ellátó szervnek, személynek nem minősülő természetes személyre, jogi személyre, illetve jogi személyiség nélküli szervezetre vonatkozóan törvénynek kell kimondania valamely adat nyilvánosságát, megjelölve a nyilvánosságra hozandó adatkört is."[299] Ezen az értelmezésen alapulnak azok az állásfoglalások, amelyek szerint valamely üzleti titoknak minősülő adat – hiába van közfeladatot ellátó szerv kezelésében, és hiába nem minősül személyes adatnak – nem közérdekű adat.[300]

Ez az értelmezés a közérdekű adat fogalmát a „közérdekből nyilvános adat" fogalmára tekintettel kívánja szűkíteni. A szűkítés csak abban az esetben fogadható el, ha a közérdekű adat fogalmában a fenti két feltétel között „és" relációt tételezünk fel; az interpretáció szerint a közérdekű adat tevékenységére vonatkozó és kezelésében lévő (személyes adatnak nem minősülő) adatok közérdekű adatok, míg a szerv kezelésében lévő további adatok nem ilyenek, hanem azok lehetnek közérdekből nyilvános adatok (illetőleg a nyilvánosság törvényi elrendelése esetén e körbe sem tartozó, egyéb adatok).

Ez az interpretáció álláspontunk szerint több okból sem helytálló. A közérdekű adat fogalmának meghatározása a törvényben több alkalommal változott; az eredeti szövegezés szerint „közérdekű adat: az állami vagy helyi önkormányzati feladatot ellátó szerv kezelésében lévő, a személyes adat fogalma alá nem eső és a törvényben meghatározott kivételek körébe nem tartozó adat"; később, egy 1995-ben hatályba lépett módosítás nyomán „az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat". Ezekkel a meghatározásokkal a jogalkotó a közérdekű adatkénti minősülést egyértelműen ahhoz kötötte, hogy az adat meghatározott szervek birtokában van. Ha ez megállapítható, akkor az adat – az 1995-ös módosítás nyomán – csak akkor nem közérdekű, ha személyes adat, minden egyéb esetben közérdekű adatnak minősül, még akkor is, ha a nyilvánosságát törvény korlátozza (például üzleti titkok esetében).[301]

2003 júniusában lépett hatályba az az újabb módosítás, amely alapján közérdekű adat „az állami vagy a helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb

[299] ABI 2005, 542; ABI 2005, 546; ABI 2005, ABI 2005, 574.

[300] ABI 2005, 531

[301] Lásd például ABI 1999, 139; ám a megváltozott gyakorlatra lásd például a 1122/A/2004. ügyet: „Az üzleti titok maga nem közérdekű adat, de nem is jelenti a közérdekű adatok megismerésének abszolút korlátját."

közfeladatot ellátó szerv, illetve személy kezelésében lévő (ideértve a tevékenységére vonatkozó adatot is), a személyes adat fogalma alá nem eső adat" A szövegezés szerencsétlen, ám nem a közérdekű adat fogalmának szűkítésére (ti. annak a szerv tevékenységére vonatkozó adatok körére történő korlátozására) irányuló jogalkotói szándékra utal, hanem ellenkezőleg: arra, hogy a jogalkotó meghatározott adatokat (amelyek a szerv tevékenységére vonatkoznak) attól függetlenül kívánt közérdekű adatként minősíteni, hogy azok mely szerv vagy személy birtokában vannak. Ezt a meghatározást váltotta fel az Avtv.-novella által meghatározott – és a 2005. évi XIX. törvény által kiegészített - hatályos szöveg.

Kiemelendő azonban, hogy az adatvédelmi biztosi gyakorlatban a közelmúltban teret nyert ez az értelmezés: egy újabb állásfoglalás szerint például nem minősül közérdekű adatnak az – állami feladatot ellátó – Országos Atomenergia Hivatal kezelésében lévő, harmadik személytől származó üzleti titok. „Az üzleti titok maga nem közérdekű adat, de nem is jelenti a közérdekű adatok megismerésének abszolút korlátját".[302] Azonban az új értelmezés mellett tovább él a korai adatvédelmi biztosi gyakorlat is, amely szerint – a személyes adatok kivételével – bármely, a közfeladatot ellátó szerv kezelésében lévő adat közérdekű adat (amelynek nyilvánosságát azonban egyéb jogszabály korlátozhatja, pl. üzleti titkok esetén): „Az a tény, hogy egy adatfajta közérdekű adatnak minősül, nem jelenti egyúttal azt is, hogy nyilvános. Amennyiben ugyanis [...] üzleti titoknak minősül, úgy nyilvánossága korlátozott, illetőleg korlátozható".[303]

4. A korai adatvédelmi biztosi gyakorlat azon alapul, hogy *a személyes adatok védelméhez való jog és a közérdekű adatok nyilvánossága* közötti hierarchiát „esetről esetre lehet megállapítani", meghatározott esetekben az Avtv. és más, személyes adatkezelést szabályozó jogszabályok megtartását ellenőrző biztos által is kimondható (személyes

[302] ABI 2005, 531. A korai gyakorlat szerint a hasonló adatok olyan közérdekű adatnak minősültek, amelyek nyilvánosságát törvény korlátozza.

[303] ABI 2005, 515. Ez a kérdés összefüggésben áll a személyes adatok védelmének terjedelmének problémájával is. A korai értelmezés a nyilvánosság főszabálya mellett törvényi kivételt kíván meg annak korlátozásához. Az új értelmezés kiindulópontja ellentétes : annak elfogadása esetén jogi személyek (jogi személyiség nélküli szervezetek) adatai főszabály szerint – a személyes adatokhoz hasonlóan – titkosak, s azt előíró törvényi szabályozás esetén minősülhetnek nyilvánosnak. A új értelmezés alátámasztható a személyes adatokkal kapcsolatos védelem jogi személyekre történő kiterjedésével kapcsolatos alkotmánybírósági határozatokkal (lásd a 2. § 1. bekezdéséhez fűzött magyarázatot), s annak hívei a „közérdekből nyilvános adat" fogalma mögött húzódó jogalkotó szándékot is úgy ítélik meg – álláspontunk szerint tévesen -, mint amely ezen személyek adatainak védelmét kívánja erősíteni.

adatokról), hogy „az adatok közérdekűsége élvez elsőbbséget”.[304] E körbe tartoznak azok az állásfoglalások, amelyek szerint: „Az önkormányzati képviselők említett adatai [bérek, juttatások, különböző önkormányzati tulajdonú társaságban betöltött tisztségek és az ezért kapott díjazás] közérdekű adatnak minősülnek; magánszférájuk másokénál szűkebb”;[305] a kutatóintézetek vezetőinek nevére irányuló adatkérés közérdekű adatkérésnek minősül;[306] vagy amely szerint „[a]z Avtv. ezzel összhangban kimondja, hogy »a közfeladatot ellátó szerv hatáskörében eljáró személyek neve és beosztása közérdekű adat«”[307] (az Avtv. e rendelkezést soha nem tartalmazta, az idézett szabály szerint ez az adatkör „bárki számára hozzáférhető, nyilvános adat”); „meghatározott személyi kör esetében az egyébként személyesnek minősülő adatok közérdekűvé tétele elengedhetetlen demokratikus követelmény”[308], és „a Magyar Televízió elnökének fizetése feltétlenül beletartozik ebbe a körbe”,[309] „a képviselők hiányzása a plenáris és bizottsági ülésekről közérdekű adat”,[310] az önkormányzat által bérbe adott mezőgazdasági ingatlan bérlőjének személye közérdekű adat[311] stb. E korai állásfoglalások jellemzője az, hogy személyes adatokat nyilvánítanak – conta legem – közérdekű adatokká.[312] Később a gyakorlat változott: a fordulat éve 1999 volt, ekkor született meg egy kereskedelmi bank VIP-hitelben részesült ügyfeleinek listájával kapcsolatban az az állásfoglalás, amely szerint: „Törvényi felhatalmazás alapján a közhatalmat gyakorlók vagy politikai közszereplést vállalók azon személyes adatai, amelyek köztevékenységük és annak megítélése szempontjából jelentősek lehetnek, nyilvánosságra kerülhetnek, ilyenkor ezek a személyes

[304] ABI 1999, 358. Az adatvédelmi biztos természetesen értelmezheti ajánlásaiban, állásfoglalásaiban az Alkotmányt, ám éppen a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához fűződő jog konfliktusai során nem tekinthet el a két alkotmányos jog gyakorlásának kereteit meghatározó Avtv. rendelkezéseitől. (Lásd Sólyom 2001b, 86.)

[305] ABI 1997, 62; hasonlóan ABI 1998, 127; ABI 1999, 68.

[306] ABI 1997, 69.

[307] ABI 1997, 95.

[308] ABI 1997, 257.

[309] ABI 1997, 259, hasonlóan és a Magyar Rádió elnökének fizetésére is ABI 1998, 135.

[310] ABI 1998, 134; ABI 1998, 339.

[311] ABI 1999, 133.

[312] Az ezen esetekben követett gyakorlat felfogható úgy is, hogy a biztos közvetlenül az Alkotmány értelmezésével állapította meg a személyes adatok védelme és a közérdekű adatok megismerhetősége között adott tényállás esetén fennálló viszonyt. Ilyen alkotmányértelmezésre azonban – épp az Avtv. e kérdést illető részletes szabályozására tekintettel – a biztosnak nincs lehetősége; Alkotmányt akkor értelmezhet, ha „az ügyben két alapjog ütközését kell megoldani (s ez kívül esik a személyes adat/közérdekű adat elhatárolásán)” – Sólyom 2001b, 86.

adatok a közérdekű adatokéhoz hasonló jogi elbírálás alá esnek."[313] Innentől fogva a biztosi állásfoglalások töretlenül tükrözik az álláspontunk szerint helyes értelmezést: a biztos az országgyűlési képviselők javadalmazását személyes adatként értelmezi, és úgy foglal állást, hogy az Avtv. akkor hatályos 3. § (3) bekezdése alapján a parlament törvényben rendelheti el ezek nyilvánosságra hozatalát:[314] „Ez az elv [az Avtv. 19. § (4) bekezdésében foglalt szabály] megkívánja azt, hogy a jegyző (tisztviselő) illetményének megismerése valamilyen közérdekű adat megismerésével kapcsolatban váljék szükségessé. Ezek az adatok nem közérdekű adatok, személyes adat mivoltuk továbbra is fennáll, csak annak védelme szűkül le adott esetben egy másik alkotmányos követelmény – a közérdekű adatok megismerhetősége – tekintetében";[315] az MTV vezető beosztású munkatársainak javadalmazása akkor közérdekű adat, ha nem minősül személyes adatnak, azaz közérdekű adat „egy meghatározott vezetői kör javadalmazására fordított összeg", illetőleg az MTV állományába tartozó, de huzamosabb ideig munkát nem végző alkalmazottak száma és a számukra kifizetett bér összege;[316] stb.

A közérdekből nyilvános adat fogalmának az Avtv.-be történő bevezetése nyomán a törvény által nyilvánosnak minősített személyes adatok egyben közérdekből nyilvános adatnak is minősülnek, ám ennek a jelenlegi szabályozás szerint semmilyen következménye nincs.

5. Az *adat* fogalmát az adatvédelmi biztosi gyakorlat a személyes adat fogalmához hasonlóan széles módon interpretálja. A biztos szerint:

– közérdekű adat az ORTT által nyilvántartott rádiók, televízió postacíme, telefonszáma;[317]

– közérdekű adat a vállalkozások jogszerű működésének ellenőrzésére hivatott hatóságok elmarasztaló határozata (különösen a környezetvédelem területén);[318]

– a nyilvános képviselő-testületi ülésen kép- és hangfelvétel készítésére irányuló kérelem közérdekű adat iránti kérelemnek minősül;[319]

– MTV Rt. által a beszállítóknak egy év alatt összesen kifizetett késedelmi kamat összege, hasonlóan az MTV Rt. „adósságának szerkezete".[320]

---

[313] ABI 2000, 127.

[314] ABI 1998, 355.

[315] ABI 1999, 131.

[316] ABI 2000, 121.

[317] ABI 1998, 135.

[318] ABI 1998, 137.

[319] ABI 1998, 130.

Igen lényeges, hogy a korai adatvédelmi biztosi gyakorlattal ellentétben egyes közelmúltbeli állásfoglalásokban az „adat" fogalmának megszorító értelmezése nyert teret. Az adatvédelmi biztos nyilatkozatban is megerősítette: „a jogszabályok szövege, tehát maga a kihirdetett jogszabály nem fogható fel közérdekű adatként"[321]. A 2005. évi XIX. törvény által bevezetett új szövegezés („bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől") a szűkíti hasonló jogalkalmazói jogértelmezések lehetőségét.

1.9.9. A bíróságok gyakorlata a közérdekű adatok vonatkozásában

A közérdekű adatok megismerésével kapcsolatos szabályokkal kapcsolatos bírósági gyakorlatra lásd alább a 19. és következő §-okhoz fűzött magyarázatot. A közérdekű adat fogalmának értelmezésével kapcsolatos fejlemény, hogy 2005 januárjában egy elsőfokú bíróság úgy foglalt állást, hogy nem minősül adatnak a közfeladatot ellátó szervhez – adott esetben az Alkotmánybírósághoz – benyújtott, jogi érvelést tartalmazó indítvány.[322] Az ügyben szintén az „adat" fogalma volt értelmezés tárgya, vagyis a lehetséges, hogy a bíróság a 2005. évi XIX. törvény által módosított meghatározás alapján más következtetésre jutott volna.

1.9.10. A közérdekből nyilvános adat

1. Az Avtv. 2. § 5. pontjában foglalt meghatározás szerint „*közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli". A közérdekből nyilvános adat fogalmát a 2003. évi novella vezette be a törvénybe, majd a 2005. évi XIX. törvény rövid idő múlva módosította. A novella vonatkozó szakaszának miniszteri indokolása szerint: „A közérdekből nyilvános adat fogalmának bevezetésével egyértelműen el lehet határolni a közszféra főszabályként és természeténél fogva nyilvános adatait és a magánszféra kivételesen, valamely, az adatok bizalmas kezelésénél fontosabb közérdekből nyilvánossá tett adatainak kezelését, megszüntetve ezzel egy, a megfelelő jogérvényesítést akadályozó

[320] ABI 2000, 383.

[321] Szabó Máté 2004c, 42.

[322] Az üggyel kapcsolatos dokumentumokat lásd a felperes Társaság a Szabadságjogokért weboldalán: http://www.tasz.hu/index.php?op=contentlist2&catalog_id=1528.

gyakorlati problémát. Közérdekből nyilvános adat például a magánszemélyek vagy szervezetek közpénzek felhasználásával kapcsolatos adata vagy a gazdasági tevékenységükkel kapcsolatos környezetvédelmi adatok, de e körbe tartozik a közszereplő személyek nyilvánosság számára megismerhető személyes adata is."

A 2003. évi novellával módosított törvényszövegben a kategóriát a jogalkotó a továbbiakban nem használta (nem határozott olyan meg jogokat, kötelezettségeket, amelyek a csak a közérdekből nyilvános adatok körére vonatkoznak), a 2005. évi XIX. törvény által bevezetett módosítások azonban már építenek az új fogalomra. Az Avtv. módosított szövege egyes – személyes és nem személyes – adatokat közérdekű adatnak minősít (19. § (4)-(5) bekezdése), és az adatkör megjelenik az adatvédelmi biztos feladat- és jogköreinek szabályozásában is (25. § (1) bekezdés, 26. § (1) bekezdés).

Közérdekből nyilvános adat a meghatározás szerint nem lehet közérdekű adat. A jogalkotó olyan kategóriát határozott meg, amely magában foglal minden adatot, amely nyilvánosságát (hozzáférhetőségét) törvény elrendeli (beleértve a személyes adatoka), kivéve azokat, amelyek a 2. § 4. pontjában adott meghatározás alá esnek. Más megfogalmazásban azokról az adatokról van szó, amelyek

a) nem állami vagy helyi önkormányzati, vagy jogszabályban meghatározott egyéb közfeladatot ellátó szerv kezelésében vannak vagy nem ilyen szervek tevékenységére vonatkoznak, de törvény nyilvánosságra hozatalukat vagy hozzáférhetővé tételüket közérdekből elrendeli (pl. Avtv. 19. § (4) bekezdése);

b) személyes adatok, amelyek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli (pl. Avtv. 19. § (5) bekezdése).

Álláspontunk szerint a 2005. évi XIX. törvény által bevezetett módosítások nyomán sem világos a „közérdekből nyilvános adat" fogalmának helye az Avtv. rendszerében. [323] Mindamellett az újabb keletű adatvédelmi biztosi gyakorlatban a fogalom egyre nagyobb szerepet kap (lásd alább).

[323] A helyzet hasonló, mint az „adatfeldolgozás" fogalmánál: ott a törvény fogalomrendszerében idegen kategória jogalkalmazói értelmezése úgy hatott vissza a jogalkotásra, hogy az adatfeldolgozás kereteit feleslegesen szűkítő szabályozás született; a „közérdekből nyilvános adat" hasonlóan véggigondolatlan bevezetése pedig láthatóan a közérdekű adatok nyilvánosságára vonatkozó szabályok megszorító jogalkalmazói értelmezése előtt nyitotta meg a teret.

1.9.11. Az adatvédelmi biztos közérdekből nyilvános adatokra vonatkozó gyakorlata

Az adatvédelmi biztosi gyakorlatban a „közérdekből nyilvános adat" fogalmának bevezetése nyomán nyert teret az a jogértelmezés, amely szerint: „A jogi személyek, jogi személyiség nélküli szervezetek adatai nem válnak […] közérdekű adattá pusztán amiatt, mert bekerülnek egy közfeladatot ellátó szerv kezelésébe. Közfeladatot ellátó szervnek, személynek nem minősülő természetes személyre, jogi személyre, illetve jogi személyiség nélküli szervezetre vonatkozóan törvénynek kell kimondania valamely adat nyilvánosságát, megjelölve a nyilvánosságra hozandó adatkört is."[324]

Ez az értelmezés szakít azzal a korábbi joggyakorlattal, amely szerint a közfeladatot ellátó szervek kezelésében lévő összes adat – a személyes adatok kivételével – közérdekű adat. Az interpretáció nem támasztható alá az Avtv. 2. § 4. és 5. pontjában rögzített fogalmakkal: a törvény a közérdekből nyilvános adatok köréből kizárja a 4. pontban meghatározott közérdekű adatkört, tehát minden olyan adatot, amely a közfeladatot ellátó szerv kezelésében van, illetőleg annak tevékenységére vonatkozik.

Megjegyzendő, hogy a fenti gyakorlat kibontakozásával párhuzamosan a biztos egyes esetekben továbbra is a korábbi interpretációra építi állásfoglalásait: pl. az MTI Rt. mint közfeladatot ellátó szerv „kezelésében lévő valamennyi nem személyes adat közérdekű adatnak minősül"[325].

Nézetünk szerint nem helytálló az, hogy valamely – nem személyes – adat „nem válik közérdekűvé" amiatt, hogy a közfeladatot ellátó szerv kezelésébe kerül; hiszen az ilyen adat közérdekű adatkénti minősülése közvetlenül következik a közérdekű adat fogalmának 2. § 4. alatti meghatározásából.

1.9.12. Az Alkotmánybíróság vonatkozó gyakorlata

A közérdekből nyilvános adat fogalma immár az Alkotmánybíróság gyakorlatában is megjelenik. A 26/2004. (VII. 7.) AB határozat indokolása egyes, az állami adóhatóság kezelésében lévő adatokat említ közérdekből nyilvános adatként (tekintet nélkül arra, hogy ezek az adatok az Avtv. meghatározása szerint nyilvánvalóan közérdekű adatok, vagyis nem

[324] ABI 2005, 542; ABI 2005, 546; ABI 2005, 574

[325] ABI 2005, 145 és ABI 2005, 294

lehetnek közérdekből nyilvános adatok). A 44/2004. (XI. 23.) AB határozat indokolása szerint: „A személyes adat nyilvánosságra hozatalát a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 3. § (4) bekezdése szerint törvény közérdekből elrendelheti. Ekkor a személyes adat közérdekből nyilvános adattá válik és a »közérdekű adatokéhoz hasonló jogi elbírálás alá esik, amelynek a szabályait az adatvédelmi törvény III. fejezete tartalmazza«"[326]

1.10. Adatkezelő, adatfeldolgozó, adatkezelés, adatfeldolgozás, valamint e fogalmak kapcsolata

1.10.1. Az adatkezelő

1. Az Avtv. 2. § 8. pontja szerint „adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja". Az adatkezelő az adatvédelmi normák elsődleges címzettje, az az alany, aki az adatkezelésért (és az esetleg azzal okozott kárért) felel (az adatkezelő elnevezése németül: *für die Verarbeitung Verantwortlicher,* angolul: *data controller*). Az adatkezelés folyamata az ő ellenőrzése alatt folyik.

Az adatkezelő természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet lehet. Nem lehet adatkezelő például polgári jogi társaság (Ptk. 568. §), családi gazdaság [326/2001. (XII. 30.) Korm. rendelet]. Adatkezelő lehet maga az adatalany is (például abban az esetben, ha nem saját személyes céljaira szolgáló olyan adatbázist épít, amelyben saját személyes adata is szerepel).[327]

Az adatkezelő

[326] Az értelmezés ezen útján elindulva megkérdőjelezhető az Avtv. alapelveinek érvényessége a személyes adatok meghatározott – nyilvános – körére. Ha – miként az mind az Alkotmánybíróság, mind az adatvédelmi biztos gyakorlata szerint fennáll – a közérdekű adatokra nem alkalmazható pl. a célhozkötöttség elve, akkor e tekintetben mit jelent az, hogy a közérdekből nyilvánosságra hozott személyes adatok „a közérdekű adatokéhoz hasonló" jogi elbírálás alá esnek? Következhet-e ebből pl. a célhozkötöttség elvének feladása a nyilvános személyes adatok kezelésének vonatkozásában? Az adatkezelés elveinek érvényesíthetősége a nyilvánosság közegében valós probléma – lásd erről az 5. §-hoz fűzött magyarázatot.

[327] Ellenkezően Szabó Máté 2003.

– meghatározza az adatkezelés célját,

– meghozza az adatkezelésre vonatkozó döntéseket,

– végrehajtja vagy végrehajtatja az adatkezelésre vonatkozó döntéseket.

2. Az *„adatkezeléssel kapcsolatos döntéssel”* kapcsolatban ki kell emelni az alábbiakat:

Az irányelv nem követeli meg azt, hogy az adatkezelő bármilyen „döntést” hozzon az adatkezelés folyamatában, csupán azt, hogy – a cél mellett – meghatározza annak a *módját*.[328] Álláspontunk szerint ez nem jelenti azt, hogy az adatkezelő korlátozott körben ne delegálhatna az adatkezeléssel (illetőleg feldolgozással – a fogalmak kapcsolatáról lásd alább) kapcsolatos döntéseket az adatfeldolgozóra, ez egyes tagállami jogokban megengedett [ám lásd az irányelv 17. cikk (3) bekezdéséből eredő korlátokat].[329] A magyar jogalkotó azonban kizárta, hogy az adatfeldolgozó „adatkezelésekre vonatkozó döntéseket” hozzon: ebben az esetben már adatkezelőnek minősül.

További vizsgálatot igényel azonban az „adatkezelésre vonatkozó döntés” fogalma. Adatkezelésre vonatkozik a meghatározott adatkezelési művelet végzéséről (például személyes adatok törléséről, továbbításáról) hozott döntés, ám az a döntés is, amely a továbbítás megkezdéséről szól (például online kapcsolat létesítése, a „küldés” billentyű megnyomása stb.). Álláspontunk szerint a jogalkotó csak az előbbi (érdemi) döntések delegálásának lehetőségét kívánta kizárni, az utóbbi döntések nyilvánvalóan az adatfeldolgozás folyamatába illeszkednek, adatfeldolgozó igénybevétele esetén elkerülhetetlen, hogy azokat ő hozza meg.

3. További értelmezési kérdést jelent, hogy *szervezet nevében eljáró természetes személy* esetében miképpen határozható meg az adatkezelő személye. Ha az adatkezelő nem magánszemély, akkor szükségszerű, hogy az adatkezelési műveleteket (a cél meghatározását, a döntések meghozatalát) a jogi személy vagy a jogi személyiség nélküli szervezet nevében természetes személy végzi. A gyakorlatban is felvetődik az a kérdés, hogy ilyen esetben minősülhet-e, és ha igen, mely feltételek bekövetkezése esetén adatkezelőnek a természetes személy.

---

[328] A német szövegben: „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet”, az angol szövegben „determines the purposes and means of the processing of personal data”.

[329] „Az adatkezelőnek nem kell minden esetben gyakorolnia (ezt az adatkezelés módjának meghatározásához fűződő) jogosítványát, és a lehetőségek bizonyos skálájának keretei között delegálhatja azt az adatfeldolgozó részére – ám az adatkezelő az a személy, akinek a hatalmában áll meghozni a végső döntést a tekintetben, hogy az adatokat például visszatartsák vagy hozzáférhetővé tegyék.” Jay–Hamilton 1999, 35.

Az egyik értelmezés szerint – amely az adatvédelmi biztos által megfogalmazott „egy adatkezelés – egy adatkezelő" szabályból is következik – az adatkezelő minden esetben *egy* alany. Ha tehát például a biztosítótársaság jogtanácsosa a követelésérvényesítésre vonatkozó belső szabályok szerint keresetet nyújt be a társaság nevében a polgári bíróságon (vagyis személyes adatot továbbít), akkor az adatkezelő a biztosítótársaság, amelynek belső szabályai meghatározzák az adatkezelési célt és rögzítik az adatkezeléssel kapcsolatos döntési algoritmust. Abban az esetben, ha a jogtanácsos a társaság adatbázisát lemásolja és jogszerűtlen módon továbbítja egy konkurens cégnek, kizárólag ő az adatkezelő, ám már egy másik adatkezelés vonatkozásában.

A másik értelmezés szerint lehetséges az, hogy a szervezet és a nevében eljáró személy egyszerre minősüljön adatkezelőnek ugyanazon adatkezelés vonatkozásában.[330] Ennek hiányában ugyanis azon jogszerűtlen adatkezelések esetében, amelyek vonatkozásában az adatkezelő nem természetes személy, csak korlátozottan érvényesül a büntetőjogi fenyegetés (lásd alább).

Álláspontunk szerint az első értelmezés a helyes, azzal a kiegészítéssel, hogy – az adatvédelmi biztosi értelmezéstől eltérően – lehetségesnek tartjuk az adatkezelői minőség párhuzamos megállapítását (az irányelvvel összhangban) abban az esetben, ha a szervezet és a természetes személy közösen határozzák meg az adatkezelési célt, illetőleg hozzák meg a döntéseket az adatkezelés vonatkozásában (például üzleti együttműködés stb. keretében). A felvetett esetben azonban – amelyben a természetes személy a szervezet nevében jár el – nem ez a helyzet: az adatkezelés célját és az arra vonatkozó döntéseket maga a szervezet határozza meg (amelynek nevében természetesen mindenkor természetes személyek járnak el), az adatkezelő tehát egyedül a szervezet. A természetes személy ilyen helyzetben tipikusan akkor válik adatkezelővé, amikor a szervezet nevében történő adatkezeléssel együttjáró jogosítványokat felhasználva az eredeti céltól eltérő, jogszerűtlen adatkezelésbe kezd: ezen új, általa kontrollált adatkezelés vonatkozásában már természetesen ő az adatkezelő.[331] Ezt az értelmezést támasztja alá az irányelvre vonatkozó nemzetközi szakirodalom is,[332] és ez áll

[330] Lásd erre Szabó Máté 2003.

[331] Például a rendőr, aki a beosztásából eredően számára nyújtott adatbázis-hozzáféréssel visszaélve jogosulatlanul továbbít személyes adatokat: BH 2000/384.

[332] Dammann–Simitis 1997, 112: „Ha az adatkezelés valamely kft., rt. vagy más jogi személy üzleti tevékenységéhez tartozik, akkor ez az adatkezelő, mert a cégvezető, a vezető tisztségviselők és a munkatársak az adatkezelés céljáról és módjáról nem a maguk nevében, hanem a jogi személy megbízásából és arra kihatással döntenek."

összhangban a „harmadik személy” fogalmának az Avtv.-ben szereplő meghatározásával (lásd a 2. § 19. pontjához fűzött kommentárt).

A fentiekből az is következik, hogy ha a természetes személy a szervezet mint adatkezelő nevében jár el (tehát nem együttműködve határozzák meg a célt és hozzák meg a vonatkozó döntéseket, hanem adatkezelőnek kizárólag a szervezet minősül), akkor az esetleges jogosulatlan adatkezelés esetén a büntetőjogi szankció álláspontunk szerint nem alkalmazható, mivel a magyar jogban a jogi személy büntetőjogi felelőssége származékos, vagyis a jogi személlyel szemben büntetőjogi intézkedés alkalmazásának csak akkor lenne helye, ha van olyan természetes személy, akivel szemben a büntetőeljárás lefolytatható[333] – más volna a helyzet, ha a magyar szabályozás elismerné a jogi személy önálló büntetőjogi jogalanyiságát. Ilyen körülmények között nem tartjuk kizártnak, hogy a hasonló esettel szembesülő bíróság meg fogja állapítani a vezető tisztségviselő, tag, alkalmazott stb. büntetőjogi felelősségét (holott az álláspontunk szerint nem végez adatkezelést), és ehhez kapcsolódóan a jogi személlyel szemben intézkedést alkalmaz.

4. További, az adatkezelő fogalmával kapcsolatban a gyakorlatban felmerült kérdés, hogy lehetséges-e *egy adatkezelés vonatkozásában több adatkezelő* párhuzamos tevékenysége. Erre a problémára a következő pontban visszatérünk.

5. A 2005. évi XIX. törvény úgy módosította a meghatározást, hogy az adatkezelő fogalma már nem csak személyes adatok, hanem általában bármely „adat” vonatkozásában értelmezhető. A meghatározás ilyen értelmezésével kapcsolatos jogalkalmazói gyakorlat egyelőre nincs. Az „adatkezelő” fogalom fő elemei (az adatkezelés céljának meghatározása, döntések meghozatala) a személyes adatok védelmének körében értelmezhetők. Bár az Avtv. III. fejezetében szereplő normák címzettjei egyes esetekben a 19. § (1) bekezdésében meghatározott szervek, a törvény más esetelben használja az „adatkezelő szerv”, „adatot kezelő szerv” fogalmat (20. § (3) bekezdés, 21. § (7) bekezdés, stb.), és az szerepet kaphat a közérdekből nyilvános adatok kezelése során is. A meghatározás nyomán lehetséges olyan jogalkalmazói gyakorlat, amely a korábbihoz képest szűkíti a III. fejezetben szabályozott tájékoztatási kötelezettség körét, annak alanyaként kizárólag azt a szervet meghatározva,

[333] Lásd a 2001. évi CIV. törvényt. A kivételek e gondolatmenet szempontjából nem relevánsak. Kiutat jelenthet a törvény 2. § (2) bekezdése, amely szerint az „[…] e törvényben meghatározott intézkedések alkalmazhatók akkor is, ha a bűncselekmény elkövetése a jogi személy javára vagyoni előny szerzését eredményezte, és a jogi személy ügyvezetésre vagy képviseletre feljogosított tagja vagy tisztségviselője a bűncselekmény elkövetéséről tudott” – ám a jogalkotói cél e rendelkezéssel azon eseteknek a szabályozás hatálya alá vonása volt, amelyekben a bűncselekményt a szervezettel kapcsolatban nem álló természetes személy valósítja meg.

amely a szóban forgó közérdekű (esetleg közérdekből nyilvános) adat „gazdája” (az adatkezelés célját, az adatkezelés módját meghatározza).

1.10.2. Az adatvédelmi biztos gyakorlata az adatkezelő fogalmának értelmezésével kapcsolatban

1. Az *adatkezeléssel kapcsolatos döntés* mibenlétével kapcsolatban kiemelendő az az állásfoglalás, amelyben a biztos egy esetben idesorolta azt a döntést, amelyet a követeléskezelő társaság hoz, amikor az adós részére – a megbízójával kötött szerződésben meghatározott esetben – részletfizetést kínál fel.[334] Az állásfoglalás nézetünk szerint téves: nem adatkezelésre vonatkozó, hanem – az ajánlás szövegezése szerint is – az adatokra „támaszkodó” döntésekről van szó; érdemi adatkezelésre vonatkozó döntéseket az adott esetben a követeléskezelő társaság nem hozott.[335]

Érdekes megkülönböztetést tesz a biztos az internet közegében történt két adatkezelés adatkezelői között: míg az internetes fórumon közölt személyes adat esetén a közlő az adatkezelő, mert „Azon információhalmaz, mely egy fórumon elhangzó vélemények szintézisével áll elő, adatkezelők sokaságára esik szét, hisz minden egyes személyes adatot tartalmazó hozzászólás önálló adatkezelésnek […] minősül”, addig személyes adatok rendezett, adatbázisba szervezett, honlapon történő közzétételénél a honlap üzemeltetője az adatkezelő[336].

2. A *szervezet nevében eljáró természetes személy* adatkezelői minőségével kapcsolatos az az állásfoglalás, amely szerint a társaság igazgatósági, illetőleg felügyelőbizottsági (fb) tagját önálló adatkezelőnek minősíti abban az esetben, ha az a társasággal megbízási jogviszonyban áll, míg a társaság adatkezelői minőségét állapítja meg abban az esetben, ha a cég és az fb-tag között munkajogviszony van.[337] Nézetünk szerint az állásfoglalás téves: a döntő az, hogy a szóban forgó adatkezelés célját, illetőleg az arra vonatkozó döntéseket a fentiek szerint ki határozza meg: ez az alany az adatkezelő, függetlenül a jogviszony jellegétől.

3. Az adatvédelmi biztosi gyakorlatban az adatvédelmi nyilvántartásba történő bejelentés értelmezése körében jelent meg az a gondolat, amely szerint *meghatározott adatkezeléshez minden esetben egy adatkezelő kapcsolható.* „Több önállóan bejegyzett cég

[334] ABI 2001, 200.

[335] Részletesebben lásd alább a 2. § 15. pontjához fűzött magyarázatot.

[336] ABI 2005, 399

[337] ABI 2000, 94.

nem használhat közös adatbázist, több […] cég közös akciója esetén az adatok felelős kezelőjét egyértelműen meg kell határozni."[338] „Az Avtv. alapelvei kimondják, hogy bár egy adatkezelő természetesen több adatkezeléssel is rendelkezhet, egy adatkezelésnek csak egy felelős adatkezelője lehet".[339] Nézetünk szerint ez az álláspont téves. Az Avtv. nyelvtani értelmezése nem vezet ilyen eredményre, az irányelv vonatkozó szabálya pedig kifejezetten utal az együttes adatkezelés lehetőségére.[340] A gyakorlatban ráadásul működnek olyan adatbázisok, ahol több adatkezelő is hozzáférhet az adatokhoz, azokat törölheti stb.; nyilvánvaló, hogy az ilyen adatbázisok üzemeltetését az Avtv. fent idézett definíciójára hivatkozva nem lehet jogellenesnek minősíteni, sőt, *abból következik,* hogy ilyen esetekben az adatkezelők párhuzamosan minősülnek adatkezelőként.

1.10.3. Az Irányelv vonatkozó rendelkezése

Az irányelv 2. cikk *d)* pontja szerint „»adatkezelő« az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját; ha a célokat és módokat egy adott nemzeti vagy közösségi jogszabály határozza meg, az adatkezelőt vagy a kinevezésére vonatkozó külön szempontokat ez a nemzeti vagy közösségi jogszabály jelöli ki".

1.10.4. Az adatkezelés fogalma

Az Avtv. 2. § 9. pontjában adott definíció szerint „*adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is". Az adatkezelés fogalmával kapcsolatban értelmezési kérdésként merül fel egyrészt a fogalom terjedelme, másrészt az egyes adatkezelések körülhatárolásának lehetőségei. Végül problematikus az adatkezelés és adatfeldolgozás fogalmának viszonya is.

[338] ABI 1999, 109; hasonlóan ABI 1999, 234.

[339] ABI 1999, 178.

[340] Tagállami megoldásra lásd például a brit adatvédelmi törvény I. rész 1. (1) pontját.

1. Mint az az Avtv. miniszteri indokolásából kiderül, a jogalkotói szándék szerint: „Az adatkezelés az adatokra alkalmazható minden elképzelhető műveletet felölel.” A törvény egyes adatkezeléseket külön is meghatároz (adattovábbítás, nyilvánosságra hozatal, adattörlés, adatzárolás, adatmegsemmisítés – lásd alább a 2. § 10–14. pontjánál), illetőleg példálódzó felsorolással kiemel [fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is]. Az „adatkezelések összekapcsolását” a törvény nem határozza meg, ám az „összekapcsolást” mint adatkezelést sorolja fel a 2. § 9. pontja, és az „adatkezelések összekapcsolására vonatkozó rendelkezés található a 8. § (1)–(2) bekezdésében (lásd erre a 8. §-hoz fűzött kommentárt).

A felsorolás nyomán nincs tere olyan értelmezésnek, amely a hang- és képadatok felvételét kizárja az adatkezelés fogalmának köréből; álláspontunk szerint azonban nemcsak a hang- vagy képfelvétel személyes adat (hanem maga a hallható hang és látható kép is), továbbá nemcsak azok rögzítése adatkezelés[341], hanem azok érzékelése is.

A 2003. évi novellát megelőzően az Avtv. olyan meghatározással élt, amelyben a felsorolás taxatívként is értelmezhető volt [„adatkezelés az alkalmazott eljárástól függetlenül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is”]. Ezzel kapcsolatban vitakérdésként merült fel, hogy miként minősül az adatokba történő *betekintés,* az adatokhoz való *hozzáférés*. Ezzel a kérdéssel kapcsolatos a megfigyelést szolgáló kamerarendszerek (illetőleg ennek analógiájára például a rögzítést nem végző, ám távolról az érintett szavainak lehallgatására szolgáló eszközök) alkalmazásának adatvédelmi jogi megítélése.

További kérdés, hogy mely esetekben minősül adatkezelésnek az adat (illetőleg az adathordozó) birtokban tartása. Ha magánszemély részére valaki olyan – névtelen – kérdőívet ad át, amelyen saját szokásaira, meggyőződéseire vonatkozó adatokat tüntetett fel, akkor az adott magánszemély adatkezelést végez;[342] ám nem ilyen egyszerű a kérdés megítélése, ha az átadott adathordozón az adat kódolva van (például a magánszemély azonosító kódjait tartalmazó chipkártyát ad át olyan személynek, aki arról csak az egyik kódot képes kiolvasni – a többi kódra vonatkozóan megvalósul-e az adatkezelés –, lásd erre vonatkozóan fent a 2. § 1. pontjához fűzött magyarázatot).

[341] Ennek megítélése az adatvédelmi biztosi gyakorlatban nem kérdéses, pl. adatkezelés a fénykép készítése: ABI 2005, 74, stb.

2. Az adatvédelmi nyilvántartásba történő bejelentkezés kötelezettségével kapcsolatban merült fel az adatvédelmi biztosi gyakorlatban, hogy *miképpen határolható körül egy adatkezelés.*[343] A nyilvántartásba az egyes adatkezeléseket kell bejelenteni; ám egy ügyféladatbázis építése esetén például számos adatkezelésnek minősülő művelet elkülöníthető, így az adatfelvétel, az adattárolás, a felhasználás, továbbítás, a törlés. További kérdés az, hogy ha már egy adat kezelésével megvalósul az adatkezelés, akkor egy egész adatállomány kezelése párhuzamos adatkezelések összessége, vagy továbbra is csak egyetlen adatkezelés.

3. Az *adatkezelés* fogalmával kapcsolatban is megemlítendő, ám részletesen az *adatfeldolgozás* meghatározásának magyarázatánál tárgyaljuk azt a problémát, amely abból ered, hogy az Avtv. fogalomrendszere e két tevékenységet megkülönbözteti.

4. A 2005. évi XIX. törvénnyel történt módosítás nyomán az adatkezelés fogalma immár nem csak személyes adatokra, hanem bármely adatra vonatkoztatható; egyelőre nem ítélhető meg, hogy a személyes adatok körén kívül szükség lesz-e a fogalom jogalkalmazói értelmezésére.

1.10.5. Az adatvédelmi biztos gyakorlata az adatkezelés fogalmának értelmezésével kapcsolatban

1. A *betekintés, megfigyelés* adatvédelmi jogi megítélésével kapcsolatban az adatvédelmi biztos gyakorlata ingadozó volt.[344] Az Avtv. szövegébe a 2003. évi novella által bevezetett fogalommeghatározás nyomán immár lehetséges olyan érvelés, hogy az adatokhoz való hozzáférés az Avtv. szerinti adatkezelésnek minősül (arra is figyelemmel, hogy a betekintést [consultation] az irányelv is kifejezetten a fogalommeghatározás körébe vonja).

A legkorábbi jogesetekben az adatvédelmi biztos nem foglalt állást abban a kérdésben, hogy a megfigyelést szolgáló kamerák üzemeltetése adatkezelés-e, csak rögzítette azt a követelményt, hogy az ilyen eszközöket „jól látható módon kell elhelyezni […], és egyéb úton

---

[342] ABI 2004, 76.

[343] ABI 1998, 174.

[344] A személyes adatokat tartalmazó nyilvántartásokba történő betekintés adatkezelésnek minősül: ABI 1997, 169; hasonlóan ABI 2000, 262. Az adatokhoz való hozzáférés nem adatkezelés: ABI 2000, 283; hasonlóan ABI 2005, 340.

is fel kell hívni az állampolgárok figyelmét jelenlétükre".[345] Más esetben az adatvédelmi biztos úgy foglalt állást, hogy egy háziorvos nem szerelhet fel térfigyelő kamerákat oly módon, hogy azok közterületre is irányulnak, mert „a hatályos jogszabályok között nincsen olyan törvényi felhatalmazás, amely arra jogosítaná fel a háziorvost, hogy az orvosi rendelő környékét kamerákkal tartsa megfigyelés alatt. Törvényi felhatalmazás hiányában kizárólag saját tulajdonban, illetve használatban lévő ingatlanra irányítottan lehet képfelvevő berendezést működtetni, de ilyenkor is fel kell hívni az oda látogatók figyelmét az elhelyezett kamerákra (figyelmeztető táblával). Amennyiben más személy tulajdonában álló ingatlan, közterület van a kamera látómezejében, jogellenes adatkezelés valósul meg."[346] A két állásfoglalást hét év választja el, ám mindkettő implikálja azt, hogy a megfigyelőkamera működtetése adatkezelés, hiszen követelményeket fogalmaz meg azzal kapcsolatban (ha a cselekmény nem volna adatkezelés, akkor erre az Avtv. 24. §-a szerint nem volna lehetőség), sőt, az utóbbi állásfoglalás jogosulatlan adatkezelés lehetőségére is utal. Ezzel szemben az adatvédelmi biztos más esetben úgy foglalt állást, hogy „az adatkezelés törvényi definíciójába nem tartozik bele sem egy kép, sem a hang technikai továbbítása, a személyes adatok – rögzítés nélküli – megfigyelése, meghallgatása".[347]

Nem véletlen az, hogy a biztosi gyakorlat a kérdésben ellentmondásokkal terhelt. A megfigyelőkamerák működtetése, a szóbeli adattovábbítás stb. mind veszélyeztetheti a magánszférát: annak megállapítása, hogy e cselekmények nem tartoznak az adatvédelmi jog hatálya alá, számos esetben lerontaná az adatvédelmi jog által biztosított garanciákat. Az ezzel ellentétes értelmezés – bár módot ad a biztosnak a fellépésre a fentiekhez hasonló esetekben – annak ellenzői szerint abszurd következményekkel járhat: adatkezelésnek minősülne ebben az esetben bármely személyes adat érzékelése is (például utcán álló gépjármű rendszámának leolvasása, az aktuális pletyka meghallgatása).[348]

---

[345] ABI 1997, 172.

[346] ABI 2004, 82. A figyelemfelhívás kötelezettségére lásd még a 7. § (1) bekezdéséhez fűzött kommentárt.

[347] 179/K/2004. sz. ügy

[348] A két értelmezésre vonatkozó német álláspontokat idézi Földes 2004, 25; azonban ebben a kérdésben az irányelv eltér a BDSG-től: Dammann–Simitis 1997, 110. Ezt az ellentmondást feloldaná az az értelmezés, amely szerint a megfigyelő kamera „technikai továbbítást" valósít meg, amely – mivel az adatkezelés fogalma a személyes adattal végzett „bármely műveletre" kiterjed – adatkezelésnek minősül (Szabó Máté 2004b). Ezt a nézetet elfogadva az adat „közvetlen" érzékelése nem, csak bármely technikai eszköz által történő érzékelése minősülne adatkezelésnek, tehát a következmény az volna, hogy egy személyes adat leolvasása szabad szemmel nem minősülne adatkezelésnek, ám szemüveggel, távcsővel vagy kamerával már igen. Ám a „bármely művelet" körébe tartozik a közvetlen megfigyelés is. A főszövegben ismertetett álláspontunk szerint a felsorolt esetek

Álláspontunk szerint az adathoz való hozzáférés, az adat megismerése, akár megfigyelőkamera közvetítésével, akár közvetlen érzékeléssel *adatkezelésnek minősül*. Ezt támasztja alá az adatkezelés meghatározásában szereplő „bármely művelet" fordulat, valamint az irányelv alábbi meghatározása is.[349] Azt, hogy a fogalom ilyen értelmezése ne eredményezze az Avtv. tárgyi hatályának kiterjesztését olyan esetekre, amelyekben a jogi szabályozás szükségtelen, a törvény tárgyi hatályára vonatkozó rendelkezések biztosítják [mindenekelőtt az 1/A. § (3) bekezdése].

2. Az adatvédelmi biztos szerint nem adatkezelés a származásra irányuló (illetőleg általánosítva: bármely személyes adatra irányuló) kérdés feltétele[350].

3. Az adatkezelés elsődleges jellemzője az adatvédelmi biztosi gyakorlat szerint az *adatkezelési cél*. Ennek változása esetében mindenkor új adatkezelésről beszélhetünk.[351]

4. Az irányelv nem ismeri az „adatfeldolgozás" kategóriáját. Az abban használt fogalmak pontosan tükrözik azt a helyzetet, hogy *egy* tevékenységről van szó (data processing, melyet magyarul adatkezelésnek fordítunk), az e tevékenységet megbízás alapján végző személy a „data processor", az a személy pedig, aki az adatkezelés célját és módját meghatározza, a „data controller".[352] Ezzel ellentétben a magyar törvény fogalomrendszere több értelmezésre is lehetőséget ad. E ponton igen fontos – mint az adatfeldolgozással kapcsolatban alább részletesen tárgyaljuk, gyakorlati jogalkalmazási következményekkel járó – eltérés van az irányelv és az Avtv. definíció-rendszere között: az irányelv az adatkezelési műveletek végzésére csak egy fogalmat (data processing, Datenverarbeitung, adatkezelés – a hivatalos fordításban és a korai AB-határozatokban „adatfeldolgozás") vezet be, nem ismeri az Avtv. által „adatfeldolgozásként" meghatározott kategóriát.

1.10.6. Az irányelv vonatkozó rendelkezései

Az irányelv 2. cikkének *b)* pontja szerint személyes adatok kezelése (adatkezelés) „a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy

---

mindegyike adatkezelés.

[349] „Már az adatkezelő – vagy valamely munkatársa – általi elolvasás (Lesen) – történjen az papíron létező dokumentumból vagy lehívással a képernyőről – megfelel az adatkezelés fogalmának." Dammann–Simitis 1997, 110.

[350] ABI 2005, 278

[351] Az adatvédelmi biztosi gyakorlatból lásd például ABI 2000, 212.

[352] Lásd irányelv 2. cikk *b), d)* és *e)* pontjait.

megváltoztatás, visszakeresés, betekintés, felhasználás, közléstovábbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés". Az irányelv hivatalos fordítása – csakúgy, mint a 15/1991. (IV. 13.) AB határozat – az adatfeldolgozás fogalmát használja; az irányelv angol szövegében a fogalom „data processing", németül „Verarbeitung (personenbezogener Daten)". Az irányelv fogalomrendszerében nem szerepel az adatfeldolgozás; a „data processing" végezhető mind az adatkezelő, mind az adatfeldolgozó által.

1.10.7. Az adatfeldolgozás

1. Az Avtv. meghatározása szerinti (2. § 15. pont) *adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Az adatfeldolgozás fogalmát – az adatfeldolgozó meghatározásával együtt – egy 1999. évi módosítás vezette be az Avtv. szövegébe, majd a 2003. évi novella módosította. A módosítás igényét az teremtette meg, hogy korábban az Avtv. nem ismerte azt az alanyt, akit az adatkezelő az adatkezelés során megbízottként igénybe vehet, akinek speciális szakértelmét az adatkezelés folyamatába bevonhatja,[353] méghozzá oly módon, hogy ahhoz további jogalap (az érintett hozzájárulása vagy törvényi felhatalmazás) nem szükséges [szükséges azonban az érintett tájékoztatása – lásd a 6. § (2) bekezdését].

Az alany (az adatfeldolgozó) fogalmának a törvénybe való bevezetésével egyidejűleg a jogalkotó – eltérve az irányelv definíciórendszerétől – szükségét látta az adatfeldolgozó által végzett tevékenység meghatározásának is, amely az adatvédelmi biztos leszűkítő jogértelmezésén és annak a 2003. évi novellára történő hatásán keresztül oda vezetett, hogy mára az adatfeldolgozó tevékenységi köre a magyar jogban igen szűken behatárolt. E folyamat leírását és kritikáját lásd részletesen alább.

2. Az adatfeldolgozás csak az adatfeldolgozással kapcsolatos technikai művelet lehet. A személyes adaton végzett bármely művelet adatkezelésnek minősül (lásd az Avtv. 2. § 9. pontjához fűzött kommentárt), ezért nehéz az adatkezelési művelet (például törlés, továbbítás) és az azzal kapcsolatos „technikai művelet" (törlés, továbbítás) elhatárolása. Van-e olyan művelet, amely az adatkezelés körébe tartozhat-e, ám az adatfeldolgozás körébe nem? Van-e

[353] Az adatvédelmi biztos ezt már korán érzékelte, és éves beszámolóiban szorgalmazta a fogalom bevezetését: ABI 1997, 14; ABI 1997, 50; ABI 1998, 28 stb.

olyan adatfeldolgozási művelet, amely egyben ne minősülne adatkezelési műveletnek is? Álláspontunk szerint nincs: a két fogalom – még a 2003. évi novella által történt módosítás után is – azonos terjedelmű. (Ez az álláspont ellentmond az adatvédelmi biztosi gyakorlatban kialakult értelmezésnek – lásd alább.) Az elhatárolás az alanyok szerint, az adatkezelő és az adatfeldolgozó fogalmának megkülönböztetésével történhet: míg az adatkezelőnek joga van az adatkezelési/feldolgozási műveletek céljának meghatározására és az adatkezelésre/adatfeldolgozásra vonatkozó döntések meghozatalára, addig az adatfeldolgozó a magyar jog szerint ilyen döntéseknek csak végrehajtója lehet.

3. További értelmezési kérdést jelent, hogy az adatkezelő és az adatfeldolgozó közötti adatforgalom törvényen (magán az Avtv. rendelkezésén) alapuló adattovábbítás-e (az Avtv. korábbi szabályozása alapján, amely a harmadik személy fogalmát nem határozta meg, álláspontunk szerint ez volt a helyes értelmezés), vagy nem is minősül adattovábbításnak. A 2. § 10. pontjának (adattovábbítás) és a 2. § 16. pontjának (harmadik személy) együttes értelmezése alapján a 2003. évi novellát követően az adatfeldolgozónak történő „továbbítás" nem adattovábbítás az Avtv. szerint. Ez nem érinti a 9. § alkalmazását külföldi adatfeldolgozónak történő továbbítás esetén.

1.10.8. Az adatvédelmi biztos gyakorlata

1. Az adatfeldolgozás fogalma csak az Avtv. 1999 júniusában hatályba lépett módosításával került be a törvényszövegbe. A módosítás nyomán – amelyet az adatvédelmi biztos beszámolóiban már hosszabb ideje szorgalmazott[354] – az Avtv.-be bekerült az adatfeldolgozó és – sajátosságként – az adatfeldolgozás fogalma is, ez utóbbi a következő meghatározással: „az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől".

Mint már utaltunk rá, a jogalkotó ezzel az irányelv fogalmi rendszerétől eltérve vezette be az adatfeldolgozó tevékenységének meghatározását a magyar jogba. Az adatkezelés és az adatfeldolgozás fogalma közötti viszony azonban nem volt egyértelmű. Rövidesen megszületett azonban az adatfeldolgozás fogalmának adatvédelmi biztosi értelmezése a 2000

[354] ABI 1997, 14; ABI 1998, 28 stb.

júniusában kiadott „Adósság- és követelésbehajtással foglalkozó gazdasági társaságok személyes adatok kezelésének gyakorlatával kapcsolatos adatvédelmi biztosi ajánlásban”.[355]

A követeléskezelő cégek nagy tömegű, ám viszonylag kis mennyiségű követelésnek a hitelező helyetti beszedésével foglalkoznak. A szóban forgó ügyben az adatkezelőként szereplő távközlési cég a követeléskezelő társaságoknak mint adatfeldolgozónak továbbította a személyes adatokat, s a követeléskezelők e cég nevében és javára eljárva voltak kötelesek a behajtást és az attól elválaszthatatlan adatkezelési műveleteket végezni. A követeléskezelő cég tevékenysége abban állott, hogy az ügyféllel telefonos kapcsolatot létesített, illetve ha ez nem sikerült, akkor legfeljebb két alkalommal tértivevényes levélben kereste meg őt. A társaság a megbízó nevében részletfizetési lehetőséget ajánlhatott fel.

Az adatvédelmi biztos vizsgálatát kezdeményező panaszosok azt sérelmezték, hogy személyes adataikat az adatkezelő „megkérdezésük nélkül” továbbította a követeléskezelő társaságnak; a megbízó a vizsgálat során úgy érvelt, hogy a követeléskezelő társaság adatfeldolgozást végez, és ebben az esetben nem szükséges az érintett hozzájárulása az „adattovábbításhoz”, amely a törvény fogalomrendszerében nem is minősül adattovábbításnak.[356]

Az adatvédelmi biztosi ajánlás szerint „az adósságbehajtó társaságok nem tekinthetők adatfeldolgozónak, mivel a birtokukba került személyes adatokkal *nem adatkezelési végrehajtási technikai műveleteket hajtanak végre,* hanem azokat felhasználják és azokra támaszkodva a szerződés keretei között döntéseket hoznak, a polgárral szerződésben álló gazdasági társaság tevékenységébe tartozó feladatot látnak el. Az adatkezelő nem adhat át rendelkezési-döntési jogot az adatok felett.”[357]

---

[355] ABI 2001, 195.

[356] ABI 2001, 197. Az Avtv. akkor hatályos szövege alapján az adatfeldolgozónak történő továbbítás álláspontom szerint adattovábbításnak minősült, de arra maga az Avtv. adott felhatalmazást.

[357] Figyelemre méltó az ajánlásban foglalt azon értelmezés, amely szerint az adatfeldolgozó kizárólag „adatkezelési végrehajtási technikai műveleteket” végezhet, s nem „használhatja fel” az adatokat. Pedig ez utóbbi művelet sem más, mint egy adatkezelési cselekmény végrehajtása: vagyis ha a célt az adatkezelő határozza meg, illetve az adatkezelésre vonatkozó döntést (kit kell megkeresni, mikor stb.) az adatkezelő hozza meg, magát a felhasználást (megkeresést) az adatfeldolgozó is végezheti. Vitatható az is, hogy az adatok *alapján* hozott döntés ugyanaz, mint az „adatkezelésre vonatkozó döntés” az adatkezelő fogalmának meghatározásában. Az Avtv. által használt „adatkezelési műveletek, technikai feladatok elvégzése” fordulat álláspontunk szerint megalapozatlanul változott az ajánlásban „adatkezelési technikai műveletek” elvégzésére. Az ajánlás idején hatályos szöveg helyes értelmezése szerint az adatfeldolgozás lehet *a)* adatkezelési műveletek elvégzése vagy *b)* technikai műveletek elvégzése. Mivel a *b)* körbe tartozó műveletek mindegyike egyben adatkezelés is, valójában

Az ajánlásban és azt követő gyakorlatában tehát az adatvédelmi biztos megszorítóan értelmezte az adatfeldolgozás akkor hatályos fogalmát, kifejezetten egyes, technikai jellegű műveletekre szorítva azt. A biztos több más esetben is adatkezelésnek minősített olyan műveleteket, amelyeket a felek (az adatkezelő és a megbízott) álláspontja szerint adatfeldolgozási konstrukcióban végeztek.[358]

Az adatvédelmi biztosi gyakorlat elfogadta adatfeldolgozásnak:

– az adatrögzítést, az adóbevallások feldolgozását;[359]

– az adatokat tartalmazó iratok „szkennelését", az adatok felismerését, a hibák javítását;[360]

– a portaszolgálat üzemeltetését, amelynek keretében az ezzel megbízott vagyonvédelmi gazdasági társaság mint adatfeldolgozó veszi fel a megbízó (adatkezelő) épületébe belépő személyek személyes adatait.[361] Adatfeldolgozóként minősült a Magyar Posta abban az esetben, amelyben a megbízó (adatkezelő) belföldi postautalvány igénybevételével küldött pénzt a címzett (adatalany) számára;[362]

- adatfeldolgozó a hírközlési szolgáltató, ha a támogatás iránt folyamodó előfizetők kérelmét átveszi, azokból kimutatásokat készít, majd a dokumentumokat további tárolás nélkül továbbítja az adatkezelő Nemzeti Hírközlési Hatóságnak.[363]

Az Avtv. 2004. január 1-jén hatályba lépő módosítása a fent ismertetett adatvédelmi biztosi értelmezésnek megfelelő irányba módosította az „adatfeldolgozás" meghatározását: az „adatkezelési műveletek, technikai feladatok elvégzése" szövegrész helyébe „adatkezelési műveletekhez kapcsolódó technikai feladatok" került.

---

az „adatfeldolgozás" fogalmának tartalma megegyezik az adatkezelésével.

[358] Például ABI 2001, 127: „Az együttműködési megállapodás szerint a […] mint a kamarai tagok adatainak kezelője a kártyák előállításához szükséges adatokat a […] Bank Rt.-nek mint adatfeldolgozónak adja át, amely az adatokat […] kizárólag a kártyák előállításához használhatja fel. […] Az adatvédelmi biztos vizsgálata megállapította, hogy a megállapodás az adatfeldolgozó Avtv.-ben meghatározott fogalmának téves értelmezésén alapul. A […] Bank Rt. tevékenysége egy adatfeldolgozó feladatain (adatkezelési műveletek, technikai feladatok elvégzése) túlterjed, valójában – a kártya kibocsátójaként és a projekt finanszírozójaként – adatkezelőnek minősül."

[359] ABI 2001, 66.

[360] ABI 2002, 48.

[361] ABI 2002, 75.

[362] ABI 2002, 117.

[363] ABI 2005, 469

2. Az adatvédelmi biztosi gyakorlat az adatfeldolgozónak történő „továbbítást” már a 2003. évi novella hatálybalépését megelőzően sem tekintette az Avtv. szerint adattovábbításnak.[364]

1.10.9. Az irányelv vonatkozó rendelkezései

A magyar adatvédelmi jog az adatfeldolgozás szabályozásában igen jelentősen tér el az irányelvtől – bár a fogalomrendszer eltérése látszólag kis mértékű, annak a jogalkalmazásban igen súlyos következményei vannak.

Az irányelvben nem található meg az a fogalom, amelyet az Avtv. „adatfeldolgozásként” határoz meg. Az irányelv 2. cikkének *b)* pontja tartalmazza azonban – a hivatalos fordítás szerint – a „személyes adatok feldolgozása” fogalom definícióját, amely azonban az Avtv. által „adatkezelésként” meghatározott fogalomnak felel meg („személyes adatok feldolgozása [»feldolgozás«] a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés”).

Az irányelv tehát nem ismeri az „adatfeldolgozás” kategóriáját. Az abban használt fogalomrendszer pontosan tükrözi azt a helyzetet, hogy egy tevékenységről van szó (data processing, melyet magyarul adatkezelésnek fordítunk), az e tevékenységet megbízás alapján végző személy a „data processor”, az a személy pedig, amely az adatkezelés célját és módját meghatározza, a „data controller” – nem is szükségszerűen két alany, inkább két funkció elválasztásáról van szó.

Az irányelv és a hazai szabályozás közötti fogalomrendszer eltérése az alábbi táblázattal szemléltethető. A táblázatban az Avtv. meghatározásaihoz rendeltük az irányelv azonos tartalmú fogalmait (az angol szöveg, illetőleg a hivatalos magyar fordítás szerint), és egy tagállami jog (a brit) tartalmilag azonos fogalmait.

Avtv.	irányelv	Brit törvény

[364] ABI 2002, 75.

adatkezelő	data controller („adatkezelő”)	data controller
adatkezelés	data processing („adatfeldolgozás”)	data processing
adatfeldolgozó	data processor („feldolgozó”)	data processor
adatfeldolgozás	–	–

Az irányelv – és az annak alapján elfogadott tagállami jogszabályok – nem korlátozzák az adatfeldolgozó által végezhető adatkezelési műveletek körét, illetőleg azokban ismeretlen számos olyan korlátozás, amelyet a magyar jogalkotó az adatfeldolgozás szabályozásával kapcsolatban meghatároz (például további adatfeldolgozó igénybevételének tilalma). A magyar szabályozásra jellemző többletkorlátozások az adatfeldolgozási tevékenységgel kapcsolatban az alábbiak:

– az adatfeldolgozói tevékenység kör szűk meghatározása (lásd részletesen fent);

– az adatfeldolgozóként igénybe vehető alanyok körének meghatározása [Avtv. 4/A. § (4) bekezdése];

– az adatfeldolgozó adatfeldolgozó általi igénybevételének tilalma [Avtv. 4/A. § (2) bekezdése];

– az adatfeldolgozó által saját célból végzett adatfeldolgozás tilalma [Avtv. 4/A. § (3) bekezdése]. Ezeket a szabályokat elemezzük részletesen az alábbiakban.

1.10.10. Az Avtv. által az adatfeldolgozással kapcsolatban meghatározott követelmények (a 4/A § elemzése)

1. Az Avtv. 4/A § (1) bekezdése szerint „az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel.” Az adatfeldolgozásra vonatkozó 4/A. § 1999-ben került a törvény szövegébe, majd azt a 2003. évi novella újabb rendelkezésekkel egészítette ki. Maga az adatfeldolgozás fogalmi köre és szabályozási koncepciója a magyar jogban lényegesen eltér az irányelvben foglaltaktól és a legtöbb

tagállami megoldástól; lásd erre a 2. § 15. és 16. pontjához fűzött kommentárt, valamint alább az irányelv vonatkozó rendelkezéseivel foglalkozó részt.

Az adatkezelőnek az adatfeldolgozó jogainak és kötelezettségeinek meghatározása során tekintettel kell lennie az Avtv.-nek az adatkezelő és adatfeldolgozó fogalmát, valamint az általuk végzett tevékenységet (az adatkezelést és az adatfeldolgozást) meghatározó rendelkezéseiből folyó követelményekre (az adatfeldolgozó nem dönthet az adatkezelés céljáról és módjáról, csupán a döntések végrehajtását szolgáló „technikai feladatokat" végezhet – lásd részletesebben a 2. § 8., 9., 15. és 16. pontjához fűzött kommentárokat), valamint a 4/A. § által megfogalmazott korlátokra [további adatfeldolgozó igénybevételének tilalma – 4/A. § (2) bekezdése, saját célú adatfeldolgozás tilalma – 4/A. § (3) bekezdése stb.].

A 4/A. § (1) bekezdése az irányelv 17. cikkének (3) bekezdését teszi át a hazai jogba, amely szerint:

„Adatfeldolgozón keresztül történő adatfeldolgozásra olyan szerződésnek vagy jogi aktusnak kell vonatkoznia, amely az adatfeldolgozót az adatkezelővel szemben köti, és amely különösen a következőket tartalmazza:

– az adatfeldolgozó kizárólag az adatkezelő utasítása alapján járhat el,

– az (1) bekezdésben megállapított kötelezettségek annak a tagállamnak a jogszabályai szerint kerülnek meghatározásra, amelyben a feldolgozó letelepedett, és azok a feldolgozóra is vonatkoznak."

A 17. szakasz (3) bekezdése az ugyanazon szakasz (1) bekezdésében[365] szabályozott adatbiztonsággal kapcsolatos kötelezettségeket úgy rendeli meghatározni, hogy azok az adatfeldolgozó letelepedésének helye szerinti tagállami joggal összhangban álljanak.

2. Az adatfeldolgozó felelősségét, illetőleg az adatfeldolgozásra vonatkozó egy – a magyar adatvédelmi jogra egyedülállóan jellemző – szabályt rögzít a 4/A § (2) bekezdése, amely szerint „az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért,

[365] A 17. cikk (1) bekezdése: „A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás 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 adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének."

törléséért, továbbításáért és nyilvánosságra hozataláért. Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe." A törvény az adatfeldolgozó *felelősségét* tevékenységi körén belül, „illetőleg az adatkezelő által meghatározott keretek között" a személyes adatokon végzett meghatározott műveletekért állapítja meg. Mivel a feldolgozás művelete valamennyi adatkezelési művelethez köthető (sőt álláspontunk szerint az adatkezelés és adatfeldolgozás fogalmaival jelölt műveletek tartalma nem különböztethető meg: lásd a 2. § 8., 9., 15. és 16. pontjához fűzött kommentárokat), ezért az adatfeldolgozó minden általa végzett adatfeldolgozási műveletért „felelős".

E felelősség szabályait a 4/A. § (2) bekezdése és a 18. § határozza meg. A 18. § (1) bekezdése szerint az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt a veszélyes üzemi felelősségnek megfelelő feltételek mellett köteles megtéríteni. „Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért is." Ha tehát az adatfeldolgozó tevékenysége az érintettnek okoz kárt, úgy azért az Avtv. 18. § (1) bekezdésében meghatározott szabályok szerint az adatkezelő felel, s az adatkezelőnek visszkereseti igénye van az adatfeldolgozóval szemben. E felelősséget az adatkezelő és adatfeldolgozó közötti jogviszonyra vonatkozó szabályok szerint kell megítélni.

3. A 4/A. § (2) bekezdésének második mondata tiltja az adatfeldolgozó által további adatfeldolgozó igénybevételét. Minden olyan esetben, amelyben az adatkezelő kettő vagy több adatfeldolgozót kíván bevonni az adatkezelés/adatfeldolgozás folyamatába, az együttműködést szabályozó szerződéses rendszert úgy kell kialakítani, hogy minden adatfeldolgozó közvetlenül az adatkezelővel legyen jogviszonyban.

4. Az adatvédelmi biztos a közelmúltban kifogásolta a hitelintézetekről és pénzügyi vállalkozásokról szóló, a biztosítóintézetekről és a biztosítási tevékenységről szóló, valamint a tőkepiacról szóló törvények kiszervezésre vonatkozó szabályait. E szabályok módosításával ugyanis megnyílt a lehetőség az adatfeldolgozás kiszervezésére, amelyet a biztos úgy értékelt, hogy „Ez nem egyeztethető össze az Avtv. adatkezelést és adatfeldolgozást értelmező rendelkezéseivel, tekintettel arra, hogy az adatfeldolgozás az Avtv. értelmében eleve olyan tevékenység, amelyet az adatkezelő mással végeztet, ezért az adatfeldolgozás kiszervezése az Avtv. szabályai alapján nem értelmezhető"[366]. A biztos kifogásolta azt is, hogy az adatfeldolgozás kiszervezése által olyan helyzet jön létre, amelyben az adatfeldolgozó más adatfeldolgozót vesz igénybe, ez pedig az Avtv. 4/A§ (2) bekezdésével ellentétes helyzet.

[366] ABI 2005, 111.

Nézetünk szerint az állásfoglalás téves: a kiszervezésre vonatkozó szabályok párhuzamosan érvényesülnek az Avtv. adatfeldolgozásra vonatkozó szabályaival, azaz a személyes adatokkal végzendő tevékenység kiszervezése általában az Avtv. szerinti adatfeldolgozásnak minősül. Az adatvédelmi biztos adott esetben önkényesen tulajdonította az Avtv-ben használt jelentést a pénzügyi szervezetekre vonatkozó jogszabályok által használt „adatfeldolgozás" fogalomnak.

3. Az adatfeldolgozó tevékenységének az adatkezelő tevékenységétől való elhatárolásában is döntő jellemzőjét fogalmazza meg a 4/A § (3) bekezdése, és ezen túl további, kizárólag a magyar adatvédelmi jogra jellemző követelményt állít fel: „az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni."

Az adatfeldolgozó által hozott *érdemi döntés tilalma* olyan követelmény, amely az Avtv.-nek az adatkezelésre és adatfeldolgozásra, illetőleg az ezeket végző alanyokra vonatkozó meghatározásaiból (2. § 8., 9., 15. és 16. pontjai) is következik. A (3) bekezdés e kötelezettséget pozitív módon is meghatározza, valamint a tárolás és őrzés tekintetében is előírja az adatkezelő rendelkezéseinek követését az adatfeldolgozó számára

Az „adatkezelő" fogalom meghatározásának lényeges eleme, hogy ez az alany az, amelyik „az adatkezelésre […] vonatkozó döntéseket meghozza" (Avtv. 2. § 8. pontja). Ez egyben azt is jelenti – és ezt az adatvédelmi biztosi gyakorlat is alátámasztja –, hogy ha valamely jogalany ilyen döntést hoz, azzal adatkezelővé válik.[367]

Az „adatkezeléssel kapcsolatos döntéssel" kapcsolatban ki kell emelni az alábbiakat:

Az irányelv nem követeli meg azt, hogy az adatkezelő bármely „döntést" hozzon az adatkezelés folyamatában, csupán azt, hogy – a cél mellett – meghatározza annak a *módját.*[368] Álláspontunk szerint ez nem jelenti azt, hogy az adatkezelő ne delegálhatna az adatkezeléssel (illetőleg feldolgozással – a fogalmak kapcsolatáról lásd alább) kapcsolatos döntéseket az adatfeldolgozóra, ez egyes tagállami jogokban megengedett.[369] A magyar jogalkotó azonban

[367] ABI 2001, 200. (Az értelmezés nézetünk szerint téves, ám ez nem érinti a gondolatmenetet – lásd a 2. § 8. pontjához fűzött kommentárt.)

[368] A német szövegben: „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet".

[369] Jay–Hamilton 1999, 35.

kizárta, hogy az adatfeldolgozó „adatkezelésekre vonatkozó döntéseket” hozzon: ebben az esetben már adatkezelőnek minősül. Nem „érdemi” álláspontunk szerint az a döntés, amely az adatfeldolgozás folyamatába illeszkedik, nem hat ki annak céljára, módjára, hanem tárgya valamely, az adatkezelő rendelkezései által megszabott keretek között végrehajtandó technikai művelet végrehajtása.

A (3) bekezdés rögzíti azt a követelményt is, amely szerint az adatfeldolgozó mind az adatfeldolgozást, mind az adatok tárolását és megőrzését az adatkezelő rendelkezései szerint köteles végezni. Az, hogy az adatkezelő rendelkezésének adott esetben milyen mélységben kell megszabnia az adatfeldolgozás folyamatát (vagy másik oldalról: a döntések mely szintje minősül „érdemi” döntésnek, és mely döntéseket hozhatja meg az adatfeldolgozó), az adott tényállástól függ, elsősorban az adatfeldolgozás célja, az adatok jellege szerint ítélendő meg. Lehetséges például, hogy az adatkezelő rendelkezése az adatfeldolgozó számára csak határidőt rögzít az adatfeldolgozás elvégzésének tekintetében: ebben az esetben az adatfeldolgozó nem hoz érdemi döntést akkor, amikor meghatározza például azt, hogy az adatok egyik részét délelőtt, a másik részét délután dolgozza fel. Olyan eset is elképzelhető, amelyben ez a döntés „érdemi”, például kihat az adatalanyok jogaira vagy kötelezettségeire: ilyen esetben az adatfeldolgozó e kérdésben csak az adatkezelő rendelkezése szerint járhat el.

A 2003. évi novellával megállapított szöveg nyomán a magyar adatvédelmi jog sajátosságává vált *az adatfeldolgozó saját célra végzett adatfeldolgozásának tilalma*. A rendelkezés valószínűsíthetően a jogalkotó által sem kívánt következményekkel jár, így például kizárja ilyen tevékenységét akár saját ügyfelei, munkavállalói vonatkozásában is.

Mivel az adatfeldolgozás minden esetben adatkezeléshez kapcsolódik, ez a rendelkezés azt jelenti, hogy az adatfeldolgozó nem láthatja el tevékenységét, ha saját célból is végez adatkezelést. A jogalkotó szándék feltehetően arra irányult, hogy a szabályozás kizárja a feldolgozott adatbázis saját célú hasznosításának lehetőségét. A rendelkezéssel kapcsolatban azonban felmerül az a kérdés, hogy miképp kezeli ebben az esetben az adatfeldolgozással (például tárolással, szkenneléssel, archiválással) foglalkozó gazdasági társaság saját, személyes adatokat tartalmazó adatbázisait (munkavállalók adatbázisa, üzleti partnerek adatbázisa, stb.).

Az adatvédelmi biztos számos esetben állapította meg valamely adatfeldolgozó adatkezelői minőségét, ha megítélése szerint a szóban forgó szerv vagy személy tevékenysége túlterjeszkedett az adatfeldolgozás törvényben meghatározott keretein. Az adatfeldolgozásra vonatkozó adatvédelmi biztosi gyakorlatban kulcsfontosságú az az állásfoglalás, amelyben a biztos kizárta az ún. követeléskezelő társaságok adatfeldolgozóként történő minősülését, mert

álláspontja szerint e társaságok az átadott adatokra támaszkodva (!) döntéseket hoznak.[370] Az ügy ismertetését lásd a 2. § 15. pontjához fűzött magyarázatban.

A 4/A. § (3) bekezdése az irányelv 17. cikkének (3) bekezdését teszi át a hazai jogba, amely szerint: „Adatfeldolgozón keresztül történő adatfeldolgozásra olyan szerződésnek vagy jogi aktusnak kell vonatkoznia, amely az adatfeldolgozót az adatkezelővel szemben köti, és amely különösen a következőket tartalmazza: […] az adatfeldolgozó kizárólag az adatkezelő utasítása alapján járhat el."

4. Az adatfeldolgozási szerződésről a 4/A § (4) bekezdése rendelkezik: „az adatfeldolgozásra vonatkozó megbízási szerződést írásba kell foglalni. Az adatfeldolgozásra nem adható megbízás olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt."

Az Avtv. kizárólag az adatfeldolgozásról szóló „megbízási" szerződés *írásba foglalását* írja elő. A 2. § 16. ponthoz hasonlóan a „megbízás" szóval a jogalkotó ebben az esetben sem a polgári jogi megbízást jelöli, hanem az a hétköznapi szóhasználat szerint értelmezendő; álláspontunk szerint az adatfeldolgozásra vonatkozó vállalkozási stb. szerződésre is irányadó az írásba foglalás követelménye.

Álláspontunk adatfeldolgozásra vonatkozó szerződés írásba foglalása az Avtv. szabályozása szerint is megtörténik az adatfeldolgozásra vonatkozó, az Avtv. szabályozási tárgya szempontjából releváns rendelkezések írásba foglalásával.

Az Avtv. 4/A. § (4) bekezdésének alkalmazásában írásba foglaltnak minősül a szerződés, ha azt fokozott elektronikus aláírással ellátott elektronikus dokumentum tartalmazza,[371] illetőleg ha az levélváltás, táviratváltás, távgépírón történő üzenetváltás vagy külön törvényben meghatározott maradandó eszközzel történő nyilatkozatváltás útján jött létre.[372]

Az Avtv. 4/A. § (4) bekezdésében rögzített, *az adatfeldolgozók alanyi körét behatároló rendelkezés* a magyar adatvédelmi jog sajátos szabályai közé tartozik; „a felhasználandó személyes adatokat felhasználó üzleti tevékenységben érdekelt" fordulat értelmezéséhez a 2003. évi novella miniszteri indokolása sem ad támpontot, amely megismétli a törvény rendelkezését, ám azt nem értelmezi. Felmerülhet olyan értelmezés is, amely szerint egy cégcsoport tagvállalatainak üzleti tevékenységéhez kapcsolódó személyes adatkezelésével

[370] ABI 2001, 200.

[371] 2001. évi XXXV. törvény 4. § (1) bekezdése; 1978. évi 2. tvr. 38. § (2) bekezdése.

kapcsolatos adatfeldolgozási műveleteket (például marketing-adatbázis tárolását) a rendelkezés miatt a csoport informatikai vállalkozása nem végezheti, mert a tagvállalat közvetve érdekelt a cégcsoport sikerében, ezáltal „érdekelt" a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben. Ez az értelmezés álláspontunk szerint téves.

Az értelmezés a „felhasználás" és az adatfeldolgozás („technikai feladatok elvégzése") fogalmak közötti megkülönböztetésre épülhet. Az adatfeldolgozó csupán technikai feladatokat végez, tevékenységének célja az adatkezelő által meghatározott adatkezelési céllal azonos; döntései nem érdemiek. A „felhasználás" szintén feltételez egy célt – ez az az üzleti tevékenység, amelyben a 4/A. § (4) bekezdésében meghatározott vállalkozás érdekelt. Álláspontunk szerint ez az érdekeltség közvetlen lehet; azaz valamely vállalkozásnak akkor nem adatható adatfeldolgozásra megbízás, ha ugyanazon személyes adatokat saját céljára üzleti haszonszerzés végett kezeli.

További problémát okoz az, hogy a jogalkotó az „adatok" fogalmat használja; nem kizárt ugyanis, hogy az adatfeldolgozó (például telemarketinggel és direktmarketinggel is foglalkozó cég) olyan adatbázist dolgoz fel (például adatokat vesz fel telefonon egy másik direktmarketing-cég számára), amelynek egyes elemeit – akár más forrásból – saját céljára maga is kezeli (tehát a telefonos megkeresésekhez az adatkezelőtől kapott adatbázisban szerepel olyan személyes adat, amely megtalálható a cég saját adatbázisában). Lehetséges olyan értelmezés, hogy bármely adategyezés már kizárja az ilyen cég adatfeldolgozóként való alkalmazását, ám olyan is, amely szerint csak a teljes „adatállomány" egyezősége lehet alapja a cég kizárásának az adatfeldolgozók köréből.

Az adatvédelmi biztos egy állásfoglalása szerint „az Avtv. 4/A. § (4) bekezdésében meghatározott korlátozás álláspontom szerint a konkurens vállalatokat zárja ki, illetve azt a lehetőséget, hogy a megbízott adatfeldolgozó saját üzleti tevékenységéhez használja fel a tudomására jutott személyes adatokat."[373] Ez az állásfoglalás még a fent ismertetett értelmezéseknél is szigorúbb: bármely konkurens céget kizár a lehetséges adatfeldolgozói körből. Álláspontunk szerint ez az álláspont téves, mert a jogalkotó kifejezetten „*a* feldolgozandó adatok" felhasználásában való üzleti érdekeltséget szabályoz, tehát nem azonos adatfajtára, általában személyes adatokra stb. utal.

Az irányelv 17. cikk (4) bekezdése szerint: „A bizonyítékok megőrzése céljából a szerződés vagy jogi aktus adatvédelemre és az (1) bekezdésben említett intézkedésekkel [az

[372] 1978. évi 2. tvr. 38. § (2) bekezdése.

[373] 1245/x/2003–3. sz. ügyirat.

(1) bekezdés az adatbiztonsággal kapcsolatos követelményeket rögzíti – lásd a 10. § (1) és (2) bekezdéséhez fűzött kommentárokat] kapcsolatos előírásokra vonatkozó részeit írásba vagy egyéb, azzal egyenértékű formába kell foglalni."[374] Az irányelv rendelkezése egyszerre szigorúbb és precízebb, mint az Avtv. szabályozása: *valamennyi* adatvédelmi jogi relevanciájú szerződés (vagy más jogi aktus) *részleges* – csak az adatvédelmi és adatbiztonsági tárgyú rendelkezésekre kiterjedő – írásba foglalását vagy azzal egyenértékű formában való rögzítését írja elő.

5. Sajátos, a törvény területi hatályának problematikájához kapcsolódó esetet rendez a 4/A § (6) bekezdése: „e törvényben foglaltakat kell alkalmazni, ha az Európai Unió területén kívül személyes adatok kezelését folytató adatkezelő az adatfeldolgozással a Magyar Köztársaság területén székhellyel, telephellyel (fióktelepel) vagy lakóhellyel (tartózkodási hellyel) rendelkező adatfeldolgozót bíz meg, vagy itt lévő eszközt használ fel, kivéve, ha ez az eszköz csak az Európai Unió területén átmenő adatforgalom célját szolgálja. Az ilyen adatkezelőnek ki kell jelölnie egy képviselőt a Magyar Köztársaság területén."

