AZ ADATVÉDELMI BIZTOS BESZÁMOLÓJA
2007

AZ ADATVÉDELMI BIZTOS BESZÁMOLÓJA

2007

Adatvédelmi Biztos Irodája
Budapest, 2008

Kiadja az Adatvédelmi Biztos Irodája
Felelős kiadó: Dr. Péterfalvi Attila
HU ISSN 1416 - 9762
Nyomda és kötészet: Argumentum Kiadó és Nyomda Kft.
Borító terv: Király Ildikó

TARTALOM

ELŐSZÓ

Tisztelt Olvasó!

Jelen Beszámolót mint az adatvédelmi biztos jogkörét gyakorló országgyűlési biztos terjesztem az Országgyűlés elé, az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény 2. § (4) bekezdése alapján.

Korábban is előfordult, hogy év közben szűnt meg országgyűlési biztos megbízatása, így az előterjesztő nem csak a saját munkájáról számolt be. Most azonban más a szituáció, 2007 olyan év volt, amely során az adatvédelmi biztosi pozíciót – néhány nap kivételével – ugyanaz a személy, dr. Péterfalvi Attila töltötte be, ugyanakkor természetesen jelen Beszámolót sajátomként is vállalom.

Budapest, 2008. március

Dr. Szabó Máté
az állampolgári jogok országgyűlési biztosa,
az adatvédelmi biztos jogkörében eljárva

BEVEZETŐ

Az adatvédelmi biztosi intézmény tizenkettedik éve volt 2007, a „jubileum" az év közepére esett. Nem kerek évforduló, ez az év mégis jelentős volt: a második adatvédelmi biztos hat éves megbízatása járt le, az első biztos mandátumának megszűnését követő fél éves szünet miatt az év végén, decemberben. Sajnálatos, hogy a második ciklus úgy ér véget, mint az előző: bizonytalanságban, úgy, hogy az Országgyűlés nem tudott utódot választani. Külön sajnálatos ez a biztosi intézmény természetéből adódóan: itt nincs testület, nincs hatáskörrel rendelkező apparátus, az országgyűlési biztos egy személyben gyakorolja jogait. Igaz, hogy a vonatkozó törvény módosításának köszönhetően mára egyértelmű a helyettesítés rendje, ez mégis csak félmegoldás. Ennek oka elsősorban az, hogy az adatvédelmi biztos tevékenysége feladatköréből, sajátos jogosítványaiból, nemzetközi jellegű és az Európai Unióhoz köthető kötelezettségeiből adódóan az ombudsman intézményétől kissé idegen.

A fenti hasonlóságtól eltekintve a második ciklus sokban különbözött az előzőtől. A legnagyobb különbség az ügyszám: míg 2001 előtt százas nagyságrendről beszéltünk, mára ezrekben mérhető a vizsgálatok száma, és bár az apparátus növekedési üteme nem követte teljesen a munkateher változását, az ügyintézési határidő nem nőtt. Érdekes, hogy az ügyszámnövekedés mögött nem áll valamiféle konkrét indikátor, ezt mutatja az, hogy szinte valamennyi területen többé-kevésbé azonos ütemű a növekedés. Egyformán nőtt az adatvédelem, az információszabadság, és a jogszabálytervezetek véleményezésével kapcsolatos munka. A legjelentősebb változás, a nemzetközi ügyek megjelenése jellegéből adódóan úgy jelent többletmunkát, hogy az a statisztikában nem jelenik meg. Aki a részletes adatokra kíváncsi, elolvashatja az éves beszámolók erről szóló fejezeteit.

Ha az elmúlt hat év legmarkánsabb változását keressük, kétségkívül hazánk Európai Unióhoz való csatlakozásáról kell szólni. Az adatvédelmi biztosnak korábban is voltak nemzetközi jellegű kötelezettségei, ez azonban más jellegű volt. Az Unió valamennyi tagállamában egy 1995-ben elfogadott Irányelv alapján szabályozott a személyes adatok védelme, és valamennyi tagállamban működik – az Irányelv alapján – adatvé-

delmi hatóság. Ezen hatóságok képviselőiből áll az úgynevezett 29-es Munkacsoport (az elnevezés oka, hogy a Munkacsoportról az Irányelv 29. cikke szól), melynek a magyar adatvédelmi biztos is tagja. A csatlakozás azonban lényegesen többről szólt, mint egy újabb testületi tagságról, ennek részeként elengedhetetlen volt az adatvédelmi törvény harmonizálása az Irányelvvel. Ez szükséges volt, hiszen az inkább alapjogi természetű törvény több szempontból ellentétes volt az inkább gyakorlatias, a gazdasági élet szükségszerűségeit is szem előtt tartó Irányelvvel. Ugyanakkor nehéz is volt, hiszen az adatvédelmi törvény módosítása kétharmados többséget igényel. Így csak a legszükségesebb változtatásokra került sor, melyek jelentősen kiegészítették az adatvédelmi biztos jogkörét is, beépítve egy hatósági jellegű hatáskört.

Az uniós tagsággal járó lényeges többletfeladat abból adódik, hogy az Unió tevékenysége számos ponton érinti a személyes adatok védelméhez való jogot. Akár a jelen beszámoló, akár a korábbiak nemzetközi ügyekről szóló fejezete láttatja ezen tevékenység sokszínűségét. Az egyik lényeges terület a jogalkotásban való közreműködés, valamint az egyes adatkezelési módszerekről való véleményalkotás. A másik fontos kérdéskör a bel- és igazságügyi együttműködésből fakad, amely az adatvédelmi biztosnak ellenőrzési feladatokat jelent. Ennek egyik jelentős eleme a Schengeni Információs Rendszer, melyhez hazánk nem sokkal 2007 vége előtt csatlakozott. Ez volt talán az elmúlt időszak legfontosabb eseménye a nemzetközi ügyek között, ennek megfelelően a vonatkozó fejezet részletesen tárgyalja.

Az adatvédelmi biztos által védett két jog közül az egyiket, a közérdekű adatok nyilvánosságát a csatlakozás kevésbé érintette, mivel az Unió hatáskörébe tartozó kérdések elsősorban az adatvédelem területére hatnak ki. Ugyanakkor a csatlakozás következtében egyre intenzívebbé váltak a kapcsolatok a többi tagállammal, és bár a külföldi gyakorlatot korábban is tanulmányoztuk, ma még inkább odafigyelünk arra, hogy adott kérdést hogyan kezelik a többi tagállamban. Emellett természetesen van közvetlen vonatkozása is az Uniónak az információszabadságra: egyrészt az Unió, illetve intézményei maguk is kezelnek közérdekű adatot, másrészt az egyre intenzívebbé váló uniós jogalkotás az információszabadságot sem hagyta érintetlenül.

Az információszabadságot ettől függetlenül is jellemezte egy igen erőteljes ügyszám-növekedés, és a terület nem volt mentes az érzékeny, nagy

érdeklődésre számot tartó vizsgálatoktól sem (ezek közül elég csak a rendőrségi jelentések nyilvánosságára utalni). Visszatérő, nagy jelentőségű kérdésként 2007-ben is sokat foglalkoztunk a bíróságok működésének nyilvánosságával, valamint a közpénzek átláthatóságával.

2001-ben, éppen a két biztos közötti időszakban történt az ikertornyok elleni támadás New York-ban, és ez máig számottevő hatással van a munkánkra. Ezt követően ugyanis a demokratikus országok a zászlajukra tűzték a terrorizmus elleni harc célját, amely fontosságát vitatni nem lehet, az eszközei viszont sokszor igencsak megkérdőjelezhetőek. Mert mi is a legfőbb eszköz? A válasz egyszerű: a megfigyelés. A nyomozó hatóságok egyre több jogot kívánnak maguknak azért, hogy titokban, minimális garanciákkal adatot gyűjthessenek bárkiről, bárhogy. A biztonsági kérdések szakértői a különböző adatkezelések összekapcsolásában látják azt az eszközt, amely pótolhatatlan a terrorcselekmények megelőzésében és felderítésében. Kevesen veszik észre, hogy az egységes nyilvántartási rendszerek felvázolt modellje alig-alig különbözik attól, amely a rendszerváltozás előtt az állam legfőbb eszköze volt a polgárok ellenőrzésére. Mindeközben folyamatosan jelennek meg az új adatkezelési technológiák; leglátványosabb talán a biometrikus azonosítási rendszerek térhódítása volt.

Nem marad persze adós a magánszféra sem. Itt viszont sokrétűek a célok, és változnak is, de a lényeg ugyanaz: a döntéshozók csak adatkezeléssel vélik őket megvalósíthatónak. Ma már mindennapos, hogy magánszféránkból – azért, hogy biztonságban legyünk, hogy védjék vagyonunkat, hogy vélt visszaélésektől óvjanak meg (kiket is?) – állandóan fel kell adnunk, a munkahelyen, bankban, biztosítónál. És persze olyan is van, hogy az adatkezelés mögötti cél változik: így lett a bankok által áhított pozitív adóslista legfőbb indoka az eladósodottság megállítása, holott eredetileg még azzal indultunk, hogy ezáltal a hitelek válnak olcsóbbá.

A brit Privacy International nevű szervezet, közösen az amerikai Electronic Privacy Information Center-rel 1997 óta minden évben felméri a megfigyelésnek és a magánélet védelmének szintjét. Nem meglepő, hogy 2007-ben mindenhol csökkenésről számoltak be. A korábban az adatvédők számára példának tekintett Németország a 2006-os elsőségét cserélte 2007-ben egy hetedik helyre. A felmérés igen kritikus volt, éppen ezért nem lehet elmenni amellett, hogy hazánk az Unión belül az előkelő második helyet szerezte meg. Ez azt jelenti, hogy a magánszféra védelme nálunk még viszonylag megfelelő. Bízzunk benne, hogy ez a szint nem fog csökkenni.

Végezetül még egy megjegyzés: a beszámoló az immár tizenkét éve megszokott szerkezetet követi. Bár ez elvileg egy személy, az adatvédelmi biztos munkája, a szövegben általában többes szám első személy szerepel. Ez természetesen nem királyi többes, hanem a biztost és munkatársait jelöli. Ennek oka nem csupán az, hogy az Adatvédelmi Biztos Irodájának munkatársai részt vesznek a beszámoló elkészítésében. Sokkal inkább az, hogy az ő munkájukból adódik össze az, ami a „külvilág" felé az adatvédelmi biztos tevékenységeként, eredményeként jelenik meg. Így utolsó biztosi beszámolómban ezúton is megköszönöm áldozatos munkájukat, amellyel úgy hiszem, sikeresen járultak hozzá a magánszféra védelméhez és a közérdekű adatok nyilvánosságához.

Dr. Péterfalvi Attila

I. TEVÉKENYSÉGÜNK FŐBB ADATAI

Az Adatvédelmi Biztos Irodájában 2007-ben összesen 2724 vizsgálat indult meg, vagyis ennyi volt a hozzánk beérkező olyan iratok, levelek, küldemények száma amelyet ügyként kezeltünk, és az iroda elektronikus iktatórendszerében (ELIK) nyilvántartásba vettünk. Ez a hatalmas ügyszám minden korábbi évet messze felülmúl. A korábbi legmagasabb ügyszám 2005-ben 2350 beadvány volt. A 2724 vizsgálat során 2008. január 31-ig összesen 9153 iratot dolgoztunk fel. A valamilyen intézkedést igénylő iratok száma meghaladta a 13000-et.

Az iroda elektronikus levélforgalma a következőképpen alakult. A kéretlen e-maileket, spameket leszámítva összesen 3319 intézkedést igénylő e-mail érkezett az Adatvédelmi Biztos Irodája hivatalos postafiókjába az adatved@obh.hu címre, melyek közül 1244 levelet ügyként iktattunk. Ez 365-el több az előző évnél. (2005-ben 730, 2006-ban 879 új ügy érkezett be villámpostán.) Az utóbbi három év adatainak összevetése után megállapítható, hogy az elektronikus indítványozási kedv is megnőtt. A jogszabály előkészítések során a kodifikációt végzők 2007-ben 574 jogszabály tervezetet küldtek elektronikus formában véleményezésre. Ez az előző évhez képest jóval több ügyet jelent, ám azt is figyelembe kell venni, hogy a jogalkotás intenzitása 2007-ben megnőtt. A már folyamatban levő vagy lezárt ügyekhez 690 e-mail érkezett. Az egyéb tárgyú megkeresések, tájékoztatók, elektronikus hírlevelek száma 167 volt. Külföldről összesen 617 e-mail érkezett, ezek a különböző uniós bizottságok, munkacsoportok, illetve az Európai Unió adatvédelmi biztosának hivatalából érkező, valamint az ombudsmanok, adatvédelmi biztosok és hatóságok nemzetközi együttműködését, kapcsolattartását, információcseréjét szolgáló küldemények voltak, de volt köztük konzultációs, illetve panaszbeadvány is. 2007 márciusa óta üzemel, és ugyanezen célok szolgálatába állt a privacy@obh.hu elektronikus postafiók is, melyet a Nemzetközi Főosztály használ. Ebbe összesen 765 e-mail érkezett. Külön említjük meg az Európai Unió 29-es munkacsoportját, amelytől egy év alatt további 220 e-mailt kaptunk. Vagyis a nemzetközi e-mail forgalmunk összesen 1602 volt. Miként a korábbi években már a jogszabály–véleményezésről, ettől az évtől kezdődően a nemzetközi ügyeinkről is kijelenthető, hogy szinte teljes mértékben megvalósult a

„paperless office", vagyis a feleslegesen papírt használó, és ez által pazarló ügyintézés megszűnt. Az Országgyűlési Biztos Hivatala levélszerverére érkező elektronikus küldemények szűrését ellátó rendszeren 67151 kéretlen levél, spam jutott át és érkezett meg a postaládánkba, amelyek kezelése és „humán szűrése" jelentős többletmunkát ró az iroda munkatársaira.

Az iroda által ügyként kezelt és iktatott iratok száma (2724) – az előző évhez viszonyítva (2211) – több mint 23 százalékkal, 513 üggyel nőtt, tehát a több éve tartó, drasztikus ügyszámemelkedés a tavalyi megtorpanást követően ismét folytatódott. A jogszabály-véleményezések száma 278-ról 517-re, a panaszügyeké 1241-ről 1435-re, a konzultációs ügyeké 434-ről 504-re emelkedett. A nemzetközi ügyek száma 145-ről 127-re csökkent. Kiemelendő, hogy a panaszügyek száma évről-évre jelentősen emelkedik.

Az Adatvédelmi Biztos Irodájába érkezett ügyek megoszlása

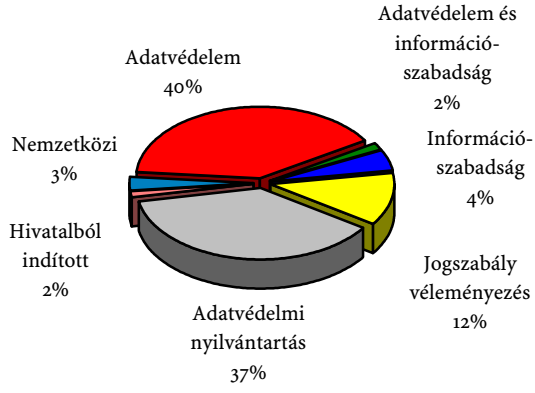
Ebben az évben a korábbi évekhez hasonló rendszerben, áttekinthető és egyszerű ábrákon szemléltetjük az irat és ügyforgalmat bemutató statisztikai elemzést. Az adatvédelmi nyilvántartás a már jól megszokott módon önálló fejezetben szerepel. Az összes, vagyis a 2724 ügyből, az adatvédelmi ügyek száma 1700 (1524), a jogszabály-véleményezéseké 517 (278), az információszabadságot érintő ügyek száma 193 (169) volt, illetve 75 (45) beadvány mindkét alkotmányos alapjogot érintette. Az információszabadságot is érintő ügyeink száma tehát összesen 268 (214). A nemzetközi ügyeink száma 127 (145) volt. (A zárójelben feltüntetett adatok az előző, 2006. évre vonatkoznak.) Hivatalból összesen 70 (27) vizsgálat indult, titokvédelmi tárgyú vizsgálat öt volt. Az adatvédelmi nyilvántartásba küldött iratok (bejelentkezések, módosítások, törlések) száma 991 volt, az elutasított személyes, illetve közérdekű adatokra vonatkozó kérelmekről a kézirat lezárásáig 381 jelentést kaptunk. A jelentések beküldésének határideje 2007. február 1-je, de a több éves tapasztalat azt mutatja, hogy ez követően, illetve a kézirat lezárása (február 15.) után is igen sok jelentés érkezik.

Ha az adatvédelmi biztos hatáskörébe tartozó két információs alapjogot érintő beadványok számát, illetve arányát vesszük szemügyre,

akkor megállapítható, hogy az információszabadságot és a közérdekből nyilvános adatokat is érintő ügyek (268) aránya az adatvédelemhez képest közel 16 százalék, ez az adat az elmúlt évek adataihoz képest folyamatosan kis mértékű (egy százalékot meghaladó) emelkedést mutat.

Az Adatvédelmi Biztos Irodájába érkezett ügyiratok és nyilvántartási kérelmek

2007 (%)



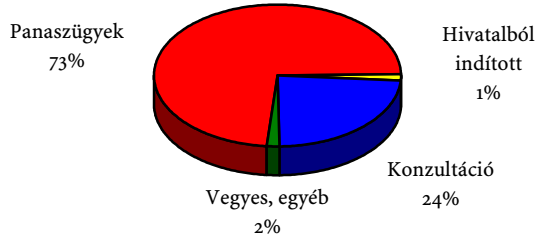
A vizsgálatok általános jellemzői

A főbb ügytípusok

A 2724 iktatott ügyirat közül ebben az évben 1380 adatvédelemmel és információszabadsággal kapcsolatos panaszügy érkezett, ez tizenegy százalékos emelkedésnek felel meg. Megjegyzendő, hogy vannak egyéb tárgyú panaszügyek is, melyek száma 54 volt. A konzultációs beadványok száma 434-ről 504-re emelkedett. A jogszabály-véleményezések száma jelentősen, 278-ról 517-re emelkedett. A nemzetközi ügyeink száma 127 volt, számuk csökkent. A nemzetközi és európai ügyek részletes ismertetése a beszámoló Nemzetközi ügyek fejezetében olvasható.

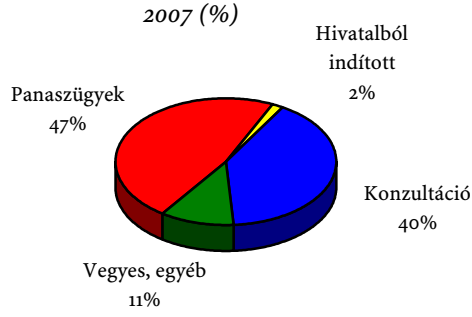
Az adatvédelmet érintő 1736 ügy megoszlása a következőképpen alakult: részben vagy egészben adatvédelmi panaszügy 1271, adatvédelemmel kapcsolatos konzultációs ügy 412, hivatalból indított adatvédelmi vizsgálat 26 volt. A 27 egyéb, illetve vegyes ügy körébe az információs jogok védelmével kapcsolatos levelezések, tájékoztatók, előadások, konzultációk, tárgyalások írott anyagai tartoznak.

Az adatvédelmi ügyek megoszlása
2007 (%)



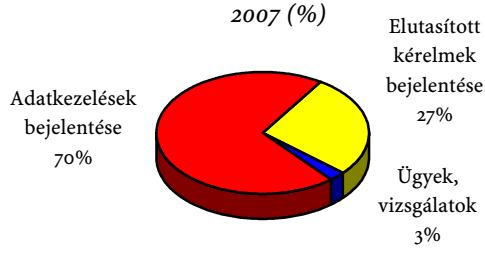
Kizárólag az információszabadságot, vagyis a közérdekű adatok nyilvánosságát érintő ügyek száma 229. Ebből 108 panasz, 92 konzultációs ügy, és 4 hivatalból indított vizsgálat volt, 25 egyéb, illetve vegyes ügy volt.

A közérdekű adatok nyilvánosságát érintő ügyiratok megoszlása
2007 (%)



Az adatvédelmi nyilvántartásba beküldött adatkezelési bejelentéseket, valamint az elutasított személyes és közérdekű, vagy közérdekből nyilvános adatokra vonatkozó elutasított kérelmekről adott jelentéseket az Adatvédelmi Nyilvántartási Főosztály külön iktatási rendszerben tartja nyilván. A vizsgálatot igénylő nyilvántartási ügyek száma 37, az adatkezelési bejelentések száma 991 volt. Az adatvédelmi törvény 13. §-ának (3) bekezdése, valamint a 20. §-ának (9) bekezdése alapján az adatkezelők az érintettek személyes adataik kezelésére vonatkozó tájékoztatási kérelmének számáról, valamint közérdekű adat megismerésére irányuló kérelmek elutasításáról és annak indokairól évente értesítik az adatvédelmi biztost. A beszámoló elkészítéséig összesen 381, 2007. évre vonatkozó jelentés érkezett. Az adatok szolgáltatására felhívó közlemény a honlapunkon, a jelentések statisztikai elemzése az Adatvédelmi Nyilvántartásról szóló fejezetben olvasható.

Az adatvédelmi nyilvántartás ügyiratainak megoszlása
2007 (%)

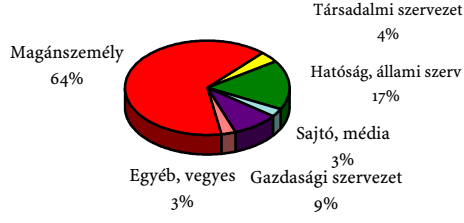


Az indítványozók aránya

Az alábbi ábra az adatvédelmi biztoshoz forduló személyek, szervezetek számáról, illetve arányáról ad tájékoztatást. 2007-ben ismét növekedett azon beadványok (panaszok, konzultációk) száma, amelyeknek indítványozói magánszemélyek voltak: 1425 ügy (2006-ban: 1228). Az indítványozók összetétele, aránya a korábbi évekhez képest nem változott jelentősen. Örvendetes, hogy ebben az évben a sajtó munkatársai részéről jóval több beadványt kaptunk, mint az elmúlt években, összesen 63-at, (tavaly mindössze 23-at) ami az ügyeink 3 százaléka. A gazdasági szervezetek részéről is emelkedett az indítványok száma, összesen 201 (2006-ban mindössze 144) beadvány érkezett, amely az összes ügy 9 százaléka.

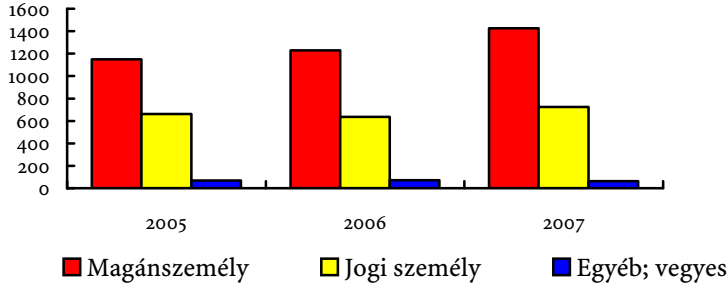
Az indítványozók aránya

2007 (%)



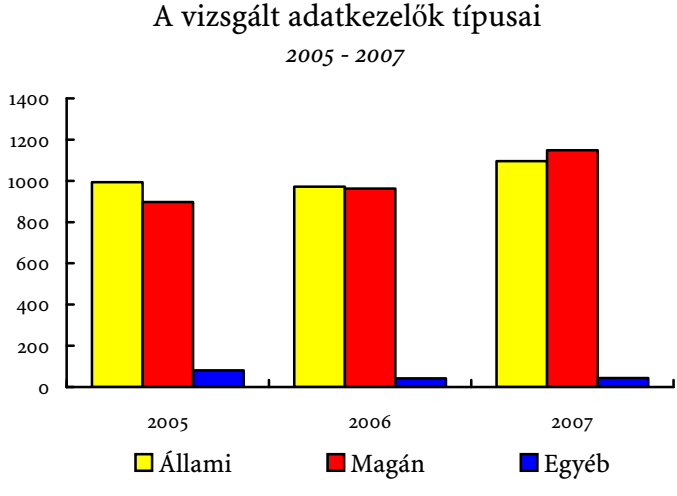
A jogi és a magánszemély indítványozók aránya

2005 - 2007



A vizsgált adatkezelők típusai

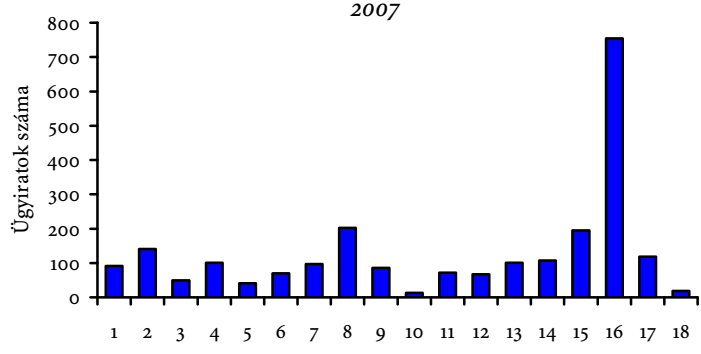
Az adatvédelmi biztos és irodája 2007-ben összesen 2288 (2006-ban 1976) adatkezelőt, illetve az általuk folytatott adatkezelést vizsgált (volt olyan vizsgálat, amelyben több adatkezelő is érintett volt, illetve volt olyan adatkezelő, amely több adatkezelése miatt, különböző vizsgálatok tárgya volt). Az utóbbi három év idősor adatait összehasonlítva megállapítható, hogy 2007-ben először fordult elő, hogy több magán adatkezelőt vizsgáltunk, mint államit. Emelkedett a magán adatkezelőket érintő vizsgálatok száma (963-ról 1149-re) és ugyancsak emelkedett a vizsgált állami-, önkormányzati adatkezelők száma is (971-ről 1096-ra).



A vizsgált adatkezelők kategóriái

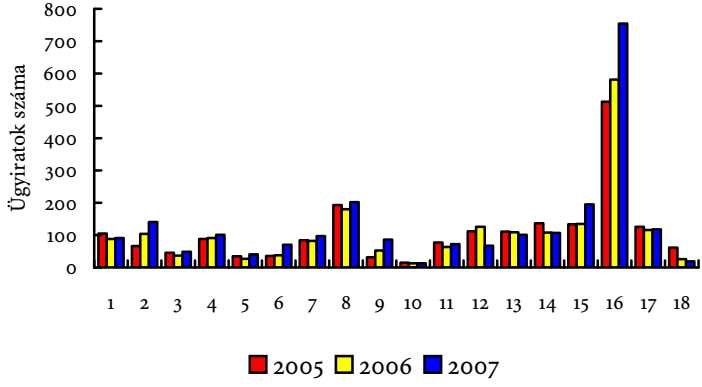
A vizsgált adatkezelők között 754 vizsgálattal továbbra is első helyen kell megemlíteni a nyilvántartási rendszerünk szerint az „egyéb" kategóriába tartozó adatkezelőket. Ezek között találhatóak a gazdasági társaságok adatkezelései 418 vizsgálat, magánszemély adatkezelőket érintő vizsgálatok 164, munkáltatók adatkezelései 85, társasház, lakásszövetkezet 42, direktmarketing és piac-, illetve közvélemény kutató társaságok 25 vizsgálattal. Az egyéb kategóriába soroltuk a kéretlen, üzleti célú reklámot, ajánlatot tartalmazó elektronikus levelekre (spam-ekre) vonatkozó vizsgálatokat is, melyek száma tovább emelkedett. Az egyéb közhatalmi szerveket (bíróságok, ügyészségek, dekoncentrált közigazgatási szerveket) érintő beadványok száma 104-ről, 141-re emelkedett. Növekedett továbbá az államigazgatási jogkörben eljáró egyéb szerveket érintő vizsgálatok száma 52-ről, 86-ra, és a közüzemi szolgáltatók ügyeiben is több vizsgálat folyt, 135-ről 195-re emelkedett az ügyek száma. Az adóhivatalt és a pénzügyőrséget érintő vizsgálatok is megszaporodtak, 38-ról 70-re nőtt a számuk.

A vizsgált adatkezelők kategóriái



A vizsgált adatkezelők kategóriái

2005 - 2007



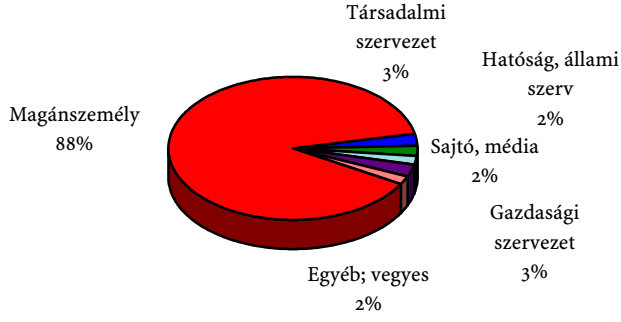
1 Központi közigazgatási szerv
2 Egyéb közhatalmi szerv
3 Nemzeti adatbázis, nagy adatkezelő
4 Fegyveres és rendvédelmi szerv
5 Társadalombiztosítás/munkaügy
6 Adóhivatal, pénzügyőrség
7 Egészségügyi intézmény
8 Helyi önkormányzat és szervei
9 Államigazgatási jogkörben eljáró egyéb szerv
10 Szakosított felügyeleti szerv
11 Oktatási intézmény/kutatóintézet
12 Társadalmi szervezet
13 Sajtó/média
14 Pénzintézet
15 Közüzemi szolgáltató
16 Egyéb adatkezelő (áruküldők, társasházak, munkáltatók…)
17 Külföldi adatkezelő
18 Nincs adatkezelő

Panaszügyek

Ha az adatvédelmi biztoshoz forduló állampolgárt konkrét jogsérelem érte, vagy annak közvetlen veszélye állt fenn, a beadványát panaszügyként kezeljük. E fejezetrész tehát már csak azon vizsgált ügyek halmazát elemzi, amelyek konkrét panaszt, bejelentést tartalmaztak. A panaszügyeknek alapvetően két fajtáját különböztethetjük meg. Az egyik esetben az indítványozó vizsgálat lefolytatása nélkül a hatályos jogszabályok, a csatolt dokumentumok, illetve az általa leírtak alapján kér az ügyre vonatkozó (általános) állásfoglalást az adatvédelmi biztostól és kéri, hogy tájékoztassuk a jogorvoslati lehetőségekről. Ebben az esetben az érintett adatkezelő általában nem is szerez tudomást a vizsgálatról csak akkor, ha az olyan általános vagy fajsúlyos jogsértést tár fel, amelyet mindenképpen orvosolni kell. Ha „csupán" egyéni jogsértést állapítunk meg az indítványozó joga eldönteni, hogy kéri-e az adatvédelmi biztos közbenjárását és eljárását az ügyében, vagy saját maga fordul az adatkezelőhöz és érvényesíti jogait. A másik esetben az indítványozó eleve igényli a panaszolt adatkezelés és adatkezelő vizsgálatát. A jogsérelmet leíró, vagyis panaszügyként kezelt beadványok száma 2007-ben 1435 (2006-ban 1241) volt. A panaszvizsgálatok száma tehát tovább nőtt, még soha ennyi panaszt nem nyújtottak be az adatvédelmi biztoshoz, mint 2007-ben. A vizsgált panaszügyek indítványozóinak összetétele, aránya a következő: a magánszemély panaszosok aránya nem változott számottevően, ezúttal is a már megszokott 88 százalék volt. A társadalmi szervezetek 42, hatóságok, állami szervek 29, gazdasági szervezetek 41 panaszt nyújtottak be. Miként az összes indítványnál, a panaszügyeknél is megfigyelhető a sajtó, média képviselőinek élénkülő indítványozó kedve, 29 panaszügyet terjesztettek elő az előző évi 12-höz képest.

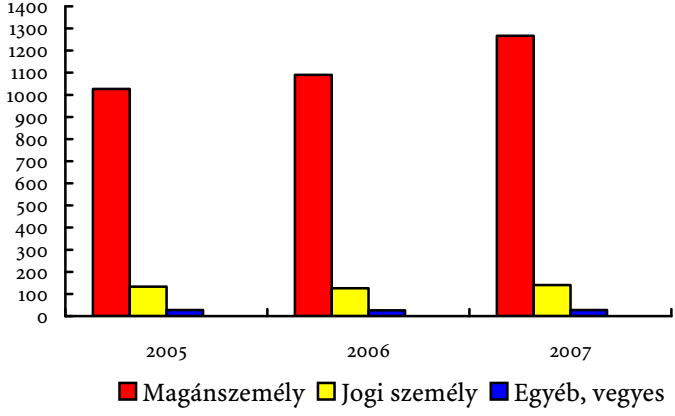
A panaszosok aránya

a 2007. év panaszügyeiben (%)



A jogi és a magánszemély panaszosok aránya

panaszügyek 2005 - 2007

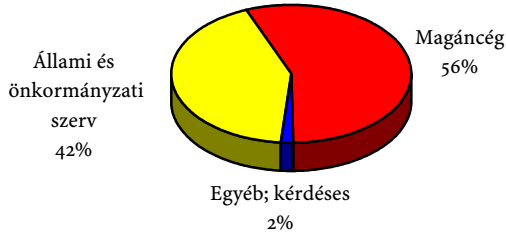


A bepanaszolt adatkezelők típusai

2007-ben a kifogásolt adatkezelések száma nem változott számottevően, az indítványozók összesen 1531 adatkezelőt, illetve adatkezelést kifogásoltak. Egy indítvány több, illetve többféle panaszt is tartalmazhat, sőt előfordul, hogy mindkét alapjogot érinti, vagy ami szintén nem ritka, hogy a két alapjog konfliktusa, vélt vagy valós ütközése a beadvány tárgya. 2007-ben a bepanaszolt adatkezelések 42 százaléka állami, önkormányzati, 56 százaléka valamely magánszervezet vagy személy adatkezelését érintette. Az elmúlt évek folyamatait, arányait is figyelembe véve ezen adat azt jelzi, hogy nemcsak megfordult a magán, illetve az állami, önkormányzati adatkezelések panaszolásának aránya, hanem a kifogásolt magán adatkezelések száma és aránya évről-évre tovább nő.

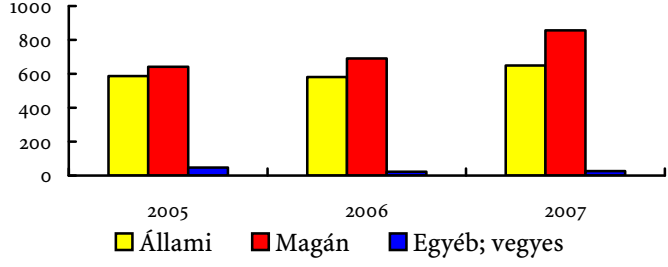
A bepanaszolt adatkezelők típusai

a 2007. év panaszügyeiben (%)



A bepanaszolt adatkezelők típusai

panaszügyek 2005 - 2007

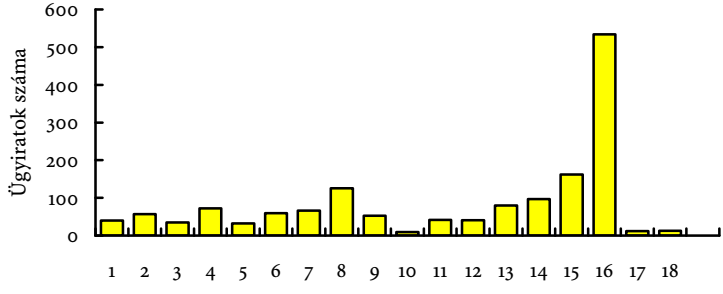


A bepanaszolt adatkezelők kategóriái

2007 folyamán a legtöbb panaszbeadvány az egyéb adatkezelőkkel szemben (magánszemélyek, egyéb gazdasági társaságok, munkáltatók, társasházak, áruküldők, közvélemény kutatók) érkezett, összesen 534 panaszt vizsgáltunk (szemben a tavalyi 412 esettel). A közüzemi szolgáltatókat 162, a helyi önkormányzatok és hivatalok eljárását 126, a pénzintézeteket 97, az adóhivatal, illetve a pénzügyőrség adatkezelését 59 esetben, az államigazgatási jogkörben eljáró szervek eljárását 53 beadványban kifogásolták a panaszosok. 2007-ben mindössze két adatkezelői kategóriában csökkent a panaszok száma: az egyik a központi közigazgatási szervek, vagyis a minisztériumok, a másik a társadalmi szervezetek, pártok, alapítványok, egyesületek. Ez azért is érdekes, mert mindkét kategóriában növekedést tapasztaltunk az elmúlt években. A legszembetűnőbb növekedés a már részletezett egyéb adatkezelők mellett a közüzemi szolgáltatóknál, a helyi önkormányzatoknál, és az egyéb közhatalmi szerveknél tapasztalható.