A 4. § (6) bekezdésének alkalmazása során is felmerül az a kérdés, amely a külföldre irányuló adattovábbításra vonatkozó szabályozás (9. §) értelmezése során – mi a megítélése *az Európai Gazdasági Térségről szóló egyezményben részes állam* területén személyes adatok kezelését folytató adatkezelőnek? Álláspontunk szerint az ilyen adatkezelő e rendelkezés alkalmazásában az Európai Unió területén belül adatkezelést folytatónak minősül.

Az adatfeldolgozó az Avtv. 2. § 16. pontjában rögzített meghatározás szerint természetes vagy jogi személy, illetőleg jogi személyiséggel nem rendelkező szervezet lehet. A jogalkotó mindhárom alanyi kör esetén szabályozás alá igyekszik vonni a tartós működésre módot adó, illetőleg arra utaló körülményeket, ám nem használ az irányelvhez hasonló absztrakt fogalmat (establishment).

Az Avtv. 4. § (6) bekezdése az 1/A. § (1) bekezdés alóli kivételt állapít meg a harmadik országbeli adatkezelő által az Európai Unió területén átmenő adatforgalom célját szolgáló, a Magyar Köztársaság területén lévő eszköz alkalmazásával folytatott adatfeldolgozásra. A főszabálytól eltérően nem az adatkezelés/adatfeldolgozás helyét, hanem magának az eszköznek a földrajzi elhelyezkedését írja elő mint a magyar jog hatályának megállapításakor releváns tényezőt. Ez azt jelenti, hogy ha az eszköz a harmadik ország területén van, akkor e rendelkezés alapján a magyar jog hatálya akkor sem állapítható meg, ha

[374] A szerző fordítása. A hivatalos fordítást lásd a függelékben.

az hírközlési hálózaton át az országból elérhető.[375] Ilyen esetekben azonban vizsgálható, hogy adatkezelés vagy adatfeldolgozás végbemegy-e a Magyar Köztársaság területén. Álláspontunk szerint a Magyar Köztársaság területén adatkezelésre vagy adatfeldolgozásra használt eszköz alkalmazásával végzett tevékenység az Avtv. 1/A. § (1) bekezdése alapján e rendelkezés hiányában is minden esetben az Avtv. hatálya alá esne (az irányelvben a külön szabályozásnak az az indoka, hogy az nem az adatkezelés helye alapján állapítja meg a területi hatályt – lásd alább).

A képviselő kijelölésének kötelezettsége álláspontunk szerint az EU területén átmenő adatforgalomra nem vonatkozik. A harmadik országbeli adatkezelőnek képviselőt kell kijelölnie a Magyar Köztársaság területén. A képviselő kijelölésének kötelezettsége elvileg segíti az adatalanyt a törvényben meghatározott jogok gyakorlásában; sajnos az Avtv. rendelkezései máshol – például az adatvédelmi nyilvántartásba bejelentő adatkör kapcsán – a kijelölt képviselőről nem szólnak.

Az irányelv az alkalmazandó jogról szóló 4. cikk (1) bekezdésének *c)* pontja szerint: „A személyes adatok feldolgozására minden tagállam az ezen irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza, amennyiben [...] az adatkezelő nem telepedett le a Közösség területén, és a személyes adatok feldolgozása céljából gépi vagy más olyan eszközt alkalmaz, amely a fenti tagállam területén található, kivéve, ha ezt az eszközt kizárólag a Közösség területén átmenő adatforgalom céljára használják.” A 4. cikk (2) bekezdése szerint: „Az (1) bekezdés *c)* pontjában említett körülmények esetén az adatkezelőnek – az ellene indítható jogi keresetek sérelme nélkül – ki kell jelölnie egy, az adott tagállam területén letelepedett képviselőt.”

Az Avtv. 4. § (6) bekezdése tehát az irányelvnek a tagállami jog területi hatályára vonatkozó rendelkezésének egyik pontját ülteti át – inkább az 1/A. §-ban lenne a helye. Az, hogy a jogalkotó mégis az adatfeldolgozás körében rendezi ezt a kérdést, az adatkezelés és az adatfeldolgozás fogalmának sajátosan a magyar jogra jellemző megkülönböztetéséből fakad. Felvethető az is, hogy az adatfeldolgozó vonatkozásában szükség van-e a rendelkezésre egyáltalán, hiszen az 1/A. § (1) bekezdése a törvény hatálya alá von minden, a Magyar Köztársaság területén folytatott adatkezelést *és adatfeldolgozást,* tehát azokat is, amelyeket az adatfeldolgozó harmadik állambeli adatkezelő megbízásából végez.

Eltérés az irányelv és a hazai szabályozás között az is, hogy míg az előbbi éppen a 4. cikk (1) bekezdésének *c)* pontjában tesz némi engedményt a territorialitás elvének (a

[375] ABI 1997, 128.

tagállami jog hatályos, ha az adat „feldolgozására” használt eszköz a tagállam területén van), addig a magyar adatvédelmi jog területi hatálya főszabályként akkor állapítható meg, ha az adatkezelés/adatfeldolgozás a Magyar Köztársaság területén történik, míg a 4. § (6) bekezdésében foglalt kivétel az adatfeldolgozó telephelyéhez igazodik.

1.10.11. Az adatfeldolgozó fogalma

1. Az Avtv. szerint „*adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából – beleértve a jogszabály rendelkezése alapján történő megbízást is – személyes adatok feldolgozását végzi” (2. § 16. pont). Az Avtv. 2. § 16. pontja az adatfeldolgozó fogalmát az adatfeldolgozás definíciójából vezeti le. Az adatfeldolgozás fogalma azonban nem határolható el az adatkezeléstől (lásd fent az Avtv. 2. § 15. pontjához fűzött kommentárt), ezért az elhatárolás az adatkezelő fogalmából kiindulva lehetséges. Ennek alapján adatfeldolgozónak minősül az a természetes személy, jogi személy vagy jogi személyiség nélküli szervezet, amely az adatkezelő által meghozott, az adatkezelésre vonatkozó döntéseket az adatkezelő megbízásából végrehajtja, ám ilyen döntéseket nem hozhat [lásd az Avtv. 4/A. § (3) bekezdését], illetőleg az adatkezelés célját nem határozza meg.

2. Az adatfeldolgozó tehát természetes személy, jogi személy vagy jogi személyiség nélküli szervezet lehet (tehát például polgári jogi társaság nem). Az adatfeldolgozó az adatkezelő „megbízásából” végzi tevékenységét, amelyről jogszabály is rendelkezhet. A „megbízás” szó a rendelkezés alkalmazásában nem a polgári jogi megbízást jelenti, hanem az a hétköznapi szóhasználat szerint értelmezendő („valakire ráruházza valamely feladat elvégzésének a kötelességét, illetve jogát”);[376] az adatkezelő és adatfeldolgozó közötti jogviszony tehát lehet vállalkozás is.

1.10.12. Az irányelv vonatkozó rendelkezései

Az irányelv 2. cikk *e)* pontja szerint „feldolgozó az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely személyes adatokat dolgoz fel az adatkezelő nevében”. Az irányelv nem különböztet adatkezelés és adatfeldolgozás között; csak az Avtv.-ben használt „adatkezelés” fogalmával egyenértékű, ám a hivatalos fordításban „adatfeldolgozás”-ként fordított műveletet ismeri. A fenti meghatározás tehát az Avtv. definícióinak alkalmazásával úgy olvasandó, hogy a „feldolgozó az a természetes személy

[376] *Magyar Értelmező Kéziszótár* (Budapest, Akadémiai), 1992, 901.

[stb.], amely személyes adatokat *kezel* az adatkezelő nevében". Az angol fordítás kifejezi azt, hogy az adatfeldolgozó (data processor) – az irányelv rendszerében – bármely adatkezelési (data processing) műveletet végezhet; a német fordítás (Auftragsverarbeiter) pedig utal arra, hogy ez az alany az adatkezelőtől elsősorban abban különbözik – az irányelv rendszerében! –, hogy tevékenységét megbízás alapján végzi. (Az adatfeldolgozó megjelölésére a korai irodalomban felmerült a „másodlagos adatkezelő", „megbízott adatkezelő" fogalom is.)[377]

1.11. Az adatkezelés jogalapja

1. Az Avtv. 3. § (1) bekezdése szerint „személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete elrendeli. Az információs önrendelkezési jog központi eleme fejeződik ki a 3. § (1) bekezdésében, amelyet – a célhoz kötöttség elvére vonatkozó szabályok mellett – az Avtv. legfontosabb szabályának tekinthetünk. A 15/1991. (IV. 13.) AB határozat szerint: „Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek."[378]

A 3. § (1) bekezdés ugyanakkor olyan szabály, amely az Avtv.-vel kapcsolatos alkalmazási nehézségek legtöbbjének – közvetlen vagy közvetett módon – okozója. A rendelkezés szerint a magyar adatvédelmi szabályozás az adatkezelést csak abban a két esetben tekinti jogszerűnek, ha az érintett hozzájárulása rendelkezésre áll, vagy az adatkezelést törvény (illetőleg annak felhatalmazása alapján önkormányzati rendelet) „rendeli el". A törvényi „elrendelés" egyes esetekben – például ha az adatkezelést az érintett létfontosságú érdeke indokolja – magában az Avtv.-ben található.

[377] Például ABI 1997, 50.

[378] Lásd még 46/1995. (VI. 30.) AB határozat; 24/1998. (VI. 9.) AB határozat; 56/2000. (XII. 19.) AB határozat stb.

Az információs önrendelkezési jog fogalmából következően főszabály szerint az adatkezelés jogalapja *az érintett hozzájárulása*. A törvényben meghatározott adatkezelés e felfogás szerint kivétel, amely valamely törvény által kifejezett, társadalmi konszenzus által meghatározott esetben, az Alkotmány szabta keretek között korlátozza az egyén információs önrendelkezési jogát.[379]

Az érintett hozzájárulása akkor érvényes, ha az megfelel a 2. § 6. pontjában írt definíciónak. A hozzájárulás fogalmának elemzéséhez lásd ezért a 2. § 6. pontjához fűzött kommentárt.

2. Értelmezésre szorul, hogy mely esetekben lehet valamely törvény vagy törvény felhatalmazása alapján, az abban meghatározott körben helyi önkormányzati rendelet (a továbbiakban ezen alpontban együttesen: törvény) által adott szabályozást az adatkezelés *„elrendelésének" tekinteni*. Az „elrendelés" szó jelentése („kötelezően előír") alapján ugyanis az az értelmezés adódik, hogy a törvénynek *kifejezett* parancsoló szabályt kell tartalmaznia, amely az adatok kezelését meghatározott célból előírja. Ezt erősíti a 3. § (3) bekezdése is: „Kötelező adatkezelés esetén az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg."

Ezen értelmezéssel szemben áll az az interpretáció, amely szerint az olyan norma, amely az adatkezelést szükségszerűen magában foglaló tárgyat szabályoz, maga is olyan normának minősül, amely a 3. § (1) bekezdés *b)* pontjának értelmezésében „elrendeli" az adatkezelést.

A kifejezett törvényi „elrendelés" kívánalma minden adatkezeléssel járó – különösen az Avtv. elfogadását megelőzően szabályozott – jogintézmény esetén igen nagy terhet róna a jogalkotóra.

Példa lehet minderre az engedményezés intézménye. A Polgári Törvénykönyv 328. § (1) bekezdése szerint: „A jogosult követelését szerződéssel másra átruházhatja." A (3) bekezdés szerint: „Az engedményezésről a kötelezettet értesíteni kell; a kötelezett az értesítésig jogosult az engedményezőnek teljesíteni." Az engedményezéssel az engedményes a régi jogosult helyébe lép. Az engedményezés sikeres lebonyolításához nyilvánvalóan szükséges a követelésre vonatkozó adatok, közöttük a kötelezettre vonatkozó adatok átadása az eredeti jogosult részéről az engedményes részére. Ha a kötelezett természetes személy, ezek az adatok személyes adatnak minősülnek. Az engedményezéshez a kötelezett

[379] Lásd például ABI 1999, 317.

hozzájárulása nem szükséges, vagy hozzájáruláson alapuló adatkezelésről az adott esetben nem lehet szó. Vajon a Ptk. hivatkozott rendelkezései értelmezhetők-e úgy, hogy azok „elrendelik" az engedményezés megtörténtéhez szükséges adattovábbítást?[380]

Álláspontunk szerint a jogalkalmazó által elfoglalt helyes álláspont az lenne (és ezzel az alább hivatkozott két adatvédelmi biztosi állásfoglalás is egybevág), ha az Avtv. előtt törvényi szabályozást nyert jogintézmények esetén a jogintézmény működéséhez nyilvánvalóan szükséges adatkezelést a gyakorlat mint a 3. § (1) bekezdés *b)* pontja alá esőt ítélné meg. Ilyen esetekben azonban fokozottan vizsgálni kell az Avtv. által meghatározott további követelmények (célhoz kötöttség, szükségesség) meglétét.

Figyelemre méltó, hogy a jogalkotó a törvény 8. §-ában az adattovábbítás szabályozásakor a „törvény azt megengedi" fordulatot használja, majd 2003. évi novella esetében is differenciál „elrendelés" és „lehetővé tétel" között. Egyes esetekben [törvény által közérdekből előírt nyilvánosságra hozatal, 3. § (4) bekezdése] a novella szövegével megállapított normaszöveg a korábbiakhoz hasonlóan az „elrendelés" szóval él. Más esetekben [például a külföldre irányuló adattovábbítás módosított szabályozása, 9. § (1) bekezdése] a szabályozás a „lehetővé teszi" megfogalmazást használja. Sajnos a miniszteri indokolás a kérdésre nem tér ki.

Mindezek alapján álláspontunk az, hogy a 3. § (1) bekezdésének *b)* pontjában foglalt „elrendeli" szót „lehetővé teszi" értelemben kell interpretálni az Avtv. alkalmazása során; olyan esetekben azonban, ahol a törvényi rendelkezés nem közvetlenül az adatkezelésről, hanem csupán az adatkezelést szükségképpen feltételező jogintézményről, hatáskör gyakorlásáról stb. szól, fokozottan kell vizsgálni az adatkezelés jogszerűségének megítélése szempontjából releváns további körülményeket.

1.11.1. Az adatvédelmi biztos gyakorlata

1. Az adatvédelmi biztos az „elrendelés" fogalmát kiterjesztően értelmezi. A fenti példában feltett kérdést megválaszolva: az adósság- és követelésbehajtással foglalkozó gazdasági társaságok személyes adatok kezelésének gyakorlatával kapcsolatos adatvédelmi

[380] Az engedményezés esete (ahol tehát az intézmény működése szükségszerűvé teszi az adatkezelést) és a valóban „elrendelésként" minősíthető esetek (ahol jogszabály előírja kötelezően előírja meghatározott adatkör kezelését) között helyezkedik el az a szabályozás, amely felhatalmazást ad az adatkezelésre; például a Ptk. 80. § (2) bekezdése, amely szerint „[k]épmás vagy hangfelvétel nyilvánosságra hozatalához – a nyilvános közszereplés kivételével – az érintett személy hozzájárulása szükséges" – nyilvános közszereplés esetén tehát a képmás vagy hangfelvétel, mint személyes adat, kezelhető.

biztosi ajánlás a követeléskezelés alternatívájaként tárgyalja az engedményezés intézményét, és megállapítja: „Az engedményezésre vonatkozó szabályok lehetővé teszik a természetes személy adósok adatainak átadását. […] Az engedményezés alapján történő adatátadásra is vonatkoznak azonban az Avtv. adatkezelés célhoz kötöttsége elvének szabályai."[381] Hasonlóan ítéli meg az adatvédelmi biztosi gyakorlat a polgári bíróság által az eljárás lefolytatása, a pervezetés során végzett adatkezelést; azonban ebben az esetben is minden eljárási cselekmény végzésénél figyelemmel kell lenni a célhoz kötöttség követelményére.[382]

Az ebben az ügyben követett értelmezés tehát megnyitja az utat a 3. § (1) bekezdés *b)* pontjának olyan értelmezése előtt, amely szerint a jogalkotó meghatározott – adatkezelést szükségszerűen hordozó intézmény törvényi szabályozásával egyben az Avtv. hivatkozott szakaszának is eleget tesz. Ám ezen értelmezésnek is nyilvánvalóan megvannak a határai: a biztos 2003-ban jogellenesnek minősített egy olyan esetet, amelyben egy miniszter általános felügyeleti jogára hivatkozva utasította az alárendeltségében lévő szerveket, hogy azok teljes adatállományukat adják át megőrzésre.[383] Az adott esetben a miniszter általános felügyeleti jogkörével, illetőleg az általa végzendő ellenőrzési feladatokkal indokolta az adatkezelést, amelynek célja tisztázatlan volt. Az adatvédelmi biztos ezt az érvelést nem fogadta el.

1.11.2. Az Alkotmánybíróság gyakorlata

1. Az Avtv. 3. § (1) bekezdésének szabálya azt írja elő a normaalkotó számára, hogy – törvényi felhatalmazás alapján alkotott önkormányzati rendelet kivételével – az adatkezelést csak törvényben rendelhet el.

Az Alkotmány 35. § (2) bekezdése szerint „a Kormány a maga feladatkörében rendeleteket bocsát ki […] A Kormány rendelete […] törvénnyel nem lehet ellentétes." Az Alkotmány 37. § (3) bekezdése szerint: „A Kormány tagjai feladatuk ellátása körében rendeleteket adhatnak ki. Ezek azonban törvénnyel vagy a Kormány rendeletével és határozatával nem lehetnek ellentétesek." A jogalkotásról szóló 1987. évi XI. törvény 1. § (2) bekezdése szerint: „[…] az alacsonyabb szintű jogszabály nem lehet ellentétes a magasabb szintű jogszabállyal". Személyes adat kezelésének kormányrendeletben, miniszteri rendeletben, illetőleg nem törvényi felhatalmazás alapján alkotott önkormányzati rendeletben foglalt elrendelése tehát – mivel az Avtv. 3. § (1) bekezdésébe ütközik – formailag alkotmányellenes.

[381] ABI 2001, 195.

[382] ABI 2004, 77.

2. A személyes adat kezelését elrendelő törvény minden esetben korlátozza az Alkotmány 59. § (1) bekezdésében rögzített személyes adatok védelméhez fűződő alapjogot. Az Alkotmány 8. § (2) bekezdése szerint: „A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg."

Az alkotmányos alapjogok korlátozásának az Alkotmánybíróság gyakorlata szerint *formai* és *tartalmi* követelményei vannak. A formai feltételek egy része a jogalkotási eljárással, az elfogadott jogszabály érthetőségével stb. kapcsolatos (ezek összefoglalva a jogbiztonsággal kapcsolatos követelmények),[384] más része pedig a jogkorlátozó norma jogforrási szintjével. Az alapjogot korlátozó norma tartalmi alkotmányosságának megítélése során az Alkotmánybíróság a korlátozás szükségességét és arányosságát vizsgálja. Az Alkotmánybíróság állandó gyakorlata szerint a személyes adatok védelméhez fűződő jog minden korlátozásának „meg kell felelnie az alapjogi korlátozás mindenkori alkotmányos feltételeinek, azaz az Alkotmány 8. § (2) bekezdésében foglalt követelményeknek. Ez azt jelenti, hogy az információs önrendelkezési jogot, az Alkotmány 59. § (1) bekezdésében biztosított szabadságjogot mint alapjogot csak elkerülhetetlen esetben lehet alkotmányosan korlátozni, akkor ha a korlátozás elkerülhetetlenül szükséges és az a korlátozással elérni kívánt célhoz képest arányos." [46/1995. (VI. 30.) AB határozat, ABH 1995. 223.]

A tartalmi korlátozás alkotmányosságának további feltételét fogalmazta meg az Alkotmánybíróság kifejezetten az információs önrendelkezési jog összefüggésében a 15/1991. (IV. 13.) AB határozatban: „Bármilyen jogszabály, amely – az alkalmazott eljárásra tekintet nélkül – személyes adat felvételéről, gyűjtéséről, tárolásáról, rendezéséről, továbbításáról, nyilvánosságra hozásáról, megváltoztatásáról, a további felhasználás megakadályozásáról, az adatból új információ előállításáról, vagy akármilyen más módon történő felhasználásáról (a továbbiakban: a személyes adat feldolgozásáról) rendelkezik, csak akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra nézve, hogy az érintett személy az adat útját a feldolgozás során követni, és jogait érvényesíteni tudja. Az erre szolgáló jogintézményeknek tehát biztosítaniuk kell az érintett beleegyezését a feldolgozásba, illetve pontos garanciákat kell tartalmazniuk azokra a kivételes esetekre nézve, amikor az adatfeldolgozás az érintett beleegyezése (esetleg tudta) nélkül történhet. E garanciális jogintézményeknek – az ellenőrizhetőség érdekében is – objektív korlátok közé kell

[383] ABI 2003, 217; ABI 2004, 38. skk.

[384] Halmai–Tóth 2003a, 118.

szorítaniuk az adat útját.” [Az információs önrendelkezési jog alkotmányos garanciáiról lásd bővebben az 1. § (1) bekezdését.]

3. Az Alkotmánybíróság *formai okból* minősítette alkotmányellenesnek a következő, a személyes adatok védelméhez fűződő joggal kapcsolatos korlátozásokat:

– A 11/1990. (V. 1.) AB határozatban tárgya egy IM rendelet, amely a törvényi szabályozáson túl további adat (a személyi szám) feltüntetését írta elő a cégbejegyzés kérelmezésekor kitöltendő nyomtatványokon. Az AB szerint: „A személyi szám nyilvános használatának kötelező elrendelése a személyes adat védelméhez fűződő alapvető jog (Alkotmány 59. §) gyakorlásának korlátozása; ilyen tartalmú rendelkezést *miniszteri rendelet nem írhat elő*. A személyi szám közlésének és nyilvánosságra jutásának rendelettel való előírására az igazságügy-miniszternek nem volt törvényes felhatalmazása; a rendelkezés sérti az Alkotmány 8. §-ának (3) bekezdését, illetőleg az Alkotmány 59. §-át, tehát alkotmányellenes.” (Kiemelés tőlem – *J. A.*)

– A 29/1994. (V. 20.) AB határozatban a testület meghatározott személyes adatok kezelésének *rendeletben történő szabályozásáról* foglalt állást. „Az R. mellékletei az igazolvány tartalmául olyan személyes adatok feltüntetését írják elő, amelyek csakis törvényi szabályozás tárgyai lehetnek, figyelemmel az igazolványban feltüntetett személyes adatok felhasználására is. Mivel a formai alkotmányellenesség a köztársasági Alkotmány hatálybalépése után keletkezett, az Alkotmánybíróság gyakorlata alapján az érintett mellékletek megsemmisítését önmagában a formai alkotmányellenesség indokolttá teszi. Az Alkotmány 8. § (2) bekezdése szerint ugyanis alapvető jogokra vonatkozó szabályokat csak törvény állapíthat meg, s annak gyakorlása csak olyan törvényi korlátozásnak vethető alá, amely az alapvető jog lényeges tartalmát nem érinti. A személyi szám használatának kötelező elrendelése a társadalombiztosítás egészségügyi szolgáltatásának igénybevételére jogosító igazolvány felhasználási körében (munkáltató, egészségbiztosítási pénztár, háziorvosi és egyéb egészségügyi szolgálat stb.) a személyes adat védelméhez fűződő alapvető jog [Alkotmány 59. § (1) bekezdése] gyakorlásának korlátozása; ilyen tartalmú rendelkezést kormányrendelet és melléklete nem írhat elő.”

– A 12/1996. (III. 22.) AB határozat *kormányrendeleti szinten szabályozott adatkezelés* alkotmányosságáról foglalt állást. A felsőoktatási intézményekbe való felvételről szóló kormányrendelet egy szabálya elrendelte azt, hogy a jelentkezési laphoz hatósági erkölcsi bizonyítványt kell csatolni (amely a vonatkozó szabályozás szerint a büntetett előéletre utaló különleges adatot is tartalmaz). A rendelet szabályozása alapján az erkölcsi bizonyítvány csatolása a jelentkezés alaki feltétele volt: a felvétellel kapcsolatos tartalmi

összefüggésben nem állt. Az Alkotmánybíróság szerint az Avtv. 3. § (2) bekezdése és 3. § (3) bekezdése alapján kormányrendelet nem írhatja elő különleges adat kezelését, mivel pedig az Alkotmány 35. § (2) bekezdése szerint a Kormány rendelete törvénnyel nem lehet ellentétes, a kormányrendelet szóban forgó rendelkezése alkotmányellenes.

– Az 59/1998. (XII. 11.) AB határozatban az Alkotmánybíróság az egészségügyi hozzájárulásról szóló akkor hatályos törvény végrehajtására kiadott *kormányrendelet* azon szabályozásával kapcsolatban foglalt állást, amely szerint több jogviszonyban álló személy után egy meghatározott foglalkoztatónak kellett a hozzájárulást megfizetnie, az érintettnek pedig a további munkaviszonyaival kapcsolatos – a munkaidőről és/vagy jövedelemről szóló – igazolást kellett ehhez a foglalkoztatóhoz benyújtania; az érintettnek az egészségügyi hozzájárulás fizetését érintő további foglalkoztatásában bekövetkezett változásokat is be kellett jelentenie e meghatározott foglalkoztatónak. Ezzel az egészségügyi hozzájárulást megfizető foglalkoztató értesült a további jogviszonyokról, sőt az azokhoz kapcsolódó egyéb adatokról (jogviszony kezdete, munkaidő, jövedelem) is. Az Alkotmánybíróság formai alkotmányellenességet megállapítva megsemmisítette a rendelkezést: „ebben az esetben a foglalkoztatott a foglalkoztatói irányába az Alkotmány 59. § (1) bekezdése szerinti, személyes adatnak minősülő jövedelemadatok kiszolgáltatására kötelezett, amely az Alkotmány 8. § (2) bekezdése alapján […] törvényi szintű szabályozást igényel. […] A Vhr. 1. § (3)–(4) bekezdései ellentétben állnak továbbá az Avtv. 8. § (1) bekezdésével is, amely az adattovábbításhoz vagy az érintett hozzájárulását, vagy törvényi szintű szabályozást kíván meg. Jelen esetben az érintett nincs abban a helyzetben, hogy hozzájárulásának megadása felől szabadon dönthetne, a Vhr. 1. § (3)–(4) bekezdései alapján a más jogviszonyával kapcsolatos adatokat, ezekben bekövetkezett változásokat a foglalkoztatóinak köteles kiszolgáltatni."

– A 25/2002. (VI. 21.) AB határozatban a testület a személyes gondoskodást nyújtó szociális ellátások térítési díjairól szóló kormányrendelet szabályozását vizsgálta. A rendelet úgy határozott meg egy jövedelemnyilatkozat benyújtására alkalmazott formanyomtatványt, hogy az a szociális ellátásról szóló törvényben meghatározott adatkörön túl is tartalmazott – vagyonra vonatkozó – adatot. Az Alkotmánybíróság a kormányrendeleti szintű szabályozást – mint törvénnyel ellentéteset, és így az Alkotmány 37. § (3) bekezdésébe ütközőt – megsemmisítette. A 27/2002. (VI. 28.) AB határozat azért semmisített meg egy miniszteri rendeletet, mert az – kötelező AIDS szűrővizsgálatra kötelezettek körét meghatározva, sőt a fertőzött személy veszélyeztetett környezetének, szexuális partnereinek felkutatását előírva – más jogok mellett az információs önrendelkezési jog „jelentős és közvetlen" korlátozását írta

elő. Az AB megállapította azt is, hogy a miniszteri rendelet alkotására szóló felhatalmazás alapvető jogok és kötelességek szabályozását engedi, ami ellentétes a jogalkotásról szóló 1987. évi XI. törvény 15. § (2) bekezdésével.[385] A szabályozás tehát mind az Alkotmány 8. § (2) bekezdését, mind – mivel a jogalkotási törvénybe ütközött – a 37. § (2) bekezdését sértette. A döntéshez csatolt különvélemény szerint a szabályozást az Alkotmánybíróságnak nem kellett volna megsemmisítenie, mert az „a törvény gyakorlati végrehajtása szabályaira irányul, további korlátozást nem tartalmaz". A döntés jelentősége abban áll, hogy meghozatala idején még nem szerepelt az Avtv. szövegében a 3. § (3) bekezdés, amely szerint a kezelendő adatok körét minden esetben az elrendelő törvény vagy önkormányzati rendelet határozza meg [lásd részletesebben a 3. § (3) bekezdést] – ám már a 15/1991. (IV. 13.) AB határozat rögzíti, hogy a kezelt adatok körének rendeletben történő meghatározására vonatkozó felhatalmazás alkotmányellenes.

– A 38/2003. (VI. 26.) AB határozattal az adatvédelmi biztos indítványára az Alkotmánybíróság megsemmisítette azt a PM rendeletet, amely előírta, hogy az eladó – meghatározott mennyiséget vagy értéket elérő termékértékesítés esetén – köteles az áfatörvényben meghatározott (és a vevő [átvevő, megrendelő] nevét és címére is kiterjedő) adattartalommal. Az AB szerint a szabályozás rendeleti szinten ír elő kötelező adatkezelést, így az Avtv. 3. § (1) bekezdésébe ütközik, vagyis sérti az Alkotmány 37. § (3) bekezdését. A testület megítélése szerint a rendelet az áfatörvényben foglalt egyik felhatalmazó rendelkezést is sértette; az Alkotmány 37. § (3) bekezdésébe ütközés megállapítása után az AB már nem vizsgálta, hogy a szóban forgó szabályozás sérti-e az 59. § (1) bekezdését.[386]

– Az 50/2003. (XI. 5.) AB határozat megsemmisített egy – személyes adatok kezelését végző – vizsgálóbizottság felállításáról rendelkező *országgyűlési határozatot*. Az alkotmányellenességet a testület az Alkotmány 2. § (1) bekezdése és 8. § (2) bekezdése alapján mondta ki, így nem vizsgálta az Alkotmány 59. §-ához való viszonyt. A határozat szerint az Országgyűlés mulasztásban megnyilvánuló alkotmányellenességet idézett elő azzal,

[385] A felhatalmazás szerint – amelyet nem is a törvény (az egészségügyről szóló 1972. évi II. törvény), hanem annak végrehajtási rendelete [16/1972. (IV. 29.) MT rendelet] tartalmazott – „Felhatalmazást kap a népjóléti miniszter, hogy a lakosság egészségének védelme érdekében […] egyes betegségekre bejelentési kötelezettséget állapítson meg, ezzel kapcsolatban meghatározza a bejelentésre kötelezettek körét, a bejelentés idejét és módját, valamint a bejelentendő adatokat."

[386] Az alkotmánybírósági döntés előzményeiről lásd ABI 2004, 43.

hogy nem biztosította törvényi szabályozással, hogy az országgyűlési bizottságok vizsgálatai során érvényesüljenek a személyes adatok védelmének követelményei.[387]

– A 47/2003. (X. 27.) AB határozatban a testület a bűnmegelőzési ellenőrzésre vonatkozó jogi szabályozás vizsgálata során mondta ki azt, hogy az intézménnyel kapcsolatos egyes adatkezeléseknek *belső utasításban* való szabályozása az Alkotmány 59. § (2) bekezdésébe ütközik.

4. *Nem* állapított meg az Alkotmánybíróság *formai* alkotmánysértést például a következő esetekben:

– Az 54/2000. (XII. 18.) AB határozat tárgya olyan, rendeleti szintű szabályozás volt, amely *névkitűző viselését* tette kötelezővé egyes, a belügyminiszter irányítása alá tartozó szervezetek hivatásos és szerződéses állományába tartozó személyek számára. A szabályozás szerint: „A hivatásos és szerződéses állományviszonnyal rendelkező rendőr-, határőr-, illetve a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság szervezetében szolgálatot teljesítő tűzoltó-, valamint polgári védelmi tábornok, főtiszt, tiszt, zászlós és tiszthelyettes (a továbbiakban: igényjogosultak) a társasági, illetve a köznapi öltözetén névkitűzőt visel."

Az Alkotmánybíróság szerint az adott esetben az információs önrendelkezési jog korlátozása már törvényi szinten megtörtént: a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló törvény rendelkezése szerint „a fegyveres szerv megnevezését, a hivatásos állomány tagja nevét, továbbá a beosztására, rendfokozatára és kitüntetésére vonatkozó adatot a hivatásos állomány tagja beleegyezése nélkül nyilvánosságra lehet hozni"; a szerződéses jogviszonyban álló személyekkel kapcsolatban pedig érvényesül az Avtv. 19. § (2) bekezdésében foglalt azon rendelkezés, amely szerint az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szervek „hatáskörében eljáró személyek neve, beosztása vagy besorolása és munkaköre – ha törvény másként nem rendelkezik – bárki számára hozzáférhető, nyilvános adat". Az Alkotmánybíróság szerint az „érintett szervek […] hivatásos és szerződéses állományú tagjai információs önrendelkezési jogának korlátozása a név, valamint a beosztására, rendfokozatára és kitüntetésére vonatkozó adat tekintetében már az Avtv. és a Hszt. idézett rendelkezésével megtörtént. A Rendelet csupán az alapjog-korlátozás részletszabályait tartalmazza." Az Alkotmánybíróság hivatkozik a 64/1991. (XII. 17.) AB határozatra, amely szerint az alkotmányos jogok „csupán távolról, közvetetten érintő, technikai és nem korlátozó jellegű" szabályozása rendeleti szinten is történhet. „Az alapjog-korlátozás […] valójában törvényi

[387] Lásd még ABI 2004, 36.

szinten történt meg, ezért a részletszabályok törvényi felhatalmazáson alapuló rendeleti előírása alkotmányossági szempontból nem kifogásolható." A testület ezek után vizsgálta magának a névkitűző viselésével történő „nyilvánosságra hozatalnak" mint korlátozásnak a szükségességét és arányosságát is (lásd alább). (Álláspontunk szerint azzal, hogy az AB adott esetben nem magának a nyilvánosságra hozatalnak, hanem a névkitűző viselésével történő nyilvánosságra hozatalnak tartalmi alkotmányosságát vizsgálta a továbbiakban, maga is implikálta, hogy a vonatkozó szabályozás nem csupán technikai jellegű. A vizsgálatnak vagy csupán a nyilvánosságra hozatal tartalmi alkotmányosságára kellett volna kiterjednie, vagy meg kellett volna állapítani a rendeleti szabályozás formai alkotmányellenességét.)

– Az 56/2000. (XII. 19.) AB határozatban az Alkotmánybíróság az akkor hatályos egészségügyről szóló törvény végrehajtásáról szóló MT rendelet azon szabályainak alkotmányosságát vizsgálta, amelyek előírták, hogy vélelmezni kell a beteg hozzájárulását egészségügyi dokumentációja átadásához, ha az általa választott háziorvos feladatait annak körzetében (rendelőjében) időlegesen vagy véglegesen más háziorvos látja el, illetőleg ha a települési önkormányzat a körzethatárokat módosítja, és az érintett a módosítás következtében új körzet ellátási területéhez tartozik.

Az Alkotmánybíróság szerint az az előírás, amely a hozzájárulást a helyettesítő orvosnak történő továbbítás esetén vélelmezi, alkotmányos. Az érvelés szerint ebben az esetben a vizsgált rendelkezés „nem minősül az egészségügyi állapottal összefüggő adatok továbbítását előíró rendeleti szabálynak", mivel az csak az Eüatv.-ben, tehát törvényi szinten megfogalmazott szabályok „meghatározott esetben való alkalmazását fogalmazza meg". Az Eüatv. hivatkozott rendelkezései szerint „a betegellátót […] a titoktartási kötelezettség azzal a betegellátóval szemben is köti, aki az orvosi vizsgálatban, a kórisme megállapításában, illetve a gyógykezelésben vagy műtétnél nem működött közre, kivéve, ha az adatok közlése a kórisme megállapítása vagy az érintett további gyógykezelése érdekében szükséges", és „[az Eüatv.] 4. § (1) bekezdése szerinti célból történő adatkezelés és adatfeldolgozás esetén az egészségügyi ellátóhálózaton belül az egészségügyi és személyazonosító adatok továbbíthatók, illetve összekapcsolhatók". A körzethatár-változás esetén érvényesülő vélelem rendeleti szabályozását azonban az AB alkotmányellenesnek minősítette, mivel az az egészségügyről szóló törvény önrendelkezési jogot és a személyes adatok védelméhez fűződő jogot érvényre juttató rendelkezéseivel ellentétes: „Az Alkotmánybíróság szerint önmagában a körzethatárok szükségessé váló módosítása nem teszi indokolttá, hogy azok az állampolgárok, akik már választottak háziorvost, a jogszabály erejénél fogva más

háziorvoshoz kerüljenek át. Ilyenkor ugyanis […] a választott háziorvos ellátja feladatait, ezért az orvos és betege közötti kapcsolattartást semmi sem akadályozza."[388]

– Az 57/2003. (XI. 21.) AB határozatban az Alkotmánybíróság *önkormányzati rendeletben* foglalt adatvédelmi szabályozás alkotmányosságáról foglalt állást. Mivel a szóban forgó – az önkormányzat tulajdonában álló, nem lakás céljára szolgáló helyiségek bérbeadásának feltételeiről szóló – önkormányzati rendelet megalkotása törvényi felhatalmazáson alapult, az Alkotmánybíróság a megsemmisítésre irányuló indítványt elutasította.

5. *Tartalmi alkotmányellenességet állapított meg* az Alkotmánybíróság például a következő adatvédelmi tárgyú esetekben:

– A 20/1990. (X. 4.) AB határozatban a testület olyan törvényi rendelkezés alkotmányellenességét állapította meg, amely a pártok és társadalmi szervezetek országos vezetőit vagyonnyilatkozat tételére kötelezte. A határozat indokolása szerint: „Az Alkotmány 8. §-ának – az 1990. évi XL. törvény 51. §-ának (1) bekezdése által időközben hatályon kívül helyezett – (3) bekezdése az 1990. évi III. törvény elfogadásának idején az alapvető jogok gyakorlásának csak olyan korlátozását tette lehetővé, amely az állam biztonsága, a belső rend, a közbiztonság, a közegészség, a közerkölcs vagy mások alapvető jogainak és szabadságának védelme érdekében szükséges. A »jelenleg működő pártok és társadalmi szervezetek országos vezetői« esetében, akik állami funkciókat nem töltenek be, az Alkotmányban felsorolt célok egyike sem indokolta a magántitkaik és személyes adataik védelméhez fűződő alapvető joguk korlátozását. […] A törvényalkotó, amikor az állami funkciót betöltők körén kívüli személyekre is kiterjesztette a vagyonnyilatkozat-tételi kötelezettséget, kényszerítő ok nélkül korlátozta az Alkotmány 59. §-ában biztosított jogokat, és ezzel az alapjog *lényeges tartalmát korlátozta.* A rendelkezés nem felel meg az alapjogot korlátozó normákkal szemben támasztott arányosság feltételeinek sem. Ez ugyanis megköveteli, hogy az elérni kívánt cél fontossága és az ennek érdekében okozott alapjogsérelem súlya összhangban legyen egymással. A törvényhozó a korlátozás során köteles az adott cél elérésére alkalmas legenyhébb eszközt kiválasztani. Ha az alkalmazott korlátozás a *cél elérésére alkalmatlan,* az alapjog sérelme megállapítható.

– *Tartalmi alkotmányellenességet* állapított meg az Alkotmánybíróság a döntő jelentőségű és ezért többször említett 15/1991. (IV. 13.) AB határozatban.

[388] Az ügyet korábban vizsgálta az adatvédelmi biztos is, lásd ABI 2000, 243.

– A 46/1995. (VI. 30.) AB határozat szerint alkotmányellenes – mint „*nem elkerülhetetlenül szükséges és aránytalan alapjogi korlátozás”* – a személyazonosító jel használatának időbeli kiterjesztése, az azt elrendelő törvényben meghatározott cél („a külső és belső gazdasági-pénzügyi egyensúlyi helyzet javítása és a tartós gazdasági növekedés feltételeinek kibontakoztatása”) nem indokolja kellőképpen az alapjogi korlátozást. A határozatban az Alkotmánybíróság alkotmányellenesnek nyilvánította azt a rendelkezést is, amely a személyazonosító jel használatára jogosultak alanyi körét terjesztette volna ki, és módot adott volna arra, hogy ezek az adatkezelők a személyazonosító jelet mind az egymással, mind a népesség-nyilvántartással történő kapcsolattartás során felhasználják. „Az Avtv. 11–16. §-ai szerint az érintett tájékoztatást kérhet személyes adatainak kezeléséről, arról, hogy kik és milyen célból kapták meg személyes adatait, az adatvédelmi nyilvántartásba betekinthet, az adattovábbításra vonatkozó nyilvántartásról tájékoztatást kérhet stb. Az Avtv. 8. § (1) bekezdése pedig úgy rendelkezik, hogy az adatok csak akkor továbbíthatók, valamint a különböző adatkezelések csak akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy külön törvény azt megengedi, feltéve, ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. A támadott törvényi felhatalmazás ez utóbbi feltételnek, garanciális követelménynek nem felel meg, mert lehetővé teszi az adatállományok olyan összekapcsolását, ahol az adat útja már nem követhető, ezzel pedig az adatalany alkotmányos jogérvényesítését akadályozza. Az adattovábbításra és adatszolgáltatásra vonatkozó törvényi rendelkezés csak akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra nézve, hogy az érintett személy az adata útját követni tudja, és jogainak érvényesítésére lehetősége van. A vizsgált törvényi rendelkezés – összefüggésben a Gst. [a gazdasági stabilizációt szolgáló egyes törvénymódosításokról szóló 1995. évi XLVIII. törvény] 146. §-ában és 151. §-ában meghatározott szabályokkal – azonban ezekre a követelményekre nézve nem tartalmaz megfelelő garanciákat. Az adatok összekapcsolására vonatkozó törvényi felhatalmazás pedig lehetővé teszi, hogy az érintett személyi adatait mind az állami, mind az önkormányzati, mind pedig a nem állami szféra – sőt eshetőlegesen a természetes személyek is – akadálytalanul használhassák. […] Ezáltal az érintettekről kialakulhat a valóságnak csak részben megfelelő személyiségprofil, melynek alapján az adatfeldolgozó döntéseit meghozza, s amely az érintettet a megnövekedett hatalmú államigazgatással szemben kiszolgáltatottá teszi.” A „határtalanná vált” adatfeldolgozás és adatáramlás így sérti a célhoz kötöttség alkotmányos követelményét. A testület „nem talált olyan alkotmányos jogot vagy érdeket, amely az Alkotmány 59. §-ában garantált információs önrendelkezéshez való jognak a fentiek szerint az Nytv. [a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992.

évi LXVI. törvény] módosításából szükségképpen folyó korlátozását elkerülhetetlenné" tette volna, vagy azt sérelemmel arányossá tenné, ezért a rendelkezéseket megsemmisítette.

6. *Nem* állapított meg a *tartalmi alkotmányellenességet* a bíróság az alábbi esetekben:

– Az 58/1995. (IX. 15.) AB határozatban a testület *alkotmányosnak* mondta ki azt, hogy az akkor hatályban lévő büntetőeljárási törvény (Be.) rendelkezése szerint a terhelt elmeállapotáról készült szakvéleményt, illetve a szakértő véleményét az eljárás szereplői és a nyilvános tárgyaláson bárki megismerhette. Az AB szerint a terhelt elmeállapotával kapcsolatos különleges adatnak az eljárás szereplői általi megismerését indokolja a hatóság tagjai esetében az állam büntetőigényének érvényesítése, a további eljárási szereplők esetében pedig eljárási funkcióik betöltése. Az e körön kívüli megismerés lehetőségét korlátozza az, hogy bíróság a tárgyalásról vagy annak egy részéről a nyilvánosságot kizárhatja. „Nem alkotmányellenes az, hogy a törvény a bíróságra bízza az egymással esetleg konkuráló alapelvek között az elsődlegesség eldöntését. Felnőttkorú terhelt ellen folyó eljárásban a határozat nyilvános kihirdetése – nemzetközi kötelezettségeinkre tekintettel is – elkerülhetetlen, de a bíróságnak módja van arra, hogy ennek során is figyelemmel legyen a személyes adat védelmére."

– Az Alkotmánybíróság a 876/B/1996. sz. határozatával elutasította az 1995. évi CXIX. törvény (az ún. direktmarketing-törvény) azon szabályainak megsemmisítésére irányuló indítványt, amelyek a DM-cégeknek lehetőséget adnak a központi népesség-nyilvántartásból, illetőleg egyes más adatforrásokból történő adatigénylésre. Bár ebben az esetben kétséges a korlátozás alkotmányos céljának fennállása, az AB szerint „a támadott jogszabályok esetében a Tv. a személyes adatok felhasználásának célját és az adatfelhasználás garanciális szabályait meghatározta. Ezért az Alkotmánybíróság a Tv. 3. § (1) bekezdés *d)* pontja és 4. §-a alkotmányellenességének megállapítására és megsemmisítésére vonatkozó indítványt elutasította."

– A 30/1997. (IV. 29.) AB határozat tárgya a képviselők jogállásáról szóló törvény módosítása. A szóban forgó rendelkezések szerint a képviselőnek be kell jelentenie a törvényben felsorolt, összeférhetetlenség alá nem eső munka- és tagsági viszonyokat, valamint megbízatásokat, továbbá az ezzel kapcsolatban szerzett jövedelmet az Országgyűlés elnökének; tovább vagyon-, jövedelem- és gazdaságiérdekeltség-nyilatkozatot kell tennie, amelynek kivonata nyilvánosságra kerül. *Az AB szerint a szabályozás annak céljához – a képviselők vagyoni viszonyai átláthatóságának és ellenőrizhetőségének biztosításához – szükséges mértékben, arányosan korlátozza az érintettek információs önrendelkezési jogát.* Az indítvány kifogásolta azt is, hogy a törvény nem szabályozza az adatkezelés rendjét, nem

biztosított a szolgáltatott személyes adatok védelme – az AB szerint azonban az adatokat kezelő országgyűlési bizottságra is vonatkoznak az Avtv. szabályai, így ez az érvelés megalapozatlan. A testület a vagyonnyilatkozat kivonatának nyilvánosságra hozatalával kapcsolatban állapított meg alkotmányellenességet: a 60/1994. (XII. 24.) AB határozatban megalapozott gyakorlat szerint a közérdekű adatok megismerésének joga elsőbbséget élvez a közhatalmat gyakorlók, politikai közszereplést vállalók olyan személyes adatainak védelmével szemben, amelyek köztevékenységük megítélése szempontjából jelentősek lehetnek, a kivonat nyilvánosságra hozatala átláthatóvá, ellenőrizhetővé teszi a képviselők vagyoni és érdekeltségi viszonyait, ezáltal növeli az Országgyűlés tevékenységébe vetett bizalmat. A testület szerint: „A képviselők tevékenységének átláthatósága és tájékozott megítélése szempontjából nem minősül szükségtelen és aránytalan alapjogi korlátozásnak az, hogy a törvényben meghatározott adatokra nézve a közérdekű adatok nyilvánosságának alkotmányos elve érvényesül." Az AB nem fogadta el azt az érvet sem, hogy a bejelentés és a nyilatkozattétel kötelezettsége a célok elérésére alkalmatlan eszközök, mivel „ha a képviselő ellen összeférhetetlenségi eljárás indul, a Mentelmi, összeférhetetlenségi és mandátumvizsgáló bizottságnak módjában áll ellenőrizni az adatok valósságát".

– A 24/1998. (VI. 9.) AB határozatban az Alkotmánybíróság a pénzmosás megelőzéséről és megakadályozásáról szóló törvény és végrehajtási rendelete egyes rendelkezéseinek alkotmányosságával kapcsolatban foglalt állást. A támadott rendelkezések szerint a pénzügyi szolgáltató szervezet köteles kijelölni egy vagy több személyt, akik az alkalmazottaktól érkezett, pénzmosás gyanújával kapcsolatos bejelentést továbbítják az ORFK részére. A bejelentés eljárási rendjét és a bejelentés kapcsán keletkezett adatok kezelésének módjával kapcsolatos szabályokat a törvény által előírt iránymutatások és mintaszabályzatok alapján elkészítendő belső szabályozás tartalmazza. A testület szerint a banktitok továbbítása az ORFK számára a bűnmegelőzés érdekében történik, „amely az Alkotmány 2. § (1) bekezdéséből, azaz a jogállamiságból következő alkotmányi cél, így a pénzmosás megelőzése érdekében az ORFK felé a banktitok felfedése alkotmányosan indokolt és szükséges lehet, ha egyébként nem érinti az alapjog lényeges tartalmát". A vonatkozó szabályozás emellett rögzíti a lényeges garanciális követelményeket is (a pénzügyi szolgáltató a bejelentéssel kapcsolatos körülményekről harmadik személynek tájékoztatást nem adhat, az ORFK a kapott információt – más büntetőeljárás esetét kivéve – kizárólag a pénzmosás elleni küzdelem céljaira használhatja fel). Mindennek alapján a testület szerint a szabályozás „*az információs önrendelkezési alapjogot az elkerülhetetlen és arányos*

korlátozás mértékén túl nem korlátozza, így maga a korlátozás nem érinti az Alkotmány 8. § (2) bekezdése szerint az alapjog lényeges tartalmát".

– Az 54/2000. (XII. 18.) AB határozatban a testület alkotmányosnak minősítette azt a szabályozást, amely a belügyminiszter irányítása alá tartozó szervezetek hivatásos és szerződéses állományába tartozó személyeket – a nyilvánosságra hozatal meghatározott módjaként – névkitűző viselésére kötelezte. Az AB szerint „az állampolgárok jogainak hatékony védelme érdekében szükséges az, hogy az állam nevében közhatalmat gyakorlók személyének azonosítása, a vele szemben intézkedő hivatalos közeg „egyediesítése" az állampolgár által könnyen elvégezhető legyen", „Az állampolgár panaszhoz, jogorvoslathoz való joga ugyanis csak így garantálható". Az arányosság kérdésében a testület úgy foglalt állást, hogy „*a legitim cél*, az állampolgárok jogainak hatékony megóvása, bármilyen könnyen felismerhető egyedi azonosító jel (például név, szám) alkalmazásával elérhető. A megfelelőbbnek, célszerűbbnek tekintett módszer kiválasztása a jogalkotó hatáskörébe tartozik. Az alkotmányos célnak egyaránt megfelelő módszerek közötti választás nem alkotmányossági kérdés." Az AB nem vizsgálta az arányosság körébe a legkevésbé korlátozó móddal kapcsolatos követelményt, a nyilvánosság egyes „szintjeit".

– A 16/2001. (V. 25) AB határozatban az Alkotmánybíróság a C típusú nemzetbiztonsági ellenőrzéshez hozzájáruló személy házastársának nyilatkozatára vonatkozó szabályozást vizsgálta. A vizsgálat alapján úgy foglalt állást, hogy a házastárs hozzájáruló nyilatkozata az ellenőrzés lefolytatásának nem feltétele, annak jogkövetkezménye nincs, vagyis az ellenőrzés során a házastársra vonatkozó személyes adatokat a nemzetbiztonsági szolgálatokról szóló törvényben foglalt felhatalmazás alapján kezelik. Az AB szerint: „Az ellenőrzés – és ezen belül a házastársra vonatkozó adatok ellenőrzésének – törvénybe foglalt célja annak megállapítása, hogy a jelölt megfelel-e az állami élet és a nemzetgazdaság jogszerű működéséhez szükséges nemzetbiztonsági feltételeknek. A cél eléréséhez elkerülhetetlen eszköz alkalmazását jelenti a házastársra vonatkozó adatok ellenőrzése, tehát a korlátozás szükséges jellegű. […] A személyes adatok védelmének korlátozása arányos, mert a nemzetbiztonsági szolgálatok az adott cél eléréséhez feltétlenül szükséges, ugyanakkor […] az érintett személyiségi jogait legkevésbé korlátozó eszközt kötelesek igénybe venni, továbbá a titkos információgyűjtés módszereit és eszközeit jogszerűen csak akkor alkalmazhatják, ha az Nbtv.-ben meghatározott feladatok ellátásához szükséges adatok más módon nem szerezhetők be. […] Mivel *az alapjog-korlátozás célhoz kötött, szükséges és arányos,* ezért nem állapítható meg az Alkotmány 8. §-a (1)–(2) bekezdésének megsértése. Ezért az Alkotmánybíróság az indítványt e vonatkozásban elutasítja."

– A 35/2002. (VII. 19.) AB határozatban az Alkotmánybíróságnak a sporttörvény azon rendelkezéseivel kapcsolatban kellett állást foglalnia, amelyek a sportrendezvényt szervezők számára a részvevők személy- és vagyonbiztonsága céljából a helyszín kamerás megfigyelését írta elő, valamint szabálysértési és büntetőeljárás megkönnyítése céljából felhatalmazta a szervezőt arra, hogy a rendezvény résztvevőit kamerával „vagy más úton" rögzítse, és a felvételeket 30 napig tárolja. E nyilvántartásból a szabályozás szerint adatokat igényelhettek „az azonos vagy hasonló jellegű" sportrendezvényt szervezők is.

Az Alkotmánybíróság többségi határozata nem elemzi külön a megfigyelésre, illetőleg a rögzítésre vonatkozó szabályozást. A testület alkotmányosnak fogadta el azokat a rendelkezéseket, amelyek felhatalmazzák a szervezőt szabálysértés vagy büntetőeljárás lefolytatásának megkönnyítése céljából a sportrendezvény résztvevőinek kamerával vagy más úton történő rögzítésére, a felvételek harminc napig történő tárolására, a nézők egyedi azonosítására alkalmas biztonsági beléptetési és ellenőrző rendszer alkalmazására, valamint a sportrendezvény látogatásától eltiltott személyek nyilvántartására. (E nyilvántartásban a szabályozás szerint az azonosító adatokon túl a személyleírás is szerepel.) Az AB szerint „a néző kamerával történő megfigyelésére és e megfigyelés eredményének rögzítésére a személyi és vagyonbiztonságot veszélyeztető, valamint a rasszista, gyűlöletkeltő magatartások megelőzése, megakadályozása érdekében, vagyis más alapjog – így az emberi élet, méltóság és egészség – megóvása és alkotmányos értékek védelme érdekében kerül sor. Az Avtv. 16. §-a is utal arra, hogy az érintett jogait törvény – egyéb, nevesített okok mellett – a bűnmegelőzés, a bűnüldözés érdekében, valamint az érintett vagy mások jogainak védelme érdekében korlátozhatja." Mindennek alapján „a sportrendezvények helyszínén az ún. kamerarendszer alkalmazására és az eltiltott nézők nyilvántartására vonatkozó szabályozása korlátozza ugyan a néző információs önrendelkezési jogát, de – tekintettel a korlátozást tartalmazó rendelkezéssel védeni kívánt célokra – nem minősül a néző információs önrendelkezési joga szükségtelen és aránytalan korlátozásának, s ezért nem alkotmányellenes." Az Alkotmánybíróság a szervező által vezetett nyilvántartás szabályozását is alkotmányosnak minősítette, mert az meghatározott alanyi körre vonatkozik (csak a sportrendezvény látogatásától eltiltott személyekre), csak meghatározott célból ír elő adatkezelést (szabálysértési vagy büntetőeljárás lefolytatásának céljából), valamint meghatározza az adatok törlésének határidejét is (30 napban). „Az Stv. [a sportról szóló 2000. évi CXIV. törvény] vázolt szabályozása szerint ugyanis a sportesemény szervezője által megvalósított adatkezelés alkotmányosan védett célhoz, a közrend, a közbiztonság védelméhez köthető; az érintett az adatkezelésről értesül, a rögzített adatok átadása a

nyomozó hatóságok számára pedig törvényi szabályozásban megengedett, ugyanakkor az adat útja az érintett által ebben a vonatkozásban követhető. Mindezek alapján az Alkotmánybíróság az Stv. […] eljárás alá vont szabályozásait a célhoz kötöttség követelményére tekintettel nem minősítette az információs önrendelkezési jog sérelmének."

A testület ugyanakkor megállapította annak a rendelkezésnek az alkotmányellenességét, amely szerint a „rögzített felvételeket, valamint […] nyilvántartásból adatot – a külön jogszabályban meghatározott állami szerveken kívül – az érintett személy és az azonos vagy hasonló jellegű sportrendezvényt szervező igényelhet. Az érintett kérelmére történő adatközlésre a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 12. §-ának (1) bekezdését megfelelően alkalmazni kell." A szabály az AB szerint azért alkotmányellenes, mert valamennyi nézőre vonatkozóan felhatalmazást ad az azonos vagy hasonló sporteseményt szervezőknek is az adattovábbításra. Ez a „rendelkezés – a jogalkotó szándéka szerint feltehetően – a rendbontás elkerülését szolgáló, az esetleges, jövőbeni veszélyt elhárító, megelőző intézkedések körébe tartozik. Az Alkotmánybíróság álláspontja szerint kizárólag csak a tényleges és a közvetlen, s nem az eshetőleges veszély értelmezhető a célhoz kötöttség követelményét kielégítő alkotmányos ismérvként. A vizsgált rendelkezés alkotmányossági szempontból indokolhatatlan, mivel nemcsak a sportrendezvény látogatásától már eltiltott személyekről készített felvételek átadását teszi lehetővé, s az ilyen személyes adatnak minősülő felvételek átadása az adatvédelemre vonatkozó garanciáik hiányában az azonos vagy hasonló jellegű sportrendezvényt szervezők számára is lehetséges. A sérelmezett szabályozás ezáltal egy távoli, elvont veszély elhárítására irányul, és ennek érdekében ír elő ún. »készletre« történő adatkezelést, s nem tartalmaz kellő alkotmányos garanciákat."

Kiss László és Kukorelli István alkotmánybírák különvéleményükben úgy foglaltak állást, hogy a vizsgálatot a törvény végrehajtási szabályaira is indokolt lett volna kiterjeszteni. Az információs hatalom kiterjesztésének veszélyeit és a ebben a megfigyelés, közelebbről a sportrendezvényeken történő kamerás megfigyelés szerepét alaposan feldolgozó különvéleményben a két alkotmánybíró a vizsgált szabályozással kapcsolatban úgy foglal állást, hogy az abban foglalt jogkorlátozás nem szükséges: „a törvény nem határolja körül azokat a sportrendezvényeket, amelyek olyan rendkívüli kockázattal járnak, ami elengedhetetlenné tenné a kamerázást. […] Másrészt, a […] külföldi tapasztalatokra hivatkozva azt mondhatjuk, hogy még a legnagyobb nézőszámot vonzó sportrendezvények esetében is vannak más, alapvető jogot nem vagy kevésbé korlátozó eszközök a személyi- és vagyonbiztonság védelmére. Megfelelő színvonalú sportlétesítmények (csak ülőhelyek

létesítése, riválisszurkolótáborok elkülönítése, kerítések lebontása stb.), felkészült rendezőapparátus, a nézők tájékoztatása és kiszolgálása, valamint szükség esetén a rendőrség segítségnyújtása mellett nincs kényszerítő szükség arra, hogy a szervezők a sportrendezvény helyszínét és résztvevőit folyamatosan kamerával figyeljék és a felvételeket rögzítsék." Kis és Kukorelli szerint alkotmányellenes az a rendelkezés is, amely szabálysértési vagy büntetőeljárás lefolytatásának megkönnyítése céljából hatalmazza fel a szervezőt felvételek készítésére és rögzítésére. A két alkotmánybíró szerint e rendelkezések mögött az a jogalkotó feltételezés húzódhat, hogy „a kötelező kamerás felvétel alkalmazása körébe tartozó sportrendezvények teljes ideje alatt közbiztonsággal kapcsolatos absztrakt veszély van. Tehát nem arról van szó, hogy akkor készülnek felvételek mások személy- és vagyonbiztonsága vagy a szervező magánérdekeinek biztosítása érdekében, amikor ezek az érdekek konkrét veszélynek vannak kitéve, hanem ilyen veszélyhelyzet hiánya esetén is a sportrendezvény teljes időtartama alatt." A különvélemény utal arra, hogy a felvételek készítése és rögzítése nem más, mint bizonyítékok gyűjtése, ez pedig a nyomozó hatóság feladata – ám még a rendőrségről szóló törvény is csak a „rendőrség mint közhatalmat gyakorló szerv konkrét esetben történő intézkedési feladatához köti az intézkedés szempontjából fontos körülményről történő felvételkészítést". További szempont, hogy a szabályozás egy magánjogi viszony egyik alanyára testál közhatalmi feladatot. Összességében a különvélemény megfogalmazói nem látják bizonyítva a szabályozás alapjául szolgáló absztrakt veszély fennállását, és álláspontjuk szerint „nincs kényszerítő szükség a szabálysértési és büntetőeljárások lefolytatásának megkönnyítését célzó sporttörvényi szabályozásra". A szóban forgó rendelkezések a különvélemény szerint nemcsak az információs önrendelkezési jogot sérti, hanem az Alkotmány azon szakaszát is, amely a rendőrség alapvető feladata a közbiztonság védelme: „jelen esetben nincs kényszerítő szükség magánszervezetek felhasználására az állam büntető igényének érvényesítéséhez".[389]

1.11.3. Az irányelv vonatkozó rendelkezései

Az irányelv 7. cikke („Az adatfeldolgozás jogszerűvé tételére vonatkozó kritériumok) az alábbiak szerint szól:

„A tagállamok rendelkeznek arról, hogy a személyes adatok csak abban az esetben dolgozhatók fel, ha:

[389] Ezen határozat érdekessége még a személyes adat fogalmáról és személyes adatok védelmének terjedelméről Harmathy Attila által párhuzamos indokolásában kifejtett álláspont. Lásd erről a 2. § 1. pontjához fűzött

a) az érintett ahhoz egyértelmű hozzájárulását adta; vagy

b) az adatfeldolgozás 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 adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges; vagy

d) feldolgozásuk az érintett létfontosságú érdekei védelméhez szükséges; vagy

e) az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges, vagy

f) az adatfeldolgozás az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek az 1. cikk (1) bekezdése értelmében védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében."

A 7. cikkben felsorolt esetek a tagállamok által megengedhető adatkezelések katalógusát adják. A tagállamok joga csak a 7. cikkben felsorolt esetben tehet lehetővé jogszerű adatkezelést – ám nem köteles az adatkezelés minden, a 7. cikkben felsorolt esetét jogszerűnek elismerni.

Két esetben [hozzájárulás – 3. § (1) bekezdése és az érintett létfontosságú érdeke – 3. § (8) bekezdése] maga az Avtv. szabályoz a 7. cikkben felsorolt kritériumot. A 3. § (1) bekezdése ezen túl azt a feltételt rögzíti, hogy az adatkezelést törvényben (önkormányzati rendeletben) kell „elrendelni". Az ilyen „elrendelést" tartalmazó törvény vagy rendelet megalkotása során figyelemmel kell lenni arra, hogy a norma korlátozza a személyes adatok védelméhez fűződő alkotmányos jogot, vagyis az akkor alkotmányos, ha az Alkotmánybíróság gyakorlatában kialakult tesztnek megfelel. Az adatkezelést elrendelő törvény vagy rendelet ezen túl kizárólag a 7. cikkben szabályozott esetekben rendelhet el adatkezelést, *ha a szóban forgó adatkezelés az irányelv hatálya alá tartozik*.

1.12. A célhoz kötöttség elve és az Avtv. 5. §-ben foglalt további követelmények

1.12.1. Az 5. § (1) bekezdés – a szűk értelemben vett célhoz kötöttség

kommentárt.

1. Az Avtv. 5. § (1) bekezdése szerint „személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak." A célhoz kötöttség egyszerre alkotmányos követelmény, amely az AB által a személyes adatok védelméhez fűződő jog alkotmányosságának vizsgálatakor alkalmazott teszt szükségességi elemét konkretizálja,[390] és az Avtv. 5. § (1) bekezdésében lefektetett törvényi követelmény, amelynek minden – tehát nem csak törvény által elrendelt – adatkezelés során, annak teljes folyamatában érvényesülnie kell. A célhoz kötöttség követelménye szorosan összefügg az 5. § (2) bekezdésében rögzített, általunk szükségességnek nevezett követelménnyel, ám el is határolható attól. A célhoz kötöttség körében azon ügyeket tárgyaljuk, amelyek során az adatkezelési cél nem állapítható meg, illetőleg eltér a jogszerű céltól; a szükségesség körében pedig azokat az eseteket, amelyekben az adatkezelés a megjelölt célt szolgálja, ám annak megvalósulásához nem elengedhetetlenül szükséges.

2. Az adatkezelési célnak „meghatározottnak" kell lennie: mind az alkotmánybírósági gyakorlat, mind az adatvédelmi biztosi esetekből kiolvasható jogalkalmazói jogértelmezés szerint; ez van továbbá összhangban az irányelv rendelkezéseivel is.[391] A meghatározott cél – a célhoz kötöttség AB határozatokban megjelenő és az Irányelvvel összhangban történő értelmezése szerint – csak *jogszerű* cél lehet.

A célt az adatkezelőnek (2. § 6. pontja), törvény vagy önkormányzati rendelet által „elrendelt" adatkezelés esetén ennek a törvénynek vagy rendeletnek kell meghatároznia [3. § (4) bekezdése]. Az adatkezelés célját az adatkezelőnek, illetőleg a szabályozás tárgya szerint illetékes miniszternek, országos hatáskörű szerv vezetőjének, polgármesternek, főpolgármesternek, a megyei közgyűlés elnökének be kell jelentenie az adatvédelmi nyilvántartásba [28. § (1) bekezdés *a)* pontja].

A cél meghatározásával kapcsolatos további probléma az, ha a jogalkalmazó olyan törvényi rendelkezést értelmez adatkezelésre történő felhatalmazásként, amely valamely adatkezelést feltételező jogintézményt szabályoz [például engedményezés, polgári per lefolytatása során végzett adatkezelések – lásd a 3. § (1) bekezdéséhez fűzött magyarázatot]. Ezekben az esetekben az adatkezelési cél a jogintézmény céljával esik egybe, s a valódi garanciát a szükségesség követelményének érvényesítése nyújtja.

[390] Vö. 65/2002. (XII. 3.) AB határozat.

[391] Dammann–Simitis 1997, 140.

3. Mint az az 5. § (1) bekezdésének második mondatából („Az adatkezelésnek minden szakaszában meg kell felelnie e célnak") is következik, a célhoz kötöttség nemcsak az adatkezelő és más személyek (érintett, adatfeldolgozó, harmadik személy) közötti adatátadás (adattovábbítás, annak nem minősülő „továbbítás") során érvényesül, hanem az adatkezelés minden egyes szakaszára, azokra is, amelyeket az adatkezelő kizárólag szervezetén belül végez. Ez a követelmény azt jelenti, hogy az adatkezelőnek olyan belső eljárásrendet kell kidolgoznia, amely biztosítja, hogy az adatkezelés folyamata ne lépjen ki az adatkezelési cél által meghatározott keretekből: az adatkezelőnek csak azok a munkatársai férhessenek hozzá az adathoz, akiknek tevékenysége az adatkezelés célját valósítja meg stb. Amíg az adatkezelés folyamata igazodik az adatkezelési célhoz, addig az adatkezelő munkavállalói, köztisztviselői stb. álláspontunk szerint nem minősülnek adatkezelőnek (lásd erről a 2. § 8. pontjához fűzött kommentárt) – a célhoz kötöttség szervezeten belüli sérelme azonban ahhoz is vezet, hogy – az eltérő adatkezelési célra vonatkozó döntést hozó személyétől függően – vagy a céltól eltérő műveletet végző (például jogosulatlanul betekintő) munkavállaló, vagy maga az adatkezelő szervezet új, jogosulatlan adatkezelés tekintetében válik adatkezelővé.

4. A célhoz kötöttség elvének értelmezése kérdéses lehet *nyilvánosságra hozott adatok* tekintetében.[392] A célhoz kötöttség minden adatkezelésre vonatkozó, általános követelmény. Az adatkezelésnek abban az esetben is célhoz kötöttnek kell lennie, ha annak tárgya az érintett vagy más által nyilvánosságra hozott személyes adat. Az adatkezelés jogalapját ebben az esetben vagy a nyilvánosságra hozatalt elrendelő törvény (például a cégnyilvántartásról, a cégnyilvánosságról és a bírósági cégeljárásról szóló 1997. évi CXLV. törvény, a továbbiakban: Ctv.), törvényi elrendelés híján pedig az Avtv. 3. § (5) bekezdése biztosítja.

A célhoz kötöttség nyilvános adatokkal kapcsolatban történő érvényesülésének példájaként a *cégnyilvánossággal* kapcsolatban végzett személyes adatkezeléseket vizsgáljuk részletesebben. A Ctv. 3. § (2) bekezdése szerint „a cégjegyzék fennálló, illetve törölt adatai, valamint a cégiratok teljeskörűen nyilvánosak, azokat [...] bárki megtekintheti és azokról feljegyzést készíthet. Teljeskörűen nyilvános a benyújtott, de még el nem bírált bejegyzési kérelem és mellékletei is azzal, hogy a bejegyzési (változásbejegyzési) kérelem elbírálásának folyamatban létére a cégnyilvántartásnak utalnia kell." A 3. § (3) bekezdése szerint „a cégnyilvántartásban a törölt adatnak megállapíthatónak kell maradnia". A Ctv. ezen, a cégnyilvánosságot megteremtő szabályai egyben az Avtv. szerinti adatkezelésre, a

[392] A kérdés általában úgy is felvethető, hogy alkalmazni kell-e az Avtv. szabályait nyilvános személyes adatokra. Lásd részletesebben alább.

cégnyilvántartásban foglalt, az Avtv. szerint személyes adatnak minősülő adatok nyilvánosságra hozatalára (bárki számára hozzáférhetővé tételére) vonatkozó szabályok. Az adatkezelési cél a Ctv. 3. § (1) bekezdéséből megállapíthatóan „a forgalom biztonsága és a hitelezői érdekek védelme".

A Ctv. az Igazságügyi Minisztérium Cégnyilvántartási és Céginformációs Szolgálatának működését úgy szabályozza, hogy a szolgálat által, illetve igénybevételével történő adatkezelés is megfeleljen a célhoz kötöttség követelményének. A szolgálat által végzett adatkezelés a személyes adatok tekintetében az Avtv. szerint adattovábbítás [Ctv. 4. § (1) bekezdése], amely több cég adataira is vonatkozhat [„csoportos adatszolgáltatás", Ctv. 5. § (1) bekezdése]. Ilyen adatszolgáltatás azonban csak korlátozottan kérhető abban az esetben, „ha a csoportosított cégadatok valamely személy cégtulajdonosi minőségére, cégjegyzési jogosultságára vagy arra vonatkoznak, hogy valamely személy mely cégeknél lát el vezető tisztséget vagy felügyelő bizottsági tagságot" [Ctv. 5. § (2) bekezdése]. E rendelkezés nyilvánvalóan a célhoz kötöttség elvének érvényre juttatását szolgálja – a Ctv. e §-hoz fűzött indokolása utal is az Avtv.-re –, amennyiben az ilyen adatkérés célja a törvényben meghatározott szervek (bíróság, ügyészség, bírósági végrehajtó, közigazgatási szerv stb.) működését szabályozó cél, vagy „más információkérő" számára a törvényben biztosított jogainak gyakorlása. E rendelkezések tehát a Ctv.-ben megjelölt cél mellett egyéb – az egyes szerv tevékenységét szabályozó törvényben meghatározott, vagy esetileg fennálló – célt követel meg a magánszemély cégtulajdonosi vagy vezető tisztségviselői, felügyelőbizottsági tagsági minőségére irányuló adatkérés esetében.

A következő kérdés, hogy vajon a cégnyilvántartásból származó, a Ctv. alapján nyilvánosságra hozott adatok esetében is tekintetbe kell-e venni az Avtv. szabályait, vagy elképzelhető olyan értelmezés, hogy az egyszer már jogszerűen nyilvánosságra hozott személyes adatok további kezelése (tárolása, feldolgozása stb.) szabadon, a célhoz kötöttség figyelmen kívül hagyásával is történhet. Ezzel ellentétes álláspontunkat, amely szerint a Ctv. cégnyilvánosságra vonatkozó szabályai alapján nyilvánosnak, illetve hozzáférhetőnek minősített személyes adatok további kezelése esetében is az Avtv. szabályai szerint kell eljárni – így mindenekelőtt figyelembe kell venni az adatkezelés jogalapjára és a célhoz kötöttségre vonatkozó szabályokat –, alátámasztja mindenekelőtt a Ctv., amelynek egyes rendelkezéseivel a jogalkotó kifejezetten az ilyen – egyébként nyilvános adatkörbe tartozó – adatok célhoz kötött felhasználását kívánta garantálni. Ilyen rendelkezés például a Ctv. 5. § (2) bekezdése, amely a természetes személyre irányuló kereséseket vagy egyéb – magán a Ctv. cégnyilvánosságra vonatkozó szabályain kívüli – törvényi jogcím megléte, vagy az

érintett hozzájárulása esetén teszi lehetővé, alátámasztva ezzel azt is, hogy a Ctv.-ben meghatározott célok – forgalom biztonsága, hitelezők védelme – ilyen adatkezelések esetében nem állnak fenn, vagyis ezekben az esetekben a cégnyilvánosság körén kívüli adatkezelésekről van szó. Az eltérő célú adatkezelés pedig – az Avtv. 3. § (1) bekezdésében rögzített szabállyal összhangban – csak törvényi felhatalmazáson vagy hozzájáruláson alapulhat. A Ctv. 5. § (4) bekezdése kifejezetten szól arról, hogy a természetes személyre irányuló adatkérést kielégítő adatszolgáltatás során az adatkérésre vonatkozó egyes körülmények (időpont, jogcím, kért adatok, adatok felhasználójának személye) azért rögzítendők, hogy az adat célhoz kötött felhasználása ellenőrizhető legyen. Maga a Ctv. megalkotása során tehát a jogalkotó foglalt úgy állást, hogy a nyilvánosan hozzáférhető személyes adatok kezelése során is figyelemmel kell lenni a célhoz kötöttség követelményére, s csak e követelmény teljesítése esetében lehet ezeket az adatokat például csoportosítani, hasznosítani stb.[393]

A nyilvánosságra került adatok célhoz kötöttségével kapcsolatos fenti álláspontunkat támasztja alá az adatvédelmi biztosi gyakorlat is (lásd alább).

Rá kell azonban mutatni arra, hogy egyes – alább idézett – alkotmánybírósági határozatokkal látszólag alátámasztható olyan érvelés is, amely szerint a nyilvános („közérdekből nyilvános") személyes adatok a közérdekű adatok jogi sorsát osztják. Mivel a közérdekű adatok vonatkozásában a célhoz kötöttség nem értelmezhető, ezen érvelés szerint a nyilvánosságra hozatal aktusával a további adatkezelések célhoz kötöttségének követelménye elenyészik. Ez az értelmezés szükségszerűen oda vezet, hogy az Avtv. személyes adatok védelmére vonatkozó I. és II. fejezetének hatálya nem terjed ki a nyilvánosságra hozatalt

[393] A célhoz kötöttség hasonló felfogását tükröző rendelkezések találhatók egyes más, szektorális adatvédelmi jogszabályokban is. A kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény szerint például a tudományos kutató, piac- és közvélemény-kutató, valamint közvetlen üzletszerző szerv a jogszerűen nyilvánosságra hozatal céljából készített és nyilvánosságra hozott adatállományban, név- és címjegyzékben, valamint kiadványban – így különösen telefonkönyv, szaknévsor, statisztikai névjegyzék – szereplő adatot akkor gyűjthet a törvényi felhatalmazás alapján (az érintett hozzájárulása nélkül), „ha az adatgyűjtéskor vagy az adategyeztetéskor az érintettet tájékoztatták az eredetitől eltérő célra történő adatfelhasználás lehetőségéről, illetőleg a letiltás jogáról" [1995. évi CXIX. törvény 3. § (1) bekezdés *b)* pontja].

követő időre.[394] Álláspontunk szerint ez az értelmezés téves, és eredetét a közérdekű (és újabban „közérdekből nyilvános") adat fogalmának az alkotmánybírósági gyakorlatban meghonosodott, az Avtv. fogalomrendszerétől eltérő használatából nyeri.

5. A célhoz kötöttség követelményének tartalmát mind az Alkotmánybíróság, mind az adatvédelmi biztos számos esetben értelmezte. A gyakorlatot az alábbiakban részletesen tárgyaljuk, ám előzetesen is kiemeljük az alábbiakat: az adatkezelési cél az adatkezelés elsődleges attribútuma: az adatkezelési *cél változása minden esetben új adatkezelést eredményez;* cél nélküli adatkezelés az adatalany *hozzájárulása esetén sem végezhető;* a célhoz kötöttség elve *nem érvényesül közérdekű adatok „kezelése" során*.

1.12.2. Az adatvédelmi biztos célhoz kötöttséggel kapcsolatos gyakorlata

1. Az adatvédelmi biztosi gyakorlatban *a célhoz kötöttség vizsgálata szinte minden ügyben megtörténik*. Számos példát találunk, ahol a biztos cél nélküli adatkezelést minősített jogszerűtlennek. Hiányzott az adatkezelési cél, és így az adatkezelés az 5. § (1) bekezdése alapján jogszerűtlennek minősült abban az esetben, amelyben az APEH az önkormányzat területén működő összes szállásadói tevékenységet folytató személy adatainak továbbítását kérte az önkormányzati adóhatóságtól. A törvényi szabályozás lehetővé tette ugyan meghatározott személyekre vonatkozó adat továbbítását („ha az valamely adó [vámteher] vagy adóhiány feltárását, behajthatóságának megállapítását lehetővé teszi vagy valószínűsíti"), ám a célhoz kötöttség követelménye kizárja a készletező, „totális adatgyűjtést".[395] Hiányzik az adóazonosító jel kezelésének célja abban az esetben, ha az adatkezelő (bank) nem teljesít olyan kifizetést, amelynek kapcsán az ügyfélnek adófizetési kötelezettsége keletkezik.[396] Hiányzik a cél abban az esetben, amelyben a tanulók adatai kezelésének célja esetleges jövőbeni pályázatok benyújtásának lehetősége, „általános jelleggel, majdani esetleges felhasználás céljából személyes adatok nem kezelhetők".[397] Bár

[394] Bártfai Zsolt álláspontja (személyes közlés). Megjegyzendő, hogy létezik olyan tagállami adatvédelmi jog, amely nem vonja a védelem körébe a nyilvános adatokat, lásd például az osztrák adatvédelmi törvény (DSG 2000) 1. § (1) bekezdését. Ez a megközelítés álláspontunk szerint a magánszféra-védelem korábbi szakaszát tükrözi, és nem számol a nyilvános adatok automatizált csoportosításának, rendezésének lehetőségeiből származó veszélyekkel.

[395] ABI 1999, 272.

[396] ABI 1999, 277.

[397] ABI 1999, 326–327.

az óvoda továbbíthatja a gyermek felvételével kapcsolatos személyes adatokat a fenntartónak, az adott esetben az adattovábbítás célja nem a fenntartói tevékenységgel, hanem a gyermek szülőjével kapcsolatos peres ügy bonyolítása volt, ezért az adattovábbítás jogellenes, mert sérült a célhoz kötöttség követelménye.[398]

A biztos a célhoz kötöttség hiányát előíró jogszabálytervezeteket is bírált: így például kifogásolta azt a szabályozást, amely szerint a szállásadók kötelesek lettek volna az általuk vezetett vendégkönyvet az illetékes rendőrkapitányságnak átadni, amely azt öt évig őrizte volna – a biztos szerint az adatkezelésnek nincs célja, az „készletező" adatgyűjtés.[399]

2. Az adatvédelmi biztosi gyakorlat megköveteli a cél pontos meghatározását. Így például az a meghatározás, amely szerint igen széles adatkörre (a gyermek és családja tagjainak egészségi állapotára, politikai attitűdjére, vagyoni helyzetére, családi állapotára) vonatkozó adatkezelés célja az egyesületi „tagok jobb megismerése, személyesebb kapcsolattartás", az adatvédelmi biztos szerint nem elég konkrét, „ráadásul a kérdések nagy része még ezen tág célmeghatározás kereteibe sem illeszthető be".[400]

3. A célhoz kötöttség (illetőleg a szükségesség) elvének alkalmazásával kapcsolatos jellemző esetcsoport az, ahol valamely szerv *törvényben meghatározott feladata gyakorlása során olyan adatot kezel, amely eltér a törvényi felhatalmazásban foglalt céltól,* illetőleg olyan adatokat, amelyek – a biztos szerint – nem szükségesek a cél megvalósításához [ez utóbbi esetcsoportról lásd a (2) bekezdésnél]. A célhoz kötöttség jelentette például az adatkezelés korlátját abban az esetben, amelyben az adóhatóság a biztos megállapítása szerint törvényi felhatalmazás alapján igényelt adatokat az állampolgároktól jövedelemadó ellenőrzése céljából, ám egyes adatok kezelése nem volt kapcsolható a törvényben meghatározott célhoz, mivel azok az érintett vagyoni és nem jövedelmi viszonyait jellemezték.[401]

4. Az adatvédelmi biztos egyes esetekben a célhoz kötöttség elvét hívta segítségül azon ügytípusba tartozó esetek vizsgálata során is, amelyben a tárgy az egyes társaságok részéről folytatott *ügyfél-azonosítási gyakorlat* volt: nevezetesen az, hogy az ügyféltől több igazolvány (bankkártya stb.) bemutatását kérik, sőt ezeket le is fénymásolják. A biztos szerint: „A személyazonosító igazolvány hatósági igazolvány, amely a személyazonosságot hitelt érdemlően igazolja, tehát az ügyfél jogszerűen további igazolványok bemutatására sem

[398] ABI 2004, 73.

[399] ABI 1998, 166.

[400] ABI 1997, 182–184.

[401] ABI 1998, 236.

kötelezhető. Az Avtv. rendelkezéseivel ellentétesen a szolgáltatók nem tartják szem előtt az adatkezelés célhoz kötöttsége követelményének érvényesítését, indokolatlanul széles körben gyűjtenek adatokat."[402] Nézetünk szerint ez az állásfoglalás téves: megfelelő cél megjelölésével (akár egyszerűen az érintett azonosítása, akár a kockázat csökkentése, kizárása) ennek az adatkezelésnek a célhoz kötöttsége könnyen igazolható; további vizsgálatot az adatkezelés szükségessége [lásd alább a (2) bekezdésben], esetleg a hozzájárulás érvényessége igényel.

5. További, az adatvédelmi biztos gyakorlatában felmerült kérdés *a kockázatelbírálás során kezelhető adatkör meghatározásának problémája:* vajon adatvédelmi jogilag miként minősül azon – például banki, biztosítói – gyakorlat, amelynek keretében az adatkezelő a hitelezési (biztosítási) kockázat meghatározásához, lehetséges csökkentéséhez kezel igen széles körben adatokat? Az ilyen ügyekben általában a szükségesség vizsgálandó (mert az adatkezelési cél jellemzi az adatkezelés egész folyamatát). Ám vannak kivételek: ilyen az az eset, amelyben az adatvédelmi biztos meghatározott bankkártyák kibocsátása során végzett adatkezelés jogszerűségéről foglalt állást. A biztos abból indult ki, hogy a szóban forgó „kártya sajátossága az, hogy – a hitelkártyákkal ellentétben – […] birtokosa nem végezhet a kártyához tartozó folyószámla egyenlegét meghaladó műveleteket, vagyis a kártya rendeltetésszerű használata során az ügyfél általában nem kerül adósi pozícióba, s ha igen, adóssága akkor sem haladhatja meg a bank részéről a folyószámla és a […] kártya ellenértékeként felszámolt díjakat."[403] A kártya igényléséhez használt űrlapon a kibocsátó hitelintézetek igényelték az ügyfél munkahelyére, egyéb banknál vezetett számláira, (alkalmazott esetén) az éves bruttó és nettó jövedelemre, (vállalkozó esetén) a vállalkozás tevékenységi körére, nevére vonatkozó adatokat, a vagyonra (ház, telek, gépkocsi) vonatkozó adatokat, a család egy főre jutó havi jövedelmére vonatkozó adatot, valamint az ügyfél egyéb bankkártyáira, banki kapcsolataira vonatkozó adatokat. A biztos szerint – mivel az ügyfél csak rendeltetésellenes használat esetén kerül adósi pozícióba, amelyet a banknak kell kizárnia – „a kibocsátó kizárólag az ügyfél azonosításához szükséges adatokat igényelheti". A további adatok kezelése – bár az állásfoglalás az 5. § (2) bekezdésére is hivatkozik – cél

[402] ABI 1999, 95.

[403] Az állásfoglalás az ilyen kártyát betéti kártyának nevezi, ám a „betéti kártya" ilyen meghatározását a Magyar Bankszövetség vitatta – az adatvédelmi biztos azonban a vonatkozó MNB rendelkezésre hivatkozott: lásd ABI 1999, 289., valamint alább az 5. § (2) bekezdéséhez fűzött kommentárt. Az állásfoglalás szempontjából nem releváns, hogy a bankkártyák e csoportját miképp nevezzük, ám a félreértések elkerülése végett a főszövegben mellőzzük a „betéti kártya" megnevezés használatát.

nélküli, így az 5. § (1) bekezdését sérti. Az ügy jelentősége, hogy ebben az esetben az adatvédelmi biztos a célhoz kötöttség elvéből és az adatfelvétel tisztességességének és törvényességének elvéből [7. § (1) bekezdés *a)* pontja] lefektette az általános szerződési feltételek keretei között végzett, tehát döntően az egyik fél által meghatározott adatkezelésekkel kapcsolatos azon követelményt, amely szerint „[a] blankettaszerződést kidolgozó félnek […] fokozottan kell ügyelnie arra, hogy a szerződés a másik felet csak azon adatainak kiszolgálására kötelezze, amelyek indokoltak a szerződés célját tekintve, s a többi, a szerződés által előírt adatkezelés (például bizonyos feltételek bekövetkezése esetén a szerződő fél adatainak továbbítása harmadik személy részére) is az ügylet céljához igazodjon" – egyébként az Avtv. mindkét hivatkozott rendelkezése sérül.[404]

6. A cél olyannyira jellemző az adatkezelésre, *hogy annak megváltozása az adatvédelmi biztosi gyakorlat szerint új adatkezelést eredményez.* Példa erre az az eset, amelyben egy bank a hitelelbírálást követően – elutasítás esetén is – kezelte az érintettek adatait, „termékek fejlesztését elősegítő statisztikák" készítése céljából. Ez olyan, a korábbitól eltérő célú adatkezelésnek minősül, amelynek jogalapját újra meg kell teremteni, vagyis a jogszerűséghez az érintett hozzájárulását kell beszerezni.[405]

Megjegyzendő, hogy egyes esetekben az adatvédelmi biztos jogszerűnek minősített (sőt kezdeményezett) olyan adatkezeléseket, amelyek célja az eredeti céltól eltér, ám azzal nem összeegyeztethetetlen, értelmezésével elfogadva az irányelvből kiolvasható megkülönböztetést elsődleges és további, azzal összeegyeztethető célok között (lásd erről alább az irányelv vonatkozó szabályozásának tárgyalásánál). Ilyen esetek például azok, amikor az adatvédelmi biztos jogszerűtlennek minősíti azt, hogy egy nyilvántartást kezelő szerv (például az adóhatóság) kiszolgáltassa harmadik személynek (például az üdülőtulajdonosokért fellépő érdek-képviseleti szervnek) az érintett (például az üdülőtulajdonos) adatát, ám gyakorlatias módon azt javasolja megoldásként, hogy az adatkezelő keresse meg az érintettet, és kérje hozzájárulását a harmadik személynek történő egyszeri adattovábbításhoz (a példánál maradva: az adóhatóság keresse meg az üdülőterületen ingatlantulajdonnal rendelkezőket, és kérje hozzájárulásukat ahhoz, hogy továbbíthassa adataikat a szerveződő érdek-képviseleti szervhez). Álláspontunk szerint ebben az esetben maga az adatkezelő az érintettek megkeresésével céltól eltérő adatkezelést valósít meg (hiszen

[404] ABI 1999, 253.

[405] ABI 2000, 212.

például az adott esetben az adatkezelés célja az adózással kapcsolatos eljárások lefolytatása, ellenőrzés, amelynek körébe ez az eltérő célú adatkezelés nem illeszthető)[406].

7. A célhoz kötöttség az információs önrendelkezési jog gyakorlásának „legfontosabb garanciája", olyan általános követelmény, amely minden adatkezelésre vonatkozik. A cél nélküli adatkezelés tilalma abszolút tilalom; *az érintett hozzájárulása esetén sem lehet jogszerűen cél nélküli adatkezelést végezni*. „Adatkezelés – az adatalany hozzájárulásával végzett adatkezelés is – csak akkor lehet törvényes, ha a célhoz kötöttség követelménye érvényesül."[407] „[Á]ltalános jelleggel, majdani esetleges felhasználás céljából személyes adatok nem kezelhetők."[408] Az Avtv. által szabályozott hozzájárulás (2. § 6. pontja) csak akkor érvényes, ha az megfelelő tájékoztatáson alapul, amelynek ki kell terjednie az adatkezelés céljára is [6. § (2) bekezdése].

8. Az adatvédelmi biztos állást foglalt *a nyilvános személyes adatok kezelésének célhoz kötöttségével kapcsolatban* is. Egy ügyben az Országgyűlés egyik vizsgálóbizottsága intézett megkeresést egyes állami szervekhez (ORFK, VPOP Országos Parancsnoksága stb.), amelynek teljesítéséhez az adott szerveknek előzetesen a cégnyilvántartás segítségével kellett volna meghatározott személyeket azonosítaniuk. A biztos szerint „a cégnyilvántartásból származó adatok kezelésének (például gyűjtésének, tárolásának, bizonyos szempontok szerinti feldolgozásának) jogszerűségét [...] az érintett személyek vitathatnák, mivel ezen adatokat személyazonosításkor a szervezet már nem cégadatokként, hanem személyes adatokként kezelné. Az ilyen adatkezelések sem az adatkezelés célhoz kötöttsége általános elvének, sem a szervezet adatkezelésére vonatkozó azon törvényi előírásoknak nem felelnének meg, amelyek a más adatkezelési rendszerekből történő adatátvételt szabályozzák."[409] Vagyis a biztos szerint a megkeresett szervek – hozzájárulás hiányában – csak törvényi felhatalmazással, illetve célhoz kötötten kezelhetik a cégnyilvántartásból származó adatokat.[410] Az adatvédelmi biztos szerint az ingatlan-nyilvántartás nem használható arra

[406] A példabeli esetre lásd ABI 2004, 71.

[407] ABI 1999, 252.

[408] ABI 1999, 327.

[409] ABI 2001, 46.

[410] Lásd még hasonlóra ABI 1999, 62. Ebben az ügyben az önkormányzati adóhatóság azon gyakorlata volt a vizsgálat tárgya, amelynek keretében újsághirdetés alapján azonosítottak adóköteles vagyontárgyakat, majd a hirdetésben megadott telefonszám használójának adatait a tudakozó segítségével ismerték meg; ezután ezt a személyt az adóhatóság megkereste, és tájékoztatta arról, hogy ha tulajdonos, akkor adóbevallási kötelezettsége van; felszólították arra is, hogy ha nem ő az, akkor közölje a tulajdonos adatait. A biztos szerint „az önkormányzati adóhatóság által követett módszer, hogy a telefontársaság tudakozójának nyilvános […]

célra, hogy abból valamely természetes személy valamennyi ingatlanát lekérdezzék: „Az ingatlan-nyilvántartás nyilvánossága az ingatlanforgalom biztonságát szolgáló intézmény. E nyilvánosság azonban nem jelenti azt, hogy a nyilvántartás adatai – csoportosítva – az adatkezelés eredeti céljától eltérő célból is nyilvánosságra hozhatók."[411]

Megjegyzendő, hogy az adatvédelmi biztos beszámolóiban feltűnnek a fentivel ellentétes – álláspontunk szerint téves – értelmezésre módot adó állásfoglalások is. A biztos szerint életrajzi adatok publikálhatók, ha azokat korábban már jogszerűen nyilvánosságra hozták.[412] Egy másik esetben a biztos úgy foglalt állást, hogy a beadványozó „korábban jogszerűen nyilvánosságra hozott adatok ismételt nyilvánosságra hozatalával" elektronikus úton jogszerűen tehet hozzáférhetővé saját maga által összeállított, személyes adatokat tartalmazó adatbázist.[413] Ide sorolható az az eset is, amelyben a biztos az Avtv. követelményeivel összhangban állónak találta azt a rendeleti szabályozást, amely rendőrök, határőrök, tűzoltók számára egyenruhájukon névkitűző viseletét írta elő – az adatvédelmi biztos szerint ez a szabály az Avtv. 19. §-a alapján igazolható, mivel az ott meghatározott szervek hatáskörében eljáró személyek neve és beosztása – ha törvény másként nem rendelkezik – nyilvános adat.[414]

Álláspontunk szerint a nyilvánosságra hozott adat is csak a célhoz kötöttség követelményének szem előtt tartásával kezelhető; az azon végzett bármely adatkezelési művelet – ha az az Avtv. hatálya alá esik – az érintett hozzájárulása vagy törvényi felhatalmazás nélkül csak az eredeti célra történhet.[415]

---

adatbázisából szereznek információt az adótárgy birtokosáról, a törvény által nem megengedett, tehát tilos. Az eljárás nem felel meg a törvényesség követelményének." A célhoz kötöttség az ügy megítélésében nem játszott szerepet.

[411] 164/K/2004.

[412] ABI 1999, 123.

[413] ABI 2000, 113.

[414] Lásd alább az 54/2000. (XII. 18.) AB határozatot is. A biztos – az AB-hoz hasonlóan – nem vizsgálta az ügy tárgyaként szereplő adatkezelés célját, illetőleg szükségességét. Sajátos, hogy Burkert (1997, 125) éppen a rendőr kitűzőjét említi példaként a magánszféravédő technológiák tárgyalásakor: PET-nek minősül az a megvalósítás, amely szerint a rendőr kód vagy szám és nem név alapján azonosítható a polgár számára. Lehetséges, hogy az adatkezelés igazolható valamely céllal, és szükséges is, ám az állásfoglalás kimerül a törvényi felhatalmazás felidézésében.

[415] Ezzel ellentétes álláspont képviselője érvelhetne úgy, hogy a 3. § (5) bekezdésében a nyilvánosságra hozatal céljából átadott adatok tekintetében szabályozott hozzájárulás bármely célú adatkezeléshez történő hozzájárulásként értelmezhető. Álláspontunk szerint a nyilvánosságra hozatalkor mindig meghatározható azon cél, amely a személyes adatok nyilvánosságra hozatalát indokolja.

9. Az adatvédelmi biztosi gyakorlatban megjelenik *a célhoz kötöttség közérdekű adatokra történő értelmezhetőségének* kérdése is: a biztos szerint ez az elv közérdekű adatok „kezelésére" nem értelmezhető.[416] Ezzel ellentétes állásfoglalás ugyan az adatvédelmi biztosi gyakorlatban fellelhető, ám nem tekinthető uralkodó értelmezésnek.[417]

10. A adatvédelmi biztos helyszíni vizsgálatok keretében igen gyakran vizsgálta a *szervezeten belüli adatkezelés célhoz kötöttségét.*[418] Állásfoglalása szerint: „A szervezeten belüli adatkezelési rendnek is az Avtv.-ben az adatkezelésekkel szemben meghatározott követelményekhez kell igazodnia".[419]

1.12.3. Az Alkotmánybíróság gyakorlata

1. Az Alkotmánybíróság a személyes adatok védelméhez fűződő alkotmányos jogot információs önrendelkezési jogként értelmező kulcshatározata [15/1991. (IV. 13.) AB határozat] szerint a célhoz kötöttség „[a]z információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája". Az AB szerint ez azt jelenti, hogy „személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak. Az adatfeldolgozás célját úgy kell az érintettel közölni, hogy az megítélhesse az adatfeldolgozás hatását jogaira, és megalapozottan dönthessen az adat kiadásáról; továbbá, hogy a céltól eltérő felhasználás esetén élhessen jogaival. Ugyanezért az adatfeldolgozás céljának megváltozásáról is értesíteni kell az érintettet. Az érintett beleegyezése nélkül az új célú feldolgozás csak akkor jogszerű, ha azt meghatározott adatra és feldolgozóra nézve törvény kifejezetten megengedi. A célhoz kötöttségből következik, hogy a *meghatározott cél nélküli,* »készletre«, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes."

---

[416] Az alább tárgyalt 19/1995. (III. 28.) AB határozatra történő utalással lásd például ABI 1998, 130.

[417] ABI 1999, 395: „Fel kell hívni az adatkérők figyelmét arra, hogy az ingyenesen […] bárki számára hozzáférhető közérdekű adatok »értékesítése«, anyagi ellenszolgáltatásként történő továbbadása jogszerűtlen és ellentétes a hatályos szabályozással." A szövegből nem derül ki, hogy az ilyen továbbítás célja vagy módja jogellenes, s az sem, hogy mely jogszabályba ütközne a továbbértékesítés – az állásfoglalás nézetünk szerint téves.

[418] ABI 1998, 143. skk.; ABI 1999, 142. skk.

[419] ABI 2000, 283.

A 15/1991. (IV. 13.) AB határozatban által megsemmisített szabályozás célja „az állampolgár jogai érvényesítésének és kötelezettségei teljesítésének előmozdítása, az állami szervek, a gazdálkodó és társadalmi szervezetek, egyesületek, valamint magánszemélyek társulásai (a továbbiakban együtt: szervezetek) munkájának segítése" volt, amely az AB szerint „teljesen inadekvát ahhoz képest, hogy az ország teljes lakosságát érintő adatfeldolgozó rendszer felállításáról van szó, sőt, olyan rendszerről, amely a személyes adatok és a velük kapcsolatos jogok sorsát alapvetően meghatározzák (lásd személyi szám). A semmitmondó szöveg alkalmatlan arra, hogy az adatfeldolgozásnak bármiféle irányt vagy határt szabjon, azaz hogy célhoz kötöttségről egyáltalán beszélni lehessen."

A célhoz kötöttség elvéből következik az is, hogy az Alkotmánybíróság szerint „az univerzális személyi szám lényegénél fogva ellentétes az információs önrendelkezési joggal. Ezért az Alkotmánnyal csakis a meghatározott célú adatfeldolgozásra korlátozott használatú azonosító szám egyeztethető össze." A 15/1991. (IV. 13.) AB határozatban kifejtettek szerint az egész államigazgatás „nem tekinthető olyan egységnek, amelyen belül egyetlen egységes személyazonosító kódot lehetne bevezetni vagy használni" (ún. osztott információs rendszerek elve). A jogalkotó ezt a követelményt nem a célhoz kötöttséghez kapcsolódóan, hanem az adatminőségre vonatkozó szabályok között rögzítette [lásd a 7. § (2) bekezdését].

2. Az Alkotmánybíróság következetes gyakorlatából is kiolvasható az a követelmény, amely szerint *az adatkezelési célnak pontosan meghatározottnak kell lennie*. A 65/2002. (XII. 3.) AB határozat alkotmányellenesnek minősítette az Eüatv. azon rendelkezését, amely egészségügyi adatnak minősítette a szexuális szokásokkal kapcsolatos adatokat abban az esetben, „amennyiben a 4. § (1) bekezdése szerinti célból indokolt". Az Eüatv. hivatkozott §-a négy adatkezelési célt sorol fel, ám az Alkotmánybíróság szerint a „meghatározott célok együttesen aránytalanul széles, pontosan meg nem határozott körben teszik lehetővé a szexuális szokásokra vonatkozó adatok kezelését. A szexuális szokásokra vonatkozó különleges adatok kezelése céljának túl tág meghatározása pedig nem felel meg az alapjog-korlátozással szemben támasztott szükségességi mércének." Az AB szerint: „ A különleges személyes adatoknak minősülő, szexuális szokásokkal összefüggő adatok kezelésével szemben követelményként érvényesül, hogy az adatkezelésnek konkrét célhoz kötöttnek kell lennie. Az adatkezelési cél túlságosan tág módon történő meghatározása, azaz ha nincs összefüggésben az adatkezelés a megjelölt céllal, továbbá, ha arra bizonytalan esetkörben kerül sor, illetve arra nem a szükséges mértékre korlátozott személyi kör jogosult, akkor az adatkezelés meghatározott cél nélkül, illetve korlátlan módon válik lehetővé."

3. Az Alkotmánybírósági gyakorlat is alátámasztja azt, hogy a célhoz kötöttség elve mint adatvédelmi alapelv nem érvényesül közérdekű adatok „kezelése", így megismerése és felhasználása során sem. Az Alkotmánybíróság egy, a közérdekű adatok felhasználását „csak a köz érdekében" lehetővé tévő önkormányzati rendelet vizsgálata során kimondta: „Az Avtv. nem tartalmaz olyan korlátozó rendelkezést, amely a közérdekű adatok megismerését célhoz kötötté teszi. Ezáltal a szabályozás megengedi azt is, hogy a kérelmező ne csupán közérdekből, hanem például saját jogos érdekei érvényesítése vagy csoportérdek megvalósítása céljából kezdeményezze a közérdekű adat megismerését. Az Avtv. szerint a közérdekű adatot kezelő szerv nem jogosult az adatkérés céljának vizsgálatára sem. […] Az Alkotmány 61. § (1) bekezdése nemcsak a közérdekű adatok megismeréséhez, hanem ezeknek az adatoknak a terjesztéséhez való jogot is biztosítja. A közérdekű adatok terjesztése egyaránt jelentheti az adatok köz-, illetve magáncélú megismertetését és felhasználását."[420]

4. Az alkotmánybírósági gyakorlatban azonban elkülöníthető az az esetcsoport is, amelyben a testület meghatározott személyes adatok „közérdekűvé válását" mondta ki: „A személyes adat nyilvánosságra hozatalát a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 3. § (4) bekezdése szerint törvény közérdekből elrendelheti. Ekkor a személyes adat közérdekből nyilvános adattá válik és a »közérdekű adatokéhoz hasonló jogi elbírálás alá esik, amelynek a szabályait az adatvédelmi törvény III. fejezete tartalmazza«" [44/2004. (XI. 23) AB határozat]. Ez a határozat alátámaszthat olyan értelmezést, amely szerint azok személyes adatok kezelése során, amelyek nyilvánosságra hozatalát törvény elrendelte, a nyilvánosságra hozatalt követően a célhoz kötöttség nem áll fenn (mivel ezen adatok a közérdekű adatok jogi sorsát osztják).

Az idézett döntés a személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog egymáshoz való viszonyát az átvilágítás kontextusában meghatározó, egyes személyek jogállamisággal ellentétes tevékenységének tényét (tehát az Avtv. szerint személyes adatot) közérdekű adatnak minősítő 60/1994. (XII. 24.) AB határozatra utal. Ám 1994-es határozatában az AB rögzíti: „Az Alkotmánybíróság ebben a határozatában […] a »közérdekű adat« fogalmát az Alkotmány 61. § (1) bekezdésére vonatkoztatja, s nem abban az értelemben használja, ahogy azt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 2. § 3. pontja meghatározza, illetve ahogy arról az Avtv. 19. § (3) bekezdése

[420] 19/1995. (III. 28.) AB határozat.

rendelkezik. A vizsgált törvény az Avtv.-től függetlenül, az Alkotmány 61. §-ra tekintettel elrendeli bizonyos személyes adatok nyilvánosságra hozatalát." Az AB a szóban forgó személyes adatok nyilvánosságáról foglal állást, a határozatból nem olvasható ki az, hogy az adatok személyes adat volta adott esetben megszűnne.

1.12.4. Az irányelv vonatkozó rendelkezése

Az irányelv a célhoz kötöttség (és a szükségesség) követelményét az adatminőségről szóló 6. cikkben rögzíti: az (1) bekezdés *b)* pontja szerint a személyes adatok „gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon. A személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat." Az irányelv szabályozása szerint a tagállami jogalkotónak van némi tere a célhoz kötöttség elvének „relativizálására", amennyiben az adatkezelés elsődleges célja mellett további, azzal összeférhető célokból is megengedheti az adatkezelést; ilyen például az irodalom szerint, ha az adatkezelő ügyféladatbázisát saját szolgáltatásának marketingjére használja fel.[421] A magyar jogalkotó – az Avtv. keretein belül – nem ismeri el az elsődleges céllal „összeférő" másodlagos célokból végzett adatkezelés jogszerűségét.[422]

1.12.5. A szükségesség elve (5. § (2) bekezdés)

1. Az Avtv. 5. § (2) bekezdése szerint „csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig."

A (2) bekezdésben foglalt rendelkezés („a szükségesség elve") szorosan összefügg a célhoz kötöttség követelményével (gyakran annak részeként említik), ám el is határolható attól. Míg a célhoz kötöttség az adatkezelés céljának pontos meghatározását írja elő, a szükségesség elve tiltja a meghatározott cél elérésére alkalmatlan adatkezelést, valamint az adatkezelés terjedelmét a cél megvalósításához elengedhetetlen adatkörre, és a cél megvalósulásához szükséges adatkezelési cselekményekre és időtartamra korlátozza. Ehhez a

[421] Dammann–Simitis 1997, 140.

rendelkezéshez kapcsolódik a 7. § (1) bekezdésének *c)* pontjában lefektetett azon szabály, amely szerint az adatok tárolásának módja „alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani".

2. Nehezen meghatározható az adatkezelés megvalósításához szükséges adatkör, ha az adatkezelés célja adósminősítés, vagy hasonló olyan cél, amely az adatkezelő kockázatának csökkentését célozza. Ezekben az esetekben a többletinformáció szinte korlátlanul felhasználható a becslés pontosítására. A szükségesség követelményének való megfelelés ilyenkor esetről esetre, a tényálláshoz képest vizsgálandó. Az adatkezelés céljához illeszthető adatok körét korlátozza az, hogy az adatkezelés célja csak jogszerű lehet, így az olyan adat kezelése, amellyel kapcsolatban az adatkezelési cél megvalósulása az adatalany hátrányos megkülönböztetését, illetőleg általában az egyenlő bánásmód követelményének megsértését eredményezi, tilos.[423] [Az egyenlő bánásmód és a hátrányos megkülönböztetés fogalmához lásd az Alkotmány 70/A. § (1) bekezdését, valamint az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvényt.]

3. Abból a követelményből, amely előírja, hogy a csak „az adatkezelés céljának megvalósulásához elengedhetetlen" adat kezelhető, álláspontunk szerint nem következik az, hogy az adatkezelőnek jogi kötelezettsége több, az adatkezelési cél megvalósítására alkalmas módszer, eljárás közül – a költségekre tekintet nélkül – azt alkalmaznia, amely kevesebb személyes adat kezelésével jár. Amennyiben azonban több olyan mód, eljárás van, amellyel az adott cél elérhető, és azok költsége azonos vagy hasonló, akkor álláspontunk szerint a szükségesség elvéből következik az adatkezelő kötelezettsége az adatkezeléssel nem járó,

---

[422] De a példabeli esetre lásd a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény 3. § (1) bekezdésének *a)* pontját.

[423] Ezzel kapcsolatban említendő az az állásfoglalás, amelyet a biztos egy politikai párt adatkezeléséről adott ki. A párt képviselőjelöltjeivel szerződést kötött, amelyben azoknak nyilatkozniuk kellett arról, hogy nem szenvednek alkohol- vagy kábítószer-függőségben és nem homoszexuálisok. Az állásfoglalás szerint a párt a képviselőjelölttel bármilyen, jogszabályba nem ütköző tartalmú szerződést köthet; a szerződés tartalmára azonban a vizsgálat – annak ismerete hiányában – nem terjedt ki; a különleges adatok kezelésére vonatkozó írásbeli hozzájárulás a szerződésbe foglalható. Adatvédelmi jogi szempontból a kérdés az, hogy ebben az esetben az adatkezelés célja jogszerű-e, vagyis adott esetben a meghatározott személyek kizárása a képviselő-jelöltségből a 2003. évi CXXV. törvény 7. § (2) bekezdése szerint igazolható-e, mint amelynek „tárgyilagos mérlegelés szerint az adott jogviszonnyal közvetlenül összefüggő, ésszerű indoka van".

illetőleg szűkebb körű (kevesebb személyes adatra kiterjedő, kevesebb adatkezelési műveletet magában foglaló) adatkezeléssel járó megoldás választására.[424]

4. A törvény e bekezdésében megfogalmazott alapelvből (a „szükségesség elvéből") következik az elektronikus közegben végzett adatkezelések szektorális szabályozásában a német és nyomában a magyar szabályozásban megjelent „adattakarékosság elve". Az adattakarékosság elve szerint az adatkezelőnek már az adatkezelési rendszerek tervezésekor, majd működtetésük során folyamatosan biztosítania kell azt, hogy ne, illetőleg csak a minimális mértékben kerülhessen sor személyes adatok kezelésére (lásd az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 13/A. §-át).

5. Hasonlóan a szűkebb értelemben vett célhoz kötöttség elvéhez, a szükségesség elvének is minden személyes adatkezelés során érvényesülnie kell: ez azt jelenti, hogy az érintett hozzájárulásával sem kezelhető olyan adat, amely a meghatározott adatkezelési cél megvalósításához nem szükséges.

6. Fokozottan figyelemmel kell lenni a szükségesség követelményére azokban az esetekben, amelyekben valamely jogintézmény működése adatkezelést feltételez, vagyis a jogalkotó az intézmény működését szabályozó törvényi rendelkezéseket ismeri el adatkezelést lehetővé tévő felhatalmazásnak. A kezelhető adatkör ilyenkor a szükségesség elvének segítségével határolható körül. Ilyen például az engedményezés esete.[425]

1.12.6. Az adatvédelmi biztos gyakorlata

[424] Ezzel összhangban konkretizálja a szükségesség elvét az információs társadalommal összefüggő szolgáltatások területén a 2001. évi CVIII. törvény 13/A. § (3) bekezdése: „A szolgáltatónak *az egyéb feltételek azonossága esetén* úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig." Ez az ún. adattakarékosság elve.

[425] ABI 2001, 202.

1. A célhoz kötöttség elvéhez hasonlóan az adatvédelmi biztos szinte minden esetben vizsgálja a szükségesség követelményének való megfelelést is. Ilyen esetek például a következők:

– Az önkormányzati tulajdonú vagy fenntartású intézmények közalkalmazottainak bér- és munkaügyi adatai törvényi felhatalmazás alapján továbbíthatók a képviselő-testület, illetőleg a fenntartó részére; ám a biztos úgy foglalt állást, hogy a képviselő-testület megalapozott döntéséhez általában nem szükséges a közalkalmazottakra vonatkozó adatok „név szerinti bontásban" való közlése, hanem a cél eléréséhez általában elegendő a létszám-, képzettségi és béradatokat közölni.[426]

– Az Avtv. 5. § (2) bekezdését sérti, ha az érintett hajléktalan voltát feltüntetik a munkaügyi központ által elkészített, a reménybeli munkáltatónak bemutatandó ajánlaton;[427]

– Etnikai önazonosságra vonatkozó adatok kezelése sértené a célhoz kötöttség és a szükségesség elvét, ha az iskolában általános, mindenki számára elérhető felzárkóztató programot indítanak.[428]

– Gyermeknevelési támogatás igényléséhez a polgár kötelezhető arra, hogy jövedelmi adatairól tájékoztatást adjon, de nem kötelezhető vagyonnyilatkozat tételére – a támogatás folyósításának feltétele ugyanis a havi nettó jövedelem meghatározottnál alacsonyabb szintje, ám a vonatkozó törvényi szabályozás a vagyoni helyzetre vonatkozó kizáró okot nem tartalmaz, vagyis a cél megvalósulásához az adatkezelés nem elengedhetetlen.[429] A biztos kifogásolta azt, hogy a támogatás igényléséhez használt űrlap szerint elvált szülőnek a válásról szóló bírósági végzést is be kell nyújtania – a cél elérésére a kevesebb személyes adatot tartalmazó házassági anyakönyvi kivonat is alkalmas.[430]

– A közüzemi szolgáltató az ingatlan tulajdonosváltozásának igazolására benyújtott okirat (például adásvételi szerződés) adatai közül csak a szükségeseket kezelheti.[431]

---

[426] ABI 1999, 68.

[427] ABI 1997, 186; hasonlóan ABI 1999, 298 – álláspontunk szerint inkább az 5. § (1) bekezdésének sérelméről van szó, vagyis az adatkezelési cél hiányáról.

[428] ABI 1998, 290.

[429] ABI 1999, 64. Valójában ebben az esetben is hiányzik az adatkezelési cél, mivel az ügyben vizsgált szabályozás szerint a vagyoni helyzetre vonatkozó adatokat jogszerűen nem lehetett figyelembe venni a döntésnél.

[430] ABI 2000, 260.

[431] ABI 1999, 79.

2. A biztosi gyakorlaton belül elkülöníthető azon esetcsoport, amelyben a szükségesség elvének való megfelelés kockázatkezelési és -felmérési célú adatkezelések kapcsán merül fel.

Az adatvédelmi biztos ilyen esetben vizsgálta azt, hogy az adatkezelő valóban vállal-e kockázatot, és ha úgy találta, hogy a szóban forgó szolgáltatás nem jár kockázattal (abban az értelemben, hogy az ügyfél nem kerülhet adósi pozícióba), akkor a kezelhető adatkört az azonosító adatokban határozta meg, a kockázatfelmérést szolgáló vagyoni, jövedelmi adatokra vonatkozó adatkezelés céljának hiányát megállapítva (lásd fent a célhoz kötöttség tárgyalásánál).[432] Ez az állásfoglalás azonban nem vonatkozik azokra az esetekre, amelyekben „az ügylet a bank részéről történő hitelnyújtást is magában foglal", ilyen esetekben „az ügyfél további adatainak kezelése is indokolt lehet".[433] Ha az „adatkezelések […] olyan ügylethez kapcsolódnak, amely során a bank hitelt nyújt, […] szélesebb adatkör kezelése is indokolt lehet".[434] Az adatvédelmi biztos általános érvénnyel mondta ki: „A hitelintézeteknek mint adatkezelőknek mind a bankkártyával kapcsolatos, mind egyéb szolgáltatásaik vonatkozásában olyan helyzetet kell teremteniük, hogy a kezelt adatkör minden egyes ügylet esetében az adott ügylethez kapcsolódó adatkezelési célhoz igazodjon."[435] A szükségesség mértékének megfelelő adatkör csak a meghatározott adatkezelési célhoz képest határozható meg, ezért a biztos javasolta a Magyar Bankszövetségnek olyan szabályzat kidolgozását, amely meghatározta volna az egyes szolgáltatások során kezelni szükséges adatokat,[436] ám a kezdeményezés visszhangtalan maradt.[437]

Más esetben az adatvédelmi biztos javasolt olyan adatkört, amely megítélése szerint meghatározott adatkezelő által meghatározott célból kezelendő: a közműtársaságok során az ügyfél azonosítására álláspontja szerint a név, a lakcím, a fogyasztási hely adatai, valamint a születési hely, idő és az édesanya neve szolgálhat, mivel ezek „a fogyasztót az őt terhelő változás-bejelentési kötelezettség elmulasztása esetén is azonosíthatóvá teszik a személyi

[432] ABI 1999, 253.

[433] ABI 1999, 253.

[434] ABI 1999, 281.

[435] ABI 1999, 290.

[436] ABI 1999, 98; ABI 1999, 290.

[437] ABI 2000, 90.

adat- és lakcímnyilvántartásból".[438] A személyi igazolványszám kezelése azonban hasonló esetben „jogellenes, de ezzel együtt célszerűtlen is".[439]

3. A szükségességgel (és a célhoz kötöttséggel) hozható kapcsolatba az a másik esetcsoport is, amely hatóságok (adóhatóság, rendőrség stb.) adatkéréseinek megítélésével kapcsolatos. Ezek az esetek párhuzamba állíthatók a fent tárgyalt kockázatelbírálással kapcsolatos ügyekkel: „a bűnüldözés", a „nyomozás sikerének érdeke", a „közteherviselés" olyan célok, amelyeket az adatkezelés valóban szolgál, ám ezek egyrészt nem minden esetben minősülnek az 5. § (1) bekezdése szerinti, meghatározott, pontosan körülhatárolt célnak, másrészt számos esetben sérül a szükségesség 5. § (2) bekezdésében lefektetett követelménye is.[440]

Jellegzetes, ebbe a csoportba sorolható esetek a következők:

– A rendőrség emberölés ügyében nyomozott, az elkövetés módja alapján az elkövetőről feltételezték, hogy pszichopata. A rendőrség a környékbeli pszichiátriai intézményt minden ott ápolt beteg személyes adatainak továbbítására szólította fel. Az adatkérést az intézmény az adatvédelmi biztos szerint – megfogható gyanú hiányában – jogszerűen tagadta meg.[441] Ezzel ellentétesen foglalt állást a biztos abban az esetben, amelyben a rendőrség bombamerénylet elkövetője után nyomozott, és mivel a bombakészítés módja az interneten is megtalálható, a környéken működő összes internetszolgáltatót felhívta az előfizetők adatainak továbbítására. A vizsgálat ebben az ügyben – álláspontunk szerint tévesen – nem terjed ki a szükségesség követelményére, csupán a formális törvényi felhatalmazásra.[442]

– Bár az állásfoglalásban az adatvédelmi biztos a célhoz kötöttség elvére hivatkozik, álláspontunk szerint ebbe a körbe sorolható az az eset, amelynek során az APEH az önkormányzati adóhatóságtól az önkormányzat területén lévő összes szállásadói tevékenységet folytató személy továbbítását kérte; a biztos szerint „az adatkezelés célja határozza meg az adatfelvételbe bevont érintettek körét és a cél eléréséhez szükséges

[438] ABI 1999, 78.

[439] ABI 1999, 80.

[440] Számos hasonló esetben az adatvédelmi biztos állásfoglalása nem közvetlenül az Avtv.-n, hanem a büntetőeljárási és rendőrségi törvény szabályain alapul; ezeket az ügyeket itt nem tárgyaljuk (lásd például ABI 1998, 247; ABI 1999, 321 stb.).

[441] ABI 1997, 56.

[442] ABI 1997, 76 és ABI 1997, 153; az állásfoglalással kapcsolatban maga a biztos is kétségeit fejezi ki: ABI 1997, 57.

adatfajtákat"; „[…] amennyiben gyanú merül fel arra, hogy bizonyos szállásadó magánszemély adózási kötelezettségének nem, vagy nem megfelelő mértékben tett eleget, úgy arra vonatkozó adatokat kérhet az APEH, azonban minden szállásadóra kiterjedő adatgyűjtést nem folytathat".[443]

– Egy konzultációs beadványra adott válaszában az adatvédelmi biztos kifejti, hogy azokban az esetekben, amelyekben a rendőrség többfelhasználós szerverek egyik felhasználója ellen indult büntetőeljárás során lefoglalja a szervert, „az adatvédelmi törvény […] 5. § (2) bekezdése alapján [és az Rtv. meghatározott rendelkezései alapján] adott esetben lehetne érvelni amellett, hogy a rendőrség lefoglalás helyett más intézkedéseket alkalmazzon […, a] helyzet megítélése azonban az eset körülményeitől függ".[444]

A szükségesség elve alapján kifogásolta az adatvédelmi biztos az – azóta hatályon kívül helyezett – adózás rendjéről szóló törvény azon rendelkezésén alapuló egyes adatkezeléseket: „Az adóhatóság az adózót – a vele szerződéses kapcsolatban állt vagy álló adózók adókötelezettségének, adóalapjának, adókedvezményének, adójának vagy költségvetési támogatásának megállapítása, illetve ellenőrzése érdekében, az adóhatóság törvényben meghatározott eljárásának lefolytatásához – felhívásban nyilatkozattételre kötelezheti az általa ismert, illetve nyilvántartásában szereplő adatról, tényről, körülményről." Az APEH e felhatalmazás alapján kért adatot utazási irodáktól minden olyan magánszeméllyel kapcsolatban, akik egy meghatározott összeget meghaladó részvételi díjú utakra jelentkeztek. A biztos szerint ez „készletező" adatgyűjtés, ráadásul olyan természetes személyek adataira is kiterjed, amelyek nem adózók (ebben az esetben már a jogalap is hiányzik).[445]

4. Az adatvédelmi biztosi gyakorlat is alátámasztja azt, hogy a célhoz kötöttség elvéhez hasonlóan a szükségesség elvének is maradéktalanul érvényesülnie kell a hozzájárulás alapján végzett adatkezelések során is.[446]

5. A fenti említett adattakarékosság elvének előzményeként kiemelendő az adatvédelmi biztos azon állásfoglalása, amelyben arra a kérdésre, hogy a számítógépes hálózat felhasználói szabályzatában rögzített, egyes oldalak látogatására vonatkozó tilalmak ellenőrizhetők-e a látogatott webhelyek naplózásával, úgy foglalt állást, hogy „amennyiben

[443] ABI 1999, 272.

[444] ABI 2000, 288.

[445] ABI 2004, 56.

[446] ABI 1999, 252.

nincs egyéb – kevesebb adatkezeléssel járó – hatékony módja annak, hogy a felhasználói szabályzat rendelkezéseit ellenőrizzék, a naplózás jogszerű".[447]

1.12.7. Az Alkotmánybíróság gyakorlata

Az Alkotmánybíróság gyakorlatában az adatkezelés szükségességének eleme a jogkorlátozás arányosságának vizsgálataként jelenik meg. Az arányosság mint az alapvető jog alkotmányos korlátozásának követelménye éppen egy adatvédelmi tárgyú különvéleményben jelent meg 1990-ben, s azt a testület azóta többé-kevésbé következetesen vizsgálja adatkezelést elrendelő jogszabályok alkotmányossági vizsgálatakor [lásd erről részletesen a 3. § (1) bekezdéséhez fűzött magyarázatot].[448]

Van azonban példa ezzel ellentétes AB-határozatra is; ilyen például az a döntés, amelynek tárgya olyan, rendeleti szintű szabályozás volt, amely névkitűző viselését tette kötelezővé egyes, a belügyminiszter irányítása alá tartozó szervezetek hivatásos és szerződéses állományába tartozó személyek számára.[449] A jogszabály szerint: „A hivatásos és szerződéses állományviszonnyal rendelkező rendőr-, határőr-, illetve a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság szervezetében szolgálatot teljesítő tűzoltó-, valamint polgári védelmi tábornok, főtiszt, tiszt, zászlós és tiszthelyettes […] a társasági, illetve a köznapi öltözetén névkitűzőt visel".

Az Alkotmánybíróság szerint az adott esetben a szabályozás rendeleti szintje nem problematikus, mert az információs önrendelkezési jog korlátozása már törvényi szinten megtörtént: a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló törvény rendelkezése szerint „a fegyveres szerv megnevezését, a hivatásos állomány tagja nevét, továbbá a beosztására, rendfokozatára és kitüntetésére vonatkozó adatot a hivatásos állomány tagja beleegyezése nélkül nyilvánosságra lehet hozni"; a szerződéses jogviszonyban álló személyekkel kapcsolatban pedig érvényesül az Avt. 19. § (2) bekezdésében foglalt azon rendelkezés, amely szerint az állami vagy helyi önkormányzati feladatot, valamint

[447] ABI 2000, 284.

[448] „Egy alapvető jog korlátozásának alkotmányosságához azonban nem elég, hogy egy másik alapvető jog és szabadság érvényesítése és védelme érdekében történik. Az állam csak akkor nyúlhat az alapvető jog korlátozásának végső eszközéhez, ha a másik jog védelme vagy érvényesülése semmilyen más módon nem érhető el, és a korlátozás csak olyan mértékű lehet, amennyi ehhez feltétlenül szükséges." 2/1990. (II. 18.) AB határozat, Sólyom László különvéleménye.

[449] 54/2000. (XII. 18.) AB határozat.

jogszabályban meghatározott egyéb közfeladatot ellátó szervek „hatáskörében eljáró személyek neve és beosztása[450] – ha törvény másként nem rendelkezik – bárki számára hozzáférhető, nyilvános adat". Az Alkotmánybíróság szerint az „érintett szervek […] hivatásos és szerződéses állományú tagjai információs önrendelkezési jogának korlátozása a név, valamint a beosztására, rendfokozatára és kitüntetésére vonatkozó adat tekintetében már az Avtv. és a Hszt. idézett rendelkezésével megtörtént. A Rendelet csupán az alapjog-korlátozás részletszabályait tartalmazza." A testület hivatkozik a 64/1991. (XII. 17.) AB határozatra, amely szerint az alkotmányos jogokat „csupán távolról, közvetetten érintő, technikai és nem korlátozó jellegű" szabályozás rendeleti szinten is történhet. „Az alapjog-korlátozás […] valójában törvényi szinten történt meg, ezért a részletszabályok törvényi felhatalmazáson alapuló rendeleti előírása alkotmányossági szempontból nem kifogásolható." Az AB ezek után vizsgálta magának a névkitűző viselésével történő „nyilvánosságra hozatalnak" mint korlátozásnak a tartalmi alkotmányosságát is. Az AB szerint „az állampolgárok jogainak hatékony védelme érdekében szükséges az, hogy az állam nevében közhatalmat gyakorlók személyének azonosítása, a vele szemben intézkedő hivatalos közeg »egyediesítése« az állampolgár által könnyen elvégezhető legyen", „[a]z állampolgár panaszhoz, jogorvoslathoz való joga ugyanis csak így garantálható". Az arányosság kérdésében a testület úgy foglalt állást, hogy „a legitim cél, az állampolgárok jogainak hatékony megóvása, bármilyen könnyen felismerhető egyedi azonosító jel (például név, szám) alkalmazásával elérhető. A megfelelőbbnek, célszerűbbnek tekintett módszer kiválasztása a jogalkotó hatáskörébe tartozik. Az alkotmányos célnak egyaránt megfelelő módszerek közötti választás nem alkotmányossági kérdés." Az AB ebben az esetben nem vizsgálta az arányosság körébe a legkevésbé korlátozó móddal kapcsolatos követelményt, a nyilvánosság egyes „szintjeit".

1.12.8. Az irányelv vonatkozó rendelkezései

Az irányelv 6. cikk (1) bekezdésének *c)* pontja szerint a személyes adatokkal szembeni követelmény, hogy azok „gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek" legyenek.

[450] A jelenleg hatályos szöveg szerint: „neve, beosztása vagy besorolása és munkaköre".

1.12.9. Az 5. § további, a célhoz kötöttséggel kapcsolatos rendelkezései

1. A törvény 5. § (3) bekezdése szerint kötelező adatszolgáltatáson alapuló adatkezelést közérdekből lehet elrendelni. A jogalkotó tehát a „közérdekben" határozza meg azt a célt, amelynek érdekében a 3. § (1) és (2) bekezdésében meghatározott jogszabályban kötelező adatkezelés előírható. [Lásd még a 3. § (4) bekezdését, amely szintén „közérdekből" teszi lehetővé személyes adat nyilvánosságra hozatalát. Az Alkotmánybíróság szerint azonban „»közérdek« önmagában nem elég alapjog-korlátozás indokolására – hacsak maga az Alkotmány kifejezetten nem engedélyezi, mint például a kisajátítás esetében. [Vö. 64/1993. (XII. 22.) AB határozat, ABH 1993. 373, 381.] A személyiszám-határozat kifejezetten el akarta kerülni, hogy az adatvédelmet csupán a közérdekre hivatkozva át lehessen törni [15/1991. (IV. 13.) AB határozat, ABH 1991. 40, 42.]"[451]; ezen alkotmánybírósági gyakorlattal a háttérben a rendelkezés normatív tartalma elenyészik.

2. Az 5. § (4) bekezdése szerint „a személyes adatot – akár az érintett hozzájárulásával, akár jogszabály alapján – különösen akkor lehet kezelni, ha ez közérdekű feladat vagy az adatkezelő törvényi kötelezettségének teljesítéséhez, az adatkezelő vagy az adatátvevő harmadik személy hivatalos feladatának gyakorlásához, az érintett létfontosságú érdekeinek védelméhez, az érintett és az adatkezelő között létrejött szerződés teljesítéséhez, az adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez, társadalmi szervezetek jogszerű működéséhez szükséges."

Az Avtv. 5. § (4) bekezdése sajátos megoldással a célhoz kötöttség körében rögzíti azt, hogy egyes, az irányelvben jogalapként meghatározott „kritériumok" mellett személyes adatok kezelhetők (az irányelv vonatkozó szabályait lásd alább).

A szabályozás ilyen módja azt eredményezi, hogy a jogalkotó az 5. § (4) bekezdésben felsoroltak ellenére csak a hozzájárulást, a létfontosságú érdeket, illetve a külön jogszabályban meghatározott eseteket ismeri el jogalapnak; erre irányuló kifejezett szabályozás híján azonban például jogszerű igények érvényesítése, vagy szerződés teljesítése magában nem jogalap. Ezekben az esetekben tehát az adatkezelés jogalapja továbbra is az érintett hozzájárulása vagy a jogszabályi felhatalmazás: ez például arra a következményre vezet, hogy a szerződés teljesítése érdekében végzett adatkezelés is hozzájáruláson alapul [lásd erre a 3. § (7) bekezdéséhez fűzött kommentárt]. A jogalkotó ilyen szándéka önmagában nem kifogásolható: rá kell azonban mutatni arra, hogy az 5. § (4) bekezdése nem alkalmas

[451] 60/1994. (XII. 24.) AB határozat. Vö. Halmai–Tóth 2003, 126.

arra sem, hogy az irányelv 7. cikkében foglalt szabályozást (a tagállami jogalkotóra vonatkozó korlátozást) átültesse. Az irányelv felsorolása taxatív: a tagállamok *csak* a felsorolt esetekben minősíthetnek jogszerűnek adatkezelést. Az Avtv. felsorolása példálódzó: sem a jogalkotó, sem az adatkezelő számára nem tiltott, hogy a felsorolt eseteken kívül rendeljen el vagy végezzen adatkezelést. [Emiatt az 5. § (4) bekezdése nélkülözi a normatív tartalmat is.]

3. Az irányelv 7. cikke „az adatfeldolgozás jogszerűvé tételére vonatkozó kritériumok" alcím alatt szabályozza azt, hogy a tagállamok joga mely esetekben minősíthet valamely adatkezelést jogszerűnek. A 7. cikk szerint: „A tagállamok rendelkeznek arról, hogy a személyes adatok csak abban az esetben dolgozhatók fel, ha:

a) az érintett ahhoz egyértelmű hozzájárulását adta; vagy

b) az adatfeldolgozás 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 adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges; vagy

d) feldolgozásuk az érintett létfontosságú érdekei védelméhez szükséges; vagy

e) az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges, vagy

f) az adatfeldolgozás az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek az 1. cikk (1) bekezdése értelmében védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében."

Az Avtv. a felsoroltak közül az *a)* és a *d)* pontban foglalt jogalapokat tartalmazza kifejezetten, a további esetekben a szabályozás külön – a 3. §-ban meghatározott – jogszabályban (törvényben, önkormányzati rendeletben) történhet. Ez a megoldás számos következménnyel jár: ilyen a nagy mennyiségű szektorális szabályozás, illetőleg az, hogy meghatározott adatkezeléseket a gyakorlat abban az esetben is hozzájáruláson alapulónak (lásd a megfigyelőkamerák működtetésével kapcsolatos adatkezelést) vagy törvényi felhatalmazáson alapulónak minősít (lásd az APEH-adatmentés ügyet), ha az érvényes hozzájárulás kétséges, illetve a jogalkotói szándék nem adatkezelés elrendelésére irányult.

4. Egyes célokkal meghatározott adatállományokról rendelkezik az Avtv. 5. § (5) bekezdése, amely szerint „kizárólag állami vagy önkormányzati szerv kezelheti az állam bűnüldözési és bűnmegelőzési, valamint közigazgatási és igazságszolgáltatási feladatainak

ellátása céljából kezelt bűnügyi személyes adatokat, illetve a szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó adatállományokat." A *bűnügyi személyes adat* fogalmát a 2. § 3. pontja határozza meg: a fogalom „a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adatot" jelenti.

Bűnügyi személyes adatnak valamely személyes adat tehát akkor minősülhet, ha az

a) olyan az érintettel összefüggésbe hozható adat, amely

aa) a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben,

ab) a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett; vagy

b) a büntetett előéletre vonatkozó személyes adat.

A meghatározás *aa)* és *ab)* pontja közötti „vagy" kapcsolat a meghatározásban szereplő „összefüggésben" szó utáni vessző használatából következik. A jogalkotói cél feltételezhetően „és" kapcsolat megfogalmazására irányult (a 2003. évi novella indokolása szerint „a törvény külön meghatározza a „bűnügyi személyes adat" fogalmát, amely nemcsak a büntetett előéletre vonatkozó adatot, hanem a bűnmegelőzéssel és a bűnüldözéssel összefüggésben keletkező információkat is magában foglalja"). Az adatvédelmi biztosi vagy bírósági gyakorlat a fogalmat még nem értelmezte.

A bűnügyi személyes adat fogalma – még az *aa)* és *ab)* elemek közötti „és" kapcsolat esetében is – rendkívül széles; a jogalkotó tehát csak ezen adatok *meghatározott célú* kezelésével kapcsolatban határozza meg az adatkezelők körét. Ez a cél „az állam bűnüldözési és bűnmegelőzési, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása". A tilalom tehát az ettől eltérő célból végzett adatkezelésekre nem vonatkozik, azokat bűnügyi személyes adat vonatkozásában az Avtv. által meghatározott keretek között bármely adatkezelő végezheti (így például a védőügyvéd).

Álláspontunk szerint az 5. § (5) bekezdése nem zárja ki azt, hogy az adatkezelő állami vagy önkormányzati szerv a rendelkezésben meghatározott célból végzett adatkezelés keretében adatfeldolgozót (Avtv. 2. § 16. pontja) vegyen igénybe.

5. A *szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó adatállományok kezelésére vonatkozó rendelkezés* sajátossága, hogy az „adatállományok" kezelését szabályozza, míg az Avtv. 2. § 9. pontja az adatkezelés fogalmát

személyes adatok vonatkozásában határozza meg. Az adatállomány „az egy nyilvántartó rendszerben kezelt adatok összessége” (Avtv. 2. § 18. pontja), míg a személyesadat-nyilvántartó rendszer „személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető” (Avtv. 2. § 17. pontja). A fogalmak elemzését lásd a hivatkozott törvényhelyekhez fűzött kommentároknál.

Az 5. § (5) bekezdése tehát nem zárja ki azt, hogy állami vagy önkormányzati szerven kívül más adatkezelők szabálysértési, polgári peres és nemperes ügyekre vonatkozó személyes adatokat kezeljenek; ám kizárja az ilyen adatokból álló „adatállományok” kezelését a meghatározott körön kívüli adatkezelők számára.

A nyelvtani értelmezés szerint a jogalkotó a szabálysértési, polgári peres és nemperes ügyekre vonatkozó adatállományok esetén az adatkezelést általában megtiltja az állami és önkormányzati szervek körén kívül álló adatkezelők számára. A jogalkotói cél a 2003. évi novella indokolásából nem olvasható ki, ám a szöveg szerint a tilalom kiterjed például az ügyvéd által végzett adatkezelésre is, ha a kezelt adatok rendezettsége eléri azt a szintet, amely az Avtv. meghatározása szerint adatállománynak minősül.

6. Az irányelv 8. cikkének (5) bekezdése szerint: „A bűncselekményekre, büntetőítéletekre vagy biztonsági intézkedésekre vonatkozó adatok feldolgozása kizárólag a hatóság ellenőrzése mellett történhet, vagy ha a nemzeti jog megfelelő külön biztosítékot nyújt, az olyan eltérésekre is figyelemmel, amelyet a tagállamok a megfelelő külön biztosítékot nyújtó nemzeti rendelkezések alapján engedélyezhetnek. Mindazonáltal a büntetőítéletekről teljes körű nyilvántartást csak a hatóság ellenőrzésével lehet vezetni. A tagállamok rendelkezhetnek arról, hogy a közigazgatási szankciókkal vagy polgári ügyekben hozott határozatokkal kapcsolatos adatokat szintén csak a hatóság ellenőrzésével lehessen feldolgozni.” Az Avtv. 5. § (4) bekezdése az irányelv e rendelkezését ülteti át a magyar jogba.

1.13. Az adatok minőségével kapcsolatos követelmények és az univerzális azonosító kód alkalmazásának tilalma

1. Az Avtv. 7. § (1) bekezdése szerint „a kezelt személyes adatoknak meg kell felelniük az alábbi követelményeknek:

a) felvételük és kezelésük tisztességes és törvényes;

b) pontosak, teljesek és ha szükséges időszerűek;

c) tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.”

A *„tisztességes és törvényes”* formula az Európa Tanács adatvédelmi egyezményében és az irányelv angol szövegében szereplő „fairly and lawfully” fordítása. (Az irányelv 6. cikke maga is az ET-egyezmény főbb alapelveit emeli át.) A „tisztességes” adatkezelés a rendelkezés nyomán maga is a jogszerűség követelményévé válik. Az irodalom szerint a „tisztességesség” követelménye olyan háttérklauzula, amelynek alkalmazásával további szabály felhívása nélkül is kimondható a jogellenesség (Auffangklausel).[452] Az irányelv e rendelkezésének indokolása példaképpen azokat az eseteket említi, amelyekben az érintett személyes adatait tudta nélkül, titokban szerzik meg (például telefonlehallgatás útján). A magyar jog szerint – mivel az Avtv. 3. § (1) bekezdése csak a hozzájárulással vagy törvényes (önkormányzati rendeletben meghatározott) felhatalmazással végzett adatkezelést ismeri el *jogszerűnek* – ezek az esetek mindenkor jogszerűtlennek minősülnek, így a jogalkalmazónak nem kell a „tisztességes” adatkezelés követelményére hivatkoznia. Példa lehet, hogy a térfigyelő kamerák működtetése során végzett adatkezeléssel kapcsolatban a magyar jogalkalmazónak mindenképpen vizsgálnia kell az adatkezelés jogalapját (vagyis azt, hogy megvalósul-e az Avtv. 2. § 6. pontjában meghatározott hozzájárulás a figyelmeztető felirat, piktogram elhelyezésével)[453] – vagyis a 7. § (1) bekezdése ilyen esetekben már nem juthat szerephez. [Az irányelv 7. cikke olyan szabályozást is lehetővé tesz a tagállamok számára, amely – a jogszabályi felhatalmazás esetén kívül – az érintett hozzájárulásának híján más esetekben is jogszerűnek minősíti az adatkezelést – a tisztességességre vonatkozó követelmény ilyen szabályozás mellett juthat jelentőséghez. Lásd erre a 3. § (1) bekezdéséhez fűzött kommentárt.]

2. A kezelt adatokkal kapcsolatban az Avtv. rögzíti a *pontosság, a teljesség és szükség szerint az időszerűség* követelményét is. Ezek a követelmények valójában a célhoz kötöttség követelményéhez kapcsolódnak;[454] ha az adatkezelés szempontjából az adat nem pontos, hiányos, vagy nem aktuális, akkor azt törölni vagy helyesbíteni kell. Az irányelv 6. cikk (1) bekezdésének *d)* pontjában foglaltakat az Avtv. 7. § (1) bekezdés *b)* pontja, valamint a 14. § (1) bekezdése (valóságnak nem megfelelő adat helyesbítésének kötelezettsége), valamint a 14. § (2) bekezdésének *c)* pontja (hiányos vagy téves adat törlésének kötelezettsége) ülteti át.[455]

Az időszerűség követelményét az Avtv. csak feltételesen állítja fel. (Az adat abban az esetben is lehet pontos és teljes, ha nem időszerű, mert egy korábbi állapotot tükröz.) Azt,

[452] Dammann–Simitis 1997, 139.

[453] Vö. ABI 2004, 82.

[454] Lásd az irányelv szövegének indokolását: Dammann–Simitis 1997, 137.

[455] Az adatvédelmi biztosi gyakorlatra lásd például ABI 1999, 66.

hogy mely esetekben szükséges az adatok időszerűségét biztosítani, az adatkezelés célja szerint kell megítélni. Az irodalom példája szerint az időszerűség minden lekérdezés időpontjában követelmény, például egy hitelinformációs rendszerben található személyes adatok vonatkozásában.[456]

3. A *tárolás módjára* vonatkozó rendelkezés a célhoz kötöttséghez kapcsolódó szükségesség elvét [Avtv. 5. § (2) bekezdése] konkretizálja – magára az adatkezelés módjára ad előírást, tulajdonképpen az ún. „adattakarékosság elvét" (Datensparsamkeit) előlegezi meg.[457] Ha a tárolás céljához az érintett azonosítása már nem szükséges, úgy az adatot vagy meg kell semmisíteni (Avtv. 2. § 14. pontja), vagy törölni kell (Avtv. 2. § 12. pontja – hogy a két fogalom elhatárolható-e, arra lásd a vonatkozó kommentárokat), vagy azt meg kell fosztani személyesadat-jellegétől. Ez utóbbi akkor történik meg, ha az érintett és az adat kapcsolata többé nem állítható helyre [nemcsak az adatkezelő, hanem harmadik személy által sem – lásd erre a 2. § (1) bekezdését és a hozzá fűzött kommentárt].[458]

1.13.1. Az adatvédelmi biztos gyakorlata

Az adatvédelmi biztos több esetben hivatkozott a tisztességesség követelményére. Ilyen eset volt például az, amelyben egy biztosítótársaság olyan nyilatkozatot követelt ügyfeleitől, amelynek értelmében azok „felmentik valamennyi – a múltban és jövőben egyaránt – őket vizsgáló orvosukat az orvosi titoktartás alól, és felhatalmazzák ezen személyeket, hogy a biztosítók részére egészségi állapotukról adatot szolgáltassanak".[459] A biztos szerint a hozzájárulás ezen módja a tisztességes és törvényes adatfelvétel követelményébe ütközik, s felveti azt is, hogy az azt tartalmazó szerződéses kikötés mint általános szerződési feltétel semmis is lehet (ám ezzel kapcsolatban „hatáskör hiányában" nem foglal állást).

Egy másik esetben bankkártya kibocsátásához igényelt túl széles körű adatkezelést kifogásolva foglalt állást az adatvédelmi biztos. „Nem lehet eltekinteni attól, hogy a szóban forgó esetekben a polgár csak a bank által előírt feltételekkel, a bank által kért adatok rendelkezésére bocsátásával tehet ajánlatot (adhéziós szerződés)", és ilyen esetben „[a]

[456] Dammann–Simitis 1997, 142.

[457] Lásd erről a történeti részt, valamint alább, az elektronikus kereskedelmi törvény adatvédelmi rendelkezéseiről írottakat.

[458] Vonatkozó gyakorlatra lásd például ABI 2000, 110.

[459] ABI 2000, 95.

szerződési tartalom meghatározásából kizárt polgár jogait aránytalanul korlátozó általános szerződési feltétel […] sérti az Avtv. 7. § (1) bekezdésének *a)* pontját […]".[460]

A biztos a 7. § (1) bekezdését hívta segítségül abban az esetben is, amikor a rendőrség által alkalmazott „Felhívás adatközlésre" című nyomtatványon elmulasztották feltüntetni, hogy az adatszolgáltatás megtagadása csak akkor jár szankcióval, ha az jogos indok nélkül történik.[461] Az utóbbi esetben álláspontunk szerint az Avtv. 6. § (1) bekezdése is sérül, tehát a „tisztességesség" követelményét nem feltétlenül kellett segítségül hívni. Az előbbi eset azonban figyelemre méltó: a hozzájárulással kapcsolatban rögzített követelmények érvényesítésének (a hozzájárulás „kiüresedése" megakadályozásának) valóban hatékony eszköze lehet a tisztességességre vonatkozó szabály, különösen, ha azon keresztül a jogalkalmazó (ebben az esetben már a bíróság) a Ptk. általános szerződési feltételekre vonatkozó szabályaihoz is eljut. Lásd erről még a 2. § 6. pontjához fűzött kommentárt.

1.13.2. Az irányelv vonatkozó rendelkezései

Az „adatok minőségéről szóló elvekről" az irányelv 6. cikke szól; ám annak szabályozási köre tágabb, mint az Avtv. 7. § (1) bekezdéséé, magában foglalja az célhoz kötöttség és az azzal összefüggő szükségesség elvét is [6. cikk (1) bekezdés *b)* és *c)* pontja, Avtv. 5. § (1) és (2) bekezdése]. Az irányelv 6. cikkének vonatkozó szabályai az alábbiak:

„(1) A tagállamok rendelkeznek arról, hogy a személyes adatok:

a) feldolgozását tisztességesen és törvényesen kell végezni;

[…]

d) pontosak, és ha szükséges, időszerűek kell legyenek; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy a hibás vagy hiányos adatok, tekintettel gyűjtésük vagy további feldolgozásuk céljaira, törlésre vagy helyesbítésre kerüljenek;

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé. A tagállamok állapítják meg a személyes adatok történelmi, statisztikai vagy tudományos célból, hosszabb ideig történő tárolásának megfelelő garanciáit.

(2) Az adatkezelő feladata gondoskodni arról, hogy az (1) bekezdés rendelkezései teljesüljenek."

[460] ABI 1999, 252; lásd még az 5. § (1) bekezdéséhez fűzött kommentárt.

1.13.3. Az univerzális azonosító kód alkalmazásának tilalma

1. Az Avtv. 7. § (2) bekezdése szerint korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos. E törvényi rendelkezés előzménye az 15/1991. (IV. 13.) AB határozatban rögzített azon tétel, amely szerint „a korlátozás nélkül használható, általános és egységes személyazonosító jel […] alkotmányellenes". A bíróság szerint a megsemmisített szabályozás legfőbb fogyatékossága az volt, hogy az „nem tartalmaz[ott] a személyi szám használatára vonatkozó semmiféle korlátozást vagy feltételt."

Az Alkotmánybíróság határozatában elismerte az általános személyazonosító kód használatának egyes előnyeit: az ilyen kód segítségével „az adatok könnyen hozzáférhetőek, valamint kölcsönösen ellenőrizhetőek lesznek", és további előny, hogy a kódok „költséget és időt takarítanak meg az érintett adatalanyok számára, mert elkerülhetővé teszik az ismételt adatszolgáltatást". A testület szerint azonban az egységes személyazonosító kód használata az előnyöket meghaladó adatvédelmi kockázatokat vet fel: „A személyi szám különösen veszélyes a személyiségi jogokra." Ennek oka, hogy „a személyi szám elterjedt használata esetén a magánszféra megszűnik, mert a legtávolabb eső különböző célú nyilvántartásokból összehozott adatokból előállítható az ún. személyiségprofil, az érintett tetszőlegesen széles tevékenységi körére kiterjedő és intimszférájába is behatoló művi kép, amely ugyanakkor az adatok kontextusból kiragadott volta miatt nagy valószínűséggel torz is." A bíróság mindezek alapján megállapította, hogy „A személyi szám logikája […] ellentétes az adatvédelemhez való jog konstitutív elemeivel: a célhozkötött, osztott információs rendszerek elvével, és azzal a főszabállyal, hogy az adatot az érintettől, annak tudtával és beleegyezésével kell felvenni. Ha az adatvédelem elveit következetesen alkalmazzuk, a személyi szám értelmét veszti, mert „előnyeit" nem lehet kihasználni."

Az AB már a határozatban elébe ment a várható bírálatoknak: „Személyes adatokat természetesen össze lehet kapcsolni névvel, és szükség szerint kiegészítő azonosítók segítségével, mint pl. az anya neve, vagy lakcím. A mai számítógép kapacitások mellett ezek terjedelme sem jelent különösebb problémát. A „természetes" adatok azonban változhatnak (pl. a név férjhezmenéssel vagy névváltoztatással), s előfordulhat, hogy a megkülönböztetéshez további adatok szükségesek; továbbá változó adatok esetén (mint a

[461] ABI 2000, 190. Bár az állásfoglalás a 7. § (1) bekezdés egészét idézi, nézetünk szerint a 7. § (1) bekezdés *a)* pontjának sérelmére utal.

lakcím) az adatok követése és karbantartása szükséges. Az ezzel járó nehézségek és kiadások jelentős tételként jönnek számba az adatfeldolgozás költség/haszon elemzésénél, s minthogy természetes fékjét képezik az indokolatlan adatgyűjtésnek, amire a kéznél lévő személyi szám késztet." A cél tehát természetes fék beépítése volt: ennek érdekében a bíróság kimondta, hogy „az univerzális személyi szám lényegénél fogva ellentétes az információs önrendelkezési joggal. Ezért az Alkotmánnyal csakis a meghatározott célú adatfeldolgozásra korlátozott használatú azonosító szám egyeztethető össze. Az ilyen korlátozott használatú „személyi számot" bevezető törvénynek szabályozási és ellenőrzési garanciákat kell tartalmaznia arra, hogy ezt a számot más összefüggésben ne használhassák. Sem az „állami szféra," sem az államigazgatás egésze nem tekinthető olyan egységnek, amelyen belül egyetlen egységes személyazonosító kódot lehetne bevezetni vagy használni."

A személyi szám-határozat nyomán megszülető Avtv. kifejezetten rögzíti az osztott információs rendszerek követelményét: 7. §-ának (2) bekezdése szerint „Korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos." (Itt jegyezzük meg, hogy ez a szabályozás megfelel az Európai Unió adatvédelmi irányelvének is (az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról), amelynek 8. cikk (7) bekezdése kifejezetten a tagállamokra utalja „a nemzeti azonosító számok és egyéb általános jellegű azonosító jelek feldolgozása" feltételeinek meghatározását.) A következő lényeges lépés hosszabb átmeneti idő után az a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény (a továbbiakban: Szaz. tv.) elfogadása volt.

A Szaz. tv. szerint a polgárt „természetes személyazonosító adataival, vagy az azokból kiválasztott, az adatkezelés célja szerint szükséges és megfelelő mértékű adattal kell azonosítani", ugyanakkor a természetes személyazonosító adatokkal történő azonosítás „kiegészítésére vagy helyettesítésére" az adatkezelő azonosító kódot is használhat [Szaz. tv. 4. § (1)–(2) bekezdése]. A Szaz. tv. meghatározása szerint: „*Az azonosító kód olyan, matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely a polgárt az adatkezelés során egyértelműen azonosítja*." Az azonosító kódot maga törvény minősíti személyes adatnak (5. § (2) bekezdés). A törvény szerint az adózással kapcsolatos nyilvántartás azonosító kódja az adóazonosító jel, az egészségügyi, szociális és a társadalombiztosítási és a magánnyugdíj rendszerrel kapcsolatos nyilvántartások azonosító kódja a társadalombiztosítási azonosító jel (TAJ-szám), a személyiadat- és lakcímnyilvántartás azonosító kódja pedig a személyi azonosító (Szaz. tv. 6. §). A törvény

szerint az azonosító kódokat az adatkezelő „az érintettel, illetve más adatkezelővel való, meghatározott célú kapcsolattartása során csak azt az azonosító kódot használhatja, amelyre a feladatot meghatározó törvény őt felhatalmazza”; más adatkezelő számára az azonosító kód használata csak az érintett („polgár”) előzetes írásbeli hozzájárulásával lehetséges; „a polgárt a hozzájárulás megadása, megtagadása, illetve visszavonása miatt hátrány nem érheti, a hozzájárulás megadásáért bármilyen előny kilátásba helyezése tilos”. A párhuzamosan törvényi felhatalmazás alapján több azonosító kódot kezelő adatkezelő a különböző azonosító kódokat tartalmazó nyilvántartásokat elkülönítetten köteles vezetni. (Szaz. tv. 7. §). A törvény részletesen meghatározza az adóazonosító jel, a tajszám és a személyazonosító jel kezelésének szabályait, valamint az azonosító kódokat alkalmazó alrendszerek együttműködését és annak korlátait. Lényeges, hogy a Szaz. tv. hatálya nem terjed ki a kizárólag belső azonosításra szolgáló technikai kódokra [Szaz. tv. 2. § (2) bekezdése].

2. Alkotmánybíróság gyakorlata az ágazatspecifikus azonosítók kialakult rendszerének alkotmányosságának (illetőleg egy eseteleges általánosan használt azonosító alkotmányellenességének) tekintetében töretlen: legutóbb a 26/2004. (VII. 7.) sz. határozatában foglalt állást hasonló kérdésben, hivatkozva a személyi szám-határozatot („Az Alkotmánybíróság már 1991-ben kimondta, hogy az Alkotmánnyal csakis a meghatározott célú adatfeldolgozásra korlátozott használatú azonosító szám egyeztethető össze”). Álláspontunk szerint csekély az esélye annak, hogy az osztott információs rendszerek elvének a fent ismertetett határozatlan lefektetett elvét a bíróság feladná, még akkor is, ha dr. Sólyom László szerint [a Szaz. tv. elfogadásakor] „…a kevés karakterből álló numerikus azonosító eredeti előnyei a műszaki fejlődés következtében érdektelenné váltak; így a személyi számból az elvi kérdések maradtak fenn”462.

Az adatvédelmi biztosi gyakorlat szintén töretlenül az AB által felállított értelmezést követi: egyedi vizsgálatok esetén a biztos általában olyan általános követelményeket vizsgál, mint az egyes azonosító kódok elkülönült kezelése463, valamely azonosító kód kezelésének jogszerűsége a Szaz. tv. alapján.464 Jogszabály-véleményezések során számos esetben fellépett az osztott információs rendszerek elvének védelmében.465 Az elektronikus közigazgatás megteremtésének igényével együtt gyakran vetik fel a legutóbbi időkben az

[462] Sólyom László: Az adatvédelem és az információszabadság jogi előtörténete Magyarországon, in: Majtényi et al. (szerk.): Az elektronikus információszabadság, Eötvös K. Intézet, 2005., 182. o.

[463] ABI 1998, 95

[464] ABI 1999, 270

[465] ABI 1999, 274

osztott információs rendszerek elvének „meghaladottságát", vagy azt, hogy az azonosítók elkülönített kezelése technológiai eszközökkel biztosítható akkor is, ha azok egy hordozón (például kártyán) vannak jelen. A biztos többször fellépett ilyen kezdeményezések ellen: így pl. 1997-ben a Központi Adategyeztetés és Továbbítás Országos Rendszere (KATOR) ellen. „A tervezett rendszer az adatvédelem nemzetközileg elfogadott elveit (például az adatkezelések célhoz kötöttségének elvét, vagy az osztott információrendszerekre vonatkozó követelményeket) figyelmen kívül hagyja, és olyan rendszer létrehozását célozza meg, amely beleillik az állampolgárok totális ellenőrzését szolgáló egyéb - az elmúlt hónapokban felszínre került - kormányzati törekvések sorába.
A nemzetközi gyakorlatban kevés példát lehet arra találni, hogy az eltérő céllal létrehozott és működtetett adatbázisokat olyan módon kapcsolják össze, ahogyan azt a jelentés javasolja. A személyiségi jogok javaslatból kiolvasható korlátozását ezért is elfogadhatatlannak tartom. E terv megvalósulása oly mértékben sértené az állampolgárok információs önrendelkezési jogát, melyre nincs alkotmányos indok.
Az adatbázisok összekapcsolásának tervezett módja véleményem szerint akkor sem fogadható el, ha azt korszerű számítástechnikai módszerek alkalmazásával, »virtuális adatbázis« és »központi index« használatával kívánják megoldani, vagy ha az »egy személy - egy hely - egy idôpont« elv érvényesítésével azt a hamis illúziót kívánják kelteni, hogy ez a központosított nyilvántartás az állampolgárok érdekét szolgálja."[466]

A gyakorlat ebben is töretlen: a biztos 2003. évről szóló beszámolója szerint az előterjesztők „- valószínűleg csak átmenetileg – elálltak" a három azonosító kártya adatait tartalmazó új kártya bevezetésének tervétől.[467] E megjegyzés előzménye az IM által 2003. áprilisában előterjesztett, majd utóbb visszavont, az Avtv. átfogó módosítására irányuló törvényjavaslat volt (T/3735). Az Avtv. átfogó módosításán túl a javaslat módosította volna a Szaz. tv.-t is a következő rendelkezés beillesztésével: „A polgár részére - kérelmére - megfelelő biztonsági rendszerrel ellátott azonosító kártya is kiadható, amely természetes személyazonosító adatait és azonosító kódjait tartalmazza. Az azonosító kártyát úgy kell kialakítani, hogy adattartalmából az adatkezelő csak azokat az adatokat és azonosító kódokat ismerhesse meg, amelyek kezelésére jogosult." A kezdeményezés célja tehát egy olyan megoldás jogi alapjának megteremtése volt, amely kriptográfiai eszközök alkalmazásával

[466] 72/K/1997

[467] ABI 2004, 43

mentette volna át az osztott információs rendszerek doktrínáját az információs társadalom közegébe. Az adatvédelmi biztos kifejtette aggályait, az alkotmánybírósági tesztig e módosítás el sem jutott.

1.14. A külföldre irányuló adattovábbítás szabályozása

1. Az Avtv. 9. § (1) bekezdésében foglalt főszabály szerint „Személyes adat (beleértve a különleges adatot is) az országból – az adathordozótól vagy az adatátvitel módjától függetlenül – harmadik országban lévő adatkezelő vagy adatfeldolgozó részére akkor továbbítható, ha

a) ahhoz az érintett kifejezetten hozzájárult, vagy

b) azt törvény lehetővé teszi, és a harmadik országban az átadott adatok kezelése, illetőleg feldolgozása során biztosított a személyes adatok megfelelő szintű védelme."

A külföldre irányuló adatáramlás szabályozása az Avtv. hatályba lépése óta többször módosult, s a módosítások során minden esetben enyhült. Az „azonos védelem" koncepcióját felváltotta az irányelv által is ismert „megfelelő védelem" fogalmára építő szabályozás, majd – a 2005. évi XIX. törvény módosítása nyomán – jelentősen enyhült a harmadik országokba irányuló adattovábbítás szabályozása is.

2. A külföldre történő adattovábbítás első jelentős módosítását az Avtv. 2004. január 1-jén hatályba lépett novellája vezette be. A 9. § korábbi szövege szerint: „Személyes adat az országból – az adathordozótól vagy az adatátvitel módjától függetlenül – külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek." A korábbi szöveg számos problémát okozott: az azonos védelem követelményének lefektetésével túlzottan szigorú követelményt határozott meg, ráadásul értelmezési kérdésként merült fel az adatfeldolgozási célú adattovábbítás megítélése.[468]

---

[468] A korábban hatályban volt szöveggel kapcsolatban felmerülő legfontosabb értelmezési kérdés az volt, hogy mely esetben biztosítottak az „adatkezelés feltételei" a külföldi adatkezelőnél. Az Avtv. miniszteri indokolása szerint: „A § az ET Adatvédelmi Egyezményének szabályozásával teremt összhangot, és „alkalmazásával felesleges korlátozni az adattovábbítást olyan országba, amely az Egyezményt törvénybe iktatta." Az indokolásnak megfelelően értelmezte a rendelkezést az adatvédelmi biztos és az igazságügyi miniszter által kiadott tájékoztató [8001/1999. (IK. 6.) IM], amely a levéltári kutatások kapcsán sorolja fel az azonos védelmet nyújtó államokat, valamint az adatvédelmi biztos állásfoglalásai is [például A Citibank Rt. adatkezelésével

Az új szabályozás legfontosabb jellemzője az volt, hogy elvált az Európai Unió tagállamaiba és az ún. „harmadik országokba" (az Avtv. 2. §-ának 20. pontjába foglalt

---

kapcsolatos vizsgálat megállapításait összegző adatvédelmi biztosi ajánlás, 1999. december 22., ABI 2000, 206.]. Az indokolás szerint: „Más esetben viszont meg kell vizsgálni, hogy a magyarországival azonos védelem feltételeit a célország törvényes rendelkezései tartalmazzák-e, s amennyiben nem, azokról egyéb módon – például két- vagy többoldalú szerződésben – gondoskodni kell". Ilyen szerződés született a náci korszak zsidóüldözéseivel kapcsolatos, személyes adatokat tartalmazó iratanyagnak az izraeli Yad Vashem Archívumba történő továbbítása kapcsán [lásd a 13/2002. (I. 31.) Korm. rendeletet a Magyar Köztársaság Kormánya és Izrael Állam Kormánya között a magyarországi levéltárakban őrzött, védett személyes adatot tartalmazó Holocaust-dokumentumok másolatának a jeruzsálemi Yad Vashem, a Holocaust Mártírjai és Hősei Megemlékezési Hivatala részére történő átadása és felhasználása tárgyában készült adatvédelmi szerződés kihirdetéséről, illetve előzményként a náci korszak zsidóüldözéseivel kapcsolatos, személyes adatokat tartalmazó iratok mikrofilmre vételéről és a jeruzsálemi Yad Vashem Archívumba továbbításáról szóló adatvédelmi biztosi ajánlást: 1996. december 31., ABI 1997, 223]. További problémát jelentett annak megítélése, hogy miképp minősül a külföldre irányuló, adatfeldolgozási célból történő adattovábbítás. Az Avtv. korábban hatályos 1. § 5. pontja szerint „adattovábbítás: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik", s a törvénynek a novellát megelőzően hatályos szövege a „harmadik személy" fogalmát nem határozta meg. Értelmezési kérdés volt, hogy az adatkezelő és az adatfeldolgozó közötti adatforgalom adattovábbítás-e (a korábban hatályos magyar szabályozás alapján, amely a harmadik személy fogalmát az irányelvtől eltérően nem határozta meg, ez az álláspontunk szerinti helyes értelmezés), vagy nem is minősül adattovábbításnak (az irányelv fogalomrendszere szerint ez így van, mivel az – a magyar törvénnyel ellentétben – meghatározza a harmadik személy fogalmát, és abból kizárja az adatfeldolgozót). Amennyiben adattovábbításról van szó, úgy alkalmazni kell a külföldre történő adattovábbításra vonatkozó 9. §-t; amennyiben nem, akkor lehetséges olyan érvelés, hogy a külföldön történő adatfeldolgozás nem esik a 9. § hatálya alá, tehát az olyan országokban is végezhető, amelyek nem biztosítják a magyar jognak megfelelő védelmi szintet a személyes adatok számára. További kérdésként merült fel, hogy amennyiben adattovábbításról van szó, úgy ez törvényes felhatalmazáson (magán az Avtv. rendelkezésén) alapul, vagy ahhoz hozzájárulásra van szükség. A lehetőségek tehát az alábbiak voltak: *a)* az adatfeldolgozónak történő adattovábbítás a törvényi meghatározás szerinti „adattovábbítás", amely csak hozzájáruláson alapulhat; *b)* az adatfeldolgozónak történő adattovábbítás törvényen (magán az Avtv. rendelkezésén) alapuló adattovábbítás; *c)* az adatfeldolgozónak történő adattovábbítás nem minősül adattovábbításnak. Álláspontunk szerint az adatfeldolgozó számára történő adattovábbítás az Avtv. 2004. január 1-jéig hatályos szabályozása szerint az Avtv. 2. § 7. *a)* pontja alapján törvényen alapuló adattovábbításnak minősült, s így nem volt szükség az érintett hozzájárulására. Ezen értelmezés szerint nem volt szükséges hozzájárulás az adatfeldolgozónak történő (akár bel-, akár külföldre irányuló) adattovábbításhoz, csupán az, hogy az adatkezelés feltételei a külföldi adatfeldolgozónál minden egyes adatra nézve érvényesüljenek. Ezt az értelmezést támasztja alá az adatvédelmi biztosi gyakorlat is; egy Németországba irányuló, adatfeldolgozási célú adattovábbítás kapcsán például a biztos megállapította, hogy „az Avtv. lehetővé teszi, hogy az adatkezelő egyes adatkezelési műveletek, technikai feladatok ellátásával adatfeldolgozót bízzon meg; ehhez az érintett hozzájárulása nem szükséges" (ABI 2003, 297).

meghatározás szerint ilyennek minősült „minden olyan ország, amely nem tagja az Európai Uniónak") történő adattovábbítás, s ez utóbbi esetben a jogalkotó a „megfelelő védelemnek" az irányelvben foglalt koncepciójával helyettesítette a korábbi, „ekvivalens védelmet" előíró szabályozást[469].