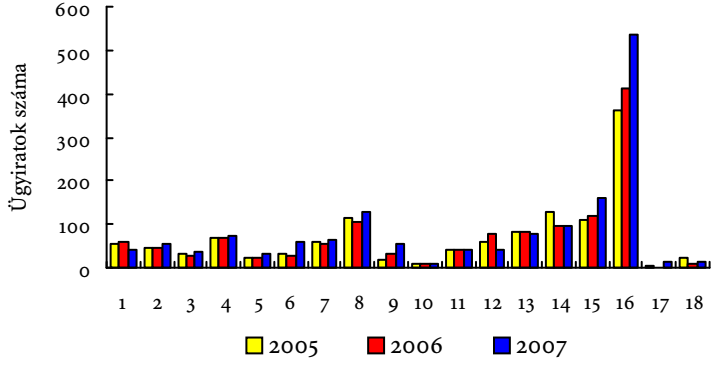
A bepanaszolt adatkezelők kategóriái

a 2007. év panaszügyeiben



A bepanaszolt adatkezelők kategóriái

panaszügyek 2005 - 2007



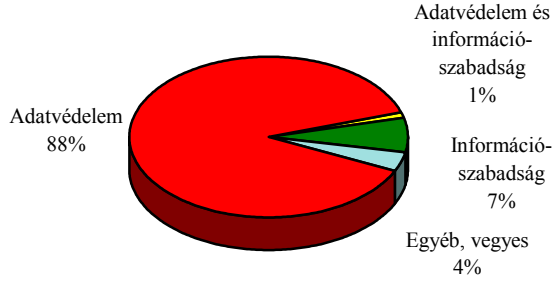
1 Központi közigazgatási szerv
2 Egyéb közhatalmi szerv
3 Nemzeti adatbázis, nagy adatkezelő
4 Fegyveres és rendvédelmi szerv
5 Társadalombiztosítás/munkaügy
6 Adóhivatal, pénzügyőrség
7 Egészségügyi intézmény
8 Helyi önkormányzat és szervei
9 Államigazgatási jogkörben eljáró egyéb szerv
10 Szakosított felügyeleti szerv
11 Oktatási intézmény/kutatóintézet
12 Társadalmi szervezet
13 Sajtó/média
14 Pénzintézet
15 Közüzemi szolgáltató
16 Egyéb adatkezelő (áruküldők, társasházak, munkáltatók…)
17 Külföldi adatkezelő
18 Nincs adatkezelő

Információs ágak a panaszügyekben

Az összes panaszügy (1435) közül személyes adataik kezelése miatt 1264-en tettek panaszt. A közérdekű adatok kezelésének gyakorlatát 117 esetben kifogásolták az adatvédelmi biztosnál. A panaszügyekben, információs ágak szerinti megoszlását tekintve, ismét nagyon magas az adatvédelem aránya (88 százalék), míg az összes ügyet tekintve a mindkét alapjogot érintő beadványok száma 75, ebből csupán 17 volt panaszügy. 54 panaszügy nem érintette egyik információs ágat sem. A panaszügyek számának ütemes emelkedésével lépést tartanak az információszabadság érvényesülését kifogásoló panaszok, vagyis a két alapjogot érintő ügyek aránya állandónak mondható.

Információs ágak aránya a panaszügyekben

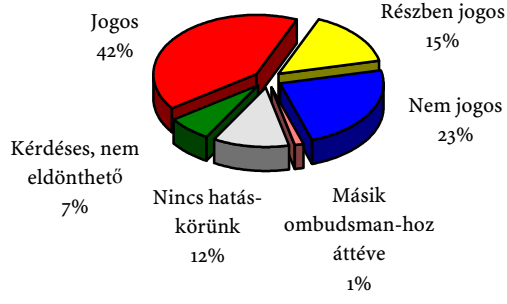
a 2007. év panaszügyeiben (%)



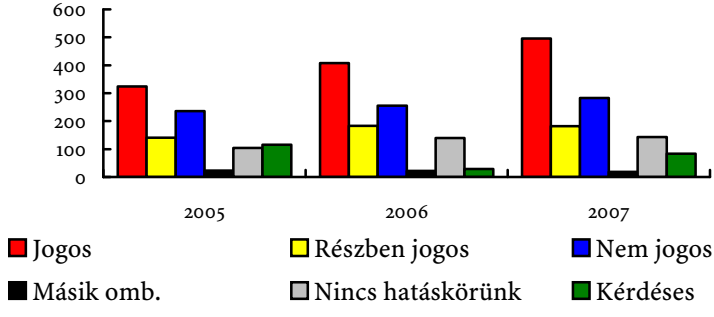
A panaszok jogossága

A már lezárt panaszügyek (1435-ből 1206-ot zártunk le a beszámoló megírásáig, az előző évben ez a szám 1241/1037) 57 százalékában – 678 esetben – állapítottuk meg, hogy jogos vagy részben jogos volt az indítványozó panasza. 2006-hoz képest tehát nem változott a jogos és részben jogos panaszok aránya, viszont ezen belül 4 százalékkal nőtt a jogos panaszok hányada. 143 esetben nem rendelkezett hatáskörrel az adatvédelmi biztos az ügy kivizsgálására, 18 ügyet pedig másik országgyűlési biztoshoz tettünk át. A kérdéses, illetve az adatvédelmi biztosi vizsgálat útján el nem dönthető panaszok száma 84 volt.

A panaszok jogossága
a 2007. év panaszügyeiben (%)



A panaszok jogossága
panaszügyek 2005 - 2007

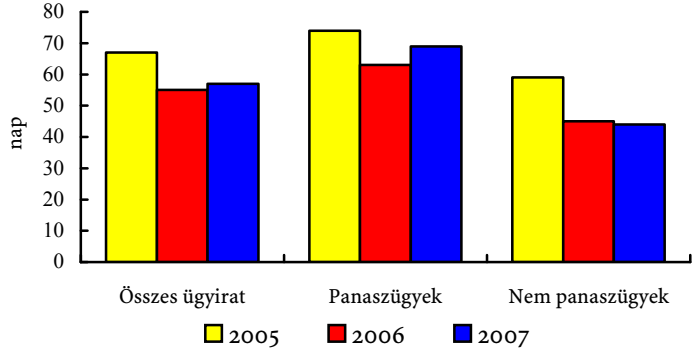


Átlagos ügyintézési idő

Annak ellenére, hogy a beadványok és ezen belül a panaszok száma 2007-ben drámaian megugrott, az átlagos ügyintézési idő ehhez képes alig változott, sőt a nem panasz ügyek esetében tovább tudtuk csökkenteni az ügyintézés idejét. Ennek egyik oka, hogy a jogszabály-véleményezéseket igen rövid, néhány napos határidővel kell elkészítenünk és ebből az ügyfajtából közel kétszer annyi volt, mint tavaly. A grafikon három éves adatainak összehasonlítása után látható, hogy az átlagos ügyintézési idő csupán két nappal emelkedett. A lezárt panaszügyek átlagos ügyintézési ideje az ügyszámnövekedéshez képest sem nőtt számottevően. Míg 2005-ben 72 nap, 2006-ban csak 63 nap, 2007-ben már 69 nap volt az átlagos ügyintézési idő.

Átlagos ügyintézési idő

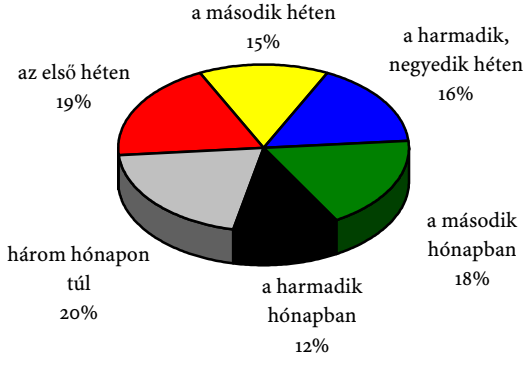
2005 - 2007



Az ügyintézés időtartama 2007-ben a következőképpen alakult. Az iktatott 2724 ügy közül 1362-ben az első hónapban adtunk érdemi választ a beadványt tevőnek, ez az összes ügy fele. A második hónapban további 493 beadványra válaszoltunk, amely további 18 százalékot tesz ki. Ez már az összes lezárt ügy több mint kétharmada. Az ügytorlódás jelei is felfedezhetőek, mivel a harmadik hónapban és azon túl adott érdemi válaszok száma is viszonylag magas (316, illetve 553 ügy). Egyértelmű, hogy az ügyszámnövekedés mértékéhez képest szinte alig változott az

átlagos ügyintézési idő, és egyáltalán nem szokatlan, hogy az adatvédelmi biztos vizsgálata egyes ügyekben elhúzódik. A beszámoló elkészítésekor 398 beadvány – ebből 229 panaszügy – vizsgálata még folyamatban van.

Az ügyintézés időtartama a 2007-es évben
("Hány ügyre válaszoltunk érdemben") %



II. VIZSGÁLATOK

A. Személyes adatok

Bevezetés

A „személyes adatok" címet viselő fejezet bevezetője hagyományosan összefoglalója az előző évnek, és bemutatja azt, hogy a korábbiakhoz képest hogyan alakultak a személyes adatok védelméhez való joggal kapcsolatos vizsgálataink. Az elmúlt év talán legérdekesebb mutatóját a korábbi fejezet már megmutatta: a 2001 óta folyamatos ügyszámnövekedést követő 2006-os „megtorpanás" után 2007-ben ismét emelkedett ügyeink száma. Bár ezen emelkedésen „osztozik" az adatvédelem a közérdekű adatok nyilvánosságával, a jogszabály-véleményezéssel és a nemzetközi ügyekkel, mégis jelen fejezet vonatkozásában is megállapítható: a vizsgálatok száma nagymértékben emelkedett, mind a panaszügyeket, mind a konzultációs ügyeket tekintve.

Mindaddig, amíg az ügyszám folyamatos emelkedéséről számolhattunk be, egyszerű volt a lehetséges okok megtalálása: az érintettek egyre inkább megismerik lehetőségeiket, tudják, hogy milyen esetben lehet az adatvédelmi biztoshoz fordulni, és élnek is e jogukkal, míg az adatkezelők használják az Irodával való konzultáció lehetőségét. Nehéz ugyanakkor az intézmény ismertségének terjedésére fogni azt, hogy egy enyhe megtorpanást miért követett egy markáns növekedés, miközben azt nem előzte meg olyan jelentőségű jogszabály-változás, vagy „ismeretterjesztés" amelynek ez eredménye lehetett volna. Való igaz, hogy 2007-ben is voltak olyan ügyek, melyeket viszonylag nagy számban kifogásoltak az állampolgárok: a gázár-támogatás rendszere, egy-egy spam-kampány, vagy az évek után újra előkerülő, adóazonosítóból születési dátumot generáló függvény elleni panasz (mellyel kapcsolatban a biztos ismét leszögezte: egyrészt az azonosítót kezelő szervek amúgy is birtokában vannak a születési időnek, másrészt az azonosító generálásának alapja ez a dátum, így inkább az lenne a gond, ha nem lenne visszafejthető). Ilyen ügyek azonban korábban is voltak, elég 2006-ra és a választásokra gondolni.

A fentiek okán nem is próbálkozunk meg az ügyszám-növekedés lehetséges okainak elemzésével. Ehelyett bízunk abban, hogy inkább az intézmény ismertsége áll a háttérben, és nem a jogsértések számának növekedése.

Ha a vizsgálatok szerkezetét nézzük, az elmúlt évekhez hasonlóan ismét nagy arányban találjuk meg a gazdasági szféra adatkezelőit, melyek immár „megbízhatóan" több munkát adnak, mint az állami szféra. Ez jelenik meg abban is, hogy a fejezet elején a „nagy adatkezelésekről" egyre rövidebben szólunk, és egyre kevésbé találkozunk nagy horderejű, súlyos jogsértésekkel például a személyi adat- és lakcímnyilvántartás szerve, vagy az adóhatóság esetében. Ezen jelenség mögött nagy valószínűséggel az áll, hogy az állami szervek egyre inkább rendezett jogszabályi környezetben, jogkövetően dolgoznak – az már más kérdés, hogy egy-egy ilyen jogszabály megalkotása előtt igencsak nagy csatákat kell vívni a nagyra törő adatkezelési tervek ellen –, míg a magánszféra adatkezelői, bankok, biztosítók, munkáltatók újabb tervei, célkitűzései, és az ezek érdekében alkalmazott eszközök bántják a polgárok jogérzetét. Sajnálatos, de megfigyelhető az is, hogy noha a polgárok napjainkban már magabiztosabban lépnek fel jogaikért például a rendőrséggel, adóhatósággal szemben, egyre inkább védtelennek érzik magukat a bankok ügyfeleiként, vagy munkavállalókként.

Látható, hogy az ügyszám-növekedés nem járt együtt a vizsgálatok szerkezeti változásával, vagyis ha az egészen belüli százalékos arányokat nézzük, jelentős átrendeződésről 2007-ben nem tudunk beszámolni. Majdnem ugyanazt állapíthatjuk meg tehát 2007-ben, az adatvédelmi biztos intézménye második hatéves ciklusának végén, mint 2001-ben, hat évvel korábban: a folyamatos ügyszám-növekedés mellett az ügyek megoszlása többé-kevésbé stabil képet mutat. A teljes hat évet tekintve voltak persze lényeges változások: az ügyszámok megtöbbszöröződése, a magánszféra törvényen alapuló nagy adatkezeléseinek kialakulása, a biztos jogosítványainak változása és ezek használata, az Uniós tagsággal összefüggő feladatok megjelenése, stb. Ezek elemzése azonban nem ezen fejezet feladata, az inkább megvalósulhat „kívülről", akkor, ha jelen beszámoló elkészültével és elfogadásával tényleg lezárható a hat év.

A bevezetőben még egy eseményről szólni kell.

Az Európa Tanács január 28-át az Adatvédelem Napjává nyilvánította annak tiszteletére, hogy ezen a napon írták alá Strasbourgban az Egyezményt az „egyének védelméről a személyes adatok gépi feldolgozása során". Az első adatvédelem napjára az Adatvédelmi Biztos Irodája is készült: sor került egy, az adatvédelemmel összefüggő karikatúra pályázatra, az Iroda munkatársai középiskolákba látogattak el és előadásokat tartottak. Az Európai Unió tagállamainak adatvédelmi biztosaiból, hatóságaiból álló 29-es Munkacsoport határozatában foglaltaknak megfelelően az európai adatvédelmi hatóságok vállalták, hogy a jövőben is együttműködnek az Európa Tanáccsal az Adatvédelem Napjának sikeréért.

Nagy állami (önkormányzati) adatkezelők

A Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

A nevében megújult Központi Hivatal adatkezelését a nyilvántartásokban tárolt hatalmas mennyiségű személyes adathoz képest csak kevesen kifogásolták. A név- és lakcímadatok direkt marketing célú felhasználását illetően az elmúlt évekhez képest idén kevesebb panasz érkezett, a kedvező tendencia inkább a hagyományos, postai úton küldött megkeresések visszaszorulásával és a kéretlen elektronikus reklámlevelek (spamek) sajnálatos térhódításával hozható összefüggésbe.

Egy polgár azt sérelmezte, hogy a parkolási társaságtól fizetési felszólítást kapott, holott a fizetés nélküli parkolás időpontjában a gépjármű már nem volt a tulajdonában. A vizsgálat során kiderült, hogy a panaszos, mint a gépjármű eladója csak jelentős késedelemmel jelentette be az elidegenítés tényét, így hátránya részben saját mulasztásából származik. A nyilvántartás aktualizálásához ugyanis elengedhetetlen a polgárok jogkövető eljárása. Amennyiben a polgárok a jogszabályokban előírt bejelentési kötelezettségüknek nem, vagy csak késedelmesen tesznek eleget, úgy a nyilvántartást vezető hivataltól sem várható el, hogy az adatbázisok napra készen a valós állapotokat tükrözzék.

A közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról szóló 35/2000. (XI. 30) BM rendelet 76/A. §-ában foglaltak szerint a gépjármű tulajdonjogában bekövetkezett változás bejelentését a változástól számított 15 napon belül, a régi tulajdonos a tulajdonjog változásáról készült okirat benyújtásával (megküldésével) teljesíti. A közúti közlekedési nyilvántartásról szóló 1999. évi LXXXIV. törvény (továbbiakban: Kknyt.) 33. § (1)-a pedig az új tulajdonos kötelezettségeként írja elő a bejelentés megtételét az erre okot adó körülmény bekövetkeztétől számított 15 napon belül. Az eladó bejelentésekor az eladás tényét rögzítik a járműnyilvántartásban. Az új tulajdonos adatainak bejegyzésére abban az esetben kerül sor, ha annak jogszabályi feltételei teljesülnek. Mivel sem az eladó, sem a vevő nem tettek eleget törvényi kötelezettségüknek, a körzetközponti feladatokat ellátó települési önkormányzat jegyzője közlekedési igazgatási eljárást kezdeményezett bejelentési kötelezettség elmulasztása miatt. *(438/P/2007)*

Fegyveres és rendvédelmi szervek

A fegyveres és rendvédelmi szervek közül a legtöbb beadvány a rendőrséget érintette. A 2006-os őszi események után a Rendőrség átlátható működésének kívánalma eddig nem tapasztalt mértékben megerősödött, amely 2007-ben is mindvégig tapasztalható volt. E kívánalom vonatkozásainak jelentős része a közérdekű adatok megismerhetőségével kapcsolatos, így ebben a fejezetben csupán a személyes adatokhoz kötődő kérdéseket érintjük.

A rendőri igazoltatásokkal összefüggő panaszok száma érezhetően megemelkedett. A rendőrség tevékenységével kapcsolatos kritikusabb állampolgári szemlélet érzékelése mellett az egyes panaszügyek vizsgálatán túl arra is választ kerestünk, hogy ez a tendencia csak mennyiségi emelkedést jelent, vagy a rendőrség gyakorlatának valós megváltozását tükrözi. Kétségtelen, hogy az utcai események időnként eddig szokatlan feladatok elé állították a rendőrség állományát, a rendőri intézkedésekre, köztük az igazoltatásra vonatkozó jogszabályi környezet azonban változatlan maradt.

A panaszok leginkább arról számoltak be, hogy bizonyos helyzetekben, helyszíneken úgy került sor igazoltatásra, hogy annak látszólag indoka nem volt, így például békés demonstráción részt vevő, vagy az utcán nemzeti lobogóval sétáló polgárokat igazoltattak. Ilyen esetek-

ben rendre „zaklatásszerű" intézkedésként élték meg a panaszosok az igazoltatást, illetve az ezzel járó adatrögzítést. Válaszul az adatvédelmi biztos, megismételve korábbi álláspontját, arról tájékoztatja a panaszosokat, hogy az eljáró rendőr csak azzal a személlyel összefüggésben rögzíthet adatokat, akinél ezt további intézkedés szükségessége vagy egyéb releváns körülmény indokolja. Amennyiben ez a feltétel nem teljesül, úgy az adatok tárolása jogellenes. *(2075/P/2007, 2266/P/2007, 2485/P/2007)*

A Rendőrségről szóló 1994. évi XXXIV. törvény (továbbiakban: Rtv.) folyamatban lévő módosításának révén változni fognak az igazoltatásra vonatkozó szabályok, így a rendőr, illetve az állampolgárok jogaira és kötelezettségeire nézve világosabb szabályok fognak születni. A nyár folyamán üdvözöltük az Országos Rendőr-főkapitányság állampolgároknak szánt tájékoztató anyagának tervét. A tájékoztató az igazoltatással kapcsolatos tudnivalókat foglalja össze a polgárok számára. Támogattuk, hogy az ORFK minél szélesebb körben terjessze a tájékoztató anyagot az állampolgárok között.

Az igazoltatások révén gyűjtött adatok kezelésével összefüggésben két vizsgálat is folyamatban van. Állampolgári panasz alapján vizsgáljuk, vajon megfelel-e a jogszabályi feltételeknek az igazoltatás „rabosítás-szerű" módja, amelynek során az előállított polgár videokamera előtt kell, hogy elmondja személyazonosító adatait. Az eljárás módja adatvédelmi szempontból aggályos, azonban az ilyen módon keletkezett adatok kezelésének körülményeit feltáró vizsgálat még nem zárult le.

Egy másik beadvány alapján azt vizsgálta az adatvédelmi biztos, hogy megalapozott-e az az állampolgári állítás, mely szerint a zavargások során meghatározó szerepet játszó személyekről belső nyilvántartás készült, illetve a „szélsőjobboldali politikai szervezethez tatozó" megjelölés valóban szerepel-e bizonyos regiszterekben. A vizsgálat határozottan cáfolta ezt a félreértésből eredő következtetést. *(2430/K/2007)*

A rendőrség közterületi kamerás megfigyelésére vonatkozó szabályokat – részben az adatvédelmi biztos észrevételei alapján – az év során módosították. Ennek részleteiről bővebben a „Kamerák" című fejezetben számolunk be.

A büntetés-végrehajtási intézetekben rendszeresített kapcsolattartói nyilvántartás és az intézetekben alkalmazott korlátozó intézkedések tárgyában számos beadvány érkezett hivatalunkhoz.

A büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény (továbbiakban: Bvsztv.) 2007. június 1-jével bekövetkezett módosításával a kapcsolattartóként megjelölt személyek nyilvántartásba vételét rendelték el. A Bvsztv. 28/A. §-a alapján a büntetés-végrehajtási szervezet, illetőleg a javítóintézet, a végrehajtás rendjének és biztonságának megőrzése érdekében és a kapcsolattartó személyazonosságának a látogatás alkalmából történő megállapítása céljából – a kapcsolattartóként megjelölt személy hozzájárulásával – nyilvántartja mindazoknak a személyeknek a személyes adatait, akikkel az elítélt kapcsolatot tart fenn (kapcsolattartó). A kapcsolattartók nyilvántartása kiterjed a kapcsolattartó családi és utónevére, lakcímére (székhelyére), telefonszámára és kapcsolattartói minőségére.

A Bvsztv. lényegében egy kötelező adatkezelést hozott létre, ugyanakkor a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Avtv., adatvédelmi törvény) rendelkezéseivel összhangban a nyilvántartandó kapcsolattartók önkéntes hozzájárulását is megköveteli adataik felvételéhez. A biztos megkereséssel fordult a büntetés-végrehajtás országos parancsnokához, akinek értékelése tükrében úgy vélte, hogy a nyilvántartás jelenlegi rendszere apróbb korrekciókra szorul. Egyebek mellett szorgalmazta, hogy az Országos Parancsnokság valamennyi büntetés-végrehajtási szervezet számára – a Bvsztv. által meghatározott adatkört igénylő – egyező tartalmú és megjelenésű nyilatkozatot rendszeresítsen annak érdekében, hogy a nyilvántartás naprakész lehessen, és egy esetleges átszállítás alkalmával az új büntetés-végrehajtási intézetben ne kelljen új nyilatkozatokat beszerezni.

Ugyanakkor kétséges, hogy a nyilvántartás felállításával egyidejűleg bevezetett intézkedések – amelyek lényegében az érintkezés valamennyi formáját érintik – indokoltak-e, összhangban vannak-e a büntetések és intézkedések végrehajtásáról szóló 1979. évi 11. törvényerejű rendeletben foglaltakkal és megfelelnek-e az alkotmányossági követelményeknek. Összegezve elmondható, hogy a kapcsolattartói nyilvántartás vezetése megfelel az adatvédelmi törvény rendelkezéseinek. Annak vizsgálatára azonban már nem rendelkezik az adatvédelmi biztos hatáskörrel, hogy a nyilvántartás jogszerű vezetése révén a kapcsolattartás minden formájának korlátozása sérthet-e egyéb alkotmányos jogokat. Ezért a szóban forgó panaszokat ennek kivizsgálása érdekében az állampolgári jogok országgyűlési biztosához áttette. *(1383/P/2007, 1381/P/2007)*

A rendőrség – és általában a nyomozó hatóságok – munkáját érintő sajátos ügycsoportot azok a beadványok képezik, amelyek az elektronikus kommunikáció során továbbított üzenetek büntetőeljárás során történő felhasználását érintik. A probléma lényege abban áll, hogy míg a vonatkozó jogszabályok a hagyományos levelezést tekintik általánosnak, és ezzel állítják párhuzamba az elektronikus levelezést, a gyakorlatban az utóbbi vált elterjedtebbé. A hagyományos levelek esetében eltérő szabályok vonatkoznak a kézbesített levelekre, és a még „úton lévőkre", és megfelelő garanciák védik az érintetteket attól, hogy levelezésükben tudtukon kívül kutakodjanak. Ezeket a szabályokat ugyanakkor sokszor nehéz leképezni az elektronikus levelezésre.

Az elektronikus levelezés „hagyományos" formája abban hasonlít a postai levélre, hogy meghatározott személyek között történő kommunikáció, melynek tartalmát a feladó és a címzett ismeri, a levelek az ő számítógépükön (rendszerükön) találhatók. Számos esetben azonban a levelezés tartalomszolgáltató útján történik, ilyenkor az adatok ténylegesen nem a küldő vagy a fogadó személy számítógépén vannak, hanem a szolgáltató szerverén, melyhez a feladó és a címzett az Interneten keresztül fér hozzá. Ebbe e körbe tartoznak az ingyenes levelezőrendszerek, melyeknél tényleges adatmozgás nem történik. A büntetőeljárásról szóló 1998. évi XIX. törvény (továbbiakban: Be.) azonban nem szűkíti le az adatkört az elektronikus levelezésre, hanem tágabban fogalmaz, amikor „számítástechnikai rendszer útján továbbított és tárolt adatokat" említ, hasonló a logikája az Rtv.-nek is.

Egyértelműnek tűnhet, hogy a hagyományos leveleket megillető védelem szintjét ki kell terjeszteni az elektronikus levelezésre is, a közlés jellege ezt mindenképpen indokolja. Ugyanakkor, míg a postai levél „elfogása", telefon lehallgatása hosszabb ideje szerepel a nyomozó hatóságok eszköztárában, és egyértelműen szabályozott, addig napjainkra az e-mail, ezen belül a közbenső tartalomszolgáltatón keresztül történő kommunikáció mindennapossá, és az előzőeknél elterjedtebbé vált. Ezt azonban a jogalkotás nem követte.

Ez számos helyzetben bizonytalanságot okoz. Ezt mutatja, hogy a Rendőrség sokszor bizonytalan abban a tekintetben is, hogy ki minősül hírközlési szolgáltatónak, és emiatt nem megfelelő jogalapot jelölnek meg. Aggályos az is, amikor egy-egy szolgáltató szerverén tárolt adatokhoz a lefoglalás eszközével próbálnak hozzáférni.

> Valószínűleg az is nehézséget okoz, hogy olyan hagyományos fogalmakat kell egy új technológiára, módszerre alkalmazni, mint például a kézbesítés. Ez a postai levélnél egyértelmű, az e-mailnél nem. Ugyanis, hiába állapítható meg egyértelműen, hogy a címzett megtekintette-e a levelezését, vagy adott levelet, az ügyészség szerint ezen levelek már a megküldéssel kézbesítettnek tekintendők. Az adatvédelmi biztos a legfőbb ügyésznek jelezte, hogy ezzel nem ért egyet.

Mivel a kérdést konkrét ügyben nem sikerült megoldani, konzultációt kezdeményeztünk az érintett szervek és a szolgáltatók bevonásával annak érdekében, hogy a jogalkotás hiányosságait az egységes jogalkalmazás kiküszöbölhesse. *(476/K/2007)*

Állami adóhatóság

Az idei évben is számos beadvány érintette közvetlenül vagy közvetve az állami adóhatóság adatkezelését.

A vagyonosodási vizsgálatok kapcsán az APEH rendszerint adatszolgáltatásra hívja fel az adóalanyt. Az adatigénylés jogszerűségét évről évre többen vitatják, kifogásaik túlnyomórészt alaptalannak bizonyulnak. Az adóhatóság ugyanis a tényfeltárás érdekében a szabad bizonyítási rendszer kínálta eszközök közül belátása szerint választhatja ki a megfelelőt, így az ügyfelet nyilatkozattételre is felhívhatja. Természetesen az adóhatóság adatkezelése során is irányadó az adatvédelmi törvény 5. §-ában foglalt célhoz kötöttség elve, mely szerint személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig. Abban az esetben amikor a formanyomtatványon kért információk relevánsak lehetnek az adózó valós jövedelmi helyzete megállapításában, túlzott, az adatkezelés célját meghaladó adatigénylésről nem beszélhetünk. *(451/P/2007, 1756/P/2007)*

Közvetve szintén a vagyonosodási vizsgálatokhoz kapcsolódott az az ügy, melyben egy autókereskedő cégnél végzett ellenőrzés során magánszemélyekről is szükségszerűen információkhoz jutott az adóhatóság.

Az APEH elnökének tájékoztatása szerint az ellenőrzés célja a cég által vezetett nyilvántartások valóságtartalmának vizsgálata volt. Egy ilyen ellenőrzés során, különösen, mikor az adózó tevékenységi köre a szolgáltatáshoz, értékesítéshez kapcsolódik, elengedhetetlen, hogy az adóhatóság az ellenőrzésben érintett adózókkal kapcsolatba került vevők, ügyfelek adatait is megismerje. A biztos álláspontja szerint, ha az ilyen vizsgálat célja nyilvánvalóan nem a szervezet esetleges mulasztásainak, jogsértéseinek szankcionálása, hanem burkoltan a magánszemély adózókról való információgyűjtés, az ilyen eljárás adatvédelmi szempontból helytelen lehet. A konkrét ügyben azonban nem volt megállapítható, hogy célzottan a későbbiekben vizsgálandó személyek kiválasztásához gyűjtött volna adatokat az adóhatóság. Eljárása az adójogi és adatvédelmi rendelkezéseknek egyaránt megfelelt. *(1924/K/2006)*

Szintén jogszerűen értesült az adóhatóság több száz regisztrációs adót visszaigénylő személy kilétéről. Az adózás rendjéről szóló 2003. évi XCII. törvény (továbbiakban: Art.) 54. § (3) bekezdésében foglaltak szerint ugyanis az adóhatóság jogosult a hatáskörébe tartozó, adóval kapcsolatos, a titoktartási kötelezettség alá tartozó adatról, tényről, körülményről vagy iratról más adóhatóság (vámhatóság) tájékoztatására, ha az valamely adó (vámteher) vagy adóhiány feltárását, behajthatóságának megállapítását, illetve adóigazgatási eljárás lefolytatását lehetővé teszi vagy valószínűsíti. E felhatalmazás alapján a fővámhivatalok a mintegy 26 és félezer magánszemélyből 366 ügyfél esetében valószínűsítették a rendelkezésre álló iratok alapján az adóhiány fennállását és éltek az állami adóhatóság illetékes igazgatósága felé jelzéssel.

Telefonos bejelentésekből és beadványból értesültünk arról, hogy számos termékfelvásárló tanácstalan az adóhatóságnak szolgáltatandó, illetve termékfelvásárlás alkalmával az őstermelőktől kérhető személyes adatok köre tekintetében. A jogszabályi háttér áttanulmányozása után e tevékenység sajátosságait és az adatkezelés célhoz kötöttsége elvét is figyelembe véve megállapítást nyert, hogy indokolatlan és túlzott mértékű az adóhatóság termékfelvásárláshoz köthető adatigénylése.

Az Art. 31. § (2) bekezdése alapján, a munkáltató és a kifizető 2007. január 1-jétől havonként elektronikus úton bevallást tesz az adó és/vagy társadalombiztosítási kötelezettséget eredményező, magánszemélyeknek teljesített kifizetésekkel, juttatásokkal összefüggő valamennyi adóról, járulékról és a bekezdés 1-27. pontjaiban meghatáro-

zott adatokról. A bevallási kötelezettség a magánszemély személyi adataira (neve, születési neve, anyja neve, születési helye és ideje), nemére, állampolgárságára is kiterjed. Az általános forgalmi adóról szóló 1992. évi LXXIV. törvény 56. § (1) bekezdése értelmében a mezőgazdasági tevékenységet folytató adóalany termékértékesítésekor, szolgáltatásnyújtásakor a kompenzációs felár érvényesítése érdekében köteles a terméket átvevőnek, vagy a szolgáltatást igénybe vevőnek hitelesített írásos nyilatkozatban megadni nevét, címét, adóigazgatási azonosító számát. A törvény 4. számú melléklet III. része meghatározza a felvásárlást igazoló bizonylat tartalmi elemeit, melynek – egyebek mellett – része az adóalany neve, címe, adóazonosító száma és a mezőgazdasági őstermelő igazolványának száma. A felvásárlási jegyek tartalma szerint ugyanakkor az eladó születési idejére, helyére, valamint anyja nevére vonatkozó rovatokat „csak adóazonosító jel hiányában szükséges kitölteni", vagyis azok feltüntetése főszabályként nem kötelező. Az adóhatóság pedig amúgy is az adóazonosító jelén tartja nyilván az őstermelőt. A biztos az APEH elnökének írt levelében ismertetett álláspontja szerint a nem egyértelmű jogi szabályozás amellett, hogy felesleges adminisztrációt eredményez, az adatkezelés célhoz kötöttségének elvével sincsen maradéktalanul összhangban. Az APEH elnöke sajnos nem osztotta a biztos álláspontját és ragaszkodott a jelenlegi gyakorlat fenntartásához. *(1924/K/2006)*

A Business Software Alliance (BSA) tevékenységének jogosságát vitató panaszbeadványok elbírálása során áttekintettük a BSA-APEH között kötött megállapodást is. A kérelmezők számára megküldött állásfoglalás hangsúlyozta, hogy adótitkokat az APEH nem adhat át a BSA-nak. Az adatok továbbítására az adóhatóságnak megállapodás alapján nincsen módja, erre külön törvényi felhatalmazásra lenne szükség. Ilyen tartalmú kitételt egyébként az APEH és a BSA között létrejött megállapodás sem tartalmaz. *(516/P/2007, 2240/P/2007, 2298/K/2007, 2301/P/2007, 2305/P/2007, 2401/P/2007, 2407/P/2007/, 2446/P/2007)*

Önkormányzatok

2007-ben a helyi önkormányzatok adatkezeléseit érintő ügyeink száma megközelítette a kétszázat. A vizsgálatok alapos szemügyre vétele után megállapítható, hogy jelentősen nőtt az olyan beadványok aránya, amelyek a helyi önkormányzatok kezelésében lévő közérdekű, vagy közérdekből nyilvános személyes adatok, illetve a törvény alapján védett

személyes adatok hozzáférhetővé tételére, vagy olyan személyes adatok jogellenes továbbítására vonatkoztak, amelynek felelős adatkezelője az önkormányzat valamely szerve.

Az önkormányzati adatkezelések rendkívül sokrétűek, szerteágazóak, néha igen bonyolultak; alapos és speciális jogi ismereteket igényelnek, mivel a jogi szabályozás általában többszintű, és igen összetett. Ennek oka a sajátos kettősség: a helyi önkormányzatoknál általában élesen, néha kevésbé láthatóan, de elkülönülnek a helyi önkormányzati ügyekkel, valamint a közigazgatási hatósági ügyekkel kapcsolatos adatkezelések. A bonyolultságot tovább fokozzák az önkormányzati hatósági ügyekhez köthető speciális adatkezelési jogosultságok, vagyis amikor a képviselő testület, illetve a polgármester maga jár el hatóságként, vagy például az a tény hogy a (körzetközponti) helyi önkormányzat jegyzője egyúttal a központi nyilvántartások területi szerve is. Az önkormányzatok azonban nem csak adatkezelők, hanem adatigénylők és adatszolgáltatók is egyúttal, sőt mindezek mellett a törvény által meghatározott körben személyes adatok kezelésére vonatkozóan jogalkotási hatalommal felruházott szervezetek.

Az adatkezelési jogosultságokat és kötelezettségeket általában pontosan meghatározzák a vonatkozó jogi normák, melyek alapos ismerete nélkülözhetetlen. A jogszabályok nagy számára és összetettségére való tekintettel azonban némely esetben az is nehéz lehet, hogy a tisztviselők érzékeljék egy adatkezeléssel is járó ügy „specialitását", megszokottól való eltérését, és azt, hogy emiatt eltérő gyakorlati és jogi megközelítést és ismeretet igényel. A másik nehéz kérdéskör a különböző nyilvántartások és adatkezelések elkülönítése, elválasztása és az adatbázisok összekapcsolásának tilalma. Kisebb önkormányzatoknál, ahol egy ügyintéző feladatkörébe több ügycsoport is tartozhat, ennél fogva több adatbázist is egyazon személy kezel, kérdéses, hogy biztosítható-e egyáltalán adott ügy jogszabály által előírt adatok ismerete alapján való elbírálása, más adatok „bevonása" nélkül.