3. A 9. § (1) bekezdését alkalmazni kell mind az adatkezelő, mind az adatfeldolgozó számára történő „adattovábbítás" esetében. (Megjegyzendő, hogy az adatfeldolgozónak történő „adattovábbítás" – az adattovábbítás 2. § 10. pontjában foglalt és a harmadik személy 2. § 19. pontjában foglalt meghatározása szerint – nem minősül az Avtv. által meghatározott adattovábbításnak.)

4. A 9. § (1) bekezdésének körén kívüli esetekben az adatfeldolgozónak történő adattovábbítás nem minősül adattovábbításnak az Avtv. meghatározása szerint, így ezekben az esetekben egyértelmű, hogy az adatfeldolgozási célú adattovábbításhoz nem szükséges az érintett hozzájárulása. Mivel azonban a 9. § (1) bekezdésében szabályozott tényállás esetén a jogalkotó külön előírja azt, hogy a harmadik országba történő adatfeldolgozási célú „adattovábbításhoz" szükséges hozzájárulás/törvényi felhatalmazás, ezért felmerül az az értelmezési kérdés, hogy ilyen esetben – külön törvényi rendelkezés híján – szükséges-e az érintett hozzájárulása ehhez az „adattovábbításhoz". Lehetséges olyan értelmezés, hogy az adatfeldolgozási célú adattovábbításra az Avtv. adatfeldolgozásra vonatkozó rendelkezései felhatalmazzák az adatkezelőt (Avtv. 2. § 8. pontja, 4/A. §), ám álláspontunk szerint abból, hogy a jogalkotó a 9. § (1) bekezdésében a harmadik országba irányuló, adatfeldolgozási célú adattovábbítás esetén külön előírta a megfelelő jogalap megteremtésének kötelezettségét, az következik, hogy ebben az esetben – egyéb adatfeldolgozási célú adattovábbításoktól eltérően – szükség van az érintett hozzájárulására. A külföldre irányuló, adatfeldolgozási célú adattovábbításról lásd még alább a (4) bekezdéshez fűzött magyarázatot.

5. A 2005. évi XIX. törvény által bevezetett módosítás további újdonságot hozott azzal, hogy a harmadik országokba történő adattovábbítás korábban konjunktív feltételei közül kiemelte az érintett hozzájárulását (a) pont)), ezzel lehetővé téve azt, hogy az érintett

[469] Utalni kell arra, hogy az ET adatvédelmi egyezménye – amelyet az 1998. évi VI. törvény hirdetett ki – főszabály szerint – „azonos védelem" fennállása esetén kivételt sem engedve – tiltja a másik szerződő fél területére irányuló adattovábbítás korlátozását. A gyakorlatban ezzel kapcsolatban korábban azért nem merült fel értelmezési probléma, mert az ET-egyezményben részes államok Románia kivételével vagy EU- (EGT-) tagállamok, vagy „megfelelő védelemmel" rendelkeznek a Bizottság határozata szerint – nincs tehát közöttük „harmadik ország". A 2005. évi XIX. törvény által bevezetett módosítás a Romániába történő továbbítás kérdését is megoldotta, lásd ennek elemzését a főszövegben.

információs önrendelkezési jogával élve megfelelő védelmet nem biztosító államba történő adattovábbításhoz is hozzájárulását adja. Ez jelentős enyhítés a korábbiakhoz képest, hiszen ilyen államokba történő adattovábbításra a módosítást megelőzően egyáltalán nem volt mód.

6. A 9. § (1) bekezdésének hatályos szövege tehát két esetben teszi lehetővé a harmadik országba irányuló adattovábbítást: akkor, ha ahhoz az érintett hozzájárult, vagy ha azt törvény lehetővé teszi és konjunktív feltételként a harmadik országban az átadott adatok kezelése, illetőleg feldolgozása során biztosított a személyes adatok megfelelő szintű védelme. A megfelelő védelem fennállásának eseteiről lásd a (2) bekezdést.

1.14.1. Az adatvédelmi biztos gyakorlata

1. Az adatvédelmi biztos számos esetben állást foglalt azzal kapcsolatban, hogy adott esetben az adatkezelés mely szakaszában valósul meg a külföldre irányuló továbbítás. A biztos nem értékelte külföldre irányuló adattovábbításként a külföldi (egyesült államokbeli) kutató magyarországi levéltárban végzett kutatását,[470] ám természetesen külföldre irányuló adattovábbításnak minősül, ha a kutató a kijegyzetelt adatokat külföldre viszi.[471]

2. A külföldre irányuló adattovábbítás bármely módon történhet: annak minősülhet valamely személyes adatokat tartalmazó magánlevél külföldre vitele,[472] személyes adatokat tartalmazó adatbázishoz külföldről történő hozzáférés engedélyezése.[473] Az adatvédelmi biztosi gyakorlatban megjelent az a probléma is, amelyet a külföldre történő adattovábbítás szabályozásának az interneten történő adattovábbításra történő alkalmazása jelent: „az Avtv. 9. §-ának érvényesíthetősége a korábbiakban is kétséges volt, ám azzal, hogy az elektronikus adatforgalom hétköznapi és tömeges lett, a szabály komolytalanná vált”.[474] Az idézett ajánlás még a külföldre történő adattovábbítás korábbi szabályozását bírálja, a helyzet e tekintetben változott: a 9. § hatályos szövege alapján már – az érintett hozzájárulásával - továbbítható személyes adat megfelelő védelmet nem biztosító államba (az interneten – külföldre – történő adattovábbítás témájához lásd még alább az Európai Bíróság gyakorlatát is).

[470] ABI 2000, 370.

[471] ABI 1997, 242.

[472] ABI 1998, 154 – természetesen figyelemmel az 1/A. § (3) bekezdésében meghatározott kivételre.

[473] ABI 2002, 127.

[474] ABI 2002, 185.

1.14.2. Az irányelv vonatkozó rendelkezései

1. Az irányelv 25. cikkében foglalt főszabály szerint „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" (1. bekezdés). Ha valamely ország nem biztosít megfelelő védelmi szintet, akkor arról a tagállamok és a Bizottság értesíti egymást [25. cikk (3) bekezdése]. A Bizottság az irányelv 31. cikk (2) bekezdésében foglalt eljárás szerint határozhat arról, hogy valamely harmadik ország biztosítja-e a megfelelő védelmi szintet [25. cikk (4) és (6) bekezdése]. Ha a Bizottság azt állapítja meg, hogy a harmadik ország a megfelelő védelmi szintet nem biztosítja, akkor „a tagállamok megteszik a megfelelő intézkedéseket az azonos típusú adatoknak a szóban forgó harmadik országba irányuló továbbításának megakadályozására" [25. cikk (4) bekezdése].

A fent idézett főszabály szerint [25. cikk (1) bekezdése] csak azon harmadik országokba lehetséges a tagállamok számára az adattovábbítást jogszerűként szabályozni, amelyek képesek biztosítani az adatok számára a megfelelő védelmi szintet. Ugyanakkor az irányelv 26. cikke számos kivételi kört fogalmaz meg. A 26. cikk (1) bekezdése szerint „a 25. cikktől 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 továbbítássorozata, amely a 25. cikk (2) bekezdése értelmében 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 létfontosságú 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."

A 26. cikkben foglalt szabályozás szerint a tagállami jogalkotónak számos, a magyar jog által nem ismert esetben is lehetővé kell tennie a jogszerű adattovábbítást harmadik országokba. Számos kivételi kör olyan esetekre utal, amelyekben a magyar jog szerint egyébként is hozzájárulás vagy törvényi felhatalmazás szükséges az adatkezeléshez: a nyilvánvaló magyarázat ebben az esetben az, hogy az irányelv és a hazai jog szabályozása az adatkezelés jogalapjait tekintve is lényegesen eltérő.

Az irányelv 25. cikkének (1) bekezdése az „adott ország" által nyújtott védelemről rendelkezik, a (2) bekezdés szerint pedig „a harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni; különös figyelmet kell fordítani az adatok jellegére, a tervezett adatfeldolgozási művelet vagy műveletek céljára és időtartamára, a kiindulási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre". Az irányelv 29. cikke alapján működő munkacsoport az értékelésre vonatkozóan iránymutatást is kiadott (lásd alább).

2. Az irányelv 25. cikk (6) bekezdése szerint: „A Bizottság a 31. cikk (2) bekezdésében említett eljárásnak megfelelően megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít e cikk (2) bekezdése értelmében, az egyének magánéletének, jogainak és szabadságainak védelmére vonatkozó belföldi jog, vagy a vállalt nemzetközi kötelezettségek, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján." Annak értékelése, hogy a védelem megfelelő szintű-e, az irányelv már idézett 25. cikk (2) bekezdése alapján történik. Az értékelés során az irányelv 29. cikke alapján működő munkacsoport szerint figyelembe kell venni:

– a célhoz kötöttség elvének érvényesülését;

– az adatminőség és arányosság elvét;

– az átláthatóság elvét (amelyet a munkacsoport a céllal és az adatkezelő személyével kapcsolatos információ nyújtásának kötelezettségével azonosít);

– az adatbiztonság elvét; a hozzáférés, helyesbítés és tiltakozás jogának biztosítását;

– a továbbítással kapcsolatos korlátozásokat (e követelmény azt jelenti, hogy a szabályozás szerint a címzett az adatokat csak olyan további címzettnek továbbíthatja, amelynél az adatkezeléssel kapcsolatos elvek teljesülnek).[475]

A Bizottság ez idáig *Svájc, Argentína, Guernsey, Man szigete,* valamint *Kanada* és az *Egyesült Államok Kereskedelmi Minisztériuma által kibocsátott ún. Safe Harbor-irányelvek* illetőleg *az Egyesült Államok Vámügyi és Határvédelmi Irodája számára továbbított, légiutasokra vonatkozó adatok* esetében állapította meg azt, hogy a harmadik ország (vagy az adott instrumentum) a személyes adatok számára „megfelelő védelmet" nyújt.[476] Míg azonban Svájc, Argentína, Guernsey és Man szigete esetében a megfelelő védelem fennállása további vizsgálatot nem igényel, addig Kanada és az Egyesült Államok esetében további feltételeknek is teljesülnie kell. A vonatkozó bizottsági határozat szerint Kanada csak abban az esetben biztosít megfelelő védelmet, ha az adattovábbítás címzettje a Personal Information Protection and Electronic Documents Act hatálya alá esik. Az Egyesült Államokba történő adattovábbítás esetén csak akkor biztosított a megfelelő védelem, ha a továbbítás a Bizottság és az Egyesült Államok Kereskedelmi Minisztériuma között létrejött ún. Safe Harbor Agreementben meghatározott követelmények teljesítését önként vállaló (a Safe Harbor-

---

[475] European Commission. *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection directive* (24 July 1998), http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp12en.htm.

[476] Lásd a Bizottság 2000. július 26-i, az Európai Parlament és Tanács 95/46/EK irányelve szerinti határozatát a személyes adatok számára Svájcban biztosított megfelelő védelemről (2000/518/EK), a Bizottság 2000. július 26-i, az Európai Parlament és Tanács 95/46/EK irányelve szerinti határozatát a személyes adatok számára az Egyesült Államok Kereskedelmi Minisztériuma által kibocsátott Safe Harbor-irányelvek és az ezekhez kapcsolódó gyakran ismételt kérdések által biztosított megfelelő védelemről (2000/520/EK), a Bizottság 2001. december 20-i, az Európai Parlament és Tanács 95/46/EK irányelve szerinti határozatát személyes adatok számára a kanadai Personal Information Protection and Electronic Documents Act által biztosított megfelelő védelemről (2002/2/EK), a Bizottság 2003. június 30-i, az Európai Parlament és Tanács 95/46/EK irányelve szerinti határozatát a személyes adatok számára Argentínában biztosított megfelelő védelemről [C 2003(1731)], a Bizottság 2003. november 21-i határozatát a személyes adatok számára Guernseyn biztosított megfelelő védelemről (2003/821/EK), a Bizottság 2004. április 28-i határozatát a személyes adatok számára Man szigetén biztosított megfelelő védelemről (2004/411/EK) és a Bizottság 2004. május 14-i határozatát az Egyesült Államok Vámügyi és Határvédelmi Irodája rendelkezésére bocsátott, a légiutasok utasnyilvántartási adatállományában tárolt személyes adatok megfelelő védelméről (2004/535/EK).
Az Európai Unióhoz történt csatlakozását megelőzően Magyarország is megfelelő védelmet nyújtó államnak minősült a Bizottság 2000-ben hozott határozata szerint.

programban részt vevő) címzett számára történik. A Bizottság határozata szerint – az abban foglalt követelmények kielégítése mellett – megfelelő védelmet biztosít az Egyesült Államok Vámügyi és Határvédelmi Irodája számára továbbított, az Egyesült Államokból érkező, illetve az oda tartó légijáratokra vonatkozó utasnyilvántartási adatállományokban tárolt személyes adatok vonatkozásában.

1.14.3. Az Európai Bíróság gyakorlata

2003-ban a Lindqvist-ügyben[477] az Európai Bíróságnak előzetes döntéshozatali eljárás során kellett megválaszolnia azt a kérdést, hogy az irányelv 25. cikke szerint harmadik országba történő adattovábbításnak minősül-e az, ha valamely tagállamban egy személy személyes adatokat tölt fel egy internetes oldalra (amely oldalt az adott vagy más tagországban letelepedett szolgáltató tesz elérhetővé [hostol]), és amely adatok így bárki számára elérhetőkké válnak, aki internetkapcsolattal rendelkezik – ideértve a harmadik országokban lévő személyeket is; a Bíróságnak választ kellett adnia arra a kérdésre is, hogy változik-e a tényállás megítélése, ha az oldalt senki nem tölti le harmadik országból, illetőleg ha a szerver harmadik országban van.

A Bíróság észlelte azt, hogy milyen súlyos következményekkel járhatna egy olyan értelmezés, amely a honlapon történő hozzáférhetővé tételt külföldre irányuló adattovábbításként interpretálja. „Ha a 95/46 irányelv 25. cikkét úgy kellene értelmezni, hogy minden olyan esetben, amelyben személyes adatokat töltenek fel egy honlapra, harmadik országba irányuló adattovábbítás megy végbe, akkor az ilyen továbbítás szükségszerűen minden olyan harmadik országba történő továbbítás lenne, amelyekben rendelkezésre állnak az internet-hozzáférés technikai eszközei. Az irányelv IV. fejezetében foglalt különös szabályok alkalmazása így szükségszerűen általánossá válna az interneten végzett műveletekkel kapcsolatban. Így ha a Bizottság a 95/46 irányelv 25. cikkének (4) bekezdése szerint úgy foglalna állást, hogy akár egyetlen harmadik ország nem biztosít megfelelő védelmet, akkor a tagállamoknak meg kellene akadályozniuk, hogy bármely személyes adat felkerüljön az internetre.”[478] A Bíróság úgy foglalt állást, hogy a kérdésben foglalt eset nem minősül harmadik országba történő adattovábbításnak.

[477] C 101/01.

[478] Lindqvist, 69.

A döntésben megjelenik az a motívum is, amely szerint adott esetben nincs szó direkt továbbításról – az adatot azok érik el, akik azt lehívják; a „harmadik országba történő továbbítás" fogalma pedig nem meghatározott az irányelv által.[479] A Bíróság tehát adott esetben szabadon értelmezte a fogalmat. A döntésnek álláspontunk szerint a magyar jogalkalmazói gyakorlatra is hatással kell lennie – a Bíróságéhoz hasonló intrerpretáció az Avtv. értelmezése során könnyen követhető, hiszen a 2. § 10. pontjában meghatározott fogalom szerint nyilvánvalóan nem adattovábbításról van szó a leírt tényállásban (a hozzáférhetővé tétel nem meghatározott harmadik személy számára történik).

1.14.4. A „megfelelő védelem" a magyar jogban

1. Az Avtv. 9. § (2) bekezdése határozza meg azokat az eseteket, amelyekben a magyar adatvédelmi jog elismeri a megfelelő védelem fennállását. E szabály szerint „a személyes adatok megfelelő szintű védelme akkor biztosított, ha

a) az Európai Közösségek Bizottsága – külön törvényben meghatározott jogi aktus alapján – megállapítja, hogy a harmadik ország megfelelő szintű védelmet nyújt,

b) a harmadik ország és a Magyar Köztársaság között az érintetteknek a 11. § szerinti jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban, vagy

c) a harmadik országbeli adatkezelő vagy adatfeldolgozó az adatkezelés vagy adatfeldolgozás szabályainak ismertetésével igazolja, hogy az adatkezelés vagy adatfeldolgozás során megfelelő szinten biztosítja a személyes adatok védelmét, az érintettek jogait és azok érvényesítését, különösen, ha az adatkezelést vagy az adatfeldolgozást az Európai Unió Bizottsága külön törvényben meghatározott jogi aktusának megfelelően végzi.

A 9. § (2) bekezdését a 2005. évi XIX. törvény állapította meg, az 2005. június 1-én lépett hatályba. A korábban hatályos szabályozás szerint „az Európai Unió által meghatározott" megfelelő védelmet csak a „harmadik ország joga" nyújthatta[480]. A módosítás

[479] Lindqvist 56, 59, 60.

[480] Egyes szekorális törvényekben a mai napig megmaradt az ekvivalens védelem követelménye és az az előírást, amely szerint a védelem meghatározott szintje jogszabályhoz kötött. A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény 158. § (1) bekezdése szerint „Nem jelenti a biztosítási titok sérelmét a biztosító által a harmadik országbeli biztosítóhoz vagy harmadik országbeli adatfeldolgozó szervezethez (harmadik országbeli adatkezelő) történő adattovábbítás abban az esetben, ha a biztosító ügyfele (adatalany)

nyomán a korábban szabályozott eset csak egyike azoknak, amelyekben a megfelelő védelem a törvény szerint biztosított. Ezek az esetek a következők:

a) „Az Európai Közösségek Bizottsága – külön törvényben meghatározott jogi aktus alapján – megállapítja, hogy a harmadik ország megfelelő szintű védelmet nyújt". A 2005. évi XIX. törvény 13. § (3) bekezdése szerint „Az Avtv. 9. § (2) bekezdés *a)* pontja szerinti jogi aktuson a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv 25. cikk (6) bekezdése alapján kiadott jogi aktust kell érteni", vagyis azokat a határozatokat, amelyekben a Bizottság Svájc, Argentína, Guernsey, Man szigete, valamint meghatározott adatkezelések vonatkozásában Kanada és az Egyesült Államok által nyújtott védelem megfelelőségét ismerte el (lásd erről fent az (1) bekezdéshez fűzött magyarázatot).

b) „A harmadik ország és a Magyar Köztársaság között az érintetteknek a 11. § szerinti jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban". E körben első helyen az Európa Tanácsa adatvédelmi egyezményét kell említeni. Az 1998. évi VI. törvénnyel kihirdetett egyezmény 12. cikk 2. bekezdése szerint: „Egyik Fél sem tilthatja vagy kötheti külön engedélyhez, a magánélet védelmének kizárólagos céljából, a személyes adatoknak az országhatárokat átlépő áramlását, ha az egy másik Fél területére irányul"; a (3) bekezdés ugyan lehetőséget ad a kivételre, de csak abban az esetben, ha a másik fél szabályozása nem nyújt azonos védelmet.[481] Bár a *legtöbb részes állama tagja az Európai Uniónak (illetőleg az EGT-egyezménynek), az Európa Tanács adatvédelmi egyezményének szerződő felei között van olyan állam (Románia), amely az Avtv. alkalmazásában harmadik országnak minősül.* Mivel Románia adatvédelmi jogának „megfelelőségéről" mindeddig nem született bizottsági határozat, a Romániába történő – hozzájárulás híján, törvény alapján végzett – adattovábbítás esetén a védelem megfelelősége a 9. § (2) bekezdés b) pontja alapján állapítható meg.

---

ahhoz írásban hozzájárult, és a harmadik országbeli adatkezelőnél a magyar jogszabályok által támasztott követelményeket kielégítő adatkezelés feltételei minden egyes adatra nézve teljesülnek, valamint a harmadik országbeli adatkezelő székhelye szerinti állam rendelkezik a magyar jogszabályok által támasztott követelményeket kielégítő adatvédelmi jogszabállyal."

[481] A (3) bekezdés *b)* pontjában szabályozott kivétel a gondolatmenet szempontjából nem releváns.

A multilaterális ET-egyezmény mellett több kétoldalú szerződés is rögzít olyan garanciákat, amelyek a 9. § (2) bekezdés b) pontja szerinti megfelelő védelmet biztosítanak[482].

c) „A harmadik országbeli adatkezelő vagy adatfeldolgozó az adatkezelés vagy adatfeldolgozás szabályainak ismertetésével igazolja, hogy az adatkezelés vagy adatfeldolgozás során megfelelő szinten biztosítja a személyes adatok védelmét, az érintettek jogait és azok érvényesítését, különösen, ha az adatkezelést vagy az adatfeldolgozást az Európai Unió Bizottsága külön törvényben meghatározott jogi aktusának megfelelően végzi."

E rendelkezés megteremti a lehetőséget arra, ahozzájárulás híján, törvény alapján történő adattovábbításra azokban az esetekben is, amelyekben a megfelelő védelem fennállását az irányelv 25. cikk (6) bekezdése szerinti bizottsági határozat nem állapította meg, és a védelmet a b) pont által meghatározott nemzetközi szerződés sem biztosítja. Jogalkalmazói gyakorlat még nem áll rendelkezésre abban a kérdésben, hogy miképpen „igazolja" a külföldi adatkezelő vagy adatfeldolgozó a megfelelő védelem fennállását; ennek garanciáit célszerű a magyar adatvédelmi jog által meghatározott követelményeket rögzítő szerződésbe foglalni. Az Európai Unió Bizottsága által meghatározott, ezen alpont által hivatkozott jogi aktus – a 2005. évi XIX. törvény 13. § (4) bekezdése szerint - a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről szóló, 2001. június 15-i 2001/497/EK bizottsági határozat, illetőleg a személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2001. december 27-i 2002/16/EK bizottsági határozat (e határozatokat a függelékben közöljük).

Felhívjuk a figyelmet arra, hogy álláspontunk a határozatokban foglalt általános szerződési feltételek alkalmazása – bár a 9. § (2) bekezdésének c) pontja szerint biztosítja a megfelelő

---

[482] Lásd a 13/2002. (I. 31.) Korm. rendeletet a Magyar Köztársaság Kormánya és Izrael Állam Kormánya között a magyarországi levéltárakban őrzött, védett személyes adatot tartalmazó Holocaust-dokumentumok másolatának a jeruzsálemi Yad Vashem, a Holocaust Mártírjai és Hősei Megemlékezési Hivatala részére történő átadása és felhasználása tárgyában készült adatvédelmi szerződés kihirdetéséről, a 231/2004. (VIII. 6.) Korm. rendeletet a Magyar Köztársaság Kormánya és az Amerikai Egyesült Államok Kormánya között a magyarországi levéltárakban őrzött, és az Egyesült Államok Holocaust Emlékmúzeuma részére átadott Holocaust-dokumentumokban található személyes adatok védelme tárgyában Washingtonban, 2003. november 5-én létrejött adatvédelmi szerződés kihirdetéséről.

védelmet, tehát lehetőséget ad a 9. § (1) bekezdésének b) pontja szerinti adattovábbításra – önmagában nem biztosítja azt, hogy a külföldi adatkezelőnél/adatfeldolgozónál végzett tevékenység megfelel az Avtv. szabályainak. Harmadik országokba történő továbbítás esetén is különös figyelmet kell fordítani arra, hogy a magyar adatvédelmi jog sajátos – pl. az adatfeldolgozásra vonatkozó – többletkövetelményei érvényesüljenek.

1.14.5. A külföldre irányuló adattovábbítás jogsegélyegyezmény végrehajtása érdekében

1. Az Avtv. 9. § (3) bekezdése szerint „személyes adatok nemzetközi jogsegélyegyezmény végrehajtása érdekében, az egyezményben meghatározott célból és tartalommal továbbíthatók harmadik országba."

A külföldre irányuló adattovábbítás különös esetét szabályozó (3) bekezdés szövegét a 2005. évi XIX. törvény határozta meg, annak értelezésére vonatkozó jogalkalmazói gyakorlat még nincs. A rendelkezés sajátossága, hogy a jogsegélyegyezmény végrehajtása céljából végzett adatkezelések esetében az érintett hozzájárulása nélkül is módot ad az adattovábbításra megfelelő védelem hiányában is.

1.14.6. Adattovábbítás az Európai Gazdasági Térségbe

1. A 9. § (4) bekezdése szerint az *Európai Gazdasági Térség tagállamaiba* irányuló adattovábbítást úgy kell tekinteni, mintha a Magyar Köztársaság területén belüli adattovábbításra kerülne sor.[483] E rendelkezés kapcsán is fel kell hívni a figyelmet arra, hogy a „harmadik személy" és az „adattovábbítás" fogalmának meghatározásából az következik, hogy az adatfeldolgozónak történő továbbítás nem minősül az Avtv. szerinti adattovábbításnak, ám a 9. § (1) bekezdésben a jogalkotó mégis rendelkezik az adatfeldolgozónak történő továbbításról is.

[483] Ez a rendelkezés – a novella többi szabályától eltérően – a Magyar Köztársaságnak az Európai Unióhoz történő csatlakozásáról szóló nemzetközi szerződést kihirdető törvény hatálybalépésének napján, 2004. május 1-jén lépett hatályba. Szerencsére már nincs gyakorlati jelentősége annak a kérdésnek, hogy miképp kellett megítélni az EU tagállamaiba irányuló adattovábbításokat a korábbi 9. § helyébe lépett 9. § (1) bekezdés hatálybalépésétől, 2004. január 1-jétől 2004. május 1-jéig terjedő átmeneti időszakban, tekintettel arra, hogy az (1) bekezdés nyilvánvalóan az EU-n kívüli, az irányelv fogalomhasználata szerinti „harmadik országokba" irányuló adattovábbításról szól.

Az EGT területén végzett adatfeldolgozással kapcsolatban felmerülő kérdés, hogy vajon a magyar törvény által előírt, az irányelvből nem következő és a tagállami jogokban általában ismeretlen többletkövetelményeknek érvényesülniük kell-e akkor, ha a Magyar Köztársaság területén végzett adatkezeléshez tartozó adatfeldolgozást valamely EU-tagállam területén végzik. Az Avtv. ezen sajátos követelményei a következők:

a) az adatfeldolgozóként igénybe vehető alanyok körének meghatározása [Avtv. 4/A. § (4) bekezdése];

b) az adatfeldolgozói tevékenységi kör szűk meghatározása, amely az Avtv. 2. § 16. pontjában foglalt definícióból következik (lásd részletesebben a 2. § 16. pontjához kapcsolódó magyarázatnál);

c) az adatfeldolgozó más adatfeldolgozó általi igénybevételének tilalma [Avtv. 4/A. § (2) bekezdése];

d) az adatfeldolgozó által saját célból végzett adatfeldolgozás tilalma [Avtv. 4/A. § (3) bekezdése].

Az Avtv. hatálya az 1/A. § (1) bekezdése szerint a Magyar Köztársaság területén végzett adatkezelésre és adatfeldolgozásra terjed ki. Az EGT-tagállamban végzett adatfeldolgozás jogszerűségének megítélésekor az adott EGT-tagállam adatvédelmi joga lesz irányadó. Kérdés azonban, hogy az adatfeldolgozásra irányuló szerződésben az adatkezelő köteles-e kikötni azt, hogy a szóban forgó adatfeldolgozás vonatkozásában érvényesüljenek a fenti *a)–d)* pontban írt követelmények.

Egy esetben, az *a)* pontban említett követelmény esetén egyértelmű az, hogy a kötelezettség – mivel az adatkezelő számára fogalmazta meg a jogalkotó – ebben az esetben is érvényesül. Álláspontunk szerint azonban a magyar adatkezelő akkor jár el helyesen, ha a *b)–d)* pontban foglalt kötelezettségeket is rögzíti az adatfeldolgozási szerződésben. Ezt az álláspontot támasztja alá az, hogy a 4/A. § (1) bekezdése szerint az adatkezelő az adatfeldolgozó jogait és kötelezettségeit „e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között” határozhatja meg. Ezt az eljárást indokolja az is, hogy az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért is [Avtv. 18. § (1) bekezdése].

1.15. Az automatizált egyedi döntés magyarországi szabályozása

1. Az Avtv. 9/A (1) bekezdése határozza meg az automatizált egyedi döntés fogalmát, és rögzíti az alkalmazásával kapcsolatos főbb követelményeket. Eszerint „kizárólag számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésére csak akkor kerülhet sor, ha ahhoz kifejezetten hozzájárult, vagy azt törvény lehetővé teszi. Az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani."

Az automatizált egyedi döntésre vonatkozó szabályozás – amely eredetileg a francia adatvédelmi jogból származik[484] – az Avtv. 2003. évi novellájával került a szövegbe. A jogalkotó szándéka az irányelv 15. cikkének megfelelő szabályozás átültetése volt. Az automatizált egyedi döntésnek minősülő eljárások igen elterjedtek azokban a szektorokban, ahol az egyén jellemzőinek értékelése előre meghatározott szempontrendszer szerint, meghatározott algoritmus alapján történik, így például a hitelkockázat, a biztosítási ügylettel kapcsolatos kockázat megítélése során. A jogalkotó emellett a munkavállalók felvételénél, teljesítményük mérésénél történő felhasználás egyre gyakoribbá válásával is indokolja a szabályozás szükségességét.[485] Fontos vizsgálni azt a kérdést is, hogy mennyiben tartozik az automatizált egyedi döntésekre vonatkozó szabályozás hatálya alá az olyan CRM- (customer relationship management, ügyfélkapcsolat-kezelési) megoldások alkalmazása, amelyek az ügyféllel folytatott kommunikáció folyamatának alakítása során támaszkodnak az ügyfélről tárolt személyes adatokra, illetőleg a kommunikációs folyamat hatékonyságának növelése céljából dolgoznak fel ilyen adatokat. Az automatizált egyedi döntés adatvédelmi jogi szabályozásának célja Dammann és Simitis szerint kettős: egyrészt azt célozza, hogy az egyén ne váljon „számítógépes műveletek puszta tárgyává" azáltal, hogy személyük értékelése tárolt adatok alapján, számítógépes úton történik meg, másrészt az is cél, hogy a személyiségi jogot érintő döntéssel kapcsolatos felelősséget telepíteni lehessen.[486]

2. A 9/A. § csak azokban az esetekben alkalmazható, amelyekben az érintett valamely jellemzőinek értékelése *kizárólag* számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozással történik. Az adatvédelmi biztos értelmezése szerint: „Automatizált egyedi döntésről akkor beszélünk, ha a döntési folyamatban való emberi részvétel kizárt, az adatbevitel módja ebből a szempontból irreleváns."[487]

---

[484] Dammann–Simitis 1997, 83; Jay–Hamilton 1999, 209.

[485] Lásd a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény módosításáról szóló 2003. évi XLVIII. törvény 8. §-ához fűzött miniszteri indokolást, valamint Dammann–Simitis 1997, 83.

[486] Dammann–Simitis 1997, 219.

[487] 1245/x/2003–3. sz. ügyirat

Nem kell alkalmazni a rendelkezést abban az esetben, ha az automatizált folyamat eredményeképpen előálló értékelés csupán egy ezt követő emberi döntés alapjául szolgál akár önmagában, akár más tényezőkkel együttesen. Az egyedi döntést azonban az automatizált feldolgozás eredményének ismeretében embernek kell meghoznia.[488] „Az informatika segítséget jelenthet a döntésben, ám semmi esetre sem lehet annak kizárólagos alapja; térnek kell maradnia az emberi értékelés számára."[489]

3. A jogalkotó a rendelkezésben az „adatfeldolgozás" fogalmát használja. Az adatkezelés és adatfeldolgozás fogalmának elemzését lásd föntebb. Álláspontunk szerint a 9/A. § esetében nem helyes az „adatfeldolgozás" fogalmának használata „adatkezelés" helyett (hiszen a rendelkezés tárgya kifejezetten *érdemi* döntés meghozatala a személy valamely jellemzőjének értékeléséről), ám remélhető, hogy a gyakorlatban a fogalomhasználat nem okoz majd problémát.[490]

4. A 9/A. § szövegéből és az irányelv 15. cikkéből sem következik az, hogy az automatizált adatfeldolgozás tárgya kizárólag azon személlyel összefüggésbe hozható személyes adat lehet, amely személyes jellemzőinek értékelésére sor kerül. Az automatizált egyedi döntést megelőző adatfeldolgozás során más személy személyes adatainak feldolgozására is sor kerülhet.[491]

5. A novella indokolása pontosan nem határozza meg, hogy a rendelkezés alkalmazásában mit kell az érintett *„személyes jellemzőjének"* tekinteni, ám támpontot ad annak rögzítésével, hogy „ezt a módszert [az automatizált egyedi döntést] egyre elterjedtebben alkalmazzák például a munkavállalók felvételénél vagy teljesítményének értékelésénél, hitelkérelmek elbírálásánál, biztosítási kockázat megállapításánál". Az irányelv

[488] „Egyedül az számít, hogy a végső döntés nemcsak formálisan ember által hozott egyedi döntés, hanem azért az ember tartalmi felelősséget is vállal." Dammann–Simitis 1997, 219. Ezzel ellentétesen foglal állást a brit törvény elemzése során Jay–Hamilton 1999, 210: „A tilalom csak abban az esetben alkalmazható, ha valamely döntés kizárólag automatizált feldolgozáson alapul. Ez arra utal, hogy bármely emberi beavatkozás, legyen az a legcsekélyebb, elegendő a tilalom alóli mentesüléshez."

[489] Lásd az irányelv e cikkéhez kapcsolódó indokolást: Dammann–Simitis 1997, 216. skk., Drobesch–Grosinger 2000, 278. skk.

[490] Az „adatfeldolgozás" szó használatának magyarázata lehet az irányelv fogalomrendszere (a „data processing" mint általános, az adatkezelési cselekmények összességére használt fogalom, melynek hivatalos fordítása „adatfeldolgozás") és a magyar szabályozásban használt definíciórendszer közötti eltérés. Lásd erről fentebb a 2. § 15. pontjához fűzött magyarázatot.

[491] A brit adatvédelmi szabályozás például nem egyértelmű e kérdésben, vö. Jay–Hamilton 1999, 211.

szerint „személyes szempontok”[492] „a munkahelyi teljesítmény, a hitelképesség, a megbízhatóság az életvitel stb.”

Dammann és Simitis szerint az irányelv alkalmazásában nem minősül „személyes szempontnak” az „orvos-fiziológiai értékek megállapítása és ezeknek valamely indikátorba sűrítése (vérvizsgálat, fertőzéssel szembeni ellenállás meghatározása), a „reakcióképesség gyorsaságának mérése, vagy a vagyoni helyzet megítélése”.[493] Ugyanakkor automatizált egyedi döntésnek minősül például „a credit scoring eljárása, amely túlmegy a forgalmi adatok kvantitatív-statisztikai elemzésén”, „a szervátültetés recipiensének kiválasztására irányuló eljárás, ha abban orvosi adatok mellett szociális helyzetre utaló adatok is szerepelnek, az állás betöltésére irányuló vagy más pályázatok, ha azok során képességek, készségek, személyiségjegyek és hasonlóan összetett jellemzők játszanak szerepet a feldolgozás során, vagy az olyan eljárások, amelyek a munkavállalók szociális szempontok szerinti besorolására irányulnak végrehajtása céljából”.[494]

Az irányelv alább idézett cikkéhez kapcsolódó indokolás további támpontot nyúlt az automatizált egyedi döntés fogalomkörébe vonható eljárások körülhatárolásához. „A feldolgozásnak a személyre vonatkozó adatokat változóként kell felhasználnia a személyiség standardprofiljának meghatározásához (azt mint jót vagy mint rosszat besorolva), amely mindenképpen kizárja azt az esetet, amelyben a rendszerben nincs meghatározva személyiségprofil; például nem tartozik e meghatározás alá az a helyzet, amelyben egy személy nem tudja kivenni egy bankautomatából a kívánt összeget, mivel hitelkeretét már kimerítette.”[495]

Egyes szerzők jóval bővebben határozzák meg az automatizált egyedi döntések körét az irányelv értelmezésében: „a döntés bármivel kapcsolatos lehet”.[496] Álláspontunk szerint ez az nézet helytelen, a fent idézett véleménnyel egyetértve az irányelv értelmezése során is a szűkebb interpretációval értünk egyet, valamint – különös tekintettel az Avtv. által használt „személyes jellemző”-fogalomra – a magyar adatvédelmi jog értelmezésekor is azt tekintjük irányadónak.

---

[492] A fordítás ebben az esetben is kifogásolható: az irányelv angol szövegében a „personal aspects”, a németben „einzelne Aspekte” áll – az adott kontextusban ezt az irányelv hivatalos fordításánál jobban visszaadja a novella által használt „személyes jellemző”.

[493] Dammann–Simitis 1997, 219.

[494] Dammann–Simitis 1997, 219. skk.

[495] Dammann–Simitis 1997, 217; Drobesch–Grosinger 2000, 279.

[496] „The decision may be about anything […]”, Jay–Hamilton 1999, 210.

6. A magyar szabályozás jellemzője, hogy nem veszi át az irányelv által a döntéssel szemben támasztott azon feltételt, amely szerint csak az a döntés minősülhet automatizált egyedi döntésnek, amely „jogi hatással járna, vagy őket [a személyeket] jelentős mértékben érintené".[497] A 9/A. § hatálya ezért kiterjed olyan döntésekre is, amelyek az irányelv alapján nem minősülnek automatizált egyedi döntésnek.

7. Az automatizált egyedi döntésekkel kapcsolatos szabályozással kapcsolatban a gyakorlatban is felmerült már az az értelmezési kérdés, hogy az üzleti szféra szereplői által egyre gyakrabban alkalmazott *ügyfélkapcsolat-kezelési (CRM-) rendszerek* vajon a 9/A. § hatálya alá esnek-e. Ezen rendszerek az ügyfél egyes (felhasználási szokásaival, az általa generált forgalommal stb. kapcsolatos) személyes adatai alapján a személyt meghatározott kategóriába sorolják, és személyre (illetőleg a meghatározott csoportra) szabott kiszolgálást biztosítanak a szervezet részéről. Egyes esetekben a CRM-rendszer keretében az ügyfél rendelkezésre álló személyes adataiból új személyes adatok generálása is történhet („ügyfélérték").

Elemzésünk során adottnak vesszük azt, hogy a rendszerben az ügyfél személyes adatainak kezelése történik.

A továbbiakban a fent tárgyaltaknak megfelelően előbb azt a kérdést kell megválaszolni, hogy „kizárólag számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozás" történik-e az adott esetben. A 9/A. § nem hatályosul abban az esetben, ha a rendszer csak támogatja az ügyintézőt valamely döntés meghozatalában, az ügyfél besorolásában; ám a fentiek szerint az ügyintéző döntése nem alapulhat kizárólag a CRM-rendszer által végzett elemzésen.

Ezután vizsgálni kell azt, hogy adott esetben „az érintett személyes jellemzőinek értékeléséről" van-e szó.

E ponton mutatkozik meg az irányelv és az Avtv. szabályozásának eltérése, amennyiben az irányelv által feltételül támasztott jellemzők – „jogi hatás", az érintettet „jelentős mértékben érintő" döntés – nyilvánvalóan nem kapcsolódnak a CRM-rendszer üzemeltetéséhez, amennyiben a döntés valóban csak az ügyfélkapcsolat módjára, az érintettnek felkínált termékek körére stb. terjed ki. Az Avtv.-ből azonban e feltételek hiányoznak, így az értelmezés során egyedül a „személyes jellemző"-fogalom releváns.

[497] A brit jog rendelkezése szerint a döntés „jelentős hatással van az egyénre" (significantly affects that individual). A jelentős hatás nem feltétlenül jogi következmény, vö. Jay–Hamilton 1999, 210. Az osztrák adatvédelmi törvény által használt szöveg szorosan követi az irányelvben foglaltakat.

Álláspontunk szerint – különösen az irányelv szabályozásának fent ismertetett céljára, valamint arra, hogy az Avtv. novellájának miniszteri indokolása szerint az automatizált egyedi döntés „szabályait az irányelvben (15. cikk) foglaltakkal összhangban kell megállapítani" – a helyes értelmezés az, hogy a CRM-rendszerek üzemeltetése során automatikus úton, a rendszer által hozott döntések – *amennyiben azok célja kizárólag az ügyfélkapcsolat hatékonyabbá, gördülékenyebbé tétele,* s azok nem járnak együtt a szolgáltatás igénybevételével kapcsolatos lényeges feltételek meghatározásával – nem tekintendők az érintett személyes jellemzőire vonatkozó értékelésnek, s így *nem esnek a 9/A. § hatálya alá.*

8. A 9/A. § (1) bekezdése szerint automatizált egyedi döntés alkalmazására „csak akkor kerülhet sor, ha *ahhoz kifejezetten hozzájárult, vagy azt törvény lehetővé teszi*".

A törvényi felhatalmazással kapcsolatban megjegyzendő, hogy a jogalkotó a 2003. évi novellával az Avtv.-be illesztett szövegben a „lehetővé teszi" megfogalmazást használja, ezért ebben az esetben nem merülnek fel az „elrendeli" szó használatából eredő értelmezési kérdések [lásd erről a 3. § (1) bekezdéséhez fűzött elemzést]. A hozzájárulásnak ki kell elégítenie az Avtv. 2. § 6. pontjából következő feltételeket. Értelmezési kérdés, hogy a 9/A. § (1) bekezdésében a „kifejezett" jelző használata további követelményt támaszt-e a hozzájárulás érvényességével kapcsolatban. Álláspontunk szerint nem: a 2. § 6. bekezdése, valamint annak értelmezése a joggyakorlatban önmagában biztosítja azt, hogy az adatvédelmi jogban a hozzájárulás fogalma minden esetben „kifejezett" hozzájárulásként értelmezendő. (Lásd erről a 2. § 6. pontjához fűzött magyarázatot.)

Az Avtv. szabályozása megengedőbb az automatizált egyedi döntések alkalmazásával kapcsolatban, mint az irányelv. Ez utóbbi kizárólag abban az esetben teszi lehetővé automatizált egyedi döntés alkalmazását, ha az szerződés teljesítéséhez vagy megkötéséhez kapcsolódik (amelyet az érintett kért, vagy jogos érdekeinek biztosítására megfelelő lehetőségei vannak), vagy azt olyan jogszabály írja elő, amely az érintett jogos érdekeit biztosító intézkedéseket is meghatározza. A magyar szabályozás sajátossága, hogy *hozzájárulás alapján egyéb esetekben is lehetővé válik* automatizált egyedi döntés alkalmazása.

Ez a szabályozás magyarázható azzal, hogy teret enged az érintett információs önrendelkezési joga gyakorlásának ebben az esetben is, illetőleg azzal is, hogy a magyar szabályozásban az automatizált egyedi döntés meghatározása szélesebb körű, mint az irányelvben, ezért olyan rendszerek is a szabályozás hatálya alá tartozhatnak, amelyek alkalmazásával nem születnek az adatalanyt „jelentős mértékben érintő", rá nézve „jogi hatással járó" döntések.

Álláspontunk szerint ennek ellenére aggályos adott esetben a hozzájárulás alapú alkalmazásnak ilyen széles körben teret engedni. Az irányelv vitája során az Európai Parlamentben felmerült az a javaslat, hogy az automatizált egyedi döntés a szabályozás szerint hozzájárulás esetében is alkalmazható legyen, ám az indokolás szerint „ha az érintett számára kedvezőtlen hatalmi viszony áll fenn (például munkakereső személy esetében), […] hozzájárulása […] nem jelentene kielégítő garanciát”.[498]

9. A magyar szabályozás mind hozzájárulás alapján, mind törvényi felhatalmazás alapján hozott automatizált egyedi döntés esetén kötelezővé teszi azt, hogy az érintett számára álláspontjának kifejtésére lehetőséget biztosítsanak.

Álláspontunk szerint az érintett álláspontjának kifejtése nem kötelezi az automatizált egyedi döntés alkalmazóját, hogy a döntést felülvizsgálja. (A döntés eredményét az álláspont fogalmilag nem befolyásolja – ilyen esetben a döntés nem minősülhetne automatizált egyedi döntésnek –, az álláspont kifejtésére csak a döntés meghozatalát, a személyes jellemzők értékelését *követően* kerülhet sor.) Az automatizált egyedi döntést alkalmazónak azonban biztosítania kell azt, hogy az álláspont kifejtése alkalmas legyen az érintett jogos érdekeinek védelmére. Ezt biztosíthatja, ha ilyen esetben az álláspont figyelembevételével az automatizált egyedi döntést alkalmazó az értékelést felülvizsgálja. Álláspontunk szerint azonban elégséges az is, ha a döntést alkalmazó az automatizált egyedi döntés nyomán előállt értékelést megismerő személyek, illetőleg szervezetek számára megismerhetővé teszi az érintett állásfoglalását (tehát például a hitelinformációs rendszer üzemeltetője az érintettre vonatkozó adatok között feltünteti az érintettnek saját minősítésével kapcsolatos állásfoglalását). Összefoglalva: a követelmény az, hogy az automatizált egyedi döntést, az abban foglalt értékelést felhasználó, arra támaszkodó személy vagy szervezet minden esetben megismerhesse az érintett állásfoglalását, ha az érintett tett ilyet.

1.15.1. Az irányelv vonatkozó rendelkezései, eltérések a magyar szabályozástól

Az irányelv 15. cikke szerint:

„(1) A tagállamok minden személynek biztosítják a jogot arra, hogy ne terjedhessen ki rájuk olyan döntés hatálya, amely rájuk nézve jogi hatással járna, vagy őket jelentős

[498] Dammann–Simitis 1997, 217. A rendelkezést az irányelvet követve ülteti át például az osztrák és a brit jog (Drobesch–Grosinger 2000, 279; Jay–Hamilton 1999, 211).

mértékben érintené, és amely kizárólag automatizált feldolgozáson alapul, és amelynek célja a rá vonatkozó egyes olyan személyes szempontok kiértékelése, mint például a munkahelyi teljesítmény, a hitelképesség, a megbízhatóság, az életvitel stb.

(2) Ezen irányelv többi cikkére is figyelemmel, a tagállamok úgy is rendelkezhetnek, hogy az első bekezdésben említett döntés hatálya kiterjedhet a személyre, amennyiben a döntést:

a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve, hogy az érintettnek a szerződés megkötése vagy teljesítése iránti kérelmét 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."

Az irányelv 15. cikkének (2) bekezdése a (magyar szabályozáshoz képest szűkebben meghatározott) automatizált egyedi döntés alkalmazására felhatalmazást adó szabályozás mindkét, a tagállami jogalkotó számára lehetővé tett esetében rendelkezik arról, hogy ilyen tagállami szabályozás mellett biztosítani kell azt, hogy az érintett „jogos érdekeinek biztosítására megfelelő biztosítékok állnak rendelkezésre, mint például a véleményének kinyilvánítását lehetővé tévő intézkedések" (kivéve, ha a szerződés teljesítés vagy megkötése iránti kérelmét teljesítik), illetőleg jogszabály által lehetővé tett automatizált egyedi döntés esetén a jogszabálynak rendelkeznie kell „az érintett jogos érdekeit biztosító intézkedésekről" is.

1.15.2. Az automatizált egyedi döntéssel kapcsolatos tájékoztatás joga

1. Az Avtv. 9/A § (2) bekezdése szerint „az automatizált adatfeldolgozás esetén az érintettet – kérelmére – tájékoztatni kell az alkalmazott matematikai módszerről és annak lényegéről.".

Az érintett tájékoztatáshoz való jogát a 9/A. § (2) bekezdése „az automatizált adatfeldolgozás esetén" biztosítja. Eldöntendő, hogy a tájékoztatáshoz való jog kizárólag automatizált egyedi döntés esetén biztosítandó (vagyis akkor, ha „kizárólag számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésére" kerül sor), vagy minden olyan esetben, amelyben az érintett adatait automatikus feldolgozásnak vetik alá.

A 9/A. § alcíme, valamint a 2003. évi novella – kevés támponttal szolgáló – miniszteri indokolása alapján elképzelhető olyan érvelés, amely szerint a tájékoztatáshoz való jog csak az automatizált egyedi döntés keretében végrehajtott automatizált adatfeldolgozás során illeti meg az érintettet.

Az irányelv alább idézett rendelkezése azonban az alkalmazott „logikáról" való tájékoztatási kötelezettség szabályozásának *minimumát* szabja meg akkor, amikor a tagállam számára az automatizált egyedi döntéssel kapcsolatban írja azt elő. Álláspontunk szerint a törvény szövegének nyelvtani értelmezéséből az következik, hogy a 9/A. § (2) bekezdésében szabályozott tájékoztatáshoz való jog nemcsak automatizált egyedi döntés keretében végzett, hanem minden automatizált adatfeldolgozás vonatkozásában megilleti az érintettet. Ez azt jelenti, hogy a tájékoztatási kötelezettség kiterjed olyan adatfeldolgozásokra is, amelyek nem a személyiség jellemzőinek értékelésével kapcsolatosak, ám amelyek tárgya – akár más adatok mellett – az érintett személyes adata.

2. A 9/A. § (2) bekezdése szerint „az alkalmazott matematikai módszerről és annak lényegéről" kell tájékoztatást adni. Az irányelv az „alkalmazott logika" kifejezést használja, a 2003. évi novella miniszteri indokolásának vonatkozó része szerint pedig az érintettet „[k]érelmére tájékoztatni kell az alkalmazott matematikai (logikai) módszerről is".

A rendelkezés szerint az érintettet egyrészt a matematikai módszerről kell tájékoztatni (annak megnevezésével, körülírásával), másrészt ennél mélyebb felvilágosítást kell nyújtani, hiszen a tájékoztatásnak ki kell terjednie a módszer lényegére is.

A tájékoztatás terjedelmének meghatározása nem egyszerű feladat. Az irányelv preambuluma is utal arra, hogy a tájékoztatás joga „nem befolyásolhatja hátrányosan az üzleti titkot vagy a szellemi tulajdont, és különösen a szoftvert védő szerzői jogot", ám „e szempontok nem vezethetnek oda, hogy az érintett nem kap semmilyen tájékoztatást".[499] Az irányelv és ennek nyomán a magyar szabályozás tehát a tájékoztatási kötelezettséget olyan mértékben kívánta meghatározni, amely kellően részletes ahhoz, hogy az érintett adatai sorsáról, ám kellően általános ahhoz, hogy az alkalmazott algoritmussal kapcsolatos üzleti titok vagy az alkalmazott szoftverrel kapcsolatos szerzői jog sérüljön.

Az irányelv alább hivatkozott 12. cikkét értelmezve az irodalom kiemeli, hogy „az érintett számára érthetővé kell tenni azt a logikai struktúrát, amelynek alapján a program lefut".[500] A tájékoztatási kötelezettség nem feltétlenül terjed ki minden felhasznált szoftverre

[499] Preambulum 41. bekezdése.

[500] Dammann–Simitis 1997, 196.

(például az alkalmazott operációs rendszer a szabályozás szempontjából általában irreleváns), illetőleg a szoftver kódjának részleteire sem. Az érintettet elegendő a felhasználói program azon működési elveiről (tragenden Funktionsprinzipien) tájékoztatni, amelyek ismerete elegendő annak megértéséhez, hogy „konkrét személyes adataiból mely módon vezetnek le meghatározott értékelést vagy osztályba sorolást, és ezen értékek milyen jelentéssel bírnak az adatfeldolgozásért felelős adatfeldolgozó rendszerében”.[501]

1.15.3. Az adatvédelmi biztos gyakorlata

Az adatvédelmi biztos értelmezése szerint: „Az alkalmazott matematikai módszerről, illetve annak lényegéről való tájékoztatás akkor felel meg a jogalkotói szándéknak, ha az valóban érdemi tájékoztatás, vagyis az ügyfél számára közérthető.”[502]

1.15.4. Az irányelv vonatkozó rendelkezései

A 9/A. § (2) bekezdése az irányelv 12. cikkének azon rendelkezését ülteti át a magyar jogba, amely szerint: „A tagállamoknak biztosítaniuk kell minden érintett számára a jogot, hogy az adatkezelőtől […] korlátozás nélkül, ésszerű időközönként, túlzott késedelem vagy költség nélkül […] tájékoztatást kapjon a rá vonatkozó adatok automatizált feldolgozása során alkalmazott logikáról legalább a 15. cikk (1) bekezdésében említett automatizált döntések esetében.”

1.16. Adatbiztonsági szabályok a magyar adatvédelmi törvényben

1. Az adatvédelem és az adatbiztonság közötti kapcsolatrendszer egyik eleme, hogy az adatbiztonság hagyományosan az adatvédelmi jog szabályozási tárgya. (Az adatvédelem és az adatbiztonság fogalmáról, valamint a két fogalom összefüggéséről lásd a Bevezetés 2. pontját.)

2. A 10. § (1) bekezdése szerint „az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat

[501] Dammann–Simitis 1997, 196.

[502] 1245/x/2003–3. sz. ügyirat

a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.”. Ez a szabály mind az adatkezelő, mint az adatfeldolgozó számára

– általában előírja az adatok „biztonságáról” való gondoskodás kötelezettségét;

– az Avtv., valamint „egyéb adat- és titokvédelmi szabályok” érvényre juttatásához szükséges technikai, szervezési intézkedések megtételét, az ehhez szükséges eljárási szabályok kialakítását.

Az Avtv. rendelkezéseinek érvényre juttatása álláspontunk szerint úgy értelmezhető, hogy az adatkezelőnek és az adatfeldolgozónak mind a 10. §-ban meghatározott [annak (2) bekezdésében részletezett] adatbiztonsági követelmények érvényesülését biztosítania kell technikai, szervezési intézkedésekkel és eljárások meghatározásával, ám az ilyen intézkedéseknek és eljárásoknak biztosítaniuk kell az Avtv.-ben meghatározott egyéb, *szűkebb értelemben vett adatvédelmi követelmények érvényesülését is*. E törvényhely tehát újabb kapcsolatot teremt adatvédelem és adatbiztonság között: az utóbbit (az adatok technikai védelmét) szolgáló intézkedések célja egyben az adatvédelmi követelményeknek való megfelelés biztosítása is. Ezek az adatvédelmi követelmények mindenekelőtt a 7. § (1) bekezdés *b)* és *c)* pontjaiban rögzített előírások (a kezelt személyes adatok teljesek, pontosak, és ha szükséges, időszerűek; a tárolás módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani). Az adatminőségre vonatkozó előírások érvényesítésén túl a kialakított belső eljárásokkal kell biztosítani [például, hogy a személyes adatok törlése a törvény által előírt esetben például adatkezelés célja megszűnt, törvényben meghatározott határidő lejárt – 14. § (2) bekezdés *d)* pontja] valóban megtörténjen, hogy az adattovábbítási nyilvántartás valóban alkalmas legyen az érintettel szemben fennálló tájékoztatási kötelezettség teljesítésére [12. § (1) bekezdése].

Az adatkezelő és az adatfeldolgozó által megtett technikai és szervezési intézkedések, kialakított eljárási szabályok azonban nemcsak az Avtv. által meghatározott követelmények érvényre juttatását szolgálják, hanem minden olyan intézkedést, eljárást felölelnek, amely „egyéb adat- és titokvédelmi szabályok érvényre juttatásához” szükséges. Ilyen szabályok például a szektorális adatvédelmi szabályozás előírásai, vagy az adatkezelők meghatározott csoportjára vonatkozó, adatbiztonsági előírásokat tartalmazó normák (például a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény 13/B. §-a). A 10. § (1) bekezdésének ebből a fordulatából az is következik, hogy az adatkezelő magatartása akkor is sérti az adatvédelmi jogot, ha a számára irányadó, nem jogszabálynak minősülő normában rögzített adat- vagy titokvédelmi szabályokat megszegi.

1.16.1. Az adatvédelmi biztos gyakorlata

1. Az adatvédelmi biztos vizsgálatai (legalábbis az előzetes ellenőrzés intézményének az Avtv.-be illesztését megelőzően) nem alapultak valamiféle definiált adatbiztonsági követelményrendszerben meghatározott mércén. A legtöbb esetben a biztos az ún. „megyei vizsgálatok" (általában pár nap alatt lefolytatott, valamely megye több adatkezelőjére kiterjedő, hivatalból lefolytatott vizsgálat) során ellenőrizte az Avtv. 10. §-ában rögzített követelményeket.

2. Meghatározhatók azok az adatbiztonsági követelmények, amelyek érvényesülésére vizsgálatai során az adatvédelmi biztos általában hangsúlyt fektetett. Így általában vizsgálta a számítógépes nyilvántartásokban alkalmazott jogosultsági rendszert, illetőleg általában az adatokhoz való hozzáférés szabályozását a szervezeten belül,[503] az adatkezelő által vezetett nyilvántartásból történő adatkérések (-hozzáférések) naplózását, az adattovábbítási nyilvántartás vezetését.[504]

A vizsgálatok kiterjedtek arra, hogy

– egy kórházban az informatikai rendszerhez való hozzáférés során jelszavas védelem, differenciált hozzáférési jogosultságok rendszere érvényesül[505] (máshol: többszintű, beosztáshoz kötött, differenciált védelmi rendszer, jelszavak alkalmazása, iratok sorsa követhető;[506] a kezelőorvos csak saját kóddal juthat hozzá a beteg adataihoz[507]);

– „a papíralapú nyilvántartás tűz- és mozgásérzékelővel ellátott, elkülönített helyiségben, zárható szekrényekben található";[508] „a papíralapú nyilvántartás zárható fémszekrényekben található";[509]

– „a hivatal iratait zárt pincehelyiségben tárolják, ami megfelel az adatbiztonság követelményeinek";[510]

---

[503] ABI 1998, 149.

[504] ABI 1998, 149; ABI 2004, 54.

[505] ABI 1999, 146; hasonlóan ABI 1999, 143; ABI 2004, 64.

[506] ABI 2000, 130.

[507] ABI 1998, 150.

[508] ABI 2000, 133.

[509] ABI 2000, 134.

[510] ABI 2000, 139.

– a Nemzetbiztonsági Szakszolgálat épületébe történő „belépés, az épületekben való közlekedés szigorúan szabályozott és ellenőrzött”.[511]

A vizsgálatok során kifogásolta a biztos például az alábbiakat:

– a rendőrség által az utcán, rádión keresztül végzett priorálást;[512]

– a hálózat és szoftverek sajátosságai, valamint a kapacitás hiánya miatt egyes nyilvántartásokból történő lekérdezések nincsenek naplózva, így a tájékoztatási kötelezettség nehezen vagy nem teljesíthető;[513]

– megoldatlan a telefonon, telefaxon, rádión történő adattovábbítások naplózása, illetőleg az ügyiratokba való betekintés nem kellően dokumentált;[514]

– a kórházi osztályok az iktatóirodába nyitott borítékban küldik az egészségügyi adatokat – olyan szabályozást kell kialakítani, amely biztosítja, hogy csak az férjen hozzá az adatokhoz, aki arra jogosult.[515]

3. Panaszügyek vizsgálata során a biztos az adatbiztonságra vonatkozó követelmények megsértéseként értékelte, hogy egy gazdasági társaság előfizetői adatállományát tartalmazó CD-ROM illetéktelenek számára vált hozzáférhetővé: a cég „adatkezelői minőségében nem gondoskodott megfelelően az előfizetők személyes adatainak biztonságáról, így a személyes adatok védelméhez fűződő jogok súlyosan sérültek”.[516] Fegyelmi felelősség megállapításához vezetett az, hogy egy konténernyi kórházi iratot találtak a MÉH-telepen.[517]

Az Avtv. 10. §-át – az adatbiztonság követelményét – sérti az is, ha az érintettnek postázott küldemény nyíltan tartalmazza az érintett – adott esetben egészségügyi – adatait; a küldeményt zárt borítékban kell postázni.[518] A biztos általában hívta fel a figyelmet arra, hogy az elektronikus levelezés alkalmazása során „tekintettel kell lenni a fokozott biztonsági követelmények érvényesítésére, és amennyiben a továbbított adatok védelme szükséges, a hagyományos rendszer helyett korszerűbb, biztonságosabb adatátviteli rendszert kell kiépíteni”.[519]

---

[511] ABI 2004, 55.

[512] ABI 1998, 149; ABI 2004, 48.

[513] ABI 2000, 138.

[514] ABI 1999, 142.

[515] ABI 1999, 76.

[516] ABI 2000, 82.

[517] ABI 1999, 74.

[518] ABI 2000, 100.

[519] ABI 2000, 88.

4. Egyes esetekben az adatvédelmi biztos magánszféravédő technológiák alkalmazására is felhívta a figyelmet: így az Országos Felsőoktatási Hallgatói Adatbázis kapcsán kialakított állásfoglalásában szorgalmazta a „a bioscrypt, a különféle »egyirányú« rejtjelzési technikák, a kulcsletéti rendszerek, a »hitelesítés azonosítás nélkül« technológiák" alkalmazását;[520] jogszabály-véleményezés során fejtette ki álláspontját a chipkártyaként kibocsátott diákigazolvány adatvédelmi szempontból kielégítő megvalósításáról, szorgalmazva az „anonim kedvezményegységek" alkalmazását és azt, hogy a kártya adattartalma az adatalany számára átlátható legyen;[521] ajánlásban állt ki a nyilvános kulcsú rejtjelzés szabad polgári célú használata mellett.[522] Ezek az állásfoglalások azonban kivételek: a vizsgálatok általában a fenti pontokban bemutatott tárgykörökre szorítkoznak.

5. A 10. § (2) bekezdése az irányelvhez hasonlóan példálódzó felsorolást ad a tekintetben, hogy mely jogosulatlan adatkezelési cselekmények, illetőleg események ellen kell védeni a személyes adatokat. Külön védelmi intézkedések megtételének kötelezettségét a (2) bekezdés már nemcsak az adatkezelő és az adatfeldolgozó, hanem – ha az adatok továbbítása ilyen eszköz igénybevételével történik – a távközlési vagy informatikai eszköz üzemeltetője számára is előírja. Ez a szabályozás álláspontunk szerint hibás: ezen intézkedések megtételének biztosítását az adatkezelő kötelezettségeként kellene előírni (amely kötelezettség természetesen az általa igénybe vett adatfeldolgozó – így a hálózatüzemeltető – tevékenysége folyamán is érvényesülne) – ez a szabályozás állna összhangban a 18. §-ban rögzített felelősségi szabályokkal (vö. az irányelv szabályozásával).

Az Avtv. 18. § (1) bekezdése az adatkezelő veszélyes üzeminek megfelelő felelősségét írja elő „a technikai adatvédelem követelményeinek megszegésével másnak okozott kárért". Ez a felelősségi szabály igen szigorú, különös tekintettel arra, hogy az adatbiztonság területén minden esetben csak a kockázatokkal arányos védelemről lehet szó (az irányelv szerint „ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének"). A biztonsági fenyegetés „elháríthatatlansága" az esetek kis számában bizonyítható, annál gyakrabban az, hogy többletráfordítással, korszerűbb eszközökkel stb. a fenyegetés elhárítható lett volna. A ráfordítások ideális mértéke kockázatelemzés után állapítható meg, és azoknak nem az „adatkezelés körén kívül eső elháríthatatlan oknak" minősülő támadás kivédésére, hanem az

[520] ABI 1998, 269.

[521] ABI 2000, 353. skk.

adatok jellegéhez, az adatkezelő informatikai rendszere veszélyeztetettségéhez kell igazodnia, az adott helyzetben általában elvárható magatartás mércéje szerint.[523]

6. Az irányelv 17. cikkének (1) bekezdése szerint: „A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás 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 adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének."

1.17. A kártérítés mint az adatvédelmi jogsértések szankciója

1. Az Avtv. 18. § (1) bekezdése szerint „az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt köteles megtéríteni. Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért is. Az adatkezelő mentesül a felelősség alól, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő."

Új fejlemény, hogy a polgári jog által szabályozott veszélyes üzemi felelősséget a jogalkotó oly módon terjeszti ki, hogy az a bírói gyakorlat által a veszélyes üzem fogalma alá vont tevékenységekkel okozott károkon kívül meghatározott esetekben a törvény erejénél fogva is fennáll. Az első ilyen fejlemény az volt, hogy a jogalkotó – a Ptk. 1977. évi novellájával – az emberi környezetet veszélyeztető tevékenységgel okozott károkra

---

[522] ABI 2002, 187.

[523] Bár „[a] tíz évre visszamenőleges publikált bírósági döntésekben nem található olyan deliktuális kártérítési eset, ahol az általában elvárható magatartás követelményei alól ki tudta volna magát menteni a károkozó", az orvosi kárfelelősség területét kivéve (Lábady 2004, 94), álláspontunk szerint az informatikai biztonság körében valóban megkülönböztethető a társadalmi elvárhatóság és az objektív elháríthatatlanság. Az elvárhatóságot adott esetben a biztonsági kockázat szintje határozza meg, ehhez képest kell meghatározni az adatbiztonságot szolgáló intézkedéseket (ilyen szabályozásra lásd a hitelintézetekről és pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény 13/B. §-át).

terjesztette ki a veszélyes üzem működéséből eredő károkra vonatkozó szabályokat.[524] A környezetvédelmi jog megoldása azonban más – álláspontunk szerint helyesebb –, mint az Avtv. által követett szabályozás: a környezet védelmének általános szabályairól szóló 1995. évi LIII. törvény a Ptk. szabályait hívja fel, nem tartalmaz önálló szabályt.[525]

2. Abban az esetben, ha az adatkezelő szervezet, és a kárt az adatkezelési műveletet munkaviszonya keretében végző alkalmazott okozta, a bekövetkezett kárért az adatkezelő szervezet az Avtv. 18. § (1) bekezdése alapján felel a károsult harmadik személlyel szemben, míg az alkalmazott felelősségét a munkáltatóval (adatkezelővel) szemben a munkajogi szabályok szerint kell megítélni.[526]

3. Az Avtv. e szakaszához kapcsolódó miniszteri indokolása szerint az objektív felelősségként történő szabályozás oka „az érintetthez viszonyított túlereje, az érintett által gyakorolt befolyásolási lehetőség hiánya, a bizonyítási nehézség". A jogalkotó szerint: „Egy téves adatból származó következményeket figyelembe véve az adatkezelés a veszélyes üzemhez hasonlítható." Álláspontunk szerint helyes az adatkezelő felelősségének kvázi veszélyes üzemi felelősségként történő szabályozása, ám nem szabad eltekinteni attól a körülménytől, hogy az Avtv. szabályainak megsértése általános esetben nem jár bizonyítható, a jogszerűtlen adatkezeléssel okozati összefüggésben álló kárral (legyen az vagyoni vagy nem vagyoni kár).

Egészségügyi, bűnügyi adatok kezelése, hitelinformációs rendszerek üzemeltetése során számos esetben bizonyítható kár.

Ezek az esetek azonban kivételesek. A nem vagyoni kártérítéssel kapcsolatos – alább bemutatott – bírósági gyakorlat alapján kimondható, hogy az Avtv. 18. §-a a legtöbb esetben nem látja el valódi funkcióját (hiszen a legtöbb adatvédelmi jogi jogsértés esetén bizonyítható kár nem merül fel). Álláspontunk szerint a kártérítés jelenleg szabályozott formájában – a Btk. visszaélés személyes adattal elnevezésű tényállásával együttesen és az adatvédelmi hatóság

[524] A Ptk. 345. § (1) bekezdésének második mondata. Lásd erről: Gellért 2001, 1108. A környezetvédelemmel kapcsolatos szabályozás más esetben is adatvédelmi jogi szabályozási megoldások mintájául szolgál: jó példa erre az adatvédelmi audit esete. Lásd Ewer 2002.

[525] Az 1995. évi LIII. törvény 103. § (1) bekezdése szerint: „A környezet igénybevételével, illetőleg terhelésével járó tevékenységgel vagy mulasztással másnak okozott kár környezetveszélyeztető tevékenységgel okozott kárnak minősül és arra a Polgári Törvénykönyvnek a fokozott veszéllyel járó tevékenységre vonatkozó szabályait (Ptk. 345–346. §-ai) kell alkalmazni." Lásd erről Gellért 2001, 1140; lásd még a természet védelméről szóló 1996. évi LIII. törvény 81. §-át.

[526] Lásd a Munka Törvénykönyvéről szóló 1992. évi XXII. törvény VII. fejezetét.

által kiszabható bírság (vagy a nem vagyoni kártérítést felváltó ún. „sérelemdíj") hiányában – egy inadekvát szankciórendszer egyik elemének tekinthető.

4. Mint arra a miniszteri indokolás is utal: „A törvény a Ptk. megoldását követve nem tesz különbséget az objektív alapon megtérítendő vagyoni és a szubjektív alapú nem vagyoni károk között."

A jogirodalom szerint – a Ptk. 355. §-ban foglaltakat követve – a kár négy fajtáját különböztethetjük meg: ezek a beállott értékcsökkenés (damnum emergens), az elmaradt vagyoni előny (lucrum cessans), a nem vagyoni kár, valamint a „hátrány kiküszöböléséhez szükséges kárpótlás vagy költség".[527] Nem problematikus a helyzet, amennyiben értékcsökkenés vagy elmaradt vagyoni előny állapítható meg; szintén nem az, ha a károsult bizonyítani tudja nem vagyoni kárát. Számos – a legtöbb – esetben azonban csak az Avtv. szabályainak megsértése bizonyítható – felmerül a kérdés, hogy az adott esetben van-e mód nem vagyoni kártérítés megítélésére.

5. Ezzel kapcsolatban érdemes röviden áttekinteni a nem vagyoni kártérítés utóbbi évtizedekbeli fejlődéstörténetét a magyar jogban.[528] A Ptk. 1977. évi novellájával került a törvénybe az a szabály, amely szerint: „A károkozó köteles megtéríteni a károsult nem vagyoni kárát, ha a károkozás a károsultnak a társadalmi életben való részvételét, vagy egyébként életét tartósan vagy súlyosan megnehezíti, illetőleg a jogi személynek a gazdasági forgalomban való részvételét hátrányosan befolyásolja." A bírói gyakorlat a Legfelsőbb Bíróság 16. irányelve nyomán – amely a jogalkotó által megfogalmazott vagylagos feltételek (a társadalmi életben való részvétel „tartós" vagy „súlyos" megnehezülése) együttes fennállását írta elő – igen szigorúan értelmezte a nem vagyoni kártérítés megítélésének lehetőségét. A jogirodalom szerint a megszorító értelmezés az irányelv 1989-ben történt hatályon kívül helyezése után is érvényesült a joggyakorlatban, és így a nem vagyoni kártérítés nem funkcionált az általános személyiségvédelem eszközeként,[529] a nem vagyoni kártérítés kompenzációs funkciója hangsúlyosabban érvényesült, mint az elégtétel-funkció.[530]

6. A 34/1992. (VI. 1.) AB határozat megállapította, hogy a 354. § „.ha a károkozás a károsultnak a társadalmi életben való részvételét, vagy egyébként életét tartósan vagy súlyosan megnehezíti, illetőleg a jogi személynek a gazdasági forgalomban való részvételét

[527] Lásd Gellért 2001, 1227. skk.

[528] Lásd ehhez Lábady 1991; Lábady 1992; Gellért, 2001, 1195. skk.; Petrik 2001, 187. skk.

[529] A teljes személyiségvédelem irányába mutató gyakorlatot is bemutat Lábady 1992, 4. Lásd még Petrik 2001, 196.

[530] Lábady 1992, 10.

hátrányosan befolyásolja" szövegrésze alkotmányellenes, és azt megsemmisítette.[531] A 354. § a következő szöveggel maradt hatályban: „A károkozó köteles megtéríteni a károsult nem vagyoni kárát." A jogalkotó ezt követően hatályon kívül helyezte a 354. §-t, és a 355. § (1) bekezdését egészítette ki a nem vagyoni kárra (mint a kár egyik elemére) történő utalással;[532] ennek hatályos szövege szerint: „A kárért felelős személy köteles az eredeti állapotot helyreállítani, ha pedig az nem lehetséges, vagy a károsult azt alapos okból nem kívánja, köteles a károsult vagyoni és nem vagyoni kárát megtéríteni."

Határozatában az Alkotmánybíróság megállapította: „A nem vagyoni kártérítés felelősségi alakzatkénti meghatározásában [...] a jogalkotó nagyfokú *szabadsággal* rendelkezik. E szabadság alkotmányos határait csak az jelenti, hogy a felelősségi szabály nem vezethet *személyek közötti megkülönböztetésre.*"[533] A testület szerint: „Az általános személyiségi jog alkotmányos összefüggésében a jognak (így a polgári jognak is) nemcsak az egyes (egyedi) személyeket kell egyenlő méltóságú személynek tekinteni és kezelni, hanem magának a személyiségnek a különböző szintjeit és tartalmi vonatkozásait tekintve sem lehet különbséget tenni. [...] Az egyenlő méltóság alapjogán esik csorba, s ezért alkotmányellenes, ha a jog (itt a polgári jog) a személyiség valamely (jogi értelemben strukturált) rétegét, tartalmi vonatkozását kedvezményezi, *fölébe helyezi egy másiknak,* illetőleg, ha egyes személyhez fűződő jogok tekintetében *tartalmilag kirekesztő* szabályozással él. [...] A támadott törvényi szabályozásból azonban az egyenlő súlyú védelem nem következik. A tulajdonosi és egyéb vagyoni jogokat ugyanis a polgári jog azzal, hogy *minden jogellenes károkozást szankcionál* – azaz a károkozás általános tilalmát mondja ki –, *a teljes kártérítés* elvével védi (és nem különböztet aszerint, hogy a kár jelentős, avagy bagatell összegű). A nem vagyoni kártérítés intézményénél viszont a helyzet egészen más, ez a jogintézmény a

[531] Az előadó alkotmánybíró Lábady Tamás volt. A határozat nem csak a Ptk. vonatkozó rendelkezését semmisített meg, hanem a Munka Törvénykönyvéről szóló 1992. évi XXII. törvény, illetőleg egy MT rendelet és egy HM rendelet hasonló rendelkezését is.

[532] Lásd az 1993. évi XCII. törvény 15. §-át. A §-hoz fűzött miniszteri indokolás szerint: „A nem vagyoni kár ugyanis nem a felelősség egyes esetei körébe tartozik – ahová a Ptk. jelenleg sorolja –, hanem a kár fogalmának egyik eleme. Ez a helyzet az Alkotmánybíróság határozata folytán még nyilvánvalóbbá vált, hiszen a nem vagyoni kárigény érvényesítésének azok a különleges törvényi előfeltételei – amelyek gyakorlati megfontolásokból még indokolttá tehették, hogy a nem vagyoni kártérítés intézménye a speciális felelősségi alakzatok között kapjon helyet – megszűntek. A törvényjavaslat 40. §-ának (4) bekezdése ennek megfelelően a 354. §-t hatályon kívül helyezi és a Ptk. 355. §-ának (1) bekezdését egészíti ki a kár vagyoni és nem vagyoni elemeire való utalással."

[533] Kiemelés az eredetiben.

kártérítési jogon *belül* nem értelmezhető. Itt ugyanis nincs vagyoni kár, és ezért nem lehet szó »teljes«, illetőleg »nem teljes« kártérítésről sem. A jogellenesség alapja ennélfogva itt nem is a károkozás, hanem a *személyhez fűződő jogsértés*. A nem vagyoni kártérítés követelhetőségét ugyanakkor a polgári jog *a jogsértés következményei szerint differenciálja,* azaz a személyek személyhez fűződő jogait csak a *jogsértés hatása* szerint részesíti vagyoni védelemben, s a nem vagyoni kártérítést a jogi szabályozásban – a következményeket tekintve – a *súlyosabb esetekre* korlátozza. Ez a szabályozás az egyenlő méltóságra vonatkozó megkülönböztetés tilalmába ütközik, azaz személyek közötti *egyéb helyzet szerinti diszkriminációt* valósít meg azáltal, hogy az általános személyiségi joggal védett személyek között olyan ismérvek alapján differenciál, amelyek a személyiségi jogsértésnek *nem szükségszerű feltételei*."[534] A határozat szerint: „Személyek közötti megkülönböztetést jelent különösen, hogy a nem vagyoni kártérítés »élő« jogként szinte kizárólag csak az egészséghez és testi épséghez való alkotmányos jogok védelmére szolgál; a becsület, a jó hírnév sérelme és más hasonló hagyományos iniuriák, a szabadságjogok *vagy akár a modern információs önrendelkezési jog,* továbbá az egyéb nevesített és nem nevesített személyiségi jogok megsértése esetére azonban – a törvényi szűkítés folytán – nem vagy csak kivételesen alkalmazható, annak ellenére, hogy a Legfelsőbb Bíróság irányelve szerint is az intézmény a személyiségi jogok – napjainkban egyre hangsúlyozottabban jelentkező – védelmét hivatott biztosítani."[535]

Az Alkotmánybíróság tehát a nem vagyoni kártérítés fent bemutatott szabályozását mint a diszkrimináció tilalmába ütközőt semmisítette meg.[536] „A nem vagyoni kártérítés feltételeinek fennállása, a személyiségi jogsértés – e jogkövetkezményt is kiváltó – súlyossága és komolysága kérdésében a törvényhozó különbségtételt alkotmányosan nem tehet. Mindezeknek a kérdéseknek az eldöntése – az egyedi tényállások elbírálása során – a bíróságok jogalkalmazási tevékenységére tartozik." A rendelkezés azért minősült alkotmányellenesnek, mert a szabályozás – a vagyoni károk esetében fennálló helyzettel

[534] Kiemelések az eredetiben.

[535] Kiemelés tőlem – *J. A.*

[536] A határozat indokolásának nem idézett részei további alkotmányellenes megkülönböztetést állapítanak meg egyrészt a természetes személyek és a jogi személyek között (mivel a gazdasági forgalomban bekövetkezett hátrány fogalmilag vagyoni kár, ezért „a jogi személyek nem vagyoni kára dogmatikailag is, de a normának a bírói gyakorlatban állandóan és egységesen tulajdonított „élő" normatartalmát tekintve is „üres" tényállás"), másrészt a jogi személyek között (mivel nincs olyan eset, hogy a gazdasági forgalomban részt nem vevő, illetőleg monopolhelyzetben lévő jogi személyek nem vagyoni kárt tudnának bizonyítani, ezáltal a szabályozás az e két csoporton kívül álló jogi személyeknek kedvez).

ellentétben – különböztetett a bagatell és a súlyosabb következményekkel járó nem vagyoni károk között.[537]

7. A határozat kulcsfontosságú az adatvédelmi jog szankciórendszere szempontjából is. A testület az indokolás fent idézett részében utal is arra, hogy a megsemmisített rendelkezés alkalmazásával formálódó „élő jogban" a nem vagyoni kártérítés nem vagy csak kivételesen alkalmazható – egyebek mellett – az információs önrendelkezési jog megsértése esetén is. „Ez a fajta szabályozás egyben diszkriminatív is, mert a megrágalmazottat, a becsületében, személyes vagy lelkiismereti szabadságában megsértettet stb. annak bizonyítására kényszeríti, hogy élete, társadalmi életben való részvétele tartósan vagy súlyosan megnehezült, míg a testi épségét elvesztett, a »testi« jogában megsértett károsult esetében a társadalmi élet, vagy egyébként az élet elnehezülésének a közönséges élettapasztalatokból is nyilvánvaló tényét többnyire nem is kell külön bizonyítani. *Hiányzik tehát a személyiségi jogvédelem ott, ahol az elnehezülés nem bizonyítható vagy be sem következett.* A jogi szabályozás tehát e vonatkozásban is egyéb helyzet szerint diszkriminál, ez pedig az Alkotmány 70/A. § (1) bekezdése szerint megengedhetetlen, ezért alkotmányellenes."[538] Az információs önrendelkezési jog megsértése a legtöbb esetben valóban nem jár a károsult társadalmi életben való részvételének, életének tartós vagy súlyos nehezülésével – az AB határozat nyomán ezt nem is kell bizonyítani. Továbbra is bizonyítandó azonban a *bekövetkezett kár* – s ez elég ahhoz, hogy a legtöbb adatvédelmi sérelem esetén a nem vagyoni kártérítés által biztosított védelmet továbbra is alkalmazhatatlanná, *inadekváttá* tegye.

---

[537] A döntést bírálja Petrik, aki szerint a határozat hibásan tulajdonít a megsemmisített szabályozásnak olyan értelmet, amely szerint az csak az egészség és testi épség védelmét szolgálná. Érvelése szerint az „élet elnehezülése", a „társadalmi életben való részvétel elnehezülése" pedig „kizárólag a személyiség közösségi megítélésének, személyiségének megváltozott értékelése nyomán kialakult helyzetet jelenti, amely tipikusan rágalmazás, becsületsértés, jóhírnév megsértése nyomán következik be." A kizárólag a súlyosabb jogsértésre reagáló nem vagyoni kártérítésnek álláspontja szerint van elvi alapja, sőt előzményei is a magyar magánjogban. Idézi Törő Károlyt, aki szerint „Alkalmasabb a megkülönböztetésre a jogsértés hatása. Ilyen alapon történő korlátozásra szükség van. A jogintézmény tekintélyét is jelentősen csökkentené, ha ez a rendelkezés bármiféle jelentéktelen jogsérelem esetén alkalmazásra kerülne." (Törő 1979, 141. skk.) Petrik – kritikája ellenére – arról számol be, hogy utóbb módosította álláspontját (lásd Petrik 2001, 193. skk.). Lásd még erre Lábady 1991, 13: Lábady Tamás itt kifejezetten Petrikre hivatkozva fejti ki a későbbi döntésnek alapul szolgáló gondolatmenetet. A döntéssel kapcsolatban érdekes továbbá Sólyom megjegyzése, aki azt mint az élethez és emberi méltósághoz való jogot egységben felfogó monista szemlélet megnyilvánulását említi az AB gyakorlatában: Sólyom 2001a, 138.

Az AB szerint „az intézmény [a nem vagyoni kártérítés intézménye] a személyiséget ért sérelmek esetére rendelt polgári jogi jogvédelmi eszköz". A határozat indokolása több helyen is hangsúlyozza ennek a védelmi eszköznek az ellentmondásait: „[…] a nem vagyoni kártérítés jogintézménye […] olyan belső ellentmondásoktól és feszültségektől terhes, hogy az alkotmányossági kérdések a polgári jogi felelősségi rendszer kontextusában – az indítvánnyal ellentétben – csak kevéssé vizsgálhatók. A nem vagyoni károk ugyanis vagyoni mércével megmérhetetlenek, így a polgári jogi *védelem módja* – a kártérítés – *a sérelemhez képest valójában inadekvát.* A nem vagyoni károknak pénzbeli egyenértékük voltaképpen nincs is, így azok szoros értelemben vett megtérítéséről nem is lehet szó. Ezekhez az ellentmondásokhoz járul az a körülmény, hogy az intézmény történetileg büntetőjogi gyökerű."[539] „[…] a jogintézmény a kártérítési jogon belül nem értelmezhető. Itt ugyanis nincs vagyoni kár, és ezért nem lehet szó »teljes«, illetőleg »nem teljes« kártérítésről sem. *A jogellenesség alapja ennélfogva itt nem is a károkozás, hanem a személyhez fűződő jogsértés.* A nem vagyoni kártérítés követelhetőségét ugyanakkor a [döntés idején hatályos] polgári jog a jogsértés következményei szerint differenciálja, azaz a személyek személyhez fűződő jogait csak a jogsértés hatása szerint részesíti vagyoni védelemben, s a nem vagyoni kártérítést a jogi szabályozásban – a következményeket tekintve – a súlyosabb esetekre korlátozza."[540] Az intézmény tehát belső feszültségekkel terhes, nem tárgyalható a kártérítési jog keretein belül – nem véletlen, hogy alkalmazása az adatvédelmi jog területén is ellentmondásos.

1.17.1. A bíróságok gyakorlata

1. Ha az adatvédelmi jogsértéssel okozott kár bizonyítható, akkor a kártérítés intézménye a jelenlegi szabályozás mellett is ellátja funkcióját. Erre példa az a jogeset, amelyben a jogerősen kiszabott szabadságvesztése letöltését megkezdő, majd a törvényességi óvás nyomán lefolytatott új eljárásban csupán megrovásban részesített felperes azért kérte nem vagyoni kártérítés megítélését, mert a bűnügyi nyilvántartás adattartalma nem tükrözte a törvényességi óvást követő eljárások eredményét, vagyis a felperes büntetett előéletűként szerepelt – szolgálati útlevél iránti kérelmét elutasították, elhelyezkedési nehézségei támadtak, nem szerepelt a választási névjegyzékben, és nem vehetett részt egy népszavazáson sem. A Legfelsőbb Bíróság megállapíthatónak látta a nem vagyoni kártérítés megítélésének

[538] Kiemelés tőlem – *J. A.*

[539] Kiemelések az eredetiben.

[540] Kiemelés tőlem – *J. A.*

feltételeit,[541] és az ítéletet – főtárgya tekintetében – helybenhagyta.[542] Egy másik ügyben a bíróság nem vagyoni kártérítést ítélt meg annak a felperesnek, akinek személyes adatait egy telefontársaság hozzájárulása nélkül jelentette meg a telefonkönyvben: bizonyított volt, hogy az érintettet ezután otthonában több alkalommal telefonon zaklatták, és a bíróság szerint: „A zaklatások ismétlődése, az elhangzó fenyegetések a köztudomásnak megfelelően olyan pszichés megterhelést jelentenek, amely már nem vagyoni hátrányt eredményez".[543]

2. A bírósági gyakorlat azonban nem tartja megállapíthatónak a kártérítést olyan esetben, amelyben kár nem bizonyítható. A fent részletesen ismertetett 34/1992. (VI. 1.) AB határozat megszületését követően volt arra irányuló próbálkozás, hogy a nem vagyoni kártérítés intézményének új értelmet adjanak a bírói gyakorlatban. Mivel az eset adatvédelmi tárgyú, az alábbiakban részletesen ismertetjük.

1996 első felében egy bankfúzió előzményeként két bank (a Dunabank és az ING Bank) olyan szerződést kötött, amely szerint D. Bank bizonyos szolgáltatásait a továbbiakban az I. Bank végzi.[544] Ezek a bankszámlavezetéssel, a bankszámlaügyletekkel, valamint a készpénz-helyettesítő fizetőeszközökkel kapcsolatos tevékenység keretében végzett szolgáltatások voltak. A szerződés megkötése után az I. Bank értesítette az ügyfeleket az érintett üzletágak átvételéről.

Az érintett ügyfelek közül néhány magánszemély mindkét banktól tájékoztatást kért arra vonatkozóan, hogy az ING Bank, az adattovábbítás címzettje, miképp jutott személyes adataik birtokába. Az ügyben született adatvédelmi biztosi ajánlás által rögzített tényállás szerint: „A Dunabank [az ügyfeleknek küldött] válaszában kifejtette: az Állami Bankfelügyelettől engedélyt kapott, hogy meghatározott pénzintézeti tevékenységeket – az I. Bankkal kötött megbízási szerződés alapján – az ING Bank útján gyakoroljon. E megbízás során került sor a bankszámla-tulajdonosok személyes adatainak – bankszámlájuk forgalmára, egyenlegére vonatkozó adatoknak és a Dunabankkal kötött szerződésben szereplő egyéb adatoknak – az átadására. […] Az ING Bank hivatkozott arra, hogy a Dunabank Rt.-vel kötött megállapodás alapján látja el a kérdéses bankszámlák vezetését. E szerződéshez az Állami

[541] A Ptk. akkor hatályos rendelkezéseinek megfelelően adott esetben a felperes társadalmi életének tartós megnehezülését.

[542] BH 1992/58. Hivatkozza Lábady 1992, 7 is.

[543] BH 2002/222.

[544] A tényállást az adatvédelmi biztosi vizsgálat alapján foglaljuk össze: lásd a Dunabank Rt. és ING Bank Rt. között létrejött adattovábbítással kapcsolatos adatvédelmi biztosi vizsgálat megállapításait összegző ajánlást, ABI 1998, 220. skk.

Bankfelügyelet is jóváhagyását adta, és ezáltal a Dunaank Rt.-től jogszerűen szerezte meg az ügyfelek bankszámlájával kapcsolatos adatokat."[545]

Az ügyben magánszemélyek fordultak előbb a Dunabankhoz. és az ING Bankhoz tájékoztatást kérve, majd panaszt nyújtottak be az adatvédelmi biztoshoz. Az adatvédelmi biztos megállapította: mivel a Dunabank az adattovábbításhoz nem szerezte be az ügyfelek hozzájárulását, a biztos értelmezése szerint pedig a továbbítás időpontjában hatályos, a pénzintézetekről és pénzintézeti tevékenységről szóló 1991. évi LXIX. törvény (Pit.) sem adott felhatalmazást az adattovábbításra, ezért „azzal, hogy a Dunabank Rt. az ügyfelek banktitoknak minősülő adatait az ING Bank Rt.-nek átadta, mindkét pénzintézet megsértette az adatvédelmi törvény, valamint a [Pit.] előírásait".[546]

Az érintett magánszemélyek ezt követően Dunabank felszámolójához 4 000 000 Ft nem vagyoni kártérítés iránti igényt jelentettek be, „arra hivatkozva, hogy az adós személyhez fűződő jogukat megsértette, amikor hozzájárulásuk nélkül, illetőleg kifejezett tiltakozásuk ellenére átadta személyes, banktitoknak minősülő adataikat az ING Bank Rt. részére, a két pénzintézet között az ügyfelek hozzájárulása nélkül létrejött szerződés alapján".[547] A felszámoló a nem vagyoni kártérítés iránti igényt nem ismerte el, ezért a csődtörvény vonatkozó rendelkezései szerint a polgári bírósághoz továbbította a kérelmeket. „Az elsőfokú bíróság a felek nyilatkozatait, valamint az általuk csatolt okiratok adatait mérlegelve megállapította: az adós azáltal, hogy 1996. március 1-jétől az ING Bankkal kötött szerződése alapján – a kérelmezők hozzájárulása nélkül, kifejezett tiltakozásuk ellenére – átadta az I. Bank részére a kérelmezők banktitoknak minősülő személyes adatait, megsértette a kérelmezők információs önrendelkezési jogában megnyilvánuló személyiségi jogát, amely miatt a kérelmezők a Ptk. 84. §-a (1) bekezdésének *e)* pontja szerint kártérítést követelhettek a polgári jogi felelősség szabályai szerint. A kérelmezők vagyoni kárt nem jelöltek meg. Nem vagyoni kártérítés iránti követelésüket az elsőfokú bíróság alaposnak találta, annak megállapításával, hogy a követelések összege eltúlzott. Az elsőfokú bíróság hivatkozott az Alkotmánybíróság 34/1992. (VI. 1.) AB határozatában foglaltakra és a Ptk. 354. §-ára, melyek alapján nem vagyoni kártérítésként a kérelmezők javára személyenként 100 000 Ft megállapítására látott lehetőséget, és annak nyilvántartásba vételére kötelezte a felszámolót a »d« pontos követelések között. Kötelezte továbbá a felszámolót, hogy a kérelmezők jogi képviselője részére »a« pontos követelésként 3000 Ft ügyvédi munkadíjat fizessen meg 15

[545] ABI 1998, 220–221.

[546] ABI 1998, 227.

napon belül. A kérelmek ezt meghaladó részét az elsőfokú bíróság a végzés indokolásából kitűnően elutasította." Lényeges, hogy a kérelmezők „[v]agyoni igényt nem érvényesítettek, mert vagyonban mérhető káruk nem keletkezett, ezért követelésük alapjaként magát a jogsértést jelölték meg", és ezt az érvelést – amelyet a kérelmezők az Alkotmánybíróság fent ismertetett 34/1992. (VI. 1.) sz. határozatára alapoztak – az elsőfokú bíróság elfogadta.

A Dunabank felszámolója a végzés ellen fellebbezést nyújtott be, amelyben a kérelmezők nem vagyoni kártérítés iránti igényének teljes elutasítását kérte. Az adatvédelmi biztosi eljárásban használt érveken kívül[548] a felszámoló érvelésének középpontjában a felmerült kár, illetőleg annak hiánya állt. „A felszámoló hivatkozott arra is, hogy a kérelmezőknél nem merült fel olyan vagyoni kár, illetőleg nem vagyoni hátrány, amelynek csökkentéséhez vagy kiküszöböléséhez kártérítés megállapítása indokolt lenne. Előadta, hogy a kérelmezők az adataik kezelésével összefüggésben olyan hátrányt nem jelöltek meg, melynek figyelembevételével szó lehetne nem vagyoni kártérítésről. Utalt arra, hogy a Ptk. 355. §-a a károsult vagyoni és nem vagyoni kárának megtérítéséről szól, és ezért nem vagyoni kár esetén is szükséges a károsult részéről valamilyen hátrány megjelölése, melyből a bíróság a nem vagyoni kártérítés meghatározásakor kiindulhat. Hivatkozott arra, hogy az elsőfokú bíróság végzésében alkalmazott Ptk. 354. §-át az Alkotmánybíróság 1993. november 1-jei hatállyal hatályon kívül helyezte, és nem módosította. Állította, hogy a kérelmezőket nem érte semmilyen hátrány, ezért javukra nem vagyoni kártérítés megítélésére még a jogalap megállapítása esetén sem kerülhetne sor. Hivatkozott továbbá arra is, hogy a kérelmezők nem hátrányt szenvedtek az adóstól, hanem kifejezetten előnyt élveztek amiatt, hogy a fellebbezés

---

[547] BH 2002/224.

[548] „Elsődlegesen vitatta az adós kártérítési felelősségének jogalapját. Arra hivatkozott, hogy az I. Bank a kártyaüzletágnak az adóstól való megvásárlását követően felszólította a kártyabirtokosokat, hogy nyilatkozzanak arról: kívánnak-e az I. Bankkal kártyaszámla-szerződést kötni. A kérelmezők nemleges válaszát követően az adós a banktitoknak minősülő adatokat nem adta át az I. Bank részére, hanem azok a D. Banknál maradtak. Állította továbbá azt is, hogy 1996. március 1-jétől az I. Bank Rt. átvette az adós banki alkalmazottai közül azokat, akik a kártyaüzletág tevékenységét végezték, a korábbival azonos helyiségben és azonos számítógépekkel, ennek folytán a kérelmezők banktitoknak minősülő adatai nem váltak szélesebb körben ismertté, mint amilyenben az üzletág átadása előtt voltak. Ezért álláspontja szerint az adós terhére banktitoksértésben, a kérelmezők információs önrendelkezési jogának megsértésében megnyilvánuló személyiségi jogsértést jogszerűen nem lehetett megállapítani. Hivatkozott továbbá arra is, hogy az I. Bank Rt. a kérelmezők személyes adataihoz – mint az adós megbízottja – közreműködőként jutott, amelyhez a kérelmezők az adóssal kötött szerződésük létrejöttekor az üzletszabályzat 3.5 pontjában foglaltak alapján hozzájárultak" (BH 2002/224).

benyújtásáig nem számoltak el az adóssal a kártyaszámláik vonatkozásában, amelyeken az adós […].-t illetően 66 788 Ft, […]-t illetően 43 807 Ft, […]-t illetően pedig 6448,95 Ft tartozást tart nyilván. *Fellebbezésében a felszámoló kiemelten azt kifogásolta, hogy az elsőfokú bíróság magát az adós részére megállapított jogsértést tekintette kárnak, és a jogsértés súlyával arányban álló kártérítést szabott ki, amely jogi álláspontot a Ptk. 355. §-ára figyelemmel nem talált elfogadhatónak.*"[549]

A Legfelsőbb Bíróság helyt adott a fellebbezésnek. Bár egyetértett azzal, hogy az elsőfokú bíróság megállapította az adós Dunabank Rt. kártérítési felelősségének jogalapját, a bíróság nem fogadta el a kérelmezők azon álláspontját, amely szerint azok „ az elsőfokú eljárás során állított nem vagyoni káruk, vagyoni hátrányuk mibenlétét nem jelölték meg abból a jogi álláspontból kiindulva, hogy *csak az adós által elkövetett jogsértést kellett bizonyítaniuk nem vagyoni kártérítési igényük megalapozásához,* amelynek eleget tettek".[550] A Legfelsőbb Bíróság szerint: „Tévesen állították a kérelmezők, hogy az adós nem vagyoni kártérítési kötelezettsége kizárólag a terhére megállapított, személyükhöz fűződő jogsértésből következik, melynek megállapításához konkrét károkat, hátrányukat nem kellett igazolniuk. Ezzel szemben az ítélkezési gyakorlat következetes a tekintetben, hogy a személyhez fűződő jogok megsértésével összefüggő hátrányok bekövetkezését a kárigényt érvényesítő károsultaknak bizonyítaniuk kell (Pp. 164. §), a bíróságnak csak a köztudomású tényeket kell hivatalból figyelembe vennie".[551]

A döntés szerint: „A személyhez fűződő jog megsértése miatt igényelt kártérítésnek ugyanazok a feltételei, mint bármilyen egyéb jogellenes károkozásért követelt kártérítésnek. A személyhez fűződő jog megsértésének igazolása ugyanis önmagában csak a jogellenes magatartás megállapítására ad alapot. *A sérelmet szenvedő fél nem vagyoni kártérítést csak akkor igényelhet, ha bizonyítja olyan hátrány bekövetkezését, amely indokolja a nem vagyoni kárpótlás megállapítását.* A kérelmezők azonban nem is kívánták igazolni, hogy az adós jogsértése miatt milyen hátrányuk következett be. Eltérő jogi álláspontjuk miatt ugyanis szükségtelennek tartották bármilyen hátrány bekövetkezésének igazolását. Az adós nem vagyoni kártérítésre való kötelezését a Ptk. 84. §-a (1) bekezdésének *e)* pontja szerint mintegy büntetésként igényelték az adós igazolt jogsértése miatt. Ilyen okból és ilyen módon azonban az adós terhére nem vagyoni kártérítés megállapítására nem kerülhetett sor. Az Alkotmánybíróság 34/1992. (VI. 1.) AB határozata indokolásából ugyanis *nem vezethető le az*

[549] Kiemelés tőlem – *J. A.*

[550] Kiemelés tőlem – *J. A.*

a kérelmezők által levont következtetés, mely szerint a személyhez fűződő jog megsértése automatikusan beálló következménye a károkozó nem vagyoni kártérítési felelősségének megállapítása."[552] A Legfelsőbb Bíróság mindennek alapján a kérelmezők nem vagyoni kártérítés iránti kérelmét elutasította.

A Legfelsőbb Bíróság fenti eseti döntése nyomán kibontakozni látszó joggyakorlat tehát továbbra sem biztosítja a személyiségi jogvédelmet ott, ahol – az AB határozatára utalva – az élet „megnehezülése" hiányzik, kár nem következett be. Ennek alapján az Avtv. rendelkezéseinek megsértése – kivételes esetektől eltekintve – nem hordozza a jogsértő számára kártérítési felelősség megállapításának kockázatát. Álláspontunk szerint a Legfelsőbb Bíróság gyakorlata, amely a kártérítési felelősség megállapításának feltételeit – ismét az AB határozatra utalva – nyilvánvalóan „a kártérítési jog keretein belül" határozza meg, helyes. A nem vagyoni kártérítés valóban „inadekvát", alkalmatlan szankció az adatvédelmi jogi jogsértések esetén.

1.17.2. Az irányelv vonatkozó rendelkezései

Az irányelv nem követeli meg az adatkezelő felelősségének objektív felelősségként történő szabályozását.[553] A 22. cikk szerint (1) bekezdése szerint: „A tagállamoknak rendelkezniük kell arról, hogy mindenki, aki jogellenes adatfeldolgozási művelet vagy az ezen irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett károkért." A (2) bekezdés szerint: „Az adatkezelő részben vagy egészben mentesül e felelősség alól, ha bizonyítja, hogy a kárt okozó eseményért nem felelős."

---

[551] A Legfelsőbb Bíróság ezzel kapcsolatban hivatkozik a BH 1996.304. számon közzétett eseti döntésre.

[552] Kiemelések tőlem – *J. A.* A hátrány bekövetkezésének mint a nem vagyoni kártérítés igénylésének feltételével kapcsolatban lásd még a például a BH 1997/127, a BH 1997/435 és a BH 2001.12 számon közzétett jogeseteket.

[553] Az objektív és szubjektív, tárgyi és vétkességi felelősség megkülönböztetésével kapcsolatban lásd Gellért 2001, 1122. skk. Idézi Eörsi Gyulát: „Szubjektív, vétkességen alapuló felelősség elvileg is, gyakorlatilag is sok átmenettel közelít az objektív felelősséghez. A kettő egymásnak egyáltalán nem ellentéte, hanem az ún. objektív felelősség egy merev szabállyal kiemelt határesete a rugalmasan megfogalmazott és alkalmazott szubjektív felelősségnek." Az új Ptk. kodifikációja során felmerült, hogy annak kártérítési felelősségről szóló könyve a Marton Géza által kidolgozott, objektív felelősségre épülő felelősségi rendszerre alapuljon (Lábady 2002, 96–99.), ám a megoldást végül elvetették (Lábady 2004, 94.).

1.17.3. Várható változások, szabályozási javaslat

A 18. § tehát a jelen helyzetben – a nem vagyoni kártérítés által nyújtott személyiségvédelem fogyatékosságai miatt – az adatvédelmi jog alkalmatlan szankciórendszerének egyik eleme. Ez a helyzet várhatóan változik majd: az új Polgári Törvénykönyv koncepciója a nem vagyoni kártérítés intézményének megszüntetése mellett előirányozza intézményének bevezetését a magyar magánjogba. A sérelemdíj olyan esetben is megítélhető lenne, ha a sértetti oldalon a hátrány bekövetkezése nem bizonyítható, ám a sértettnek elégtétel nyújtása indokolt – a koncepció szerint a sérelemdíj ebben az esetben „magánjogi büntetés".[554]

A koncepció az Avtv. 18. §-ában szabályozott veszélyes üzemi felelősségi konstrukció felülvizsgálatát és az alkalmazott felelőssége körében történő szabályozását is előirányozza.[555] Álláspontunk szerint a 18. §-ban foglalt szabályozás – a „technikai adatvédelem" követelményeinek megszegésével okozott károk esetét kivéve – indokolt (ám célszerű azt a környezet veszélyeztetésével okozott kárra vonatkozó szabályozáshoz hasonlóan a Ptk.-ba illeszteni).

1.18. Az adatvédelmi biztos

1. Az Avtv. 23 § (1) bekezdése szerint „a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében az Országgyűlés adatvédelmi biztost választ azok közül az egyetemi végzettségű, büntetlen előéletű, kiemelkedő tudású elméleti vagy legalább 10 évi szakmai gyakorlattal rendelkező magyar állampolgárok közül, akik az adatvédelmet érintő eljárások lefolytatásában, felügyeletében vagy tudományos elméletében jelentős tapasztalatokkal rendelkeznek és köztiszteletnek örvendenek."

Az Avtv. megalkotását megelőző hosszas műhelymunka során a törvény rendelkezéseinek érvényesülése felett őrködő független ellenőrző szervezet létrehozásának igénye egyértelmű volt, ám kezdetben még nem dőlt el, hogy az „igazgatási jellegű országos főhatóság" vagy „ombudsmanszerű, az országgyűlésnek alárendelt szerv" legyen-e.[556] Később

[554] Koncepció 2004, 31. skk., valamint 186.

[555] Koncepció 2004, 195.

[556] Sólyom 1998a, 57.

az irodalomban teret nyert az a gondolat, hogy az ombudsmanmodell szerint létrehozott adatvédelmi biztos a megfelelő megoldás.[557] és ebben a szellemben született meg az Avtv. is.

2. Az (1) bekezdés az adatvédelmi biztosi méltóság betöltésének személyi feltételeit határozza meg. Az Alkotmány 32/B. § (4) bekezdése szerint: „Az állampolgári jogok, illetőleg a nemzeti és etnikai kisebbségi jogok országgyűlési biztosait a köztársasági elnök javaslatára az Országgyűlés a képviselők kétharmadának szavazatával választja. Az Országgyűlés egyes alkotmányos jogok védelmére külön biztost is választhat. A külön biztos a szakterületén önálló intézkedési joggal rendelkezik." A törvény az adatvédelmi biztossá választás feltételeit hasonlóan szabályozza az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvényhez (a továbbiakban: Obt.), ám nem követeli meg a biztostól a jogi egyetemi végzettséget.

1.18.1. Az adatvédelmi biztos és az állampolgári jogok országgyűlési biztosára vonatkozó szabályozás

1. A 23. § (2) bekezdése szerint „az adatvédelmi biztosra – e törvényben foglalt eltérésekkel – az állampolgári jogok országgyűlési biztosáról szóló törvény rendelkezéseit kell alkalmazni." A (2) bekezdés az adatvédelmi biztosra mint külön biztosra az Avtv.-ben foglalt eltérésekkel az Obt. szabályait rendeli alkalmazni; az Obt. 2. § (5) bekezdése szerint: „Ahol e törvény az országgyűlési biztost említi, azon – eltérő rendelkezés hiányában – […] a külön biztost is érteni kell."

2. Az Avtv. legfőbb eltérései az Obt. szabályozásától az alábbiak:

– Az adatvédelmi biztos az Avtv. 24. § *a)* pontja szerint „ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabály megtartását"; vizsgálati jogosultsága tehát az általános biztossal szemben nem csak hatóságokra illetőleg közszolgáltatást végző szervekre terjed ki, hanem bármely, az Avtv. hatálya alá tartozó adatkezelésre és adatkezelőre.

– Az Avtv. már a 2003. évi novella előtt is biztosított az adatvédelmi biztosnak kvázi hatósági jogkört [a titokminősítéssel kapcsolatban – lásd a 26. § (4) bekezdését], ám a novella által bevezetett szabályok szerint a biztos „elrendelhet" adatzárolást, -törlést vagy -megsemmisítést, megtilthatja a jogosulatlan adatkezelést vagy adatfeldolgozást stb. [Avtv. 25. § (2) bekezdése]. Az általános biztos és helyettese nem rendelkezik ilyen hatáskörökkel, a hagyományos ombusmannmodellnek megfelelően vizsgálatokat, eljárásokat

[557] Lásd például Majtényi 1990.

kezdeményezhetnek, ajánlásokat tehetnek a felügyeleti szervnek stb. A 2003. évi novella álláspontunk szerint oly mértékben módosította az adatvédelmi biztos hatásköreit, hogy az már nem illeszkedik az ombudsmanmodell keretei közé – létrejöttek az adatvédelmi hatósági működés feltételei, ám a kellő eljárási garanciák nélkül.

Az Obt. tehát elsősorban az adatvédelmi biztos jogállásával (választásával, megbízatásának megszűnésével, mentességgel, összeférhetetlenséggel stb.) kapcsolatban hatályosul az Avtv. háttérjogszabályaként – az adatvédelmi biztos eljárására vonatkozóan, különösen a 2003. évi novellát követő helyzetben szabályai kisebb szerephez jutnak. A 2005. évi módosítás által megállapított 24/A § (2) bekezdése szerint „Az adatvédelmi biztos eljárására az Obtv. 16. § (1) és (2) bekezdését, 17. § (3) és (4) bekezdését, 18. § (1), (6) és (8) bekezdését nem kell alkalmazni" (lásd részletesen alább).

3. Az első adatvédelmi biztos mandátumának lejárta után a tisztség több hónapon át betöltetlen volt; az országgyűlés azonban megválasztotta az állampolgári jogok országgyűlési biztosát és annak helyettesét; vita alakult ki abban a kérdésben, hogy az *új adatvédelmi biztos megválasztásáig helyettesítheti-e ez állampolgári jogok országgyűlési biztosa és annak helyettese az adatvédelmi biztost*. Az egyik álláspont szerint ez az Obt. 2. § (4) bekezdése alapján – „Ha külön biztos akadályoztatva van, jogkörét az országgyűlési biztos, illetőleg az országgyűlési biztos általános helyettese gyakorolja." – az állampolgári jogok országgyűlési biztosa teljes jogkörrel helyettesíthette volna az általános biztost; ezzel szemben állt az a nézet, amely szerint a meg nem választott adatvédelmi biztos nincs „akadályoztatva", helyettesítése nem lehetséges. Ez utóbbi értelmezés szerint az általános biztos és helyettese csak saját hatáskörében, az Obt. alapján eljárva vizsgálhat adatvédelmi és információszabadsággal kapcsolatos ügyeket. Az általános biztos és helyettese végül mégis „helyettesítették" az adatvédelmi biztost, ám oly módon, hogy nem gyakorolták annak kvázi hatósági hatásköreit. Álláspontunk szerint ilyen esetben az általános biztos és helyettese az Obt. alapján vizsgálhat a személyes adatok védelméhez, illetőleg a közérdekű adatok megismeréséhez és terjesztéséhez fűződő jogokkal kapcsolatos alkotmányos visszásságot; vizsgálatai csak az Obt. 16. § (1) bekezdésében meghatározottakra (hatóságok, közszolgáltatást végző szervek) terjedhet ki, más adatkezelőket nem vizsgálhat.

4. A 2005. évi törvénymódosítással beiktatott 24/A § szerint az adatvédelmi biztos eljárására és intézkedéseire az Obt. alábbi rendelkezéseit nem kell alkalmazni:

1. Az Obt. 16. § (1) bekezdése szerint „Az országgyűlési biztoshoz bárki fordulhat, ha megítélése szerint valamely hatóság […] illetve közszolgáltatást végző szerv (a továbbiakban

együtt: hatóság) eljárása, ennek során hozott határozata (intézkedése), illetőleg a hatóság intézkedésének elmulasztása következtében alkotmányos jogaival összefüggésben sérelem érte, vagy ennek közvetlen veszélye áll fenn, feltéve, hogy a rendelkezésre álló közigazgatási jogorvoslati lehetőségeket - ide nem értve a közigazgatási határozat bírósági felülvizsgálatát - már kimerítette, illetve jogorvoslati lehetőség nincs számára biztosítva." Az adatvédelmi biztos bármely adatkezelésre vonatkozó jogszabály megtartását vizsgálhatja, nem csak hatóság vagy közszolgáltatást végző szerv adatkezelését; a közigazgatási jogorvoslat lehetősége, és az, hogy az érintett azt kimerítette-e, az adatvédelmi biztos eljárása szempontjából irreleváns. Az Obt. 16. § (2) bekezdése szerint „Az országgyűlési biztos az alkotmányos jogokkal kapcsolatos visszásság megszüntetése érdekében az (1) bekezdésben megjelölt feltételek fennállása esetén hivatalból is eljárhat." – a jogalkotó e rendelkezés kivételként való rögzítésével nem az adatvédelmi biztos hivatalból történő eljárását kívánta kizárni (lásd az Avtv. 24. § a) pontját), hanem azt, hogy a hivatalból történő vizsgálat köre az alkotmányos visszásság megszüntetése végett indított eljárásokra szoruljon. (Az „alkotmányos visszásság" az állampolgári jogok országgyűlési biztosa gyakorlatában központi jelentőségű, ám az adatvédelmi biztosi „esetjogban" nem kapott szerepet.)

2. Az Obt. 17. § (2) bekezdése szerint „Ha az országgyűlési biztos megítélése szerint a beadványban szereplő visszásság csekély jelentőségű, az országgyűlési biztos a beadványt nem köteles vizsgálni. Erről a beadványt tevőt értesíti." Az adatvédelmi biztos az Avtv. 24. § b) pontja alapján köteles azon beadványok vizsgálatára, amelyek vonatkozásában hatásköre megállapítható, nem tekinthet el a bagatell ügyek vizsgálatától sem.[558] Az Obt. 17. § (3) bekezdése az országgyűlési biztos vizsgálati lehetőségét az 1989. évi XXXI. törvény (az 1989. október 23-i alkotmánymódosítás) hatálybalépését követően indult eljárásokra szorítja – kivéve az adatvédelmi biztos esetében.

3. Az Obt. 18. § (1) bekezdése szerint „Az országgyűlési biztos a jogerősen befejezett ügyekre vonatkozóan jogosult bármely hatóság ellenőrzésére, ennek során - külön törvény eltérő rendelkezése hiányában - a hatóság helyiségeibe beléphet. Az országgyűlési biztos jogainak gyakorlása érdekében a fegyveres erők, a nemzetbiztonsági szolgálatok, a rendőrség és a rendészeti szervek működésére szolgáló területekre a hatáskörrel rendelkező miniszter által szabályozott módon léphet be. Ez a szabályozás az ellenőrzést érdemben nem akadályozhatja." Az Obt. 18. § (6) bekezdése szerint „Az országgyűlési biztos az

[558] Az Obt. 17. § (2) bekezdését az általános biztos is igen ritkán alkalmazza. „A biztos ugyanis – mindegyik biztos – *de minimis curat*." Sólyom 2001b, 88

iratbetekintési jogát a fegyveres erőknél, a nemzetbiztonsági szolgálatoknál, a rendőrségnél, az Adó- és Pénzügyi Ellenőrző Hivatal nyomozó hatóságánál, a Vám- és Pénzügyőrségnél, valamint az ügyészség nyomozást végző szervénél az e törvényben foglalt korlátozások szerint gyakorolhatja". A (7) bekezdés úgy rendelkezik, hogy „A nemzetbiztonsági szolgálatok, a rendőrség, a határőrség, az Adó- és Pénzügyi Ellenőrző Hivatal nyomozó hatósága, a Vám- és Pénzügyőrség, valamint az ügyészség nyomozást végző szerve titkos információgyűjtő tevékenységével is kapcsolatos kérdésre vagy bejelentésre az országgyűlési biztos a válaszát úgy fogalmazza meg, hogy abból a felsorolt szervek egyes esetekhez kapcsolódó titkos információgyűjtő tevékenységére ne lehessen következtetéseket levonni."
Az adatvédelmi biztos szélesebb körű jogosítványait az Avtv. 26. § (1)-(2) és (4) bekezdései rögzítik.

1.18.2. Az adatvédelmi biztos feladatkörei

Az Avtv. szerint (24. §) az adatvédelmi biztos

a) bejelentés alapján vagy – ha az adott ügyben bírósági eljárás nincs folyamatban – hivatalból ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok megtartását;

b) kivizsgálja a hozzá érkezett bejelentéseket;

c) gondoskodik az adatvédelmi nyilvántartás vezetéséről;

d) elősegíti a személyes adatok kezelésére és a közérdekű adatok nyilvánosságára vonatkozó törvényi rendelkezések egységes alkalmazását;

e) feladatkörében általános jelleggel, valamint meghatározott adatkezelő részére ajánlást bocsáthat ki;

f) véleményezési jogot gyakorol az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv tevékenységével kapcsolatosan külön törvényben meghatározottak szerint közzéteendő adatokra vonatkozó különös, illetőleg egyedi közzétételi listák tekintetében;

g) külön törvényben meghatározott szervekkel vagy személyekkel együttműködve képviseli a Magyar Köztársaságot az Európai Unió közös adatvédelmi felügyelő testületeiben;

h) gyakorolja és ellátja az e törvényben meghatározott hatásköröket és feladatokat.

1. Az adatvédelmi biztos „ellenőrzi" az Avtv. és más, „adatkezelésre" vonatkozó jogszabály megtartását. Az adatkezelés fogalma az Avtv.-ben a 2005. évi módosítás nyomán már nem csak személyes adatok vonatkozásában értelmezett (2. § 9. pontja), az adatvédelmi biztos a személyes adatok, közérdekű adatok, közérdekből nyilvános adatok, valamint

titokfelügyeleti jogkörében a minősített adatok kezelésével kapcsolatos jogszabályok megtartását ellenőrzi. A 2005. évi módosítás rögzítette a hivatalból és a kérelem alapján történő eljárás lehetőségét, bár az adatvédelmi biztos korábban is indított vizsgálatokat hivatalból (lásd alább).

2. Az adatvédelmi biztos kivizsgálja a hozzá érkező bejelentéseket. A 27. § (1) bekezdése szabályozza azt, hogy ki fordulhat az adatvédelmi biztoshoz – lásd erről részletesen alább.

3. A biztos gondoskodik az adatvédelmi nyilvántartás vezetéséről (lásd alább).

4. A 2003. évi novella fogalmazta meg azon kötelezettségét, amely szerint „elősegíti a személyes adatok kezelésére és a közérdekű adatok nyilvánosságára vonatkozó törvényi rendelkezések egységes alkalmazását". A novella miniszteri indokolása ezzel kapcsolatban megállapítja, hogy ennek „már kialakult a gyakorlata" – az adatvédelmi biztos az egységes jogalkalmazást saját jogértelmezéseinek (állásfoglalásainak, ajánlásainak) beszámolókba való összefoglalásával, nyilvánosságra hozatalával, valamint az ún. konzultációs ügyek „befogadásával" tesz eleget (lásd alább).

5. A 2005. évi módosítás egészítette ki a felsorolást az ajánlások kibocsátásra vonatkozó ponttal. Ajánlást a biztos „általános jelleggel" is kiadhat: a jogalkotó ezzel törvénybe iktatta azt az adatvédelmi biztos által korábban követett gyakorlatot, amelyre jellemző, hogy „ajánlásai igen gyakran tartalmaznak olyan megállapításokat is, amelyek a vizsgált ügy(ek) tanulságait általánosítva, szabályként fogalmazzák meg".[559]

6. Az f) pont a közérdekű adatok elektronikus közzétételére vonatkozó, előkészítés alatt álló szabályozásra tekintettel fogalmazza meg a biztos véleményezési jogkörét az abban szereplő különös és egyedi közzétételi listák tekintetében.

7. Az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. 11. § (3) bekezdése szerint a Közös Nemzetközi Adatvédelmi Ellenőrző Testületben Magyarországot az adatvédelmi biztos képviseli.

7. Az Avtv. 25. § (1) bekezdése szerint „az adatvédelmi biztos figyelemmel kíséri a személyes adatok védelmének és a közérdekű adatok és a közérdekből nyilvános adatok nyilvánossága érvényesülésének feltételeit. Javaslatot tesz az adatkezelést, a közérdekű adatok és a közérdekből nyilvános adatok nyilvánosságát érintő jogszabályok megalkotására, illetve módosítására, véleményezi az ilyen jogszabályok tervezetét. Kezdeményezheti az

[559] Sólyom 2001b, 89

államtitokkörben, valamint a szolgálati titokkörben meghatározott adatfajták szűkítését vagy bővítését."

A 25. § (1) bekezdése általános kötelezettséget fogalmaz meg a biztos számára: folyamatosan *figyelemmel kell kísérnie az adatvédelem és információszabadság érvényesülésének feltételeit;* e feltételek alakítása érdekében pedig élhet mind a 25. § (1) bekezdésében felsorolt jogszabályalkotás vagy -módosítás kezdeményezésével kapcsolatos jogkörével, mind az államtitok- és szolgálati titok körében meghatározott adatfajtákkal kapcsolatos jogkörével („titokfelügyelet"). A 25. § (1) bekezdése azonban általában felhatalmazást ad a biztosnak arra, hogy eseti vagy meghatározott típusú adatkezelésekkel kapcsolatos tematikus vizsgálatokat folytasson; a két jog „érvényesülésének feltételei" ráadásul magukban foglalják a technológiai fejlődést is, vagyis a biztos e rendelkezés alapján például a magánszféravédő technológiákkal kapcsolatban alkalmazásának terjesztésében is kezdeményező szerepet vállalhat.

8. A *magánszféra védelmében* emelte fel a szavát a biztos abban az esetben, amikor a televízió-előfizetési díj behajtásának módját kifogásolta: a szabályozás bizonyos feltételek mellett módot adott az adóhatóság hatáskörében eljáró személyeknek, hogy a televíziókészülék birtoklásának ellenőrzése céljából magánlakásba belépjen.[560] Ajánlásban fogalmazza meg a biztos azokat a feltételeket is, amelyek betartásával elkerülhető, hogy valamely nem személyes adatkezelésnek minősülő (hanem statisztikai adatokra vonatkozó) adatkezelés semmiképpen ne válhasson az érintettek azonosításával jogszerűtlen személyes adatkezeléssé.[561] Itt említhető a biztos jogszabály-véleményezéssel kapcsolatos tevékenysége is, amely minden esetben „a személyes adatok védelmének és a közérdekű adatok nyilvánossága érvényesülésének feltételeivel", e feltételek alakulásával kapcsolatos értékelést is hordoz. Az ilyen értékelés során a biztos megfogalmazza álláspontját választott szabályozási megoldásnak, valamint a szabályozás tartalmának célszerűsége, az Avtv.-vel való összeegyeztethetősége mellett annak alkotmányosságáról is, álláspontját gyakran az AB vonatkozó döntéseire alapozva. (Lásd például az ún. „adórendőrség" adatkezelésének szabályozásáról a jogszabály-előkészítővel folytatott vitát.[562])

9. A *közérdekű adatok nyilvánosságának körében* a biztos vizsgálta azt a beadványt, amelyet azzal kapcsolatban nyújtottak be hozzá, hogy „nem sérül-e jóvátehetetlenül a közérdekű adatok nyilvánosságához, megismeréséhez való jog azáltal, hogy a kormány

[560] ABI 1998, 165 és ABI 1999, 55.

[561] ABI 1998, 271.

hatályos ügyrendje alapján a kormányülésekről sem magnetofonfelvétel, sem szó szerinti jegyzőkönyv nem készül".[563] Ez a vizsgálat nem lehet a 24. § *a)* szerinti, az Avtv. vagy más adatkezelésről szóló jogszabály megtartásának „ellenőrzése", hiszen az adott esetben a közérdekű adat nem áll rendelkezésre (hiszen azt nem is rögzítik), ám mindenképpen illeszkedik a biztosnak a 25. § (1) bekezdése által biztosított feladatkörébe. A biztos ajánlásában végül úgy foglalt állást, hogy „nem tekinthető alkotmányos követelménynek" a teljes körű dokumentáció készítése a kormányülésekről.[564]

10. A fenti ügyekben a biztos a 25. § (1) bekezdésében rögzített feladatkörében járt el. Létezik ezen túl egy olyan ügycsoport is, amelyben a biztos adatvédelmi jogsértésekhez vezető tényállásokat *más jogszabályok alapján* is vizsgált,[565] illetőleg – álláspontunk szerint helytelenül – megindultak vizsgálatok olyan ügyekben, amelyeknek tárgya *nem személyes adatok kezelése* volt (hanem például az elhunyt adatain keresztül a kegyeleti jogok esetleges sérelme,[566] nem személyes adatnak minősülő, de érzékeny [büntetett előéletre vonatkozó] adatok kezelése,[567] üzleti titkok kezelése).[568]

11. Az Avtv. 27. § (1) bekezdése szerint: „Bárki az adatvédelmi biztoshoz fordulhat, ha véleménye szerint személyes adatainak kezelésével vagy a közérdekű adatok megismeréséhez fűződő jogainak gyakorlásával kapcsolatban jogsérelem érte, vagy annak közvetlen veszélye fennáll, kivéve ha az adott ügyben bírósági eljárás van folyamatban", a 24. § *d)* pontja pedig az adatvédelmi biztosi feladatkörének elemeként határozza meg azt, hogy a biztos kivizsgálja a hozzá érkező bejelentéseket. Az Avtv. 27. § (1) bekezdése Obt. 16. § (1) bekezdésével állítható párhuzamba. Az Obt. 16. § (2) bekezdése azonban külön rögzíti a

---

[562] ABI 1999, 169. skk.

[563] ABI 2000, 293.

[564] ABI 2000, 300.

[565] Az MTI vezérigazgatójának utasításának vizsgálata során, amelyben megtiltja a távirati iroda alkalmazásában álló újságírónak publikációi saját néven való közlését, a biztos az utasítás jogszerűtlenségét kimondó állásfoglalást elsősorban arra alapozta, hogy „a Magyar Köztársaságban mindenkinek joga van a szabad véleménynyilvánításra", másodsorban arra, hogy a szerzői jogi törvény szerint „a szerzőnek joga van arra, hogy nevét művén feltüntessék", és csak harmadsorban arra, hogy az Avtv. biztosítja a jogot arra, hogy személyes adatával mindenki maga rendelkezzék. ABI 1997, 70. (Álláspontunk szerint az állásfoglalás téves.)

[566] ABI 1997, 85.

[567] ABI 1998, 158: Álláspontunk szerint ebben az ügyben azt kellett volna vizsgálni, hogy személyes adatokról van-e szó: ha igen, akkor az adatkezelés jogszerűtlen; ha nem, további követelmények megfogalmazására nincs szükség.

[568] ABI 1999, 330.

hivatalból való eljárás lehetőségét, az Avtv. 27. §-a nem szól erről a kérdésről – ennek alapján akár olyan értelmezés is lehetséges, hogy a jogalkotó szándéka szerint az adatvédelmi biztos nem járhat el hivatalból. Álláspontunk szerint azonban nem ez a helyzet: az Avtv. 24. § *a)* pontjából és 25. § (1) bekezdéséből az következik, hogy a biztos nem csak bejelentésre megindított eljárásban végezhet „ellenőrzést" [24. § *a)* pontja], sőt, kifejezetten kötelezettsége, hogy figyelemmel kísérje az adatvédelem és az információszabadság érvényesülésének feltételeit, és aktív módon igyekezzen azokat alakítani.

Az adatvédelmi biztos – legalábbis működésének korai éveiben – általában elutasította az öncélú hivatali vizsgálatokat, a „népboldogító, rossz értelemben megnyilvánuló aktivizmust";[569] az ombudsmani szerepfelfogásból következően inkább a „követő", a polgárok igényéhez szabott jogvédelem biztosítását tartotta elsődleges feladatának. Azokat a kivételes eseteket, amelyekben hivatalból történő vizsgálat indítása álláspontja szerint indokolt lehet, a következőképpen fogalmazta meg: „akkor, ha az alkotmányos jogában megsértett erre [vizsgálat kezdeményezésére] képtelen […], vagy ha mintegy az egyéni panaszok összegzéseként kell nagy rendszereket egységes szempontok alapján megvizsgálni […], továbbá, ha a polgárok nagy számát érintő adatkezelés kapcsán jogsértés gyanúja merül fel".[570] Később felmerült, hogy a biztos kezdeményezőbb szerepet vállalhatna a jogszabály-előkészítés befolyásolására, valamint – az információszabadság-ügyek alacsony számára tekintettel – a közérdekű adatok nyilvánosságával kapcsolatos ügyek területén.[571] A biztos hivatalból indított eljárást például az ún. Központi adategyeztető és továbbító országos rendszerrel kapcsolatos tervek vizsgálatára;[572] a diákigazolványok előállításának körülményeinek vizsgálatára;[573] a televíziótársaságok híradói, bűnügyi tudósításai adatvédelmi szempontú vizsgálata céljából;[574] némelykor azonban, súlyos jogsértés gyanúja esetén a fent meghatározott körön kívüli egyedi ügyek vizsgálatára is sor került hivatalból.[575] A legutóbbi időkben hivatalból vizsgált a biztos egyes, az elektronikus közigazgatással kapcsolatos projekteket, így az állami adatvagyon biztonságos tárolását és az

[569] ABI 1997, 24.

[570] ABI 1997, 24; hasonló állásfoglalásra lásd még ABI 1998, 139; ABI 2000, 21.

[571] ABI 1999, 15.

[572] ABI 1998, 87.

[573] ABI 1997, 24.

[574] ABI 2000, 196.

állampolgároknak a közigazgatási szolgáltatások igénybevétele során történő azonosítását célzó, számos adatvédelmi kérdést felvető eTár/eSzignó-tervet.[576]

A hivatalból indított vizsgálatok körébe tartoztak az ún. *megyei vizsgálatok,* amelyek keretében az adatvédelmi biztos egy megyébe ellátogatva vizsgált két-három napon át különböző területeken működő adatkezelőket, majd vizsgálata eredményeiről tájékoztatta a helyi és az országos sajtót.

12. Az adatkezelésre vonatkozó jogszabályok értelmezési gyakorlatának egységesítéséhez járulhatnak hozzá az ún. *konzultációs vizsgálatok* is. Ilyen esetben nem az Avtv. 27. § (1) bekezdésében meghatározott érintett fordul az adatvédelmi biztoshoz, és nem is előzetes ellenőrzés lefolytatásáról van szó. E körbe tartoznak azok a vizsgálatok, amelyekben adatkezelők – elsősorban nagyszámú adatalanyt érintő adatkezelésekkel kapcsolatban – kérik a biztos iránymutatását, jogértelmezését. Az immár az Avtv. 24. § *d)* pontja által előírt feladatkörbe illeszkedő tevékenységet az adatvédelmi biztos működésének kezdeteitől végezte. A biztos az általa kialakított gyakorlat szerint általában akkor biztosított konzultációs lehetőséget állami szektorbeli adatkezelők számára, ha akár az adatkezelés, akár a még nem megvalósult adatkezelésre vonatkozó terv, koncepció nagyszámú adatalanyt érint, „stratégiai jellegű" volt, magánszférabeli adatkezelők számára pedig szintén az érintett adatalanyok száma, illetőleg az volt a döntő, hogy „közüzemi, általános ellátási tevékenységen alapuló" szolgáltatásról van-e szó; kizárta azonban a biztos „olyan tanácsok nyújtását, amelyek közvetlenül üzleti hasznot eredményeznek", mivel ez „sem hivatalunk közpénzből való fenntartásával, sem eljárásunk illetékmentességével, sem a versenyszféra tisztességes működésével nem lenne összeegyeztethető".[577]

További lényeges korlátja a konzultációs vizsgálatoknak, hogy az adatvédelmi biztos konzultációs vizsgálata nyomán kialakított előzetes véleménye nem jelenti a szóban forgó adatkezelés „jóváhagyását", legitimálását: későbbi vizsgálat ilyen esetben is megállapíthatja az adatkezelés jogellenességét.[578]

A konzultációs ügyekben történő vizsgálat az előzetes ellenőrzési intézmény előképének tekinthető; az ilyen ügyek jelentős részének tárgya a hatályos törvény 31. § (3)

---

[575] Például hivatalból került sor (sajtótudósításokat követően) a Magyarországi Szcientológiai Egyház egy adatkezelésének vizsgálatára (ABI 1999, 119) vagy a www.halapenz.hu weboldalon végzett adatkezelés vizsgálatára (http://abiweb.obh.hu/abi/aktualis/2_h_2004-5.htm).

[576] ABI 2004, 43.

[577] ABI 1998, 155; lásd még ABI 1999, 109; ABI 1999, 158.

[578] ABI 1998, 156.

bekezdése alapján bejelentésre kötelezett adatkezelés volt (például a gyanúsítotti nyilvántartás).[579]

13. A biztos vizsgálatai során igen sok esetben jelzi a jogszabály-előkészítőnek illetőleg a jogalkotónak a szabályozás hiányát illetőleg hibáit. *A jogszabálytervezetekre vonatkozó véleményezési jogkörét* az adatvédelmi biztos úgy értelmezi, hogy az a közigazgatási egyeztetést követően megfogalmazott, az addig beérkezett észrevételeket tartalmazó „kiérlelt" tervezetekkel kapcsolatban gyakorolható érdemben: „a jogszabályok véleményezésével kapcsolatos jogát az adatvédelmi biztos nem a tárcaszintű vagy a minisztériumi belső koordináció folyamatában, egy még formálódó tervezettel kapcsolatban, hanem a döntésre jogosult szervezet, vagy személy (országgyűlés, kormány, miniszter) elé kerülő – a koordináció során végleges formát öltött – változattal kapcsolatban kívánja érvényesíteni".[580]

14. A 25. § (1) bekezdése szerint az adatvédelmi biztos „[k]ezdeményezheti *az államtitokkörben, valamint a szolgálati titokkörben meghatározott adatfajták szűkítését vagy bővítését*". Ezt a jogkört meg kell különböztetni az Avtv. 26. § (4) bekezdésében meghatározott esettől, amelyben a biztos meghatározott adat minősítésének indokolatlansága esetén szólítja fel a minősítőt a minősítés megszüntetésére (lásd ott).

Az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény (a továbbiakban: Ttv.) szerint: „Államtitok az az adat, amely [a] törvény 1. számú mellékletében (a továbbiakban: államtitokkör) meghatározott adatfajta körébe tartozik, és a minősítési eljárás alapján a minősítő megállapította, hogy az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése vagy felhasználása, illetéktelen személy tudomására hozása, továbbá az arra jogosult részére hozzáférhetetlenné tétele közvetlenül sérti vagy veszélyezteti a Magyar Köztársaság törvényben meghatározott honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi, külügyi vagy nemzetközi kapcsolataival összefüggő, valamint igazságszolgáltatási érdekeit." Államtitokká tehát egy adat Ttv. által taxatív felsorolással meghatározott *minősítők* által, a Ttv. és a vonatkozó kormányrendelet[581] által *előírt módon* minősíthető abban az esetben, ha az *szerepel a Ttv.-nek az államtitokká minősíthető adatfajtákat meghatározó mellékletében*, valamint eleget tesz a *fent idézett törvényi rendelkezésben meghatározott feltételnek.* A minősítő a minősítés során állapítja meg az államtitok érvényességi idejét is, amelynek lehetséges maximális időtartalmát a Ttv.

[579] ABI 1999, 162.

[580] ABI 1997, 305.

mellékletébe foglalt államtitokköri jegyzék határozza meg. Megjegyzendő, hogy a Ttv. szabályozásától függetlenül ex lege államtitoknak minősülnek egyes adatok más-más jogszabályok szerint.[582]

A Ttv. szerint: „Szolgálati titok az e törvény […] szerint minősítésre felhatalmazott által meghatározott adatfajták körébe (a továbbiakban: szolgálati titokkör) tartozó adat, amelynek az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése és felhasználása, illetéktelen személy részére hozzáférhetővé tétele, továbbá az arra jogosult részére hozzáférhetetlenné tétele sérti vagy veszélyezteti az állami vagy közfeladatot ellátó szerv működésének rendjét, akadályozza a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását, és ezáltal közvetve a Magyar Köztársaság törvényben meghatározott érdekeit hátrányosan érinti." Ebben az esetben tehát nem a Ttv., hanem a minősítő határozza meg a szolgálati titokkört, amely keretet szab a minősítésnek. A Ttv. szerint nem lehet szolgálati titokká minősíteni az Avtv. 19. § (2) bekezdésében meghatározott adatfajták körébe tartozó adatot. A szolgálati titokkör megállapítása során a Ttv. szerint ki kell kérni az adatvédelmi biztos véleményét; a szolgálati titokkört a *Magyar Közlöny*ben kell közzétenni. A szolgálati titokkört rendeletben, közleményben (például a Magyar Köztársaság ügyészsége, Pénzügyi Szervezetek Állami Felügyelete) vagy utasításban (például az Országos Rendőr-főkapitányság) teszik közzé.

Az adatvédelmi biztos a „az államtitokkörben, valamint a szolgálati titokkörben meghatározott adatfajták szűkítését vagy bővítését" kezdeményezheti. Mivel az államtitokköri jegyzéket a Ttv. rögzíti, az ilyen kezdeményezés minden esetben jogszabály módosítására irányuló javaslat; a biztos természetesen véleményezi a Ttv.-ben foglalt államtitokkör módosítására irányuló törvényjavaslatokat is.[583] A biztos az ex lege államtitoknak minősülő adatok szabályozásának módosítására is tehet javaslatot (bár itt nem „államtitokkörről", hanem meghatározott adatokról van szó), a 25. § (1) bekezdésének második mondatában szabályozott feladatkörében. A szolgálati titokkört az adatvédelmi biztos annak kiadása előtt a Ttv. fent hivatkozott rendelkezése alapján előzetesen véleményezi,[584] de a 25. § (1) bekezdése alapján egyébként is kezdeményezheti annak módosítását.

---

[581] 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről.

[582] Lásd a rendőrségről szóló 1994. évi XXXIV. törvény 63. § (2) bekezdését, a nemzetbiztonságról szóló 1995. évi CXXV. törvény 30. § (4) bekezdését, 42. § (1) bekezdését stb. Az ezzel kapcsolatban felmerülő értelmezési problémákról lásd Dudás 1999, 9.

[583] Például ABI 2000, 156.

[584] Lásd ABI 1999, 141 stb.

9. A 2005. évi XIX. törvény által bevezetett módosítás nyomán a biztos a 25. § (1) bekezdésében meghatározott jogköröket a közérdekből nyilvános adatok vonatkozásában is gyakorolhatja – olyan adatok tekintetében tehát, amelyek nem mindegyike személyes adat, és amelyek soha nem közérdekű adatok. Az adatvédelmi biztos ezáltal még a korábbinál is inkább „információs biztos" – az adatkezelési normák („az információszabályozás") korábbinál is szélesebb körének érvényesülése felett őrködik.

15. Az Avtv. 25. § (2) bekezdése úgy rendelkezik, hogy „az adatvédelmi biztos a jogellenes adatkezelés észlelése esetén az adatkezelőt az adatkezelés megszüntetésére szólítja fel. Az adatkezelő haladéktalanul köteles megtenni a szükséges intézkedéseket, és erről 30 napon belül írásban tájékoztatni az adatvédelmi biztost."

A (2) bekezdésben szabályozott felhívás formáját az Avtv. nem határozza meg; az Obt. szabályozása szerint az országgyűlési biztos vizsgálatának lezárását követően ajánlást tesz [20. § (1) bekezdése]. A kialakult gyakorlat szerint az ügyek vizsgálatát a biztos a panaszosnak és a vizsgált szervnek küldött válaszlevéllel („állásfoglalás") zárja; egyes esetekben – nagyobb jelentőségű ügyek, illetőleg fontos, elvi jelentőségű állásfoglalásokat a biztos „ajánlásként" ad ki. „Az „ajánlás" és a „válaszlevél" csak formájában, de nem jogi jellegében különbözik.[585]

16. A 25. § (3) bekezdése szerint „az adatvédelmi biztos tájékoztathatja a nyilvánosságot eljárásának megindításáról, a jogellenes adatkezelés (adatfeldolgozás) tényéről, az adatkezelő (adatfeldolgozó) személyéről és a kezelt adatok köréről, valamint az általa kezdeményezett intézkedésekről, meghozott határozatokról." A nyilvánosság tájékoztatásával kapcsolatos jogkört – igaz, a biztos számára mérlegelést nem adva, kötelezettségként – az Avtv. a 2003. évi novella illetőleg a 2005. évi XIX. törvény hatálybalépését megelőzően is tartalmazta.

A nyilvánosság tájékoztatásával mint szankcióval kapcsolatos az az értelmezési kérdés, hogy a biztos csak a (2) bekezdésben foglalt határidő lejárta után fordulhat a nyilvánossághoz, vagy már előbb is, illetőleg ajánlásai, állásfoglalásai mely feltételekkel férhetők hozzá a nyilvánosság számára. Egyes álláspontok szerint az adatvédelmi biztos a (3) bekezdés alapján csak abban az esetben fordulhat a nyilvánossághoz, ha az adatkezelő nem tett eleget a (2) bekezdésben szabályozott „felszólításának".[586] Ugyanakkor az adatvédelmi biztos szerint az ajánlások/állásfoglalások nyilvánosságát az Avtv. közérdekű adatokra

[585] ABI 1998, 38.

[586] Ilyen kritikára lásd például ABI 1999, 198; ABI 2000, 179.

vonatkozó szabályozása szerint kell megítélni: ha az ajánlás tartalma közérdekű adat, akkor a biztos köteles arról a közvéleményt tájékoztatni abban az esetben is, ha az ajánlást annak címzettje elfogadta; ha az ajánlás szövege „nem közérdekű adat", akkor a nyilvánosságra hozatal abban az esetben történik meg, ha a (2) bekezdésben rögzített 30 napos határidő lejárt.[587] Ezen álláspont szerint az adatvédelmi biztosnak joga van ahhoz, hogy „bizonyos, közérdeklődésre mindenképp számot tartó esetekben akár már a vizsgálat befejeztével, az érintett szervezet vezetőjének válaszát meg sem várva tájékoztassa a nyilvánosságot megállapításairól, javaslatairól".[588]

17. Álláspontunk szerint a nyilvánosságra hozatalt a (3) bekezdés korábbi szövegezése mint a jogellenes adatkezelés folytatásának lehetséges szankcióját szabályozta, ezért az adatvédelmi biztosnak a (2) bekezdésben meghatározott határidő előtt, illetőleg a felszólításra megszüntetett adatkezelés vonatkozásában nem volt szabad a (3) bekezdésben szabályozott módon a nyilvánosságot „tájékoztatnia" (vagyis sajtón keresztül vagy más úton kifejezetten az adott ügy körülményeit ismertetnie). Az adatvédelmi biztosi ajánlások, állásfoglalások azonban – a személyes adattartalomtól eltekintve – közérdekű adatnak minősülnek, így azokat az Avtv. 19–21. §-ában szabályozott keretek között kérelemre hozzáférhetővé kell tenni. Megjegyzendő, hogy a 19. § (6) bekezdése szerint az üzleti titok megismerésére a közérdekű adatok vonatkozásában is a Ptk. rendelkezései az irányadók; ilyen adatokat vizsgálatai során az adatvédelmi biztos is megismerhet. Ez azonban álláspontunk szerint nem zárta ki azt, hogy a biztos közérdeklődésre számot tartó ügyben a média munkatársainak *megkeresésére* nyilatkozzon álláspontjáról.

18. A 2005. évi XIX. törvény által módosított rendelkezés a biztos számára lehetőséget ad arra, hogy az eljárás megindításától kezdve folyamatosan tájékoztassa a nyilvánosságot annak fejleményeiről. A jogalkotó immár nem szankcióként szabályozza a nyilvánosságra hozatalt, vagyis az új rendelkezés egyáltalán nem ad teret a hivatkozott megszorító értelmezéseknek.

19. A 25. § (4) bekezdése szerint „ha az adatkezelő vagy adatfeldolgozó a személyes adatok jogellenes kezelését (feldolgozását) nem szünteti meg, az adatvédelmi biztos határozatban elrendelheti a jogosulatlanul kezelt adatok zárolását, törlését vagy megsemmisítését, megtilthatja a jogosulatlan adatkezelést vagy adatfeldolgozást, továbbá

[587] ABI 1998, 19–20.

[588] ABI 1999, 201.

felfüggesztheti az adatok külföldre továbbítását. A határozat ellen közigazgatási úton jogorvoslatnak nincs helye."

A 2003-ban novellált és 2005-ben is módosított szabályozás szerint az adatvédelmi biztos abban az esetben, ha az adatkezelő vagy adatfeldolgozó a jogellenes adatkezelést/adatfeldolgozást nem szünteti meg, „elrendelhet", „megtilthat" és „felfüggeszthet" különböző adatkezelési/adatfeldolgozási műveleteket. Az adatvédelmi biztos e sajátos kvázi hatósági jogkörei eltávolítják a szabályozást az ombudsmannmodelltől; az ombudsmannak – kivételes és soha nem jelentős esetektől eltekintve[589] – hatósági jogköre nincs.[590]

Az adatvédelmi biztos hatósági jogköreivel kapcsolatban számos, elsősorban eljárási kérdés merül fel. Az Avtv. nem határoz meg eljárási szabályokat a biztos e cselekményeinek gyakorlásával kapcsolatban; ilyen rendelkezéseket az Avtv. 23. § (2) bekezdése és 24/A § (1) bekezdése alapján felhívható Obt. sem tartalmaz, mivel annak szabályozása a klasszikus ombusmanmodellt tükrözi. Az „elrendelés", „megtiltás", „felfüggesztés" gyakorlásának tehát nincsenek formai és tartalmi kritériumai; nem érvényesülnek az államigazgatási határozatokkal kapcsolatos, az Áe. illetőleg a Ket. által meghatározott feltételekhez hasonló követelmények (például a határozat kötelező tartalmi elemeivel, kézbesítésével kapcsolatban). A 2005. évi XIX. törvény hatálybalépését megelőzően az Avtv. még azt sem rögzítette, hogy az „elrendelésnek" határozattal kell történnie. Ezen eljárási garanciákat a jogalkotónak álláspontunk szerint mielőbb meg kell teremtenie, akár az Áe. (Ket.) hatályának az adatvédelmi biztosi eljárásra történő kiterjesztésével, akár sajátos eljárás a jelenleginél részletesebb szabályozásával.

A biztos álláspontunk szerint csak a (2) bekezdésben rögzített határidő elteltével alkalmazhatja a (4) bekezdésben meghatározott szankciókat (zárolás, törlés elrendelése, nyilvánosság tájékoztatása stb. – ezzel kapcsolatban lásd alább).

20. A 25. § (5) bekezdése rendelkezik az adatvédelmi biztos határozatának felülvizsgálatáról. „Az adatkezelő, az adatfeldolgozó vagy az adatkezeléssel érintett személy az adatvédelmi biztos (4) bekezdés szerinti határozatának felülvizsgálatát – annak kézhezvételét követő 30 napon belül – jogszabálysértésre hivatkozással kérheti a bíróságtól, amely a felülvizsgálat során a polgári perrendtartásról szóló törvénynek a közigazgatási perekre vonatkozó szabályai szerint jár el. A bíróság jogerős döntéséig a vitatott

[589] Lásd például az Avtv. 26. § (4) bekezdésében meghatározott hatáskört.

[590] Majtényi 1990, 30; Sólyom 2001b, 84 stb.

adatkezeléssel érintett adatok nem törölhetők, illetve nem semmisíthetők meg, az adatok kezelését azonban az adatvédelmi biztos határozatának kézhezvételekor fel kell függeszteni és az adatokat zárolni kell."

Az eljárás körülményei a 2005. évi XIX. törvény hatálybalépését megelőzően teljességgel tisztázatlanok voltak atekintetben, hogy , álláspontunk szerint az intézkedés végrehajtására a keresetlevél benyújtásának halasztó hatálya van-e; ennek különösen az adatok törlésének, illetőleg megsemmisítésének elrendelése esetén van jelentősége. A módosítás által megállapított 25. § (5) bekezdés e kérdést megfelelően szabályozza.

Az adatvédelmi biztos hatósági jogköreinek szabályozásával együtt biztosítja a törvény a 2003. évi novella nyomán a bírósági jogorvoslat lehetőségét a biztos határozata ellen. A jogerős ítéletig az adatkezelést fel kell függeszteni, illetőleg az adatokat zárolni kell, vagyis lehetetlenné kell tenni azok továbbítását, megismerését, nyilvánosságra hozatalát, átalakítását, megváltoztatását, megsemmisítését, törlését, összekapcsolását vagy összehangolását és felhasználását (2. § 13. pontja). Az adatok a bíróság jogerős döntéséig nem törölhetők és semmisíthetők meg.

A bírósági eljárásra a Pp. XX. fejezetét kell alkalmazni, annak alkalmazását a szabályozás kifejezetten elrendeli a Pp. 324. § (2) bekezdés *c)* pontja szerint. E rendelkezést a 2005. évi XIX. törvény emelte be az Avtv-be, miután egyes esetekben a per a Pp."általános szabályai szerint, a személyhez fűződő jogok megsértése miatt indult meg, az adatkezelővel a felperesi, míg az érintettek jogait védő biztossal az alperesi pozícióban"[591].

21. Az adatvédelmi biztos a feladatai ellátása során az adatkezelőtől minden olyan kérdésben felvilágosítást kérhet, az összes olyan iratba betekinthet, illetve iratról másolatot kérhet, adatkezelést megismerhet, amely személyes adatokkal, közérdekű adatokkal vagy közérdekből nyilvános adatokkal összefügghet, és minden olyan helyiségbe beléphet, ahol adatkezelés folyik. (Avtv. 26. § (1)-(2) bek.) Az adatkezelő köteles a részére kibocsátott ajánlásra harminc napon belül érdemben válaszolni. (Avtv. 26. § (3) bek.).

Az adatvédelmi biztos vizsgálatai során gyakran él az (1) és (2) bekezdésben foglalt jogosítványaival. Egyszerűbb panaszügyek esetében általában írásban kér felvilágosítást az adatkezelőtől, ám az ún. megyei vizsgálatok esetében vagy nagyobb jelentőségű ügyekben helyszíni vizsgálatokra is sor kerül.[592] A 2005. évi XIX. törvény rögzítette az ajánlás

[591] ABI 2005, 46

[592] Helyszíni vizsgálatokra lásd például ABI 1998, 69; BI 1999, 199; ABI 1999, 213.

megválaszolására vonatkozó határidőt, valamint a biztos vizsgálati jogosultságával kapcsolatos, az Obt. főszabályától való eltérést (lásd a 24/A § (2) bekezdését).

22. Az adatvédelmi biztos hagyományosan hatósági jellegű jogköre a titokfelügyelettel kapcsolatos. Az Avtv. 26. § (5) bekezdése szerint „ha az adatvédelmi biztos eljárása során az adat minősítését – a nemzetközi szerződés alapján keletkezett minősített adatok kivételével – indokolatlannak tartja, a minősítőt annak megváltoztatására vagy a minősítés megszüntetésére szólítja fel. A felszólítás megalapozatlanságának megállapítása iránt a minősítő 30 napon belül a Fővárosi Bírósághoz fordulhat. A bíróság az ügyben zárt tárgyaláson soron kívül jár el."

Az adatvédelmi biztos – azon túl, hogy az államtitokkörben és szolgálati titokkörben meghatározott adatfajták bővítését vagy szűkítését kezdeményezheti a 25. § (1) bekezdése alapján – akkor is felléphet, ha álláspontja szerint meghatározott adat minősítése indokolatlan. [A minősítés feltételeinek alapvető szabályairól lásd a 25. § (1) bekezdéséhez fűzött magyarázatot.]

Az adatvédelmi biztos 25. § (5) bekezdésében szabályozott jogköre kifejezetten azt az esetet szabályozza, amikor az államtitokká vagy szolgálati titokká minősítés érvényes, ám nem indokolt. A Ttv. mind az államtitok, mind a szolgálati titok esetén a minősítőre bízza a minősítés indokoltságának mérlegelését; államtitokká minősítés során a minősítőnek azt kell megállapítania, hogy annak „az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése vagy felhasználása, illetéktelen személy tudomására hozása, továbbá az arra jogosult részére hozzáférhetetlenné tétele közvetlenül sérti vagy veszélyezteti a Magyar Köztársaság törvényben meghatározott honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi, külügyi vagy nemzetközi kapcsolataival összefüggő, valamint igazságszolgáltatási érdekeit"; míg szolgálati titok esetében azt, hogy annak „az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése és felhasználása, illetéktelen személy részére hozzáférhetővé tétele, továbbá az arra jogosult részére hozzáférhetetlenné tétele sérti vagy veszélyezteti az állami vagy közfeladatot ellátó szerv működésének rendjét, akadályozza a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását, és ezáltal közvetve a Magyar Köztársaság törvényben meghatározott érdekeit hátrányosan érinti". E két tartalmi feltétel határozza meg a minősítés indokoltságát; további feltételek szükségesek a minősítés érvényességéhez [lásd fent a 25. § (1) bekezdésénél és alább]. A biztos a 25. § (5) bekezdésében meghatározott jogkörében tehát azt

állapíthatja meg, hogy az adat minősítése során a fenti tartalmi feltételek nem állnak fenn, a minősítés „indokolatlan".[593]

Az adatvédelmi biztos felszólítása következtében a minősítés nem szűnik meg; a felszólítás jogkövetkezménye a minősítő kötelezettsége a minősítés megváltoztatására vagy megszüntetésére, illetőleg ha ezt nem tartja indokoltnak, akkor a bírósági eljárás kezdeményezésére. A szabályozás problematikus abban a tekintetben, hogy ha a minősítő változtatja vagy szünteti meg a minősítést, és a bírósági eljárást sem kezdeményezi, akkor a minősítés az adatvédelmi biztos felszólítása ellenére fennmarad.[594]

Az irodalomban található olyan nézet, amely szerint az adatvédelmi biztos a 25. § (4) bekezdése alapján a minősítési eljárás jogszerűségét is vizsgálhatja;[595] ez azonban csak abban az esetben van így, ha a hivatkozott feltételek (vagyis az indokoltság) fennállása is része a minősítés jogszerűségének. Magának a minősítési eljárásnak, a minősítés érvényességének a vizsgálata (valóban a minősítő járt-e el?, a minősített adat állam- vagy szolgálati titokkörbe tartozik-e?, a minősítési eljárás maga a jogszabályokban előírt módon történt-e?),[596] továbbá a minősítés érvényességi idejének vizsgálata[597] nem történhet a 25. § (4) alapján.[598] Az adatvédelmi biztosi vizsgálat – a 24. § *a)* pontja alapján – természetesen e kérdésekre is kiterjedhet, ám ezekben az esetekben a biztos nem élhet a 25. § (5) bekezdésében szabályozott felszólítással.[599]

---

[593] Lásd például ABI 1997, 162. (A minősítés indokolatlansága miatt ebben az esetben is felmerül az eljárással kapcsolatos alaki hiba, amely miatt a biztos szerint az adat „már most sem tekintendő államtitoknak".)

[594] Ilyen esetre lásd ABI 2004, 56: „Mivel egyik lépésre sem került sor, a biztos ismételten felhívta az elnök figyelmét a titkosítás megszüntetésére."

[595] Dudás 1999, 8.

[596] A minősítés érvényességének fogalmáról az adatvédelmi biztos és a belügyminiszter között folytatott vitára lásd ABI 2000, 330. skk.

[597] A minősítés érvényességi idejének problémájáról lásd Dudás 1999, 9.

[598] „Ha az adatvédelmi biztosi vizsgálat a minősítést magát nem, hanem az érvényességi időt minősíti túlzottnak, az joghatását tekintve nem különbözik az egyéb adatvédelmi biztosi ajánlástól. Az adatkezelő ez utóbbi esetben haladéktalanul köteles megtenni a szükséges intézkedéseket, és erről 30 napon belül írásban tájékoztatni az adatvédelmi biztost […]. Ám ha nem fogadja el az ajánlást, nem kötelező neki magának bírósághoz fordulnia" (ABI 1998, 307).

[599] A 24. § *a)* pontjára történő hivatkozást lásd például ABI 2000, 335 és ABI 2000, 350. A korabeli nemzetbiztonsági szolgálatokért felelős tárca nélküli miniszter ellentétes véleményére lásd ABI 2000, 346: „A törvény céljából kiindulva és az adatvédelmi biztos szerepköréből levezetve, feladata a közérdekűséggel összefüggésben csak az indokoltsági feltételek kimondására terjedhet ki."

Az adatvédelmi biztos a fentiekkel összhangban számos esetben vizsgálta a minősítési eljárás jogszerűségének a minősítés indokoltságán kívüli elemeit; ezekben az esetekben a vizsgálatok ajánlással, állásfoglalással végződtek. Például „a vizsgálat megállapította, hogy az államtitokká minősítés a levél tartalma alapján jogszerű, ellenben annak időtartama indokolatlanul hosszú, így azt csökkenteni kellene. A […] miniszter a minősítés időtartamát véleményünk figyelembevételével 30 évre változtatta."[600]

Más esetben a biztos megállapította, hogy mivel az ügy tárgyát képező adatok nem tartoztak a Ttv. által meghatározott államtitokkörbe, illetőleg a minősítést nem a törvényben meghatározott minősítő végezte, minősítési javaslat nem készült (vagyis a minősítési eljárás alakilag hibás), az adatok nem tekinthetők államtitoknak.[601] Szintén nem a minősítés indokolatlansága, hanem a formai követelmények megsértése miatt nem minősült az adat államtitoknak a biztos szerint abban az esetben, amelyben a dokumentumhoz „csak utólag csatoltak hozzá egy – a minősítési jelölést tartalmazó – fedlapot, de magán a tervezeten a minősítési jelölés nem szerepelt" – pedig a vonatkozó kormányrendelet[602] szerint a minősítési jelölést (államtitok esetén: „Szigorúan titkos!")[603] magán az adathordozón, papíralapú adathordozó esetén pedig minden egyes lapon, annak felső és alsó részén is fel kell tüntetni.[604] A biztos szerint azonban nem mondható, hogy „a minősítés minden (nem jelentős) alaki hibája feltétlenül érvénytelenné tenné azt".[605]

Előfordult olyan eset is, hogy az adatvédelmi biztos a 26. § (5) bekezdése alapján indítványozta államtitokká minősített adatok minősítésének megszüntetését, mindamellett felhívta az adatkezelő figyelmét arra is, hogy az adatok – mivel nem a törvényben meghatározott minősítő járt el – nem tekinthetők jogszerűen minősítettnek.[606]

1.19. Az adatvédelmi nyilvántartás és az előzetes ellenőrzés

1. Az adatvédelmi nyilvántartás – e tipikusan már az első generációs adatvédelmi törvényekben megjelent intézmény – hatályos magyar szabályozását az Avtv. 28. és

[600] ABI 1998, 67 és 1998, 301. skk.

[601] ABI 1999, 137; ABI 2000, 17. skk.; ABI 2000, 321. skk.; a korabeli belügyminiszter ellentétes értelmezésére ABI 2000, 332.

[602] A minősített adat kezelésének rendjéről szóló 79/1995. (VI. 30.) Korm. rendelet 16. §.

[603] A minősítési jelölésekre lásd a Ttv. 9. §-át.

[604] ABI 1999, 137; ABI 1999, 363. skk.

[605] ABI 2000, 340.

[606] ABI 2000, 381.

következő §§-ai adják. A 28. § (1) bekezdése a nyilvántartás adattartamát az alábbiak szerint határozza meg:

„28. § (1) A személyes adatokat kezelő köteles e tevékenysége megkezdése előtt az adatvédelmi biztosnak nyilvántartásba vétel végett bejelenteni

a) az adatkezelés célját;

b) az adatok fajtáját és kezelésük jogalapját;

c) az érintettek körét;

d) az adatok forrását;

e) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját;

f) az egyes adatfajták törlési határidejét;

g) az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;

h) a belső adatvédelmi felelős nevét és elérhetőségi adatait."

Az adatkezelések nyilvántartásba vételének (sőt, akár engedélyeztetésének) kötelezettsége már az első generációs adatvédelmi törvényekben megjelent; a nagy adatbázisok korában ez jelentette az adatkezelés transzparenciájának egyik legfontosabb garanciáját. Bár idővel a nyilvántartások szerepe csökkent, a bejelentési kötelezettség alól mentes adatkezelések száma nőtt, az adatvédelmi nyilvántartás szabályozása az irányelv által előírt kötelezettség (igaz, azt helyettesítheti a nemzeti szabályozásban belső, tehát az adatkezelő által vezetett adatvédelmi nyilvántartás előírása is).

2. Az Avtv. az adatvédelmi nyilvántartás vezetésének kötelezettségét az adatvédelmi biztos feladatkörének részeként szabályozza [24. § *c)* pontja], és kimondja azt, hogy az adatvédelmi nyilvántartásba bárki betekinthet [11. § (2) bekezdése]. Az adatvédelmi nyilvántartás magyar szabályozása a centralizált modellt követi: nem eredményez a bejelentés alóli mentességet a belső adatvédelmi nyilvántartás vezetése – az Avtv. erre vonatkozó kötelezettséget sem tartalmaz, bár a fogalom a normaszövegben egy helyen szerepel [31/A. § (2) bekezdés *e)* pontja].

3. A nyilvántartásba vétel egyszerű regisztrációs aktus: „A nyilvántartásba vételt az adatvédelmi biztos nem tagadhatja meg, de ha törvénysértő adatkezelést észlel, már a bejelentkezéssel egy időben megteheti a szükséges intézkedéseket"[607]: vagyis hivatalból

[607] ABI 1998, 170; hasonlóan ABI 1999, 180.

vizsgálatot indíthat.[608] 2004. január 1-jétől az adatvédelmi biztos a nyilvántartásba vételt megelőzően bármely adatkezelés vonatkozásában előzetes ellenőrzést végezhet [lásd a 31. § (1) bekezdéséhez fűzött magyarázatot].