Mindezek miatt hasznos, ha az adatkezelők felelős döntésük meghozatala előtt kérik ki véleményünket. Továbbra is javasoljuk, hogy lehetőség szerint minden polgármesteri hivatalban legyen olyan tisztviselő, aki az adatvédelemmel és az információszabadsággal egyaránt hivatásszerűen törődik, és jelzi a munkatársainak, ha a munkájuk során adatvédelmi visszásságot tapasztal.

Ebben az évben sem tér el a biztosi beszámoló attól a már jól bevált gyakorlattól, hogy a helyi önkormányzatok kezelésében levő közérdekű, közérdekből nyilvános adatokra vonatkozó ügyeink ismertetése az információszabadság fejezetben található meg. Tekintettel az önkormányzatok által is előszeretettel telepített, üzemeltetett közterületi kamerarendszerekre a távfigyelés, térfigyelés adatvédelmi kérdéseit elemző, összegző vizsgálatokat, állásfoglalásokat külön alfejezetben tárgyaljuk.

Helyi rendeletalkotás

Az iménti bevezetőben már szót ejtettünk arról, hogy törvény meghatározott körben felruházhatja a helyi önkormányzatokat olyan önkormányzati rendelet megalkotására, amely személyes adatok kezelését rendeli el, vagyis a helyi önkormányzat az érintettek személyes adatai védelméhez való jogát alkotmányos keretek között korlátozhatja. Ilyen jogszabály például a hulladékgazdálkodásról szóló 2000. évi XLIII. törvény (továbbiakban Hgt.) amelynek helyi végrehajtási rendeleteivel kapcsolatban számos (általában alaptalan) panasz érkezett hozzánk. A hulladékszállítás a jogszabály alapján olyan közszolgáltatás, amelynek igénybevétele főszabály szerint kötelező. Többen is kifogásolták, hogy személyes adataikat a önkormányzat továbbította a vele szerződésben álló kommunális szolgáltatóhoz.

A Hgt. 23. §-a szerint a települési önkormányzat képviselő-testülete önkormányzati rendeletben állapítja meg – egyebek mellett – a közszolgáltatással összefüggő személyes adatok (közszolgáltatást igénybe vevő neve, lakcíme, születési helye és ideje, anyja neve) kezelésére vonatkozó rendelkezéseket. E rendelkezés alapján az önkormányzat, illetve a hulladékszállítást végző cég is kezelheti a felsorolt személyes adatokat. A közszolgáltatásért a fogyasztónak hulladékkezelési közszolgáltatási díjat kell fizetnie. A hulladékszállítási díjat sok településen a kommunális adó megfizetésével teljesítik a polgárok. A hulladékkezelési közszolgáltatás igénybevételéért az ingatlantulajdonost terhelő díjhátralék és az azzal összefüggésben megállapított késedelmi kamat, valamint a behajtás egyéb költségei adók módjára behajtható köztartozásnak minősülnek, amelynek behajtásáról a jegyző gondoskodik. *(431/P/2007, 569/P/2007, 600/P/2007, 789/P/2007, 1583/P/2007, 2313/P/2007)*

A Fővárosi Közgyűlés által megalkotott rendeletek adatkezelést elrendelő szabályaival kapcsolatban is folyamatban van egy vizsgálat. Egy állampolgár a 19/2005. (IV. 22.) Főv. Kgy. rendeletnek az üzemképtelen gépjárművek tárolására vonatkozó XI. Fejezetének az 55. § (5) bekezdését sérelmezte, mely szerint, „akinek lejárt a gépjárműve forgalmi engedélye" annak kívülről jól láthatóan a szélvédőre ki kell írnia a gépjárművére a nevét, címét, valamint el kell helyeznie a közterület használati hozzájárulást tartalmazó okiratot, vagy az ez iránti kérelem fénymásolatát.

E kérelem a Közgyűlés egy másik rendelete alapján számos személyes adatot tartalmaz. A közterület használati hozzájárulás személyes adat tartalmáról hasonló körben a Kgy. rendelet 8. §-a rendelkezik. Az indítványozó hangsúlyozta, hogy a rendelet alapján mindenki számára olvasható módon kell elhelyezni a személyes adatokat (a gépjármű tulajdonosának személyes adataival együtt) és a gyakorlatban a kérelemhez kell csatolni indokolást is, ami az ő esetében az lett volna, hogy betegség miatt nem áll módjában a tulajdonosnak az üzemképtelen gépjárművet eltávolíttatni. A rendelet módosította a közgyűlés. *(1934/P/2007)*

Több állampolgári panaszbeadvány érkezett az Adatvédelmi Biztos Irodájához, melyek szerint Dunakeszi Város Polgármesteri Hivatala az építményadó bevallásban olyan adatok megadását is kérte, melyek az adó megállapításhoz nem szükségesek (például a tetőszerkezetre, szobák padlóburkolatára, tájolására, felújításra, az ingatlan komfortfokozatára, az adózó bankszámla számára vonatkozó adatok). A helyi adókról szóló 1990. évi C. törvény 51. §-a a személyazonosító adatok, az adóazonosító jel, és az adó megállapításához szükséges adatok kezelésére ad felhatalmazást a helyi adóhatóság számára. Ellenben a vizsgált adóbevallás III. fejezetében az adótárgyra jellemző adatokra vonatkozó kérdéssor, valamint a pénzintézeti számlaszám kezelése nem felelt meg a célhoz kötöttség elvének.

Mindezek alapján vizsgálat indult, amely során a dunakeszi jegyző is egyetértett azzal, hogy több adat esetében valóban kifogásolható az adatkezelés jogszerűsége, ezért a nyomtatvány felülvizsgálatát javasolta a képviselő-testületnek, amelyet 2007. február 27-i hatállyal a biztosi állásfoglalásnak megfelelően módosítottak. A jogszabály rendelkezett arról is, hogy a rendelet hatályba lépéséig terjedő idő-

szakban benyújtott adóbevallási nyomtatványokról mindazon adatokat, amelyek a mellékletében nem szerepelnek, az önkormányzati adóhatóságnak törölnie kell oly módon, hogy azon adatok ne legyenek rekonstruálhatók. Az adatkezelő tehát megszüntette a jogellenes adatkezelést. Az állásfoglalás az adatvédelmi biztos honlapján olvasható. *(63/P/2007, 182/P/2007, 218/P/2007)*

Képviselő-testület, és a bizottságok adatkezelése

Az egyik települési önkormányzat pénzügyi bizottságának elnöke arról kért állásfoglalást, hogy a polgármesteri hivatal telefonhívásainak részletes híváslistáját megismerhetik-e a bizottság tagjai.

A helyi önkormányzatokról szóló 1990. évi LXV. törvény (továbbiakban: Ötv.) 92. § (3) bekezdése értelmében a pénzügyi bizottság az önkormányzatnál és intézményeinél ellenőrizheti a pénzkezelési szabályzat megtartását, a bizonylati rend és bizonylati fegyelem érvényesítését. Az Ötv. kommentárja szerint célszerű, hogy a bizottság rendszeresen ellenőrizze az operatív gazdálkodást. Az ellenőrzés keretében a bizottságnak joga van ahhoz, hogy a bevételekről és kiadásokról szóló kimutatásokat megismerje. Ez a felhatalmazás azonban nem foglalja magában azt a jogot, hogy a bizottság tagjai személyes adatokat is kezeljenek. Az ellenőrzés joga – az adatok kezelésére vonatkozó törvényi feltételek fennállása esetén is – kizárólag a munkáltatói jogkör gyakorlóját illeti meg. *(156/K/2007)*

Egy tanár beadványában azt kifogásolta, hogy az általa meg nem nevezett önkormányzat, amely fenntartója az iskolájának, a 2007. február 21-i sztrájk megkezdése előtt egy jegyzék összeállítására kötelezte az intézményt, amely tartalmazta a munkavállalók nevét, aláírását, és beosztását is.

Sztrájk szervezésével kapcsolatosan – elsősorban bérszámfejtés céljából – a munkáltató, illetőleg a bérszámfejtést végző személy jogosult kezelni azt az adatot, hogy a sztrájkban pontosan mely munkavállaló vett részt. A sztrájkról szóló 1989. évi VII. törvény 6. § (3) bekezdése értelmében a sztrájk miatt kiesett munkaidőre – eltérő megállapodás hiányában – a dolgozót díjazás és a munkavégzés alapján járó egyéb juttatás nem illeti meg. A sztrájk megtartása előtti időpontban azonban a munkavállalóktól csak akkor kérhető a sztrájkban való részvételével kapcsolatos adat, ha azt a sztrájk megtartása alatt nem tudják beszerezni. A munkavállaló sztrájkban való részvételével kapcsola-

tosan csak a munkáltató, illetőleg a bérszámfejtést végző személy kezelhet adatot. Harmadik személy, így az iskola fenntartója nem rendelkezik törvényi felhatalmazással az ilyen tartalmú adatok megismerésére. A sztrájk szervezésével kapcsolatos ajánlás az adatvédelmi biztos honlapján olvasható. *(342/P/2007)*

Már az előző évek beszámolóiban is utaltunk arra, hogy sok esetben nehezedik nyomás a képviselő testület hivatalainak adatkezelőire olyan ügyekben, amikor a helyi önkormányzat képviselő-testületének tagjai olyan személyes adatok továbbítását igénylik a tisztviselőktől, amelyek megismerésére, kezelésére semmilyen jogszabály nem hatalmazza fel az adatigénylőt. Teszik ezt annak ellenére is, hogy esetleg tudatában vannak, vagy lehetnének annak, hogy a személyes adatok jogszabályban meghatározott kezelőit törvény kötelezi az érintettek adatainak védelmére. Egyik estben egy városi önkormányzat vezető beosztású köztisztviselője arról kért tájékoztatást, hogy az önkormányzati képviselők és tisztségviselők milyen személyes adatokat, illetve adótitkokat ismerhetnek meg feladataik ellátása során.

Az adatvédelmi törvény, valamint az Art. alapján, ha az adózási adat nem magánszemélyre, hanem valamely szervezetre, cégre vonatkozik, akkor az „magánadatnak", cégadatnak minősül, amely kezelésére nem vonatkoznak az adatvédelmi törvény szabályai. Azonban az adótitok védelmére vonatkozó szabályokat valamennyi adatra alkalmazni kell, így az adózással összefüggő adatokat csak az Art. 54. §-ában meghatározott esetekben lehet mások tudomására hozni. A képviselő-testület, és a képviselők tevékenységéhez, tájékoztatásához (például: költségvetési kérdések, rendeletalkotás esetén) elegendő anonimizált, összesített adatok, elemzések átadása. Ezen adatokat nem csak a képviselők, hanem bárki megismerheti. Az önkormányzat helyi adók vonatkozásában fennálló adó-megállapítási joga nem teszi szükségessé meghatározott személyek adózási adatainak kezelését (továbbítását, nyilvánosságra hozatalát). Az Ötv. 19. § (2) bekezdése informálódási jogot biztosít a képviselőknek egyrészt „önkormányzati ügyekben", másrészt „a képviselői munkájához szükséges" mértékben. A képviselői minőség azonban önmagában nem jogosítja fel a képviselőket személyes adatok megismerésére és kezelésére. Az adatvédelmi törvénnyel csak olyan értelmezés van összhangban, amely szerint a képviselő konkrét ügyben – az erre hatáskörrel rendelkező bizottság tagjaként, illetve a képviselő-testület ülésén – a személyes

adatok kezelését igénylő eljárás részeként ismerheti meg a személyes adatokat. A jegyzői adóhatósági jogkör gyakorlása nem jelentheti az adótitok jogosulatlan továbbítását, nyilvánosságra hozását. Amennyiben adótitkok mások tudomására jutnak, akkor ezen harmadik személyek sem jogosultak arra, hogy az adatokat továbbítsák, vagy nyilvánosságra hozzák. Az Art. alapján a helyi adók (például: adóbehajtás, adómérséklés és adóelengedés) ügyében a jegyző adóhatóságként jár el a törvényben foglaltak végrehajtása érdekében, és a képviselő-testületnek nincs ezzel összefüggő feladata. Vagyis a képviselő-testület akkor kezelhet, ismerhet meg személyes adatokat, ha tevékenységéhez kapcsolódóan, meghatározott célból erre törvény felhatalmazza. *(845/K/2007)*

Az egyik megyei jogú város önkormányzatának irodavezetője állásfoglalást kért arról, hogy megismerhetik-e a személyes adatokat is tartalmazó, zárt ülésen tárgyalandó bizottsági előterjesztéseket azok a képviselők, akik nem tagjai a döntési jogkörrel felruházott, az előterjesztést tárgyaló bizottságnak.

Az önkormányzatok zárt testületi ülései dokumentumainak kezeléséről 2005. január 17-én *1926/H/2004* számon az adatvédelmi biztos állásfoglalást bocsátott ki, amely a honlapján hozzáférhető. Eszerint az önkormányzat szerveinek nem csak azt kell megakadályozniuk, hogy a zárt testületi ülések jegyzőkönyveihez illetéktelenek hozzáférhessenek, hanem azt is, hogy – a személyes adatok tekintetében az adatvédelmi törvény 5. és 10. §-ával összhangban – az önkormányzat szervei maguk se sértsék meg a személyes adatok védelméhez fűződő, illetve egyéb más védett érdekeket. A képviselő-testület bizottságainak működésére a képviselő-testület működésére vonatkozó szabályokat kell alkalmazni. Amennyiben azonban a képviselő-testület az Ötv. alapján nem rendel el zárt ülést, ez a döntés kihat az előterjesztés és a bizottsági ülések jegyzőkönyveinek minősítésére is. Az Ötv. különböző rendelkezései alapján a képviselő-testületi ülés résztvevői, továbbá a képviselő-testület bizottságainak tagjai, a polgármesteri hivatalnak az előterjesztés és a jegyzőkönyv elkészítésében résztvevő dolgozói, valamint – a képviselő-testület (bizottság) ülését követően – a törvényességi ellenőrzést végző közigazgatási hivatal vezetője jogosult a zárt ülés előterjesztései, illetve a jegyzőkönyvének tartalmát megismerni. *(2434/K/2007)*

A Dél-Alföldi Regionális Közigazgatási Hivatal vezetője arról kért állásfoglalást, hogy adatvédelmi és titokvédelmi előírások szempontjából nézve korlátozható-e a kisebbségi szószóló részvétele a személyiségi jogokat érintő egyedi ügyek (például szociális kérelmek, személyi ügyek) zárt képviselőtestületi tárgyalása esetén.

A biztosi álláspont szerint nem ellentétes az adatvédelmi törvény rendelkezéseivel, ha a kisebbségi szószóló részt vesz a képviselő-testület ülésein, zárt ülésein. Az Ötv. 12. § (5) bekezdése kifejezetten tartalmazza, hogy a kisebbségi szószóló részt vesz a zárt ülésen. A nemzeti és etnikai kisebbségek jogairól szóló 1993. évi LXXVII. törvény (továbbiakban: Nektv.) 40. § (1) bekezdés a) pontja nem szűkíti a szószóló jogait az Ötv.-hez képest, hanem ellenkezőleg, kiterjeszti részvételét a képviselő-testületi üléseken túl a bizottságokra is. Helytelen álláspont az, miszerint az Ötv.-hez képest a Nektv. „már csak az általa képviselt kisebbséget érintő napirendek" megléte esetén biztosít részvételi lehetőséget és tanácskozási jogot, a Nektv. ugyanis e helyütt azt tartalmazza, hogy a szószóló jogosult tanácskozási joggal részt venni a testület és bármely bizottság „kisebbséget érintő napirendjének tárgyalásán". Ebbe bármelyik kisebbség érintettsége beletartozik, nemcsak a szószóló sajátja. Nem az szerepel a törvényben, hogy az „adott", vagy „saját" kisebbséget érintő ügy esetén vehet részt az ülésen. A kisebbség helyi szólója nem jogellenes módon ismeri meg az ülésen elhangzott információkat, de köteles betartani az adatvédelmi törvény és más jogszabályok titokvédelmi rendelkezéseit. Az így megismert adatokat (személyes adat, de akár döntés előkészítő irat, üzleti titok) nem hozhatja nyilvánosságra, nem élhet vissza azokkal. *(587/K/2007)*

Polgármesteri hivatal és a jegyző

Egy állampolgár beadványában az egyik Balaton parti település jegyzőjének eljárását kifogásolta. Az indítványozó az egyik szomszédjával ráépítési jogvitába keveredett. Emiatt a szomszéd egy, a panaszos tulajdonában lévő másik ingatlant érintően (melyhez semmilyen köze sem volt) közérdekű bejelentést tett a helyi építési hatósághoz engedély nélküli építés miatt, majd az eljárás során iratbetekintést kért, melyet a jegyző biztosított számára anélkül, hogy a közigazgatási eljárás során tisztázta volna ügyféli jogállását. Ennél fogva a bejelentő olyan személyes adatok birtokába jutott, amelyekhez egyébként nem lett volna joga, tehát

az adattovábbítás ellentétes volt az adatvédelmi törvény szabályaival, mert az adatok kezeléséhez (továbbításához, vagyis a betekintési jog gyakorolhatóságához) szükséges eljárásjogi feltételek hiányoztak, így az adatok továbbítása törvényes jogalap nélkül történt.

A vizsgálat során a biztos Dél-Dunántúli Regionális Közigazgatási Hivatal vezetőjéhez fordult, és kérte, hogy vizsgálja meg a polgármesteri hivatal iratbetekintésre vonatkozó adatkezelési és eljárási gyakorlatát. A vizsgálat megállapításai szerint iratbetekintést a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól 2004. CXL. alapján kizárólag az ügyfelek számára biztosítottak, ennek dokumentálását azonban nem végezték el. A hivatalvezető álláspontja szerint az egyedi építési ügyre vonatkozó bejelentés nem tekinthető közérdekű bejelentésnek sem, (vagyis e szerint a bejelentést tevő állampolgár, még a közérdekű bejelentések elintézésére vonatkozó törvény alapján sem kaphatott volna tájékoztatást arról, hogy mi lett a bejelentése nyomán (esetleg) meginduló eljárás végeredménye). Az ellenőrzés során és azt követően is felhívták a jegyző figyelmét, hogy a jövőben dokumentálják az iratbetekintéseket, és az egyes ügyekben vizsgálják nagyobb körültekintéssel az eljárás szereplőinek ügyféli jogállását. Az ügyben kiadott állásfoglalás az adatvédelmi biztos honlapján olvasható. *(677/P/2007)*

Az egyik fővárosi kerületi gyermekjóléti központ és családsegítő szolgálat adatkezelése miatt beadványt kaptunk, amely azt kifogásolta, hogy a szolgálat munkatársainak adatkezelése sértette a szolgálathoz forduló szülő személyiségi és személyes adatai védelméhez való jogát. A panaszos és férje között családi konfliktusok támadtak, ezért fordult segítségért a családsegítő szolgálathoz. Később egy iratbetekintés során „megszerezte", illetve lemásolta az aktában található, a szolgálat munkatársai által leírt belső feljegyzéseket, melyek – véleménye szerint – személyével összefüggésben sértő és megalapozatlan kijelentéseket is tartalmaztak.

A személyes gondoskodást nyújtó szociális intézmények szakmai feladatairól és működésük feltételeiről szóló 1/2000. (I. 7.) SzCsM rendelet alapján a családsegítés keretében folyamatosan figyelemmel kísérik az érintett személyt, illetve a családot veszélyeztető körülményeket és a veszélyeztetett személy, illetve család szociális ellátások és szociális szolgáltatások iránti szükségleteit. A családsegítés a személyes gondoskodást végző és a szolgáltatást igénybe vevő személy együttes

munkafolyamata, melynek tartalma és menete írásbeli együttműködési megállapodásban kerül rögzítésre, feltéve, hogy a jogszabály szerinti szakmai tevékenység az első interjú kapcsán tett intézkedéssel nem zárható le. A megállapodás tartalmazza a szolgáltatást igénybe vevő személy problémáit, az elérendő cél érdekében megvalósítandó feladatokat, az együttműködés módját, a folyamatba bevonandó szolgáltatókat, intézményeket, a találkozások rendszerességét, a segítő folyamat várható eredményét és a lezárás időpontját. A családsegítés a szolgáltatást igénybe vevő személy otthonában, családi környezetében tett látogatások, illetve a családsegítő szolgálatnál folytatott segítő beszélgetés és segítő munkaformák útján valósul meg.

Az adatvédelmi biztos a rendelkezésére álló információk, illetve a Szociálpolitikai és Munkaügyi Intézet – mint a családsegítés szakmáját felügyelő országos módszertani intézmény – szakvéleménye alapján állásfoglalásában megállapította, hogy a szociális munkás belső feljegyzései természetszerűen tartalmazhatják a szociális munkás szubjektív feltételezéseit, azonban ezeket külön kell kezelni a hivatalos, döntés-előkészítő iratoktól. A szociális munkások a probléma feltárása során több információs forrást vehetnek igénybe – ezek tartalmilag gyakran ellentmondanak egymásnak –, melyek alapján a szakember hipotéziseket fogalmaz meg, s melyeket a későbbiek során vagy megerősít, vagy elvet. A hivatalos feljegyzésekbe a megerősítést nyert diagnosztikus megállapítások kerülnek. Ezek elvileg nem jelenthetnek újdonságot a kliens számára, hiszen a probléma feltárása vele együtt történt. A saját szakmai feljegyzések tehát azt a célt szolgálják, hogy a szociális munkás szakmai reflexióit rögzítsék, ezek azonban nem kerülnek be a hivatalos esetdossziéba, noha kétségkívül tartalmazhatnak az érintettekre vonatkozó megállapításokat, benyomásokat, értékítéleteket. E belső használatra készített jegyzeteket a nyilvántartástól elkülönítetten kell kezelni, és ki kell zárni a lehetőségét is annak, hogy ezek a feljegyzések feldolgozatlanul „kikerüljenek", és hivatalos eljárások, döntések alapjául szolgáljanak. A biztos hangsúlyozta, hogy a belső feljegyzések más információforrásból származó idézeteket és a családsegítő szubjektív benyomásait rögzíthetik ugyan, de ellenőrizetlen ténymegállapításokat, minősítéseket nem tartalmazhatnak. *(717/P/2007, 904/K/2007, 1427/K/2007)*

Ugyancsak egy rendkívül speciális adatvédelmi kérdésben, nevezetesen a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény (továbbiakban: Sztv.) egyik ellátási formájára, az adósságkezelé-

si szolgáltatására vonatkozó adatkezelési kérdésekben kérte az egyik megyei jogú város jegyzője álláspontunkat. Az Sztv. 55/A. §-ának (5) bekezdése alapján az önkormányzat a lakhatást veszélyeztető mértékű adósság felhalmozódásának elkerülése céljából a követelés jogosultjával megállapodást köthet, melynek keretében – az adós írásbeli beleegyezése esetén – a követelés jogosultja az adós lakóhelye szerint illetékes település jegyzőjét félévente tájékoztatja a legalább háromhavi tartozást felhalmozó adósokról.

Tekintettel arra, hogy az önkormányzati lakások hasznosítását és a bérleti szerződésből fakadó jogok és kötelezettségek teljesítését, érvényesítését részben az önkormányzat tulajdonában álló gazdasági társaság végezte, a személyes adatok kezelésének feltételeit a felek között létrejött szerződés határozta meg. A kérdés tehát az volt, hogy az Sztv. idézett 55/A. § (5) bekezdésében foglalt követelés jogosultja (például a lakbérhátralék vagy egyéb követelés tekintetében) az önkormányzat, vagy a tulajdonában levő vagyonkezeléssel, hasznosítással megbízott gazdasági társaság – a jogosultnak kell ugyanis az érintett hozzájárulását beszerezni (a személyes adatokat a szociális nyilvántartásba továbbítják, amely elkülönül az önkormányzati vagyonkezelői és tulajdonosi célokat szolgáló adatkezeléstől). Tehát a lakásbérleti szerződések megkötése és teljesítése céljából kezelt személyes adatokat csak akkor továbbíthatják a szociális nyilvántartást is kezelő szociális igazgatást végző szervezeti egységhez, ha ahhoz az érintettek a törvény rendelkezése alapján írásban hozzájárultak és a két adatkezelő között létrejött a törvény szerinti megállapodás, melynek célja az adósságfelhalmozás megelőzése. (Kivétel ez alól a szociális eljárás keretében kiutalt bérlakások esete.) Ugyanez a helyzet azon „jogosultakkal" is, akik az önkormányzat tulajdonosi körén kívül álló szolgáltatókból állnak.

Az adatokat az idézett törvényhely alapján tehát nem az önkormányzat adja át a szolgáltatóknak, hanem éppen fordítva, az érintettek írásbeli felhatalmazása alapján a szolgáltatók jelzik a szociális igazgatási részlegnek, hogy potenciális ügyfelük lehet a követelésük alanya. A kérelemre megindult szociális eljárás során a kérelmezőnek kell igazolnia, bizonyítania, hogy mekkora a tartozásának az összege.

Az önkormányzat tulajdonosi minőségében akkor ismerheti meg a lakbérhátralékkal rendelkezők adatait, ha az érintett bérlőkkel szerződéses jogviszonyban áll, vagyis a lakásbérleti szerződés egyik alanya (bérbeadóként) az önkormányzat. *(1174/K/2007)*

Az önkormányzati adóhatóság által közérdekből nyilvánosságra hozható személyes adatok kezelésére vonatkozó állásfoglalást kért egy község jegyzője, amikor azt kérdezte, hogy az APEH gyakorlatához hasonlóan helyi szinten is lehet-e valamilyen adattartalommal negatív vagy pozitív adóslistát készíteni és azt a helyben szokásos módon közzé tenni.

Az adatvédelmi törvény és az Art. rendelkezései alapján az adóhatóság által kezelt személyes adatok egyúttal adótitkot is képeznek és nem csak a természetes személy adózók, de más adózók adótitoknak minősülő adatát is csak a törvényben meghatározott feltételek fennállása esetén jogosult az önkormányzati adóhatóság (a jegyző) nyilvánosságra hozni. Pozitív adóslistát természetes személyek esetében elvileg csak a személyes adataik és adótitkaik kezeléséhez is megadott hozzájárulásuk alapján lehetne készíteni és nyilvánosságra hozni. Azonban egy ilyen lista összeállítására és közzétételére – amely szintén adatkezelésnek minősül – nincs semmilyen törvényes jogalapja a jegyzőnek, törvény felhatalmazásának hiányában még az érintettek hozzájárulásával sem kezelhet ilyen célból adótitoknak is minősülő személyes adatokat. Az Art. 55. § (3) bekezdése alapján, az ott meghatározott feltételek megléte esetén az adóhatóság (az önkormányzati adóhatóság is) közzéteszi azoknak az adózóknak az adatait, akiknek (amelyeknek) a terhére az előző negyedév során jogerőre emelkedett határozatban meghatározott összegű adóhiányt állapított meg, feltéve, hogy az erről szóló határozatban előírt fizetési kötelezettségüknek a határozatban megállapított határidőben nem tettek eleget. A biztos javasolta a jegyzőnek, hogy a helyi adózási morált az Art. VII. és VIII. fejezetében foglalt eljárási hatáskörök szigorúbb és következetesebb alkalmazásával állítsák helyre. *(1979/K/2007)*

Szektorális adatkezelések

Egészségügy

A 2007-es év egyik legfontosabb közéleti kérdése a kormány által meghirdetett egészségügyi reform, illetőleg ennek jogalkotási vonatkozásai voltak. Ennek nagy jelentőségű adatvédelmi vonatkozása is volt: az ellátórendszer átfogó átalakulása óriási mennyiségű egészségügyi adat továbbításával jár együtt. Az egészségügyi reform kapcsán mindenkép-

pen szükséges megemlíteni a végrehajtást felügyelő Egészségügyi Minisztérium eljárását. A véleményezésre megküldött tervezeteket a törvény kifejezett rendelkezése ellenére sok esetben nem tették közzé a honlapon, másrészt számos esetben olyan rövid határidőt szabtak a tervezetek véleményezésére, amely gyakorlatilag lehetetlenné tette a megalapozott vélemény kialakítását. Ennek kirívó példája volt, amikor a reform egyik pillérének tartott egészségügyi törvény tervezetének véleményezésére mindössze három napot biztosított a tárca.

Az elmúlt évek hasonlóan nagy horderejű intézkedése az Irányított Betegellátási Rendszer kialakítása volt, amely kezdetektől fogva adatvédelmi aggályokat hordozott. Az Alkotmánybíróság 2007-ben határozatot hozott az Irányított Betegellátási Rendszerrel kapcsolatos indítványról. Az Alkotmánybíróság megállapítása szerint a jogalkotó mulasztásban megnyilvánuló alkotmánysértést követett el azzal, hogy az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (továbbiakban: Eüak.), valamint a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény (továbbiakban: Ebtv.) az ellátásszervezők által történő adatkezelésre vonatkozó tájékoztatással összefüggésben nem alkotta meg mindazokat az eljárási szabályokat, amelyek biztosítják, hogy az érintett adatai kezelésének megtiltásáról az adattovábbítást megelőzően nyilatkozhasson.

Az Alkotmánybíróság az adatvédelmi biztos kezdeményezésére vizsgálja a vizitdíj visszatérítésével kapcsolatos szabályok alkotmányellenességét. Az Ebtv., és végrehajtási rendelete szerint, ha az érintett az adott évben húsz alkalmat meghaladóan fizet vizitdíjat, azt a területileg illetékes önkormányzat jegyzőjétől visszaigényelheti. A vitatott rendelkezés alkalmazása során ugyanakkor olyan személyek ismerhetik meg a visszaigénylő érintett adatait, akiknek ez feladatuk ellátásához szükségtelen. A kifogásolt rendelkezések tehát az Eüak. által nem nevesített célra történő adatkezelést írnak elő. Ily módon a vizitdíjat fizető érintettek személyes adatainak védelméhez fűződő joga azzal, hogy alapvetően fiskális szempontok alapján az ellátóhálózaton kívüli olyan szerv kezelésébe kerül az egészségi állapottal összefüggésbe hozható adat, mely szervnek az Eüak.-ban szereplő adatkezelés nem tartozik a feladatkörébe, szükségtelen és aránytalan korlátozásnak van kitéve.

Az Eüak. 1. §-a szerint személyes adatot csak törvényes cél eléréséhez szükséges esetekben és mértékben lehet kezelni. A törvény szerkezeti felépítéséből adódóan az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelése elsődlegesen pontosan meghatározott célokból, és az egészségügyi ellátóhálózaton belül kell, hogy történjen. Az ellátóhálózaton kívüli ilyen adatkezelésre csak kivételes körülmények között kerülhet sor.

A nyugta adattartalmából következtetni lehet az érintett egészségi állapotára, mert maga a vizitdíj visszaigénylésének ténye is közvetlenül utalhat arra, hogy az érintett egészségi állapota gyenge vagy krónikus betegségben szenved, illetve a nyugtát kiállító intézmény neve adott esetben következtetni enged arra, hogy az érintett milyen típusú kezelésben részesült. Az indítvány szerint a vizitdíjról kiállított nyugta az érintettel összefüggésbe hozható különleges adatokat tartalmaz, amelyet mind az adatvédelmi törvény, mind az egészségügyi adatok kezelését szabályozó szektorális törvény fokozott védelemben részesít.

A kifogásolt rendelkezések az Eüak. által nem nevesített célra történő adatkezelést írnak elő, ily módon a vizitdíjat fizető érintettek személyes adatainak védelméhez fűződő joga sérül azzal, hogy alapvetően fiskális szempontok alapján az ellátóhálózaton kívüli olyan szerv kezelésébe kerül az egészségi állapottal összefüggésbe hozható adat, mely szervnek az Eüak.-ban szereplő adatkezelés nem feladata. *(420/H/2007)*

Hivatalból indult vizsgálat a megszűnő egészségügyi intézmények dokumentációjának elhelyezési kérdéseivel kapcsolatban, mivel a dokumentáció kezelése jelentős mértékben érinti a betegek információs önrendelkezési jogának érvényesülését. Az ügyben született ajánlás szerint jelentős figyelmet kell fordítani ennek kapcsán a nem papíralapú dokumentáció sorsára is. A felmerült kérdések tisztázására széles körű vizsgálat zajlott az érintett döntéshozó szervek, valamint a megszűnő intézmények vezetőinek bevonásával.

A vizsgálat során a következő kérdések merültek fel: biztosítottak-e az átalakítások végrehajtására, valamint az adatok biztonságos kezelésének, (esetlegesen digitális) mentésének, az adatalanyok jogainak érvényesítéséhez szükséges adatkezelési rendszerek kialakítására fordítandó pénzeszközök, továbbá mi a tárca, illetve a fenntartó Fővárosi Önkormányzat stratégiája és álláspontja az adatkezeléssel kapcsolatban. A biztos megkeresése kiterjedt arra is, hogy az egészségügyi

reform rendelkezései befolyásolják-e az érintettek információs önrendelkezési jogának gyakorlását, kezelik-e a jogutódhoz átkerülő intézményi eszközökön tárolt személyes adatokat, illetve milyen felhatalmazás és milyen adatvédelmi szabályok szerint.

Az egészségügyi miniszter tájékoztatása szerint az intézmények megszüntetésével kapcsolatos feladatok végrehajtására az érintett intézmények vezetői kaptak megbízást. Ezek között kiemelten szerepel az intézményekben kezelt egészségügyi dokumentáció szakszerű kezelése és elhelyezése. A miniszter információt kért az érintett intézmények vezetőitől az iratanyagok elhelyezése céljából az iratok mennyiségéről és fajtáiról. Az információ összesítése után kerül sor az elhelyezéshez szükséges feldolgozásra. Az üggyel kapcsolatos aktuális feladatokat az intézményvezetőkkel tartott rendszeres egyeztető értekezleten határozzák meg. Tájékoztatta továbbá a biztost, hogy június, július folyamán a Magyar Országos Levéltár képviselőjével minden intézményben felmérték a tárolt dokumentumokat és ezekről emlékeztetők is készültek.

2007 októberében konzultáció zajlott az Egészségügyi Készletgazdálkodási Intézet főigazgatójával is a megszűnő és átalakuló intézmények dokumentumainak elhelyezéséből fakadó feladatokról. A konzultáció során a biztos tájékoztatást kapott az intézmények irattárainak általános állapotáról, mely sok helyütt nem elégíti ki a törvényi követelményeket és ennél fogva alkalmatlan az érintett személyek információs önrendelkezési jogának érvényesítésére.

A kérdés jelentőségét tovább növeli, hogy az Eüak. előírja, hogy az egészségügyi dokumentációt – a képalkotó diagnosztikai eljárással készült felvételek, az arról készített leletek kivételével – az adatfelvételtől számított legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. Képalkotó diagnosztikai eljárással készült felvételt, valamint a felvétel esetén az arról készített leletet kell – a felvétel készítésétől számított – legalább 30 évig megőrizni. Az adatmegőrzés érdekében folyamatosan biztosítani kell, hogy az adathordozó az adott technikai feltételek mellett olvasható maradjon, vagy olvasható állapotba kerüljön. Ezen előírás érvényesülésére vonatkozó intézkedést, tervet a megkeresettek által nyújtott tájékoztatás nem tartalmaz.

A vizsgálat során megállapítottuk, hogy az intézmények átalakításával összefüggően – mivel a dokumentáció sorsa nem tisztázott – az érintettek információs önrendelkezési jogát súlyos sérelem fenyegeti. Az érintettek számára ugyanis feltehetően egyáltalán nem lesz világos és

áttekinthető adataik és egészségügyi dokumentációjuk sorsa, így iratmegismerési joguk gyakorlása mellett az Eütv.-ben foglalt jogaikkal sem tudnak élni, azaz egészségük megőrzését, gyógyításukat illetve gyógyulásukat veszélyeztetheti az a helyzet, melyben az őket ellátó intézmény (orvos) nem tudja az érintettek egészségügyi „előéletét" megismerni. A dokumentáció sorsának nem szakszerű kezelése miatt feltehetően sem az ellátó, sem az ellátott nem lesz abban a helyzetben, hogy a megszűnő, vagy átalakuló intézményben tárolt dokumentációhoz hozzáférhessen, illetve annak hollétéről tudomást szerezzen.

Felhívtuk az egészségügyi miniszter figyelmét arra, hogy az intézmények átalakítása során kiemelt jelentőséget tulajdonítson az egészségügyi dokumentáció kérdésének, és tegyen megfelelő intézkedéseket arra, hogy az átalakuló és megszűnő intézmények – fenntartótól függetlenül – egységesen és az ellátottak jogainak figyelembe vételével döntsenek az egészségügyi dokumentáció kezeléséről. Szükséges emellett az egészségügyi dokumentáció átadása-átvétele olyan rendszerének kialakítása, mely folyamatosan biztosítja a beteg ellátásához kapcsolódó információk megismerését annak érdekében, hogy az érintettek ellátása ne szenvedjen csorbát.