4. A nyilvántartás alapegysége az elsősorban az *adatkezelés,* amely elsősorban annak céljával jellemezhető. Az adatkezelés körülhatárolása azonban nem triviális feladat: egy adatkezelés több olyan mozzanatból állhat, amelyek magukban is adatkezelési műveleteknek minősülnek (felvétel, tárolás, felhasználás, törlés ugyanazon célú adatkezelés keretében, például valamely ügyféladatbázis adattartalma vonatkozásában). Az adatkezelések körülhatárolása a gyakorlatban mégsem okoz problémát – ennek magyarázata, hogy az adatkezelők nem adatkezeléseket, hanem a meghatározott célból kezelt *adatállományokat* jelentik be. (Az adatvédelmi biztos beszámolói is több esetben „nyilvántartás", „adatbázis" bejelentését említik – lásd alább a 30. §-hoz fűzött magyarázatot.) Ez a gyakorlat álláspontunk szerint nem problematikus, sőt, indokolt lehet az adatállomány fogalmának bevezetése nyomán (Avtv. 2. § 18. pontja) a szabályozást e ponton a jövőben megváltoztatni. Az adatállományt jellemez valamely elsődleges adatkezelési művelet, és mindenképpen egy adatkezelési cél (üzleti partnerek adatbázisa, cél a kapcsolattartás; marketing-adatbázis, cél a kapcsolatfelvétel).

5. Egyes esetekben (meghatározott adatkezelők által új adatállományok feldolgozása, illetőleg új adatfeldolgozási technológia alkalmazása) az adatvédelmi nyilvántartásba bejelentendő adatkezelés egyben a 31. § (3) bekezdésében meghatározott, előzetes ellenőrzéssel kapcsolatos bejelentési kötelezettség hatálya alá is esik – erről lásd a hivatkozott törvényhelyhez fűzött magyarázatot.

1.19.1. Az adatvédelmi biztos gyakorlata

1. A bejelentés megtétele főszabály szerint az *adatkezelő* kötelezettsége, jogszabályban elrendelt adatkezelés esetén pedig azt a szabályozás tárgya szerint illetékes miniszter, országos hatáskörű szerv vezetője, illetőleg a polgármester, főpolgármester, a megyei közgyűlés elnöke teszi meg [lásd a (2) bekezdést].

2. Ha a bejelentkező adatfeldolgozónak minősül, az adatvédelmi biztos nem utasítja el a nyilvántartásba vételt, hanem azt adatkezelőként veszi nyilvántartásba.[609]

[608] Ilyen vizsgálatra lásd például: ABI 1999, 106.

[609] ABI 2000, 164.

3. Az adatvédelmi nyilvántartásba való bejelentkezési kötelezettséggel kapcsolatban fogalmazta meg az adatvédelmi biztos azt az álláspontunk szerint vitatható tételt, amely szerint egy adatkezeléshez csak egy adatkezelő kapcsolódhat. „Az Avtv. alapelvei kimondják, hogy bár egy adatkezelő természetesen több adatkezeléssel is rendelkezhet, egy adatkezelésnek csak egy felelős adatkezelője lehet."[610]

4. Az adatvédelmi biztos elmarasztaló állásfoglalásaiban egyes esetekben hangsúlyosan jelenik meg az adatvédelmi nyilvántartásba való bejelentkezés kötelezettségének elmulasztása. Ilyen volt az az ügy, amelyben a pénzügyminiszter egyes, felügyelete alá tartozó szerveket (APEH, Államháztartási Hivatal, Magyar Államkincstár, VPOP, PSZÁF, Szerencsejáték Felügyelet) arra szólított fel, hogy azok adatállományaikat – tisztázatlan célból – továbbítsák a Pénzügyminisztériumba. A biztos beszámolója szerint a bejelentés elmulasztásával „az adatkezelők […] sokmilliós – személyes adatokat tartalmazó – adatállományokat rejtettek el az adatvédelmi biztos elől, és ezzel azokat kivonták az adatalanyok kontrollja alól is".[611] Természetesen ez csak következménye annak, hogy – a biztos állásfoglalása szerint – az adatkezelésnek jogalapja sem volt (hiszen abban az esetben vagy az érintett hozzájárulása, vagy a kihirdetett jogszabály biztosította volna az érintett számára az adatkezelés megismerhetőségét, a kontrollt).

1.19.2. Az irányelv vonatkozó rendelkezései

Az irányelv az adatkezelés transzparenciájára vonatkozó nyilvántartás szabályozásának két elemét külön szabályozza. Meghatározza egyrészt az felügyelő hatóság „értesítésének" kötelezettségére (a bejelentési kötelezettségre) vonatkozó szabályokat és az értesítés tartalmát (18. és 19. cikk), másrészt külön az adatvédelmi nyilvántartást és az abban tárolt adatok nyilvánosságát, valamint az adatkezelő tájékoztatási kötelezettségét az értesítési kötelezettség alá nem eső adatok tekintetében (21. cikk), az alábbiak szerint:

„*18. cikk*

A felügyelő hatóság értesítésére vonatkozó kötelezettség

(1) A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő vagy annak képviselője, ha van ilyen, értesítse a 28. cikkben említett felügyelő hatóságot [a magyar szabályozás szerint az adatvédelmi biztost] akár egyetlen, akár több, összefüggő célt szolgáló,

[610] ABI 1999, 178.

[611] ABI 2004, 39.

részben vagy egészen automatizált módon történő adatfeldolgozási művelet vagy műveletsorozat elvégzését megelőzően.

(2) A tagállamok kizárólag a következő esetekben és feltételek mellett rendelkezhetnek az értesítés módjának egyszerűsítéséről vagy az értesítési kötelezettség alóli felmentésről:

– amennyiben az olyan adatfeldolgozási műveletek kategóriái esetében, amelyek – figyelembe véve a feldolgozandó adatokat – valószínűleg nem befolyásolják hátrányosan az érintettek jogait és szabadságait, meghatározzák az adatfeldolgozás célját, a feldolgozásra kerülő adatokat vagy adatkategóriákat, az érintettek körét vagy köreit, azokat a címzetteket vagy címzettek kategóriáit, akik számára az adatokat továbbították, továbbá az adatok tárolásának időtartamát, és/vagy

– amennyiben az adatkezelő a rá vonatkozó nemzeti jogszabályokkal összhangban kijelöl egy személyesadat-védelmi tisztviselőt, aki elsősorban az alábbiakért felelős:

– az ezen irányelv alapján elfogadott nemzeti rendelkezések belső alkalmazásának független módon való biztosítása,

– az adatkezelő által végzett adatfeldolgozási műveletek nyilvántartásának vezetése, amely tartalmazza a 21. cikk (2) bekezdésében említett adatokat,

ezáltal biztosítva, hogy az adatfeldolgozási műveletek várhatóan ne befolyásolják hátrányosan az érintettek jogait és szabadságait.

(3) A tagállamok rendelkezhetnek arról, hogy az (1) bekezdés ne vonatkozzon arra az adatfeldolgozásra, 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.

(4) A tagállamok a 8. cikk (2) bekezdésének *d)* pontjában említett adatfeldolgozási műveletek esetében [alapítvány, egyesület vagy bármely más nonprofit szervezet által végzett adatkezelés politikai, világnézeti, vallási vagy szakszervezeti céllal, a szervezet tagjai vagy azzal rendszeres kapcsolatban álló személyek vonatkozásában] rendelkezhetnek az értesítési kötelezettség alóli felmentésről vagy az értesítés módjának egyszerűsítéséről.

(5) A tagállamok kiköthetik, hogy egyes vagy az összes, személyes adatot érintő, nem automatizált adatfeldolgozási művelet értesítési kötelezettség alá tartozzon, vagy rendelkezhetnek arról, hogy ezen adatfeldolgozási műveletek egyszerűsített értesítés tárgyát képezzék.

19. cikk

Az értesítés tartalma

(1) Az értesítésben foglalt adatokat a tagállamok határozzák meg. Az értesítésnek legalább a következőket tartalmaznia kell:

a) az adatkezelő, vagy – ha van ilyen – annak képviselőjének neve és címe;

b) az adatfeldolgozás célja vagy céljai;

c) az érintettek körének vagy köreinek, továbbá a rájuk vonatkozó adatok vagy adatkategóriák leírása;

d) azoknak a címzetteknek vagy címzett kategóriáknak a leírása, akik számára az adatokat továbbították;

e) harmadik országokba irányuló tervezett adattovábbítások,

f) általános leírás, amely lehetővé teszi a 17. cikk értelmében az adatfeldolgozás biztonsága érdekében hozott intézkedések megfelelő mivoltának előzetes értékelését.

(2) A tagállamok határozzák meg azokat az eljárásokat, amelyek keretében a felügyelő hatóságot az (1) bekezdésben említett adatokat érintő bármilyen változásról értesíteni kell. […]

21. cikk

Az adatfeldolgozási műveletek nyilvánosságának biztosítása

(1) A tagállamoknak intézkedéseket kell tenniük az adatfeldolgozási műveletek nyilvánosságának biztosítására.

(2) A tagállamoknak rendelkezniük kell arról, hogy a 18. cikk szerinti adatfeldolgozási műveletekről a felügyelő hatóság nyilvántartást vezessen.

A nyilvántartásnak legalább a 19. cikk (1) bekezdésének *a)–e)* pontjában felsorolt adatokat tartalmaznia kell.

A nyilvántartást bárki megtekintheti.

(3) Az értesítéshez nem kötött adatfeldolgozási műveletek kapcsán a tagállamoknak rendelkezniük kell arról, hogy az adatkezelők vagy a tagállamok által kijelölt egyéb szerv kérelemre, bárki számára megfelelő formában bocsássa rendelkezésre legalább a 19. cikk (1) bekezdésének *a)–e)* pontjában felsorolt adatokat.

A tagállamok rendelkezhetnek arról, hogy ez a rendelkezés ne vonatkozzon arra az adatfeldolgozásra, 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.”

1.19.3. Szabályozási javaslat

Számos jel mutat arra, hogy a bejelentkezési kötelezettséget az adatkezelők tömegesen mulasztják el.[612] A 2003. évi novella szabályozta az adatvédelmi felelősi intézményt – megfontolandó lehet a jogalkotó számára legalább azon esetekben, amelyekben a szervezetnél adatvédelmi felelős megbízása kötelező, a központi adatvédelmi nyilvántartásba történő bejelentkezés kötelezettsége helyett belső adatvédelmi nyilvántartás vezetésének előírása. A nyilvántartásba vételi kötelezettség egyes esetekben ráadásul a számos kivételi kör ellenére is kiterjed olyan adatkezelésekre, amelyekkel kapcsolatban a bejelentési kötelezettség abszurd következményekkel jár – ezzel kapcsolatban az is felmerült, hogy a biztos a nyilvántartás adattartamának szűkítésére irányuló törvénymódosítást fog kezdeményezni.[613]

1.19.4. A kivételi körök

1. Az Avtv. 30. §-a szerint

„Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely

a) az adatkezelővel munkaviszonyban, tagsági, tanulói viszonyban, ügyfélkapcsolatban álló személyek adatait tartalmazza;

b) egyház, vallásfelekezet, vallási közösség belső szabályai szerint történik;

c) az egészségügyi ellátásban kezelt személy betegségére, egészségi állapotára vonatkozó személyes adatokat tartalmaz, gyógykezelés vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;

d) az érintett anyagi és egyéb szociális támogatását célzó és nyilvántartó adatokat tartalmaz;

e) a hatósági, az ügyészségi és a bírósági eljárás által érintett személyeknek az eljárás lefolytatásával kapcsolatos személyes adatait tartalmazza;

f) a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve hogy – külön törvényben meghatározottak szerint – az adatok személlyel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;

g) a sajtótörvény hatálya alá tartozó társaságok és szervek olyan adatait tartalmazza, amelyek kizárólag saját tájékoztatási tevékenységüket szolgálják;

h) a tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra;

---

[612] Lásd például ABI 1999, 179. Az 1999-ben beérkezett bejelentések figyelembevételével a biztos megválasztását követő negyedik évben a bejelentkezett magánszférabeli adatkezelők száma 134 volt: ABI 2000, 169.

[613] ABI 2000, 286.

i) az adatkezelőtől levéltári kezelésbe került át;

j) a természetes személy saját célját szolgálja.

A 30. § igen széles körű kivételeket állapít meg az adatvédelmi nyilvántartásba való bejelentkezés kötelezettsége alól, amely kivételeket az adatvédelmi biztosi gyakorlat – lásd alább – igyekszik megszorítóan értelmezni.

A megszorító értelmezés különösen jellemző a biztos *a)* pontot illető értelmezési gyakorlatára. Emögött az a megfontolás áll, amely szerint: „A kivételek körének ilyen széles megengedése nyilván nem lehetett a jogalkotó szándéka, hiszen ez teljesen funkciótlanná tenné az adatvédelmi nyilvántartást."[614]

A 30. § *a)* pontjában meghatározott, munkavállalókra vonatkozó adatkezelésre vonatkozó kivételi körrel kapcsolatban az adatvédelmi biztos kimondta, hogy „kizárólag azokat az adatkezeléseket nem kell bejelenteni, amelyeket a munkáltatók számára a jogszabályok kötelezően előírnak"; a biztos szerint ebbe a körbe tartoznak például a társadalombiztosítással, a személyi jövedelemadózással kapcsolatos, meghatározott szervek irányába történő adattovábbítások.[615] A biztos értelmezése szerint nem kell bejelenteni „a munkáltatók által végzett, jogszabályban előírt adatkezeléssel kapcsolatos nyilvántartásokat (például közszolgálati nyilvántartás, a munkáltató keretein belül folytatott bérszámfejtés kapcsán létrejött adatbázis)" sem.[616] Azonban más esetben a biztos értelmezése szerint ezek az adatkezelések is bejelentési kötelezettség alá esnek: nevezetesen akkor, „ha az adatokat nem a munkavállaló adja meg, illetve az adatkezelés célja eltér a jogszabályokban minden munkáltató számára előírt adatkezelési céloktól".[617] Az interpretációt alátámasztja az Avtv. miniszteri indokolása, amely szerint az „e [30. §-ban meghatározott] kivételekben meghatározott adatkezeléseket is be kell jelenteni, ha céljuk vagy tartalmuk több vagy más – például a továbbítást, nyilvánosságra hozást vagy egyéb hasznosítást illetően –, vagy a statisztikai előkészítés során személyes azonosítóiktól nem fosztják meg őket". Álláspontunk szerint az értelmezés az *a)* pont vonatkozásában mindenképpen téves: a jogalkotó az indokolásban azon kivételi körökre utal, ahol a kivételt az adatkezelés célja határozza meg [például az *e)* pont esetén]. Az *a)* pontban foglalt esetekben a kivétel álláspontunk szerint

[614] ABI 1998, 171.

[615] ABI 1998, 175.

[616] ABI 1998, 175.

[617] ABI 1998, 175.

minden, a szövegben felsorolt adatalany személyes adatait „tartalmazó" adatkezelésre vonatkozik.

Az adatvédelmi biztos értelmezése szerint az *a)* pont alatt szabályozott ezen kivételi körbe tartozik a megbízási, köztisztviselői, közalkalmazotti, illetőleg munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottak személyes adataival kapcsolatos adatkezelés is, mert „az érintett információs önrendelkezési joga szempontjából ezek a jogviszonyok nem különböznek", ám a bejelentkezési kötelezettség fennáll, ha „az ilyen típusú adatkezelési tevékenységet a munkaviszonyra irányuló jogviszony keretein kívül végzik […] például bérszámfejtő cég megbízás alapján".[618] Nézetünk szerint az az álláspont is vitatható, amennyiben a megbízott által végzett tevékenység adatfeldolgozásnak minősül (2. § 15. pontja). A biztos szerint a kivételi kör nem terjed ki a fegyveres testületeknél szolgálatot teljesítők szolgálati viszonyára sem.[619]

2. Az adatvédelmi biztos másik, az *a)* pontban foglalt kivételi körrel kapcsolatos állásfoglalása szerint, bár „az önkéntességen alapuló tagsági vagy ügyfélkapcsolati viszonyban álló személyek esetében az adatkezelő mentesül a bejelentési kötelezettség alól, mivel az adatalanyok a kapcsolat kialakítása során érvényesíthetik információs önrendelkezési jogukat", a kivételi kör nem terjed ki azokra az esetekre, amelyekben a tagság kötelező (az adott esetben az akkor hatályos szabályok szerint kötelező kamarai tagság volt az ügy tárgya).[620] „Az adatvédelmi biztos állásfoglalása alapján […] a jogalkotói szándék szerint ez a mentességi kör az önkéntes belépésen alapuló tagsági viszonyra vonatkozik."[621]

3. Az „ügyfélkapcsolat" fogalmát értelmezve a biztos úgy foglalt állást, hogy az Avtv. által használt fogalom nem azonos az Áe. ügyfélfogalmával; a „bejelentkezési kötelezettség alóli mentességet eredményező ügyfélkapcsolatról csak akkor lehet szó, ha az Avtv. indokolásában említett, a mentességet megalapozó tényezők fennállnak, vagyis az adatkezelés célja az érintett számára ismert, az adatfelvétel közvetlenül tőle történik, valamint a személyes adatok kezelése az érintettel fennálló jogviszonyhoz vagy szolgáltatáshoz kapcsolódik".[622]

4. A *c)* pontban foglalt kivételi körrel kapcsolatban az adatvédelmi biztos megállapította, hogy „bár generális szabályként a gyógykezelés vagy az egészség megőrzése céljából végzett adatkezelés kivételként szerepel, de minden rendezett adatbázis létét (például

[618] ABI 1998, 176.

[619] ABI 2000, 168.

[620] ABI 1997, 66.

[621] ABI 1998, 176.

[622] ABI 1998, 176.

alapítványokkal, pályázatokkal kapcsolatos személyes adatok kezelését) be kell jelenteni az adatvédelmi nyilvántartásba". Álláspontunk szerint a rendelkezés egyszerre határozza meg a célt (gyógykezelés, egészség megőrzése) és az adatalanyok (az egészségügyi ellátásban kezelt személy), valamint az adatok (betegségre, egészségi állapotra vonatkozó személyes adatok) körét, így hatálya további értelmezés nélkül is egyértelműen meghatározható.

5. A *d)* pontban megfogalmazott kivételi körrel kapcsolatban megemlítendő, hogy a biztos állásfoglalása szerint be kell jelenteni a nyilvántartásba a gyámügyi igazgatás területén végzett adatkezeléseket.[623]

1.19.5. Az előzetes ellenőrzés

1. Az Avtv. 31. § (1) bekezdése szerint az adatvédelmi biztos a nyilvántartásba vételt megelőzően előzetes ellenőrzést végezhet. Az előzetes ellenőrzés intézményét az Avtv. 2003. évi novellája vezette be a törvénybe.[624]

Az adatvédelmi biztos (1) bekezdésben meghatározott jogköre bármely adatkezelés vonatkozásában biztosítja az előzetes ellenőrzés lefolytatásának lehetőségét az adatvédelmi nyilvántartásba történő bejegyzést megelőzően. A szabályozással kapcsolatos értelmezési kérdés, hogy ebben az esetben az előzetes ellenőrzés befejezése feltétele-e az adatvédelmi nyilvántartásba történő bejegyzésnek. A szövegezés erre utal: a biztos az ellenőrzést „a nyilvántartásba vételt megelőzően" végezheti. Álláspontunk szerint kívánatos lenne, ha a szabályozás azt tükrözné, hogy – összhangban a korábbi adatvédelmi biztosi gyakorlattal – a bejegyzés az ellenőrzés megtörténtétől és eredményétől független aktus.

2. Az adatvédelmi biztos által az (1) bekezdés alapján végzett esetleges előzetes ellenőrzés – az Avtv. novellájának indokolásából kiolvasható jogalkotó szándék szerint – nem korlátozza az adatkezelőt az adatkezelés megkezdésében. Ebben az esetben az ellenőrzésre a (3) bekezdésben meghatározott 30 napos határidőt sem kell alkalmazni. A biztos számára az ellenőrzés eredményéhez képest rendelkezésre állnak a (4) bekezdésben írt eszközök („a kezelendő adatok körének, illetőleg az adatfeldolgozás módszerének megváltoztatására hívhatja fel az adatkezelőt", illetőleg jogszabály-módosítást is kezdeményezhet); álláspontunk szerint azonban egyébként sem kizárt a vizsgálat hivatalból történő lefolytatása [lásd a 25. § (1) bekezdéséhez fűzött magyarázatot], és bármely, az Avtv.-ben írt szankció alkalmazása.

---

[623] ABI 2000, 167.

[624] Az irányelv nyomán már 1997-ben szorgalmazta az intézmény meghonosítását Balogh 1997b.

3. A normaszöveg szerint az (1) bekezdés alapján végzett előzetes ellenőrzésre „a nyilvántartásba vételt megelőzően", az Avtv. miniszteri indokolása szerint „az adatkezelés adatvédelmi nyilvántartásba vételét megelőzően" kerülhet sor. Álláspontunk szerint ennek alapján nem végezhető előzetes ellenőrzés abban az esetben, ha az adatkezelő a 29. § (2) bekezdése alapján az adatkezelésre vonatkozó adatok megváltozását jelenti be, kivéve, ha a változás az adatkezelés célját érinti – nézetünk szerint ebben az esetben a bejelentés új adatkezelés bejelentéseként értékelendő [lásd a 29. § (2) bekezdéséhez fűzött magyarázatot].

3. Az Avtv. 31. § (2) bekezdése szerint „új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően az adatvédelmi biztos előzetes ellenőrzést végezhet a következő adatkezeléseket végző adatkezelőknél:

a) országos hatósági, munkaügyi és bűnügyi adatállományok;

b) pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelései;

c) távközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezelései;

d) külön törvényben meghatározott egyedi statisztikai adatokat tartalmazó adatállományok."

Az előzetes ellenőrzés (2) bekezdésben meghatározott esetében az adatvédelmi biztos meghatározott, széles alanyi körre kiterjedő „adatállományokat", illetőleg meghatározott adatkezelők által végzett adatkezeléseket vonhat előzetes ellenőrzés alá „új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően". A jogalkotó szerint „[e]zek közös jellemzője, hogy adatkezelésük a lakosság széles körét érinti így fokozottabb a személyes adatok sérelmének veszélye".[625]

4. Az Avtv. 2. § 18. pontja szerint „adatállomány: az egy nyilvántartó rendszerben kezelt adatok összessége"; 2. § 17. pontja szerint „személyesadat-nyilvántartó rendszer (nyilvántartó rendszer): személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető". A fogalmak értelmezéséhez lásd a hivatkozott rendelkezésekhez fűzött magyarázatokat.

A rendelkezéssel kapcsolatban vizsgálandó az a kérdés, hogy mely módon határolható körül egy „adatállomány". Elképzelhető olyan álláspont, amely szerint döntő az adatkezelési cél, vagyis elsősorban ez ad támpontot adott esetben valamely adatállomány körülhatárolásához. Ezt támasztja alá az adatvédelmi biztos értelmezése is, amely szerint a célhoz kötöttség elvéből következően nem elfogadható az az értelmezés, amely szerint egy

[625] A 2003. évi XLVIII. törvény miniszteri indokolása.

nagy adatkezelő szervezet (az adott esetben: bank) egy nyilvántartó rendszernek, vagyis az általa kezelt személyes adatok egy adatállománynak minősülnének.[626] (Elvileg ez álláspontunk szerint elképzelhető, amennyiben egy szervezet csak egy célból végez személyes adatkezelést – ez azonban a gyakorlatban egy kereskedelmi bank esetében valószínűtlen.) Lehetséges ugyanakkor olyan értelmezés is, amely szerint az adatállomány, illetve a nyilvántartó rendszer formálisan határozható meg, tehát a céltól függetlenül körülhatárolható a 2. § 17. pontjában foglalt definíció alapján. A két értelmezés nyomán eltérően határozható meg az is, hogy mely esetben „új" valamely adatállomány: míg az előbbit elfogadva az adatkezelési cél változása is „új" adatállományt eredményez, az utóbbi esetében valamely új, a 2. § 17. pontjában meghatározott definíció szempontjából releváns körülmény avathatja „újjá" az adatállományt.

Álláspontunk szerint a jogalkotói cél arra irányult, hogy személyes adatok tömeges kezelésének megkezdése előtt tegye lehetővé az adatvédelmi biztos számára az előzetes ellenőrzést. Nézetünk szerint tehát az adatkezelési cél változása nyomán az „adatállomány" nem feltétlenül minősül újnak, ám nyilvánvalóan annak minősül – a cél által elsődlegesen meghatározott – adatkezelés [lásd a 2. § 9. pontjához fűzött magyarázatot]. Ilyen esetben tehát az adatvédelmi biztos nem a 31. § (2) bekezdésben szabályozott előzetes ellenőrzést végez, illetőleg az adatkezelő bejelentési kötelezettsége nem a 31. § (3) bekezdésén alapul; a bejelentést az adatkezelés céljának megváltozásáról a 29. § (2) bekezdése alapján kell megtenni, az adatvédelmi biztosnak pedig e bejelentés nyomán van módja a fellépésre.

Nézetünk szerint nem új az adatállomány abban az esetben sem, ha annak tartalma folyamatosan változik, sőt, az az adattartalom akár teljes kicserélődése nyomán sem minősül újnak az adatállomány, ha az adatvédelmi biztos által az előzetes ellenőrzés során vizsgált körülmények (az adatok „feldolgozásának" módszere, a kezelt adatfajták stb.) nem változnak.

5. Az adatállomány fogalmának alkalmazásával a jogalkotó kizárja az előzetes ellenőrzést abban az esetben, ha az új adatkezelés nem minősül új adatállomány „feldolgozásának": tehát ha az adatkezelés nem strukturált adatállomány vonatkozásában történik stb.

6. Az adatvédelmi biztosi értelmezés szerint: „Annak eldöntése, hogy egy adatkezelési módszer vagy technológia újszerű-e, mindig az adott esetben dönthető el."[627] „Adatfeldolgozási technológia" lehet hardver-, szoftvereszköz, vagy ezek bármely együttese;

[626] 1245/x/2003–3. sz. ügyirat, publikálva a http://www.adatvedelem.vilaga.hu oldalon.

[627] 1245/x/2003–3. sz. ügyirat, publikálva a http://www.adatvedelem.vilaga.hu oldalon.

ám már működő rendszerek esetén a rendelkezés alkalmazásában az újszerűség csak a releváns elemek újdonságát jelentheti. „Új adatfeldolgozási technológia" lehet például valamely bűnüldözési célból alkalmazásba vett arcfelismerő rendszer, a hardvereszközökkel (kamerák, számítógépek) és szoftverekkel együtt; ám ha a rendszert már üzembe helyezték, a későbbiekben nem feltétlenül minősül „új technológiának" valamely számítógép cseréje vagy az operációs rendszer frissítése. Ám az is lehetséges, hogy egyes elemek cseréjével a rendszer által végzett személyes adatkezelés feltételei is megváltoznak: ezekben az esetekben az ilyen technológia már „új technológiának" minősül.

Ebben a kérdésben – a fenti, esetenkénti mérlegelés szükségére utaló biztosi állásfoglaláson túl – még nem áll rendelkezésre elemezhető jogalkalmazói gyakorlat. A magyar adatvédelmi biztosi eddig kerülte a technológiai megoldások beható vizsgálatát (lásd erre a 10. §-hoz fűzött magyarázatot): az új adatfeldolgozási technológia kapcsán végzett előzetes ellenőrzés megteremti erre a lehetőséget. Hogy a lehetőség valóban meghozza-e majd a technikai adatvédelem vizsgálatát, az függ a biztosi szerepfelfogástól, de a hazai harmadik generációs adatvédelmi szabályozás fejlődésétől is (például attól, hogy legalább a közigazgatáson belül kialakul-e egy, a személyes adatok kezelését végző rendszerekre is alkalmazandó biztonsági keretrendszer).

7. Az adatvédelmi biztos a (2) bekezdésben meghatározott előzetes ellenőrzést új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően is csak meghatározott adatállományok tekintetében, illetőleg meghatározott adatkezelőknél végezheti. Ezek közös jellemzője az Avtv. miniszteri indokolása szerint, hogy „a lakosság széles körét érinti[k]".

Az *országos hatósági, munkaügyi és bűnügyi adatállományok* közé sorolható például az 1999. évi LXXXV. törvényben szabályozott bűnügyi nyilvántartás vagy az 1991. évi IV. törvény – 2003-ban megállapított – 57/B. §-ában szabályozott Egységes munkaügyi nyilvántartás. A jogalkotó az *a)* pont esetében az adatállományok, nem pedig adatkezelők vonatkozásában határozta meg az előzetes ellenőrzés lehetőségét, vagyis annak lehetősége attól függetlenül fennáll, hogy az ilyen adatállományokat mely szervezet vagy személy kezeli.

A *pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelései*vel kapcsolatban elsősorban az szorul értelmezésre, hogy mely szervezetek tartoznak a „pénzügyi szervezet" fogalma alá. Az Avtv. indokolásából kiolvasható jogalkotói cél alapján – és az adatvédelmi biztos értelmezése szerint is[628] – a jogalkotó azokra a

[628] 1245/x/2003–3. sz. ügyirat, publikálva a http://www.adatvedelem.vilaga.hu oldalon.

szervezetekre utal, amelyekre a Pénzügyi Szervezetek Állami Felügyeletéről szóló 1999. évi CXXIV. törvény szerint a PSZÁF hatásköre kiterjed. Ezek a szervezetek a következők:

– a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény,

– a tőkepiacról szóló 2001. évi CXX. törvény,

– a biztosítóintézetekről és a biztosítási tevékenységről szóló 1995. évi XCVI. törvény,

– az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény,

– a magánnyugdíjról és a magánnyugdíjpénztárakról szóló 1997. évi LXXXII. törvény,

– a közraktározásról szóló 1996. évi XLVIII. törvény,

– az egyes szakosított hitelintézetekről szóló törvények,

– a kockázati tőkebefektetésekről, a kockázati tőkealapokról szóló 1998. évi XXXIV. törvény,

– a fogyasztói csoportokról szóló külön jogszabály.

Közüzemi szolgáltató a Ptk. 387–388. §-ában szabályozott közüzemi szerződés alapján szolgáltatást nyújtó szolgáltató.

Az adatkezelők e körénél az adatvédelmi biztos a (2) bekezdés szerint azok „ügyfelekre vonatkozó adatkezelései" vonatkozásában végezhet előzetes ellenőrzést: az Avtv. 1/A. § (1) bekezdésében meghatározott hatályából következően – valamint az adatkezelés fogalmának a 2. § 9. pontjában rögzített definíciójából következően – az ellenőrzés lehetősége abban az esetben áll fenn, ha az adatkezelés során kezelt ügyféladatok (vagy azok egy része) természetes személlyel kapcsolatba hozhatók.

A *távközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezeléseivel* kapcsolatban utalni kell az elektronikus hírközlésről szóló 2003. évi C. törvényre (a továbbiakban: Eht.), amelynek 186. § (2) bekezdése szerint: „Ahol e törvény hatálybalépését megelőzően kiadott jogszabály olyan meghatározást használ, amely tartalmát tekintve megfelel e törvény […] szerinti meghatározásnak, e törvény meghatározását kell érteni, így különösen, ahol […] távközlést említ, ott elektronikus hírközlést, […] távközlési szolgáltatást […] említ, ott elektronikus hírközlési szolgáltatást […] kell érteni." Az Eht. 188. § 13. pontja szerint elektronikus hírközlési szolgáltatás az „olyan, más részére általában ellenszolgáltatásért végzett szolgáltatás, amely teljesen vagy nagyrészt jeleknek elektronikus hírközlő hálózatokon történő átviteléből, és ahol ez értelmezhető, irányításából áll, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások felhasználásával továbbított tartalmat szolgáltató vagy ilyen tartalom felett szerkesztői ellenőrzést gyakorló szolgáltatásokat, valamint nem foglalja magában az információs

társadalommal összefüggő, más jogszabályokban meghatározott szolgáltatásokat, amelyek nem elsősorban az elektronikus hírközlő hálózatokon történő jeltovábbításból állnak"; a hivatkozott paragrafus 14. pontja szerint pedig elektronikus hírközlési szolgáltató az „elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság". Az adatvédelmi biztos ellenőrzése az ilyen szolgáltatók által végzett, a szolgáltatást igénybe vevő természetes személy adatait (is) tartalmazó adatkezelésre terjed ki. Az igénybe vevők köre nem azonos az előfizetők körével; a szolgáltatást igénybe vevő személy nem feltétlenül előfizetője az adott szolgáltatásnak.

E körbe tartoznak végül a *külön törvényben meghatározott egyedi statisztikai adatokat tartalmazó adatállományok.* A statisztikáról szóló 1993. évi XLVI. törvény 17. § (2) bekezdése szerint „a statisztikai célt szolgáló, a természetes és a jogi személy, valamint a jogi személyiséggel nem rendelkező adatszolgáltatóval kapcsolatba hozható adat". Az adatvédelmi biztos által az Avtv. 31. § (2) bekezdése szerint végzett előzetes ellenőrzés olyan adatállományokra terjedhet ki, amelyek személyes adatnak minősülő egyedi statisztikai adatokat, vagy ilyeneket is tartalmaznak; az adatkezelő a szabályozás szempontjából nem releváns.

8. A 31. § (3) bekezdés szerint „az adatkezelőnek az új adatállomány feldolgozására vagy az új adatfeldolgozási technológia alkalmazására irányuló szándékát a tevékenység megkezdését megelőzően 30 nappal be kell jelentenie az adatvédelmi biztosnak. Az adatvédelmi biztos az előzetes ellenőrzésre vonatkozó igényét a bejelentéstől számított 8 napon belül köteles jelezni az adatkezelőnek, és az ellenőrzést 30 napon belül köteles elvégezni. Az adatkezelő a feldolgozást csak az adatvédelmi biztos előzetes ellenőrzésének befejezése után kezdheti meg." A 31. § (3) bekezdésében meghatározott bejelentési kötelezettséget a jogalkotó azokban az esetekben írja elő, amelyekben a (2) bekezdésben szabályozott előzetes ellenőrzés lehetősége fennáll. A feldolgozás vagy a technológia alkalmazásának szándékát a tevékenység megkezdését megelőzően 30 nappal be kell jelenteni a biztosnak. Ez a bejelentés nem azonos az adatvédelmi nyilvántartásba történő bejelentési kötelezettséggel (28–30. §); a két bejelentési kötelezettség célja, tartalma, a bejelentési kötelezettség fennállásának feltételei, a vonatkozó határidők is mások. A 31. § (3) bekezdésben meghatározott bejelentési kötelezettség olyan esetekben is fennállhat, amelyeket az Avtv. 30. §-a alapján nem kell bejelenteni az adatvédelmi nyilvántartásba [a 31. § (2) bekezdés szerinti, az adatkezelővel ügyfélkapcsolatban álló személyek személyes adatait tartalmazó adatkezelés stb.].

9. Értelmezési kérdésként merülhet fel, hogy az ellenőrzést a biztos a bejelentéstől, vagy az adatkezelő számára történő jelzéstől számított 30 napon belül köteles elvégezni; mivel a rendelkezés a tevékenység (szándékolt) megkezdését megelőzően 30 nappal kötelezi az adatkezelőt a bejelentés megtételére, ezért az ellenőrzés elvégzésének határnapját a bejelentéstől kell számítani. Sajnos a törvény ebben az esetben is igen nagyvonalúan szabályozza az eljárási kérdéseket, így nem szól arról a kérdésről, hogy mely aktus tekinthető az előzetes ellenőrzés befejezésének.

10. A 31. § (4) bekezdése szerint „az ellenőrzés alapján az adatvédelmi biztos a kezelendő adatok körének, illetőleg az adatfeldolgozás módszerének megváltoztatására hívhatja fel az adatkezelőt. Ha az adatvédelmi biztos az adatkezelést elrendelő jogszabályt kifogásolja, ajánlást tehet a jogszabály módosítására."

A (4) bekezdés a 31. § (1) és (2) bekezdésében szabályozott előzetes ellenőrzés vonatkozásában határozza meg a biztos által az ellenőrzés alapján végezhető cselekményeket. Az (1) bekezdés alapján történő előzetes ellenőrzés esetén az ellenőrzés elvégzése nem hátráltatja az adatkezelés megkezdését; kérdés azonban, hogy miképp kell eljárnia az adatkezelőnek, ha az adatvédelmi biztos a (2) bekezdésben meghatározott előzetes ellenőrzés lefolytatását követően felhívja az adatkör, illetőleg az adatfeldolgozás módszerének megváltoztatására.

Álláspontunk szerint ilyen felszólításnak csak abban az esetben lehet helye, ha az adatkezelés jogszerűtlen. Kérdés azonban, hogy a felszólítás ellenére az adatkezelő megkezdheti-e az adatkezelést vagy sem – ez attól függ, hogy mely cselekménnyel „fejeződik be" az adatkezelés a (3) bekezdés alkalmazásában. Ha az ellenőrzés külön aktussal, vagy a felhívás közlésével „befejeződik", akkor az adatkezelés a (3) bekezdés alapján akkor is megkezdhető, ha az adatvédelmi biztos az adatkör vagy a módszer megváltoztatására hívta fel az adatkezelőt. Lehetséges lenne, hogy a jogalkotó az ellenőrzési eljárás keretében szabályozza az adatkör/adatfeldolgozási módszer módosítására, annak jóváhagyására vonatkozó eljárást is: ennek hiányában azonban álláspontunk szerint „befejeződik" az eljárás a felhívás közlésével.

Külön szabályozás híján a felhívás álláspontunk szerint a 25. § (2) bekezdés szerinti felszólításnak minősül, és annak nem teljesítése a 25. § (3) bekezdésében foglalt szankciókat vonhatja maga után, az ott meghatározott feltételek szerint.

11. Az adatvédelmi biztos ajánlást tehet az adatkezelést elrendelő jogszabály módosítására is. Ez a szabályozási megoldás azzal az eredménnyel jár, hogy a biztos által kifogásolt adatkezelés jogszabályi elrendelés esetén is megkezdhető; a biztos 31. § (4)

bekezdésében foglalt jogköre nem tér el a 25. § (1) bekezdésben biztosított általános, jogszabály módosítására irányuló javaslattételi jogkörtől.

1.19.6. A belső adatvédelmi felelős és az adatvédelmi szabályzat

1. Az Avtv. 31/A. § (1) bekezdése szerint „az adatkezelő, illetőleg az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó – jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező – belső adatvédelmi felelőst kell kinevezni vagy megbízni:

a) az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőnél és adatfeldolgozónál;

b) a pénzügyi szervezetnél;

c) a távközlési és közüzemi szolgáltatónál."

A belső adatvédelmi felelős intézménye a 2003. évi Avtv.-novella nyomán jelent meg a törvényben.

2. A belső adatvédelmi felelőst a jogalkotói szándék szerint „ugyanazoknál a nagy adatállományokat kezelő szervezeteknél" kell előírni, mint amely esetén a törvény az előzetes ellenőrzés lehetőségének ad teret. Ennek megfelelően az országos hatósági, munkaügyi vagy bűnügyi adatállomány, a pénzügyi szervezet, a távközlési és közüzemi szolgáltató fogalmáról lásd a 31. § (2) bekezdéséhez fűzött magyarázatot.

3. Az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetőleg feldolgozó adatkezelőnél és adatfeldolgozónál a jogalkotó egyértelmű szabályozást ad: az adatvédelmi felelőst ki kell neveznie azon szervezetnek is, amely csak adatfeldolgozóként működik. Arra tekintettel, hogy a szabályozás során a jogalkotó az előzetes ellenőrzéshez hasonlóan kívánta meghatározni a kötelezetti kört, valamint a 31/A. § (1) bekezdésének *a)* pontjában kifejezetten utal az adatfeldolgozóra, míg *b)* és *c)* pontjában nem, a *b)* és *c)* pontban meghatározott esetben nézetünk szerint csak az adatkezelő köteles adatvédelmi felelős kinevezésére. E tekintetben a jogalkalmazói gyakorlat egyelőre nem ismert.

4. Az adatvédelmi biztos szerint: „A belső adatvédelmi felelős álláspontom szerint megbízási szerződés keretében is elláthatja feladatát, nem szükséges, hogy az adatkezelővel munkaviszonyban álljon. Az adatvédelmi felelősi tisztség ellátása mellett az adott szervezetben más munkakört is betölthet."[629]

[629] 1245/x/2003–3. sz. ügyirat, publikálva a http://www.adatvedelem.vilaga.hu oldalon.

5. A belső adatvédelmi felelős kötelezettségeiről a (2) bekezdés rendelkezik, amely szerint a felelős

„*a)* közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

c) kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;

e) vezeti a belső adatvédelmi nyilvántartást;

f) gondoskodik az adatvédelmi ismeretek oktatásáról."

A belső adatvédelmi felelős feladatait felsoroló (2) bekezdéssel kapcsolatban jelenik meg a törvényben a „belső adatvédelmi nyilvántartás" fogalma [*e)* pont]. Ezzel kapcsolatban felmerül az a kérdés, hogy vajon a belső adatvédelmi nyilvántartás megegyezik-e az adattovábbítási nyilvántartással [amelyet az adatkezelőnek a 12. § (1) bekezdése alapján kell vezetnie], vagy az adatvédelmi felelősnek ezen túl kell önálló belső adatvédelmi nyilvántartást vezetnie. A jogalkotó mindenesetre nem ad támpontot az esetleges önálló adatvédelmi nyilvántartás kötelező tartalmával kapcsolatban. [Ilyen nyilvántartás vezetése álláspontunk szerint abban az esetben is célszerű, ha annak kötelezettsége nem vezethető le a 31/A. § (2) bekezdéséből: az adatvédelmi felelős csak abban az esetben képes áttekinteni a szervezet adatkezelését, ha naprakész listával rendelkezik a szervezet által folytatott – nem csak a bejelentésköteles! – adatkezelésekről, azok legfontosabb adatairól.]

6. A 31/A § (3) bekezdése szerint „az (1) bekezdésben meghatározott adatkezelőknek, valamint – az adatvédelmi nyilvántartásba bejelentési kötelezettség alá nem eső adatkezelők kivételével – egyéb állami és önkormányzati adatkezelőknek, e törvény végrehajtása érdekében, adatvédelmi és adatbiztonsági szabályzatot kell készíteniük." A törvény az (1) bekezdésben meghatározott adatkezelők számára minden esetben, míg az állami és önkormányzati adatkezelőknek csak abban az esetben írja elő adatvédelmi és adatbiztonsági szabályzat készítésének kötelezettségét, ha azok rendelkeznek olyan adatkezeléssel, amely nem esik a 30. §-ban meghatározott, az adatvédelmi nyilvántartásba való bejelentkezés alóli kivételi körbe.

Az adatvédelmi és adatbiztonsági szabályzat fordulat ellenére álláspontunk szerint lehetséges e két terület külön történő szabályozása [sőt, adott esetben ez a nem személyes

adatnak minősülő egyes adatok (minősített adatok, üzleti titkok) kezelésének sajátosságai miatt elkerülhetetlen].[630]

Az adatvédelmi biztos konzultációs beadványra adott válasza szerint: „Az adatvédelmi szabályzat egy belső, az adatkezelő szervezetén belül kötelező erejű norma, amely az adatkezelés részleteit határozza meg, és elősegíti a jogszabályok rendelkezéseinek végrehajtását, valamint az érintettek jogainak érvényesítését. Az adatvédelmi és adatbiztonsági szabályzat célja

– a törvény általános rendelkezéseinek egyéniesítése,

– hozzáférési jogok meghatározása,

– ellenőrzési mechanizmusok meghatározása,

– felelősségi viszonyok tisztázása,

– az egyes adatkezelési műveletek részletezése (például törlési határidők).”

[630] Kiindulásként alkalmazható – bár a hatályos jogi környezethez illesztendő – mintaszabályozatot közöl például Dietz–Hanzmann 1999.

1. A technológia mint a magánszféra-védelem új eszköze és mint a szabályozás tárgya

1.20. A polgári célú rejtjelzés szabályozása

1.20.1. A nyilvános kulcsú titkosítás

1. A jogi védelem hatékonyságának csökkenésével együtt új, hatékony technológiák kerültek előtérbe – ezek alkalmazásával a magánszféra-védelem hatékonyabban érvényesíthető, ám egyes esetekben sérülnek hagyományos egyensúlyhelyzetek (például a bűnüldözés érdeke és a magánszféra védelme között). Ilyen esetekben a jogalkotónak be kell avatkoznia az egyensúly helyreállítása érdekében. Ilyen új, magánszféra-védelemre is alkalmazható technológia (de a fent hivatkozott meghatározás szerint nem magánszféravédő technológia) a nyilvános kulcsú rejtjelzés.

2. A titkosítóalgoritmusok fejlesztésével, a rejtjelzés tökélyre vitelével sokáig kizárólag a kormányok alkalmazásában álló matematikusok foglalkoztak, azonban az 1970-es évektől már felmerült a rejtjelzés polgári célú használatának igénye. A banki szektor által használt számítógéprendszereken folytatott kommunikáció biztosítására 1971-től folytak kutatások az IBM-nél: bár az eredmények publikálását a National Security Agency kezdetben rossz szemmel nézte, végül e kutatások eredményeképp jöhetett létre a szimmetrikus rejtjelzés szabványos algoritmusa, a DES. A szimmetrikus rejtjelzés lényege azonban az, hogy a küldő és a fogadó fél ugyanazt a kulcsot használja: a kulcs eljuttatása a másik félhez pedig problematikus – ez a módszer tehát még nem alkalmas arra, hogy egy számítógép-hálózat nagyszámú, egymást nem ismerő felhasználója, előzetes kulcscsere nélkül, biztonságosan kommunikálhasson. Erre a problémára keresett és talált megoldást Diffie és Hellmann: 1976-ban írták meg első cikküket a nyilvános kulcsú titkosításról, Rivest, Shamir és Adleman pedig nem sokkal ezután egy működőképes, nyilvános kulcsú titkosítást megvalósító eljárással állt elő.[631] Ezzel megszületett a nyilvános kulcsú infrastruktúra, amelyben egymást nem ismerő

[631] A nyilvános kulcsú titkosítás feltalálásának és az azzal kapcsolatos politikai vitáknak a történetéről lásd Levy 2001. Érdekesség, hogy a nyilvános kulcsú titkosítás valódi feltalálója nem Diffie és Hellmann, hanem James Ellis, a General Communication Headquarters elnevezésű brit nemzetbiztonsági szolgálat alkalmazásában álló matematikus volt, aki már 1969-ban megalkotta a modellt. A kriptográfia technológiájáról és a szabályozásával kapcsolatos jogi kérdésekről tudományos igénnyel ír Koops 1999.

felek is képesek a másik személyazonosságáról meggyőződni, ha az digitális aláírást használ, valamint képesek előzetes kulccsere nélkül is a másik fél számára titkosított üzenetet küldeni.

3. A felhasználó a nyilvános kulcsú rendszerben két kulcsot használ: egy nyilvánosat, és egy titkosat. A nyilvános kulcsot közzéteszi, míg a titkos kulcsot rajta kívül senki nem ismerheti meg. Elektronikus aláírás generálásakor a felhasználó az üzenetet (vagyis annak egy meghatározott módon képzett lenyomatát) titkos kulcsával aláírja, a címzett pedig a küldő nyilvános kulcsa segítségével ellenőrizheti, hogy az üzenet nem változott, s azt valóban a küldőként megjelölt személy írta alá. Rejtjelzésnél a folyamat fordított: az üzenetet a küldő a címzett nyilvános kulcsával titkosítja, majd ezután azt kizárólag a címzett képes visszafejteni saját titkos kulcsával.[632] A nyilvános kulcsú rejtjelzés igen hatékony, s – RSA algoritmus használata esetén – megfelelő hosszúságú kód használata esetén az üzenet megfejtésére a jelenleg rendelkezésre álló számítógépes kapacitás mellett nincs mód addig, ameddig nem ismeretes a prímtényezőkre bontást megkönnyítő matematikai eljárás.

A titkosítótechnológiák tehát lehetővé teszik az osztott információs rendszerek doktrínájának „átmentését" az elektronikus közigazgatás keretei közé. Azonban nem szabad megfeledkezni arról sem, hogy a titkosítótechnológiák alkalmazása maga is további jogi és szabályozási kérdésekhez vezet el. *E kérdések legfontosabbika álláspontunk szerint a titkosítást lehetővé kulcsokhoz történő hozzáférés szabályozásának kérdése.*

A titkosítótechnológiák használatának ösztönzése egyfelől alapvető fontosságú az elektronikus közigazgatás fejlesztéséhez szükséges bizalom megteremtéséhez, a személyes adatok védelmének e környezetben történő érvényesüléséhez, s ebből a megfontolásból az államnak azt ösztönöznie kell. Más oldalról a titkosítótechnológiák elterjedése veszélyeztetheti a titkos információgyűjtést. Ezen eszközök elterjedése folytán veszélybe kerülhet az az egyensúly, amely hagyományosan fennáll egyrészt a magánszféra védelméhez, másrészt a bűnüldözéshez, nemzetbiztonsághoz fűződő érdek között a hagyományos kommunikációs csatornák esetén. Az új rejtjelzőtechnológiák használata mellett ugyanis még az állam rendelkezésére álló erőforrásokkal is lehetetlennek bizonyulhat a titkos információgyűjtés.

4. Ezt a problémát láthatóan érzékelte a magyar jogalkotó is. Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eatv.) 13. § (4) bekezdése szerint „az aláíró az aláírás-

létrehozó adatot kizárólag az aláírás létrehozására használhatja, betartva a tanúsítványban jelzett esetleges egyéb korlátozásokat is". A törvényhez kapcsolódó részletes miniszteri indokolásnak e szakaszhoz kapcsolódó szövege szerint „a (4) bekezdés nemzetbiztonsági érdekből nem teszi lehetővé az aláírás-létrehozó adatnak [magánkulcsnak] titkosítás céljából történő használatát". A jogalkotó tehát az Eatv.-ben szabályozott elektronikus aláírás titkosítási célú használatát megtiltotta. (A szabályozás több szempontból sem szerencsés: a nyilvános kulcsú infrastruktúrában a nyilvános kulcsot – vagyis az Eatv. fogalomrendszere szerint „aláírás-ellenőrző adatot" – használják titkosításra; ráadásul az Eatv. hivatkozott rendelkezése csak az Eatv. fogalomrendszere szerinti aláírás-létrehozó adat, tehát elektronikus aláírás céljára képzett kulcs titkosításra történő használatát tiltja, egyéb kulcsét nem.)[633]

1.20.2. A nyilvános kulcsú titkosítás szabadsága és a bűnüldözéshez fűződő érdek konfliktusa

1. Miben is áll pontosan a nyilvános kulcsú rejtjelzés veszélye a bűnüldözéshez, nemzetbiztonsághoz fűződő érdekre? A nyilvános kulcsú rejtjelzést felhasználóbarát módon megvalósító, bárki által egyszerűen kezelhető szoftver- és hardvereszközök kifejlesztése és az interneten való közzététele – e szoftverek közül az első és legismertebb a Phil Zimmermann által írt, ingyenesen elérhető Pretty Good Privacy (PGP)[634] – a magánszféra és az üzleti titkok védelmének lehetőségét bármely digitális technológiát használó kommunikációs eszköz használatakor lehetővé tette. A veszélyekre rámutatnak az Egyesült Államokban fellépő egyes – magukat kriptoanarchistáknak nevező – ideológusok gondolatai. Tim May, a kriptoanarchisták képviselője így ír:

„Ahogy a nyomtatás megváltoztatta és csökkentette a középkori céhek hatalmát és a társadalom hatalmi rendszerét, úgy fogják alapjaiban megváltoztatni a titkosítóalgoritmusok a kormányok és a tőkés társaságok befolyását az üzleti tranzakciókra. A kialakuló információpiacok és a kriptoanarchia együttesen virágzó piacot teremt majd minden árunak,

---

[632] Valójában a – számítógépek által lassabban végrehajtott – nyilvános kulcsú rejtjelzési eljárást általában csak arra használják, hogy egy kulcsot titkosítsanak; a kulcs átvitele után maga az üzenet dekódolása és visszafejtése már az átküldött – kódolásra és visszafejtésre egyaránt alkalmazott – kulccsal történik.

[633] A szabályozás valójában informatikai okokkal magyarázható; az indokolásból kiolvasható jogalkotói szándékot azonban ez nem minősíti.

[634] A PGP megalkotásáról lásd Levy 1999, 188. skk.

amely szavak és képek formájában megjelenhet."[635]

Ugyancsak Tim May postázta – névtelenül – az internetre a BlackNet nevű szervezet képzeletbeli felhívását. A BlackNet identitása csupán egy, az interneten elérhető nyilvános kulcs, amelynek segítségével titkosított üzenetet küldhetünk számára. S hogy mivel foglalkozik ez a hálózat?

„A BlackNet tetszőleges formájú információ vásárlásával, eladásával és kereskedelmével foglalkozik. Az információt nyilvános kulcsú kriptográfiai rendszer segítségével adjuk és vesszük, amely vásárlóinknak tökéletes biztonságot biztosít. Ha nem mondja meg nekünk, hogy Ön ki (kérjük, ne tegye!), és véletlenül sem árul el magáról olyasmit, ami elvezethet Önhöz, nekünk nem áll módunkban azonosítani Önt, és Ön sem tud azonosítani minket. Fizikai-térbeli pozíciónk nem fontos. Csak a cybertérben elfoglalt helyünk számít. Elsődleges címünk a »BlackNet« PGP-kulcsos cím. […] A BlackNet névleg ideológiamentes, de a nemzetállamokat, exportjogszabályokat, szabadalmi törvényeket és a nemzetbiztonsági szempontokat a cybertér előtti korszak relikviáinak tartjuk. Az export- és szabadalmi törvényeket gyakran használják bevallottan a nemzeti hatalom és az imperialista, kolonialista államfasizmus érdekében."[636]

A kiáltvány folytatásában a szervezet közli, hogy mi érdekli – üzleti titkok, találmányok, bármely értékes információ –, majd leírja a fizetés menetét. A képzeletbeli szervezet még belső fizetőeszközzel is rendelkezik, az anonimitás az üzleti tranzakciók során végig biztosított – s a rendszer bármire használható, legyen az jogszerű vagy jogszerűtlen. A May által leírt rendszer persze – bár sokan komolyan vették – nem létezett. Hamar elterjedtek azonban az ún. „anonim remailerek": ezek olyan szerverek, amelyeken keresztül a felhasználó úgy küldhet és kaphat üzenetet, hogy személyazonossága ismeretlen marad a fogadó fél előtt. Egy több remaileren keresztül küldött levél feladója nehezen azonosítható, ha minden szerver más országban van.

2. A kriptoanarchisták elméleteiben felvázolt forradalmi elképzeléseknél jóval nagyobb – és valós – veszélyt jelent a titkosítás bűnözői körök által történő felhasználása. Ezen eszközök használatával a bűnözők megakadályozhatják kommunikációjuk lehallgatását olyan esetben, amikor „hagyományos" kommunikációs csatornánál erre lehetőség van, vagy azt, hogy a hatóságok digitális formában tárolt, bűncselekmény bizonyítására alkalmas vagy azzal kapcsolatos információk forrásához eljussanak.

---

[635] Tim May: Crypto Anarchist Manifesto, idézi Levy 2001, 210

[636] Tim May: Bemutatkozik a Blacknet („holist" fordítása).

Példaként álljanak itt a következők: Aldrich Ames, CIA-alkalmazott, aki az USA ellen kémkedett, titkosítva tartotta anyagait a személyi számítógépén.[637] Az tokiói metró ellen ideggáztámadást végrehajtó Aum Shinri Kyo-szekta tagjai olyan számítógépes állományokat titkosítottak, amelyek egyesült államokbeli merényletek terveit tartalmazták.[638] Ramszi Yousef – annak a nemzetközi terroristacsoportnak a tagja, amely felelős a World Trade Center elleni 1993-as bombamerényletért – laptopján olyan titkosított állományokat tartott, amelyek Távol-Keleten amerikai utasszállító gépek ellen intézendő merényletek terveit tartalmazták.[639] Az 1998-ban az Egyesült Államok kenyai és tanzániai nagykövetségei ellen elkövetett robbantásos merényletek után napvilágot látott, hogy a CIA 1997-ben három másik robbantást akadályozott meg elektronikus eszközökkel végzett lehallgatás segítségével.[640] Amitai Etzioni szerint a holland szervezett bűnözésnek létezik külön „információshadviselés-osztaga". A bűnözők a bűnüldözőkkel szemben titkosító eszközök alkalmazásával védekeznek, és egy csoport informatikában jártas személy segíti őket, akik maguk PGP és PGPfone titkosító eszközök segítségével rejtjelzik kommunikációjukat. Egy esetben ezek a személyek olyan palmtopokkal látták el a bűnözőket, amelyre installálták a Secure Device-ot, egy olyan holland szoftverterméket, amely az adatokat az IDEA algoritmus segítségével 128 bites erősséggel titkosítja: a palmtopokon a nyomozó hatóságok által használt járművek nyilvántartása volt megtalálható.[641] 1995-ben az amszterdami rendőrség a szervezett bűnözés egy tagjánál PC-t foglalt le, amelyen egy olyan partíció is volt, amelyet abban az időben nem tudtak helyreállítani.[642] Koops szerint azonban a bizonyítékok így is elégségesek voltak, s a később visszafejtett, a rejtjelzett partíción tárolt adatoknak az ügy szempontjából nem volt különösebb jelentősége.[643]

[637] Etzioni 1999, 78.

[638] Dorothy E. Denning–William E. Baugh, Jr.: Encryption and Evolving Technologies. In Alan D. Campen – Douglas H. Dearth (eds.): *Cyberwar 2.0* (AFCEA International Press, June 1998). Idézi Etzioni1999, 78.

[639] House of Representatives, Committee on International Relations, Hearings on Encryption, Louis J. Freeh FBI igazgató tanúvallomása, 1997. június 26. Idézi Etzioni 1999, 78.

[640] Walter Pincus – Vernon Loeb: CIA Blocked Two Attacks Last Year"., *Washington Post,* 1998. augusztus 11. idézi Etzioni 1999, 78.

[641] Dorothy E. Denning–William E. Baugh, Jr.: Encryption in Crime and Terrorism. In Alan D. Campen – Douglas H. Dearth (eds.): *Cyberwar 2.0* (AFCEA International Press, June 1998). Idézi Etzioni1999, 78.

[642] Etzioni 1999, 78.

[643] Koops 1999, 65.

1.20.3. Egy megoldási javaslat és bukása: a kulcsletét

1. A „kriptoanarchia” lehetőségét értékelve az amerikai kormányzat igen gyorsan lépett: a National Security Agency bábáskodásával kifejlesztett Clipper chip olyan hardvereszköz volt, amely számítógépekbe, telefonokba építve erős titkosítást valósított meg, ám biztosította a bűnüldöző és nemzetbiztonsági szervek hozzáférési lehetőségét is: minden egyes kulcshoz tartozott a visszafejtést lehetővé tevő kulcs is, amelyet a chip gyártója két részre osztott, s a két rész két kormányzati szervhez került „letétbe”. A nemzetbiztonsági és bűnüldöző szervek szükség esetén a megfelelő engedélyek birtokában a két szervtől beszerezhették volna a két kulcsrészt, majd az azokból összeillesztett kulcs segítségével visszafejthették volna az üzenetet.[644] Ez az ún. „kulcsletét” rendszere.[645] Az elképzelés tetszetős,[646] hiszen kellő garanciák mellett biztosítja a bűnüldözők számára a hagyományos kommunikációs csatornák esetén megszokott eszközök használatát – a Clipper chip mégis csúfos bukásnak bizonyult. A Clinton-kormányzat által 1993 tavaszán tett bejelentés után, amely szerint támogatják a kulcsletét – önkéntesen igénybe vehető – rendszerét (nagy összegű kormányzati megrendeléseket is kaptak a chippel felszerelt eszközök gyártói), az emberi jogi szervezetek és az informatikai ipar lobbistái össztüzet zúdítottak a programra.

2. Az ellenérvek számosak: a kulcsletét technológiai megvalósítása fenyegeti a titkosítás biztonságát (a Clipper chip megvalósításában nem sokkal a program meghirdetése után biztonsági hibát találtak), az eszközzel felszerelt berendezések nem lennének exportálhatók, mert a külföldi piac nem fogadná el a kizárólag az amerikai szervek számára nyitva álló „hátsó kaput”. A kulcsletéti rendszer üzemeltetése természetesen nagy költségekkel járna. A legnagyobb probléma azonban, hogy a titkosított üzenetforgalom ellenőrzése a kulcsletét mellett sem megoldható: a kulcsok beszerzésével visszafejtett üzenet talán egy további, rejtjelzett üzenetet takar; de az is lehetséges, hogy a kódolt üzenet maga is el van rejtve valamely kép- vagy hangfájl meghatározott szabályok szerint módosított bitjeibe. A rendszer tehát feleslegesen gyengítené a biztonságot – szóltak az ellenérvek. Az amerikai kormányzat a javasolt rendszer módosításával kísérletezett: a későbbi tervek szerint kormányzati szervek helyett magáncégek is lehettek volna a kulcsokat őrző „letéteményesek” – ám a kulcsletét rendszerén alapuló infrastruktúra megteremtése a kilencvenes évek végére – miután az USA

[644] A Clipper-chip fejlesztésének történetéről és a körülötte zajló politikai vitákról lásd Levy 2001, 127. skk.

[645] E helyt nem különböztetjük meg a „key escrow”- és „key recovery”-rendszereket.

[646] A kulcsletét rendszerét jó nevű független szakértők is támogatták, például a Georgetown University professzora, Dorothy Denning. Lásd Denning 1997.

sikertelenül próbálta meggyőzni európai szövetségeseit egy nemzetközi kulcsletéti rendszer szükségességéről[647] – lekerült a napirendről.

3. Európában szintén felmerült az amerikaihoz hasonló rendszer megteremtése, azonban az Európai Bizottság 1997-es, A digitális aláírás és a titkosítás európai kereteinek megteremtéséről" szóló közleménye[648] óta nem merült fel uniós szinten olyan kezdeményezés, amely a kriptográfia használatának korlátozására irányult volna. A tagállamokban is a titkosítás belső használatának mellőzése a tendencia: a német kormány által 1999-ben elfogadott kriptográfiai politika szerint az erős titkosítás használatát kifejezetten ösztönözni kell; Franciaország 1999-ben oldotta fel a korábbi jogszabályi korlátozásokat a titkosítás használatát illetően. Nagy-Britannia szabályozása sem ismeri a kulcsletét rendszerét, azonban a 2000-ben elfogadott Regulation of Investigatory Powers Act szerint az a személy, akinek valamely titkosító kulcs a birtokában van, meghatározott feltételek szerint kötelezhető annak kiadására.[649]

4. Magyarországon 2001 februárjában az adatvédelmi biztos az internettel kapcsolatos adatvédelmi kérdésekkel foglalkozó ajánlást bocsátott ki.[650] Az ajánlásban az ombudsman kifejezte azt a véleményét, hogy „a nemzetközi példák nyomán arra az álláspontra jutottam, hogy a polgári célú kriptográfia jogszerű használatának korlátozása káros, a bűnüldözés hatékonysága szempontjából előnyei kétségesek, viszont a személyes adatok védelme szempontjából hátrányai kétségtelenek". Az ajánlás különösebb visszhangot nem keltett, ám az elektronikus aláírásról szóló törvény fent idézett szakasza válaszképp is értékelhető: a kormányzat nem osztja Majtényi álláspontját. A szándék kifejezésén túl az elektronikus aláírásról szóló törvény 13. § (4) bekezdésének szövege másra nem alkalmas: értelmetlen ugyanis a feladó magánkulcsával történő titkosítást megtiltani a nyilvános kulcsú infrastruktúrában, amely esetén a titkosítás a címzett nyilvános kulcsával történik. Csak remélhető, hogy mire a jogszabály-előkészítők a kormányzati szándékot megfelelőbb formába

---

[647] Az USA a végleges vereséget a fegyverek és kettős használatú termékek (polgári és katonai célokra is használható termékek; ilyennek minősülnek a titkosítóeszközök is) exportjának ellenőrzésével kapcsolatos nemzetközi fórum, a Wassenaari Együttműködés 1998-as ülésén szenvedte el: lásd a német Gazdasági Minisztérium közleményét a http://www.kuner.com/data/crypto/wassenaar.html oldalon.

[648] COM 97 (503)

[649] A titkosítás szabályozásának fejleményeiről lásd Bert-Jaap Koops fél évente frissített, a Föld szinte minden országáról információkat közlő felmérését a http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm oldalon; az Electronic Privacy Information Center 2000-ben készített felmérését lásd http://www2.epic.org/reports/crypto2000.

[650] ABI 2002, 185

öntik, a személyes adatok védelmét, a hazai e-kereskedelem és információs társadalom fejlődését zászlajukra tűző jogvédők és érdek-képviseleti szervezetek is megfogalmazzák majd álláspontjukat: a 13. § (4) bekezdéséről ugyanis sem az Országgyűlésben, sem azon kívül nem esett szó az elektronikus aláírásról szóló törvény vitája során.

5. 2001 végén Budapesten tartották az Európa Tanács égisze alatt született számítástechnikai bűnözésről szóló egyezmény aláíró ünnepségét.[651] Az egyezmény 18. cikke szól a „közlésre kötelezés" szabályozásáról: a szerződő felek ennek értelmében „megteszik azokat a jogalkotási és egyéb intézkedéseket, amelyek ahhoz szükségesek, hogy feljogosítsa az illetékes hatóságait, hogy kötelezhessék a területén tartózkodó személyt a birtokában vagy az ellenőrzése alatt lévő és egy számítástechnikai rendszerben vagy egy számítástechnikai adattároló-egységen tárolt meghatározott számítástechnikai adatok közlésére és a területén szolgáltatást nyújtó szolgáltatót a birtokában vagy az ellenőrzése alatt lévő, az előfizetőre vonatkozó és a szolgáltatást érintő adatok közlésére". Az egyezményhez fűzött magyarázat (Explanatory Memorandum) 176. pontja alapján a szerződő felek meghatározhatják, hogy az információt a kötelezett valamely, a közlésre kötelezést elrendelő határozatban meghatározott módon – vagyis, mint maga a magyarázat is utal rá, akár titkosítatlan formában – köteles szolgáltatni. Bár az egyezmény nem ír elő kulcsletét megvalósítására való kötelezettséget a tagállamoknak, az előkészítés szakaszában az ötlet felmerült,[652] s nem lehetetlen, hogy a szeptember 11-i események nyomán megváltozott hangulatban újra előtérbe kerül a kulcsletét mint lehetséges megoldás, akár Magyarországon is.[653]

1.21. Magánszféravédő technológiák

1.21.1. A magánszféravédő technológia fogalma

1. A magánszféravédő technológiák (PET) fejlesztésének elsődleges célja nem az adattartalomtól független adatbiztonság megteremtése, hanem kifejezetten a magánszféra-védelem. Míg az adatbiztonságot szolgáló technológiák jogi szabályozása is befolyásolhatja a magánszféra-védelem szintjét, a PET-ek közvetlenül a szűkebb értelemben vett adatvédelmi

[651] Az egyezmény szövege magyarul: http://www.stopcybercrime.net/2_2.php; a hozzá kapcsolódó Expanatory Memorandum szövege angolul: http://conventions.coe.int/Treaty/EN/cadreprojets.htm.

[652] Lásd Bert-Jaap Koops összefoglalóját: http://cwis.kub.nl/~frw/people/koops/cls2.htm#coe.

[653] A World Trade Center épületében röviddel azelőtt elkövetett merényletek Levy beszámolója szerint hozzájárultak ahhoz, hogy a Clinton-adminisztráció a nemzetbiztonsági szolgálatok mellé állt a 1993-ban a Clipper-chippel kapcsolatban: lásd Levy 2001, 244.

szabályozással is kölcsönhatásban állnak: e szabályozás ösztönözheti alkalmazásukat, és alkalmazásuk hatékonyabbá teheti az adatvédelmi jogot, biztosítva annak érvényesülését az új, digitalizált adatáramlással áthatott közegben. A magánszféravédő technológiák fejlesztésének igénye már az első adatvédelmi törvények elfogadása idején felvetődött az irodalomban, majd a harmadik generációs szabályozással kapcsolatos viták során vált kedvelt témává.[654]

2. Burkert tipológiája szerint a magánszféravédő technológiáknak négy csoportja különböztethető meg.[655] Alanyorientáltnak (subject-oriented) nevezi azokat a megoldásokat, amelyek elsődlegesen azt célozzák, hogy az adatalany és az adat kapcsolata minél nehezebben legyen helyreállítható (példája erre egy olyan hitelkártyarendszer, amely a tranzakciók során a hitelkártyaszámot használja, míg a használó neve és a kártyaszám közötti kapcsolat – a példa szerint nyilvános kulcsú titkosítással – kódolt, azt adott esetben csak a bank és az adatalany közösen képes helyreállítani). A tárgyorientált (object-oriented) megoldások arra építenek, hogy a tranzkció során kicserélt dolog ne hordozzon információt a részt vevő személyekről (ilyen eset hagyományos közegben például a készpénzes fizetés vagy a barterügylet). A tranzakcióorientált (transaction-oriented) megoldások a tranzakció során keletkező információkra fókuszálnak: ilyenek lehetnek például azok az eszközök, amelyek a tranzakcióra vonatkozó adatokat meghatározott idő eltelte után megsemmisítik. Végül az előbbi három elemeiből áll össze a negyedik, a rendszerorientált (system-oriented) megoldás, amely „olyan interakciós zónákat teremt, amelyekben az alanyok személyazonossága rejtett, amelyben a tárgyak nem hordozzák azok nyomát, akik megérintik őket, és amelyben a interakciót nem jegyzik fel, és ilyen feljegyzéseket nem őriznek”.[656] Hagyományos közegben Burkert példája a gyónás katolikus intézménye vagy a krízisintervencióval foglalkozó szervezetek által nyújtott anonim segélyszolgálatok; elektronikus közegben pedig a titkosított elektronikus levélben folytatott kommunikáció, amely után annak nyomait a résztvevők megsemmisítik.[657]

1.21.2. Egy példa: a P3P

[654] Burkert 1997, 137.

[655] Burkert 1997, 125. skk.

[656] Burkert 1997, 127.

[657] Ha erre képesek, ez a jelenlegi technológia alkalmazása mellett valószínűtlen.

1. A P3P-t mi a magánszféravédő technológia példájaként, egyes szerzők az ipari önszabályozás körében tárgyalják.[658] Álláspontunk szerint a technológia – bár fejlesztésekor szerepet játszott az állami szabályozás elhárítására irányuló törekvés egyes piaci szereplők részéről – semleges –; alkalmazása mind ipari önszabályozás, mint állami szabályozás keretében elképzelhető.

A több mint 400 tagot számláló – egyetemek, cégek, egyéb szervezetek közreműködésével működő – World Wide Consortium[659] (W3C) igen aktív az internet önszabályozási lehetőségeit támogató technológiák fejlesztésében. Az 1996-os, az internetes tartalmat szabályozni kívánó amerikai törvény, a Communications Decency Act alkotmányellenességének a Legfelsőbb Bíróság általi kimondását követően került reflektorfénybe a W3C által javasolt Platform for Internet Content Selection,[660] a PICS. Mivel a P3P sok tekintetben ezzel párhuzamos technológia, ezért röviden ismertetnünk kell a PICS legfontosabb vonásait.

2. A PICS olyan specifikációkészlet, amelynek segítségével a felhasználó által az internet eléréséhez használt, a sztenderdeknek megfelelő szoftverek képesek a felhasználó által meghatározott szempontok szerint szűrni a hálózaton elérhető anyagokat, és megakadályozni azok elérését, amelyeket a felhasználó a nemkívánatos kategóriába sorolt. Előzetesen el kell végezni a kérdéses tartalom minősítését. A minősítés bármilyen, eltérő szempontokat, illetve értékrendeket tükröző minősítési rendszer szerint történhet, s azt maga az adott állomány megalkotója, illetve harmadik fél (minősítőszolgálat, „label bureau") is elvégezheti; valamely tartalom számtalan különféle minősítőrendszer szerint sorolható be. A minősítés során az adott anyaghoz a tartalom szolgáltatója vagy a minősítőszolgálat hozzárendeli a meghatározott minősítési rendszer szerinti értékelést, „címkét". Ha a minősítést maga az állomány létrehozója végezte, a címke az adott állományba (például a web-oldal html-kódjába) kerül, minősítőszolgálat általi címkézés esetén a címke a minősítőrendszerén szerepel, de az adott állományhoz természetesen hozzárendelhető. A felhasználó által megfelelően beállított szoftver az adott állomány lekérésekor a kívánt minősítési rendszer szerint meghatározott címkét is ellenőrzi (vagy a kérdéses állományban, vagy a kiválasztott minősítőszolgálat nyilvántartásában), s ha a címke alapján az anyag nem felel meg a felhasználó előzetesen megadott kívánalmainak, akkor a hozzáférést nem engedélyezi. A PICS jelenleg www-oldalak, ftp, illetve gopher protokollokkal elérhető

[658] Lásd Schwartz 2002, 79. skk.

[659] http://www.w3.org.

állományok, Usenet hírcsoportok üzeneteinek a szűrésére alkalmas.

A PICS kialakítása során deklaráltan az volt a cél, hogy az egyfajta önszabályozás lehetőségének megteremtésével kiváltsa a Communications Decency Acthez hasonló állami szabályozási eszközöket. Ehhez sokban hozzájárult az internet korai története során oly sokak által osztott illúzió, amely szerint a hálózat „jogmentes tér", kívül esik az államok szuverenitásán. Meg kell említeni, hogy az önszabályozást illető eufória és a CDA alkotmányellenességének kimondása után az eljárást kezdeményező jogvédő szervek általi ünneplés elmúltával megjelentek olyan vélemények is, amelyek szerint az állami szabályozás éppenséggel több garanciát nyújt, mint a felhasználó által saját preferenciái alapján megvalósított önszabályozás eszközének szánt, ám az internetszolgáltatók vagy akár az államok által gyakorolt visszaélésszerű kontroll gyakorlására is alkalmas Platform for Internet Content Selection.[661] Valójában a PICS nemcsak az oldalak tartalma, hanem bármely jellemzője alapján alkalmas volt a minősítésre, címkézésre és szűrésre; a P3P közvetlen elődje volt. Egy amerikai egyetemi tanár, Joel Reidenberg – akire az európai adatvédelmi jog főbb elemeinek meghatározásával kapcsolatban tanulmányunk másik pontján hivatkozunk – a PICS segítségével minősített website-okat azon szempont szerint, hogy azok eleget tesznek-e a kanadai szabványügyi szervezet által meghatározott adatvédelmi szabványnak.[662]

3. A W3C által a felhasználó adatvédelmi preferenciáinak hatékonyabb érvényesülése érdekében kidolgozott Platform for Privacy Preferences (P3P) a PICS-hez nagyban hasonlító technológiai megoldásokat alkalmaz.[663] Az adott website meghatározott kritériumok szerint besorolja az általa követett adatvédelmi gyakorlatot. Ezt az információt meghatározott – a böngészőprogram által értelmezhető – formában (XML formátumban) kell elhelyezni a weboldal kódjában. Az oldalt meglátogató felhasználó mindennek alapján értesül arról, hogy 1. milyen adatokat gyűjt róla az oldal, 2. milyen célra használják ezeket az adatokat és 3. mely felhasználások tekintetében gyakorolhatja beleegyezési jogát akár pozitív beleegyezés (opt-in), akár a tiltakozás kifejezése (opt-out) útján. A felhasználó előzetesen beállíthatja adatvédelmi preferenciáit: megadhatja például, hogy nem kíván olyan oldalakat látogatni, amelyek cookie-kat használnak, meghatározott személyes adatának kiszolgáltatását követelik meg vagy az adatokat harmadik félnek továbbítják. A P3P specifikációja egészen összetett

---

[660] A CDA-val és a PICS-szel kapcsolatban lásd Jóri 1996; Jóri 1998; Polyák 2002.

[661] Lásd erről Lessig 1999..

[662] Lásd Cranor 2002. Cranor, Lorrie Faith 2002.

[663] Ismertetésünk alapja a PGP specifikációja: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, http://www.w3.org/p3p.

adatvédelmi szabályzatok megfogalmazását is lehetővé teszi: beállítható például, hogy az adott weboldallal kapcsolatos viták esetén mely jog az irányadó.

A P3P felhasználói oldalon telepíthető webböngészőbe és proxy-szerverre egyaránt. Szerveroldalon lehetőség van arra, hogy a website üzemeltetője számára egy szoftver az általa feltett kérdésekre adott válaszokból automatikusan generálja a válaszokból kiolvasható adatvédelmi szabályoknak megfelelő P3P-kódot, és ezt beillessze a weboldal kódjába.

A P3P már 2001 nyarától megtalálható az internet Exporer böngésző 5.0-ás verziójában, a 6.0-ás verzió pedig már arra is alkalmas, hogy a cookiek-kat a P3P rendszer segítségével meghatározott preferenciák szerint szűrje, és jelentést készítsen a weboldal által követett adatvédelmi szabályokról, ha az oldal P3P segítségével kódolt policyval rendelkezik.[664]

4. A P3P – a PICS-hez hasonlóan – nagy figyelmet keltett az Európai Unióban is. Előbb a Bizottság XV. Főbiztossága (DG XV) bocsátott ki egy állásfoglalást, amely a P3P kategória-rendszerének kiterjesztését javasolta. 1999 szeptemberében az EU adatvédelmi irányelvének 29. cikke alapján működő munkacsoport találkozott Brüsszelben a P3P fejlesztőivel. Ezt megelőzően a munkacsoport olyan állásfoglalást bocsátott ki, amely szerint a P3P önmagában nem elég ahhoz, hogy a web közegében érvényesüljenek az adatvédelmi normák.[665] Ez valóban így van: a P3P csupán egy technológia, amely eszköz lehet az adatvédelmi normák érvényesítéséhez. Használata azonban az európai adatvédelmi jogi környezetben – ahol az adott weboldal adatvédelmi politikája amúgy is csak a hatályos, szigorú adatvédelmi jogi rendelkezések keretei között érvényesülhet – mindenképp hasznos. Álláspontunk szerint a P3P kormányzati weboldalakon történő alkalmazása hozzájárulhat a felhasználók bizalmának megteremtéséhez, és ahhoz, hogy a kormányzati weboldalak által nyújtott tájékoztatást más weboldal-üzemeltetőktől is elvárják.

5. Schwartz szerint a P3P hatékonyságának gátja lehet az, hogy amerikai környezetben – ahol a weboldalak által követett általános („default") szabály az adatok maximális felhasználása – a szűrőrendszert alkalmazó felhasználó a web tartalmának nagy részétől elzárja magát.[666] Állami szabályozással támogatva azonban a megoldás alkalmas lehet a magánszféra-védelem érvényesítésére, ráadásul a felhasználó által pontosan meghatározott mértékben.

Tény azonban, hogy a szorosabb értelemben vett magánszféravédő technológiákról évtizedek óta olvashatunk az irodalomban anélkül, hogy alkalmazásba vételük széles körben

[664] Cranor 2002.

[665] Working Party Opinion 1/98: Platform for Privacy Preferences and the Open Profiling Standard.

megtörtént volna. „A PET-ek nem helyettesíthetik a közcélú szabályozást [public policy[667]]" az adatvédelem[668] terén, csak kiegészíthetik[669] azt. Érdekes Burkert gondolata, aki a magánszféravédő technológiák alkalmazásainak korlátait többek között abban látja, hogy abban a korban, amelyben az egyén hagyományos társadalmi kötelékei meglazulnak, igen erős a késztetés e kötelékek újrakötésére, fenntartására, és ez akár ahhoz is vezethet, hogy a névtelenség, amelyet az ilyen technológiák biztosítanak, elveszíti vonzerejét.[670]

Válaszkísérletek: ipari önszabályozás, szabványosítási törekvések, a CEN adatvédelmi audit keretrendszere

1.22. Ipari önszabályozás

1.22.1. A TRUSTe példája

1. Az EU adatvédelmi irányelve preambuluma szerint „a tagállamoknak és a Bizottságnak – illetékességi körükön belül – ösztönözniük kell az iparági szövetségeket és az érintett egyéb reprezentatív szervezeteket arra, hogy olyan magatartáskódexeket [codes of conduct] fogalmazzanak meg, amelyek – az irányelv végrehajtását célzó nemzeti jogszabályokat figyelembe véve – elősegítik ezen irányelv alkalmazását a meghatározott szektorokban végzett adatkezelések sajátosságaira tekintettel".[671] Az Egyesült Államokban az ipari önszabályozás elsősorban az állami szabályozás kivédésére irányul. Az alábbiakban az elektronikus adatkezelés közegével kapcsolatos példát ismertetünk: a TRUSTe-rendszert, amelynek célja, hogy weboldalak adatkezelésének megfelelőségét biztosítsa; megoldásai és korlátai is jellemzőek az ipari önszabályozási törekvések többségére. Ezután az adatvédelem területén kibontakozó szabványosítási törekvésekről szólunk.