Az ajánlás, amely számos egyéb javaslatot fogalmaz meg, teljes terjedelmében a honlapon található. *(903/H/2007)*

Hivatalból indult vizsgálat az úgynevezett jogviszony-ellenőrzés körében. A kormányzat célkitűzése szerint a járulékot nem, vagy csak részben fizető állampolgárokat ki kell szűrni a biztosítottak közül, és határidő tűzésével fel kell hívni az elmaradt járulékok rendezésére. A vizsgálat keretében az Országos Egészségbiztosítási Pénztár (OEP) illetékeseivel lefolytatott konzultáció és a rendelkezésre álló dokumentáció értelmében három, egymástól teljesen elkülönülő ténykérdés vizsgálható. Először is, hogy az érintett rendelkezik-e érvényes TAJ-számmal, másodszor, rendelkezik-e a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvényben meghatározott biztosítási jogviszonnyal, végül hogy a biztosítotti jogviszony mögött történik-e tényleges járulékfizetés.

A vizsgálat megállapítása szerint a TAJ-autorizációs szolgáltatás kizárólag az adott TAJ szám érvényességét szűri, azaz, hogy az OEP rend-

szerében a TAJ azonosító érvényes adatként szerepel-e a nyilvántartásban. Érvénytelenségi ok lehet, ha az érintett személy elhalálozott vagy véglegesen külföldre távozott. Az ellenőrzés történhet on-line, de az elektronikus hozzáféréssel nem rendelkező háziorvosok opcionálisan a saját betegkörükre nézve az OEP-től papíralapon vagy mágneses adathordozón megkaphatják TAJ-szám és születési dátum alapján a „negatív listát" is.

Magánszemélyek a jogviszony-ellenőrzést csak személyesen vagy a Megyei Egészségbiztosítási Pénztárakon keresztül írásban, illetve az ügyfélkapun keresztül kizárólag saját magukra vonatkozóan végezhetik el.

A fentiek alapján megállapítható volt, hogy az OEP úgynevezett TAJ autorizációs szolgáltatásának rendszere esetleges adatvédelmi visszaélések elkövetésére igen korlátozott módon, de alkalmas lehet abban az esetben, ha illetéktelen személy egy általa ismert személy TAJ számának birtokában teszi fel kérdéseit. A visszaélések kiküszöbölésére javasoltuk a lekérdezések naplózásának bevezetését. Amennyiben a szolgáltatás az eredetileg javasolt módon a jogviszony-ellenőrzés adataival kibővülne, ideértve a viszontazonosítást és naplózást is, elengedhetetlen követelménynek tartjuk az adatbiztonsági garanciák beépítését. *(713K/2007)*

Állampolgári panasz alapján vizsgáltuk a véradás előtt kitöltendő kérdőívet. Az adatlap kérdést tartalmaz a leendő donor esetleges homoszexuális kapcsolatára vonatkozóan. Megkerestük az Országos Vérellátó Szolgálat (OVSz) vezetőjét, valamint az Európai Unió tagállamai adatvédelmi hatóságainak képviselőit tömörítő 29-es Munkacsoport tagjait. A vizsgálat során megállapítottuk, hogy a kérdés nem sérti a donorok személyes adatok védelméhez fűződő jogát. Az adatkezelés jogalapja az egészségügyről szóló 1997. évi CLIV. törvény 226. § (2) bekezdése, mely szerint a véradót – saját, illetve az általa adott vérből előállított vérkészítményt kapó beteg egészségének védelme érdekében – a véradásra való alkalmassága tekintetében ki kell vizsgálni. Ennek során a véradó köteles a saját egészségi állapotáról, valamint életviteléről – amennyiben az a vér útján átvihető fertőző betegségek szempontjából jelentős – a vizsgálatot végző orvos kérdésére felvilágosítást adni.

Az OVSZ vezetője felhívta továbbá a figyelmet arra, hogy a levett vér a véradást követően csupán korlátozott ideig használható fel, míg egyes fertőzések, így többek között a HIV ezen idő alatt nem mutathatóak ki

teljes bizonyossággal. Az uniós adatvédelmi hatóságoktól beérkezett válaszok alapján mindez megegyezik az európai gyakorlattal. Ugyanakkor a vonatkozó alkotmánybírósági határozatokra hivatkozva érvelésében a biztos kifogásolta, hogy a donorok adatait a véradásból való tartós kizárás ellenére nyilvántartják. Álláspontja szerint mindez sérti a célhoz kötöttség követelményét. Mindezek alapján a biztos felszólította az OVSZ vezetőjét az állásfoglalásban kifejtetteknek megfelelő gyakorlat kialakítására. *(1716/P/2007)*

Számos jelzés érkezett főleg idős emberektől, akiket otthonukban telefonon kerestek meg ismeretlenek és részletesen kikérdezték, vagy próbálták kikérdezni őket egészségi állapotukról, gyógyszerszedési szokásaikról. Tekintettel arra, hogy telefonhívás esetén a hívók személyét, a kikérdezés pontos célját nem lehet minden kétséget kizáróan kideríteni és ellenőrizni (így többek között az anonimitás ígéretét sem), felhívtuk a nyilvánosság figyelmét arra, hogy az egészségi állapotra vonatkozó információk különleges, úgynevezett érzékeny adatoknak minősülnek, melyeket csak szigorú törvényi szabályok betartása mellett lehet kezelni. Mindezek alapján azt tanácsoltuk minden érintettnek, hogy egészségi állapotra vonatkozó adatot telefonon csak abban az esetben közöljenek, ha egyértelműen tisztázottak az adatkezelés körülményei. *(2117/H/2007)*

Az egyik beadványozó tervezett egészségügyi adatkezelés adatvédelmi szempontnak való megfelelése tekintetében kért állásfoglalást. A beadvány szerint az adatkezelő egészségügyi dolgozók továbbképzésével foglalkozik. Az előadások anyagát a betegekről készített felvételek képezik, ideértve a személyes beteginterjúkat is. A továbbképzésben résztvevők az elektronikusan rögzített előadásokat az interneten keresztül érhetik el. A tervezett adatkezelés a megkívánt garanciák kiépítése esetén elfogadható.

Az adatvédelmi törvény 3. § (2) bekezdése értelmében az egészségi állapotra vonatkozó különleges adat törvény felhatalmazása hiányában a megjelölt adatkezelés csak az érintett, illetve jelen esetben törvényes képviselőjének írásbeli hozzájárulása alapján történhet. Az Eüak. tételesen sorolja fel az egészségügyi és személyazonosító adat kezelésének lehetséges céljait, külön nevesítve az egészségügyi szakember-képzést. A beadvány szerint az érintett személyiségi jogainak védelme érdekében neve az oktatási anyagokban nem lesz megismerhető, illetőleg

szemkörnyéke kitakarásra kerül. Az érintettek személyes adatai védelme érdekében azonban a biztos mindenképp helyesebbnek tartotta azt a megoldást, ha például az arc nem jelenik meg a képen, feltételezve, hogy a betegség bemutatásához ehhez nincs is szükség, és a hang is eltorzításra kerül.

Tekintettel arra, hogy az adatvédelmi törvény fogalom-meghatározása szerint a személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható, az adatkezelés során különös figyelmet kell fordítani arra, hogy a hozzájáruló nyilatkozatban foglalt személyes adatok, és a felvételek ne legyenek összekapcsolhatók. Fontos továbbá, hogy a szervezeten belül ki kell jelölni egy személyt, aki az adatvédelemért felelős. *(888/P/2007)*

Munkáltatók

Lehet-e digitális arcelemző eszközzel minősíteni a munkaerő felvétel során a jelentkezőket? A 2007. évi, munkaviszonnyal kapcsolatos vizsgálatokat talán ez a beadványban megfogalmazott kérdés jellemezte a legjobban, mely két jelenségre mutat rá. Egyrészt arra, hogy a munkavállalók magánszférájának, és személyes adatainak feltérképezésére lehetőséget adó technikai eszközök folyamatosan megújuló generációival kell számolni, másrészt arra a gondolkodásmódra, hogy ha rendelkezésre áll a technológia, akkor azt gyakorta alkalmazzák is, tekintet nélkül az érintettek személyiségi jogainak esetleges sérelmére. A feltett kérdésre a válasz, hogy a jogszerűen lefolytatott, személyiségjegyek felmérésére irányuló eljárásokban a munkavállaló által kitöltött teszt minősítését először az érintettnek kell továbbítani, aki azt megismerve eldönti, hogy hozzájárul-e annak a munkáltató részére történő továbbításhoz. A digitális arcelemző eszköz azonban ilyen jellegű döntési lehetőséget nem ad az érintett számára, így szükségszerűen kiszolgáltatott helyzetbe kerül az eljárást lefolytató személlyel szemben. *(2550/K/2007)*

Több munkavállaló azzal a kérdéssel fordult Irodánkhoz, hogy lehet-e a munkaügyi felvételi eljárás során, illetőleg jogviszony alatt a hatósági erkölcsi bizonyítványon felül, úgynevezett feddhetetlenségi bizonyítványt is kérni a dolgozótól, mely a bűnügyi nyilvántartásból megkért tájékozatót tartalmazza.

A bűnügyi nyilvántartásról és a hatósági erkölcsi bizonyítványról szóló 1999. évi LXXXV. törvény (továbbiakban: Bnytv.) 3. §-a értelmében

a bűnügyi nyilvántartás közhitelű hatósági nyilvántartás, amely a bűntettesek, a kényszerintézkedés alatt állók, a büntetőeljárás alatt állók, az ujj- és tenyérlenyomatok, a fényképek, valamint a DNS-profilok egymástól elkülönült nyilvántartásaiból áll. A nyilvántartásból csak kérelemre lehet teljesíteni adatszolgáltatást, és csak olyan személyek részére, akik számára ezt törvény lehetővé teszi. Az adatkezelésben érintett személy az adatvédelmi törvény alapján igényelhet személyes adatot a nyilvántartásból.

A Bnytv. 57. §-a értelmében a hatósági erkölcsi bizonyítvány kiállítását kizárólag az érintett személy kérheti, és tartalmazza a kérelmező természetes személyazonosító adatait, büntetlensége, mentesítésben részesülése, továbbá a vádemelés elhalasztása esetén a „bűntettesek nyilvántartásában nem szerepel" közlést, illetőleg büntetett előélete esetén az egyes büntetésekre és intézkedésekre vonatkozó adatokat. A Büntető Törvénykönyvről szóló 1978. évi IV. törvény (továbbiakban: Btk.) alapján a mentesítés folytán az elítélt mentesül azon hátrányos következmények alól, amelyeket az elítéléshez jogszabály fűz. A Btk., valamint a Bnytv. rendelkezései alapján, amennyiben az elítélt mentesült a büntetett előélethez fűződő hátrányok alól, büntetlen előéletűnek tekintendő, a hatósági erkölcsi bizonyítványt pedig ennek megfelelően állítják ki számára. A bűnügyi nyilvántartásban azonban a Bnytv. rendelkezéseinek megfelelően ennél tovább, a törvény által meghatározott ideig kezelik az adatokat.

Jóllehet a Bnytv. lehetővé teszi azt, hogy az érintett személy a bűnügyi nyilvántartásban szereplő személyes adatairól tájékoztatást kérjen, ennek célja azonban az, hogy az érintett átláthassa személyes adatainak kezelését, és nem az, hogy őt a munkáltató átvilágítsa.

A Munka Törvénykönyvéről szóló 1992. évi XXII. törvény (továbbiakban: Mt.) 77. §-a értelmében a munkavállalótól csak olyan nyilatkozat megtétele vagy adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely személyiségi jogait nem sérti, és a munkaviszony létesítése szempontjából lényeges tájékoztatást nyújthat.

Az idézett jogszabályi rendelkezések alapján megállapítható, hogy az a munkáltatói szándék, miszerint a munkavállalók erkölcsi alkalmasságát – jogszabályi felhatalmazás hiányában – a bűnügyi nyilvántartásból, az érintett kérelmére, számára kiállított nyilatkozattal kívánja megállapítani, súlyosan sérti az érintett személyes adatok védelméhez való jogát, az érintettet jogellenesen diszkriminálhatja és ellentétes a

hátrányos jogkövetkezmények alóli mentesüléshez fűződő közérdekkel. *(1880/P/2007, 2478/P/2007)*

Az előző évekhez hasonlóan, ez évben is kiemelkedően magas a munkavállalók kamera-rendszer általi megfigyelésével kapcsolatos beadványok száma. Egy kft. munkavállalói azzal a beadvánnyal fordultak hozzánk, hogy a munkahelyükön, egy virágüzletben kamerákat szereltek fel. A kamera-rendszer működésének célja a megadott tájékoztatás értelmében statisztika készítése. A felek a munkaszerződést oly formában módosították, hogy *„jelen szerződés aláírásával a munkavállaló visszavonhatatlanul elismeri, hogy a munkáltató maradéktalanul tájékoztatta arról, hogy a számára munkavégzésre kijelölt területen, a nap 24 órájában üzemelő, audio és videó jelek rögzítésére zártláncú videokamerás megfigyelő rendszer van telepítve"*. A beadvány szerint az üzlet raktárában is kamera-rendszert szereltek fel, mely addig öltözőként funkcionált, a munkavállalók tiltakozására pedig azt a választ kapták, ha zavarja a kamera őket, akkor ne öltözzenek többé ott. Arra irányuló kérésüket, hogy megnézzék, mit rögzít a kamera, megtagadták. A kamera-rendszer működésének második napján már arról kaptak tájékoztatást az érintettek telefonon, hogy látják őket, fokozzák a munkatempót, melyből arra következtettek, hogy a kamera-rendszer működése a munka intenzitásának megfigyelését is szolgálja. A kamerák által felvett képeket internet segítségével a munkáltató más területeken is megtekinthette tehát.

A kialakult adatvédelmi gyakorlat értelmében, állandó munkavégzés területén főszabály szerint kamera-rendszer még akkor sem működtethető, ha a továbbított képeket egyébként nem rögzítik (a munkahelyi kamera-rendszerekkel kapcsolatos adatvédelmi biztosi állásfoglalás az adatvédelmi biztos honlapján megtalálható). Nem teremt jogalapot a kamera-rendszer működtetéséhez az érintettől kényszer útján beszerzett hozzájárulás sem. A beadványban ismertetett, munkaszerződésben történő hozzájárulás ellentétes az adatvédelmi törvény rendelkezéseivel, tekintettel arra, hogy a munkajogi szabályok értelmében a munkaszerződést csak a felek egyező akaratával lehet módosítani, azonban az adatvédelmi törvény rendelkezései értelmében az érintett bármikor, szabadon visszavonhatja hozzájáruló nyilatkozatát, ahhoz a munkáltató hozzájárulását nem kell beszereznie. *(598/P/2007)*

Továbbra is gyakoriak a munkahelyi internet és elektronikus-postafiók használatának ellenőrzésével kapcsolatos panaszok.

Egy beadványozó azzal a munkáltatói eljárással kapcsolatosan fordult az adatvédelmi biztoshoz, hogy vezetője – vélhetőleg egy kémprogram segítségével – hozzájutott a freemail postafiókjának jelszavához, és annak tartalmát tudta és beleegyezése nélkül napi rendszerességgel ellenőrizte. Az adatvédelmi biztos által kialakított álláspont szerint a munkáltató még akkor sem jogosult az elektronikus postafiókba beérkező levelek tartalmát automatikusan megismerni, ha az ellenőrzés tényéről a munkavállaló tud, ahhoz hozzájárult. Különösen sérti az érintett személyes adatok védelméhez való jogát a beadványban ismertetett eljárás, miszerint a teljesen privát használatban lévő freemail postafiók tartalmát ismeri meg a közvetlen vezető, ez okból az adatvédelmi biztos felhívta az érintett figyelmét arra, hogy a vezető magatartása kimerítheti a Btk. 177/A. §-ában szabályozott visszaélés személyes adattal tényállás vétségi alakzatát. *(2162/P/2007)*

Egy németországi vállalat magyar leányvállalatának munkatársa azzal a kérdéssel fordult hozzánk, hogy az anyavállalat utasítására jogszerűen telepíthető-e egy olyan program a dolgozók számítógépeire, mellyel a német központban lényegében minden, a számítógépen tárolt adatot, azon végezett műveletet ellenőrizhetnének.

Állásfoglalásában a biztos arra mutatott rá, hogy a munkáltatói jogkört gyakorló személy adatfeldolgozónak minősül, az anyavállalat pedig a tényleges adatkezelőnek. Ezzel a megoldással lényegében a munkáltatói jogosultság a Magyarországon bejegyzett gazdasági társaságtól a magyar joghatóság alá nem tartozó anyavállalathoz kerülne, mely alapvetően ellentétes a munkavállalók jogainak védelmével, tekintettel arra, hogy a német székhelyű anyavállalat által meghozott döntésekre a magyar joghatóság nem terjed ki. Az adatkezelésnek ez a magyar joghatóság alóli „kihúzása" akkor is sérti az érintettek személyes adatok védelméhez való jogát, ha azok az adatkezeléshez a hozzájárulásukat formailag megadták, tekintettel arra, hogy az Alkotmánybíróság által megfogalmazott azon követelmény sérül, miszerint az érintett személy adatai kezelését jogosult átlátni, az azzal kapcsolatos jogait pedig jogosult érvényesíteni. *(2511/K/2007)*

Egyre gyakoribbak azok a beadványok, melyekben a biometrikus – az eddigi ügyek alapján ujjlenyomat alapú – beléptető-rendszerek alkalmazhatóságával kapcsolatosan kértek állásfoglalást. Az ilyen ellenőr-

zések elsődleges céljaként az adatkezelők a munkahelyre érkezés, illetőleg az onnan való távozás pontos regisztrációját jelölték meg. A célhoz kötött adatkezelés elvéből kiindulva abban az esetben, ha több eljárás között választhat a munkáltató, akkor azt kell alkalmaznia, mely az érintett személyiségi jogait kevésbé korlátozza, sérti.

> Biometrikus alapú beléptető-rendszereket csak olyan területeken lehet alkalmazni, ahol a magánterületen őrzött vagyon, vagy egyéb érdek azt valóban megköveteli, nem lehet a technológiát pusztán azért bevezetni, mert kényelmesebb ellenőrzést tesz lehetővé. A rendszerrel kapcsolatos további követelmény, hogy nem lehet a munkavállalók ujjlenyomatáról képzett számsorból adatbázist képezni. *(89/K/2007, 166/K/2007, 1744/P/2007)*

Szintén az előző évekhez hasonlatosan, több munkavállaló azzal a beadvánnyal fordult hozzánk, hogy a vezetője átkutatta a rendelkezésére bocsátott öltözőszekrényt. A munkáltatók az öltözőszekrények átvizsgálását vagyonvédelmi céllal indokolták, az egyik bepanaszolt cég válaszlevelében az adatkezelést azzal is alátámasztotta, hogy maga az öltözőszekrény a vállalat tulajdonában van.

> A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény rendelkezései értelmében a személy- és vagyonvédelmi tevékenységet végző személy a törvényben meghatározott jogosultságait a jogos önhatalom keretei között vagy az érintett személy önkéntes hozzájárulása alapján gyakorolja. A vagyonőrzési feladatokat ellátó személy- és vagyonőr a megbízó közterületnek nem minősülő létesítményének őrzése során jogosult a területre belépő vagy onnan kilépő személyt csomag, illetve menet-, szállítási okmány bemutatására felhívni.
>
> A kialakult adatvédelmi gyakorlat alapján a munkavállalót – többek között a személyes adatai védelmén keresztül – megilleti a magánszféra védelméhez való jog a munkahelyén is. A munkáltató a munkavállalójának a magánszféráját indokolatlanul nem sértheti meg, például vagyonvédelem céljából a munkavállaló által a munkahelyre bevitt értéktárgyait, így különösen, ruháit, iratait, táskáit önhatalmúlag nem vizsgálhatja át. A munkavállaló öltözőszekrényének átvizsgálása személyes adatok kezelésével jár, mely adatkezeléshez a jogalapot – mivel azt törvény nem rendeli el – csak az érintett előzetes hozzájáruló nyilatkozata adhatja meg. Az adatkezelés jogalapjának megléte mellett vizsgálni kell továbbá azt is, hogy az adatkezelés megfelel-e a célhoz

kötött adatkezelés elvének. Ennek értelmében ugyanis csak akkor kezelhető személyes adat, ha az ilyen módon megvalósítani kívánt cél más módon nem megvalósítható, illetőleg csak a cél megvalósulásához szükséges mértékig.

Tekintettel arra, hogy a tulajdon védelme, vagyis a munkahelyen őrzött értékek védelme más, a munkavállalók magánszférájának csekélyebb mértékű korlátozásával is megvalósítható, a beadványban ismertetett munkáltatói eljárás a célhoz kötött adatkezelés elvével ellentétes, ezért sérti az Alkotmány 59. § (1) bekezdésében foglalt személyes adatok védelméhez való alkotmányos alapjogot. *(1511/P/2007)*

Több adatkezelő is állásfoglalást kért a belső visszaélés-jelentési rendszerekről, melyekkel elsősorban külföldi tulajdonú nagyvállalatoknál találkozhatunk. A kérdésről az elmúlt évi beszámoló „Nemzetközi ügyek" fejezete részletesen szól, mára azonban az Unió adatvédelmi biztosaiból álló munkacsoport elvi állásfoglalása helyett gyakorlati tapasztalatokról is be tudunk számolni. A módszer a különböző, általában szépen hangzó elnevezés ellenére lényegében nem más, mint egy, a munkáltató által működtetett belső besúgó rendszer. A belső visszaélés-jelentési (elterjedt szóhasználattal: whistleblowing) rendszerek kialakítását az Amerikai Egyesült Államok Kongresszusa tette kötelezővé 2002-ben a Sarbanes-Oxley törvénnyel (SOX), a vállalati pénzügyi botrányok gyakorisága miatt. Több amerikai vállalat tevékenysége folytán a SOX mellett az uniós adatvédelmi szabályok hatálya alá is tartozik itt lévő érdekeltségei okán, és a rendszert sajnálatos módon több európai nagyvállalat is átvette. A hazai gyakorlatban azonban a belső visszaélés-jelentési rendszerek alkalmazása az esetek jelentős részében az adatkezelésben érintett személyek jogainak sérelmével jár. Egyes esetekben a hazai munkáltatók – vélhetőleg az elérendő célt félreértve – olyan jelentési rendszert hoznak létre, mely voltaképpen nem más, mint besúgói hálózat, melyben a munkavállalók – csekély súlyú szabálysértések esetén is – egymást szabadon feljelenthetik.

A belső visszaélés-jelentési rendszert a magyar jog nem szabályozza, működése során azonban személyes adatok kezelésére kerül sor, amelyhez – törvény felhatalmazása hiányában – szükség van az érintett személy tájékozott hozzájárulására. A célhoz kötött adatkezelés elvéből fakadóan a belső visszaélés-jelentési rendszerek alkalmazása során a bejelenthető szabálysértések körét korlátozni kell, a kisebb

súlyú szabálysértések felderítését, szankcionálását a helyi vezetőkre kell bízni. Korlátozni érdemes továbbá azoknak a személyeknek a körét is, akik a jelentésekben érintettek lehetnek, az ellenőrzésnek elsősorban a vezetők ellenőrzésére kell irányulnia. Tájékoztatni kell a jelentést tevő személyt arról, hogy személyazonosságát nem fedik fel illetéktelen személyek előtt, személyes adatait az eljárás egész szakaszában bizalmasan kezelik, amennyiben azonban elkerülhetetlen, fel kell fedni a meginduló vizsgálat során.

Lényeges hangsúlyozni, hogy a bejelentést tevő személyen túl a „feljelentett" személyeket is megilleti a személyes adatok védelméhez való jog, őket a lehető leggyorsabban tájékoztatni kell az adatkezelés tényéről, és biztosítani kell, hogy jogaikat gyakorolhassák. A „feljelentett" személy csak kivételes esetben juthat a jelentő személyazonosságára vonatkozó információhoz, például, ha a jelentés nyilvánvalóan rosszhiszemű.

A visszaélés-jelentő rendszerek esetében alapos mérlegelést igényel a jelentések összegyűjtésének és kezelésének módja. A vállalatok belső ellenőrzési szerv helyett kialakíthatnak külső ellenőrzést is, ahová a rendszer egy részét, többnyire a jelentések gyűjtését kiszervezik. Az adatvédelmi törvény rendelkezései értelmében a munkáltató csak olyan feladatokat szervezhet ki külsős személyek részére, melyek nem adatkezelésnek, hanem adatfeldolgozásnak minősülnek. Adatfeldolgozás az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Amennyiben a külsős cég adatkezelési tevékenységet is végez – így kivizsgálja a hozzá beérkező bejelentést – azt csak az érintett személy hozzájáruló nyilatkozata alapján teheti meg.

Amennyiben a vállalatok vagy vállalatcsoportok külső szolgáltatóhoz fordulnak a visszaélés-jelentő rendszer irányításának részleges kiszervezése – adatfeldolgozás – érdekében, továbbra is felelősek maradnak az abból eredő adatfeldolgozási műveletekért.

A kérdéssel kapcsolatban még érdemes megjegyezni, hogy az ilyen rendszerek elfogadottak lehetnek az Amerikai Egyesült Államokban, idegenek azonban az európai kultúrától. Különösen aggályos alkalmazásuk az egykori „szocialista blokkhoz" tartozó államokban, ezekben – így hazánkban – ugyanis sokakban visszatetszést, rossz emlékeket kelt a munkáltatók által átvett módszer.

Az adatvédelmi biztos egyik állásfoglalásában ismertette személyes véleményét, mely szerint a rendszer elsősorban a rosszindulatú vádaskodásoknak, mások „befeketítésének" enged teret, növeli a munkavállalók egzisztenciális kiszolgáltatottságát, és feleslegesen mérgezi a munkahelyi légkört azzal, hogy azt üzeni a munkavállalónak: a munkáltató elvárja a lojalitást, de nem bízik meg benne, és vigyázzon, mert minden kollégája potenciális besúgó. Mivel a biztos a módszert elítéli, annak alkalmazásáról nem folytatott személyes konzultációt a hozzá forduló adatkezelőkkel, csak általános tájékoztatást adott. *(271/K/2007, 295/K/2007, 652/K/2007, 653/K/2007)*

Végezetül, az állami munkaügyi adatkezelők oldaláról említést érdemel az a vizsgálat, melynek eredményeképpen a múlt évben kiadott, az álláshirdetésekkel, valamint a magán-munkaközvetítők tevékenységével kapcsolatos ajánlással összefüggésben fogalmazódtak meg további adatvédelmi elvárások.

Egy állampolgár beadvánnyal fordult az adatvédelmi biztoshoz és a Dél-alföldi Regionális Munkaügyi Központ Szegedi kirendeltségének az adatkezelését tartotta sérelmesnek. Beadványa szerint a kirendeltség állást közvetített ismeretlen biztosítótársaság részére, jeligével. A beadványozó önéletrajzát csak a kirendeltség képviselőjéhez juttathatja el, a kirendeltség vezetője pedig úgy tájékoztatta, hogy nem mondhatja meg, melyik biztosítótársaság kínálja az állást, figyelemmel arra, hogy a munkáltató anonimitást kért.

A munkaközvetítők tevékenységével kapcsolatos adatvédelmi biztosi ajánlás értelmében a munkát kereső személyt tájékoztatni kell arról, hogy pontosan mely munkáltató kínál munkát. Ennek alapján az adatvédelmi biztos arra kérte az Állami Foglalkoztatási Szolgálat főigazgatóját, hogy amennyiben a munkaügyi központok, illetőleg kirendeltségek működése nem az ajánlásban megfogalmazottak megfelelően történik, a kialakult gyakorlatot vizsgálják felül és a szükséges változtatásokat tegyék meg. *(2445/K/2007)*

Oktatásügy

Az adatkezelés fejlődésének, visszásságainak terén az oktatási intézmények sem számítanak kivételnek. Nyilvánosságra hozott adatok, ujjnyomatos beléptető rendszerek, jogosulatlan adatgyűjtés éppúgy

jellemző ezen a területen, mint az élet más szféráiban. A korábbiakhoz képest érdemi javulás nem történt.

Egy állampolgár azt kifogásolta, hogy egy felsőoktatási intézmény oktatója saját honlapján nyilvánosságra hozta a hallgatók eredményeit.

> A tanár azzal indokolta magatartását, hogy ezzel meg tudja előzni, hogy minden hallgató telefonon érdeklődjön, és így gyorsan és bárhonnan meg tudják ismerni eredményüket. Az oktató figyelmét a biztos felhívta arra, hogy személyes adatot csak célhoz kötötten lehet kezelni, valamint arra, hogy a hallgatók jegyeikről való tájékoztatására azok nyilvánosságra hozatala helyett alkalmas és helyes eljárás az egyetemi információs rendszer (Neptun, ETR stb.) használata, melynek során mindenki csak a saját érdemjegyét ismerheti meg anélkül, hogy erről a világháló felhasználói tábora is értesülne.
>
> A világháló sajátosságainál fogva az adatvédelem másik alapelve, az időszerűség követelménye sem alkalmazható, hiszen a nyilvánosságra hozatal fogalmi eleme, hogy az adat időbeli korlát nélkül bárki számára megismerhető. A biztos felszólította a tanárt arra, hogy törölje honlapjáról az adatokat, amit ő – némi vita után – meg is tett. *(1338/P/2007)*
>
> Hasonlóan jogellenesnek ítélte a biztos egy egyetemnek azt az eljárását, melyben az intézmény honlapján nyilvánosságra hozta az intézménybe felvett hallgatók nevét, és a felsőoktatási rendszerben használatos Neptun-kódját. A biztos felhívta az egyetem dékánját arra, hogy törölje a honlapról az adatokat, mely meg is történt. *(1558/P/2007)*

Szintén a nyilvánosság kérdését érintette egy középiskolai érettségi vizsgabizottság elnökének kérdése, hogy ki lehet-e nyilvánosan hirdetni az érettségi eredményeket, valamint közzé lehet-e tenni a neveket és az eredményeket az intézmény évkönyvében?

> Válaszul a biztos kifejtette, hogy a közoktatásról szóló 1993. évi LXXIX. törvény 2. számú melléklete 2. pontja lehetővé teszi a tanulók magatartás, szorgalom és tudás értékelésével kapcsolatos adatainak kezelését az érintett osztályon belül, a nevelőtestületen belül, a szülőnek, a vizsgabizottságnak, a gyakorlati képzés szervezőjének, a tanulószerződés kötőjének, illetve, ha az értékelés nem az iskolában történik, az iskolának, iskolaváltás esetén az új iskolának, a szakmai ellenőrzés végzőjének. A tanulmányi eredmények gimnáziumi évkönyvekben való nyilvánosságra hozatalát az adatvédelmi törvény alapján a biztos nem támogatja. *(217/K/2007)*

A korábbi évekhez hasonlóan sok problémát okoz a felsőoktatási kollégiumi férőhelyek elosztásához szükséges, szociális rászorultságot bizonyító iratok kezelésének kérdése. Egy szülő azt kérdezte, hogy jogszerű-e az, hogy gyermeke kollégiumi férőhelye pályázatához be kell nyújtani például alkalmazott testvére keresetének igazolását, elvált szülei válási papírjának másolatát, gyermektartásról szóló bírósági határozat másolatát stb.

Válaszában a biztos felhívta a figyelmet arra, hogy a felsőoktatásról szóló 2005. évi CXXXIX. törvény (továbbiakban: Ftv.) 2. számú melléklete rendelkezik a felsőoktatási intézményekben nyilvántartott és kezelt személyes és különleges adatokról. Eszerint nyilvántarthatóak a hallgatói jogviszonnyal kapcsolatban a hallgatói juttatások, kollégiumi elhelyezés adatai, a juttatásokra való jogosultság elbírálásához szükséges adatok (szociális helyzet, szülők adatai, tartásra vonatkozó adatok). Ugyanakkor az adatvédelmi törvény legfontosabb garanciája a célhoz kötött adatkezelés, melynek értelmében csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig. Ebben az esetben különös hangsúlyt kell fektetni az elengedhetetlenség fogalmára, hiszen a kért adatok e tekintetben jelentősen meghaladják az elfogadható mértéket és ezzel megsértik a hallgatók információs önrendelkezési jogát. *(800/P/2007)*

Egy felsőoktatásban dolgozó állampolgár panaszolta, hogy a Felsőoktatási Információs Rendszerbe való adatszolgáltatáshoz egyebek mellett nemzetiségét, Neptun-kódját és e-mail címét is meg kellett adnia. Felhívtuk a figyelmet arra, hogy a munkáltatónak ezen adatok kezelésére nincs felhatalmazása, így azokat adattovábbítás céljából nem kérheti és a panaszos nem köteles megadni. A többi adatot – azaz a természetes azonosítókat és az érintett tanulmányaira vonatkozókat – a FIR nyilvántarthatja. Arról is tájékoztattuk az érintettet, hogy a felsőoktatásról szóló törvény tervezetének véleményezésekor jeleztük az aggályokat a tervezetről, de azt a kormányzat nem vette figyelembe. *(1090/P/2007)*

A technika fejlődésével elburjánzott, és már az iskolákat is elérte a kamerás megfigyelés és a biometrikus beléptetőrendszerek használatának láza. Több intézményre vonatkozóan is érkezett panasz ebben a tárgykörben. Egy gimnáziumban bevezetni tervezett ujjnyomatos beléptető rendszer ügyében egy szülő, egy jogvédő szervezet és az iskola

igazgatója is kért állásfoglalást. A rendszer az ujjnyomat 5 pontjának távolságát rögzítené, és annak alapján alakítanák ki az azonosító rendszert. A rendszer az alkalmazottak és a diákok be- és kilépését egyaránt regisztrálná valamint a személy- és vagyonvédelmet (mindenki által hozzáférhető és használatos, nyilvános helyeken elhelyezett tárgyi eszközök) kívánja szolgálni.

> A biztos válaszában kifejtette, hogy a beléptető rendszerben kezelt személyes adatok körében az ujjlenyomat azonosító pontjai távolsága személyes adat, melynek kezelése a deklarált célok tekintetében nem elengedhetetlenül szükséges, ezért annak kezelése sérti a célhoz kötött adatkezelés követelményét. Az intézmény által megjelölt célok kevesebb és minőségében más személyes adatok alapján is megvalósíthatóak. A beléptető rendszerben való biometrikus azonosító alkalmazását ellenzi, mert súlyosan sérti a tanulók és az alkalmazottak személyes adatok védelméhez fűződő jogát.
>
> Személyes adatok kezelése csak olyan helyzetben indokolt, amelyben az elérni kívánt célok megvalósulása más, alternatív, személyes adatkezelést nem igénylő intézkedéssel, rendszerrel nem biztosítható. Az intézmény által elérni kívánt célok – többek között – a biometrikus azonosítást kiváltó, vonalkódos azonosítással vagy sorszámmal ellátott mágneses beléptető kártya alkalmazásával, vagy más módon is elérhetők, illetve intézményi szabályzatok kialakításával is biztosíthatóak. *(1251/K/2007, 1306/K/2007, 1380/K/2007)*

Több esetben szándékozott valaki a tanintézményben valamilyen szempont alapján listát készíteni a tanulókról. Ezek többnyire az adatvédelmi törvénnyel ellentétesek voltak.

Az indítványozó egy iskolában átmenetileg elvállalta a gyermek- és ifjúságvédelmi feladatot. Az osztályfőnökök segítségével szeretett volna összeállítani egy listát a hátrányos helyzetű és veszélyeztetett gyermekekről úgy, hogy az osztályfőnökök a tanuló és a szülők megkérdezése nélkül adják át neki az adatokat (jövedelmi, lakhatási, betegségre vonatkozó stb.). Célja a prevenciós célú beavatkozás lett volna. A tanárok azonban megtagadták ezt az együttműködést. Az indítványozó ekkor kért felvilágosítást ahhoz, hogy gyermek- és ifjúságvédelmi munkájában a megelőző tevékenységet hogyan lássa el, mivel megítélése szerint érdemi információk nélkül nem tudja e feladatát betölteni.

A biztos válaszában kifejtette, hogy a tanulóról az ő és szülője megkérdezése és hozzájárulása nélkül, „titkos" megfigyelés útján nem szabad adatot gyűjteni. A kérdéses adatcsoportokba elegendő adatot lehet „nyílt" eljárással is gyűjteni ahhoz, hogy a tanulók védelmének, segítésének ügyében az arra illetékes – jelen esetben a gyermekvédelmi felelős – el tudjon járni. A tanárral közölt, vagy tudomására jutott információk hivatásbeli titoknak minősülnek éppen úgy, ahogy az orvosi, vagy a gyónási titok. A tanárok ennek megfelelően helyesen döntöttek, amikor a kérést elutasították. Mindezek mellett az alkotmányos alapelvek tiltják az úgynevezett „készletező adatgyűjtést", mely meghatározott törvényes cél, és a céllal összefüggően meghatározott alanyi kör nélkül kíván természetes személyekről adatot gyűjteni.

Végül a biztos tájékoztatta az indítványozót arról, hogy megítélése szerint is a gyermekvédelmi felelős tevékenységében jelentős szerepet játszik a megelőzés is, melyhez szükséges az érintettekről információkat megismerni, azonban ezt a tevékenységet is csak a meghatározott törvényes keretek között szabad folytatni. *(743/K/2007)*

Nagy jelentőségű volt az Ftv. módosításának tervezete, mely új adatbázisokat kívánt létrehozni a felsőoktatási információs rendszer kiépítésével. A tervezetben nemhogy az adatminimalizálás követelménye nem fedezhető fel, hanem a készletező adatgyűjtés kiépülése figyelhető meg, mely az Alkotmánybíróság állandó gyakorlata szerint a személyes adatok védelméhez fűződő jog indokolatlan és aránytalan – összességében alkotmányellenes – korlátozását jelenti. Az Alkotmánybíróság több állásfoglalása szerint alkotmányellenes ugyanazon adatokról több, párhuzamos nyilvántartást vezetni.

Az Ftv. korábban hatályos szabályozása szerint a regisztrációs központ a felsőoktatási intézmények nyilvántartására szolgál. Ebből a célból az adatvédelmi törvényben előírt célhoz kötöttségi követelménnyel – mint alkotmányos garanciával – ellentétes az, hogy e rendszerben is személyes adatokat kezeljenek. Szomorú, hogy a javaslatot az Országgyűlés lényeges változtatás nélkül fogadta el. *(628/J/2007)*

Távközlési szervezetek

A hírközlési szektor adatvédelmét az elmúlt évben leginkább az elektronikus hírközlési szolgáltatások nyújtása keretében feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló

2006/64/EK irányelv hazai jogba való átültetése befolyásolta. Több tervezet érkezett hozzánk a közigazgatási egyeztetés folyamán, ezekhez számos észrevételt tettünk a magánélet tiszteletben tartásához, a közlés bizalmasságához, és a személyes adatok védelméhez való jogra tekintettel. Kifejtettük, hogy a forgalmi adatok ilyen tömeges méretű megőrzése csak akkor felel meg az Emberi Jogi Bíróság által kimunkált és az emberi jogok korlátozására vonatkozó alapelveknek, ha az alapjogi korlátozás a demokratikus jogállamban szükséges, megfelelő és arányos a közrend fenntartása, a nemzetbiztonság, a közbiztonság védelme érdekében, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használata megelőzésének, kivizsgálásának, felderítésének és üldözésének biztosítása érdekében. A terrorizmus és a szervezett bűnözés elleni küzdelem jegyében sem fogadható el bármilyen intézkedés.

Az elektronikus hírközlésről szóló 2003. évi C. törvény (továbbiakban: Eht.) adatvédelmi rendelkezései között jelentős az a módosítás, amely a 2007. január 1-je után kötött szerződésekre volt kihatással. Az új szabály szerint ugyanis az előfizetői szerződésnek természetes személy előfizető esetében már nem kötelező tartalmi kelléke az előfizető lánykori neve, anyja neve, a születési helyére és idejére vonatkozó adat. Ezen adatok rögzítésére január 1-jét követően csak a leendő előfizető hozzájárulásával kerülhet sor. Az ügyfél ezen hozzájárulását az adatkezelővel kötött írásbeli szerződés keretében is megadhatja. *(437/P/2007, 1487/P/2007)*

> A biztos a hírközlési szolgáltató konzultációs megkeresésére arra az álláspontra helyezkedett, hogy az előfizető leánykori nevére, anyja nevére, születési helyére és idejére vonatkozó adatok csak az adatvédelmi törvény 3. § (1) bekezdésének a) pontjára alapítva válhatnak a szerződés részévé. A hírközlési szolgáltató a bírósági végrehajtásról szóló 1994. évi LIII. törvény 11. § (2) bekezdésére hivatkozással (a végrehajtási lap kiállításához szükséges adatkör) nem jogosult kezelni az adatokat. Ennek oka, hogy a törvénynek ez a szakasza nem adatkezelést elrendelő törvényi rendelkezés, mert nem felel meg a kötelező adatkezelést elrendelő törvényre vonatkozó törvényes elvárásoknak (Avtv. 1. § (2) és (3), 3. § (3) bek.). Ezentúl a végrehajtási eljárásra hivatkozással a végrehajtási lap kiállításához szükséges adatok szolgáltatására kötelezni az előfizetőt, egy előre nem látott, jövőben bizonytalan eseményre, úgynevezett készletező adatgyűjtést eredményez,

mert nem minden előfizetővel szemben indul meg a bírósági, illetve végrehajtási eljárás. *(270/K/2007)*

Évről évre visszatérő problémát jelentenek a hírközlési szolgáltatókhoz érkező nyomozó hatósági, rendőrségi megkeresések. Az Eht. 157. § (6) bekezdésének c) pontja, valamint a Be. 71. §-a alapján a megkeresett szerv köteles a hatósági megkeresésnek eleget tenni és a kért adatokat szolgáltatni. A nyomozóhatóság adatigénylésének a célhoz kötöttség szab határt, a hírközlési szolgáltató adatszolgáltatásának pedig az Eht. hivatkozott rendelkezése, mert csak az ott meghatározott esetekben továbbíthat adatokat. De ugyanilyen problémát okoz az adósságbehajtó, követeléskezelő cégek felé történő adattovábbítás is, amelyről az Eht. 157. § (6) bekezdésének a) pontja rendelkezik.

A hírközlési szolgáltató tehát az Eht. 157. § (6) bekezdésének c) pontja, a (8) bekezdése alapján az előfizetői jogviszonyra tekintet nélkül köteles az ügyfeléhez tartozó előfizetői számra érkezett valamennyi hívószámot kezelni, megőrizni és a Be. 71. §-a alapján a hatóságnak átadni. Az Eht. 157. § (2) bekezdésének e) pontja hívó és hívott előfizetői számok kezeléséről szól, ezért nem osztotta a biztos a szolgáltató nézetét, amely szerint csak azokat a beérkező hívószámokat tárolhatja és kezelheti, amelyek az előfizetőihez tartoznak. A törvény szövegéből nem következik efféle különbségtétel a forgalmi és a számlázási adatok között. *(369/K/2007)*

Az Eht. fenti rendelkezése alapján az adott telefonszámhoz tartozó előfizetői adatok a bíróságnak is átadhatók, azonban a bíróság csak akkor minősülhet a törvényhely szerint adatkezelőnek, ha az adatátadás büntetőeljárás lefolytatásához szükséges, azaz valamely bűncselekmény elkövetésének alapos gyanúja miatt a büntetőeljárás folyamatban van. A veszélyes fenyegetés szabálysértése miatt, a szabálysértésekről szóló 1999. évi LXIX. törvény szerint az elsőfokon eljáró bíróság nem jogosult adatigénylésre. Az elektronikus hírközlési szolgáltató köteles a közvádas bűncselekmény elkövetésének gyanúja miatt eljáró hatóságnak, bíróságnak átadni az előfizető adatait. Adatvédelmi okokra hivatkozva nem tagadhatja meg az adatszolgáltatást, szabálysértési eljárásban azonban igen. *(1762/P/2007)*

Több beadványozó kifogásolta, hogy a hírközlési szolgáltató az előfizetői adatokat és adósságbehajtással foglakozó cégnek továbbította. Az Eht. 157. § (6) bekezdésének a) pontja felhatalmazza az elektronikus hírközlési szolgáltatót arra, hogy a megbízásából követelést

kezelését végző cégeknek átadja azokat az adatokat, amelyek az adatkezelés céljához szükségesek. Amennyiben a telefonszolgáltató által engedményezéssel átadott személyes adatokat a követeléskezelő cég (engedményes) a díjtartozás behajtása érdekében használja fel, adatkezelése nem ütközik az adatvédelmi törvény rendelkezéseibe. Emellett a Polgári Törvénykönyv (továbbiakban: Ptk.) engedményezésre vonatkozó szabályai is lehetővé teszik a természetes személy adósok adatainak átadását. A követelések engedményezés útján történő átruházása esetén az adatátadásához szükséges jogcímet ugyanis maga a Ptk. teremti meg, így a követelésekhez kapcsolódó személyes adatok továbbítása adatvédelmi szempontból nem kifogásolható. *(599/P/2007, 601/P/2007, 698/P/2007, 1755/P/2007)*

A tudakozó szolgáltatással volt kapcsolatos az a hírközlési szolgáltatótól érkezett konzultációs beadvány, amely arra a kérdésre várt választ, hogy az EU területén működő, nemzetközi tudakozói szolgáltatást nyújtó cégnek a szolgáltatási területének bővítéséhez továbbítható-e a tudakozói adatbázis. A kialakított állásfoglalás szerint nem sérti az előfizető személyes adatok védelméhez fűződő jogát, ha külön hozzájárulása nélkül, de előzetes tájékoztatás alapján, az Európai Unió bármely tagállamába tudakozó szolgáltatás nyújtása céljából továbbítja a szolgáltató előfizetői adatait.

A tudakozó szolgáltatás nyújtása lehetséges országosan vagy meghatározott területen. Az országos tudakozó szolgáltatás működtetése céljából a törvény értelmében kötelesek a szolgáltatók az előfizetői adatokat átadni. Az adattovábbítás jogalapja – az országos tudakozóba – az Eht. 146. §. Az Európai Unión belüli adattovábbítás lehetőségéről az Eht. nem szól, azonban az adatvédelmi törvény 9. § (2) bekezdése szerint az Európai Unió tagállamaiba irányuló adattovábbítást úgy kell tekinteni, mintha a Magyar Köztársaság területén belüli adattovábbításra kerülne sor. A tudakozó szolgáltatás területi korlátainak feloldása – országos kereteken túl – összhangban van az Európai Unió létrejöttének egyik célkitűzésével, amely szerint az unióban meg kell valósulnia, hogy a szolgáltatások határok nélkül bárhol igénybe vehetők és nyújthatók legyenek. Az adatvédelmi törvény 3. § (1) bekezdése, valamint az adatvédelmi törvény 8. § (1) bekezdése értelmében az érintett hozzájárulását adta a tudakozó szolgáltatásban való részvételhez és a hozzájárulása az országos belföldi tudakozóban való részvételre terjedt ki.

Tekintettel arra, hogy a nemzetközi társaság a T-com szolgáltatóval azonos célból hasznosítaná az adatbázist, tehát adatkezelése nem minősülne az eredeti céltól eltérő felhasználásnak, az adattovábbítás nem sérti az előfizetők személyes adatok védeleméhez fűződő jogait.

A kérdéssel kapcsolatban ki kell emelni az adatvédelmi törvény 7. §-ban rögzített szabályt, amely az adatok minőségére vonatkozó előírásokat fogalmaz meg az adatkezelők számára. E jogszabályhely értelmében a kezelt személyes adatoknak pontosnak, teljesnek, és ha szükséges időszerűnek kell lenniük. A törvényben megfogalmazott elvárások teljesülésére különösen figyelmet kell fordítani akkor, mikor az érintett személyes adataiban nagy gyakorisággal következik be változás, vagy az érintett rendelkezése folytán módosul az adatkezeléshez adott felhatalmazás pl. az előfizető elérhetőségének adatait titkosítja. A jelenlegi konstrukcióban az előfizető szerződéses kapcsolatban magyar hírközlési szolgáltatóval áll, az esetleges adatkezeléssel kapcsolatos rendelkezési jogát vele szemben érvényesíti. Az adatátadás révén egy új, az érintett számára ismeretlen adatkezelő is a teljes adatbázis birtokába jut, az érintett információs önrendelkezési jogának gyakorolhatósága a szolgáltató további közreműködése nélkül nem biztosított és nem garantált az adatok pontossága sem. A magyar hírközlési szolgáltatónak gondoskodnia kell arról, hogy az érintettek igényeiről (adataik törlése, módosítása, számuk titkosítása) a külföldi társaság is értesüljön. *(890/K/2007)*

Az elmúlt évben két panasz érkezett a hírközlési szolgáltató telefonos ügyfélszolgálatán rögzített hangfelvétellel kapcsolatosan. Az állásfoglalás leszögezte, hogy a szolgáltató a rögzített telefonhívásról köteles tájékoztatást adni, és a hangfelvételek visszahallgathatóságát biztosítani. A törvény a tájékoztatásra formai követelményeket nem határoz meg, így a tájékoztatási kötelezettségének akkor is eleget tesz a szolgáltató, ha a hangfelvételről szó szerinti, hiteles jegyzőkönyvet készít, és azt bocsátja az ügyfél rendelkezésére. *(1175/P/2007, 358/P2007)*

Egy állampolgár arra a kérdésre várt választ, hogy a szöveges üzenetek elküldése során alkalmazott kézbesítés-jelentés mennyiben felel meg az adatvédelem előírásainak. Az állásfoglalás szerint nem aggályos a szöveges üzenetek elküldéséről szóló kézbesítés-jelentés.

A biztos az állásfoglalásban elmondta, hogy az is hordozhat személyes jellegű többletinformációt az előfizetőre nézve, hogy az adott SIM kártyához tartozó előfizetői hívószám a mobilszolgáltató hálózatában

elérhető vagy üzembe állt, ahogy az is, hogy elérhető, de nem válaszol a hívásra, vagy akár a hálózat elégtelensége miatt nem válaszol („nincs térerő"). De álláspontja szerint köztudomású tény, hogy az elektronikus hírközlési szolgáltatás igénybevétele során a fent említett, személyes tartalmat is hordozó többletinformációk keletkeznek a hívó fél számára. Különösen igaz ez a mobiltelefonok használatára, ahol a szolgáltatás igénybevételére kifejezetten a készülék (előfizetői hívószám) egyetlen személyhez való kötődése miatt kerül sor, és ahol a nyújtott szolgáltatás műszaki, technológiai jellemzői elengedhetetlenné teszik ezeknek az adatoknak a keletkezését és feldolgozását. Ezért a hívott előfizető akaratából kerül sor ezeknek a hívásforgalmi információknak a továbbítására, tehát a mobiltelefon szolgáltatás használatával az előfizetők hozzájárulnak ahhoz, hogy a hírközlési szolgáltatás teljesítése során keletkező információkat (elérhető/nem elérhető/nem válaszol) a hívó fél megismerje. A szöveges, multimédia üzenetek vonatkozásában ugyanez az elv irányadó.

Továbbá a kérdés megválaszolásához az adatvédelmi szabályokon túl az elektronikus hírközlési szolgáltatás nyújtására irányadó mögöttes polgári jogi szabályokat is vizsgálni kell. A szolgáltatás teljesítésére vonatkozó polgári jogi szabályok szerint van jelentősége annak, hogy a hírközlési szolgáltató a hívást sikeresen továbbította, vagy a szöveges üzenet kézbesítését sikeresen teljesítette-e. A postai szolgáltatások körében hasonlóképp működik a könyvelt (ajánlott) küldemények vagy a tértivevényes küldemények kézbesítése, amellyel elsősorban a hivatalos iratok kézbesítésekor találkozunk. Tehát a közlés kézbesítéséhez (akár postai úton, akár elektronikus levélben, akár hírközlési szolgáltatás keretében) jogkövetkezmények fűződhetnek, ezért a feladó a hírközlési szolgáltatótól a polgári jogi szabályok alapján elvárhatja, hogy a szerződésszerű teljesítéséről igazolást adjon. *(1790/P/2007)*

Egy állampolgár a Pannon POP3 szolgáltatáshoz kapcsolódó adatkezelést kifogásolta. A kérdéses szolgáltatáson keresztül történő levélküldésnél ugyanis a levél tartalmában minden esetben feltüntetésre kerül az e-mail cím mellett a küldő telefonszáma is. Megállapítottuk, hogy a szolgáltatás nem sérti a felhasználó személyes adatok védelméhez való jogát.

Az ügyben a biztos megállapította, hogy a szolgáltató az adatvédelmi törvény 6. § (2) bekezdése alapján az adatkezelés körülményeiről egyértelmű és részletes tájékoztatást ad a szolgáltatás igénybevételét

megelőzően. Ennek következtében az adatkezelés jogalapja az érintett tájékozott, előzetes és határozott hozzájárulása, amelyet a szolgáltatás igénybevételével fejez ki. A hozzájárulás teljes mértékben önkéntes és kényszertől mentes, hiszen a levélküldésre más lehetősége is van a felhasználónak, és ezek egyike sem jár az előfizetői hívószám továbbításával. Az adatkezelés épp a személyes adatokkal való visszaélés elkerülését szolgálja, mert a szolgáltatás a jelenlegi formájában a protokoll sajátossága miatt lehetőséget nyújt arra, hogy a feladó a küldendő levél feladó mezőjét tetszőlegesen megválassza, abban bármilyen nevet, értéket, kifejezést feltüntetessen, majd ez a címzettnél feladóként jelenjen meg. Az adatkezelés célja tehát nem kifogásolható. *(428/P/2007)*

További jellemző ügycsoportot alkotnak a hírközlési szolgáltatók direkt marketing tevékenységével összefüggő adatkezelési anomáliák. Ezek nagy száma arra utal, hogy a világos jogszabályi háttér ellenére még mindig előfordul jogellenes adatkezelés. Ebben a témakörben említésre érdemes, hogy kezdeményezésünk alapján módosult az Eht.-nek az adatok közvetlen üzletszerzési vagy tájékoztatási célra való felhasználásáról szóló 162. §-a. A módosítás a piackutatás és közvélemény-kutatás célját szolgáló híváskezdeményezések szabályával bővítette a meglévő jogszabályi rendelkezéseket.

A reklám tartalmú hívások és küldemények elkerülése érdekében a biztos arról tájékoztatta a beadványozót, hogy az Eht. 160. §-ának (4) bekezdése alapján kérheti, hogy ne szerepeljen az előfizetői névjegyzékben, vagy, hogy lakcímét csak részben tüntessék fel a telefonkönyvben, vagy kérheti azt is, hogy a telefonkönyvben tüntessék fel, hogy személyes adatai nem használhatók fel közvetlen üzletszerzésre, direkt marketing megkeresésre. Tekintettel arra, hogy a nyilvános telefonkönyv adataihoz bárki hozzáfér, előfordulhat, hogy valamilyen szerv a telefonkönyvben, illetve a szolgáltató egyéb előfizetői névjegyzékében szereplő személyes adatokat (név, lakcím) használ fel arra, hogy az előfizetőknek reklám célú megkeresést küldjön. Ez abban az esetben jogszerű, ha csak olyan személyeknek küld megkeresést, akik adataiknak ilyen célú felhasználást nem tiltották meg. Ha az előfizető szeretné elkerülni az ilyen marketing üzenetek vagy küldemények érkezését, illetve szeretné, ha személyes adatai nem szerepelnének a telefonkönyvben, és azokat a tudakozóban se adják ki, akkor a szolgáltatónál kell jeleznie ezt. A szolgáltató külön költség nélkül köteles biztosítani az adatok névjegyzékből való törlését, illetve adatok mellett a megfelelő jelzés elhelyezését. *(1327/P/2007, 1820/P/2007)*

Internet

Az elmúlt évben az előző évekhez képest az internetet érintő beadványok számának növekedési üteme megállt, ami talán annak is köszönhető, hogy mind a felhasználók, mind a szolgáltatók, üzemeltetők egyre inkább odafigyelnek az internet-használat jogi kereteinek megtartására. Ennek némileg sajnos ellentmond, hogy egy felhasználási területen változatlanul nem mutatható ki javulás: továbbra is kiugró számban érkeznek a kéretlen elektronikus leveleket érintő panaszok.

Több mint 70 olyan beadvány érkezett, melyben azt sérelmezték, hogy egyes – nehezen beazonosítható – személyek több százezer, magánszemélyekhez tartozó e-mail címet tartalmazó adatbázist kívántak áruba bocsátani, spam útján.

> Az adatállományok „forgalomba hozatala" nem ismeretlen jelenség hazánkban sem, azonban különös súllyal esik latba az a körülmény, hogy ez a kereskedelem részben személyes adatok átadására és átvételére irányul. Az érintettek magánélethez és személyes adatok védelméhez való joga megköveteli az információs társadalom szereplőitől, hogy szükségtelenül és jogellenesen ne zavarják az egyének magánéletét. Az elektronikus hirdetőknek tisztában kell lenniük a vonatkozó törvényi rendelkezésekkel. Az adatvédelmi törvény szerint az elektronikus levélcímek gyűjtése is az érintettek hozzájárulásához kötött, de még a jogszerűen gyűjtött és kezelt elektronikus e-mail címek is csak az érintett beleegyezésével továbbíthatók marketing célú felhasználásra harmadik személyek, szervek felé. Ezenkívül az adattovábbítás lehetőségének üzletszerű felkínálása gazdasági reklámtevékenységnek, valamint elektronikus hirdetésnek is minősül, így a reklámtörvény és az elektronikus kereskedelmi törvény előírásait is megszegi, aki ilyen jellegű tevékenységet folytat. Az üzleti ajánlat tehát sértheti mindazon személyek személyes adatok védelméhez fűződő jogát, akik a kérdéses ajánlatot kéretlenül megkapták, illetve azokét is, akiknek személyes adata az adatállományban hozzájárulásuk nélkül szerepel, és az adásvételnek köszönhetően később kéretlen ajánlatok célpontjaivá válnak maguk is. A fentiek értelmében nem csupán annak az adatkezelőnek a tevékenysége jogellenes, aki a törvényi előírások megszegésével e-mail címeket gyűjt, adatállományba rendez, majd értékesít, hanem azé is, aki az adatállomány megvásárlásával maga is jogellenesen használja fel az adatokat.
>
> Az erről szóló közlemény az adatvédelmi biztos honlapján olvasható.

Dinamikusan növekvő területet jelent az internetes közösségi oldalak működése. Egyre több ilyen portál jelenik meg a világhálón, és egyre több ember regisztrál ezeken az oldalakon. Mivel a kapcsolatépítő weboldalak fő sajátossága, hogy a felhasználók széles körben megismerhetővé teszik személyes – egyes esetekben különleges – adataikat, ezért a személyes adatok védelme szempontjából is pontosan és részletesen kell az üzemeltetőknek szabályozniuk a felhasználási feltételeket. Az ilyen jellegű portálokkal összefüggő beadványok nagy száma azt mutatja, hogy mind felhasználói, mind üzemeltetői oldalon jobban el kell mélyülni az adatvédelmi szabályok ismeretében.

Egy állampolgár bejelentéssel fordult az adatvédelmi biztoshoz, melyben azt kifogásolta, hogy az iWiW elektronikus levelezőrendszere azt követően is megőrzi az üzenetek teljes szövegét, hogy az üzenetet mind a feladó, mind a címzett törölte a postafiókjából. Az elektronikus levél az URL címe alapján továbbra is hozzáférhető. A szolgáltató tájékoztatása szerint a rendszer a törlési igény beérkezésétől számított 5 munkanapon belül törli a leveleket, abban az esetben, amennyiben a levelet a feladó illetve az összes címzett törölte postaládájából. Normális üzemmenet során, amíg valamelyik fél nem törölte a levelet, addig a levél a hozzá tartozó URL-en keresztül továbbra is elérhető, mivel a rendszer minden levélből fizikailag csak egy példányt tárol. Azonban ezen időszak alatt is csak a küldő és a címzett(ek) férhetnek hozzá, másnak ehhez nincs jogosultsága. Feltehetően az automatizmust irányító folyamat, amely a logikailag törölt levelek fizikai törlését végezte, meghibásodott, ezért fordulhatott elő, hogy a határidő eltelte után is elérhetőek voltak bizonyos levelek. *(526/P/2007)*

Több beadványozó is sérelmezte, hogy a közösségi oldalakon visszaéltek személyes adataikkal, adatlapjukat jogellenesen megváltoztatták, illetve személyükre vonatkozó profilt illetéktelenül hoztak létre.

Egy állampolgár azt kifogásolta, hogy az iWiW portálon illetéktelen személy felhelyezte gyermekének fényképét. Az adatvédelmi törvény szerint az érintettnek van joga rendelkezni személyes adatai felett. Ez az információs önrendelkezési jog csak kivételesen és törvényben korlátozható. A főszabály tehát az, hogy az érintettre vonatkozó személyes adat csak az érintett hozzájárulásával kezelhető, ha törvény eltérően nem rendelkezik. A házasságról, a családról és a gyámságról szóló 1952. évi IV. törvény szülői felügyeletre, törvényes képviseletre vonatkozó szabályai alapján a kiskorú gyermek helyett a személyes

adatok védelméhez fűződő alkotmányos jogot a szülők gyakorolják, amennyiben ítélőképességgel még nem rendelkezik, és véleménynyilvánításra még képtelen. Mivel a gyermek képmása személyes adat és adatai kezeléséhez nem tud hozzájárulni, ezért a szülői felügyeletet ellátó szülők tudta és beleegyezése nélkül az egyéves kiskorú gyermek fényképének közzététele sérti a gyermek személyes adatok védelméhez fűződő jogát.

A panaszos szerint az oldal üzemeltetőjének kellene meggyőződnie arról, hogy ténylegesen ki a hozzátartozó. Az iWiW közösségi hálózatba regisztrálás során az érintett a közösséghez való tartozási szándékát kétszeresen erősíti meg, és az adatkezeléshez adott hozzájárulását a regisztrációs eljárásban önként adja. Az elektronikus úton történő regisztráció létrehozásánál, az űrlapok elektronikus kitöltésénél nincsen lehetőség arra, hogy a szolgáltató teljes bizonyossággal meggyőződjék arról, hogy az adatok hitelesek-e, és az adatkezeléshez adott hozzájárulást az érintett (vagy a nyilatkozat tételére jogosult) személy teszi-e. A kétlépcsős regisztrációs eljárás a virtuális térben a visszaélések számát csökkenti, de értelemszerűen nem zárhatja ki. Az elmondottak alapján az adatvédelmi biztos álláspontja szerint a regisztrációs eljárás és az adatfelvétel nem ütközik az adatvédelmi törvény rendelkezéseibe. *(526/P/2007, 536/P/2007, 745/P/2007)*

Több ügy kapcsán vizsgáltuk azt is, hogy az iWiW oldal szolgáltatója bizonyos esetekben kéri az érintett személyes azonosításra alkalmas igazolványát. Annak érdekében, hogy elkerülje a jelszavak illetéktelen megszerzését, az adatlapok jogellenes megváltoztatását és törlését, az üzemeltető a felhasználási feltételekben rögzíti, hogy az adatkezelő a felhasználó kérésére történő adatmódosítás, az e-mail cím megváltoztatása, profil törlése esetén azonosítás céljából jogosult a felhasználótól személyes azonosításra alkalmas igazolványt, illetve e-mail címet kérni. E szerződéses rendelkezés az információs önrendelkezési jogra tekintettel biztosítja, hogy kizárólag az érintett eszközölje a változtatásokat személyes adatain.

Az okiratok bemutatása a biztos álláspontja szerint nem ütközik az adatvédelmi törvény rendelkezéseibe, mindazonáltal az adatbiztonság oldaláról aggályos az okiratok másolatban történő elküldése. Ugyanis az egyén személyes jelenléte elengedhetetlen a hatósági igazolvány alapján történő személyazonosításhoz, mert az igazolvány birtokosa azt tanúsítja, hogy az abban szereplő adatok az ő személyes adatai.

Ezért a személyazonosító igazolványnak, valamint a többi hatósági igazolvány másolatának elektronikus, postai úton vagy akár telefaxon történő továbbítása nem minősül személyazonosításnak. Továbbá az is elmondható, hogy a hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági okmánynak, továbbá a fent elmondottak szerint nem alkalmas a személyazonosság megállapítására sem – még akkor sem, ha több adat összevetésére nyílik lehetőség. *(138/P/2007, 947/P/2007, 1178/P/2007, 1747/P/2007)*

A fenti üggyel hasonlóságot mutat a másik nagy közösségépítő portál, a „myVIP" hitelesítés elnevezésű szolgáltatása, amelynek során azonosító dokumentumok másolatainak kezelése történik.

Egy panaszos kifogásolta, hogy az oldalon kérik egy igazolvány „másolatát". A szolgáltatás lényege, hogy miután az érintett feltöltötte személyi igazolványa, diákigazolványa, jogosítványa, vagy útlevele fényképes oldalának másolatát, és elküldött egy emeltdíjas SMS-t, regisztrációja mellé kerül egy „hitelesítési pecsét", amely valószínűsíti, hogy a hitelesített felhasználó valódi, nem fiktív. Az eljárásról az oldalon részletes tájékoztatás olvasható, melynek alapján az adatvédelmi biztos megállapította, hogy az adatkezelés teljesen önkéntes, a hitelesítés elmaradása semmilyen következménnyel nem jár. Az érintett emellett bármikor kérheti az adatok, illetve a megadott fénykép törlését.

A tájékoztató szerint a hitelesítés célja a „fiktív felhasználók kiszűrése", mivel a hitelesítés „valószínűsíti", hogy a regisztrált felhasználó létező személy. Kétségtelen, hogy a hitelesítés nem csalhatatlan módszer a fiktív felhasználók kiszűrésére, mégis nagyobb bizonyosságot nyújthat a személyazonosságot illetően, amely az ilyen jellegű honlapok esetében – különös tekintettel a sorozatos visszaélésekre, mások nevében történő regisztrációra – lényeges lehet. Az okiratok másolata ugyanakkor adatbiztonsági kérdéseket is felvet: az adatkezelőnek fokozottan kell ügyelnie az adatok biztonságos tárolására, a hozzáférés elleni védelemre. Erre a kötelezettségre a biztos honlap üzemeltetőjének figyelmét felhívta. *(654/P/2007)*

Egyes beadványozók azt sérelmezték, hogy személyükre vonatkozó sértő, obszcén kijelentéseket, utalásokat, fényképeket jelentettek meg bizonyos adatlapokon. Mivel az ilyen tevékenység jogellenes adatkezelésnek minősül, az iWiW kft., adatvédelmi szabályzata alapján, fenntart-

ja magának a jogot, hogy minden további értesítés nélkül törölje azon felhasználókat, akik bármely más személy nevével, képmásával, e-mail címével vagy más személyes információjával visszaélnek, törölje vagy korlátozza azokat a felhasználókat, akik más egyéneket zaklattak akár üzenettáblákon, magánüzenetek formájában, listák útján vagy bármely más módon. Továbbá az iWiW kft. minden értesítés nélkül eltávolítja az olyan anyagokat, amelyeket a kizárólagos döntési jogkörében jogellenesnek, más személyiségi jogába ütköző, tisztességtelennek, fenyegetőnek, becsületsértőnek, rágalmazónak, obszcénnek vagy egyébként kifogásolhatónak talál. Ezenfelül is megilleti az adatalanyt, hogy adatai jogellenes kezelése miatt bírósághoz forduljon, valamint jelentős érdeksérelem esetén büntetőfeljelentést is tehet. *(565/P/2007, 854/P/2007)*

Egy másik, új indítású közösségi oldallal kapcsolatban szintén felmerültek adatvédelmi problémák. A KlubD elnevezésű portálon csak azok regisztrálhatnak, akik felsőfokú oklevéllel rendelkeznek. Ezért a jelentkező a regisztráció során köteles megadni a diplomájának számát, amit az üzemeltető ellenőrizni kíván oly módon, hogy a név és az oklevél számának megküldése után a felsőoktatási intézménytől kéri a diploma valódiságának visszaigazolását. Bár az ügyben a vizsgálat a tavalyi évben kezdődött, a probléma megnyugtatóan még nem rendeződött, amit több panasz is alátámaszt.

> Bár az oldal üzemeltetői az ellenkezőjét állítják, a diploma száma olyan adat (azonosító jel), amely egy konkrét természetes személlyel kapcsolatba hozható, a természetes személyre vonatkozóan információt hordoz, így személyes adatnak minősül. Az adatvédelmi törvény szerint mind az adatkezeléshez, mind az adattovábbításhoz, mind a különböző adatkezelések, adatbázisok összekapcsolásához az érintett hozzájárulása szükséges. A rendelkezés független attól, hogy az összekapcsolandó adatbázisokban különböző, vagy egymást fedő személyes adatokról van-e szó, valamint attól is, hogy az adatok összekapcsolásával új információk átadására is sor kerül-e. Adatkezelésnek minősül ugyanis minden személyes adattal végzett művelet, függetlenül attól, hogy konkrét adatátvitelről, vagy csak az adatoknak odavissza történő összekapcsolásáról van-e szó. Így alkalmazni kell az adatvédelmi törvény rendelkezéseit az olyan adatszolgáltatásra is, amikor valamely adatbázis kezelője a másik adatkezelőnél lévő adatok valódiságát, igen-nem válasszal igazolja vissza. A felsőoktatási törvény rendelkezik arról, hogy a felsőoktatási intézmény mely szemé-

lyes adatokat, milyen céllal kezelhet, illetve arról is, hogy mely szerveknek, milyen céllal továbbítható a nyilvántartásból személyes adat. A törvényben meghatározott adatkezelésen kívül a felsőoktatási intézmény csak az érintett hozzájárulásával kezelhet, továbbíthat adatot. Ezért ahhoz, hogy a szolgáltató az érintett diplomaszámát, azonosító adatait a felsőoktatási intézménynek továbbíthassa, valamint ahhoz is, hogy a felsőoktatási intézmény a nála kezelt személyes adatokat kiszolgáltassa, az érintett hozzájárulása szükséges. Az érintett adatkezeléshez történő hozzájárulását az adatkezelőnek, tehát a szolgáltatónak, illetve az oktatási intézménynek kell igazolnia. Vagyis a felsőoktatási intézmény csak abban az esetben adhatja ki a kért adatokat, ha minden kétséget kizáróan meg tud győződni a hozzájárulás meglétéről. Ennek érdekében az a legcélszerűbb, ha a szolgáltató rendelkezik az érintett írásos beleegyezésével.

Arra még nem érkezett válasz – és ezért a vizsgálat 2008-ban folytatódik –, hogy a gyakorlatban eredményes-e az adatbázisok összekapcsolása, valamint azzal összefüggésben sem kapott a biztos tájékoztatást, hogy milyen következménnyel jár a felhasználóra nézve, ha a külső adatforrás nem erősíti meg a diploma adatainak hitelességét. *(1589/K/2006, 1412/P/2007, 1421/P/2007)*

Érdemes megjegyezni, hogy kezdeményeztük a kapcsolatépítő oldal személyes adatok védelmével kapcsolatos szabályzatának és a felhasználási feltételeknek a módosítását, hogy azok minden részletükben megfeleljenek a hatályos adatvédelmi szabályoknak.

Az elmúlt évben újra érkezett néhány panasz, illetve konzultációs beadvány, melynek az úgynevezett „internetes szégyenfal" volt a tárgya. Ezek olyan internetes oldalak, ahova az oldalak készítői azoknak az adatait teszik fel, akik valamilyen formában megsértették a mindennapi élet egyes területeinek írott, vagy íratlan szabályait.

Egy beadványozó arra tett javaslatot, hogy létre kellene hozni egy internetes adatbázist, mely a magyar állampolgárok folyamatban lévő vagy lezárt hatósági eljárásainak listáját tartalmazza. Egy ilyen adatbázis rengeteg olyan adatot foglalna magában, melyek személyes adatnak, bizonyos esetekben pedig különleges adatnak minősülnek. Ahhoz, hogy egy személy személyes adataival együtt felkerüljön egy ilyen listára, szükség lenne az érintett hozzájárulására, vagy a törvény felhatalmazására. Az internetes portál természetéből kiindulva egyértelműen megállapítható, hogy az adatkezeléshez az érintett hoz-

zájárulása hiányozna. Feltehető az is, hogy e személyeknek tudomásuk sem lenne arról, hogy nevük felkerül egy ilyen listára. Továbbá nincsen olyan törvényi rendelkezés, mely feljogosítana egy ilyen oldal készítőit az érintettek személyes adatainak nyilvánosságra hozatalára, hiszen sem a polgári perrendtartásról szóló 1952. évi III. törvény, sem a Be. nem tartalmaz erre vonatkozó rendelkezést. Az elmondottakból következik, hogy nincs jogszerű lehetősége annak, hogy akár egy internetes portálon, akár más formában nyilvánosságra hozzák azon állampolgárok személyes adatait, akiknek valamilyen „hatósági ügyük" volt, vagy van folyamatban. Ugyanis az ilyen célú adatkezelés súlyosan sértené az érintettek személyes adatok védelméhez fűződő jogát, valamint a Ptk. szerint az érintettek jóhírnevének sérelmével is járhat, jelentős érdeksérelem esetén pedig Btk. 177/A. §-ában meghatározott jogkövetkezmények is alkalmazhatók. *(1935/K/2007)*

Az internettel kapcsolatban az egyik nehézséget mindig az jelentette, hogy a személyes adatok nyilvánosságra hozatala sokszor ellenőrizhetetlen módon történik. Egy panasz olyan honlapra irányult, ahol „magyar amatőrök" címmel található egy fénykép- és videó gyűjtemény. A honlapon található tájékoztatás szerint az anyagokat amatőr fotósok, videósok készítik és küldik be. A személyes adatok védelmének látszatát a honlapon két rövid szabály próbálja fenntartani, mely adatvédelmi tájékoztatónak vagy szabályzatnak nem igazán nevezhető.