2. A TRUSTe koncepciója mögött az áll, hogy annak megalkotói szerint sem a

---

[666] Schwartz 2002, 80.

[667] A „public policy" kifejezés Urbán László által javasolt fordítását használjuk (Urbán 1995).

[668] Bennett 1997, 177.

[669] Vö. Burkert 1997, 131: „A magánszféravédő technológiák nem mentesítenek bennünket attól, hogy a magánszférához és az átláthatósághoz fűződő érdek közötti egyensúlyt értéket hordozó döntéssel teremtsük meg."

[670] Ez a „mozgósítás" (mobilization). „A kormányzatok, az igazgatás, a politikai pártok, az egyházak, a vállalatok, a sarki fűszeres, a szomszéd pizzéria és a fodrász is állandóan mint egyént szólítja meg az embert, azért, hogy kapcsolatot alakítson ki vele (involve in a relationship) – mert ezek a kapcsolatok instabillá váltak és minden lehetséges alkalommal meg kell őket erősíteni." Burkert 1997, 135

[671] Consideration 61.

hagyományos iparági önszabályozás nem nyújthat hatékony megoldást (mivel nem jelent valós korlátokat az azt finanszírozó és működtető szféra számára), sem az állami szabályozás nem kívánatos az online adatvédelem terén (ez utóbbi oka, hogy a végrehajtás az adatvédelmi jog nemzetközi harmonizációja híján amúgy is szinte lehetetlen a globális internetes környezetben, s az állami beavatkozás veszélyeztetné az internet korábban tapasztalt robbanásszerű fejlődését). A problémára olyan megoldást kerestek, amely egyesíti „a kormányzati felügyelet súlyát, a piac dinamizmusának erejét, és épít a nyilvánosság által gyakorolt ellenőrzésre is". Ez a megoldás az „önkormányzás" (self-governance). A cél az elektronikus kommunikáció biztonságába vetett bizalom megerősítése, az adatvédelmi aggályok eloszlatása volt.[672]

A self-governance koncepció lényege, hogy az ipar nem önállóan cselekszik, hanem legjobb gyakorlatokat alakít ki, s támaszkodik az állami szabályozás eredményére – a jogszabályokra – is. A szabályozás egyik fő ösztönzője e koncepció szerint egy olyan „jól informált piac", amelynek szereplői eldöntik, számukra a személyes adatok felhasználásának mely szabályrendszere felel meg. A kormányzat feladata pedig a koncepció szerint az, hogy érvényt szerezzen a hatályos jognak, és arra ösztönözze az iparági szereplőket, hogy azok minél szélesebb körben adaptálják a legjobb gyakorlatokat.

Az „önkormányzás" elvét követi a TRUSTe-program is, amelynek célja, hogy az interneten megjelenő website-ok adatvédelmi politikája iránt teremtse meg a bizalmat azokban, akik ezen oldalak valamely szolgáltatását igénybe veszik. A program független mind az iparági szereplőktől, mind a kormányzattól, s azt a Kaliforniában nonprofit szervezetként bejegyzett Trusted Universal Standards in Electronic Transactions, Inc. működteti. Azok az oldalak, amelyek megfelelnek a TRUSTe által támasztott, adatvédelmi politikájukat illető feltételeknek, valamint alávetik magukat a TRUSTe vitarendezési mechanizmusának, egy ezt tanúsító logót (seal) tüntethetnek fel. (Ez a logó a magyar védjegyjog intézményei közül az ún. tanúsító védjegynek feleltethető meg, a TRUSTe üzemeltetője által a honlapfenntartókkal kötött szerződés szerint az „registered certification mark".)

A logót látva a felhasználó biztos lehet abban, hogy az adatvédelem meghatározott feltételei érvényesülnek, s ha ez mégsem így lenne, akkor független harmadik félhez fordulhat

[672] Erre utalt az 1997-ben végzett Internet Privacy Study (Boston Consulting Group/eTrust); lásd The TRUSTe story „Building Trust Online: TRUSTe, Privacy and Self Governance" című tanulmányt az American Bar Association részére, 2000. március. In *TRUSTe Online Privacy Resource Book;* ez utóbbi tanulmány alapján mutatjuk be a TRUSTe koncepcióját. A TRUSTe által a honlap-üzemeltetőkkel kötött szerződés tartalmát a TRUSTEe Lincense Agreement 7.0 verziója alapján ismertetjük.

panaszával. A TRUSTe és a programban részt vevő website között olyan szerződés születik, amely biztosítja, hogy a felhasználó állampolgárságától vagy a programban részt vevő website üzemeltetőjének földrajzi elhelyezkedésétől függetlenül felléphessen az előzetesen rögzített adatvédelmi szabályok megsértése esetében.

A TRUSTe-logót feltüntető weboldalaknak az alábbi, a tisztességes adatkezelési gyakorlatot (fair information practices)[673] megvalósító elveket kell tiszteletben tartania:

– *Az értesítés elve (notice):* a TRUSTe-logót hordozó oldalaknak egyértelműen tudatniuk kell a felhasználóval, hogy mely személyhez köthető információkat (európai terminológia szerint személyes adatokat) gyűjtenek, és azokat kinek továbbítják. Feltétel az is, hogy az ezt feltüntető szöveg jól olvasható legyen, és legfeljebb egy egérkattintásnyira helyezkedjen el a site főoldalától.

– *A döntés elve (choice):* a felhasználók számára biztosítani kell a döntést a tekintetben, hogy engedélyezik-e adataik további célokra történő felhasználását. A döntés lehetőségét az oldal oly módon is biztosíthatja, hogy a felhasználónak külön hozzá kell járulnia ezen adatkezelésekhez (opt-in), és úgy is, hogy ellentétes szándékát kell külön kinyilvánítania (opt-out). Az elv eredménye a gyakorlatban az, hogy a felhasználó megakadályozhatja azt, hogy adatait a site értékesítse, illetve továbbítsa.

– *A hozzáférés elve (access):* a felhasználónak „elvárható" (reasonable) hozzáféréssel kell rendelkeznie a site által róla tárolt adatokhoz, hogy a tárolt adatok pontatlanságait, hibáit javítani lehessen.

– *A biztonság elve (security):* site-nek a gyűjtött adatok biztonságát elvárható mértékben kell biztosítania.

A programhoz kapcsolódik a TRUSTe Wathcdog elnevezésű alternatív vitarendezési mechanizmus. Ha valamely oldal visszaélt egy felhasználó adataival, vagy nem az előzetesen meghirdetett adatvédelmi elveinek megfelelően kezeli a személyes adatokat, a felhasználó a TRUSTe-hoz fordulhat. A TRUSTe-nek az általa a site-okkal kötött szerződés szerint számos lehetősége van: felhívhatja az oldalt, hogy módosítsa a meghirdetett adatvédelmi politikát, az általa követett gyakorlatot. Felhívhatja az oldalt, hogy vesse alá adatvédelmi politikáját független harmadik fél által végzett auditnak. Súlyos esetekben az ügyben a TRUSTe az illetékes állami szervhez, az Egyesült Államokban a Federal Trade Commissionhoz fordulhat, illetve visszavonhatja a logó használatának jogát.

A vitarendezési eljárás végig e-mailben zajlik, annak menete a következő: a panaszt a fél online rendelkezésre álló űrlap kitöltésével nyújthatja be. A TRUSTe a panasz beérkezése után megvizsgálja, hogy az tárgyalható-e a vitarendezési eljárás keretein belül (ennek feltétele az, hogy a panaszt benyújtó személy már korábban megkísérelte a vitát közvetlenül az általa bepanaszolt személlyel vagy szervezettel rendezni, a panasz a panaszt benyújtó személlyel kapcsolatos, személyhez köthető információra [personally identifiable information] vonatkozik, a panasz tárgya az, hogy a TRUSTe-programban részt vevő személy vagy szervezet az általa gyűjtött, személyhez köthető információt online közzétett adatvédelmi politikájától eltérő módon használta fel, s a panasz valamely TRUSTe logó használatára feljogsított társaság ellen irányul, valamint a panasz angol nyelvű, vagy a bepanaszolt társaság megfelelő fordítói szolgáltatást bocsátott rendelkezésre).

A TRUSTe 10 munkanapon belül értesíti a panasz benyújtóját arról, hogy a panasz vizsgálható-e az eljárás keretei között; ha nem, annak okairól írásban ad tájékoztatást a panasz benyújtójának. Az eljárás megindítása előtt a TRUSTe további információkat kérhet a panaszt benyújtó személytől, akinek további 10 munkanap áll rendelkezésére a további információ szolgáltatására.

Ezek után kezdődik meg valójában a vitarendezési eljárás. A panaszt a TRUSTe továbbítja a bepanaszolt társaságnak, amelynek öt munkanap áll rendelkezésére a válaszra; amennyiben a válasz a TRUSTe álláspontja szerint „bármely szempontból nem kielégítő”, úgy további határidő meghatározásával felhívhatja a bepanaszoltat arra, hogy további információt szolgáltasson. A választ a bepanaszolt a TRUSTe-nek és a panaszt benyújtó személynek is megküldi. Ezek után a panaszt benyújtó személy számára 10 munkanap áll rendelkezésre, hogy a TRUSTe és a bepanaszolt számára saját válaszát megküldje. Ha a panaszt benyújtó személy a határidő lejártáig nem küldi meg válaszát, és vita a TRUSTe álláspontja szerint is megfelelő módon zárult le, az eljárást a TRUSTe a válaszadási határidő lejártával megszüntetheti.

Abban az esetben, ha a panaszt benyújtó személy a rendelkezésére álló határidőben megküldi válaszát, a TRUSTe ezt haladéktalanul továbbítja a bepanaszolt számára. A bepanaszoltnak újabb 10 munkanap áll rendelkezésére saját álláspontjának közlésére. Ha a válasz kielégítő, a TRUSTe megszüntetheti az eljárást; amennyiben pedig nem érkezik válasz, ez a végső döntés meghozatalakor értékelhető. Ha valamely fél még a továbbiakban

[673] Ezeket a TRUSTe-program alapját jelentő elveket a Department of Commerce fogalmazta meg Elements of Effective Self Regulation for the Protection of Privacy című munkaanyagában. Lásd The TRUSTe story

nyilatkozik, a TRUSTe azonnal továbbítja a beadványt az ellenérdekű félhez, amelynek a kézhezvételtől számított 6 munkanap áll rendelkezésére a válaszra.

Bármely fél javasolhatja telekonferencia (vagy más módon tartott megbeszélés) rendezését is. E javaslat elfogadását a TRUSTe szabadon mérlegeli. Amennyiben a javaslatot a TRUSTe elfogadja, akkor is csak a már korábban írásban tárgyalt kérdések szóbeli megvitatására van lehetőség.

Amikor a TRUSTe álláspontja szerint a vita lezárható, az esetről készített jelentését megküldi az érdekelt feleknek, amelyben közli döntését is.

A TRUSTe a Safe Harbour Agreement létrejötte nyomán immár szolgáltatásként nyújtja az alapelveknek történő megfelelés tanúsítását is.

1.22.2. Az ipari önszabályozás kritikája

1. Az önszabályozás megfelelő eszköz a magánszféra-védelem hatékonyságának növelésére – ám a magánszféravédő technológiákhoz hasonlóan az adatvédelmi jogi szabályozáshoz képest csak kiegészítő eszköz lehet. A P3P a gyakorlatban nem működik; az irodalomban számos kétely merül fel a TRUSTe-val kapcsolatban. Az irodalom értékelése szerint a TRUSTe és a hasonló tanúsító védjegyeken alapuló rendszerek[674] gyengéje az, hogy mivel kevéssé ismertek, ezért az általuk alkalmazott szankció – vagyis hogy megvonják a szabálytalan adatkezelési gyakorlatot folytató weboldal üzemeltetőjétől a megjelölés használatának a jogát – nem hatékony. A felhasználók ugyanis nem hiányolják a védjegyet.[675] 2003 folyamán a TRUSTe két esetben vonta vissza a védjegy használati jogát, és egy további esetben indított vizsgálatot a védjegyet használó vállalkozás ellen.[676]

2. Schwartz szerint összességében az önszabályozás eszközei (legyenek azok akár iparági önszabályozási kódexek, akár olyan technológiák, amelyek segítségével az adatalany kifejezheti preferenciáit, mint a P3P) állami szabályozás nélkül nem biztosítják a magánszféra hatékony védelmét. A szerző szerint – aki amerikai szempontból a cybertérben érvényesülő normákat vizsgálja – ennek lényegi oka az, hogy a minden szereplő által megszokott „főszabály" (default) a személyes adatok teljes feltárása; ebben a helyzetben az adatalanyok nincsenek tudatában személyes adataik értékének, az adatokat felhasználó iparágak pedig a

---

„Building Trust Online: TRUSTe, Privacy and Self Governance". In *TRUSTe Online Privacy Resource Book.*

[674] Például a BBBOnline: http//www.bbbonline.com.

[675] Schwartz 2002, 79.

[676] TRUSTe Year in Review 2003, http://www.truste.org/pdf/TRUSTe_2003_Annual.pdf.

status quo fenntartásában érdekeltek.[677] Ez meghiúsítja azt, hogy a „piacon" az adatalany valódi alkupozícióba kerüljön, és az önszabályozás is elsősorban az állami szabályozás elhárítására irányul. Schwartz szerint meg kellene teremteni azt a helyzetet, amelyben az üzleti szereplők rákényszerülnek arra, hogy az adatalanyok preferenciáit figyelembe véve megfizessék az adatok felhasználásának árát. Az általa javasolt fogalom a „privacy price discrimination". A valós piac kialakulására azonban csak akkor van mód, ha a főszabály a személyes adatok megismerésének *tilalma* – ehhez pedig az állami szabályozáson keresztül vezet az út.[678] Egyetértve a szerző személyes adatok piacára és az önszabályozás lehetőségeire vonatkozó elemzésével, rá kell mutatni arra, hogy a személy alkupozíciójának megteremtésére csak olyan adatvédelmi szabályozás alkalmas, amely kizárja, hogy a „hozzájáruláson alapuló" adatkezelés rutinszerűvé váljon (lásd ezzel kapcsolatban a hozzájárulás fogalmának kiüresedésére vonatkozó fejtegetést fent).

3. A hozzájáruláson alapuló adatkezeléssel kapcsolatos problémák orvoslását Burkert lehetségesnek tartja a magánszféravédő technológiák fejlesztésével és alkalmazásba vételével. A szerző szerint a probléma az, hogy rendszerek tervezői a jelenlegi helyzetben egyszerűen az érintett hozzájárulásának beszerzésére támaszkodnak, további vizsgálat nélkül. A magánszféravédő technológiák fejlesztésével azonban elérhető, hogy aki személyes adatokat kezel, az rákényszerüljön az adatkezelés valódi alapjának igazolására. A szükségesség elvének a rendszertervezés szintjén való megjelenése vezethet oda, hogy az adatkezelők politikai vitára kényszerüljenek arról, miért is van szükség a szóban forgó adatkezelésre.[679] Burkert is kiemeli e technológiák korlátai között azt, hogy hiányzik a valós alkufolyamat, és – bár fogalmat nem javasol – pontosan a Schwartz által megfogalmazott „privacy price discrimination" kialakulását tartja kívánatosnak: „a tranzakciós folyamat során kiadott személyes adat [personal information] a kívánt termék vagy szolgáltatás ellenértékének a részét képezi. Ha ez az információ nincs ott, akkor a termék vagy szolgáltatás ára valószínűleg változni fog. Ez a változás transzparenssé lenne tehető, és választási lehetőség lenne felkínálható [az adatalanynak]: a terméket eladó vagy szolgáltatást nyújtó vállalat magasabb árat kérhetne, amely a magánszféra magasabb szintjével járna együtt, vagy alacsonyabb árat kellene fizetni, de ebben az esetben olyan többletinformációt kellene

[677] Schwartz 2002, 74.

[678] Schwartz 2002, 74., 81. skk. A szerző a fejtegetések során a „personal information" fogalmat használja, ám ennek a tárgy szempontjából nincs jelentősége.

[679] Burkert 1997, 129.

szolgáltatni, amely a cég számára lehetővé tenné, hogy annak felhasználásával nyereségtöbblethez jusson."[680]

Látni kell, hogy az „alkupozíció" megteremtésére irányuló törekvések, a „privacy price discrimination" ösztönzése alapvetően eltér attól, amit az e tekintetben farizeusnak is nevezhető hazai adatvédelmi jogi gondolkodás az adatok áráról tart. Bár a hazai népesség-nyilvántartásból direktmarketing-célra szabadon vásárolhatók adatok, számos olyan adatvédelmi biztosi állásfoglalás van, amely valamely adat megadását jogszerűtlennek minősíti, illetőleg úgy foglal állást, hogy a szolgáltató az adat átadásának megtagadása esetében is kötelezhető a szolgáltatás nyújtására. A gyakorlatban ilyen esetekben tömegesen járulnak hozzá az ügyfelek az adatkezeléshez, s a hozzájárulás kiüresedik. Ebből a helyzetből álláspontunk szerint a szabályozás a kiút: monopolhelyzetben lévő adatkezelőknél az adatkezelést meghatározott körre kell szorítani, és ezen felül tiltani kell; ám monopolhelyzetben nem lévő adatkezelőknél inkább a valós adatpiac kialakulására kell törekedni, és csak akkor kell nagyobb mértékben beavatkozni, ha az adatalanyok alkupozíciója ebben az esetben sem bizonyul valósnak (ezen az elvi alapon áll az elektronikus kereskedelmi törvény a szerző által előkészített adatvédelmi fejezete; ám a látszólagos hasonlóság ellenére sérti ezt az elvet az elektronikus hírközlésről szóló törvény megoldása, amely az adatkezelést minden esetben meghatározott körre szűkíti, nem csak monopolhelyzet esetén).

1.23. Szabványosítás

1.23.1. A CSA által kidolgozott adatvédelmi szabvány

1. Az adatvédelmi szabványok közül a legkorábbi az 1996-ban kidolgozott kanadai szabvány, amelynek kidolgozására az irányelv elfogadása ösztönözte a Kanadai Szabványügyi Szövetséget (Canadian Standards Association) – az irányelv következményeképp az adatvédelem megfelelő szintjét biztosító intézkedések hiányában a kanadai fél kereskedelmet akadályozó helyzet kialakulásától tartott. A másik ok az volt, hogy az OECD-irányelvek nyomán számos „magatartáskódex" (code of practice) született, ám ezek tartalma között igen nagy eltérések voltak.[681] A CSA ezért előbb egy modell-magatartáskódexet megalkotását koordinálta (CSA Model Code), majd az nemzeti,

[680] Burkert 1997, 134.

[681] Bennett 1997, 111.

önkéntesen követendő adatvédelmi szabvánnyá vált. A szabványhoz megfelelő tanúsítási, nyilvántartási és auditmechanizmus is tartozik.[682]

A szabvány tíz alapelvet határoz meg a személyes adatok kezelést illetően; azt 45 tagú bizottság dolgozta ki, amelyben képviseltették magukat a pénzügyi szféra, a távközlés, a direktmarketing üzletág képviselői, a helyi önkormányzatok és a központi közigazgatás szervei, a fogyasztói érdekképviseletek, a szakszervezetek, valamint helyet kaptak benne biztonságtechnológiával foglalkozó informatikai szakemberek is.[683] 1997-ben Ausztráliában, 1999-ben pedig Japánban született hasonló szabvány.[684]

1.23.2. Európai szabványosítási törekvések

1. Az Európai Szabványügyi Bizottság (European Committee of Standardization, CEN) 1997 közepén hozta létre Információs Társadalom Szabványosítási Rendszer (Information Society Standardization System) nevű projektjét (CEN/ISSS), amelynek célja az információs társadalom közegében megjelenő, a szabványosítás hagyományos és újszerű módjai segítségével megoldható kérdések azonosítása és e kérdések rendezése. A CEN/ISSS szolgáltatásként határozza meg magát, amely az üzleti szereplőknek számos szolgáltatást kínál szabványok kialakításától kezdve a legjobb gyakorlatok azonosítását és cseréjét rögzítő megállapodásokig.[685] A CEN/ISSS keretében indult meg az a projekt, amelynek célja annak vizsgálata, hogy szükséges és lehetséges-e az EU adatvédelmi irányelvéhez kapcsolódóan olyan szabványok megalkotása, amelyek a piaci szereplők számára segítséget nyújthatnak az irányelv és az egyéb adatvédelmi rendelkezések követéséhez; amennyiben a projekt keretében – legalább meghatározott kérdések esetében – a válasz pozitív, akkor pedig annak meghatározása, hogy a szabványosításnak egy adott kérdésben milyen előnyei és hátrányai vannak.

2. A „Európai adatvédelmi szabvány kezdeményezés” elnevezésű projekt (Initiative on Privacy Standardization in Europe, IPSE) célja zárójelentés (Final Report) kiadása volt. A IPSE által a szabványosítás lehetséges témáiként meghatározott kérdések között már a projekt

[682] A CSA által kidolgozott szabványról lásd Bennett 1997, 115. skk.

[683] Jos Dumortier – Caroline Goemans: *Data Privacy and Standardization.* Discussion Paper prepared for the CEN/ISSS Open Seminar on Data Protection, 2000. március;
http://www.law.kuleuven.ac.be/icri/papers/doctrine/cen-paper.pdf 36.

[684] Uo.

[685] Bővebben lásd http://www.cenorm.be/isss.

indulásakor szerepelt az audit témaköre (compliance control mechanisms/audit) és az egyes, az adatvédelem szintjét tanúsító – a TRUSTe-hez hasonló – programokkal kapcsolatos követelmények meghatározása, azok értékelése.[686] A projekt keretében született első, komoly kutatási eredényeket tartalmazó dokumentum a Leuveni Katolikus Egyetem Interdiszciplináris Információs Technológiai és Jogi Kutatóintézetének keretében készített vitaanyag,[687] majd a CEN/ISSS 2002. február 3-án adta ki a Durmoniter és Goemans tanulmányára is támaszkodó zárójelentést.[688]

A zárójelentés szerint az adatvédelmi audit növekvő üzletág, ám nem biztos, hogy az auditorcégek ugyanazon követelményrendszert használják az auditok során; gyakran az IT-audittal foglalkozó szervezeti egység végzi az adatvédelmi auditot is, márpedig az adatvédelem és az adatbiztonság szempontjai sokszor ellentétben állnak egymással; az adatvédelmi auditot szolgáltatási palettájukon kínáló ügyvédi irodák pedig sok esetben nem képesek azon technológiai kérdések áttekintésére, amelyek megítélése pedig fontos az adatvédelmi jognak való megfelelés megítélése szempontjából.[689] Az auditorok számára beindítandó képzés, illetve az auditorok akkreditációs rendszere megteremtésének előfeltétele azonban az, hogy arról a standardról megállapodás szülessen, amelynek alapulvételével az auditorok az auditot végzik. A nemzetközi fejlemények között a zárójelentés is kiemeli az online tanúsító programokat (TRUSTe, BBB), amelyek közül a BBB már a japán JIPDEC nevű kormányzati szervvel, valamint az Európai Direkt Marketing Szövetséggel (FEDMA) is együttműködik. Ugyanakkor a zárójelentés arra is utal, hogy egyre nyilvánvalóbb: a számos „privacy seal" projekt egyre inkább zavarossá teszi a helyzetet a fogyasztók számára.[690] Az egymással is versenyző hitelesítő programok értékelésének szempontjait kívánatos lenne szabványba foglalni.[691]

3. A magánszféravédő technológiák kapcsán az anyag rámutat: az EU adatvédelmi irányelve kötelezi az adatkezelőket arra, hogy „megfelelő technikai és szervezeti

---

[686] Lásd IPSE – Proposed Topics of Possible Standardization Work;
http://www.cenorm.be/isss/Projects/dataprotection/ipse/itemlist.htm

[687] Jos Dumortier – Caroline Goemans: *Data Privacy and Standardization.* Discussion Paper prepared for the CEN/ISSS Open Seminar on Data Protection, 2000. március;
http://www.law.kuleuven.ac.be/icri/papers/doctrine/cen-paper.pdf.

[688] Initiative on Privacy Standardization in Europe, Final Report, CEN/ISSS Secretariat, Brussels, 2002. Lásd: http://www.cenorm.be/isss/Projects/DataProtection/IPSE/ipse_finalreport.pdf.

[689] Lásd Final Report 4.17.

[690] Lásd Final Report 4.23.

[691] Lásd Final Report 4.24.

intézkedésekkel" biztosítsák a személyes adatok védelmét.[692] Az irányelv preambulumának vonatkozó része[693] szerint ennek a követelménynek érvényesülnie kell mind a rendszer tervezésénél, mind az adatkezelési folyamat során. Mindebből az következik, hogy a rendszereket már az adatvédelmi követelményeknek megfelelően kell tervezni,[694] ám ha a technológia ezen követelmények biztosítására nem alkalmas, akkor szervezeti intézkedéseket kell tenni. Egyes adatvédelmi biztosok – például a holland – tudatosan a technológiai intézkedések elsődleges jellegét hangsúlyozzák abból a megfontolásból, hogy azok hatásai nehezebben kerülhetők meg. A szervezeti megoldások a zárójelentés szerint továbbra is fontosak maradnak a PET-ek által biztosított környezet mellett (hiszen ezek az új technológiák régi rendszerekbe nehezen integrálhatók, ráadásul az új informatikai rendszerek tervezésénél sem általános egyelőre, hogy azok megfelelnek az irányelv, illetve a nemzeti adatvédelmi jogszabályok rendelkezéseinek).

4. A rendelkezésre álló technológiák közül a zárójelentés említi a titkosítóeszközöket, az anonimitást, illetve pszeudonimitást biztosító böngészőket, e-mail szolgáltatásokat, a P3P-t, az adatvédelmiszabályzat-író szoftvereket, amelyek a website-üzemeltetőnek meghatározott kérdéssorokat tesznek fel, majd ennek alapján meghatározzák az oldal P3P-szabvány szerint specifikált adatvédelmi szabályzatát (szabályzatíró szoftvert kínál a Microsoft, valamint az OECD is nyilvánosságra hozott egyet a Microsoft és az Oracle támogatásával), az intelligens kártyákat, a biometriai azonosítást lehetővé tévő eszközöket (biometrical readers), és a cookie-k kezelését biztosító, illetve a web-bugokat kiszűrő szoftvereket. Érdekesség, hogy az anyag szerint a biometriai azonosítás adatvédelmi okokból történő elutasítása káros az adatvédelem szempontjából is, ugyanis az biztonságosabb azonosítást tesz lehetővé, mint a jelszón vagy meghatározott információk ismeretén alapuló azonosító rendszerek.[695]

Kiemelendő a jelentés megállapítása az európai adatvédelmi biztosok és a technológia fejlesztésében elöljáró üzleti szereplők közötti kapcsolatról. A CEN/ISSS szerint igen nagy problémákat okoz, hogy a már kifejlesztett rendszereket csak rendkívül nagy költséggel lehet úgy módosítani, hogy azok megfeleljenek az irányelv és az azt végrehajtó nemzeti jogszabályok követelményeinek. Az irányelv 29. cikke alapján működő munkacsoport keretében az adatvédelmi biztosok komoly erőfeszítéseket fejtenek ki a technológia befolyásolására, ám a technológiák kereteit lefektető testületekre és az ipar szereplőire nem

[692] irányelv 17. cikk.

[693] Recital 46.

[694] Lásd a német adatvédelmi jog alább tárgyalt rendelkezéseit az adattakarékosság elvével kapcsolatban.

[695] Lásd Final Report 4.26.

képesek megfelelő mértékben hatni: erre hiányoznak a forrásaik, a technológiai kérdéseket illető gyakorlatuk, illetve hiányoznak a megfelelő kommunikációs csatornák is.[696] Ebben a kérdésben az ipari szféra szereplői sem kezdeményeznek kontaktust, ráadásul európai szinten az sem világos, hogy melyik adatvédelmi hatósághoz kellene fordulni[697]..A jelentés fogalmazói szerint a jogvédő szervezetek gyakran híján vannak azon technológiai ismereteknek, amelyek szükségesek volnának ahhoz, hogy kampányszerű tiltakozások mellett komoly párbeszédre legyenek képesek az iparági szereplőkkel. A technológia fejlesztését végző szakembereknek pedig nem áll rendelkezésére olyan forrás, amelynek segítségével követhetnék az adatvédelmi jogban bekövetkező változásokat. Az IPSE álláspontja szerint a szabványügyi szervezeteknek kell megteremteniük a kapcsolatot a technológiai szabványok kidolgozói, az iparági szereplők, a jogalkotók, a jogászok és az adatvédelmi hatóságok, valamint a IT-szakemberek, biztonságtechnikusok és auditorok között.[698] Álláspontjuk szerint a CEN alkalmas fóruma lenne a párbeszédnek.

5. Az IPSE ezután mátrixban összegzi azokat a jogszabályhelyeket, amelyekkel az adatvédelmi szabvány nem állhatna ellentétben (hiszen a projekt célja olyan szabvány lehetőségének megvizsgálása volt, amely az irányelv gyakorlatba történő átültetését segíti). Ennek keretében vizsgálták az EU-irányelv, az EU távközlési adatvédelmi irányelv, az OECD-irányelvek, valamint az ET-egyezmény főbb rendelkezéseit, mégpedig a célhoz kötöttség elve, az adatminőség és arányosság, az átláthatóság, az adatbiztonság, a hozzáférés, módosítása és a letiltás joga, az adattovábbítás korlátozása, a különleges adatok, a direkt marketingre vonatkozó rendelkezések, valamint az automatikus egyedi döntések szempontjából. A mátrixba belefoglalták a négy dokumentum által lefektetett eljárási/jogkövetést segítő mechanizmusokat is, így a szankcionálásra vonatkozó rendelkezéseket, az adatalany támogatását szolgáló rendelkezéseket, valamint a megfelelő reparáció biztosítását szolgáló szabályokat.[699]

6. A követelmények meghatározása után hat különböző eszközt elemeztek: a P3P-t, az intelligens kártyákat, az OECD által közzétett adatvédelmiszabályzat-generátort, egyes

[696] Lásd a munkacsoport honlapját a http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm oldalon. A fenti megállapításra jó példa a 2005-ben elfogadott, az RFID technológiák adatvédelmi vonatkozásairól szóló munkaanyag található a http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf oldalon.

[697] Lásd Final Report 4.29.

[698] Lásd Final Report 4.32.

[699] Lásd Final Report 5.

magatartáskódexeket és mintaszerződés-modelleket, valamint a BBB – a TRUSTe-hez hasonló – online tanúsító programját. Az alábbiakban a később részletesen tárgyalt P3P és az elektronikus közigazgatásban potenciálisan nagy szerepet játszó intelligens kártyák (smart cards) IPSE keretében végzett elemzésére térünk ki.

7. Ami a célhoz kötöttség elvét illeti, a P3P – abban az esetben, ha az adott website olyan információt küld, amely szerint kizárólag a website üzemeltetéséhez szükséges adatokat kezeli képes biztosítani a célhoz kötöttség követelményét; ám ebben az esetben valójában csak közvetít a site és a felhasználó között. A jelentés szerzői szerint a site-ok többsége jelenleg nem tesz eleget a célhoz kötöttség követelményének. Ugyanez a helyzet az adatminőség/arányosság esetén is: a P3P abban nyújthat segítséget a felhasználónak, hogy az ezen követelményeknek eleget tévő site-okat azonosíthassa. Valójában az átláthatóság elve az, amelyet a P3P rendszerének értelme: a site által követett adatvédelmi szabályok meghatározott specifikáció szerinti közlése a böngészőprogrammal. A biztonság, az adatalany jogai és az adattovábbítás korlátozása kapcsán is igaz, hogy a P3P csak tájékoztatja a felhasználót az oldal által követett elvekről, az elvek érvényesítéséhez nem járul hozzá.[700]

8. Az intelligens kártyákat a jelentés úgy határozza meg, mint amelyek „olyan műanyag kártyák, amelybe adatfeldolgozásra képes nagy integráltságú félvezető áramkört (chipet) építettek" – vagyis nem minősülnek ilyenek a mágneskártyák, illetve azok a kártyák, amelyek adattartama nem változhat (stored value cards).

Az adatminőség és arányosság szempontjából a jelentés kiemeli, hogy a kártyák adatfeldolgozási képessége alkalmas hálózati adatbázisokkal való kapcsolatteremtésre, adatok ellenőrzésére. A kártya meghatározott tartományainak elérése korlátozható, a többi terület elérésétől függetleníthető, így a meghatározott alkalmazásokhoz a kívánt adatmennyiség társítható, vagyis biztosítható az arányosság alapelve.

A célhoz kötöttség elve a kártya programozásától függ. A kártya képes adatok gyűjtésére, tárolására és továbbítására; arra, hogy birtokosát azonosítsa, és számára valamely távoli adatbázisban jogosultságokat biztosítson. Ennek keretében megvalósítható a célhoz kötöttség elvének megfelelő viselkedés is.

Az átláthatóság elve a jelentés szerzői szerint kevéssé biztosított az intelligens kártyák esetében.[701] A szerzők szerint indokolt volna a kártyákhoz olyan dokumentációt mellékelni,

[700] Lásd Final Report 6.1.

[701] Jelen tanulmány szerzőjének személyes élményei is vannak arról, hogy az adatvédelmi biztos az 1990-es évek végén éppen az átláthatóságot – és az adatbiztonságot – illető kételyei miatt nem támogatott egyes, intelligens kártyák használatára épülő adatkezelési rendszerekre vonatkozó terveket.

amelyből annak felhasználója megismerheti a pontos működést, úgy programozni azokat, hogy tartalmuk a felhasználó számára olvasható legyen. A jelentés szerint biztonsági megfontolások a technológia fejlettségének jelenlegi szintjén nem indokolják az ilyen megoldások mellőzését.

Az intelligens kártyákkal kapcsolatos kétségek a jelentés szerzői szerint is széles körűek. A biztonsági fenyegetettség nagyobb, mint az egyszerű mágneskártya esetében, mivel azzal ellentétben az intelligens kártya multifunkcionális, illetve a támadó számára jóval több lehetőséget kínál, nagyobb a támadásra ösztönző erő. A szerzők szerint megfelelő technológiák – titkosítás, elérési korlátozások – használata esetén elfogadhatóra emelhető a biztonság szintje.

A hozzáférés és a módosítás joga érvényesülhet, azaz a kártya programozható úgy, hogy a felhasználó hozzáférjen a kártya tartalmához, jogosultsága esetében módosítsa is azt, illetve a kártya értesítse őt arról, ha a módosítás nem sikeres.

Az adattovábbítás korlátozása szintén programozható a kártyába; az megvalósítható a kártya által végzett adatkezelési műveletek esetében, de akkor is, ha a kártya csupán hozzáférést biztosít a jogosult felhasználó számára valamely távoli adatbázisban tárolt adatokhoz. A felhasználó számára meghatározott esetekben felkínálható a döntési lehetőség, abszolút tilalom – például adekvát védelemmel nem rendelkező országba történő adattovábbítás tilalma – esetében a kártya programozható úgy, hogy az adatot ne továbbítsa.[702]

9. A Zárójelentés végén az IPSE a következő ajánlásokat teszi:[703]

Olyan, önkéntesen követendő adatvédelmi legjobb gyakorlatokat kell meghatározni és ingyenesen vagy alacsony áron közzétenni, amelyek segítik az adatkezelőket abban, hogy működésüket az irányelv – és ha lehetséges – a nemzeti jogszabályok rendelkezéseihez igazítsák. Először egy minden szektor adatkezelésére kiterjedő dokumentumra van szükség, majd azt követheti a meghatározott szektorokra vonatkozó kiegészítés. A jelentés szerint az irányelv alapján működő munkacsoport és az ET keretében működő hasonló testület iránymutatásai mellett szükséges egy olyan dokumentum, amely a létező eredményeket összefoglalja.

Átfogó szabvány (management standard) – különösen olyan, amelyhez formális tanúsítvány (formal certification) tartozik – alkotása a jelentés szerint nem időszerű. A

[702] Lásd Final Report 6.2.

[703] Lásd Final Report 8.

jelentés szerint ilyen szabványoknak számos ellenzője van az IT-iparban, ezért – bár egyes, a szabványosítás folyamatában a fogyasztókat képviselő szervezetek, valamint több európai adatvédelmi biztos támogatná azokat – jelenleg kezdeményezésük korai.

Szerződésminták megfogalmazására van szükség. Az irányelv 17. cikke szerint minden adatkezelő, amely adatfeldolgozót vesz igénybe, köteles azzal szerződést kötni (kivéve, ha a közöttük fennálló kapcsolatot jogszabály rendezi). Ez – a nemzetközi kereskedelmi jog fogalomrendszerének egységesülését segítő INCOTERMS példáját követve – rendezné az adatkezeléssel kapcsolatos szerződések terminológiáját az unión belül. Az adatkezelő és az adatfeldolgozó közötti kapcsolat azért jó példa, mert a rendezendő kérdések (felelősség, biztonsági kérdések) tipikusak, ám számos jogalkalmazási nehézséghez vezetnek.

Az adatvédelmi auditot illető, létező gyakorlatok felmérése is szükséges. A felmérés célja az, hogy számba vegye, milyen módszerek segítségével végeznek jelenleg adatvédelmi auditot, s megállapítsa az adatvédelmi auditra vonatkozó legjobb gyakorlatot. A felmérést az összes érintett, az adatvédelmi hatóságok, auditor szervezetek, biztonságtechnikai és jogi szakértők és adatvédelmi auditot igénybe vett szervezetek részvételével kell elvégezni. Számos adatvédelmi biztos végez adatvédelmi auditot önállóan, törvényi felhatalmazás alapján vagy vizsgálatai során; mind egyes auditor társaságok, mind adatvédelmi joggal foglalkozó ügyvédi irodák szolgáltatásként kínálják azt. Az adatvédelmi audit egyre elterjedtebb, ám senki nem vizsgálta azt, miben különbözik egy adatvédelmi és egy adatbiztonsági audit, illetve általában mi az eltérés az adatvédelmi audit és bármely hagyományos audit között; szükség van az auditoroktól elvárt végzettség, szaktudás vagy tapasztalat meghatározására, s arra, hogy melyek az audit azon összetevői, amelyek kapcsán helye van a szabványosításnak.

Az internetes adatvédelmi minőségjelzőkkel (web seals) kapcsolatos felmérés készítése is kívánatos lenne abból a célból, hogy megállapítható legyen: szükséges-e további szabványosítás ezen a területen. Az internetes adatvédelmi minőségjelzők – például a TRUSTe vagy a BBB minőségjelzője – az egész világon használtak, ugyanakkor sem az adatvédelemnek nincsenek az egész világon elfogadott normái, sem olyan szabványok nem állnak rendelkezésre, amelyekhez képest e minőségjelző szolgáltatásokat értékelni lehetne. Ilyen követelmények (common criteria) meghatározása a célja ezen ajánlásnak.

A technológia adatvédelemre gyakorolt hatásának folyamatos vizsgálata is ajánlott. Ehhez szerint az első lépés egy olyan jelentés készítése, amely az összes érdekelt bevonásával készül, és számba veszi a technológia és a szabványok hatását az adatvédelemre. A következő lépés egy olyan koordinációs mechanizmus megteremtése, amely hosszú távon megteremti a

párbeszéd lehetőségét az új technológiák alakítói és az adatvédelmi joganyag felügyeletét ellátó szervek között, biztosítja, hogy az adatvédelmi biztosok értesüljenek a technológia fejlődésének új trendjeiről, és szükség esetén idejében beavatkozhassanak. Szükség van arra is, hogy a szabványosítás folyamatában megjelenjenek a jogi szempontok. A szerzők az európai szabványügyi szervezetek keretein belül javasolják olyan mechanizmus megteremtését, amelynek segítéségével az adatvédelmi jog szempontjából releváns technológiák – a cookie-k, földrajzi helyzet-meghatározó technológiák, földrajzihelyzet figyelembevételével nyújtott szolgáltatások – fejlesztését végző vállalatok időben értesülnek azokról a jogi követelményekről, amelyeket figyelembe kell venniük termékeik és szolgáltatásaik kialakítása során.

Az utolsó ajánlás az adatvédelmi szabványosítással kapcsolatos tájékoztatási tevékenység fontosságára hívja fel a figyelmet.

A CEN kezdeményezése figyelemre méltó, s kiemelendő, hogy annak nyomán elkészült a létező, adatvédelmi auditra vonatkozó gyakorlatok leltára, és az adatvédelmi audit európai keretrendszere (lásd erről részletesebben alább). Ez az ismerethalmaz Magyarországon is segítheti a remélhetőleg jogi normában is megjelenő intézmény elterjedését.

1.24. A CEN adatvédelmi audit keretrendszere

1.24.1. Az adatvédelmi audit keretrendszer megszületésének előzményei

1. A CEN adatvédelmi audit keretrendszerét az Európában alkalmazott adatvédelmi audit módszertanok felmérését követően alkották meg, s annak egyik célja kifejezetten az, hogy hozzájáruljon a nemzeti adatvédelmi audit módszertanok kialakításához.

A keretrendszer három fő részből áll. Ezek
- iránymutatás (guidance) az audit lefolytatásának módjával kapcsolatban
- az Irányelv alapelveinek való megfeleléssel kapcsolatos követelmények rendszere
- a szervezeti, eljárási és technológiára vonatkozó belső kontrollmechanizmusokkal kapcsolatos követelmények.

Mindhárom rész igen tanulságos a magyar jogi környezetben dolgozó szakember számára. Az audit lefolytatásával kapcsolatos iránymutatás minden további nélkül alkalmazható, a jogi követelmények rendszere természetszerűleg a hazai komplex adatvédelmi jogi környezethez

illesztendő, a kontrollmechanizmusokra vonatkozó követelmények pedig együtt vizsgálandók az informatikai biztonsági követelményekkel.

Számos olyan kérdés is van azonban, amelyekre ez a keretrendszer nem adhat választ. Az auditor személye, a szükséges kvalifikációk meghatározása, a tanúsítás, illetőleg a tanúsítók kijelölésének rendszere a későbbiekben határozandó meg. További feladat az adatvédelmi audit módszertanának összehangolása az alkalmazott informatikai biztonsági audit módszertannal, különösen az itt ismertetett dokumentumban is hangsúlyosan szereplő kockázatfelmérés (Risk Assessment) kérdésében.

2. A „Európai adatvédelmi szabvány kezdeményezés" elnevezésű projekt (Initiative on Privacy Standardization in Europe, IPSE) célja zárójelentés (Final Report) kiadása volt. A IPSE által a szabványosítás lehetséges témáiként meghatározott kérdések között már a projekt indulásakor szerepelt az audit témaköre (compliance control mechanisms/audit) és az egyes, az adatvédelem szintjét tanúsító – a TRUSTe-hez hasonló – programokkal kapcsolatos követelmények meghatározása, azok értékelése.[704] A projekt keretében született első, komoly kutatási eredényeket tartalmazó dokumentum a Leuveni Katolikus Egyetem Interdiszciplináris Információs Technológiai és Jogi Kutatóintézetének keretében készített vitaanyag,[705] majd a CEN/ISSS 2002. február 3-án adta ki a Durmoniter és Goemans tanulmányára is támaszkodó zárójelentést.[706] A zárójelentésben hangsúlyosan szerepel az adatvédelmi audit témája, illetőleg annak igénye, hogy az arra vonatkozó létező módszertanokat felmérjék, és lépéseket tegyenek egy standard módszertan kialakítására. A dokumentum szerint lépéseket kell tenni a létező, de igen heterogén audit-módszertanokat (egyes adatvédelmi hatóságok által végzett audit-tevékenység módszertana, a nagy könyvvizsgáló cégek által végzett adatvédelmi audit, egyes ügyvédi irodák által végzett adatvédelmi audit (nemzeti jognak való megfelelés, illetőleg a Safe Harbor irányelveknek történő megfelelés vizsgálata) felmérése érdekében, számba kell venni azokat a „legjobb

[704] Lásd IPSE – Proposed Topics of Possible Standardization Work;
http://www.cenorm.be/isss/Projects/dataprotection/ipse/itemlist.htm

[705] Jos Dumortier – Caroline Goemans: *Data Privacy and Standardization.* Discussion Paper prepared for the CEN/ISSS Open Seminar on Data Protection, 2000. március;
http://www.law.kuleuven.ac.be/icri/papers/doctrine/cen-paper.pdf.

[706] Initiative on Privacy Standardization in Europe, Final Report, CEN/ISSS Secretariat, Brussels, 2002. Lásd: http://www.cenorm.be/isss/Projects/DataProtection/IPSE/ipse_finalreport.pdf.

gyakorlatokat", amelyek ismerete a többi szereplő számára hasznos lehet, illetőleg meg kell határozni, hogy az adatvédelmi audit mennyiben különbözik a létező biztonsági auditoktól. Meg kell határozni az auditorra vonatkozó követelményeket is: milyen tapasztalat, végzettség, képzettség szükséges az adatvédelmi audit végzéséhez.

1.24.2. Az „Inventory of Data Protection Audit Practices"

1. A célok meghatározása után a CEN/ISSS felügyelete alatt 2005. áprilisában készült el az „Inventory of Data Protection Audit Practices" című dokumentum, amely CEN Workshop Agreement-ként került közzétételre (CWA 15262:2005). Ez a dokumentum a szabványos audit-gyakorlat (standard data protection auditing practice) meghatározása előtt számba vette a már egyes tagállamokban (illetőleg azokon kívül – lásd alább) létező adatvédelmi audit módszertanokat.

A felmérés az alábbiakra terjedt ki:

- *A holland adatvédelmi biztos* által kialakított ún. Co-operation Group Audit Strategy, illetőleg az ennek keretében kidolgozott Privacy Audit Framework. A keretrendszer célja, hogy valamely adatkezelő felmérje, hogy önmaga megfelel-e a holland adatvédelmi törvény rendelkezéseinek. A keretrendszer segítséget nyújt egy audit-terv (audit plan) felállításához, a holland adatvédelmi jog legfőbb jogi kérdéseinek elemzéséhez, illetőleg azon kritikus pontok azonosításához, amelyek áttekintése szükséges a jogi rendelkezéseknek történő megfeleléshez (bejelentés, átláthatóság, célhozkötöttség, jogalapok, adatminőség, jogok, biztonság, adatfeldolgozás, külföldre irányuló adattovábbítás). Maga a keretrendszer nem határozza meg az adatvédelmi rendelkezések kielégítéséhez szükséges adatbiztonsági követelményeket, ám egy kapcsolódó dokumentum mégis ad támpontokat a személyes adatok egyes kategóriáinak meghatározásához, az ezek alapján történő kockázatfelméréshez, és bizonyos intézkedések, eljárások alkalmazását javasolja általános esetben illetőleg érzékenyebb személyes adatok esetén.

- A *Schleswig-Holstein-i Independent Center for Privacy Protection* által kidolgozott „Datenschutz-Behördenaudit" – e rendszert Schleswig-Holstein tartomány közigazgatási szervei számára dolgozták ki, s annak tárgya lehet valamely adatkezelési művelet, valamely közigazgatási szerv meghatározott szervezeti egysége, vagy a közigazgatási szerv keretén

belül végzett valamennyi adatkezelés. Az audit pozitív eredménye esetén a közigazgatási szerv egy tanúsító megjelölés használatára jogosult: az eredményekről az ICPP nyilvántartást vezet.

- A *brit adatvédelmi biztos* által kidolgozott módszertan: ez a módszertan egy ún. compliance audit lebonyolításához ad iránymutatást, illetőleg az ennek során alkalmazható különféle checklist-eket tartalmaz. A célcsoport felöleli az adatkezelőket illetőleg az auditot szolgáltatásként kínáló cégeket is felöleli, így a módszertan igen széles körben használható. A brit adatvédelmi biztos által kidolgozott rendszer megkülönböztet külső és belső auditot (annak megfelelően, hogy az auditot maga az adatkezelő vagy külső szervezet végzi), adequacy és compliance auditot (az első típus során az auditor csupán a szervezet belső szabályozását (policy-k, szabályzatok, szerződések, stb.) vizsgálja, és ezek alapján von le következtetést az adatvédelmi megfelelésre, a második esetben pedig a vizsgálat tárgya az, hogy a szervezet tényleges működése megfelel-e a belső szabályozásban illetőleg szélesebb értelemben az adatvédelmi jogi szabályozásban lefektetett követelményeknek. A brit adatvédelmi biztos szerint a belső audit csupán compliance audit, míg külső személy által végzett audit során elsőként az adequacy auditot, majd a compliance auditot kell elvégezni.

- *A Deutsche Telekom* által használt rendszer: A DT rendszere az adatvédelmi követelmények belső auditálását segíti, elsősorban kérdőíveket és helyszíni vizsgálatokat használva eszközként: a vizsgálat egyrészt a megtett technikai, másrészt a szervezeti, harmadrészt pedig a személyzetet érintő intézkedésekre irányul; végeredményeként minden szervezeti egység (department) egy besorolást kap, amelynek segítségével összehasonlítható, hogy melyik egység felel meg jobban az adatvédelmi jogi illetőleg a belső szabályozásból származó követelményeknek. A végső cél az, hogy a (belső) adatvédelmi felelős a szervezet egészére nézve mélyreható képet kapjon az adatvédelmi követelményeknek való megfelelésről.

- *Az IMS Health* által kidolgozott rendszer olyan audit-módszertan, amely a 95/46/EK irányelv rendelkezéseire épít, ám rugalmas, és bármely helyi leányvállalat számára átalakítható oly módon, hogy a helyi adatvédelmi jog követelményeit tükrözze. A módszertan szintén elsősorban kérdőívekre épít: egyrészt négy „adatfolyam" felmérésére (termékekkel kapcsolatos adatok, beszállítói és fogyasztói adatok, munkavállalói adatok, online adatok) – ebben az esetben a cél az adatkezelések teljeskörű (belső) nyilvántartásba vétele, illetőleg az adatkezelésért felelős személy azonosítása minden adatkezelés esetében. A vizsgálat másik

iránya már a megfelelőség vizsgálatát tűzi ki célul a kritikus területeken, az erre használt kérdőívek a következők: szervezeti és management kérdőív, a személyes adatok kezelésére vonatkozó általános kérdőív, a munkavállalói adatok kezelésére vonatkozó kérdőív, a CCTV (zárt láncú kamerarendszerek) alkalmazására vonatkozó kérdőív, az internethasználattal kapcsolatos kérdőív, illetőleg az intranet használatával kapcsolatos adatvédelmi kérdésekkel kapcsolatos kérdőív.

- Igen figyelemreméltó a dokumentum által szintén elemzett, a *svájci Association for Quality and Management Systems (SQS)* által kidolgozott modell. A rendszer számunkra is lényeges jellegzetessége, hogy mind adatvédelmi, mind adatbiztonsági modult tartalmaz. A „jogi" audit a svájci adatvédelmi jogon alapszik (amely egyébként összhangban van a 95/46/EK irányelvvel), míg az informatikai biztonsági audit az ISO/IEC17799 szabványon. A módszertan harmadik elemet is tartalmaz, az adatvédelmi management rendszer auditját (az ISO 9901 és ISO 14001 alapján). Az auditnak való megfelelés esetén az adatkezelő tanúsító megjelölést használhat.

- A felmérés kiterjedt egyes Európán kívüli kezdeményezésekre is. Ilyen az *American Institute of Chartered Accountants és a Canadian Institute of Chartered Accountants* által közzétett „Privacy Framework". A rendszerre azért volt szükség, hogy a két szervezet által képviselt szakemberek (könyvvizsgálók) számára valamiféle elfogadott mérce álljon rendelkezésre az európai terminológiával adatvédelmi tanácsadásnak nevezhető tevékenységek (privacy strategic and business planning, privacy gap and risk analysis, benchmarking, privacy policy design and implementation, performance measurement, independent verification of privacy controls) végzése során. A CWA szerint a dokumentum – bár természetesen nem tükrözi pontosan a 95/46/EK irányelv követelményrendszerét – figyelemreméltó, mert a meghatározott követelményeket absztrahál, és ezeket példákkal, az auditort segítő magyarázatokkal illusztrálja (a követelményrendszer elemeit a rendszer a következő területekhez rendelve határozza meg: management, értesítés/bejelentés (notice), választás és beleegyezés (Choice and Consent), adatgyűjtés, az adatok felhasználása és tárolása, hozzáférés, harmadik személyeknek történő továbbítás, adatbiztonság, adatminőség, ellenőrzés és végrehajtás). További vizsgált, Európán kívüli módszertan volt az ausztrál adatvédelmi biztos által közzétett Privacy Audit Manual-ban kifejtett rendszer.

2. Az adatvédelmi audit módszertanok számbavétele mellett a CWA 15262:2005 legfőbb

eredménye, hogy azonosítja azokat a területeket, amelyek esetében a szabványosítás elképzelhető, illetőleg kívánatos. Az ezzel kapcsolatban tett főbb megállapítások a következők:

- A szabványosítás során a felmért audit-módszertanokban szereplő valamennyi fél bevonása indokolt, olyan módszertant kell kidolgozni, amelyet mindegyikük (a megbízó, a külső/belső auditor, az auditor véleményét hasznosító „végfelhasználó", illetőleg maga az auditált) használhat.
- A szabványosítás egyik területe kell, hogy legyen az auditor számára előírt követelmények rendszere.
- A szabványosítás során tekintettel kell lenni arra, hogy a rendszert alkalmazó szervezetek rendkívül sokfélék, olyan rendszert kell tehát kidolgozni, amely mind a célok, mind az audit kiterjedése (scope) tekintetében többféle audit végzésére ad lehetőséget.

1.24.3. Az audit módszertan

1. A CWA 15262:2005 publikálását követően 2006. februárjában tette közzé a CEN a személyes adatvédelmi audit módszertant, két részben (CWA 15499-1 illetőleg CWA 15499-2). Az első dokumentum magát az audit módszertant írja le, míg a második a kapcsolódó checklisteket, kérdőíveket, illetőleg űrlapokat tartalmazza.

Mi is az audit? A CWA megfogalmazói a következőképpen foglalják ezt össze:

„Az önértékelés (self-assessment) és az audit közötti lényeges különbség a vizsgáló személy viszonya (attitude) a vizsgálat tárgyához és végeredményéhez. Az auditot független fél végzi, akinek valamely végeredményhez nem fűződik érdeke. Ennek előnye, hogy az audit bizonyosságot (assurance) szolgáltat."[707]

Az adatvédelmi audit két módon teremt bizonyosságot:

- azzal kapcsolatban, hogy a személyes adatok védelméről szóló jogszabályi rendelkezéseknek és egyéb – akár nem jogi – normáknak (pl. szektorális magatartási kódexeknek) való megfelelés biztosított,
- azzal kapcsolatban, hogy az alkalmazott intézkedések és eljárások rendszere mind azok megtervezését, mind fennállását, mind hatékonyságát tekintve megfelelő minőségű ahhoz, hogy az e szabályoknak való megfelelést segítségükkel a szervezet elérje és fenntartsa[708]

Maga a keretrendszer három fő részből áll. Ezek
- iránymutatás (guidance) az audit lefolytatásának módjával kapcsolatban
- az Irányelv alapelveinek való megfeleléssel kapcsolatos követelmények rendszere
- a szervezeti, eljárási és technológiára vonatkozó belső kontrollmechanizmusokkal kapcsolatos követelmények.

Az anyag meghatározott adatkezelési művelet önkéntes (!), a megbízó által kezdeményezett adatvédelmi auditálásának keretrendszere.

[707] CWA 15499-1, 9. o.

[708] CWA 15499-1, 9. o.

Az audit keretrendszer céljai között kifejezetten szerepel az, hogy „abban az esetben, ha valamely szervezet nem rendelkezik országspecifikus audit-módszertannal, akkor ezek a szervezetek az EU keretrendszert alapként használva igazíthatják azt saját adatvédelmi joguk követelményeihez”[709]

2. Az audit folyamata a CWA 15499-1 szerint négy szakaszra (fázisra) tagolható. Ezek: az audit *megbízás* megfogalmazása, kialakítása (formulation); az audit *előkészítése* (preparation); az audit *végrehajtása* (execution) és *audit végeredményének (audit opinion) megfogalmazása*, az erről készülő jelentés megtétele és nyomonkövetése (reporting, follow-up).

Az auditra vonatkozó megbízás körében a dokumentum minimális tartalmi elemeket sorol fel, amelyek a következők:

- a megbízó és a megbízott személye
- a megbízás célja, tárgya
- a megbízás „kontextusa”
- az adatkezelő
- az audit „kiterjedése” (scope), vagyis annak tárgya (az adatkezelési művelet leírása, meghatározása), a vizsgált aspektusok (bizalmasság, integritás, folyamatosság, auditálhatóság), a vonatkozó, a megfelelés alapját jelentő követelményrendszer (vonatkozó adatvédelmi szabályozás, szabványok, legjobb gyakorlatok)
- az audit időtartama
- az audit „mélysége” (depth) (pl. kialakítás (design), az, hogy van-e egyáltalán az adott követelmény érvényesülésére vonatkozó mechanizmus (existence), hatékonyság)
- a célcsoport, az audit végeredményének felhasználója
- a jelentések gyakorisága, formája
- a szükséges időtartam és anyagi források
- a kínált „bizonyosság” szintje (the level of assurance offered)
- az információkhoz való hozzáférésre vonatkozó rendelkezések
- hivatkozás a vonatkozó jogszabályokra
- felelősség korlátozása/kizárása

[709] CWA 15499-1, 10. o.

Ezek az elemek minden további nélkül használhatók magyar jogi környezetben is, természetesen azzal, hogy figyelem előtt kell tartani az adatvédelmi audit egyes részterületeinek sajátos szabályozását (így pl. adott esetben az ügyvédi megbízási szerződésre vonatkozó követelményeket.)

Az auditra történő felkészülés szakaszában kell elkészíteni a CWA 15499-1 szerint az audit-tervet (audit plan). Az audit-terv meghatározása szerint az „azon tevékenységek rendszeres és strukturált leírása, amelyeket az auditornak el kell végeznie annak érdekében, hogy felmérje az adatkezelő szervezet által az adatok megfelelő védelme és az adatkezelés-menedzsment érdekében működtetett intézkedések és eljárások rendszerét, annak tervezését, implementációját és hatékony/folytonos működését".

A dokumentum szerint már ebben a fázisban fontos az adatbiztonsággal kapcsolatos kockázatelemzés is, így a különleges adatok, pénzügyi adatok kezeléséhez kapcsolódó kockázatok felmérése már ebben a szakaszban megtörténik. A kockázatelemzést úgy kell elvégezni, hogy az audit tárgyát kell meghatározott követelményekkel összevetni; ezek a követelmények adatvédelmi audit esetében magából az adatvédelmi szabályozásból (vagyis a jogi és nem jogi normákból), a legjobb gyakorlatokból és szabványokból következnek, illetőleg maga a megbízó és/vagy az auditor által meghatározottak.

3. Az anyag e ponton idézi a 95/46/EK irányelv megfogalmazását, amely szerint „A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás 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 adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének." (17. cikk (1) bekezdés). (Sajnos a magyar adatvédelmi törvénynek az e rendelkezést implementáló szakasza nem, illetőleg csak közvetve utal a kockázatarányos védelemre: 10. § (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek

e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.)

4. Ezzel a problémával már szembesült a jogalkotó korábban, az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal kapcsolatos szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) adatvédelmi rendelkezéseinek megalkotásakor. Az egyik átveendő elv (az adattakarékosság elve) felveti azt a kérdést, hogy a jogi kötelezettség kiterjedjen-e az adattakarékosság elvét érvényre juttató technológia választásának kötelezettségére olyan esetben is, amikor ez a szolgáltatónak többletköltséget okoz. A forrásként szolgáló BDSG szövege szerint akkor köteles az adatkezelő pszeudonim és anonim módon lehetővé tenni a felhasználást, ha „az lehetséges, és az azzal kapcsolatos költség arányban áll az elérni kívánt védelmi céllal". Egy másik, összetettebb megoldás jelenik meg a környezetvédelmi jog által ismert „elérhető legjobb technika" fogalmában (1995. évi LIII. tv. 4. § vb) pont). E fogalom keretében is értékelni kell „az elfogadható műszaki és gazdasági feltételeket" valamint „a költségeket és előnyöket". Külön jogszabályban meghatározott esetekben az elérhető legjobb technológia alkalmazása kötelezettség. Az elérhető legjobb technikához kell hasonlítani az alkalmazandó technológiát a részletes környezeti hatástanulmány kidolgozásakor (1995. évi LIII. tv. 71. §) is.

A probléma lényege tehát az, hogy kockázatelemzéssel kell feltárni azt, hogy az adatok mennyire érzékenyek, és védelmükhöz ehhez képest milyen intézkedések szükségesek. A CWA 15499-1 maga is tartalmaz egy mellékletet, amely a kockázatfelmérés során útmutatóként kíván szolgálni (Risk Assessment & Risk Analysis)[710], ám ezt az általános keretet a magyar keretrendszer esetében a jövőben mindenképp a kezelt adatok jogi tipológiájának megalkotásával kell kitölteni, illetőleg az alkalmazott informatikai biztonsági audit módszertan terminológiájához és módszertanához kell illeszteni. Szerencsére egyes esetekben a jogi környezet e munkához már Magyarországon is ad támpontokat (lásd a Hpt. adatbiztonsági rendelkezéseit).

5. Az adatvédelmi audit harmadik fázisaként határozza meg a dokumentum az audit végrehajtását. E fázis „célja, hogy az auditor megállapításainak alátámasztásához szükséges bizonyítékokat összegyűjtse", és a végeredmény egy „bizonyíték-állomány" (evidence file).

[710] CWA 15499-1, 50. és köv. o.

Az e tevékenység során felhasznált módszerek a következők lehetnek: kikérdezés, dokumentáció és más iratok tanulmányozása, megfigyelés, és automatizált audit-eszközök (szoftverek) igénybevétele. Az evidence file (amely az audit-file része) tartalmazza pl. az interjúkról készített jegyzeteket, az összegyűjtött dokumentumokat, illetőleg minden más rögzített információt, amely az auditor megállapításainak alátámasztására alkalmas. Lényeges, hogy a CWA mind a jogszabályi megfeleléshez (természetesen az Irányelv tekintetében), mind a belső kontrollmechanizmusokra vonatkozóan tartalmaz olyan kérdőíveket, amelyek a magyar jogi környezethez való illesztés után minden további nélkül alkalmazhatók[711], illetőleg kész űrlapokat, mintákat, amelyek a vizsgálat elvégzése során használhatók fel[712].

6. Végül az utolsó fázisok: az auditot lezáról vélemény megfogalmazása, jelentéstétel (reporting) és követés (follow-up). Az auditot lezáró vélemény (audit opinion) nem más, mint „az audit tárgyának a követelmények alapján történő általános értékelése”[713]. A dokumentum szerint a vélemény elkészítését megelőzően azonosítani kell a hibákat (error), és ezeket azok súlya szerint osztályozni kell három kategóriába: (exposure): olyan hiba, amely az adat bizalmasságát, integritását, stb. direkt módon veszélyezteti, vagy jogi eljárás illetőleg negatív publicitás kockázatát hordozza; (concern): olyan hiba, amely még nincs az exposure fázisban, ám egy lépésben azzá fejlődhez, és mielőbb lépéseket kell tenni annak kiküszöbölése érdekében; és (housekeeping): olyan probléma, amely csupán hatékonytalanságot okoz, ám nem fenyegeti a bizalmasságot, integritást, rendelkezésreállást, illetőleg a jogi követelményeknek való megfelelést.

Ezek után kell az audit véleményt audit jelentésbe (audit report) foglalni. Ebben meg kell határozni a követelményeket, és az ezeknek való megfelelésről szóló megállapításokat. Az audit reportnak a dokumentum szerint legalább a következőket tartalmaznia kell:
- címoldal
- vezetői összefoglaló
- tartalomjegyzék
- megbízó és auditor (az auditor aláírásával együtt)
- részletes jelentés:
-- az audit célja

[711] CWA 15499-1, 36-50. o.

[712] CWA 15499-2

-- az audit kiterjedése (scope), így

--- tárgya

--- az aspektusok (bizalmasság, integritás, folyamatosság, auditálhatóság)

--- a követelmények (a 95/46/EK irányelv és más jogszabályok, szabványok, stb. alapján)

-- az audit módszere, megközelítése (approach), és mélysége (depth)

-- dátum

-- az auditra vonatkozó esetleges korlátozások

-- vélemény

-- részletes megállapítások és javaslatok

-- olyan rész, amelyben az auditált, a management, a megbízó, stb. feltüntetheti válaszát, észrevételeit az audit eredményével kapcsolatban.

1.24.4. Jogi követelmények, és azok viszonya a magyar adatvédelmi joghoz

1. Mint fent már említettük, az audit lefolytatására vonatkozó iránymutatáson túl a dokumentum két területen határoz meg követelményeket: egyrészt összegzi a 95/46/EK irányelvből származó jogi kívánalmakat, másrészt pedig a kontrollmechanizmusokkal kapcsolatos követelményeket.

2. Elsőként vizsgáljuk meg a jogi követelményeket. Ezeket a dokumentum táblázatokban összegzi: az alábbi táblázat a CWA 15499-1 azon táblázatának fordítása, amely a 95/46/EK irányelv megfelelő szakaszaihoz rendeli az egyes, az audit során vizsgálandó adatvédelmi követelményeket. A táblázatot kiegészítettük a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) vonatkozó szakaszaival:

Az adatkezelő kötelezettségei:	Az EU irányelv vonatkozó cikkei	Az Avtv. vonatkozó szakaszai	Adatvédelmi alapelv
Megfelelni az adminisztratív kötelezettségeknek az adatvédelmi	18, 19, 20, 21	28-30 §§	Értesítés (Notification)

[713] CWA 15499-1, 19. o.

hatóság előtt (pl. bejelentés)			
Tájékoztatni az adatalanyt az adatkezelésről	10, 11	6. §, 12-13 §§	Átláthatóság
Biztosítani azt, hogy az adatokat csak meghatározott, kifejezett és jogszerű célból gyűjti (illetőleg később használja, továbbítja)	6.1.b	5. § (1) bek., 5. § (4) bek.	Adatminőség – célhoz kötöttség (Purpose limitation)
Csak a szükséges ideig tárolni a személyes adatokat	6.1.e	5. § (2) bek.	Adatminőség - tárolás
Biztosítani azt, hogy az adatok pontosak, és ha szükséges, időszerűek, és azt, hogy az adatkezelési céljára alkalmasak, relevánsak, és azon nem terjeszkednek túl	6.1.c, d	5. § (2) bek., 7. §(1) bek.	Adatminőség - arányosság
Tiszteletben tartani az adatalanyok jogait	12, 13, 14, 15	11-16/A §§	Az adatalany jogai
Biztosítani azt, hogy az adatkezelés tisztességes, és a személyes adatok kezeléséhez megfelelő jogalap áll rendelkezésre	6.1.a, 7	3. §	Jogszerű adatkezelés
Megtenni azokat a technikai és szervezési intézkedéseket, amelyek arányosak az adatkezeléshez kapcsolódó kockázattal (az adatok véletlen megsemmisülését, illetőleg azok jogosulatlan megsemmisítését, megváltoztatását, nyilvánosságra hozatalát vagy az azokhoz történő	16, 17.1	10. §, 4/A §	Biztonság és bizalmasság (Security and Confidentiality)

hozzáférést illetően) Biztosítani azt, hogy bármely, az adatkezelő ellenőrzése alatt működő személy (így az adatfeldolgozó is) csak az adatkezelő utasításai alapján, azoknak megfelelően végez adatkezelési cselekményeket			
Az adatkezelő lehetőségei:	Az EU irányelv vonatkozó cikkei	Az Avtv. vonatkozó szakaszai	Adatvédelmi alapelv
Különleges adatok és/vagy nemzeti azonosító számok vagy általános jellegű azonosító jelek kezelése; ha megengedett, az adatkezelőnek biztosítania kell, hogy az adatkezeléshez rendelkezésre áll a megfelelő jogalap	8	Korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos (7. § (1) bek.; egyébként lásd az 1996. évi XX. törvényt	Jogszerű adatkezelés – különleges adatok
Adatkezelési műveletek kiszervezése; ilyen esetben az adatkezelőnek biztosítania kell. hogy az ellenőrzése alatt működő személy kizárólag az általa adott utasítások szerint dolgozza fel a személyes adatokat.	16, 17.2/3/4	4/A §	Biztonság és bizalmasság - adatfeldolgozás
Automatizált döntések meghozatala; ilyenek esetében az adatkezelőnek biztosítania kell, hogy rendelkezésre álljon a megfelelő jogalap, valamint hogy	15	9/A §	Az adatalany jogai

az adatalany megvitathassa az automatizált egyedi döntés eredményét azon fél képviselőjével, amely a döntést hozta, vagy egyébként kifogással élhessen ennél a félnél			
Adattovábbítás harmadik országba; ilyen esetén az adatkezelőnek biztosítania kell, hogy megfelelő intézkedések biztosítsák a harmadik országban a továbbított adatok jogszerű kezelését.	25, 26	9. §	Harmadik országba történő adattovábbítás

3. A dokumentum a továbbiakban szintén táblázatban részletezi a fenti adatvédelmi követelményeket, az alábbiak szerint:

#	Követelmények
	Adatminőség
1-a	Személyes adat csak tisztességes, meghatározott, kifejezett és jogszerű célból gyűjthető
1-b	A személyes adat kezelése csak e céloknak megfelelően történhet, és/vagy további adatkezelés nem történhet e célokkal összeegyeztethetetlen célból
2	A személyes adatok a gyűjtés és további adatkezelés alapjául szolgáló cél elérésére alkalmasak, relevánsak, és azon nem terjeszkednek túl
3-a	A személyes adatok pontosak, és ahol szükséges, időszerűek
3-b	Azon adatok tekintetében, amelyek pontatlanok vagy nem teljesek a gyűjtés és feldolgozás alapjául szolgáló adatkezelési cél eléréséhez, az adatkezelő megteszi az elvárható intézkedéseket a törlés/helyesbítés érdekében
4	Az adatokat olyan formában tárolják, amely az adatalanyok azonosítását csak az adatgyűjtés és további feldolgozás alapjául szolgáló cél eléréséhez szükséges mértékben és ideig teszi lehetővé az adatalanyok azonosítását
	Jogszerű adatkezelés
5	Az adatok kezelése tisztességes és jogszerű (törvényes) abban az esetben, ha arra valamely alábbi esetben kerül sor:
	• Az adatalany az adatkezeléshez egyértelműen hozzájárult
	• Az adatkezelés valamely olyan szerződés teljesítéséhez szükséges, amelyben az adatalany fél, illetőleg az adatalany kívánságára ilyen szerződés

	kötését megelőző lépések megtételéhez szükséges
	• Az adatkezelés valamely az adatkezelő számára jogszabályban előírt kötelezettség teljesítéséhez szükséges
	• Az adatkezelés az adatalany létfontosságú érdekeinek védelme céljából szükséges
	• Az adatalany valamely közérdeket szolgáló cél teljesítéséhez vagy az adatkezelőre vagy azon harmadik félre ruházott hatáskör gyakorlásához szükséges, amely számára az adatot hozzáférhetővé teszik
	• Az adatkezelés az adatkezelő vagy az adatokat megkapó harmadik fél vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezen érdekeknél magasabb rendűek az adatalany alapvető jogai és szabadságai
	Különleges (érzékeny) adatok kezelése
6	Kezelnek különleges adatot?
Ha igen	Az adatkezelés jogszerű abban az esetben, ha az alábbiak közül egy vagy több feltétel teljesül:
	• Az adatalany az adatkezeléshez egyértelműen hozzájárult
	• Az adatkezelés az adatkezelő kötelezettségei és meghatározott jogai gyakorlása érdekében szükséges a munkajog területén, amennyiben a megfelelő biztosítékokról szóló nemzeti jogszabályok azt lehetővé teszik
	• Az adatkezelés az érintett vagy más személy létfontosságú érdekeinek védelméhez szükséges abban az esetben, ha az érintett fizikailag vagy jogilag képtelen a hozzájárulását adni
	• az adatkezelés valamely alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő biztosítékok mellett végzett törvényes tevékenysége keretében történik, politikai, világnézeti, vallási vagy szakszervezeti céllal, azzal a feltétellel, hogy a feldolgozás 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
	• az adatfeldolgozás olyan adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott, vagy amelyek jogi követelések megállapításához, gyakorlásához vagy védelméhez szükségesek

#	Követelmények
	• Ha az adatok kezelése megelőző egészségügyi, orvosi diagnosztikai célból, gondozás vagy kezelés nyújtása vagy egészségügyi szolgáltatások igazgatása céljából szükséges, és ha az adatokat a nemzeti jog vagy az illetékes nemzeti testületek által meghatározott szakmai titoktartási kötelezettség alá eső egészségügyi szakember vagy azzal egyenértékű titoktartási kötelezettség alá eső más személy kezeli
	• A nemzeti adatvédelmi jog vagy a felügyelő hatóság határozata által meghatározott kivételek esetében
De:	A bűncselekményekre, büntetőítéletekre vagy biztonsági intézkedésekre vonatkozó adatok kezelése kizárólag a hatóság ellenőrzése mellett történhet
	A nemzeti azonosító számok és egyéb általános jellegű azonosító jelek kezelése
7	Kezelnek nemzeti azonosító számot vagy egyéb általános jellegű azonosító jelet?
Ha igen :	Az adatkezelés csak akkor megengedett, ha az megfelel az alkalmazandó helyi adatvédelmi jognak.
	Átláthatóság

8	Az adatalanyt megfelelően tájékoztatják:
	Az adatok adatalanytól való felvétele során:
8-a	Az adatfelvételt megelőzően az adatalanyt tájékoztatni kell a következő információkról:
	• az adatkezelő személye, és ha van, képviselője
	• az adatok kezelésének célja
	• bármely további információ, így például:az adatok címzettjei, illetve a címzettek kategóriái, az hogy a kérdések megválaszolása kötelező vagy önkéntes, továbbá a válaszadás elmulasztásának lehetséges következményei, betekintési jog és az érintettre vonatkozó adatok helyesbítéséhez való jog,amennyiben e további információk
	Ha az adatot nem az adatalanytól veszik fel:
8-b	A a személyes adatok felvételének elvállalásakor, illetve, ha az adatokat harmadik személyhez szándékoznak továbbítani, legkésőbb az adatok első közlésekor az érintettel legalább az alábbi információkat kell közölni, kivéve, ha az érintett már rendelkezik ezekkel az információkkal:
	• az adatkezelő, vagy ha van ilyen, képviselőjének személye
	• az adatkezelés célja
	• bármely egyéb információ, mint például: az érintett adatok kategóriái, az adatok címzettjei vagy a címzettek kategóriái, betekintési jog és az érintettre vonatkozó adatok helyesbítéséhez való jog
	Abban az esetben, ha az adatalanyt nem tájékoztatják a meghatározott információkról (statisztikai célú vagy a történelmi, vagy tudományos célú adatkezelés esetében, ha a kérdéses információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel, illetve ha a rögzítést vagy a közlést jogszabály kifejezetten előírja):

8-c	Az adatkezelő megtette a szükséges intézkedéseket, így pl. biztosítja, hogy az adatokat csak tudományos illetőleg statisztikai célból kezeljék, és/vagy rögzíti a releváns szabályozást és/vagy rögzíti az adatok forrását
	Az adatalany jogai
9	Az adatkezelőnek megfelelő szervezési intézkedésekkel biztosítania kell a hozzáférés jogát. Ezeknek az intézkedéseknek biztosítaniuk kell, hogy túlzott késedelem vagy költség nélkül
	• Megállapítható legyen az adatkérő (adatalany) személyazonossága
	• Az adatalanyt informálják, hogy kezelnek-e rá vonatkozó adatot vagy sem
	• Az adatalanyt informálják legalább az adatkezelési célról, a kezelt adatok fajtáiról, és azon címzettek személyéről vagy fajtáiról, akik az adatokat megkapják

#	Követelmények
	• Az adatokat érthető formában kell közölni
	Automatizált egyedi döntés (lásd alább a 13. pontban is) esetén:
	• Az adatalanyt tájékoztatni kell az adatok automatizált kezelése során alkalmazott logikáról
10	Az adatokat ésszerű időn belül és túlzott költségek nélkül kell közölni
11	A hozzáférési kérelmet követheti helyesbítési, törlési vagy zárolása iránti kérelem. Az adatkezelőnek szervezési intézkedésekkel biztosítania kell, hogy

	• Ezen kérelmekkel megfelelő módon foglalkoznak
	• Értesítsék azon harmadik feleket bármely helyesbítésről, törlésről vagy zárolásról, amelyeknek az adatot továbbították, hacsak ez lehetetlennek nem bizonyul, vagy aránytalanul nagy erőfeszítést nem igényel
12	Az adatkezelőnek megfelelő szervezési intézkedésekkel biztosítania kell a tiltakozási jog érvényesíthetőségét. Ezek az intézkedések garantálják, hogy:
	• Az adatalany által kifejezett tiltakozást megfelelően értékelik (vajon a tiltakozás alátámasztja-e az adott körülmények között kényszerítő jogi érdek) és azzal megfelelő módon foglalkoznak
	• Az adatalany számára kifejezetten felajánlják a költségmentes tiltakozás jogát adatainak közvetlen üzletszerzés céljából történő kezelése ellen
	• Az adatalany számára kifejezetten felajánlják a költségmentes tiltakozás jogát az adatok harmadik személyeknek első alkalommal történő közlése, vagy a nevükben közvetlen üzletszerzés céljára történő felhasználás előtt
13	Az adatkezelőnek megfelelő szervezési intézkedéseket kell tennie az adatalany azon jogának érvényesítése érdekében, hogy ne terjedhessen ki rá olyan döntés hatálya, amely rá nézve jogi hatással járna, vagy őt jelentős mértékben érintené, és amely kizárólag automatizált adatkezelésen alapul, és amelynek célja a rá vonatkozó egyes olyan személyes szempontok kiértékelése, mint például a munkahelyi teljesítmény, a hitelképesség, a megbízhatóság, az életvitel, stb.
	Bizalmasság és biztonság
14	Az adatkezelőnek meg kell tenni azokat az intézkedéseket, amelyek az azonosított kockázatokat és az adatkezelés jellegét tekintve biztosítják az adatok bizalmasságát (titkosságát) és biztonságát. Az intézkedések a következők:

	• Biztonsági szabályzat (security policy) és biztonsági terv (security plan) készítése és az ezeket átültető eljárások és intézkedések implementációja
	• A biztonsági kérdések tudatosítása (Security awareness)
	• Személyzeti követelmények
	• A munkahely kialakítása (pl. annak érdekében, hogy a bizalmas adatok illetéktelen megfigyelése ne legyen lehetséges)
	• Az ICT infrastruktúrával kapcsolatos nyilvántartási és osztályozási feladatok
	• Hozzáférés management
	• Hálózatok és külső kapcsolatok
	• Szoftverhasználat rendje
	• Adatok tömeges feldolgozása
	• Adattárolás
	• Adattörlés (ideértve az elektronikus törlést és a fizikai hordozó megsemmisítését/eltávolítását)
	• Kontingenciaterv (Contingency plan)
	• Személyes adatok feldolgozásának kiszervezése
	Harmadik fél által végzett adatfeldolgozás?
15	…ha a személyes adatok feldolgozását (adatkezelési műveletek végrehajtását) harmadik félre bízzák

#	Követelmények
Ha igen:	Az adatkezelőnek olyan adatfeldolgozót kell választania, amely a technikai biztonsági intézkedések és az elvégzendő adatfeldolgozásra vonatkozó szervezési intézkedések tekintetében megfelelő garanciákat nyújt
És:	Az adatkezelő és adatfeldolgozó között szerződéses viszonynak kell fennállnia. A szerződésnek szabályoznia kell a következőket:

	• az adatfeldolgozó kizárólag az adatkezelő utasítása alapján járhat el
	• a feldolgozás biztonságával kapcsolatos technikai és szervezési intézkedések megtételére vonatkozó kötelezettségeket
	• azt, hogy a feldolgozó ellenőrzése alatt álló, a személyes adatokhoz hozzáférő bármely személy, illetőleg maga az adatfeldolgozó is kizárólag az adatkezelő utasításainak megfelelően dolgozhatja fel az adatokat, kivéve, ha jogszabály ettől eltérően rendelkezik
És:	Az adatkezelő biztosítja azt, hogy az adatfeldolgozó e követelményeknek az alábbi (a) vagy (b) módon tesz eleget:
	(a) Az adatkezelő (vagy annak megbízásából valamely független fél) rendszeresen ellenőrzi a szerződésnek illetőleg az adatfeldolgozásra vonatkozó jogszabályi rendelkezéseknek megfelelő működést
	(b) Az adatfeldolgozó rendszeresen független külső auditor által készített vizsgálati jelentést bocsát az adatkezelő rendelkezésére a szerződésnek illetőleg az adatfeldolgozásra vonatkozó jogszabályi rendelkezéseknek megfelelő működésről
	Bejelentés (ideértve az előzetes ellenőrzést is)
16	Az adatkezelő meghatározta az adatkezelési művelet tulajdonságait és azt, hogy a felügyelő hatóságnak az adatkezelést be kell-e jelenteni.
	• Amennyiben az adatkezelési művelet kivételi körbe esik, a kivételi kört rögzíteni kell, és vissza kell igazolni, hogy azt helyesen alkalmazták.
	• Amennyiben az adatkezelési műveletet be kell jelenteni, a bejelentésben foglalt információnak pontosnak, teljesnek és időszerűnek kell lennie.
17	Rendszeres időközönként, illetőleg az adatkezelési művelettel kapcsolatos bármely változást követően felül kell vizsgálni azt, hogy a kivételi kör adott

	esetben történő alkalmazása változatlanul helyénvaló-e, illetőleg a bejelentésben foglalt információ a továbbiakban is pontos-e.
18	Megállapítást nyert (a helyi adatvédelmi jog alapján), hogy szükséges-e az adott adatkezelési művelet vonatkozásában annak megkezdése előtt a felügyelő hatóság előzetes ellenőrzését kérni. Ha az előzetes ellenőrzés szükséges, erről a bejelentést/az adatkezelési művelet megkezdését megelőzően gondoskodtak.
	Harmadik országba történő adattovábbítás
19	Személyes adat nem továbbítható az Európai Unión kívüli államba, kivéve, ha az alábbi feltételek közül egy (vagy több) teljesül (a, b, vagy c):
	(a) Az illető állam megfelelő szintű védelmet biztosít
	(b) vagy: az illető állam nem biztosít megfelelő szintű védelmet, ám valamely alábbi feltétel (vagy azok közül több) teljesül:
	• az adatalany egyértelműen hozzájárult a javasolt továbbításhoz
	• a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges
	• a továbbítás az adatkezelő és valamely harmadik fél közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges
	• a továbbítás fontos közérdekből vagy jogi követelések létrejötte, érvényesítése vagy védelme miatt szükséges, illetve azt jogszabály írja elő;
	• a továbbítás az érintett létfontosságú érdekeinek védelme miatt szükséges;
	• 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.
	(c) Vagy: a helyi felügyelő hatóság engedélyezte a megfelelő védelmet nem nyújtó harmadik országba történő adattovábbítást azon az alapon, hogy a megfelelő védelem szintje egyéb módon biztosított

A fenti követelmények az Irányelv rendszerének megfelelően, kellő részletességgel határozzák meg az abból eredő követelményeket. Ugyanakkor nem szabad megfeledkezni arról, hogy az Avtv. egyes esetekben eltér az Irányelv rendelkezéseitől, egyes irányelvi szabályokat kifejezetten problémásan implementálva, másrészt az Avtv. szabályaihoz olyan jogértelmezési anyag kapcsolódik, amelynek figyelembe vétele az audit során nélkülözhetetlen. További feladatot jelent az egyes szektorális szabályozásokból (Hpt., Eatv., stb.) adódó többletkövetelmények összefoglalása és beemelése a módszertanba.

4. Csupán példaként emeljük ki az adatfeldolgozás intézményének a magyar jogban az Irányelvtől eltérő értelmezését, amely a fenti táblázatban 15. számmal jelzett követelményhez kapcsolható. Az Avtv. vonatkozó szakasza szerint „*adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől” A fogalomhoz igen széleskörű adatvédelmi biztosi gyakorlat tartozik. Az adatfeldolgozás fogalmát – az adatfeldolgozó meghatározásával együtt – egy 1999. évi módosítás vezette be az Avtv. szövegébe, majd a 2003. évi novella módosította. A módosítás igényét az teremtette meg, hogy korábban az Avtv. nem ismerte azt az alanyt, akit az adatkezelő az adatkezelés során megbízottként igénybe vehet, akinek speciális szakértelmét az adatkezelés folyamatába bevonhatja,[714] méghozzá oly módon, hogy ahhoz további jogalap (az érintett hozzájárulása vagy törvényi felhatalmazás) nem szükséges [szükséges azonban az érintett tájékoztatása – lásd a 6. § (2) bekezdését].

[714] Az adatvédelmi biztos ezt már korán érzékelte, és éves beszámolóiban szorgalmazta a fogalom bevezetését: ABI 1997, 14; ABI 1997, 50; ABI 1998, 28 stb.

Az alany (az adatfeldolgozó) fogalmának a törvénybe való bevezetésével egyidejűleg a jogalkotó – eltérve az irányelv definíciórendszerétől – szükségét látta az adatfeldolgozó által végzett tevékenység meghatározásának is, amely az adatvédelmi biztos leszűkítő jogértelmezésén és annak a 2003. évi novellára történő hatásán keresztül oda vezetett, hogy mára az adatfeldolgozó tevékenységi köre a magyar jogban igen szűken behatárolt.

Az adatfeldolgozás csak az adatfeldolgozással kapcsolatos technikai művelet lehet. A személyes adaton végzett bármely művelet adatkezelésnek minősül (lásd az Avtv. 2. § 9. pontjához fűzött kommentárt), ezért nehéz az adatkezelési művelet (például törlés, továbbítás) és az azzal kapcsolatos „technikai művelet" (törlés, továbbítás) elhatárolása. Van-e olyan művelet, amely az adatkezelés körébe tartozhat-e, ám az adatfeldolgozás körébe nem? Van-e olyan adatfeldolgozási művelet, amely egyben ne minősülne adatkezelési műveletnek is? Álláspontunk szerint nincs: a két fogalom – még a 2003. évi novella által történt módosítás után is – azonos terjedelmű. (Ez az álláspont ellentmond az adatvédelmi biztosi gyakorlatban kialakult értelmezésnek – lásd alább.) Az elhatárolás az alanyok szerint, az adatkezelő és az adatfeldolgozó fogalmának megkülönböztetésével történhet: míg az adatkezelőnek joga van az adatkezelési/feldolgozási műveletek céljának meghatározására és az adatkezelésre/adatfeldolgozásra vonatkozó döntések meghozatalára, addig az adatfeldolgozó a magyar jog szerint ilyen döntéseknek csak végrehajtója lehet. További értelmezési kérdést jelent, hogy az adatkezelő és az adatfeldolgozó közötti adatforgalom törvényen (magán az Avtv. rendelkezésén) alapuló adattovábbítás-e (az Avtv. korábbi szabályozása alapján, amely a harmadik személy fogalmát nem határozta meg, álláspontunk szerint ez volt a helyes értelmezés), vagy nem is minősül adattovábbításnak. A 2. § 10. pontjának (adattovábbítás) és a 2. § 16. pontjának (harmadik személy) együttes értelmezése alapján a 2003. évi novellát követően az adatfeldolgozónak történő „továbbítás" nem adattovábbítás az Avtv. szerint. Ez nem érinti a 9. § alkalmazását külföldi adatfeldolgozónak történő továbbítás esetén.

Az adatfeldolgozás fogalmához széleskörű adatvédelmi biztosi gyakorlat kapcsolódik, és az Avtv-ben további, kifejezetten a magyar szabályozásra vonatkozó korlátok találhatók. A magyar szabályozásra jellemző többletkorlátozások az adatfeldolgozási tevékenységgel kapcsolatban az alábbiak:

– az adatfeldolgozói tevékenység kör szűk meghatározása (lásd részletesen fent);

– az adatfeldolgozóként igénybe vehető alanyok körének meghatározása [Avtv. 4/A. § (4) bekezdése];

– az adatfeldolgozó adatfeldolgozó általi igénybevételének tilalma [Avt. 4/A. § (2) bekezdése];

– az adatfeldolgozó által saját célból végzett adatfeldolgozás tilalma [Avt. 4/A. § (3) bekezdése].

E példából is látszik, hogy – bár a követelményrendszer jól definiálható és logikusan felépíthető – a gyakorlatban a jogi követelmények teljeskörű felmérése igen nagy gyakorlatot igényel (ezért az adatvédelmi audit e moduljának/fázisának végzése célszerűen jogi végzettséghez, illetőleg esetlegesen megfelelő tanfolyam elvégzéséhez kötendő).

1.24.5. A kontrollmechanizmusokkal kapcsolatos követelmények

1. A kontrollmechanizmusokkal kapcsolatosan a dokumentum az alábbi táblázatban szereplő – álláspontunk szerint minden további nélkül adoptálható – követelményeket határozza meg:

#	Követelmények
	Szervezet
1	A szervezeti struktúra hatákony és átlátható, támogatja az adatvédelmi jogi követelményeknek történő megfelelés képességét és a szervezet saját adatvédelmi céljait
	Eljárás
2	A szervezet olyan adatvédelmi rendszerrel (data protection system) rendelkezik, amely biztosítja, hogy az adatvédelmi célokat meghatározzák, azokat ismerik és azok iránt elkötelezettek, az azoknak megfelelő intézkedéseket meghozzák, azok érvényesülését ellenőrzik és értékelik, és azt, hogy az adatvédelmi problémákat lehetőség szerint megelőzik, illetőleg azok felmerülése esetén megfelelő módon kezelik
	Technológia
3	A technológia nem a személyes adatok védelme és biztonsága ellenében hat,

	hanem azt elősegíti

A harmadik generációs adatvédelmi szabályozás és az informatikai rendszerek bizalmasságához és integritásához fűződő alapjog

1.25. A harmadik generációs adatvédelmi szabályozás

1. A harmadik generációs adatvédelmi szabályozás a fenti kihívásokra kíván – egyelőre megjósolhatatlan eredménnyel – válaszokat találni; új elvek (adattakarékosság), új intézmények (adatvédelmi audit) merülnek fel az irodalomban, kerülnek be a szabályozásba. A mindent átható informatizáltságra válaszképpen visszatér a technológiára irányuló szabályozás is: a cél a technológia formálása.

2. A harmadik generációs adatvédelmi szabályozáshoz sorolható normák közül az első az 1997-ben megalkotott német Teledienstedatenschutzgesetz (TDDSG). A TDDSG forradalmian új intézményeket és elveket vezetett be a német adatvédelmi jogba. Ezen elvek jelentőségét bizonyítja az is, hogy néhány év elteltével azok közül egyesek a szövetségi adatvédelmi törvény szabályai közé kerültek át. A TDDSG megalkotása óta ráadásul széles körű jogalkalmazási tapasztalat halmozódott fel, amely nyomán a jogszabály egyes rendelkezéseit módosították 1999-ben és 2001-ben.

A TDDSG már 1997-ben tartalmazta azt az alapelvet, amely szerint a távszolgáltatást nyújtónak olyan technikai eszközöket kell használnia, amelyek működtetése nem jár személyes adatok kezelésével, illetve a lehető legkevesebb személyes adat kezelésével jár, sőt, e szempontokat már az eszközök tervezésekor is figyelembe kell venni[715] – ez a rendelkezés egy módosítás nyomán a szövetségi adatvédelmi törvénybe is bekerült (az ún. „adattakarékosság elve").[716]

A szövetségi adatvédelmi törvényben szabályozott adatvédelmi audit intézményének lényege, hogy az adatkezelést végző eszközök előállítói és használói adatvédelmi- és adatbiztonsági szempontból független szervezetekkel auditáltathatják eljárásrendjüket, illetve eszközeiket.[717] Az intézmény a környezetvédelmi audit már az uniós joganyagban is

[715] TDDSG 3. § (4).

[716] BDSG 3. §.

[717] Lásd BDSG 9. §. Az intézmény 1997-ben jelent meg a Tartományközi Médiaegyezményben (Mediendienste Staatsvertrag 17. §).

megjelenő példáját követi.[718] A BDSG 9 a §-a szerint az audit célja az adatvédelem és az adatbiztonság javítása:

„*Az adatvédelem és adatbiztonság javítása végett az adatfeldolgozó rendszerek és programok előállítói, valamint az adatfeldolgozó szervek adatvédelmi koncepciójukat és technikai berendezéseiket független és engedéllyel rendelkező szakértőkkel megvizsgáltathatják és értékeltethetik, a vizsgálat eredményét pedig nyilvánosságra hozhatják. A vizsgálattal és az értékeléssel kapcsolatos közelebbi követelményeket, az eljárást, illetve a szakértők kiválasztásának és engedélyezésének szabályait külön törvény szabályozza"*

Az audit tárgya az adatfeldolgozó rendszerek és programok előállítóinak, valamint az adatkezelő szerveknek az adatvédelmi koncepciója (rendszer-audit) és technikai berendezései (eszköz-audit). Az audit és az eredmény nyilvánosságra hozatala önkéntes. Az auditálást független és engedéllyel rendelkező szakértők végzik. A BDSG a vizsgálat és értékelés közelebbi szempontjainak, az eljárásnak, illetve a szakértők kiválasztásának és engedélyezésének szabályait külön törvényben rendeli szabályozni. Az eredeti német koncepció (Roßnagel) szerint az audit tárgya minden esetben a törvényi megfelelésen felüli standardoknak (legjobb gyakorlatoknak) történő megfelelés, ám a gyakorlatban az audit inkább az adatvédelmi biztosi gyakorlat által értelmezett törvényi rendelkezéseknek történő megfelelés szintjére terjedhet ki (lásd részletesebben alább). Erre is van németországi példa: figyelmet érdemel az a kezdeményezés, amely az (online szolgáltatásokra kidolgozott) audit során *protection profiles*-re épít, amely a következő elemekből épül fel:: az online szolgáltatások általános összetevőinek meghatározása, az adatvédelmi követelmények operacionalizálása a szolgáltatás összetevői szerint, értékelési raszter előállítása, súlyozás a szolgáltatás összetevői és az adatvédelmi követelmények alapján, az eredmény megállapítása. Az adatvédelmi követelményeket e rendszer a következőkben összegzi: átláthatóság, a szolgáltató megjelölése, adatvédelmi nyilatkozat, termékleírás, az anyagi jogi szabályok megtartása, felelősség, szükségesség, célhoz kötöttség, hozzájárulás, törlés, zárolás, ágazati törvényben előírt kötelezettség, adat-takarékosság, technikai és szervezeti biztonsági intézkedések, az érintettek jogainak védelme. Az audit részletes szabályozása Németországban tartományi szinten (Schleswig-Holstein) történt meg.

[718] Lásd erről Flemming Moos: Datenschutz im Internet. In Kröger–Gimmy 2000, valamint Ewer 2002.

3. A harmadik generációs adatvédelmi szabályozás elemei már a magyar adatvédelmi jogban is megjelentek. A hazai szabályozásban a jogalkotó tudatosan követte a TDDSG és a BDSG megfelelő példáit az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2003-as módosításakor. A törvény a módosítás nyomán rögzíti az adattakarékosság elvét.[719] Az adattakarékosság elve több, mint az Avtv. 5. § (2) bekezdésében meghatározott alapelv, mert az adatkezelővel szemben azt a kötelezettséget állítja fel, hogy az már az adatkezelés megkezdése előtt szempontként érvényesítse a személyes adatok kezelésének – ha ez lehetséges – elkerülését, illetve az adatkezelés terjedelmének a lehető legkisebb mértékűre szorítását. A követelmény az üzemeltetésre is kiterjed, azaz például megsérti ezt az alapelvet az az adatkezelő is, amely valamely szoftver- vagy hardvereszközt úgy konfigurál, hogy annak működése a szolgáltatás nyújtásához vagy a törvényben meghatározott egyéb cél teljesüléséhez szükséges mértéken túl személyes adatok kezelését eredményezi. Ez a szabály a jogalkalmazónak a korábbinál jobb lehetőségeket teremt az adatvédelmet szolgáló techológiák alkalmazásának ösztönzésére.

Bekerült a szövegbe – szintén a TDDSG mintájára – az a szabály, amely a szolgáltató adatkezelési lehetőségeit monopolhelyzete esetén korlátozza, míg valós piaci viszonyok között módot ad a szolgáltatás nyújtásától eltérő célú adatkezelésre.[720] A rendelkezés a hozzájáruláson alapuló adatkezelésekkel kapcsolatos visszaéléseket zárja ki abban az esetben, ha a szolgáltatás más szolgáltatótól (az adott igénybe vevő által) nem vehető igénybe. A szabályozás ezen túl engedi az információs önrendelkezési jog érvényesítését, és nem tiltja a hozzájáruláson alapuló adatkezeléseket.[721]

---

[719] A 13/A. § (3) bekezdése szerint: „A szolgáltató – a (2) bekezdésben foglaltakon túlmenően – a szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A szolgáltatónak az egyéb feltételek azonossága esetén úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig."

[720] A 13/A. § (8) bekezdése szerint: „Az információs társadalommal összefüggő szolgáltatás nyújtása nem tehető függővé az igénybe vevőnek valamely (1)–(3) bekezdésében nem említett célból történő adatkezeléshez való hozzájárulásától, amennyiben az adott szolgáltatás más szolgáltatótól nem vehető igénybe."

[721] Megjegyzendő, hogy a jogszabály-előkészítők – közöttük szakértőként a szerző – tudatosan nem javasolták az adatvédelmi audit intézményének átvételét a magyar szabályozásba a német tapasztalatok hiánya miatt (lásd erre például Vossbein 2002).

1.26. Az adatvédelmi jog meghaladása?

1. Még nem mérhető fel annak a fejleménynek a jelentősége a magyar adatvédelmi jog és alkotmánybírósági gyakorlat szempontjából, hogy a német Alkotmánybíróság 2008-ban – a magánszféra alapjogi védelmét az digitalizált világban még az információs önrendelkezési joggal együtt is hézagosnak ítélve - új, az informatikai rendszerek bizalmasságának és integritásának védelméhez fűződő alapjogot vezetett le az alaptörvény általános személyiségi jogot deklaráló szakaszából[722]. A jogfejlesztés tehát érzékenyen reagál az információs társadalom kihívásaira, és a magánszféra védelmének új szabályozási eszközei jelennek meg keresi mind az adatvédelmi jogon belül - harmadik generációs adatvédelmi szabályozásként - mind azon kívül. Az új technológiák formálta új környezet a magánszféravédelem innovatív megújítását kívánja; egyébként „olyan észrevétlenül fogy el a szabadság, ahogy a tiszta víz és a levegő elfogyott”[723].

[722] BVerfG, 1 BvR 370/07 vom 27.2.2008.

[723] Sólyom 1988b, idézi Majtényi is: ABI 2001, 14.

English summary – Generations of data protection law and assessment of a second generation data protection regime

2. History of data protection – A brief summary

1. Data protection is a type of privacy protection manifesting in special legal regulation. Data protection rights ensure a person the right of disposal over all data in connection with his personality. This way it serves to sustain the protection of privacy in a world where the possibility of collecting, storing and conciliation of large pools of data is widely available. In this situation, the significance of facts and data that were previously regarded as irrelevant by legislation (that is, regarded as not belonging to the scope of individual secrets) increases: earlier, due to the lack of highly developed data-processing technologies, no threat was imposed by a situation in which these data became public and known to others, while today processing, conciliation and association of data or creating new data relying on the old ones might result in the infringement of the right of privacy. The underlying notion behind the codification of data protection law is the insufficiency of secrecy protection: within the new context, protection should apply to all data: "data protection should be differentiated from the interpretation of privacy as intimacy."[724]

Thus, the object of protection– *personal data* – is new; its aim, however, is the same as it was for secrecy protection, similar to the aim of other extra-legal tools for protecting privacy or intimacy. Before treating the issue of data protection as a specific right, it is necessary to define the goal and interest to be protected: what is protected under data protection rights by data-processing regulations?

The aim of data protection law is the *protection of privacy*. The protection of personal data within the new circumstances can offer the protection of privacy. These statements are true, however, they say little about *what* privacy *is* and *why* it needs protection.

2. Various definitions have been proposed for "privacy". According to Schoeman, privacy has been regarded

[724] Sólyom 1988a, 55.

– as a claim, entitlement or right of an individual to determine what information about himself or herself may be communicated to others;

– as the measure of control an individual has over information about himself, intimacies of personal identity, or who has sensory access to him;[725]

– as a state or condition of limited access to a person, information about him, intimacies of personal identity.[726]

Westin points out that "virtually all animals seek periods of individual seclusion or small-group intimacy. This is usually described as the tendency toward territoriality, in which an organism lays private claim to an area of land, water or air and defends it against intrusion by members of its own species."[727] Likewise, distance-setting mechanisms can be detected in the animal world; non-contact animals keep a certain distance between them, which has been called "personal distance", while within species "social distance" can be measured between groups set off from each other. If the territory accessible to an individual shrinks below the critical level, aggression becomes more sadistic, and "disruption of social relationships through overlapping personal distances aggravates all forms of pathology within a group and causes the same diseases in animals that overcrowding does in man – high blood pressure, circulatory diseases, and heart disease."[728]

Based on anthropological research, Westin states the following about the appearance of privacy in human societies: "our contemporary norms of privacy are 'modern' and 'advanced' values largely absent from primitive societies of the past and present."[729] Westin differentiates among several aspects of privacy that are characteristic of all human beings living in a society. These are primarily norms concerning privacy on the individual level, the level of family/household and the larger community. According to the results presented by Westin, privacy norms are established in each of these three areas, but they vary significantly. Westin regards as a special aspect of privacy "[t]he ways in which human beings perceive their

[725] Cf. Sólyom 1983, 315.: "The common characteristic of different understandings of privacy is the physical and psychological terrirory which is controlled by the individual, which, as a consequence, is free of external interference."

[726] Schoeman 1984a, 2. *et seq.*

[727] Westin 1984, 56.

[728] Westin 1984, 58. When listing diseases Westin refers to H. L. Ratcliffe and R. L. Snyder.

[729] Westin 1984, 59.

situation when they are alone." It is their fear of isolation that makes them think they are never alone, that spirits and supernatural powers are with them. Another, universal element is "curiosity and surveillance," namely the tendency of individuals and society to invade the privacy of others. The phenomenon of curiosity for its own sake, according to Westin, is not restricted to human beings. Gossip, a particular way of gaining information in order to satisfy curiosity, exists because "[p]eople want to know what others are doing, especially the great and powerful, partly as a means of gauging their own performances and desires and partly as a means of vicarious experience [...]." In addition to the type of curiosity that invades privacy, every society is characterized by a universal process of surveillance as well: "Any social system that creates norms – as all human societies do – must have mechanisms for enforcing these norms. Since those who break the rules and taboos must be detected, every society has mechanisms of watching conduct, investigating transgressions, and determining 'guilt'."[730] At this point a process starts moving from primitive to modern societies, which "increases both physical and psychological opportunities for privacy by individuals and family units." Regarding their significance in this process, the author points out the roles played by the anonymity of city life, mobility in work and residence, and the weakening of religious authority over individuals, by which he also stresses the tendency that alienation and lack of relations, together with bureaucracy, might lead to total control, justifying the Orwellian anti-utopia.

3. All societies have, therefore, norms of privacy, either legal or extra-legal: in Westin's broad definition, rules governing the concealment of the naked body as well as norms setting the boundaries of a familyhousehold all belong here. He also mentions that there is more privacy for an individual in a nuclear household than in an extended one,[731] while the formation of the nuclear household is a bridge towards the recognition of an individual's privacy.[732] Initially, the guaranty for autonomy has been property: "Parallel to the unfolding of capitalism,

[730] Westin 1984, 68. *et seq.*

[731] Westin 1984, 63.

[732] "Hobbes already considers the purely human relations 'unregulated,' and compared to his system the third way is shown between 'natural' conflict and the obedience of a subject. Family autonomy plays a significant role in the modern development of individual rights as well" – Sólyom 1983, 81. (and note 77). Majtényi draws a contrary conclusion, in his view the initial meaning of privacy is "the right to be left alone" attributed to Brandeis, but its "present day interpretation is pointing increasingly beyond individuality." Majtényi 2003, 580.

proprietary right functions increasingly as the guarantee for autonomous action."[733] Protection of honor appears already in classical Roman law with the extension of the injuria by the law of the XII tables,[734] and after its history bridging the Middle Ages, it remains a guaranty for ensuring the right of name and the protection of portrait rights in Swiss law,[735] while in the United States it is assimilated by privacy-protection.[736]

With the establishment of general personality right protection[737] the protection of "secrecy sphere" is included in European laws,[738] while in the United States the right to privacy first becomes a right underlying the protection of portrait rights replacing its interpretation as proprietary right, and later it becomes the framework for personal right protection, corresponding to the European idea of "general personality right."[739]

Warren and Brandeis, in their famous article published in 1890, connect the necessity of the recognition of the right to privacy in common law with the effects of the new inventions of the age and the spreading of "business methods" unknown up to that point: an example of the former is the contemporary development of photography, while for the latter the growing impact of the press – first of all the yellow press. "Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'"[740] According to Warren and Brandeis, newspapers invade privacy in an "evil" way, "[g]ossip is no longer the resource of the idle and the vicious, but has become a trade, which is pursued with industry as well as effrontery."[741] Gossip

[733] Sólyom 1983, 123

[734] Sólyom 1983, 133. *et seq*.; but "we cannot project the 'autonomy,' the single and unrepeatable individuality to the Roman Law injuria […], neither to 'privacy' as opposed to society – that is expressing it even more explicitly." Sólyom 1983, 164.

[735] Sólyom 1983, 129.

[736] More precisely: Sólyom 1983, 218. *et seq*.

[737] On its formation see Sólyom 1983, 223. *et seq*

[738] Balás P. 1941, 652. *et seq*.

[739] Sólyom 1983, 29–44, 203. *et seq*..

[740] Warren–Brandeis 1984, 76.

[741] Warren–Brandeis 1984, 76.

supply creates its demand, which "results in a lowering of social standards and of morality."[742]

The other change is the significant development of photography technology that makes it possible to take a picture of someone against his or her will. Previously, one had to sit still for a portrait. This is stressed in the legal argument of Warren and Brandeis as well, since, previously, if one were "sitting" for the portrait, "the law of contract or of trust might afford the prudent man sufficient safeguards against the improper circulation of his portrait." In the new situation, however, protection must be provided by a more stable legal background. After an overview of the practice of common law courts of justice, Warren and Brandeis come to the conclusion that the rights protected "are not rights arising from contract or from special trust, but are rights as against the world" In other words, they are real rights, but "the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual use." According to Warren and Brandeis, the proper solution is a new interpretation of the "right to privacy", a right that has already been acknowledged by judges. In common law, this right was previously used by judges when judging the publicizing of "thoughts, feelings and emotions through writing or arts" in diaries, letters and similar media,[743] but in the authors' opinion, this is only one element of the right: "the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to the personal relation, domestic or otherwise."[744]

4. Thus, with the change in the structure of publicity[745] and the appearance of the new technologies of the age, Warren and Brandeis support acknowledging the "right to privacy". The protection of the individual gained a new support replacing proprietary rights: privacy means the protection not only of privacy, but also the protection of autonomy in its wide sense, including not only the protection of proprietary autonomy. The meaning of privacy

[742] In connection with the fuction of gossip see the excellent article by Posner in which he argues that the social effect of gossip is expicitely positive: Posner 1984.

[743] Warren–Brandeis 1984, 79. *et seq*.

[744] Warren–Brandeis 1984, 86.

[745] For the change of publicity see also Sólyom 1983, 196. The question arises whether the publicity of the internet is a similar new development. In literature we can read about the appearance of new technologies which might make external monitoring of brain functions possible. Galántai 2005.

kept widening through its history, it has reached the right of general freedom of action,[746] while according to Sólyom it is characterized by "alarming generality," "magniloquence" and "philosophic imprecision."[747] Its appearance, however, is an important milestone in the development of personality rights: the development which is characterized "primarily by the detachment of protection from ownership."[748] The protection of name, portrait and sound recording is acknowledged as an answer to the challenges of technology development,[749] and general personality right is incorporated into law – first in Switzerland.[750]

5. The protection of an individual's "secrecy sphere" appears within the scope of general personality right, and is recognized partly within its frameworks. As Elemér Balás P. puts it, "the point in the secrecy sphere is that the importance of personality is so predominant concerning certain facts that, from a legal point of view, these facts and their embodiments do not count as objects of the external world, but rather have to be understood as functions of personality. The formation of the secrecy sphere is the manifestation of the life process of a personality via his will. Certain facts belonging to the outer world are such that, from the personality's point of view, they cannot be regarded as parts or as tools of the personality's life process."[751] Protection, however, at this point applied merely to the secrecy sphere.

6. General personality right, after a temporary decline during the Second World War, became the focus of legal thinking again.[752] Data protection was born with the first generation of data protection laws, which responded to the development of computer technology and the appearance of the ability to create mass databases and matching of data: although still indirect, the legal protection of the facts (data) of an individual outside the sphere of secrecy protection appears. As a next step, based on the passage of the Constitution (Grundgesetz) declaring general personality rights, the German constitutional court formulated the right of informational self-determination (informational autonomy). The new right ensured the right of

[746] Sólyom 1983, 218.

[747] Sólyom 1983, 215. In Sólyom's view "the frequency of the primitive scientific 'foundations' of privacy, in which property is derived more or less from hunger, suggest this emptiness." In a self-critical manner it is possible to refer here to the above treatment of Westin's study.

[748] Sólyom 1983, 17.

[749] Sólyom 1983, 276.

[750] Sólyom 1983, 296. *et seq.*

[751] Balás P. 1941, 652.

disposal over all data that can be associated with a person, regardless of whether the data are part of the secrecy sphere.

The notion of data protection

1. The notion of data protection (Datenschutz) became widespread beginning in the 1970s, signifying a new type of protection compared to earlier personality rights. This new protection, according to data protection regulations, applies (usually) to natural persons not only regarding specified types of data (portrait, sound recording), and it is usually not restricted to "sensitive" data, nor does it have to be matched with the consequences of data abuse. By way of introduction, it seems useful to propose a definition of data protection, to specify the term as understood within the scope of the present study, as well as the relation of the term to other notions that are often used as synonyms of data protection.[753]

2. The concept of data protection is often treated as part of *privacy protection*, or quite as its contrary, opposing privacy protection, as a specifically European (legal) solution to a problem which contributed to the appearance of the "right to private life" in American constitutional law. In my view several – legal and extra-legal – tools, and methods of privacy protection may be distinguished, and the notion itself may be applied to a far wider category of phenomena than data protection. Data protection might be understood only within the framework of privacy protection as a legal tool of privacy protection, born within a given social and technical context. We should also not disregard the fact that the notion of privacy is used today in a much broader sense in American legal thinking: as I have referred to it above, as a result of the development it has undergone since the end of last century, by now it can be interpreted as the equivalent of general personality right.

This protection existed already before the appearance of data protection: privacy protection was provided by extra-legal, natural boundaries, or the extra-legal system of social norms.

---

[752] Sólyom 1983, 309. skk.

[753] I am making an attempt to come up with a definition in spite of Mayer–Schönberger's opinion according to which "[i]n Europe, since the 1970s, 'data protection' has become a household word to describe the right to control one's own data. […] But the connotations associated with 'data protection' have shifted repetedly and substantially, and further defining the term turned out to be a futile if not tautological quest" (Mayer–Schönberger 1997, 219.).

Following the appearance of data protection these tools may be (and are) applied continually. Data protection as a specific legal protection appeared as a result of the weakening or disappearance of certain natural boundaries that earler ensured the protection of privacy. In recent years, however, parallel modes of privacy protection have regained their earlier significance. This phenomenon might be understood as the crisis of data protection. On the one hand, this crisis is prompting efforts to renew data protection as legal protection. On the other hand, it widens data protection regulations, because the size of other (mostly technological) measures and tools serving privacy protection is increasing (on this issue see below the part on data security).

Data protection, then, may be interpreted within privacy protection according to the following:

a) data protection in all cases means the *legal* protection of an individual's privacy,[754] which

b) appeared in Europe as an answer to the *dangers of electronic data processing* which were becoming widespread via the electronic revolution, beginning in the 1970s, and

c) the content of the legal protection provided by it has *changed* significantly several times since its appearance, and it is still changing at present.

3. The *right of informational self-determination* is "the right of the individual to have a basic decision over the rendition and use of his personal data."[755] In the literature, data protection is very frequently identified with rules ensuring the right of informational autonomy.[756] I disagree with this view. As I argue below, when discussing the history of data protection, the concept of the right of informational self-determination is a much later development compared to the appearance of data protection (namely, the appearance of the legal protection realized through the regulation of processing specific, personal data of individuals), and its

[754] "Data protection means the protection of the individual, the human being, in other words: the protection of the data subject and not data as such" (Majtényi 1997a, 6; Majtényi 2003, 579). "It is not 'data' that is in need of protection, it is the individual to whom the data relates" (Mayer–Schönberger 1997, 219). In Mayer–Schönberger's view this contradictory fact was noted by the first data commissioner in Germany, Spiros Simitis, in his 1979 commentary on the German Federal Data Protection Act.

[755] Decision 15/1991. (IV. 13.) AB (Constitutional Court of Hungary)

appearance can be linked first to the Census Decision of the German Constitutional Court of 1983.

Data protection cannot be considered identical to the right of informational autonomy, since the early data protection laws did not ensure an individual any disposal over his personal data. Although the appearance of the right of informational autonomy is a significant milestone in the history of data protection, it is still wrong to claim that the development of data protection cannot go beyond the basic principles of the right of informational self-determination. There is a view according to which data protection based on the right of informational autonomy is undergoing a crisis, and that the latest generation of data protection regulations is based only nominally on the right of informational self-determination.[757] Thus, data protection includes all regulations that, via the regulation of the treatment of an individual's personal data, aim at the protection of these data, irrespective of whether this regulation ensures the right of informational self-determination of an individual.

4. The right to data protection, especially in Hungary, is treated in literature frequently as the right of access to data of public interest, that is, as the twin-right of freedom of information: data protection and the freedom of information are the two basic rights of information.[758] The common treatment of these two rights is justified by the fact that in Hungary the common codification of data protection rights and the right of freedom of information was successful, and the competence of several other European data protection commissioners now includes enforcement-related issues concerning the right of freedom of information.[759]

According to another understanding, apart from the legislation concerning data protection and the freedom of information, norms regulating other issues, (for example the so-called "secrecy right" – the rules of managing qualified data, i.e. state secrets and official secrets), legal regulations concerning electronic documents and provisions concerning data security together

---

[756] See for example Dietz–Pap 1995, 14. According to the obviously mistaken understanding of another author, data protection and the publicity of data of public interest jointly "form the two elements of the right for informational self-determination" (Dósa 2003, 24.).

[757] See for example Mayer–Schönberger 1997.

[758] See for example Majtényi 2003.

[759] As in the United Kingdom, in Slovenia, as well as in Germany and the German länder Brandenburg and Berlin.

would form "data management" law or "information management" law.[760] The object of the legislation concerning information management is not personal data, but rather data (information) independent of the data carrier, the management of which is regulated by the given areas of legislation for specified reasons (protection of privacy, interest of national security etc.). The advantage of this concept is that the individual data controllers face a coherent network of norms applying to different objects of regulations, which facilitates law enforcement. It is no accident that the Hungarian data protection act was defined as an "Information Act" at the outset of its codification,[761] and that the idea of "information regulation" had appeared in legal thinking already at that time.[762] The regulation of data protection and freedom of information appears within the same act, and secrecy rights (regulation of state secrets and official secrets) are also connected to this legislation: the commissioner for data protection has specific authority for secrecy control, while the data protection law serves as background law for the law on state secrets and official secrets, etc. Data protection law, therefore, can also be regarded as a sub-branch of "information regulation," covering more than just the protection of personal data and the publicity of data of public interest.

3. Generations of data protection norms

1. The period before the appearance of data protection was not yet characterized by the massive application of devices for storing and processing data. There was very small likelihood that someone would make links between personal data, process these data and create a personality profile that would expose an individual, because such activities required large investments. Still, fear of the complete disappearance of privacy was present. It is illustrated by a 1935 poem of Attila József:

"They can tap all my telephone calls

[760] Kinga Szurday is forwarding similar thoughts in connection with the notion of "information regulation acts". In her view these consist of general acts (which are "freedom of information"-type acts, privacy acts, and data protection acts) on the one hand, and on the other special acts regulating "a given subfield of information flow." Unfortunately Szurday does not make her system entirely expicit, and does not interpret the right of "information regulation" outside the scope of data protection and freedom of information. See Szurday 1994.

[761] Sólyom 1988a.

[762] Sólyom 1988b, 27.

(when, why, to whom.)
They have a file on my dreams and plans
and on those who read them.
And who knows when they'll find
sufficient reasons to dig up the files
that violate my rights."[763]

A similar fear is reflected in George Orwell's novel *1984*. According to Chief Justice Louis Brandeis, "Subtler and more far reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[764] More than 30 years before 1928, when this opinion was formulated in the article co-authored with Warren already quoted above, Brandeis had expressed his opinion about the dangers inherent in the new technologies. But "[u]p until the 1960's, most surveillance was low-tech and expensive since it involved following suspects around from place to place and could use up to six people in teams of two working three eight hour shifts. All of the material and contacts gleaned had to be typed up and filed away with little prospect of rapidly cross checking. Even electronic surveillance was highly labor intensive. The East German police, for example, employed 500,000 secret informers, 10,000 of which were needed just to listen and transcribe citizen's phone calls."[765] Data processing was not automatic, and the large-scale, uncontrolled surveillance was too costly. All this provided a natural barrier for protecting privacy. These natural barriers disappeared gradually at the middle of the1960s, with the spread of computerized data processing.

2. When discussing the history of European data protection regulations, the literature makes a distinction between generations of norms based on specific points of view. Some distinguish among three generations of data protection norms, while some describe four such generations.

---

[763] Translated from Hungarian by John Bátki.

[764]"Quoted by the 1998 working document of the Scientific and Technological Options Assessment Unit of the European Parliament (STOA), "An Appraisal of Technologies of Political Control", point 4. The executive summary of the document is available at the web page of the European Parliament: http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm; and the full text can be read at http://cryptome.org/stoa-atpc.htm.

[765] STOA point 4. The material refers to the intelligence of the former East Germany (Stasi).

First-generation norms, which appeared in the early 1970s, are characterized by a certain technological attitude in Mayer-Schönberger's view. The regulations of the second generation norms depend less on technology, and in this generation (in the second half of the 1970s) regulations put greater emphasis on the rights of the individual. In this classification, the third-generation data protection norms are considered to be ones born after the decision of the German constitutional court on the 1983 census, and in which regulation reflects the concept of informational self-determination. The fourth-generation norms – which are described by the author with key terms such as "holistic" and "sectorial" – amend the imperfections of the third generation norms. A new development of this period is that general data protection rules are supplemented with region-specific regulations.[766]

Bäumler – who builds his categories on the development of German data protection law – does not distinguish between acts belonging to the first and the second generation in Mayer-Schönberger's system, but rather groups them together, saying that they contain general clauses and conceptual formulas. In Bäumler's classification, the results of legislation following the 1983 census belong to the second generation (including several sectorial data protection norms), while he considers third-generation those provisions of law which, on the one hand, need to adopt the EU directive into national legislation, while, on the other hand, they need to transform data protection law, they need to react to the changes in data procession technology.[767] Bizer's outline of the development of generations is similar. In his view, the newest challenge the legislator must face is extending the traditional data protection right and creating "the right that is forming technology" (Recht der Technikgestaltung)[768].
The fact that the first generation norms were directed towards (at least partly) computerized record-keeping is considered by Majtényi as their central characteristic. In this classification, the second generation norms govern all record keeping (including paper-based records as well). In Majtényi's view, the characteristic feature of the third generation norms is that European integration (the adoption of the EU directive) and sectorial challenges are taken into consideration in their framing process.[769]

[766] Mayer–Schönberger 1997.

[767] Bäumler 1999.

[768] Bizer 1999.

[769] Majtényi 2003. A move towards sectorial regulations is characteristic of the third generation norms in Bennett's opinion as well: Bennett 1997, 114.

The description of the history of regulations with successive generations seems to be well applicable to the history of European data protection. Three phases may be distinguished in its history:

a) the first phase starts with the appearance of the first data protection regulations and extends to the decision of the German Constitutional Court of 1983, stating the case of the freedom of informational self-determination,

b) the second starts with the formulation of the doctrine of informational self-determination and extends to the beginning of the third phase,

c) the beginning of the third phase is marked by the appearance of "new data protection," an answer to the crisis of data protection regulations (the landmark event being the passing of the German Teledienstedatenschutzgesetz in 1997).

1.27. First generation data protection norms

1. In the second half of the 1960s, development reached a point where it seemed that Orwell's dystopia might become real. In order to operate the developing social welfare-state, bureaucracy needed an increasing amount of information, and new technology for processing this mass of information was available.[770] Organizations owning large numbers of records (the state and the biggest companies) started to use computers. Since computer capacity was a fairly expensive, as well as limited, resource, soon the idea was born to store data at a single place for practical reasons while providing different users with remote access. In this way it was much simpler to launch, run and maintain a system.[771] The easiest tool for connecting data banks is a general artificial identifier code, and at this point administration needed it. This development, the appearance of the notion of "integrated data management," led in Germany to the so-called data protection debate (Datenschutzdiskussion),[772] and later to the data protection act.

---

[770] For the connection between large databases and social welfare state see Mayer–Schönberger 1997, 222.

[771] In Sweden in the second half of the 1960s a plan was born according to which data concerning taxation and the already joint registry and census data should be merged in a national databank. In Germany there were plans for the connection of databanks on local, state and federal levels, and there was a scheme to centralize data procession in administration on state level (for example in Hesse and Bavaria) (Mayer–Schönberger 1997, 222). According to the Hesse plan 70 data items would have been stored for one person (about the "Large Hesse Plan" see Sólyom 1988b, 25). See also Bizer 1999, 31.

[772] Bizer 1999, 31.

2. *The first generation acts,* thus, were born in a period where computers were used by few, and these few were primarily state-run data controllers. The state, by connecting various registries, threatened to gain informational superpower over the individual. Therefore when formulating the first data protection laws, their authors took into special consideration the challenges of the new technology, to make its application controllable and transparent. The characteristics of the first generation data protection acts are as follows:

a) The primary goal of these acts is transparency of the large – primarily state-owned – databases.

b) These acts do not yet ensure the right of disposal over the data of an individual for reaching this goal, but they ensure some rights (primarily the right of access and rectification) that will later become parts of the right of informational self-determination.

c) Obligations concerning registering the databases containing personal data appear within this generation of data protection norms. Thus, it is important to stress that the obligation concerning registration appeared in a context where there were few large databases.

d) With the first generation data protection norms, the legislature wished to control specifically computerized data processing: these regulations were particular tools of privacy protection at the initial phase of the information revolution, but according to the above definition they cannot be regarded as data protection acts in the sense that their object was primarily technology in the service of record keeping.

e) Some acts among the first generation norms entitled legislation the right of access to information available for public administration. This supports the idea that the direct aim of the first generation norms was not data protection as it was previously defined, but rather to create the "informational division of power", and to suppress the excess of information power of the executive branch of the government within the state and society.

3.2. The census decision and the second generation of data protection norms

1. In December 1983, the German Federal Constitutional Court declared unconsitutional (as infringement upon the Basic Law) some provisions of the act concerning the census that had been adopted the same year; this decision had a global effect on data protection policy and law. In its famous census decision (Volkszählungsurteil), the court ruled that the "basic right

warrants [...] the capacity of the individual to determine in principle the disclosure and use of his/her personal data."[773]

2. The German Federal Constitutional Court derived the right to informational self-determination from the general personal right, interpreting Art. 2 Para. 1 of the Basic Law in conjunction with Art. 1 Para. 1. The general personal right is a "mother-right", the content of which is "not specified ultimately" in legal practice,[774] but from time to time a specific right protecting the individual is established based on it. Personal right includes "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others and to what extent." According to the court, self-determination requires increased protection due to the development of technology. "It is endangered primarily by the fact that, contrary to former practice, there is no necessity for reaching back to manually compiled cardboard-files and documents, since data concerning the personal or material relations of a specific individual {personal data [cf. Federal Data Protection Act Art. 2 Para. 1]} can be stored without any technical restraint with the help of automatic data processing, and can be retrieved any time within seconds, regardless of the distance. Furthermore, in case of creating integrated information systems with other databases, data can be integrated into a partly or entirely complete picture of an individual, without the informed consent of the subject concerned, regarding the correctness and use of data." The Court stated that the situation can be dangerous both to the individual's right of self-determination and to democratic society "if one cannot with sufficient surety be aware of who knows what about them. Those who are unsure if differing attitudes and actions are ubiquitously noted and permanently stored, processed or distributed will try not to stand out with their behavior. Those who count with

[773] BVerfGe 65, 1. The text is available at http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm. The object of the case is the 1983 census law, in which the legislator ordered a census that included not only identification data but also data concerning employment ("employment census"), as well as the registration of non-agricultural enterprises (workplace census) and a survey of real estate in a statistics of buildings and flats. According to the law the compiled data were allowed to be cross-checked with the address registry for the sake of accuracy. The act allowed for further possibilities of data transfer – although only regarding anonymous data – for the state and federal statistics offices and administration bodies (for example anonymously, with the exception of data about belonging to a religious community, if such data were required for carrying out the legal scope of activities of an administrative organ; anonymously for planning and environment purposes regarding environment protection for local authorities).

[774] See the Preamble to the census-decision.

the possibility that their presence at a meeting or participation in a civil initiation might be registered by the authority, may perhaps abandon practicing their basic rights (Basic Law, Art. 8 Para. 9)." This explains the understanding of the Court of the right of informational self-determination as a right based on the general personality right, which "ensures the individual the right to dispose over the issuing and utilization of his personal data."

However, the Court stated that the right to informational self-determination was not unlimited. Limitations are acceptable for reasons of compelling public interest (überwiegendes Allgemeininteresse); norms have to comply with the requirement of explicitness, and thus have to be formulated in a way that citizens understand the requirements and the extent of the limitation. The goal of data management has to be specified, and data management can be required regarding data that are appropriate and needed for the purpose. As a further procedural guarantee the court's ruling prescribes the right of information and the obligation of data deletion once the goal is reached. The Court also held that the role of independent data protection commissioners was highly important due to the complexity of automated data processing and for the sake of effective protection. Furthermore, the decision gave a detailed account of the requirements concerning data processing for statistical reasons, based on the right of informational self-determination.[775]

2. The decision had a profound impact both in Germany and abroad: the principles laid down in it appear in the state data protection acts in subsequent years, as well as in the General Amendment to the German Federal Data Protection Act of 1990. The impact of the decision's philosophy can be felt in the 1986 amendment to the Austrian data protection act, as well as in the Norwegian, Finnish and Dutch acts[776] , and the 1992 Hungarian data protection act (based on a decision of the Hungarian Constitutional Court, which was phrased in the wake of the, the German decision).

[775] The Constitutional Court declared unconstitutional the provisions of the act that allowed for the use of data collected during the census by the administration for other purposes. The connection of the two data processing purposes – collecting data for statistics and for administration – according to the court's reasoning creates an unclear situation for the citizen, it does not fulfil the requirement of clarity, it is not useful for reaching the goal, and thus it is unconsitutional.

[776] Mayer–Schönberger 1997, 231.

3. *The second generation data protection norms*,[777] according to Mayer-Schönberger are characterized by the fact that they ensure specific rights for the individual concerning the whole process of personal data processing; the legislators realized that the decision of the citizens cannot be restricted to their consent or objection to the automated processing of their data, since technology by this time had permeated society to an extent that disagreement would have entailed excessive costs for the individual. Typical attributes of the regulations born at that time in the field of market research are the citizen's right of refusal and the right to deletion of old information.[778] Regulations became increasingly abstract and less technology-specific. The technological changes of the period – the appearance of personal computers, and their subsequent connection to networks – would have made impossible the regulation of technology. This is why the legislature, instead of regulating technology, endowed the individual with the right of informational self-determination, which, at least theoretically, would make individuals capable of defending themselves on all occasions. (Technology-specific regulations receded into the background only temporarily: the essence of third generation norms is strengthening the possibility of enforcing the right to informational self-determination within the context of a given sector, with regard to its technological specificity.) In this period, parallel to the process of technological norms (which were formed to regulate the world of integrated and centralized databases) fading into the background, registration procedures were streamlined substantially.[779] It is worthwhile to note that in Mayer-Schönberger's opinion these acts embodied a pragmatic compromise "between fostering and controlling efficient information processing." In other words, the required level of protection was lowered for the sake of operation already at this point.[780]

3.3. The third generation data protection norms

1. The third generation data protection norms try to find solutions to the above challenges, up to this point with unforeseeable success: new principles (data economy) and new institutions (data-protection audit) have appeared in literature and entered into regulations. As an answer

[777] In Mayer–Schönberger's system regulations based on the principle of informational self-determination belong to the third generation data-protection norms. Mayer–Schönberger 1997, 231.

[778] Mayer–Schönberger 1997, 232.

[779] See the example of Mayer–Schönberger on the Austrian law Mayer–Schönberger 1997, 231.

[780] Mayer–Schönberger 1997, 231.

to being pervaded with information and its technologies, regulations focusing on technologies have returned: the goal is to frame technologies.

2. The first of the third generation data-protection norms is the German Teledienstedatenschutzgesetz (TDDSG) of 1997. The TDDSG introduced revolutionary institutions and principles in German data protection law. The significance of these principles is proven, among others, by the fact that within a few years some of them were incorporated into the Federal Data Protection Law. Furthermore, since the adoption the TDDSG, wide experience has been gathered on its practical application, in the wake of which certain provisions of the law were amended in 1999 and 2001.

As early as 1997, the TDDSG included the basic principle that the technological tool used by the telecommunications service provider must be such that its operation does not involve processing personal data, or involves a minimum processing of personal data. Furthermore, these policies have to be taken into consideration when the tools are constructed.[781] (The Federal Data Protection Act was also included in an amendment to this provision (the so-called principle of "data economy" or Datensparsamkeit). [782] The essence of the data-protection audit regulated by the Federal Data Protection Act is that the manufacturers and users of the tools used for data processing go through an audit of their processes as well as their tools.[783] The institution is following the example of environment-protection audit that is included in EU legislation.[784]

3. Elements of the third generation data-protection norms have appeared already in Hungarian legislation, where the legislature consciously followed the examples set by TDDSG and BDSG when the act on electronic business services and other questions concerning the information society of 2001 (CVIII) was amended in 2003. The amended act defines the principle of data economy.[785] The principle of data economy is more than the

[781] TDDSG 3. § (4).

[782] BDSG 3. §.

[783] See BDSG 9. §. The institution appeared in 1997 in the State Media Agreement (Mediendienste Staatsvertrag 17. §).

[784] On this issue see Flemming Moos: Datenschutz im Internet. In Kröger–Gimmy 2000, and Ewer 2002.

[785] According to 13/A. (3) "The provider – in addition to the stipulations of paragraph (2) – may process personal data that are technically essential for providing the service. In case the other requirements are identical, the service provider has to choose among the available tools, and has to operate these tools in all cases while providing an information society service in such a way that personal data are processed only in case it is

basic principle defined in Article 5 (2) of the Data Protection Act, since the former requires that the data controller apply the avoidance of personal data procession, if that is possible, prior to starting the actual data processing and to minimize the data processing to the least possible amount. The requirement applies to operation as well; in other words, it is violated by the data controller who sets up software or hardware configurations in a way that the operation results in an excessive amount of data processing compared to the real need for operation or to the needs of some other goal defined by law. This rule creates more favorable opportunities for the data protection authority to enhance technologies serving data protection.

Again following the example of TDDSG, another provision was included in the Hungarian legislation: the stipulation that limits the data-management possibilities of a service provider in case of monopoly, while within real market circumstances it offers the possibility for other data processing as well, unrelated to the service.[786] The provision excludes abuse of consent-based data procession if the service is unavailable from a different service provider (by the given user). The provision allows for the enforcement of the right to informational self-determination and does not prohibit consent-based data management.[787]

4. Thus, the first elements of the third generation of data-protection regulations have already appeared, and only time can tell whether these regulations will mean a new start or the next step in a long-lasting struggle. We can hope that the withdrawal of privacy advocates is only temporary, and that privacy protection will remain effective with the help of either legal or extra-legal tools. Without an innovative renewal of data-protection law "freedom will diminish in the same unnoticed way in which clean water and air have diminished."[788]

---

essentially needed for providing the service and for meeting the other goals stipulated by law, but even in this case only to the required extent and time."

[786] According to Section 13/A (8): "Providing an information society service cannot be made subject to the consent of the person making use of the service for uses not mentioned in paragraphs (1)–(3) if the service is unavailable from another provider."

[787] It should be noted that experts preparing the bill – including the author of the present article – consciously did not suggest that the institution of data-protection audit is taken over into the Hungarian regulations, due to the lack of German experience (on this issue see for example Vossbein 2002).

[788] Sólyom 1988b, quoted by Majtényi as well: ABI 2001, 14.

Irodalom

ABI 1997. *Az adatvédelmi biztos beszámolója 1995–1996.* Budapest, Adatvédelmi Biztos Irodája.

ABI 1998. *Az adatvédelmi biztos beszámolója 1997.* Budapest, Adatvédelmi Biztos Irodája.

ABI 1999. *Az adatvédelmi biztos beszámolója 1998*. Budapest, Adatvédelmi Biztos Irodája.

ABI 2000. *Az adatvédelmi biztos beszámolója 1999.* Budapest, Adatvédelmi Biztos Irodája.

ABI 2001. *Az adatvédelmi biztos beszámolója 2000*. Budapest, Adatvédelmi Biztos Irodája.

ABI 2002. *Az adatvédelmi biztos beszámolója 2001.* Budapest, Adatvédelmi Biztos Irodája.

ABI 2003.*Az adatvédelmi biztos beszámolója 2002.* Budapest, Adatvédelmi Biztos Irodája.

ABI 2004. *Az adatvédelmi biztos beszámolója 2003.* Budapest, Adatvédelmi Biztos Irodája.

ABI 2005. *Az adatvédelmi biztos beszámolója 2004.* Budapest, Adatvédelmi Biztos Irodája

Agre, Philip E. – Rotenberg, Marc (eds.) 1997. *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts, The MIT Press.

Almási János 2002. *Elektronikus aláírás és társai*. Budapest, Sans Serif.

Batus Endre 2004. Akinek nem tetszik, tegyen a törvény módosításáért. Interjú Péterfalvi Attilával. *HVG,* augusztus 21.

Baeriswyl, Bruno – Rudin, Beat (Hrsg.) 2002. *Perspektive Datenschutz – Praxis und Entwicklungen in Recht und Technik*. Zürich–Baden-Baden–Wien, Schulthess–Nomos–Verlag Österreich.

Bainbridge, David 1996. *Computer Law.* London, FT Pitman Publishing.

Balás P. Elemér 1941. Személyiségi jog. In Szladits Károly (szerk.): *Magyar magánjog.* Budapest, Grill Károly Könyvkiadóvállalata.

Balogh Zsolt György 1992. *Adatkezelés, adatvédelem, jog*. Pécs, Pécsi Tudományegyetem. Kézirat (egyetemi doktori értekezés).

Balogh Zsolt György 1997a. Az ingójelzálog-nyilvántartás adatvédelmi kérdéseiről. *Közjegyzők Közlönye,* 3. sz.

Balogh Zsolt György 1997b. Az adatvédelmi törvény fejlesztésének kérdései, adatvédelmi szabályok Magyarországon és az Európai Unióban. *Jogtudományi Közlöny,* 6. sz.

Balogh Zsolt György 1998. *Jogi Informatika*, Budapest–Pécs, Dialóg Campus.

Balogh Zsolt György – Jóri András – Polyák Gábor 2002. *Adatvédelmi legjobb gyakorlat kialakítása az elektronikus közigazgatásban.* Pécs, Pécsi Tudományegyetem. Kézirat.

Balsai István – Sándorfi György 1999. Személyiségi jogok az átvilágítási törvényben. *Fundamentum,* 1. sz.

Bán Tamás – Könyves Tóth Pál 1997. Személyes adatok külföldre irányuló továbbíthatóságáról. *Magyar Jog,* 12. sz.

Banisar, David 2001. A privacy védelmének modelljei. In Majtényi (szerk.)

Bárd Károly – Gellér Balázs – Ligeti Katalin – Margitán Éva – Wiener A. Imre 2002. *Büntetőjog – Általános rész.* Budapest, KJK–Kerszöv.

Bäumler, Helmut 1999. Datenschutzgesetze der dritten Generation. In Bäumler–Mutius.

Bäumler, Helmut – Mutius, Albert von (Hrsg.) 1999. *Datenschutzgesetze der dritten Generation (Texte und Materialen zur Modernisierung des Datenschutzrechts).* Neuwied, Luchterhand.

Bäumler, Helmut – Mutius, Albert von (Hrsg.) 2002. *Datenschutz als Wettbewerbsvorteil.* Wiesbaden, Vieweg.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, Cornell University Press.

Bennett, Colin J. 1997: Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? In Agre – Rotenberg (eds.).

Bergkamp, Lucas 2002. The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-driven Economy. *Computer Law and Security Report,* vol. 18. no. 1.

Bizer, Johann 1999. Datenschutz durch Technikgestaltung. In Bäumler–Mutius.

Bodony István 1998. A személyes adatok védelme a bűnüldözésben. *Acta Humana,* 32. sz.

Boehme-Neßler, Volker 2002. Datenschutz in der Informationsgesellschaft – Vom Datenschutzrecht zum Informationswirtschaftrecht. *Kommunikation & Recht,* 5. sz.

Boling, Patricia 1996: *Privacy and the Politics of Intimate Life*. New York, Cornell University Press.

Burgdorff Christoph von 2003. *Der Umsetzung der EG-Datenschutzrichtlinie im nicht-öffentlichen Bereich.* Frankfurt am Main, Peter Lang.

Burkert, Herbert 1997. Privacy-Enhancing Technologies: Typology, Critique, Vision. In Agre–Rotenberg.

Burkert, Herbert 2002. Datenschutz auf dem Weg zur Transparenzordnung. In Baeriswyl–Rudin.

Craig, Paul – De Búrca, Gráinne 2003. *EU Law.* Oxford, Oxford University Press.

Cranor, Lorrie Faith. Proceedings of the Twelth Conference on Computers, Freedom and Privacy, April 16–19. 2002, San Francisco.

Dammann, Ulrich – Simitis, Spiros 1997. *EG Datenschutzrichtlinie: Kommentar.* Baden-Baden, Nomos.

Denning, Dorothy 1997. The future of cryptography. In Brian D. Loader (ed.): *The Governance of Cyberspace.* London–New York, Routledge.

Dietz Gusztávné – Hanzmann József 1999. *Adatvédelmi szabályzat.* Budapest, Novorg–KJK-Kerszöv.

Dietz Gusztávné dr. – Pap Márta 1995. *Adatvédelem, adatbiztonság*. Budapest, Novorg.

Dohr, Walter – Pollirer, Hans-Jürgen – Weiss, Ernst M. 2004. *DSG – Datenschutzrecht*. Wien, Manz.

Dósa Imre 2003. Az adatvédelmi szabályozás rendszere. In Dósa Imre – Polyák Gábor: *Informatikai jogi kézikönyv*. Budapest, KJK-Kerszöv.

Drinóczi Tímea 2004. Az információszabadság elhelyezkedése az alapjogi rendszerben, különös tekintettel a más alapjogokkal való kapcsolatára. *Infokommunikáció és Jog*, 3. sz.

Drobesch, Heinz – Grosinger, Walter 2000. *Das neue österreichische Datenschutzgesetz.* Wien, Juridica.

Druey, Jean Nicolas 2002. Von der strukturellen Schwäche des Personenschutzes im Informationsrecht. In Baeryswil – Rudin.

Dudás Gábor 1999. Az adatvédelem és a titokvédelem néhány gyakorlati kérdése. *Belügyi Szemle,* 11. sz.

Dumortier, Jos – Goemans Caroline 2000. *Data Privacy and Standardization*. Discussion Paper prepared for the CEN/ISSS Open Seminar on Data Protection. http://www.law.kuleuven.ac.be/icri/papers/doctrine/cen-paper.pdf

Eichhorn, Bert 2001. *Internet-Recht (Ein Lehrbuch für das Recht im World Wide Web)*. Troisdorf, Fortis Verlag.

Engel-Fleischig, Stefan – Maennel, Frithiof A. – Tettenborn, Alexander (Hrsg.) 2001. *Beck'scher IUKDG-Kommentar*. München, Beck.

Enyedi Nagy Mihály – Polyák Gábor – Sarkady Ildikó (szerk.) 2002. *Magyarország médiakönyve 2002.* Budapest, Enamiké.

Enyedi Nagy Mihály – Polyák Gábor – Sarkady Ildikó (szerk.) 2003. *Magyarország médiakönyve 2003.* Budapest, Enamiké.

Etzioni, Amitai 1999. *The Limits of Privacy*. New York, Basic Books.

Ewer, Wolfgang 2002. Vom Umweltaudit zum Datenschutzaudit. In Bäumler–Mutius.

Fabók András 2000. A munkavállaló személyiségi jogainak és személyes adatainak védelme. *Munkaügyi Szemle,* 4. sz.

Faludi Gábor 2001: Az elektronikus kereskedelem aktuális kérdései. In *A Polgári Jogi Tudományos Diákkör Évkönyve*. Budapest, ELTE ÁJK.

Földes Ádám 2004. Árgus szemek. Kamerás térfigyelés Magyarországon. *Fundamentum,* 2. sz.

Földi Luca 2003. A hálapénz és az adatvédelem. *Élet és Tudomány,* 48. évf. 15. sz.

Fridli Judit – Tóth Gábor Attila – Ujvári Veronika (eds.) 1997. *Data Protection and Freedom of Information.* Budapest, Társaság a Szabadságjogokért.

Galántai Zoltán 2003. *E-privacy olvasókönyv.* Budapest, Arisztotelész (online: http://galantai.inno.bme.hu/e-privacy-book/e-privacy-book-01.html)

Galántai Zoltán 2005. A kognitív szabadság fantomja. *Infokommunikáció és Jog,* 2. sz.

Gauthronet, Serge – Droudard, Etienne 2001. *Unsolicited Commercial Communications and Data Protection.* Brussels, European Commission Internal Market DG

Gellért György (szerk.) 2001. *A Polgári Törvénykönyv magyarázata.* Budapest, KJK-Kerszöv.

Gellért György (szerk. 2004. *Kommentár a Polgári Törvénykönyvről szóló 1959. évi IV. törvényhez.* Complex CD Jogtár. Budapest, KJK-Kerszöv.

Gelman, Robert G. 1998. *Protectiong yourself online.* New York, HarperEdge.

Glatz Ferenc (szerk.) 2002. *Információs társadalom és jogrendszer.* Budapest, MTA Társadalomkutató Központ.

Gönczöl Katalin – Kóthy Judit 2001. *Ombusman 1995–2001.* Budapest, Helikon.

Guadamuz, Andrés 2000. Habeas Data vs the European Data Protection Directive. *Journal of Information, Law and Technology,* 2. sz. (http://elj.warwick.ac.uk/jilt/01-3/guadamuz.html)

Halmai Gábor (szerk.) 2002. *Ügynökök és akták. Nemzetközi konferencia az átvilágításról és az állambiztonsági iratok sorsáról*. Budapest, Soros Alapítvány.

Halmai Gábor – Vásárhelyi Mária (szerk.) 1998. *A nyilvánosság rendszerváltása.* Budapest, Új Mandátum.

Halmai Gábor – Tóth Gábor Attila (szerk.) 2003. *Emberi jogok.* Budapest, Osiris.

Halmai Gábor – Tóth Gábor Attila 2003a. Az emberi jogok rendszere. In Halmai–Tóth.

Imparato, Nicholas (ed.) 2000. *Public Policy and the Internet – Privacy, Taxes and Contract*. Stanford, Hoover University Press.

INFOFILIA 1991. *Informatika – jog – közigazgatás. Nemzetközi dokumentumok I*. Budapest, InfoFilia Magyar Adatvédelem és Információszabadság Alapítvány.

INFOFILIA 1992a. *Informatika – jog – közigazgatás. Nemzetközi dokumentumok II*. Budapest, InfoFilia Magyar Adatvédelem és Információszabadság Alapítvány.

INFOFILIA 1992b. *Informatika – jog – közigazgatás. Nemzetközi dokumentumok III.* Budapest, InfoFilia Magyar Adatvédelem és Információszabadság Alapítvány.

INFOFILIA 1992c. *Informatika – jog – közigazgatás. Nemzetközi dokumentumok IV.* Budapest, InfoFilia Magyar Adatvédelem és Információszabadság Alapítvány.

INFOFILIA 1993. *Informatika – jog – közigazgatás. Nemzetközi dokumentumok V.* Budapest, InfoFilia Magyar Adatvédelem és Információszabadság Alapítvány.

Javorniczky István – Majtényi László (szerk.) 1999. *Adatőrségen – Történetek a Tüköry utcából.* Budapest, Emberi Jogi Információs és Dokumentációs Központ.

Jakab András – Cserne Péter 2001. A kétharmados törvények helye a magyar jogforrási hierarchiában. *Fundamentum,* 2. sz.

Jay, Rosemary – Hamilton, Angus 1999. *Data Protection Law and Practice*. London, Sweet and Maxwell.

Jóri András 1996. Illetlenség a hálózaton. *Café Bábel,* 3. sz.

Jóri András 1998. A cybertér pacifikálása – Állami tartalomszabályozási kezdeményezések a nemzetközi számítógépes hálózatokon. In Halmai – Vásárhelyi.

Jóri András 2001a. Titkosítás magyar módra (a polgári rejtjelzés lehetséges magyarországi szabályozásáról). *HVG,* 2001. június 16.

Jóri András 2001b. Az adatvédelmi törvény novellájának szükségességéről. *Napi Jogász,* I/4.

Jóri András 2001c. Adatvédelem. In *Internet gyakorlati kézikönyv*. Budapest, Dashöfer Kiadó.

Jóri András 2001d. Változások előtt az adatvédelem. *Cég és Jog,* október

Jóri András 2001e. Hungarian Data Protection Law – A Brief Outlook. *BNA World Data Protection Report,* November.

JÓRI András 2001f. Adatvédelem. In Zsuffa Ákos (szerk.): *E-kereskedelem*. Budapest, Budapesti Kommunikációs Főiskola.

Jóri András 2001g. Kimaradt az adatvédelem – megjegyzések az elektronikus kereskedelmi törvény tervezetéhez. *Napi Jogász,* december.

Jóri András 2002a. A polgári célú rejtjelzés szabályozásáról. *Napi Jogász,* március.

Jóri András 2002b. Fogyasztói adatbázisok – a direktmarketing-törvény egyes értelmezési kérdéseiről. *Napi Jogász,* március.

Jóri András 2002c. Magánszféra és nyilvánosság a digitális korban. In Enyedi Nagy – Sarkady–Polyák.

Jóri András 2002d: Az adatvédelmi jog kialakulása és az információs társadalom hatása a személyiségi jogokra. In Sárközy–Pázmándi.

Jóri András 2003a. A hitelinformációs rendszerek szabályozása Magyarországon és Nagy-Britanniában I–II. *Cég és Jog/Napi Jogász,* 6. és 7–8. sz.

Jóri András 2003b. Az új magyar adatvédelmi törvény elé. *Jogtudományi Közlöny,* 12. sz.

Jóri András 2003c. Az elektronikus információszabadság lehetőségei Magyarországon. In Enyedi Nagy – Sarkady - Polyák

Jóri András – Zombor Ferenc 1998. Nyilván tartanak. A cigány szó emberi jogi vonatkozásai, *Fundamentum,* 1–2. sz.

Jóri András 2005: *Adatvédelmi kézikönyv*, Budapest, Osiris.

Jóri András – Bártfai Zsolt 2005: Vitás kérdések az adatvédelmi törvény értelmezése körül. *Infokommunikáció és Jog*, 10. sz.

Kecskés László 1999. *Magyar polgári jog – Általános rész*. II. Budapest–Pécs, Dialóg Campus.

Kerekes Zsuzsa 1999. Törvényen innen és túl – Az információszabadság az Alkotmánybíróság első tíz évének gyakorlatában. *Fundamentum,* 3. sz.

Kerekes Zsuzsa 2001. „Nincs adózás képviselet nélkül" – Az információszabadság és az üzleti titok konfliktusáról. *Fundamentum,* 4. sz.

Kerekes Zsuzsa 2002. Vagyonnyilatkozat – adatvédelem – információszabadság. *Fundamentum,* 2. sz.

Kerekes Zsuzsa 2004. „Hivatali kényelem?" – Az információszabadság korlátairól. *Fundamentum,* 2. sz.

Kerekes Zsuzsa 2005. Elektronikus információszabadság – Az Egyesült Királyság példája. *Jogtudományi Közlöny,* 4. sz.

Knyrim, Rainer 2003. *Datenschutzrecht.* Wien, Manz.

Koncepció 2004. *Az új Polgári Törvénykönyv koncepciója és tematikája.* (Közzétette honlapján az Igazságügyi Minisztérium 2004. június 21-én [http://www.im.hu/fooldal/cikk/cikk.phtml?menupontid=845&cikkid=2794].)

Kondricz Péter – Timár András 2000. Az *elektronikus kereskedelem jogi kérdései*. Budapest, KJK-Kerszöv.

Koops, Bert-Jaap 1999. *The Crypto Controversy: A Key Conflict in the Information Society.* The Hague, Kluwer Law International.

Korff, Douwe 2002. *EC Study on the Implementation of the Data Protection Directive* (Comparative Summary of National Laws). Colchester, University of Essex Human Rights Centre.

Kovács Györgyi – Sziklay Júlia – Zombor Ferenc 1997. *A pszichiátriai betegek joga személyes adataik védelméhez.* Budapest, Alkotmány- és Jogpolitikai Intézet.

Köhler, Markus – Arndt, Hans-Wolfgang 2003. *Recht des Internet*. Heidelberg, C.F. Müller.

Könyves Tóth Pál 1990a. Adatvédelem és információszabadság. *Világosság,* augusztus–szeptember.

Könyves Tóth Pál 1990b. A statisztika alkotmányos alapjai és törvényes keretei. *Magyar Közigazgatá*s, szeptember.

Könyves Tóth Pál – Varga Lajos 1990. A közérdekű adatok megismerése és terjesztése. *Magyar Közigazgatás,* március.

Kröger, Detlef – Gimmy, Marc A. 2000. *Handbuch zum Internetrecht*. Berlin, Springer.

Kühne, Jörg-Detlef: Art. 13. In Sachs 2006

Kukorelli István (szerk.) 2002. *Alkotmánytan.* Budapest, Osiris.

Lakatos Miklós 2000. Az adatvédelem szabályozása a magyar népszámlálások történetében. *Statisztikai Szemle,* 10–11. sz.

Lábady Tamás 1991. A nem vagyoni kártérítés funkcióiról. *Biztosítási Szemle,* 11–12. sz.

Lábady Tamás 1992. A nem vagyoni kártérítéssel kapcsolatos bírói gyakorlat legújabb tendenciái. *Biztosítási Szemle,* 7–8. sz.

Lábady Tamás 1996. Elégtétel a nemvagyoni károkért a 20. század első felének magyar magánjogában. In *Benedek-emlékkönyv,* Pécs.

Lábady Tamás 2000a. *A magyar magánjog (polgári jog) általános része*. Budapest–Pécs, Dialóg Campus.

Lábady Tamás 2000b. Alkotmányos alapjogok és személyiségi jogok. *Jogi beszélgetések.* Budapest.

Lábady Tamás 2002. A kártérítési felelősség. *Jogászgyűlési előadás.* Budapest.

Lábady Tamás 2004: *Szerződésen kívüli kárfelelősség az új Ptk.-ban (Jogi tájékoztató füzetek 138.),* Budapest, Magyar Kereskedelmi és Iparkamara.

Ledermann, Eli – Shaphira, Ron (eds.) 2001. *Law, Information and Technology.* The Hague, Kluwer Law International.

Lenkovics Barnabás – Székely László 2001. *Magyar polgári jog – A személyi jog vázlata*. Budapest, Eötvös József Könyvkiadó.

Lessig, Lawrence 1999. *Code and Other Laws of Cyberspace.* New York, Basic Books.

Levy, Steven 2001. *Crypto.* New York, Viking Penguin.

Mádl Ferenc – Vékás Lajos 1997. *Nemzetközi magánjog és nemzetközi gazdasági kapcsolatok joga.* Budapest, Nemzeti Tankönyvkiadó.

Magyar Attila – Varga Ilona 1997. *Gyermekjogok az adatvédelem tükrében.* Budapest, Alkotmány- és Jogpolitikai Intézet.

Majtényi László 1990. Az adatvédelmi ombudsmann – az adatvédelmi törvényhozás. *Magyar Közigazgatás,* 8. sz.

Majtényi László 1992. *Ombudsmann. Állampolgári jogok biztosa*. Budapest, Közgazdasági és Jogi Könyvkiadó.

Majtényi László 1995. Az adatvédelem és az információszabadság az Alkotmányban. *Acta Humana,* 18–19. sz.

MAJTÉNYI László 1997a. *Adatvédelem, információszabadság, sajtó*. Budapest, Alkotmány- és Jogpolitikai Intézet.

Majtényi László 1997b. Az információs szabadságjogok Magyarországon. *Világosság,* 10. sz.

Majtényi László (szerk.) 2001. *Az odaátra nyíló ajtó*. Budapest, Adatvédelmi Biztos Irodája.

Majtényi László 2002a. Az információs szabadságok és az adatvédelem határai. *Világosság,* 2–3. sz.

Majtényi László 2002b. Adatvédelem és gazdaság. Távközlés, bankok, biztosítók. *Napi Jogász,* 3. sz.

Majtényi László 2003. Információs jogok. In Halmai–Tóth.

Majtényi László – Miklósi Zoltán (szerk.) 2004. *És mi lesz az alkotmánnyal?* Budapest, Eötvös Károly Intézet.

Majtényi László e. a. (szerk.) 2005: *Az elektronikus információszabadság.* Budapest, Eötvös Károly Intézet.

Majtényi László 2006. *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága*. Budapest, Complex Kiadó.

Mayer-Schönberger, Viktor 1997. Generational Development of Data Protecton in Europe. In Agre–Rotenberg.

Mihancsik Zsófia 1997. Az előítéleteket el lehet oszlatni. Majtényi Lászlóval beszélget Mihancsik Zsófia. *Beszélő,* 1997. június, 8–14. o.

Mullock, James – Leigh-Pollitt, Piers 1999. *The Data Protection Act Explained*. London, The Stationery Office.

Murswiek, Dietrich 2006: *Artikel 2.* In: Sachs.

Nedden, Burckhard 2001. Datenschutz im eGovernment. In Alexander Roßnagel (Hrsg.): *Die elektronische Signatur in der öffentlichen Verwaltung*. Baden-Baden, Nomos.

Pagenknopf Martin: *Arikel 11*. In: Sachs.

Pelle Andrea 2001. A mellőzött szabadság, avagy adatvédelem a drogpolitikában. *Fundamentum,* 1. sz.

Petrik Ferenc 2001. *A személyiség jogi védelme és a sajtóhelyreigazítás.* Budapest, HVG-Orac.

A Polgári Törvénykönyv magyarázata 2001. Budapest, KJK-Kerszöv.

Polyák Gábor 2002. Hatalomleosztás. In *Médiakönyv 2002.* Budapest, Enamiké.

Polyák Gábor 2003. Az elektronikus szolgáltatások adatvédelme. Németországi szabályozás, hazai iránymutatással. *Napi Jogász,* 3. sz.

Pulay András – Sziklássy Fábián – Tóth Péter – Udvaros H. Vilmos 1997. *Védd magad az Interneten – biztonságtechnika a számítógépes hálózatokon.* Budapest, Kossuth.

Reidenberg, Joel R. – Schwartz, Paul M. 1998. *On-line Serives and Data Protection and Privacy*. Annex to the Annual Report 1998 of the Working Party established by Article 29 of Directive 95/46/EC. Brussels, European Commission, DG Internal Market and Financial Services.

Rivest, Ron 1992. The MD5 Massage Digest Algorithm. Request for Comments 1321. *Internet Engineering Task Force,* April.

Rosen, Jeffrey 2000. *The Unwanted Gaze – The Destruction of Privacy in America*. New York, Random House.

Rosenoer, Jonathan 1997. *CyberLaw: the Law of the Internet*. New York, Springer.

Roßnagel, Alexander 2002. Marktwirtschaftlicher Datenschutz im Datenschutzrecht der Zukunft. In Bäumler–Mutius.

Sachs, Michael (Hrsg.) 2006. *Grundgesetz. Kommentar.* München, Beck.

Saeltzer, Gerhard 2004. Sind diese Daten personenbezogen oder nicht? *Datenschutz und Datensicherheit,* 4. sz.

Sári János 2000. *Alapjogok (Alkotmánytan II)*. Budapest, Osiris.

Sárközy Tamás – Pázmándi Kinga (szerk.) 2002. *Az információs társadalom és a jog átalakulása.* Budapest, MTA Társadalomkutató Központ.

Schoeman, Ferdinand D. (ed.) 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, Cambridge University Press.

Schoeman, Ferdinand D. 1984a. Privacy: Philosophical Dimensions of the Literature. In Schoeman.

Schwartz, Paul M. 2002. Privacy, Participation, Cyberspace: An American Perspective. In Baeriswyl–Rudin.

Sólyom László 1983. *A személyiségi jogok elmélete.* Budapest, Közgazdasági és Jogi Könyvkiadó.

Sólyom László 1985. Mit szabad és mit nem? Capriccio polgári jogi témákra. *Valóság,* 8. sz.

Sólyom László 1988a. Adatvédelem és személyiségi jog. *Világosság,* január.

Sólyom László 1988b. Egy új szabadságjog: az információszabadság. *Valóság,* szeptember.

Sólyom László 2001a. *Az alkotmánybíráskodás kezdetei Magyarországon*. Budapest, Osiris.

Sólyom László 2001b. Az ombudsman „alapjog-értelmezése" és „normakontrollja". In Majtényi.

Sólyom László 2005. Az adatvédelem és információszabadság jogi előtörténete Magyarországon. In: Majtényi.

Spindler, Gerald – Börner, Fritjof (Hrsg.) 2003. *E-Commerce-Recht in Europa und den USA*. Berlin, Heidelberg, Springer.

Szabó Endre 2004. Az adatvédelmi biztos első féléves tevékenysége. *Infokommunikáció és Jog,* 2. sz.

Szabó Máté Dániel 2002. Alkotmányossági kérdések a köztisztviselői eskü záradékával kapcsolatban. *Fundamentum,* 1. sz.

Szabó Máté Dániel 2003. A tanulók személyes adatainak kezelése a közoktatási intézményekben. In Szabó Máté Dániel (szerk): *Védett adataink*. Budapest, Társaság a Szabadságjogokért.

Szabó Máté Dániel 2004a. Biometrikus azonosítás és adatvédelem. *Acta Humana,* 1. sz.

Szabó Máté Dániel 2004b. Kameraügyben a helyzet változatlan. http://adatvedelem.vilaga.hu.

Szabó Máté Dániel 2004c. „Erős jogvédő szemlélettel, de a törvényi felhatalmazás keretein belül kell dolgoznunk" – beszélgetés Péterfalvi Attila adatvédelmi biztossal. *Fundamentum,* 4. sz.

Székely Iván 1994. *Az adatvédelem és az információszabadság filozófiai, jogi, szociológiai és informatikai aspektusai*. Budapest. Kézirat (kandidátusi értekezés).

Szikinger István 1997. Díszítőelem vagy tartóoszlop? [Az adatvédelmi biztos] *Fundamentum,* 1. sz.

Szurday Kinga 1994. Az adatvédelmi jogi szabályozás szerepe, feladatai és hatása a közigazgatásra és a versenyszférára. *Magyar Jog,* 11. sz.

Tóth Gábor Attila 1997. *A drogfogyasztók adatainak védelme*. Budapest, Alkotmány- és Jogpolitikai Intézet.

Tóth Gábor Attila 2001. „A társadalom kezd elfordulni jogállami eszményeitől" – Majtényi László távozó adatvédelmi biztossal Tóth Gábor Attila beszélget. *Fundamentum,* 2. sz.

Törő Károly 1979. *Személyiségvédelem a polgári jogban*. Budapest, Közgazdasági és Jogi Könyvkiadó.

Trócsányi Sára 1999. Információs kárpótlás helyett. *Fundamentum,* 1. sz.

Trócsányi Sára 2004. *A kommunikáció jogi alapjai.* Budapest, Osiris.

Trócsányi Sára – Farkas Mirella 1997. *Faji eredet, vallási hovatartozás az adatkezelésben.* Budapest, Alkotmány- és Jogpolitikai Intézet.

Urbán László 1995. Közcélú szabályozás hatáselemzése (Public policy elemzés). *Közgazdasági Szemle,* 3. sz. (http://epa.oszk.hu/00000/00017/00003/0304.html)

Verebics János 2001. *Az elektronikus gazdasági kapcsolatok joga*. Budapest, HVG–Orac.

Világhy Miklós – Eörsi Gyula 1965. *Magyar polgári jog.* I–II. Budapest.

Vossbein, Reinhard 2002. Auditierung und Zertifizierung des Datenschutzes – erste Schritte, Möglichkeiten und Probleme. In Bäumler–Mutius.

Warren, Samuel D. – Brandeis Louis D. 1984: The right to privacy [The implicit made explicit]. In Schoeman.

Westin, Alan 1984. The Origins of Modern Claims to Privacy. In Schoeman.

Zombor Ferenc 1998. Drágán keveset – A magánszféra korlátozása és a sikeres bűnüldözés. *Fundamentum,* 4. sz.