A fénykép- és videó gyűjtemény nagyobb része az érintettektől származik, akik önszántukból töltik fel a felvételeket. Ennek ellenére az adatkezelés aggályosnak tekinthető, éspedig két okból. Egyrészt azért mert az oldal „saját kép" alatt a feltöltő személyről, illetve az általa készített felvételt érti. Kérdéses lehet, hogy az adatokat feltöltő személy rendelkezik-e a felvételeken szereplő másik személy, személyek hozzájárulásával. A felvételek másik része egyértelműen jogellenes: ebbe a körbe a közterületen, nyilvános magánterületen, titokban készített fotók tartoznak. Bár a honlappal szemben hatékonyan – az internet jogi sajátosságai miatt – nem tud fellépni az adatvédelmi biztos, álláspontját meglehetősen kemény hangvételű levélben hozta az oldal képviselőjének tudomására:

„Tisztában vagyok azzal, hogy az internet számos előnye mellett a legkülönfélébb perverziók kiéléséhez is teret nyújt, elsősorban azzal, hogy biztosítja az arctalanságot, az anonimitást. Ilyen vád az Önök oldalával kapcsolatban is felmerülhet. Mindez ugyanakkor már túlmutat az adatvédelem körén, és tekintettel az internet „nemzetközi" voltára, és

arra, hogy a jog hatékonyan nem minden esetben tud fellépni, az oldallal a továbbiakban nem kívánok foglalkozni.

Szeretném ugyanakkor felhívni a figyelmét arra, hogy a közterületen, titokban készített felvételek esetén az anonimitás nem minden esetben biztosítható azzal, hogy a felvétel arc nélküli. Jelezném azt is, hogy több olyan esetről hallhattunk, amikor a „házi használatra" készített felvételt az egyik fél a másik érintett beleegyezése nélkül tette fel a világhálóra, okozva ezzel komoly problémákat az érintettnek. Az Önök oldalán, bárhogy kerestem, erre vonatkozó figyelmeztetést, amely az esetleges jogkövetkezményekre is rámutat, nem láttam.

Végezetül tájékoztatom arról, hogy álláspontomról a nyilvánosságot is tájékoztatni fogom, anélkül, hogy az Önök honlapját megnevezném (az esetleges félreértések elkerülése végett: nem a jó hírnevük esetleges megsértésétől tartok, csupán reklámozni nem szeretném Önöket). Ezzel együtt felhívom valamennyi esetleges érintett figyelmét arra, hogy a jogérvényesítéshez Irodám minden lehetséges támogatást megad." (1336/P/2007)

Végezetül röviden – újszerűsége miatt – egy olyan ügyre is érdemes kitérni, melynek a vizsgálata még folyamatban van. Egy közvéleménykutató cég (továbbiakban: adatkezelő) az internetes oldalakkal összefüggő látogató-összetétel statisztika készítéséhez egy eltérő módszert alkalmaz. Eszerint a statisztikák a látogatók forgalmi adatainak, valamint demográfiai alapadatainak (nem, kor, iskolai végzettség, lakóhelykód) összekapcsolásával készülnek. A legnagyobb hazai regisztrációs adatbázisok (továbbiakban: partner) bocsátják a cég rendelkezésére a felhasználóik által megadott demográfiai alapadatokat. Ez úgy történik, hogy a partner hozzárendel egy egyedi azonosítót minden regisztrált látogatójához, majd ezt adja tovább az adatkezelő rendszerének. Az adatkezelő állítása szerint ez az azonosító nem tartalmaz semmilyen személyes adatot, és nem kapcsolható hozzá ahhoz a személyhez, akit jelöl. Második lépésben a regisztrált látogatók demográfiai alapadatai egy lista fájlban, heti gyakorisággal kerülnek átadásra az adatkezelő rendszere felé úgy, hogy a fent említett azonosítót kapcsolják hozzá. A látogatók azonosítása kizárólag cookie-k alapján történik, az IP-címeket erre nem használja a rendszer. Az adatkezelő elmondása szerint a cookie-val történő nyomon követés a személyek azonosítására nem alkalmas, mert egy adott számítógép adott böngészőjének használóját

azonosítja, aki lehet egy személy, de lehet több is. Ezek után naponta elkészül egy lista, mely az azonos internet-felhasználókhoz tartozó cookie-kat rendezi össze a már rendelkezésre álló azonosítókkal. Ezt követően alakul ki az egyes cookie-láncokkal azonosított látogatók demográfiai profilja. Ezek a profilok olyan formában érhetők el, melyet kizárólag a feldolgozó program tud értelmezni. A napi, heti, illetve havi forgalmi adatok feldolgozása során statisztikai összegzésre kerülnek a profil adatok, aminek eredményeképpen elkészülő eredmény megadja, hogy az adott internetes portál látogatói között hány férfi és hány nő volt, milyen volt a kor-, végzettség-, lakóhely szerinti megoszlás. Mivel még sok kérdés megválaszolatlan, a fent részletezett eljárás vizsgálat alatt áll annak érdekében, hogy meg lehessen állapítani, sérti-e az internet-használók személyes adatok védelméhez fűződő jogát. *(1179/K/2007)*

Bankok, hitelintézetek

A hitelintézetek adatkezelését érintő állampolgári panaszok megközelítőleg ugyanakkora számban érkezetek az Adatvédelmi Biztos Irodájába, mint a tavalyi évben. Sajnálatos módon nem tudunk beszámolni ügyszámcsökkenésről, történt azonban néhány pozitív fejlemény. Az elmúlt évhez képest elenyésző azoknak az indítványozóknak a száma, akik a személyazonosító okmányok banki fénymásolását kifogásolták: vélhetően ez az adatkezelési gyakorlat visszaszorulóban van, illetőleg csak kivételes esetekben alkalmazzák a hitelintézetek az okmánymásolást, amikor azt fokozott banki kockázat teszi indokolttá.

> Az adatvédelmi biztos által vizsgált ügyben a bank pénzforgalmi tranzakciókra vonatkozó hatályos ügyviteli utasításai nem tartalmaztak olyan rendelkezést, amely szerint az ügyfélazonosítás során a személyazonosító igazolványról fénymásolatot kell készíteni. 2007 májusában azonban Budapesten két hét alatt négy olyan visszaélés történt a vállalkozói folyószámlákat érintően, amely során a harmadik személy által benyújtott hamisított készpénzutalvánnyal egyenként 400-500 ezer forint összegű kifizetésre került sor, különböző bankfiókokban. A további esetek elkerülése érdekében a Budapesti Régió ügyvezető igazgatója intézkedett arról, hogy ha a tranzakciót nem a bejelentett aláírással rendelkező számlatulajdonos kezdeményezi, akkor annak lefolytatásához két, személyazonosításra alkalmas okmány

bemutatását kérik, melynek másolatait a bizonylat mellett meg kell őrizni. Az okmány fénymásolásához minden esetben az ügyfél hozzájárulását kellett kérni. A pénzügyi szolgáltató elismerte, hogy az általuk ideiglenes jelleggel bevezetett gyakorlat nem felel meg az adatvédelmi törvény szabályainak, de azt a bank jogos önvédelmi eszközként kénytelen volt a visszaélések megszűnéséig fenntartani. *(1018/P/2007)*

Kedvező tendencia, hogy a központi hitelinformációs rendszer működését érintő megalapozott panaszok száma szintén csökkent. A bankszektor működését érintő beadványok közel 10%-ában a hitelfelvevők azt sérelmezték, hogy a hiteladat-szolgáltatók megítélésük szerint jogszerűtlenül továbbították személyes adataikat a központi hitelinformációs rendszerbe. Fontos kiemelnünk azt a panaszbeadványokból körvonalazódó tévhitet, miszerint, ha az adós rendezi adósságát, adatait automatikusan törlik a rendszerből, s így számára a további hitelfelvétel nem nehezül el. Ezekben az esetekben tájékoztattuk a beadványozókat, hogy a központi hitelinformációs rendszert üzemeltető vállalkozás a referenciaadatokat a késedelmes tartozás megszűnésének időpontjától számított öt évig kezeli. Az öt év letelte után törlik azokat véglegesen és vissza nem állítható módon. *(835/P/2007)*

A „teljes listás lakossági hitelinformációs rendszer", ismertebb nevén a pozitív adóslista hazai bevezetésével kapcsolatban 2007-ben is több ízben kezdeményeztek egyeztetést, konzultációt az érdekelt intézmények az Adatvédelmi Biztos Irodájával.

Az előkészítő egyeztetések során a biztos leszögezte, hogy törvényben előírt, kötelező adatkezelés csak akkor fogadható el, ha az megfelel az alkotmányosság követelményeinek, mivel a törvény által elrendelt adatkezelés a jog korlátozását jelenti. Az Alkotmánybíróság több határozatában rámutatott arra, hogy ha a korlátozás kényszerítő ok nélkül történik, vagy egyébként az nem áll összhangban az elérni kívánt céllal, azaz nem elkerülhetetlen, akkor az alapjog lényeges tartalmát érintő sérelem megállapítható. A szükségesség mellett a korlátozás másik lényeges eleme az arányosság: az alapjogot korlátozó normákkal szemben támasztott követelmény az, hogy az elérni kívánt cél fontossága és az ennek érdekében okozott alapjogsérelem súlya összhangban legyen egymással. Ennek során a törvényhozó köteles az adott cél elérésére alkalmas legenyhébb korlátozó eszközt kiválasztani. A biztos továbbra is úgy ítélte meg, hogy sem a célok mögött álló, a

szabályozást szükségessé tevő érdek nem igazolható, emellett az alkalmasság is megkérdőjelezhető. A lista „feltöltése" ugyancsak felveti az alkalmasság és az arányosság kérdését. Amennyiben az adatbázisba folyamatosan kerülnének be a törvény hatályba lépését követően felvett hitelek adatai, csak évek múlva állna rendelkezésre felhasználható adatállomány, egyértelműen megkésve. Az viszont elfogadhatatlan, hogy a pozitív listát a meglévő adatokkal feltöltsék, hiszen ez a személyes adatok védelméhez való jog visszamenőleges korlátozását jelentené, amely csak egészen kivételes esetben fogadható el. A biztos álláspontja tehát egyértelmű: a pozitív listás lakossági hitelnyilvántartást a továbbiakban sem támogatja.

Az Igazságügyi és Rendészeti Minisztérium 2007 júniusában megküldte az Adatvédelmi Biztos Irodájának e tárgyban kidolgozott koncepció tervezetét. A koncepció több olyan állítást, célkitűzést tartalmazott, amely adatvédelmi szempontból vitatható – természetesen ez nem akadálya annak, hogy az új szabályozás előkészítését a minisztériumban megkezdjék. Ha a módosító javaslat az Országgyűlés elé kerül, az aggályokat a biztos az Országgyűléssel is ismertetni fogja. *(1167/K/2007)*

2007-ben megnyugtató eredménnyel zárult az a konzultáció is, mely az adatvédelmi biztos vizsgálati jogosítványait érintette a pénzügyi szektor adatkezelői vonatkozásában. Mint arról az elmúlt évben beszámoltunk, a Pénzügyi Szervetek Állami Felügyelete az adatvédelmi biztos vizsgálati jogosultságát korlátozó felügyeleti állásfoglalásában úgy ítélte meg, hogy a biztos nem rendelkezik egyértelmű törvényi felhatalmazással banktitoknak minősülő adatok megismerésére. A Felügyelet még 2006-ban visszavonta korábbi állásfoglalását, fenntartva azt a véleményét, hogy az ügy megnyugtató megoldásához jogalkotói lépésre van szükség. 2007. július 1-jei hatállyal módosultak a pénzügyi tárgyú törvények, ily módon egyértelművé vált a jogalkalmazók számára, hogy az adatvédelmi biztos feladatai ellátásához jogosult bank-, értékpapír-, biztosítási-, és pénztártitoknak minősülő adatok megismerésére.

A biztos vizsgálati jogosítványaihoz kapcsolódóan beszámolunk arról, hogy egy nagy lakossági ügyfélkörrel rendelkező bank esetében került sor a bankszektorban első ízben az adatvédelmi törvény 31. §-ában szabályozott előzetes ellenőrzésre. A bank által bejelentett új adatállomány célja, hogy kapcsolatot teremtsen az ügyfelek és a bank különböző forrásrendszereiben tárolt termékinformációk között.

A biztos a vizsgálat során meghatározott dokumentumok csatolására hívta fel a pénzintézet belső adatvédelmi felelősét, melyet munkatársi szintű konzultáció is követett. A dokumentumok és a tárgyaláson elhangzottak tanúsága szerint a tervezett adatbázis használata során az értékesítő munkatárs az ügyfél természetes személyazonosító adatainak megadását követően lekérdezést hajt végre, melynek eredményeképpen a rendszer információt szolgáltatat arra vonatkozóan, hogy az adott ügyfél mely forrásrendszerekben szerepel. Az értékesítő munkatárs ezt követően az ügyfél kérésének megfelelően – a célhoz kötött adatkezelés törvényi követelményének figyelembevételével – lép tovább az adott forrásrendszerben tárolt termékinformációkhoz. Az egyes lekérdezéseket az informatikai rendszer naplózza, vagyis pontosan megállapítható, hogy az értékesítési területen dolgozó munkatársak közül ki, mikor, mely ügyféladathoz fért hozzá. A biztos az új adatbázissal kapcsolatban nem fogalmazott meg kifogást, az előzetes ellenőrzést további intézkedés megtétele nélkül zárta le. *(409/K/2007)*

2006 nyarán aggodalommal töltötték el mind a hazai, mind pedig az uniós állampolgárokat azok a sajtóhírek, melyek nyilvánosságra hozták a SWIFT pénzügyi üzenetek feldolgozásával foglalkozó, belgiumi székhelyű szervezet, valamint az USA hatóságai között létrejött tömeges méretű adattovábbítások részleteit. Az Európai Unió tagállamainak adatvédelmi hatóságaiból álló 29-es Munkacsoport még 2006 novemberében véleményt fogalmazott meg, meghatározva a felelősségi köröket. A Munkacsoport – a SWIFT-nek a Safe Harbour-hoz 2007 júliusában történő csatlakozását követően – a legfontosabb feladatnak azt tartotta, hogy a pénzügyi intézmények az adatvédelmi törvény rendelkezései alapján ügyfeleiknek megfelelő tájékoztatást nyújtsanak. A Munkacsoport a tájékoztatók gyakorlati bevezetésének határidejéül 2007. szeptember 1-jét jelölte meg. A tájékoztatókkal szemben megfogalmazott tartalmi követelményeket, valamint a magyar adatvédelmi hatóság ezzel kapcsolatos intézkedéseit a beszámoló „Nemzetközi ügyek" című fejezetében tárgyaljuk.

És végül egy tipikus, nagy számban előforduló adatkezelési problémára hívjuk fel a figyelmet, melyet sajnálatos módon nem sikerült 2007-ben megoldanunk, ez pedig nem más, mint a pénzintézeteknek a pénzmosás megelőzéséről és megakadályozásáról szóló 2003. évi XV. törvény (továbbiakban: Pmt.) 3. §-a alapján folytatott ügyfélazonosítási tevé-

kenysége. A Pmt. 3. § (3) bekezdése értelmében az azonosítási kötelezettség kiterjed az egymással ténylegesen összefüggő, több ügyleti megbízásra, ha ezek együttes értéke eléri a kétmillió forintot. Ebben az esetben az azonosítást azon ügyleti megbízás elfogadásakor kell végrehajtani, amellyel az ügyletek együttes értéke eléri a kétmillió forintot.

A bankok álláspontja szerint minden ügyfelet – értékhatárra tekintet nélkül – azonosítani kell, mivel csak ebben az esetben tudnak eleget tenni a törvényben előírt azon kötelezettségnek, mely szerint egymással összefüggő ügyletek esetében is vizsgálni kell a pénzmosás megvalósulásának lehetőségét.

> Mivel a törvény ilyen módon való értelmezése sérti az adatvédelmi törvény rendelkezéseit, illetve céljait, ezért 2007 januárjában a biztos felvilágosítást kért a Nemzeti Nyomozó Iroda Pénzmosás Elleni Osztályának vezetőjétől, aki elismerte, hogy a hatályos Pmt. azonosítást előíró rendelkezései nehezen, illetve többféleképpen is értelmezhetők. A pénzintézetek attól való félelmükben, hogy elmulasztják a törvény által előírt bejelentési kötelezettségüket gyakran „túljelentik magukat", azaz olyan személyeket és tranzakciókat is azonosítanak, amelyekre nem lenne szükség. Válaszában utalt arra is, hogy 2007 decemberéig új pénzmosás elleni törvény fog hatályba lépni, amelynek megalkotásánál természetesen figyelembeveszik majd az eddigi gyakorlat során felmerült problémákat. Az új Pmt. előkészítése során a biztos több ízben jelezte a szaktárca illetékes vezetőinek, hogy a fenti törvényi rendelkezés értelmezése nehézséget jelent és ennek kihatása van az ügyfelek személyes adatok védelméhez fűződő jogára. A biztos ezen észrevételét a tervezetet előkészítő munkacsoport figyelmen kívül hagyta, ezért 2007 augusztusában az ismételten megküldött, már átdolgozott tervezet kapcsán megismételte azokat.

Az új Pmt. 2007. december 14-én lépett hatályba, s ezen a ponton lényegileg megegyezik a régi szabályozással. A törvény a „ténylegesen összefüggő ügyleti megbízás" fogalmát ugyan definiálja, azonban ennek alapján a pénzintézetek továbbra is egymással összefüggőnek minősíthetik az egyazon ügyféltől származó megbízásokat, függetlenül azok összegétől. Számos panasz érkezett az Adatvédelmi Biztos Irodájába, melyben a beadványozók azt kifogásolták, hogy egy-két ezer forintos befizetések esetén is minden alkalommal azonosítják őket. A pénzintézetek az új Pmt. alapján is kitarthatnak a mindenkire kiterjedő azonosítás mellett, ugyanis enélkül nem tudják megállapítani, hogy az érintett

mikor éri el a törvényi összeghatárt, mely hárommillió-hatszázezer forintra emelkedett. Életszerűtlennek tűnik ugyanis az a rendelkezés, hogy az azonosítást csak az összeghatár elérésekor kell végrehajtani. Ha a bank korábban nem azonosította volna minden esetben a befizetőt és nem „naplózza" a befizetések összegét, úgy szinte kizárt, hogy meg tudja állapítani, hogy mikor éri el a tranzakciók összege a törvényi összeghatárt. A jogi helyzetet még komplikáltabbá teszi a 21/2006. (XI. 24) MNB rendelet, melyre a bankok adatkezelésük másik indokaként gyakorta hivatkoznak. *(2287/P/2007)*

Biztosítók

A biztosítók adatkezelését érintő állampolgári panaszok száma az idén kis mértékben ugyan, de növekedett. Az indítványok egy része egyedi adatkezelői hibákra hívta fel a figyelmet. A vizsgálatokat követően tett adatkezelői intézkedések az esetek döntő többségében elégségesnek bizonyultak arra, hogy a jövőben további jogsérelem ne következhessen be. Arról is be kell azonban számolnunk, hogy vannak a biztosítási szektorban olyan adatkezelési problémák, melyek évről-évre visszaköszönnek, s ezek kiküszöbölése már meghaladja az egyes adatkezelők kompetenciáját. Az egészségügyi adatok kezelése a biztosítási piac adatvédelmi szempontból egyik ilyen érzékeny pontja.

A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény (továbbiakban Bit.) alapján az ügyfél egészségi állapotával összefüggő adatokat a biztosító a 155. § (1) bekezdésében meghatározott célokból, az Eüak. rendelkezései szerint, kizárólag az érintett írásbeli hozzájárulásával kezelheti. Az adatkezelés célja csak a biztosítási szerződés megkötéséhez, módosításához, állományban tartásához, a biztosítási szerződésből származó követelések megítéléséhez szükséges, vagy az e törvény által meghatározott egyéb cél lehet. A megválaszolandó kérdés tehát az, vajon a szerződést megelőző tárgyalások – ajánlattétel – során a biztosító által vállalandó kockázat felméréséhez az ügyféltől kért egészségügyi adatok, vagy az azok megszerzését lehetővé tevő adatkezelési felhatalmazás a fenti célok eléréséhez nélkülözhetetlenek-e.

Az Adatvédelmi Biztos Irodájának megalakulása óta nagy számban érkeztek panaszok az úgynevezett blanketta-jellegű orvosi felmentvény ellen. Az orvosi felmentvénnyel kapcsolatban a Pénzügyi Szerve-

zetek Állami Felügyelete és az Adatvédelmi Biztos Irodája már 2004-ben egyeztette szakmai álláspontját. A Felügyelet akkor arról tájékoztatta az adatvédelmi biztost, hogy a kibontakozott szakmai vita során *„a biztosítók egységesen akként foglaltak állást, hogy az adatvédelmi biztos által kifogásolt, szinte korlátlan, általános jellegű felhatalmazás mindenképpen korrekcióra szorul. Az orvosi titoktartás alóli felmentés rendszerint az egészségi állapottal összefüggő adatok körét, tehát különleges adatokat érint. Ezek az adatok szorosan összefüggnek a biztosító kockázatvállalásával és szolgáltatásával is. Mindezek figyelembe vételével az orvosi titoktartás alóli felmentvényt célszerű a szerződés megkötéséhez, annak fenntartásához, illetve a biztosítási eseményhez kapcsolódó szolgáltatás teljesítéséhez szükséges adatok körére szűkíteni."* Sajnálatos tény azonban az, hogy nem minden életbiztosítónál vált gyakorlattá a fenti, a szakmai vita eredményeként megállapított szűkítés, ezért 2007-ben az adatvédelmi biztos ismételten tárgyalt e témában a Felügyelet főigazgatójával. A Felügyelet az úgynevezett orvosi felmentvényre konkrét szövegjavaslatot dolgozott ki, melyet a biztos véleményezett. A konzultáció eredményeként megszületett szövegjavaslatot a Felügyelet közlemény formájában 2007 decemberében közzétette honlapján. Ezt megelőzően, még november folyamán körlevélként megküldte azt valamennyi, az élet-, illetve baleset- és betegbiztosítási ágazat végzésére tevékenységi engedéllyel rendelkező biztosító első számú vezetője számára. A közleményben a Felügyelet azt is javasolta, hogy a biztosítótársaságok e nyilatkozatot a termékfeltételek szövegétől, illetve más nyilatkozatoktól és ügyféltájékoztatásoktól elkülönítetten szerkesszék meg, és tegyék lehetővé, hogy a biztosított az abban foglaltak tudomásul vételét külön aláírásával igazolhassa.

A Felügyelet és az Adatvédelmi Biztos Irodája között zajló egyeztetés tárgya kizárólag az élet-, baleset- és betegbiztosítások jelenlegi szabályozásához és gyakorlatához kötődik, és nem alkalmazható a jövőben esetleg létrejövő, magánbiztosítók részvételével működő nemzeti társadalombiztosítási rendszerre. Ennek a rendszernek az adatkezelési szabályozása kizárólag egységesen, törvényi szinten képzelhető el. *(938/A/2006)*

Az ügyek jelentős hányada 2007-ben is a kötelező gépjármű-felelősségbiztosítási jogviszonyokat érintette. Az év végi átszerződések során előfordult olyan eset is, amikor a biztosító a szerződés megkötését az

orvosi felmentvény megadásához kötötte. Egy ilyen kikötés alkalmazása ebben a biztosítási ágazatban adatvédelmi szempontból teljesen elfogadhatatlan. *(2252/P/2007)*

Mint ahogyan arról korábban beszámoltunk, a felelősségbiztosítás esetén a biztosítási jogviszony hárompólusú jogviszony, mely az érintettet megillető tájékoztatáshoz való jog gyakorlása során okoz jogalkalmazási nehézségeket. A biztosító szempontjából mind a biztosított, mind pedig a károsult harmadik személynek minősül a másik személyes adata és biztosítási titka szempontjából. Nehezen megválaszolható a kérdés, hogy a káresemény adatai közül melyek tekinthetők a károsult, és melyek a károkozó adatainak.

> Az a jogértelmezés is elfogadható, mely szerint a káresemény során a károkozó által előidézett hatás a károsultnál jelentkezik, de a károkozó tevékenységére is vonatkozik, vele is kapcsolatba hozható, rá is vonatkozik, tehát az ő személyes adata is. Ebből az értelmezésből az következik, hogy a károkozó az információs önrendelkezési jogából fakadóan jogosult részletes tájékoztatást kérni az általa okozott károkról, vagyis ebben a körben már nem tekinthető harmadik személynek. Korábbiakban olyan állásfoglalás született, hogy a részletes számítógépes javítási kalkuláció azon adatai, amelyek kapcsolatba hozhatók a károsultnak a kárfelvételi jegyzőkönyvben szereplő személyes adataival, elsősorban a károsult személyes adatainak minősülnek. A biztos ebben az ügyben is konzultált a Felügyelettel, s 2007 januárjában jelezte, hogy a károsult és a károkozó információs önrendelkezési jogának konfliktusa a Bit. biztosítási titokra vonatkozó szabályainak módosításával egyértelműen feloldható lenne, ugyanis meggyőződése, hogy az adott jogterületre vonatkozó szabályok értelmezése útján nem érhető el megnyugtató eredmény. Az egyeztetést követően a Bit. 157. § (1) bekezdése 2007. július 1-jei hatállyal kiegészült azzal a rendelkezéssel, mely szerint a biztosítási titok megtartásának kötelezettsége nem áll fenn a károkozóval szemben, amennyiben az önrendelkezési jogával élve a közúti közlekedési balesetével kapcsolatos kárrendezés kárfelvételi jegyzőkönyvéből a balesetben érintett másik jármű javítási adataihoz kíván hozzáférni. *(490/K/2006)*

Szintén a kötelező gépjármű-felelősségbiztosítással kapcsolatos adatkezelést érinti az az indítvány is, mely arra keresett választ, hogy mi a követendő eljárás a gépjármű üzembentartójának halála esetén.

Amennyiben a gépjármű birtokosa – a hagyatéki eljárás befejezéséig – használni óhajtja a gépjárművet, úgy meg kell fizetnie az örökhagyó által kötött szerződés díját és a biztosító társaságnak a halál tényét be kell jelentenie. A hagyatéki eljárás lezárását követően lesz egyértelműen megállapítható, hogy ki a gépjármű új tulajdonosa (örökös), akinek a gépjárműre – mivel az örökhagyó által kötött biztosítás érdekmúlás miatt megszűnt – új kötelező felelősségbiztosítási szerződést kell kötnie. A panaszos a biztosító adatkérését a szóban forgó esetben túlzottnak tartotta, hiszen a végrendeletet, és a hagyatéki végzés másolatát is be kellett volna csatolnia. A biztos álláspontja szerint a biztosító adatkezelése nem felelt meg a célhoz kötött adatkezelés elvének. A halál tényének bejelentéséhez ugyanis elégséges a korábbi tulajdonos halotti anyakönyvi kivonatának a bemutatása. Felhívta továbbá a biztosítótársaság figyelmét arra is, hogy a biztosító a hagyatéki eljárást lezáró jogerős határozatot is csak korlátozott mértékben ismerheti meg, azon részében, mely igazolja, hogy ki a hagyaték részét képező gépjármű új tulajdonosa. *(1127/P/2007)*

Végül a vagyonbiztosítás témaköréből ismertetünk egy esetet, melynél a biztosítót fel kellett szólítani a jogszerűtlen adatkezelési gyakorlat megszüntetésére. A panaszost a kárrendezési eljárás során a biztosító ügyintézője arra kérte, hogy a bérgépjármű költségének megtérítéséhez dokumentummal igazolja, hogy a költséget valóban megfizette a bérbeadónak. Ezen a dokumentumon *„kérik szerepeltetni a bérbeadó adóazonosító jelét, mivel azt megküldik a bérbeadó lakcíme szerinti adóhivatalhoz tájékoztatásul a jövedelemszerzésről”*.

A vizsgálattal érintett cég vezérigazgatója azt a felvilágosítást adta, hogy *„magánszemélyek közötti bérbeadási szerződés esetében a bérbeadási szolgáltatás valós voltának (és így a biztosító szolgáltatása megalapozottságának) az ellenőrzéséhez szükséges annak megállapítása, hogy a bérbeadó a bérbeadásból származó jövedelmet az adóhatóság felé bevallja-e”*. Álláspontja szerint *„indokolt, hogy a biztosító a bérgépkocsi igényt számla hiányában csakis abban az esetben téríti, ha a bérbeadásból származó jövedelem utáni közteher az állam részére befizetésre került, illetve indokolt, hogy a biztosító bejelentésével közreműködjön a bérbeadásból származó jövedelem utáni adózásban”*.

A biztosító az adatkezelés jogalapjaként egyrészt a személyi jövedelemadóról szóló 1995. évi CXVII. törvény 1. §-át, valamint a Legfelsőbb Bíróság Pfv. VIII.21.342/2004/6. számú ítéletét és az ezen alapuló bírói gyakorlatot jelölte meg. Tekintettel arra, hogy ez az érvelés nem

felel meg az adatvédelmi törvény rendelkezéseinek, az adatkezelés, adattovábbítás jogalapjaként a biztos nem fogadta el. Felhívta a biztosító figyelmét arra is, hogy az Art. nem állapít meg a biztosítótársaságok vonatkozásában ilyen adatszolgáltatási kötelezettséget az adóhivatalok felé. Amennyiben személyes adat kezelését törvény (vagy önkormányzati rendelet) nem rendeli el, akkor az adatkezelés abban az esetben jogszerű, ha ahhoz az érintett (jelen esetben a bérbeadó) hozzájárult. A bérbevevő – az információs önrendelkezés elvéből következően – a bérbeadó személyes adatai vonatkozásában a nyilatkozattételt a biztosítótársaság felé nem gyakorolhatja. Végezetül a biztos felhívta a biztosító vezetésének figyelmét arra is, hogy az adókötelezettségek teljesítését az adóhatóságok ellenőrzik. *(201/P/2007)*

Sajtó

Bár a sajtó nem tartozik a nagy adatkezelők közé, mégis évről évre kiemelt figyelmet fordítunk azokra az ügyekre, melyekben a sajtó, mint adatkezelő szerepel. 2006-ban elsősorban az országos, illetve helyi lapokban megjelenő fotók sajtó általi nyilvánosságra hozatalát, valamint a televíziók műsorszerkesztési módszereit kifogásolták a panaszosok. 2007-ben viszont a beadványok jelentős részében a panaszosok a büntetőeljárással, büntetett előélettel, valamint a büntetés- végrehajtással kapcsolatban közölt bűnügyi és igazságügyi tájékoztatásokban szereplő személyes adataik kezelését sérelmezték, illetve a sajtóval szembeni jogorvoslati lehetőségekről kértek felvilágosítást. Ezen túlmenően 2007-ben ismételten több beadvány érkezett a kereskedelmi televíziók műsorkészítésével kapcsolatban, amelyekben a panaszosok szintén a személyes adataik közzétételét sérelmezték.

Egy előzetes letartóztatásban lévő panaszos beadványában azt sérelmezte, hogy az ellene folyamatban lévő büntetőügyben nevét és a kihirdetett első fokú ítélet tartalmát leközölték a tárgyalásról tudósító újságcikkben.

A Be. 237.§ (1) bekezdése értelmében a bíróság tárgyalása nyilvános. A bíróság nyilvános tárgyalásáról pedig a sajtó jogosult tájékoztatást adni. A Be. idézett szabályaival összhangban a sajtóról szóló 1986. évi II. törvény 5. §-a szintén úgy rendelkezik, hogy a *„sajtó - az érdekeltek hozzájárulása nélkül is - tájékoztatást adhat az állami szervek, a gazdálkodó szervezetek, a társadalmi szervezetek és az egyesületek, vala-*

mint ezek bizottságai nyilvános üléséről, továbbá a bíróságok nyilvános tárgyalásairól."

A nyilvános tárgyaláson, illetve a kihirdetett ítéletben számos olyan adat válik megismerhetővé, amely személyes, illetve bűnügyi személyes adatnak minősül, ezért a nyilvános tárgyalásról készült tudósításoknál az újságíróknak a bűnügyi és az igazságügyi tájékoztatásról szóló 10/1986. (IX. 1.) IM-BM együttes rendelet (a továbbiakban: Sajtó rendelet) szabályai szerint kell eljárniuk. E rendelet 3. §-a szerint a bíróságok előtt folyamatban levő, illetőleg az általuk befejezett ügyekről adott tájékoztatás nem sértheti az ártatlanság vélelmét és az állampolgárok személyhez fűződő jogait. Nem tartalmazhat olyan megállapítást, amely a tárgyilagos döntést veszélyezteti. A tájékoztatásban közölni kell, hogy az ismertetett ügy az eljárásnak milyen szakaszában van, és hogy a tájékoztatás milyen forrásból származik.

Az előzőek alapján tehát azon adatok és információk, amelyek a tárgyaláson kihirdetett ítélet (határozat) részét képezik, nyilvánosnak tekinthetők, ezért adatvédelmi szempontból nincs annak jelentősége, hogy az ítélet jogerős-e vagy nem, arról a sajtó – az érdekeltek hozzájárulása nélkül – tudósíthatja a közvéleményt.

Az adatvédelmi biztos tájékoztatta továbbá a panaszost, hogy a Sajtó rendelet 3.§ (3) bekezdése alapján, ha az ügyről az eljárást befejező határozat meghozatala előtt közölt az újság tájékoztatást, akkor – az érdekelt kérelmére – az eljárást befejező határozatról, ha pedig a határozatot utóbb megváltoztatták, erről a döntésről is hírt kell adni a sajtóban. Fontos azonban, hogy ez a tájékoztatás az ítélet meghozatalát követő ésszerű határidőn belül jelenjen meg a sajtóban. *(207/P/2007)*

Egy másik esetben a panaszos azt sérelmezte, hogy a Kőbányai Magazinban, illetve a Zsaru című lapban róla és tettestársáról a családi és utóneve kezdőbetűinek feltüntetésével jelent meg bűnügyi tudósítás. Az újságcikkek a X. kerületi Rendőrkapitányságon „hivatalos jelleg színlelésével elkövetett zsarolás bűntettének megalapozott gyanúja miatt", indult büntetőeljárásról tudósítottak.

Az adatvédelmi törvény alapján az eljárással kapcsolatos, érintettre vonatkozó adatok bűnügyi személyes adatok. Az újságíróknak a Sajtó rendelet szabályai szerint kell eljárniuk. A rendelet 2. § (1) bekezdése alapján a bűnüldöző szervek, a bíróságok és a büntetésvégrehajtási intézetek a szükséges felvilágosításoknak és adatoknak a sajtó rendel-

kezésére bocsátásával biztosítják, hogy az előttük folyó eljárásokról, az egyes ügyekben végzett tevékenységükről a közvélemény hiteles, pontos és gyors tájékoztatást kapjon. A rendelet 3.§ (3) bekezdése csak a kiskorú személyek esetében írja elő, hogy a *„tájékoztatás során a kiskorú személy családi neve – kivéve, ha súlyos bűncselekményt követett el – csak kezdőbetűvel jelölhető, képmása és hangfelvétele pedig – a Ptk. 80. § (3) bekezdésében meghatározott eseten kívül – csak olyan módon közölhető, hogy a kiskorú ne legyen azonosítható."*

Az adatvédelmi törvény fentebb idézett rendelkezéseinek megfelelően személyes adatnak és bűnügyi (különleges) személyes adatnak is csak azok az adatok minősülhetnek, amelyek alapján egyértelműen lehetőség van egy meghatározott természetes személy azonosítására. Ennek megfelelően a családi és utónév kezdőbetűinek feltüntetése a bűnügyi tudósításokban megfelel mind az adatvédelmi törvény, mind pedig a Sajtó rendelet előírásainak, valamint az ennek megfelelően kialakított újságírói gyakorlatnak. *(1117/P/2007)*

Egy elítélt levelében az iránt érdeklődött, hogy kérhető-e a „teljes körű hírzárlat" személyével, valamint a Tököli BV Intézetből történő szabadulása időpontjával kapcsolatosan.

A Sajtó rendelet hatálya kiterjed a büntetés-végrehajtási intézetek által végrehajtott bírósági határozatokról szóló, a sajtóban közölt tájékoztatásra is. Az ügyekről adott tájékoztatás nem sértheti az állampolgárok személyhez fűződő jogait.

A büntetések és az intézkedések végrehajtásáról szóló 1979. évi 11. törvényerejű rendelet (továbbiakban: Bvtvr.) 2. § (2) bekezdés c) pontja – az adatvédelmi törvény rendelkezéseivel összhangban – szintén úgy rendelkezik, hogy az elítélt jogosult személyhez fűződő jogainak, így különösen a jó hírének, magántitkának, a személyes adatainak a védelmére, magánlakásának sérthetetlenségére. Az ismertetett jogszabályi előírások alapján az adatvédelmi biztos megállapította, hogy – törvényi felhatalmazás hiányában – az elítélt hozzájárulása nélkül a Tököli BV. Intézet nem adhat felvilágosítást a sajtónak a panaszos személyes adatairól, valamint szabadulása időpontjáról. *(2102/P/2007)*

Évek óta visszatérő probléma a polgárok személyes, sok esetben szenzitív adatainak nyilvánosságra hozatalával kapcsolatban kialakult televíziós műsorkészítési gyakorlat. Az idén is érkeztek panaszok a kereskedelmi televíziók műsorszerkesztési gyakorlatával kapcsolatosan.

Az egyik panaszos beadványában azt sérelmezte, hogy az RTL Klub Balázs című showműsorában műsorának illusztrációjához a panaszos esküvői fényképét használták fel, melyet az internetről töltöttek le.

> A fénykép az adatvédelmi törvény 2. §-ának 1. pontja alapján személyes adat. A televíziós csatorna a panaszosról készült fotót jogszerűen nem használhatta volna fel, hiszen az ilyen célú felhasználáshoz az érdekeltek nem járultak hozzá, ezért a bepanaszolt televíziós csatorna tevékenysége jogellenes adatkezelésnek minősül. *(412/P/2007)*

Szintén az RTL Klub eljárását sérelmezte két panaszos, mert róluk felvételeket készítettek, amelyek a tudtuk és beleegyezésük nélkül adásba kerültek.

> Az érintettről készült hang- és képfelvétel személyes adat, ebből következően annak rögzítése, felhasználása és nyilvánosságra hozatala adatkezelésnek minősül. A felvételkészítéshez és annak további felhasználásához – ideértve a televízióban történő nyilvánosságra hozatalt is – törvényi felhatalmazás hiányában a felvételen szereplő érintett hozzájárulása szükséges. A Legfelsőbb Bíróság egyik határozata szerint a képmás nyilvánosságra hozatalának tilalma nem vonatkozik a nyilvános eseményekről, rendezvényekről, táj-, utcarészletekről készült felvételekre, amikor az ábrázolás módja nem egyéni, amikor a felvétel összhatásában örökít meg a nyilvánosság előtt lezajlott eseményeket. A nyilvánosságra hozatalhoz a felvételen ábrázolt személy hozzájárulására van viszont szükség, ha megállapítható a felvétel egyedisége, egyéni képmás jellege.
>
> Az adatvédelmi biztos álláspontja szerint Az RTL Klub minkét esetben a panaszosok beleegyezése nélkül rögzítette és hozta nyilvánosságra a róluk készült felvételeket, és ezzel megsértette a panaszosok személyiségi jogát és a személyes adatok védelméhez fűződő jogát. Az adatvédelmi biztos tájékoztatta a panaszosokat a jogorvoslati lehetőségeikről is.*(1068/P/2007, 1665/P/2007)*

A Bors című napilap újságírója a Tököli BV. Intézetben történt bűncselekmény körülményeit feltárni szándékozó újságcikke kapcsán a BV. Intézet parancsnokának – a feltett kérdésekre adott – válaszaival kapcsolatban kért állásfoglalást.

> A Sajtó rendelet 12. §-a szerint a büntetés-végrehajtási intézetben szabadságvesztés büntetését vagy elzárását töltő, illetőleg szigorított őrizetben levő személlyel való beszélgetést, a beszélgetésről felvétel

készítését a büntetés-végrehajtás országos parancsnoka az Igazságügyi Minisztérium Tudományos és Tájékoztatási főosztályának vezetőjével egyetértésben engedélyezi. Az engedély csak akkor adható meg, ha a felvétel nyilvánosságra hozatalához a felvételen szereplő és az eljárásban részt vevő személyek hozzájárultak.

A Bvtvr. 2. § (2) bekezdés c) pontja – az adatvédelmi törvény rendelkezéseivel összhangban – szintén úgy rendelkezik, hogy az elítélt jogosult személyhez fűződő jogainak, így különösen a jó hírének, magántitkának, a személyes adatainak a védelmére, magánlakásának sérthetetlenségére. Fenti jogszabályi előírások alapján megállapítható, hogy – törvényi felhatalmazás hiányában – az érintettek hozzájárulása nélkül a Tököli BV. Intézet nem adhat felvilágosítást a sajtónak a rabok (bűnügyi) személyes adatairól, a bűncselekményről, a büntetés idejéről, a szabadulás időpontjáról, a zárkatársak bűncselekményeire vonatkozó adatokról.

Az adatvédelmi biztos arról is tájékoztatta az újságírót, hogy az elhunyt személy személyes adatainak védelmét nem az adatvédelmi törvény, hanem a polgári jogban található kegyeleti jog intézménye biztosítja. Az elhunytak adatainak kezelésével kapcsolatban a kegyeleti jog jogosultjainak van lehetősége eljárni. A Ptk. 85. § (3) bekezdése értelmében a „meghalt személy emlékének megsértése miatt bírósághoz fordulhat a hozzátartozó, továbbá az a személy, akit az elhunyt végrendeleti juttatásban részesített." Az elhunyt rab esetében tehát a (bűnügyi) személyes adatokról történő tájékoztatáshoz az érintett hozzátartozóinak a hozzájárulása szükséges. *(2102/P/2007)*

Múlt feltárása, levéltár, tudományos kutatás

Ebben az évben a korábbiaknál kevesebb a tárgyba tartozó indítvány érkezett. Elsőként érdemes egy állampolgári panaszt bemutatnunk.

A panaszos kifogásolta – miután saját személyére vonatkozóan akart információkat a levéltárból megszerezni –, hogy a levéltár az iratokat nem név szerint, hanem „dobozonként", azaz az iratot keletkeztető szerv szerint őrzi. Az indítványban foglaltakra a biztos kifejtette, hogy a levéltárak használatát és adatkezelését a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (továbbiakban: Ltv.) és a hozzá kapcsolódó egyéb jogszabályok rendezik. A levéltár célja, hogy – elsősorban a közfeladatot ellátó szervek – maradandó értékű iratait kezelje és nem az, hogy az azokban

szereplő személyes adatokat nyilvántartsa. A levéltári anyagban lévő személyes adatok kezelését a törvény megfelelően szabályozza.

A levéltári törvény előírja, hogy a közlevéltár a kérelmező által megadott – az azonosításhoz szükséges – információk alapján egyedi adatról tájékoztatást nyújt. A tájékoztatási kérelem részleges vagy teljes megtagadását a közlevéltár írásban köteles közölni. Tájékoztatás érdekében közlevéltár kutatást – díjtalan szolgáltatásként – csak jogszabály alapján vagy fenntartója utasítására végez. Amint az az indítványozó által csatolt dokumentumokból kitűnik, a levéltár a jogszabályoknak megfelelően járt el. *(510/P/2007)*

Régóta – mintegy tíz éve – van ígéret arra vonatkozóan, hogy a jogalkotó végre törvényben rendezi az anyakönyvi nyilvántartások és az azokba való betekintés ügyét.

A probléma a következő: az adatvédelmi törvény szerint az érintett jogosult a róla szóló iratokba betekinteni. Azonban az anyakönyvekről, a házasságkötési eljárásról és a névviselésről szóló 1982. évi 17. törvényerejű rendelet szerint ha törvény másként nem rendelkezik, az anyakönyvi nyilvántartásokba betekintés csak olyan állami vagy önkormányzati szerv nevében eljáró személynek engedélyezhető, aki igazolja a betekintés célját és jogalapját.

Emellett a kutatási célú felhasználáshoz figyelembe kell venni az Ltv. rendelkezéseit is. Ennek értelmében ha törvény másként nem rendelkezik, a személyes adatot tartalmazó levéltári anyag az érintett halálozási évét követő harminc év után válik bárki számára kutathatóvá. A védelmi idő, ha a halálozás éve nem ismert, az érintett születésétől számított kilencven év, ha pedig a születés és a halálozás időpontja sem ismert, a levéltári anyag keletkezésétől számított hatvan év. Bizonyos feltételekkel a védelmi idő lejárta előtt is kutatható a levéltári anyag, így például, ha a kutatás anonimizált másolattal is megvalósítható, vagy ahhoz az érintett, illetőleg annak halálát követően bármely örököse vagy hozzátartozója a kutató kérésére hozzájárult, vagy a kutatásra tudományos célból van szükség és a kutató bizonyos követelményeknek eleget tesz.

Kiegészíti a problémát az anyakönyvekről, a házasságkötési eljárásról és a névviselésről szóló 6/2003. (III. 7.) BM rendelet, mely a következőket írja elő: „*Az anyakönyvi bejegyzés, illetőleg irat megtekintésére kiadott engedély tartalmazza, hogy az mely bejegyzés vagy irat megtekintésére jogosít, és a betekintésre milyen hivatalos eljárásban van*

szükség. Az engedélyt az anyakönyvvezető bevonja és az alapiratok között elhelyezi. A levéltár őrizetében levő másodpéldány megtekintését a levéltár vezetője engedélyezi."

A fentiek alapján nem látható át az anyakönyvi iratokba való betekintés szabálya, mivel az egymásnak ellentmondó különböző szintű jogszabályok ezt nem teszik lehetővé.

Ehhez kapcsolódik még a külföldre továbbítás problémája, mely az adatvédelmi törvény szerint – az érintett engedélyén kívüli esetben – az Európai Unión kívül csak olyan országba történhet, amely országot az Unió azonos védelmet biztosítónak elismerte, vagy a biztonságos adatkezelésre szerződést kötött. Az Egyesült Államokba továbbítandó anyakönyvi adatok esetében a feltételek a levéltári törvény és a BM rendelet szerint fennállnak, az adatvédelmi törvény és az anyakönyvi tvr. szerint nem. Ennek az áttekinthetetlen helyzetnek a javítására adott ki a biztos útmutatót a vidéki levéltárosok közgyűlése előtt, melyben felhívta a figyelmet az adatvédelmi törvény szabályainak alkalmazására, így a külföldre való adattovábbítás lehetőségeire is. *(1813/H/207)*

Közüzemi szolgáltatók

Idén a legtöbb panaszbeadvány azzal a kérdéssel érkezett hozzánk, hogy jogszerű-e, ha a közüzemi szolgáltatók a mérőóra átírásához az ingatlan tulajdoni lapját, illetőleg az adásvételi szerződés másolatát igénylik az ügyfeleiktől.

A változást igazoló dokumentumokban foglalt személyes adatokat csak abban a körben ismerheti meg a szolgáltató, amelyben arra törvényi felhatalmazása van, azaz természetes személy fogyasztó esetén a nevét, lakcímét, anyja nevét, és a születési helyét és idejét kezelheti jogszerűen. Ennek megfelelően a szolgáltató akkor jár el jogszerűen, ha úgy igényli az adásvételi szerződés, illetve tulajdoni lap másolatát a fogyasztótól, ha lehetőséget biztosít neki arra, hogy azokból a fogyasztó minden olyan személyes adatot töröljön, illetve kitakarjon, amely nem tartozik a fenti körbe, és e lehetőségről a fogyasztókat tájékoztatja is. (A tulajdoni lappal kapcsolatban érdemes megjegyezni, hogy annak tartalma nyilvános, azt bárki megismerheti, ezért abból olyan adatok kitakarása, amely a fenti körbe nem tartozik jogszerű ugyan, de indokolatlan.)

Összefoglalva elmondható, hogy amennyiben a szerződésről vagy a tulajdoni lapról készített fénymásolatot úgy adja át a szolláltató részére, hogy az csak a változást dokumentáló részeket tartalmazza, a többi személyes adat azonban nem olvasható rajta, úgy az érintett jogszerűen jár el, ezen igazolás el nem fogadása esetén a szolgáltató pedig jogellenesen. *(1226/P/2007, 1390/P/2007)*

Hasonló ügyekben a Fővárosi Gázművek, az ÉGÁZ-DÉGÁZ Gázszolgáltató Zrt., valamint a Fővárosi Vízművek a jogerős hagyatéki végzés másolatát kérték ügyfeleiktől a számlatulajdonlás átírásához.

A felhasználó személyében történt változás, illetve a fogyasztásmérő átírása már új szerződés megkötését jelenti. Az ügyfél személyében beállt változást igazoló iratok, (adásvételi szerződés, hagyatéki végzés, halotti anyakönyvi kivonat, bérleti szerződés, stb.) valamint a személyazonosításra alkalmas okmány bemutatása az ügyfél jogszabályi előíráson alapuló kötelezettsége. Tehát a fogyasztó személyében beállt változást igazoló okirat, valamint a személyazonosításra alkalmas okmány bemutatása, és abból a közüzemi szerződés megkötéséhez szükséges adatok megismerése és rögzítése szükséges, és egyben elegendő a személyesen eljáró ügyféllel való szerződéskötéshez.

Ami az ügyfél személyében beállt változást igazoló iratokról, így a hagyatéki végzésről készült fénymásolatok kezelését illeti, az adatvédelmi biztos álláspontja az eddig kialakult gyakorlatnak megfelelően továbbra is az, hogy az energiaszolgáltatóknak a hatályos magyar jogszabályi előírások erre nem adnak törvényi felhatalmazást. A fogyasztásmérő átírásához szükséges adatok felvétele nem lehet célja és indoka a hagyatéki végzésről való másolat kezelésének, annál is inkább, mert a hagyatékátadó végzés legtöbb esetben nemcsak az új fogyasztó, hanem az elhunyt valamennyi örökösének személyes adatait, valamint az örökség részét képező ingók és ingatlanok részletes adatait is tartalmazza.

A fentiekre való tekintettel a panaszosok visszakérhetik a hagyatéki végzés fénymásolatát, valamint kérhetik – a jogszabályban elrendelt adatkezelések kivételével – a hagyatéki végzésben szerepelő valamennyi, a szolgáltató által jogosulatlanul kezelt adat törlését. *(944/P/2007, 1390/P/2007, 1920/P/2007)*

Kifogásolták azt is, hogy a TIGÁZ olyan borítékban küldte ki a szabálytalan gázvételezésről szóló értesítést, amelyen nemcsak az érintett

neve és címe látszik, hanem a „tárgy" rovatban a „szabálytalan vételezés" szöveg is.

> Az adatvédelmi törvény alapján megállapítható, hogy adatkezelésnek minősül az, ha a címzett nevén és címén kívül bárki részére láthatóvá válik egyéb, a címzettre vonatkozó adat. Mivel jelen esetben az érintettek hozzájárulása hiányzik és az adatkezelésre törvényi felhatalmazás sincsen, ezért a panaszos által jelzett adatkezelést az adatvédelmi biztos aggályosnak tartja. A TIGÁZ adatvédelmi felelőse az adatvédelmi biztos megkeresésére válaszolva azt a tájékoztatást adta, hogy intézkedéseket tettek annak érdekében, hogy ez a jövőben még véletlenül se fordulhasson elő. Ezért a levél tárgy rovatában ezentúl csupán az „értesítés" szöveg lesz olvasható, hogy a „szabálytalan gázvételezés" szöveg véletlenül se kerülhessen az ügyben nem érintett fél számára láthatóvá. *(922/P/2007)*

A telefonos és az internetes ügyintézés kapcsán is számos beadvány érkezik évről-évre az Irodához. A TIGÁZ az internetes reklamációk kitöltésekor a „Fogyasztói sérelem, panasz bejelentő lap" elnevezésű internetes oldalon, – illetőleg a közüzemi szerződés megkötésekor is – több panaszos szerint túl sok adatot igényel.

> A gázszolgáltatók által kezelhető adatokat a földgázellátásról szóló törvény 39. § (5) bekezdése valamint 14/A. § (1) bekezdése tartalmazza. E két jogszabályhelyet együttesen kell alkalmazni a gázszolgáltatók által kezelhető adatok körének meghatározásához. Az adatvédelmi biztos álláspontja az, hogy a gázszolgáltatóknak nincsen törvényi felhatalmazása arra, hogy a fogyasztók személyi igazolványának számát, illetve telefonszámát kezelhessék. Természetesen, amennyiben a fogyasztó hozzájárul, és a szolgáltató feladatainak ellátásához szükséges, úgy lehetőség van arra, hogy ezt a két adatot is kezeljék a szolgáltatók. A biztos állásfoglalását a TIGÁZ elfogadta.
>
> A többi adatot azonban, amelyet a TIGÁZ a közüzemi szerződések megkötésekor igényel, jogszerűen kezelheti a fentiek értelmében, így a fogyasztók anyja nevét is, a fogyasztók beazonosíthatósága, és az esetleges követelések érvényesítése céljából. A bejelentőlapon ezen többletadatok megadásának elsősorban biztonsági célja van. Azért nem elég például pusztán az ügyfél-azonosító megadása, hogy senki ne tegyen valótlan bejelentést egy olyan ügyfél-azonosítóval, amely nem az övé. A TIGÁZ a sérelmezett bejelentőlapon csak olyan adatokat igényel kötelező jelleggel, amelyet a fogyasztó már amúgy is megadott a

közüzemi szerződés megkötésekor. A telefonszámot, illetve az e-mail címet pedig vagylagosan igényli a szolgáltató abból a célból, hogy a fogyasztót a panasz kivizsgálásának eredményéről értesíthesse. Ezen okokból a panaszos által sérelmezett adatkezelést az adatvédelmi biztos nem találta jogellenesnek. *(761/P/2007, 1339/P/2007)*

Az egyik szolgáltató egy panaszostól adatpontosításra hivatkozva kérte be házassági anyakönyvi kivonatának másolatát. A szolgáltató adatvédelmi felelőse azt a tájékoztatást adta, hogy ügyintézői hiba történt, amikor az okiratok fénymásolásra kerültek, illetve amikor a házassági anyakönyvi kivonat bekérését tartalmazó levél elkészült és kipostázták. *(310/P/2007)*

Több állampolgár kifogásolta azt is, hogy a szolgáltatók nevében más cégek járnak el, és végeznek például helyszíni műszaki szemlét lakásukban. A panaszosok attól félnek, hogy ezen cégek információgyűjtést folytatnak, illetve kifogásolják, hogy a szolgáltató az adataikat átadta.

Ezek a cégek a közüzemi szolgáltatók megbízásából folytatnak ellenőrzési, számlázási, karbantartási, stb. tevékenységet. Ennek során kizárólag adatfeldolgozást végeznek. 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. Fontos megjegyezni, hogy az adatfeldolgozás is csak akkor törvényes, ha az adatkezelő előzetesen tájékoztatja az érintetteket arról, hogy személyes adataikat ki fogja kezelni, illetve feldolgozni. *(1266/P/2007)*

Eltérően kell megítélni azt, ha az adatok továbbítását követően adatkezelés is történik, vagyis amikor az átvevő cég már nem csupán adatfeldolgozást folytat. Ehhez szükség van az érintett hozzájárulására, vagy törvény felhatalmazására. Ilyen felhatalmazást a közüzemi szolgáltatók tevékenységét szabályozó törvények részben adnak, így például a villamos energiáról szóló törvény alapján követeléskezelő cégek, a fogyasztási helyek műszaki kivitelezését, felülvizsgálatát, ellenőrzését végző cégek, illetve ügyfélszolgálati tevékenységet végző cégek részére továbbíthatók adatok.

Több beadványban kifogásolták az állampolgárok, hogy annak ellenére kell szemétszállítási díjat fizetniük, hogy nem veszik igénybe ezt a

szolgáltatást, valamint érdeklődtek, hogy milyen jogszabály hatalmazza fel az önkormányzatokat arra, hogy az állampolgárok adatait a hulladékkezelést végző közszolgáltató cégeknek átadják.

A Hgt. 23. §-a határozza meg a települési önkormányzat képviselő-testületének kötelezettségeit. E szerint a képviselő-testület önkormányzati rendeletben állapítja meg többek között a közszolgáltatás keretében kötött szerződés létrejöttének módját, valamint a közszolgáltatás igénybevételének – jogszabályban nem rendezett – módját és feltételeit, valamint a közszolgáltatással összefüggő személyes adatok (közszolgáltatást igénybe vevő neve, lakcíme, születési helye és ideje, anyja neve) kezelésére vonatkozó rendelkezéseket. Ha egy önkormányzat rendelete alapján a tulajdonos köteles a szolgáltató által nyújtott helyi közszolgáltatást igénybe venni és a közszolgáltatás díját megfizetni, az adatkezelés jogszerű, mivel azt törvény felhatalmazása alapján, az abban meghatározott körben helyi önkormányzat rendelete rendeli el. *(1437/P/2007)*

Társasházak, lakásszövetkezetek

A tavalyi évhez képest a társasházak, illetve a társasházak közös képviselőinek adatkezelését kifogásoló panaszbeadványok száma jelentősen nem változott. Az állampolgárok továbbra is számos panaszt fogalmaztak meg olyan üggyel kapcsolatban, amelyre a társasházakról szóló 2003. évi CXXXIII. törvény (továbbiakban: Tht.) hiányosságai miatt az adatvédelmi törvény adatkezelésre vonatkozó értelmezését kell alapul venni. Az ügytípusok tekintetében sem történt lényeges változás. Megjelent azonban egy, a társadalom jelentős hányadát érintő kérdéskör, a gázfogyasztás és gázár-támogatás kapcsán felmerülő adatkezelési kérdések tisztázása.

A legtöbb beadvány azonban továbbra is a közös költséggel tartozók személyes adatainak nyilvánosságra hozatala kapcsán érkezett, mellyel összefüggés mind a közös képviselők, mind a társasházban lakók kérték a biztos állásfoglalását annak érdekében, hogy a jogellenes adatkezelés megelőzhető, illetve megszűntethető legyen.

A beadványozókat az ilyen jellegű ügyekben a biztos arról tájékoztatta, hogy a nem fizető, illetőleg a hátralékkal rendelkező tulajdonostársak személyére vonatkozó adatokat törvényi felhatalmazás hiányában nem lehet nyilvánosságra hozni, azokat csak az érintett tulajdonostár-

sak ismerhetik meg. Ez történhet például a könyvelés megtekintésével, vagy úgy, hogy zárt (kizárólag a tulajdonostársak részvételével megtartott) közgyűlésen ismertetik a hátralékkal rendelkező tulajdonostársak nevét. Amennyiben a közös költség fizetésében hátralékkal rendelkező tulajdonostársak adatait ily módon ismertették, nem állapítható meg a személyiségi jogok sérelme. *(26/P/2007, 97/K/2007, 118/P/2007, 134/K/2007, 209/K/2007, 1433/P/2007, 1777/K/2007, 2644/K/2007)*

Jelentős számban érkeztek beadványok a társasházban létesítendő kamerarendszerek, illetve a már működő kamerák működtetésének jogszerűségével kapcsolatban. Bizonyos esetekben maga a közös képviselő kér előzetesen állásfoglalást annak érdekében, hogy a kamerarendszer üzemeltetése ne ütközzön semmilyen jogszabályba. Sokszor azonban a felháborodott lakók írnak, akik a hozzájárulásuk nélkül működő kamerák létjogosultságát kérdőjelezik meg.

A kamerás megfigyelés útján számos személyes adat birtokába jut a megfigyelő rendszer üzemeltetője (ki mikor hagyja el a házat, mikor érkezik vissza, kivel, egészségi állapotra vonatkozó adatokat ismerhet meg stb.), így a rögzítés révén adatkezelővé válik, tevékenysége az adatvédelmi törvény fogalomrendszerében a fentiek szerint adatkezelésnek minősül. Az adatvédelmi törvény 3. § (1) bekezdése alapján személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény, vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete elrendeli. Sem a Tht., sem a lakásszövetkezetekről szóló 2004. évi CXV. törvény nem tartalmaz olyan rendelkezést, mely a társasház vagy lakásszövetkezet képviseletét ellátó személyt, vagy mást arra hatalmazna fel, hogy a társasház területén, illetve az oda vezető úton megfigyelést végezzen. Ilyen rendelkezés más hatályos jogszabályban sem lelhető fel. Törvényi felhatalmazás hiányában az adatkezeléshez az érintettek hozzájárulására van szükség: minden lakónak szükséges a hozzájárulása ahhoz, hogy a közös használatú magánterületen, mint amilyenek a garázs, illetve a bejárati ajtók előtti tér, képfelvételeket rögzíthessen a rendszer, valamint jól látható, még a belépés előtt elolvasható helyre el kell helyezni azt a figyelmeztetést, hogy az adott terület kamerával megfigyelt. Ezenfelül tájékoztatást kell adni az érintett kérésére legalább a következő körülményekről: az adatkezelés céljáról, az adatok tárolásának idejéről és módjáról, az adatkezelő személyéről, elérhetőségéről, valamint az érintett azon jogáról, hogy az adatkezelőtől tájékoztatást kérhet személyes adatai kezeléséről, valamint

kérheti a róla készült felvétel törlését, illetve tájékoztatni kell jogorvoslati lehetőségeiről is. Fontos még, hogy a kamera látómezeje nem irányulhat közterületre. *(916/P/2007, 1309/P/2007, 1664/K/2007, 2163/P/2007, 2179/P/2007, 2247/K/2007, 2310/P/2007)*

Az előző évekhez képest valamivel kevesebb beadvány érkezett abban a kérdéskörben, hogy a közös képviselő mely felhatalmazás alapján, valamint mely cél elérése érdekében vezethet a lakókról lakónyilvántartást.

A Tht. 22. §-a alapján a szervezeti-működési szabályzat előírhatja, hogy a tulajdonostárs köteles a közös képviselőnek, vagy az intézőbizottság elnökének bejelenteni egyes adatokat (többek között az ingatlan-nyilvántartás nyilvános adatait), melyekről a közös képviselő vagy az intézőbizottság elnöke nyilvántartást vezethet; a törvény a kezelhető adatkört és az adatszolgáltatás szabályait is pontosan meghatározza. Vagyis a szervezeti-működési szabályzat a jogszabállyal összhangban rendelkezhet lakónyilvántartás vezetéséről, de az adatkör nem haladhatja meg a törvényben meghatározottakat. Így például a tulajdonostársaktól nem igényelhető születési helyük, ideiglenes lakcímük, munkahelyük, adóazonosító jelük, TAJ-számuk, telefonszámuk. *(497/P/2007, 998/P/2007, 2331/P/2007)*

A gázfogyasztás, valamint a gázár-támogatás kapcsán felmerülő fogyasztási és számlázási adatok tekintetében számos lakóközösség állapodik meg arról, hogy azokat a társasház közös képviselője kezeli az összes lakó tekintetében. Ennek kapcsán érkeztek beadványok azt kifogásolva, hogy mind a közös képviselő, mind a gázszolgáltató a személyes adatok védelmére való hivatkozással megtagadta a számlázásra vonatkozó adatok kiadását.

Az adatvédelmi törvény 2. § 1. pontja szerint személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. Az említett panaszbeadványokhoz kapcsolódóan megállapítható, hogy a név és a tartozásra vonatkozó adatok személyes adatnak minősülnek. Az adatvédelmi törvény 12. § (1) bekezdése alapján az érintett kérelmére az adatkezelő köteles tájékoztatást adni az általa kezelt adatokról. Adatszolgáltatás iránti kérelmére annak benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül kell a társaságnak (vagy a közös képviselőnek) tájékoztatást adnia a kezelésében lévő, az érintett sze-

mélyére vonatkozó adatokról. Ügyelni kell azonban arra, hogy a betekintés kizárólag az érintett saját adataira vonatkozzon, a társasházban lakók személyes adatai ilyen módon nem ismerhetőek meg. *(645/P/2007, 651/K/2007, 1837/P/2007, 2556/P/2007)*

Parkolási társaságok

Ebben az évben először kerül bele a beszámolóba a parkolási társaságok adatkezelésével kapcsolatos fejezet, mivel egyre több panaszbeadvány érkezik e tárgyban is. Bár a panaszosok beadványai sokszor adatvédelmi szempontból nem megfogható kérdésekre irányulnak,– így például arra, hogy miért évekkel később értesülnek a kérdéses parkolási eseményről – mindenképpen érdemes áttekinteni e terület jogi aspektusait.

Tekintettel a parkolási társaságok sokszor törvénysértő gyakorlatára, az értesítési határidő szabályozásra, az elévülési határidő pedig lerövidült az általános öt éves elévülési időhöz képest: a közúti közlekedésről szóló 1988. évi I. törvény 15. §-a 2006. december 22-i hatállyal módosult. Közút területén vagy a közút területén kívüli közterületen létesített, illetőleg kijelölt várakozóhelyen a közút kezelője díj és pótdíj szedését rendelheti el. Amennyiben az előbbiekben meghatározott díjat nem fizették meg, a közút kezelője vagy az általa megállapodás alapján megbízott gazdálkodó szervezet a létesített, illetőleg kijelölt várakozóhely jogosulatlan úthasználatának időpontjától számított 60 napos jogvesztő határidőn belül köteles postára adni a díj- vagy pótdíjfizetési felszólítást. A díj- és a pótdíjfizetési kötelezettség egy év alatt évül el. A díj és a pótdíj után késedelmi kamat nem követelhető. *(1206/P/2007, 1424/P/2007)*

A szabálytalan parkolásokhoz köthető tartozások igényérvényesítésének megítélése elsődlegesen szintén nem adatvédelmi kérdés. Annak eldöntése, hogy a társaság érintettekkel szemben felmerült igénye jogos követelés-e, nem tartozik az adatvédelmi biztos hatáskörébe, és az egyes adatkezelési kifogások a követelés érvényesíthetőségét nem befolyásolják.

A szabálytalan parkolás megtörténtének ténye és a gépjármű vezetője közötti kapcsolatot a forgalmi rendszám teremtheti meg. A rendszám tehát nem tekinthető minden esetben személyes adatnak, csak

akkor, ha a rendszámmal meghatározott természetes személy (tulajdonos, üzemben tartó) kapcsolatba hozható; elegendő a személyes adat minőséghez az is, ha a kapcsolat helyreállításának lehetősége fennáll.

A rendszám – az adatvédelmi törvény rendelkezéseinek alapulvételével – személyes adatnak tekinthető, ha a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEKKH) gépjárműnyilvántartása alapján megállapítható, hogy a gépkocsinak mely természetes személy a tulajdonosa (üzembentartója). A Kknyt. 19. n) pontja alapján a parkolási szolgáltatást nyújtó társaságok a parkolási díj meg nem fizetése esetén a díj és a pótdíj behajtása érdekében igényelhetik a járműtulajdonos személyes adatait a nyilvántartásból.

Attól az időponttól kezdve, hogy a nyilvántartásban fellelhető adatok alapján a magánszemély tulajdonos (üzembentartó) kiléte ismertté válik az adatkezelő előtt, az adattársítás folytán a parkolás helyszínére és időpontjára vonatkozó információk is személyes adatnak tekinthetők, és a parkolási társaság követelésének érvényesítése érdekében a Kknyt. felhatalmazása alapján és a Polgári Törvénykönyv rendelkezéseire is tekintettel kezelheti ezeket a személyes adatokat. *(41/P/2007, 413/P/2007)*

A Kknyt. is lehetőséget biztosít arra, hogy az érintett személy megtilthassa, illetve korlátozhassa személyes adatainak kiszolgáltatását, azonban erre csak abban az esetben van lehetőség, ha az adatszolgáltatás nem törvényen, nemzetközi szerződésen vagy nemzetközi kötelezettségvállaláson alapul. Tekintettel arra, hogy a járműnyilvántartásból a parkolási szolgáltatást végző társaság részére történő adatszolgáltatás a fent idézett törvényen alapul, az ilyen célú adatszolgáltatást, „adatkiadást" az érintett nem tilthatja meg. *(384/P/2007)*

A tájékoztatási kötelezettséggel kapcsolatban több panaszbeadványban érdeklődtek az állampolgárok arról is, hogy kötelessége-e kiadni a parkolótársaságoknak a parkolási eseményről készült fényképet.

Az adatvédelmi törvény rendelkezéseiből nem következik, hogy az adatkezelő kizárólag oly módon tehet eleget tájékoztatási kötelezettségének, ha a birtokában lévő fényképet bemutatja az érintettnek. Eljárása akkor is megfelel az adatvédelmi törvény előírásainak, ha a fényképen megjelenő információkról (rendszám, parkolás helye, ideje) írásban, a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül tájékoztatást ad. *(41/P/2007, 413/P/2007)*

A legtöbb panasz a Centrum Parkoló Kft.-vel kapcsolatban érkezik a hivatalhoz. A Centrum Kft. azonban megkereséseinket igen nagy arányban hagyja válasz nélkül. Volt olyan vizsgálat, amely során kiderült, hogy a Centrum Kft. ügyben eljáró ügyintézője a rendelkezésre álló adatokból nem kellő körültekintéssel és alapossággal hozott döntést, a panaszos azonban nem tudta jogait érvényesíteni. A biztos „közbenjárására" a Centrum Kft. kijelentette, hogy az érintett pótdíjazási eseményei alapján fennálló követelését nem kívánja érvényesíteni a gépjármű tulajdonosával szemben. *(896/P/2007)*

Egy másik esetben az okozott problémát, hogy a panaszos nem a teljes tartozás összegét teljesítette a Centrum Kft.-nek: az 1320,- Ft-os tartozás helyett csak 1319,- Ft-ot fizetett be.

> A cég ügyvezetőjének tájékoztatása értelmében így a rendszer a panaszost továbbra is adósként tartotta nyilván, és az akkor hatályos 38/1993 (XII. 27.) Fővárosi Közgyűlési Rendelet 28. §-ának megfelelően került felszámításra az időmúlásra tekintettel a parkolási díj és a pótdíj. Ennek megfelelően a panaszos tekintetében a Centrum Parkoló Rendszer Kft. – a befizetett összeg, 1319,-Ft beszámításával – 4401,- Ft összegű tartozást tartott nyilván, és ezzel az összeggel került engedményezésre a követelés. Ebben az esetben sajnálatos módon, mivel az adatkezelés jogalapja nem szűnt meg, ezért az formálisan jogszerű. Az már más kérdés, hogy ez mennyiben felel meg a tisztességes adatkezelés elvének. *(1391/P/2007)*

Idén ismételten előkerült a Centrum Kft. egy, az interneten keringő, 2002. május 16-án kelt „Belső utasítás" elnevezésű dokumentuma. Ez a dokumentum arra kötelezi a Centrum Kft. munkatársait, hogy a fizető övezeten kívül parkoló gépjárművek adatait is gyűjtsék össze, továbbá azokat is pótdíjazzák. A felszólítást a fizető övezet egy jellemző pontjára kell munkavállalóiknak kiállítaniuk. Az utasításban hivatkozás található korábbi, hasonló tartalmú utasításokra is.

> A cég ügyvezetője válaszlevelében kifejtette, hogy már évekkel ezelőtt megtették a szükséges jogi lépéseket az ügyben: 2002. április 8-án bejelentést tett a Budapesti Rendőrkapitányságon, 2003. május 14-én pedig feljelentést tett ismeretlen tettes ellen a Budapest VI-VII. kerületi Rendőrkapitányságon. Az ügyvezető kijelentette továbbá, hogy ilyen tartalmú utasítás nem készült a társaságnál, továbbá, hogy ennek az interneten megjelent iratnak semmilyen valóságtartalma nin-

csen, az azt aláíró személy pedig soha nem dolgozott a Centrum Parkoló Rendszer Kft.-nél. *(499/P/2007)*

Több társasággal kapcsolatban is érkezett panaszbeadvány azt kifogásolva, hogy ezen cégek rendszeresen szólítják fel őket pótdíjfizetésre, holott az adott gépjármű már évek óta nem az ő tulajdonukban van. Ezek oka jelen esetben az volt, hogy az állampolgárok elfelejtették, illetve késve teljesítették bejelentési kötelezettségüket a hatóságok felé.

A közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról szóló 35/2000. (XI. 30) BM rendelet alapján a gépjármű tulajdonjogában bekövetkezett változás bejelentését a változástól számított 15 napon belül, a régi tulajdonos a tulajdonjog változásáról készült okirat benyújtásával (megküldésével) teljesíti. Az új tulajdonos pedig a Kknyt. 33. §-ának (1) bekezdése alapján a nyilvántartásba bejegyzett adatok módosítására okot adó körülmény bekövetkeztétől számított 15 napon belül köteles bejelenteni a bejegyzésre jogosult hatóságnál a jármű tulajdonjogának, a tulajdonos az üzembentartó személyének, valamint a járműokmányokban megjelölt műszaki adatoknak a változását. Ezekben az esetekben a parkolótársaságok nem követtek el jogsértést, hiszen a téves információkon alapuló adatszolgáltatás az érintettek mulasztására volt visszavezethető. *(438/P/2007, 1057/P/2007)*

A Szegedi Parkolási Társasággal összefüggésben az érintett azt kifogásolta, hogy a parkolási bérlet vásárlása alkalmával a lízingcég és közte létrejött lízingszerződésről a Szegedi Parkolási Társaság ügyintézője – hozzájárulása nélkül – másolatot készített.

A vizsgálat során a biztos megállapította, hogy a lízingszerződésében szereplő adatok kezelése a bérlet kiállításához nem szükséges. Természetesen elfogadható, hogy amennyiben a forgalmi engedélyben a gépjármű-tulajdonosként a kedvezményes parkoló-bérlet vásárlója nincsen feltüntetve, úgy a kedvezményre való jogosultságát igazolja, például a lízingszerződés bemutatásával. Az okmány bemutatásán és a kedvezmény igénybevételéhez feltétlenül szükséges adatok feljegyzésén túl azonban e szerződések másolati példányainak tárolása, és ily módon a benne foglalt egyéb személyes adatok kezelése ellentétes az adatvédelmi törvény rendelkezéseivel, különösen, ha ehhez az érintett hozzájárulását sem adta. A fentiek alapján a cég ügyvezetőjét felszólította az adatvédelmi biztos arra, hogy a szerződés másolati példányát

semmisítsék meg, és adatkezelésük során csak a szükséges adatok kezelésére szorítkozzanak. *(65/P/2007)*

Követelés-kezelők

Az egyes polgári jogi igények megítélése elsődlegesen nem adatvédelmi kérdés. Az eljárás azonban szükségszerűen adatkezeléssel is jár, és az esetlegesen megvalósuló adattovábbítások, valamint az érintettek információs önrendelkezési jogának gyakorolhatósága olyan kérdéseket vet fel, amelyek az adatvédelem területére tartozhatnak. Az egyes adósságbehajtással, vagy szebb szóval: követelés-kezeléssel foglalkozó cégek adatátvételének jogalapja különböző lehet, attól függően, hogy az alapkövetelés jogosultja maga, vagy jogi képviselő útján próbálja érvényesíteni a követelést, engedményezi a követelést, esetleg a szerződésben foglaltak alapján ruházza át követelését adósságkezelő cégre. Az évek óta visszatérő problémával 2000-ben már foglalkozott egy ajánlás, de az esetek növekvő száma, valamint az elmúlt évek jogszabály-változásai miatt elengedhetetlen annak újbóli tárgyalása.

A kérdés megítélése nagymértékben függ attól, hogy a követeléskezelők tevékenységét adatkezelésnek, vagy adatfeldolgozásnak tekintjük. Az adatvédelmi törvény alapján polgári jogi jogviszonyban adatkezelőnek a követelés jogosultja tekinthető. A követeléskezelők az esetek túlnyomó többségében az adatokon érdemi műveleteket végeznek, azokat saját tevékenységi körükön belül döntéshozatalra használják fel (követelés lejártának vizsgálata, jogérvényesítés módja, egyeztetés, fizetési feltételek meghatározása stb.). Ebben az esetben az adatok átvétele adattovábbításnak, a tevékenység adatkezelésnek minősül, amelyhez törvény felhatalmazása, vagy az érintett hozzájárulása szükséges.

A követeléskezelő három jogcímen végezheti a tevékenységét. A személyes adat átadható követeléskezelőnek, ha ahhoz az érintett hozzájárult. A hozzájárulás megadható előzetesen, a követelés alapjául szolgáló szerződésben is. A másik lehetséges jogalap törvény felhatalmazása. Nincs olyan törvény, amely általában hatalmazná fel a követeléskezelőket adatok átvételére, így csak azon adatkezelők számára végezhetik – adatkezeléssel járó – tevékenységüket, amelyeket az adatok átadására törvény felhatalmaz. A 2000. évi ajánlás óta számos ilyen törvényi felhatalmazás született: az Eht., a hitelintézetekről és a

pénzügyi vállalkozásokról szóló törvény, a távhőszolgáltatásról szóló törvény, a villamos energiáról szóló törvény, a földgázellátásról szóló törvény, a tőkepiacról szóló törvény egyaránt felhatalmazzák a hatályuk alá tartozó szervezeteket arra, hogy követelés-kezelőknek személyes adatokat adjanak át.

A fentieken túlmenően a követelés érvényesítésének a hatályos magyar jog által elismert eszköze a szerződéssel megbízott ügyvéd közreműködésének igénybevétele. Az ügyvéd törvényi felhatalmazás alapján jogszerűen juthat hozzá megbízójától az adós személyes adataihoz, ehhez tehát az adós hozzájárulása nem szükséges. Lehetőség van emellett polgári jog szerint a követelés másra történő átruházására, szerződéssel. A Ptk. szabályozza az engedményezés jogintézményét: az engedményezésre vonatkozó szabályok lehetővé teszik a természetes személy adósok adatainak átadását (Ptk. 328. § bek.). Az engedményezés annyiban különbözik a hagyományos követeléskezeléstől, hogy ebben az esetben a jogosult személyében változás történik.

Bár az engedményezés szabályai egyértelműnek tűnnek, mégis előfordul olyan eset, amikor azokat tévesen alkalmazzák. Lényeges, hogy a Ptk. alapján az engedményezésről az érintettet értesíteni kell; a kötelezett az értesítésig jogosult az engedményezőnek teljesíteni.

Egy konkrét ügyben a biztos megállapította, hogy a panaszos jogszerűen teljesítette a követelést a közüzemi szolgáltatónak a követeléskezelő helyett, mivel a két cég egyike sem értesítette időben az engedményezésről. Erre tekintettel a panaszos kérheti mindkét cégtől személyes adatai törlését. *(596/P/2007)*

A panaszok mögött nem egy esetben áll az, hogy az adós időhúzás céljából kér vizsgálatot, sokszor találkozunk azonban jogellenes adatkezeléssel is. Az adósságkezelő cégek gyakran alkalmazzák azt a kifogásolható módszert, hogy az érintettet nem csak a jogszerűen kezelt adatokat használva próbálják meg elérni, hanem egyéb – sokszor ismeretlen – forrásból származó személyes adatain keresztül keresik meg, zaklatják. Még ha az adósságbehajtó cég az adós alapkövetelésből származó személyes adataihoz jogszerűen jut is hozzá, a követelés átruházása nem teremt jogalapot az adósságkezelő cégnek további személyes adatok gyűjtésére, kezelésére. *(1795/P/2007)*

Jogellenes valamely személy tartozásával kapcsolatban más személynek (például a szomszédnak) a megkeresése, mivel ezzel az adatkezelő megsérti nem csak az adós jogait, de a megkeresett személyét is, aki a követelésnek semmilyen formában nem részese. Az ilyen jellegű, sokszor véletlennek mondott megkeresések mögött egy igencsak kétes cél is áll. A követelés-kezelő azáltal próbálja az adóst fizetésre késztetni, hogy szomszédai, munkatársai tudomására hozza a tartozás tényét, rossz színben tüntetve fel az érintettet.

Számos esetben érkezett panasz arra vonatkozóan, hogy az érintettek számukra ismeretlen tartozással kapcsolatban kaptak felszólító sms-t. Ezeket a követelés-kezelő a mobilszolgáltató korábbi ügyfelének szánta. Ez a gyakorlat azért aggályos, mert az adatvédelmi törvény az adatok minőségének követelményei között előírja, hogy a kezelt adatoknak pontosnak, teljesnek és időszerűnek kell lenniük.

> A távközlési szolgáltató adatvédelmi felelőse az adatvédelmi biztos megkeresésére írt válaszlevelében elmondta, hogy vizsgálatuk eredményei alapján azt feltételezik, hogy a követelés-kezelő a fizetésre felszólító sms-t a korábbi ügyfélnek szánta. A korábban már mások által is használt telefonszámok esetében gyakran előfordul, hogy az adott telefonszámnak az új előfizetőhöz rendelését követően akár egy-két évvel később is érkeznek az új előfizető hívószámára a régi előfizetőnek szánt hívások, közlemények olyan felektől, akik számára az adott telefonszám még a régi előfizetéshez/előfizetőhöz kapcsolhatóan váltak – jogszerűen – ismertté, és akik nem tudják, hogy időközben e telefonszámot már más kapta meg. A konkrét esetben felajánlottak egy térítésmentes számcserét a panaszos részére, és a követelés-kezelő is haladéktalanul intézkedett a telefonszám törléséről. *(458/P/2007, 698/P/2007)*

Számos beadványban érdeklődnek az állampolgárok arról, hogy a még le nem járt, illetőleg a már elévült követelések engedményezhetőek-e. Bár ez a kérdés elsődlegesen nem adatvédelmi jellegű, felmerül annak kérdése, hogy – a célhoz kötöttség elvéből adódóan – az igény érvényesíthetőségének megszűnését követően kezelhetők-e az adatok.

> Ha a jogosult a jogszabályban meghatározott idő alatt nem érvényesíti az igényét, és a jogszabály jogvesztést nem mond ki, a követelés a jogszabályban meghatározott idő elteltével elévül. Ez azt jelenti, hogy a követelést bírósági úton ugyan nem lehet érvényesíteni, maga a köve-

telés azonban nem szűnik meg. Az önként teljesített szolgáltatás azzal az indokkal sem követelhető vissza, hogy a kötelezett a teljesítéskor a követelés elévüléséről nem tudott. A Ptk. ezért a bírósági úton nem érvényesíthető követelések körében rendelkezik az elévült követelésekről is. Elvileg elévült követelés is engedményezhető, a kötelezett azonban az engedményes követelésével szemben az elévülésre ugyanúgy hivatkozhat, mint az engedményezővel szemben. Ha azonban az engedményezéskor az elévülési határidő még nem járt le, az engedményezés az elévülést megszakítja, mert a kötelezettnek az engedményről való értesítése a követelésről való rendelkezést fejezi ki. A bíróság az elévülést nem köteles hivatalból figyelembe venni, ha nem történik arra hivatkozás. *(1429/K/2007, 571/P/2007)*

További érdekes ügyek

Kamerák

A képfelvevő berendezések elterjedése mindenki számára nyilvánvaló jelenség, közterületen, magánterületen egyaránt. Természetesnek tűnik a kamerák általános alkalmazása, a képfelvételek rögzítésével járó jogkövetkezmények terén azonban gyakran teljes tájékozatlansággal találkozunk. A kamerák működésbe helyezését nagy várakozás övezi, ugyanakkor annak fogyatékosságai, kijátszhatósága csak később válik világossá a telepítő számára. Ekkorra azonban már nagy költséggel, és az esetek jelentős részében jogellenesen, kiépült a kamerarendszer. Utóbb már túl későn szembesül a beruházó azzal, hogy befektetése nem csak nem hatékony, hanem a telepítés körülményei következtében, például magánfél által közterületre irányuló megfigyelés esetén jogellenes is. Minden lehetséges fórumon hangsúlyozzuk: csak a szakszerűen és jogszerűen telepített és üzemeltetett képfelvevők képesek az eredetileg kitűzött cél (például személy- és vagyonbiztonság) elérésére.

A jogkövető magatartás fontosságát nem csak a jól látható, hanem a tulajdonképpen rejtett módon üzemelő képfelvevők kapcsán is ki kell emelnünk. A technikai fejlődés eredményeképpen ma bárki olyan eszközök birtokába juthat, amelyekkel néhány évtizeddel ezelőtt csupán a titkosszolgálatok rendelkeztek. Meglehetősen olcsón beszerezhető berendezések állnak a kíváncsi munkáltató, az alkalmi, esetleg hivatásos

„paparazzo" vagy éppen a szomszédos öltözőbe bekandikáló diák számára. Nem vitathatjuk, hogy ezeket az eszközöket nem csak az említett visszaélésekre, hanem alapvetően rendeltetésszerűen használják, a szórakoztatást, tájékoztatást szolgálják. Addig, amíg a képfelvevők alkalmazása a szűken vett családi-baráti körben széles körben elterjedt, szokásos használaton nem megy túl, az adatvédelmi törvény tárgyi hatályán kívül esőnek tekinthetjük az általuk végzett rögzítéseket, hiszen a törvényt nem kell alkalmazni a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire.

Attól a ponttól kezdve azonban, amikor a felhasználó kilép ebből a felhasználási körből, a rögzített vagy világhálón közvetített, arcok felismerését lehetővé tevő felbontású képek már az adatvédelmi törvény védelme alá esnek. Arra kell felhívnunk a figyelmet, hogy a felvétel készítője, illetve közvetítője tartozik felelősséggel az elvégzett műveletek jogszerűségéért. Ez a felelősség magában foglalja az adatkezelőt terhelő összes felelősséget és kötelezettséget, az érintettek tájékoztatásától kezdődően egészen az esetleges kártérítési kötelezettségig. A képfelvevő telepítésére készülőket ezért minden esetben arra figyelmeztetjük, hogy gondolják végig, eleget tudnak-e majd tenni kötelezettségeiknek.

Az adatvédelmi törvény főszabálya szerint az adatkezelés jogalapja az érintett hozzájárulása vagy törvényi szabályozás lehet. Az érintetti hozzájárulás bizonyos élethelyzetekben rendkívül vitatott. Kétséges, hogy önkéntes hozzájárulást lehet-e például várni egy munkavállalótól, diáktól, egészségügyi intézménybe belépő személytől akkor, amikor gyakorlatilag nincsen választási lehetősége abban, hogy az adott épületbe, területre stb. belépjen. A kamerák által rögzített vagy közvetített képek esetében a legtöbbször az érintetti hozzájárulás a jogalap, amely az említett példákon túl is gyakran „billeg". Ezért üdvözöljük azokat a törvényeket, amelyek bizonyos körben a kamerák működtetésének szabályait meghatározzák. Ezek a szabályok nagyban hozzájárulnak ahhoz, hogy az adatkezelő tájékozódhasson jogairól és kötelezettségeiről, illetve felkészülhessen az adatalanyok jogainak érvényesítésére irányuló kérelmek fogadására. Felügyeleti szempontból az adatvédelmi biztos munkáját szintén megkönnyítik, hiszen konkrét jogszabályok megszületése után az önkéntes jogkövetés könnyebben elérhető. 2005 végén lépett hatályba az úgynevezett „vagyonőr-törvény" (a személy- és vagyonvé-

delmi, valamint a magánnyomozói tevékenység szabályairól szóló törvény), amely az adatkezelők széles körére nézve írja elő a kamerázás feltételeit. A törvény kedvező hatásait az elmúlt években már érzékeltük.

Az elmúlt évben számos beadvány érkezett a különböző intézményekben, járműveken elhelyezett, illetve elhelyezendő térfigyelő kamerákkal kapcsolatban. Ezek közül a legtöbb a kórházakban, temetőkben, iskolákban, illetve a tömegközlekedési eszközökön felszerelt képfelvevő berendezésekkel foglalkozik. Az említett esetekben a térfigyelő kamerák bizonyos, jogi kategóriákkal nehezen körülírható határokat lépnek át, benyomulnak a megfigyeltek privát szférájába, érzékeny területeken „kutakodnak". Egy kórházban, temetőben, öltözőben elhelyezett kamera rögzíti az érintettek minden mozdulatát, cselekvését, viselkedését, egyébként is nehéz, kényelmetlen vagy intim helyzetben figyelik meg őket. A megfigyelés óhatatlanul személyekre, emberi magatartásokra, szokásokra, megnyilvánulásokra, illetőleg magára az emberi testre irányul, érzékeny élethelyzeteket rögzíthet. Az ilyen módon végzett megfigyelés behatol az érintett magánszférájába, és ezzel az emberi méltósághoz való jogot is sértheti. Minden esetben az ügy körülményeinek gondos vizsgálata alapján dönthető csak el, hogy a személy- és vagyonbiztonság, esetleg üzembiztonság indokolja-e a magánszféra ilyen mértékű szűkítését. Esetről esetre vizsgálandó, hogy a jogkorlátozás megfelel-e a szükségesség és arányosság alkotmányos követelményének.

A fenti célok elérésére olyan megoldás alkalmazását tartjuk elfogadhatónak, mely a legkevésbé sérti az érintett magánszféráját, emberi méltóságát. Ennek egyik módja lehet, hogy személyes jelenléttel – például biztonsági szolgálat felállításával – oldják meg a vagyonvédelmi, bűnmegelőzési feladatokat. Az is lehetséges, hogy olyan rendszert építenek ki, mely ugyan megfigyelést végez, de olyan felbontású képeket készít, amelyek nem teszik lehetővé a személyek azonosítását. Az adatkezelőnek minden esetben a lehető legnagyobb érzékenységgel kell eljárnia, a kamerák felszerelésére, felvételek rögzítésére csak a lehető legszűkebb körben kerülhet sor. Amennyiben alkalmazható olyan ésszerű beruházás révén beszerezhető eszköz, amely az elérni kívánt célt a térfigyelő kamerákkal összehasonlítva kisebb jogsérelmet okozva éri el, a térfigyelő rendszer telepítése, illetve üzemeltetése jogellenes.

A közterületi kamerázás a jelenleg hatályos jogszabályok szerint a rendőrség, valamint szűk körben a közterület-felügyelet kizárólagos joga. E két szerv közül is alapvetően a rendőrség él ezzel a felhatalmazással. Több éves tapasztalat alapján annak lehettünk tanúi, hogy az Rtv. vonatkozó szabálya nem ad ugyan lehetőséget a folyamatos rögzítésre, ezt a szabályt a rendőri szervek azonban meglehetősen rugalmasan értelmezték. Ennek okaként általában arra hivatkoznak, hogy a hatékony rendőri munkához szükség van a folyamatos rögzítésre, ugyanakkor az adatkezelésre vonatkozó törvényi szintű szabályozás hiányzik. Ebben a helyzetben az igazságügyi és rendészeti miniszterhez fordultunk annak érdekében, hogy hatáskörében eljárva gondoskodjon arról, hogy a rendőri szervek a hatályos szabályoknak megfelelő gyakorlatot alakítsanak ki, vagy tegyen javaslatot egy olyan szabályozásra, amely a rendőrség hatékony munkáját lehetővé tevő, az alkotmányos követelményekkel összhangban álló felhatalmazást tartalmaz. Jeleztük, hogy egy ilyen jogszabály-tervezetet készséggel véleményezni fogunk. Az említett jelzés alapján az Rtv. soron következő módosítása érintette a közterületi megfigyelés szabályait is. Ennek véleményezése során kifejtettük, hogy a rögzítéssel járó megfigyelés helyére és idejére vonatkozó döntést egy szakmai grémiumra kellene bízni, amelyben természetesen a rendőrség képviselőjének is helyet kell kapnia. A térben és időben korlátlan megfigyelésre szóló felhatalmazás nem állná ki az alkotmányosság próbáját.

Végül ki kell még térnünk a világhálón közzétett, valamint közvetített felvételekre. Az adatvédelmi törvény fogalom-meghatározása szerint nyilvánosságra hozatalnak minősül, ha az adatot bárki számára hozzáférhetővé teszik. Az adatvédelmi törvény egy másik definíciójának megfelelően adatkezelésnek számít többek között a nyilvánosságra hozatal is. Az adatvédelmi biztos korábbi állásfoglalásai, valamint a 2000-ben kiadott ajánlása sem tekinti adatkezelési műveletnek a puszta megfigyelést. A felvételek világhálón való elérhetővé tétele lényegi különbséget jelent a puszta megfigyeléshez képest. Felmerül a kérdés, vajon a megfigyelt képek internetes felületre történő továbbítását az idézett meghatározás szerint nyilvánosságra hozatalnak és ezáltal – a helyszíni jelenlétet helyettesítő megfigyeléssel ellentétben – adatkezelésnek kell-e tekintenünk? A kérdés azért is bír különös jelentőséggel, mert az ilyen módon történő közzététel a felvételeket bárki számára hozzáfér-

hetővé teszi, vagyis olyan személyek számára is lehetővé válik a megfigyelt területen történt események nyomon követése, akik erre egyébként nem lennének jogosultak. A számítógépes technika lehetőséget ad arra, hogy a felvételeket bárki rögzítse és aztán valamilyen ellenőrizhetetlen célra felhasználja. A további felhasználásra sem a felvételeken szereplő személyeknek, sem a felvételeket közvetítő, elhelyező személyeknek nincs befolyása. A kérdés megválaszolása a következő időszak egyik jelentős jogértelmezési feladata.

A nem valós idejű, hanem rögzített képek közzétételét illetően jogértelmezési nehézségek nem merülnek fel, hiszen az egyértelműen adatkezelési műveletnek (nyilvánosságra hozatalnak) tekintendő. Amennyiben valaki a világhálón csupán meghatározott személyek számára kíván bizonyos felvételeket elérhetővé tenni, egy olyan megoldást tartunk elfogadhatónak, ami keretek közé szorítja a hozzáférést. Azon távol lévő személyek részére, akik érdeklődnek a felvételek iránt, biztosítani lehet egy jelszót, amellyel csak a jelszót ismerők tudnak belépni a kijelölt oldalra, vagy az oldal bizonyos részeire. Ezzel az eljárással ki lehet zárni, hogy illetéktelen személyek is megtekinthessék, esetleg rögzíthessék a felvételeket. Fontos azt is megjegyezni, hogy az érintettek figyelmét ebben az esetben is fel kell hívni arra, hogy a felvett képeket az interneten közzéteszik, valamint tájékoztatni kell őket az adatkezelés egyéb körülményeiről is.

A képfelvevő berendezések alkalmazásával kapcsolatban a munka világából számos panasz, konzultációs beadvány érkezik. Ezek bemutatására fentebb, a „Munkáltatók" című fejezetben térünk ki bővebben. A társasházakat érintő beadványokat szintén külön fejezetben tárgyaljuk.

Az adatvédelmi átvilágításról

Bár a bevezetőben utaltunk arra, hogy jelen keretek között nem próbálkozunk meg hat év tendenciáinak értékelésével, egy érdekes jelenségre mégis fel kell hívni a figyelmet. Minden évben olvasható volt, hogy a magánszféra adatkezelései egyre nagyobb jelentőségre tesznek szert. Ez, az adatvédelmi biztos szemszögéből nézve azt jelenti, hogy a vizsgálatok egyre nagyobb része irányul a magánszférára. Eleinte ezek a vizsgálatok inkább panaszokon alapultak, azonban folyamatosan növekedett a konzultációs ügyek száma. Mára gyakorivá vált, hogy a

magánszféra adatkezelői, bankok, biztosítók, munkáltatók kérik az adatvédelmi biztos véleményét egy-egy konkrét kérdésről, vagy adatkezelésről. Valószínűleg a panaszügyek számának emelkedése volt az egyik olyan tényező, amely ráébresztette az érintett vezetőket arra, hogy az adatvédelemre oda kell figyelni. Nem csupán azért, mert az adatvédelmi biztos vizsgálódhat, hanem azért is, mert a jogellenes adatkezelés akár bírósági eljárást is maga után vonhat, és nem hagyhatók figyelmen kívül az esetenként igen szigorú felügyeleti szankciók sem. Nem elhanyagolható emellett a „negatív reklám", amely a jogellenes adatkezelés nyilvánosságra kerülése esetén okozhat kárt az adatkezelőnek.

A konzultációs ügyek mindig okoznak némi dilemmát. Ezek során ugyanis az adatvédelmi biztos lényegében tanácsot ad, így felmerülhet a kérdés: elfogadható-e, hogy a biztos ahelyett, hogy minden erejével a polgárok jogait védje – ami törvényes kötelessége –, ügyvédi munkadíjat spórol meg az adatkezelőnek? Nem vitatható, hogy a konzultációs kérdések nagy része összetett, igen bonyolult adatkezelési-adatfeldolgozási rendszert mutat be, melyek értékelése nehéz, és időigényes feladat. Látható az is, hogy nem egy esetben az adatkezelők az egyszerűbb és olcsóbb utat keresik a biztosnál. A kérdést ugyanakkor árnyalni is kell, hiszen a konzultációk a polgárok jogait is védik azzal, hogy a megtörtént jogsértések orvoslása helyett azok megelőzését segítik elő. Felmerül tehát a kérdés: hol húzódik az a határ, amelyen belül az adatvédelmi biztosnak meg kell válaszolnia a konzultációs kéréseket? A válasz nehéz, hiszen egyértelmű, éles határvonalak nem húzhatók. Vannak ugyanakkor olyan esetek, amikor a biztosnak inkább elutasítóan kell fellépnie. Erre példaként szolgálnak az olyan – sajnos gyakran előforduló – esetek, amikor az ügyvéd a megbízója kérdését egy az egyben átküldi, és követeli a gyors választ, lényegében a biztossal végeztetve el azt a munkát, amelyért a megbízási díjat megkapja.

A másik, gyakran előforduló kérdés az átfogóbb vizsgálatokhoz kapcsolódik. Egyre gyakrabban fordul elő, hogy nagyobb adatkezelők összetett adatkezelésekről, esetleg teljes adatkezelési rendszerükről kérnek állásfoglalást. Ez olyan mértékű munkát jelent, amelyet nem tudunk vállalni. Erre lehet megoldás a külföldön már bevett gyakorlat: az adatvédelmi átvilágítás, vagy más szóval adatvédelmi audit.

Az adatvédelmi audit csak hazánkban kevéssé ismert, más európai országokban kialakult gyakorlata, intézményrendszere van. Egyes államokban – pl. Németország – törvény rendelkezik róla, több helyen az adatvédelmi hatóság tevékeny részvételével valósul meg. Ez megjelenhet abban, hogy az adatvédelmi hatóság módszertant, keretrendszert dolgoz ki, segítséget nyújt a lebonyolításban, az értékelésben. Több országban az adatvédelmi hatóságok kiemelt tevékenysége az adatvédelmi audit, amely egyben jelentős bevételi forrás is. Az adatvédelmi audit nem idegen az adatvédelmi törvény rendelkezéseitől sem. A törvény az adatbiztonság körében előírja, hogy az adatkezelő köteles *„megtenni azokat a technikai és szervezési intézkedéseket, kialakítani azokat az eljárási szabályokat”*, melyek a szabályozási háttér által támasztott követelményeknek megfelelnek (Avtv. 10. § (1) bek.). Emellett egyes adatkezelők számára kötelezővé teszi a belső adatvédelmi felelős kinevezését – meghatározott feladatkörrel –, továbbá adatvédelmi és adatbiztonsági szabályzat készítését (Avtv. 31/A. §). Egyértelmű, hogy a törvény alapján kötelező szabályzat megalkotását nagyobb adatkezelőknél megelőzi valamilyen felmérés, és a szabályzat egyszerre szolgálja az adatvédelem és az adatkezelő érdekeit.

Hosszasan lehetne vitázni arról, hogy mely szervezeteknél célszerű időt és pénzt szánni az auditra. Az is érdekes kérdés, hogy milyen formában kell megvalósulnia egy auditnak, és milyen eredményt kell produkálnia. A legérdekesebb mégis talán az, hogy ki végezzen auditot?

Bár az adatvédelem minden gazdálkodó szervezetnél szerepet kap, nem mindenhol indokolt az, hogy nagy ráfordítással komplex auditra kerüljön sor. Ez leginkább akkor fontos, ha az adott szervezet tevékenysége döntően valamilyen adatkezelésen alapul, de indokolhatja az auditot az érintettek nagy száma, az adatkezelés mérete is. Elsősorban azon vállalatok tartoznak ide, melyek szolgáltatóként számos érintett (ügyfél) adatát kezelik. Az auditot indokoltabbá teszi az, ha nem csupán az érintettek száma nagy, de a kezelt adatkör is igen széles, esetleg változó. A másik fontos adatkezelési terület a munkaviszonyhoz kapcsolódik. Minden évben nagy arányt képviselnek vizsgálataink között a munkáltatókat érintő panaszok, konzultációk. Itt a fő nehézséget az jelenti, hogy míg a jogi szabályozás meglehetősen hiányos, a munkáltatói érdekek igen változatosak. A harmadik fontos terület egyes marketing tevékenységekhez kapcsolódik. Napjainkra a hagyományos postai úton bonyolódó direkt marketing háttérbe szorult, helyette a telemarketing, az e-mail marketing jut

fontos szerephez, az internet terjedése pedig újabb módszerek kialakulását eredményezi – elegendő itt a személyre szabott hirdetésekre gondolni.

Az audit iránya többféle lehet. Értékelés tárgya lehet az információk biztonsága, a hálózatvédelem, a „technikai" adatbiztonság. Az adatvédelmi biztos tevékenységét inkább a jogi megfelelés érinti, amely egy más felfogású auditot indokol. Nem kizárható természetesen a két terület együttes vizsgálata sem.

Míg külföldön, elsősorban Nyugat-Európában az adatvédelmi auditnak kialakult intézményei vannak – auditot végeznek szolgáltatásként gazdálkodó szervezetek, tanácsadó vállalkozások, illetve adatvédelmi hatóságok akár törvény alapján, esetleg díj ellenében, akár üzleti alapon –, hazánkban ez hiányzik. Az informatikai biztonság vizsgálatával számos vállalkozás foglalkozik, többnyire csak technikai szempontból. A jogi, szervezeti oldalról „közelítő" audit lefolytatására azonban nehezebb megfelelő személyt találni. Egyes tanácsadással foglalkozó vállalkozások már felismerték a kérdés fontosságát, így tevékenységi körük része az adatvédelmi szempontú átvilágítás és tanácsadás. Emellett – az adatkezelésekre vonatkozó szabályozás bonyolulttá válása és a hatékony jogérvényesítés intézményrendszerének kialakulása következtében – egyre több ügyvéd szakosodott kisebb-nagyobb mértékben adatvédelemmel kapcsolatos ügyekre.

Az adatvédelmi biztos pozíciójából adódóan sem auditra, sem egységes módszertan kialakítására nem vállalkozhat. Rámutathat viszont arra, hogy az ilyen jellegű tevékenységre igény van. Ezt szolgálja a honlapon is olvasható állásfoglalás. *(2585/H/2007)*

B. Közérdekű adatok

2007-ben az információszabadságot érintő ügyek száma az előző évhez képest jelentősen, mintegy 25-%-kal megnőtt. A 248 ügyből 114 volt panasz, 118 konzultációs kérdés, 7 esetben véleményeztünk szolgálati titokköri jegyzéket, 4 esetben indítottunk hivatalból eljárást és 5 egyéb ügyben kellett intézkednünk. Nem számítottuk az információszabadság ügyei közé azt a 22 beadványt, amelyben a biztos irodájának működésével, a korábban kiadott állásfoglalásokkal, ajánlásokkal kapcsolatban fordultak közérdekű adatigényléssel a hivatalhoz.

Az információszabadságot érintő ügyek indítványozók szerinti megoszlása az elmúlt három évben a következő volt:

	2005	2006	2007
Magánszemély	32%	58%	40%
Újságíró	10%	5%	14%
Maga az adatkezelő	32%	21%	22%
Civil szervezet	10%	7%	7%
Hivatalbóli eljárás	2%	3%	2%
Önkormányzati képviselő, polgármester	6%	1,5%	6%
Parlamenti képviselő	2%	1,5%	1%
Ügyvéd (valamely szervezet képviseletében)	-	-	1%
Gazdasági társaság	4%	1,5%	4%
Egyéb	2%	1,5%	3%

Az információszabadság szabályozása az Európai Unióban

Az ország uniós csatlakozása az információszabadság szempontjából elsősorban azt jelenti, hogy örvendetesen szaporodnak a többi tagállammal a szakmai konzultációk, és mind gyakrabban van módunk az európai jogalkotási folyamatokban részt venni. Az Európai Unió információszabadságra vonatkozó jogrendjének két fő területe: az Unió intézményeinek nyilvánosságát előíró szabályozás, valamint a tagállamok belső szabályozásának fő

kereteit meghatározó irányelvek. 2007-ben mindkét területet érintően állást kellett foglalnunk.

> Az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való hozzáférésről szóló 1049/2001/EK Rendelet (Rendelet) majdani módosítását előkészítő, a Bizottság által vitára bocsátott Zöld Könyvvel kapcsolatosan a Külügyminisztérium által megküldött magyar álláspont-tervezetet a biztos három területen javasolta kiegészíteni. Véleménye szerint: a) indokolt volna a Rendeletben a személyes adatok védelmét korlátozni a közfeladatot ellátó személyek esetében; b) a magyar szabályozáshoz hasonlóan helyes volna az üzleti adatok védelmét szűkíteni a közpénzekkel összefüggő ügyletek körében; c) ideje volna korlátok közé szorítani az információkhoz való hozzáférésnél a tagállami vétót. Helyes volna a Rendeletet legalább egy olyan szabállyal kiegészíteni, amely szerint a tagállam csak akkor tilthatja meg a hozzáférést a tőle származó és az Unió szervei kezelésében lévő dokumentumokhoz, ha az a saját országában is korlátozott.
>
> A biztos határozottan kifogásolta, hogy a Külügyminisztérium az álláspont-tervezetet egy órával a határidő lejárta előtt juttatta el a biztosi irodához véleményezésre, és szorgalmazta, hogy a Rendelet módosításával kapcsolatos további szakmai egyeztetéseket a Külügyminisztérium időben szervezze meg, és abba vonja be az információszabadságban járatos kormányzati és nem-kormányzati szakembereket. *(1324/K/2007)*

A tagállamok belső szabályozásának legfontosabb szabályait tartalmazza a közszféra adatainak további felhasználásáról szóló 2003/98/EK irányelv, melyet 2005. július 1-ig kellett a hazai jogunkba átültetni. Az Irányelv azt is előírta, hogy a Bizottság 2008. július 1-ig vizsgálja felül az Irányelv alkalmazását az egyes tagországokban, és a felülvizsgálat eredményét az Irányelv módosítására vonatkozó javaslataival együtt terjessze az Európai Parlament és a Tanács elé.

> Az Irányelv átültetésével kapcsolatban Magyarországon kezdettől fogva komoly viták voltak. A gondok egy része – sajátos módon – abból fakadt, hogy az információszabadság hazai szabályozása sok ponton messze előbbre tart az Irányelv követelményeinél, ezért az átültetés semmiképpen nem történhetett valamiféle automatizmus keretében. Szaporította a nehézségeket, hogy míg az Irányelv a közszféra kezelésében lévő adatvagyon hasznosításának fontosságából indul ki, a magyar szabályozás elsősorban a közszféra, a közpénzek átláthatóságát

garantáló alkotmányos jogként definiálja az információszabadságot. A két megközelítés összeegyeztetése nehéz és vitákat gerjeszt nemcsak a hazai szakemberek között, hanem az EU bizottsági szakértőkkel is.

Az Igazságügyi és Rendészeti Minisztérium, valamint a harmonizációt koordináló Gazdasági és Közlekedési Minisztérium számára az adatvédelmi biztos 2007 júliusában juttatta el az Irányelv átültetésével kapcsolatos észrevételeit. *(1370/K/2007)*

Az információszabadsággal kapcsolatos teendők új területe volt 2007-ben az Európa Tanács (ET) készülő egyezmény-tervezetével kapcsolatos állásfoglalás. 2007 októberében az Európa Tanács szakértői bizottságához eljuttatott levélben örömmel üdvözöltük a hivatalos dokumentumokhoz való hozzáférésről szóló egyezmény előkészítéséről szóló kezdeményezést. A ET szakértői munkacsoportja által 2007 júliusában összeállított tervezet az első jelentős lépés annak érdekében, hogy a 47 tagállamot magában foglaló szervezet egy alapdokumentum keretében meghatározza a hatóságok dokumentumaihoz való hozzáférés legfontosabb szabályait. A levélben utaltunk ugyanakkor arra, hogy az egyezménynek a közszféra lehető legszélesebb körére kellene előírnia az információkhoz való hozzáférést. A nyilvánosság alóli kivételek, azaz a titkok minden információszabadság-szabályozás kulcskérdését jelentik: a túl sok vagy a túl általánosan meghatározott kivételek puszta kirakati tárggyá tehetik az intézményt.

A biztos a hazai tapasztalatokra alapozva javasolta, hogy a) a közügyek jobb átláthatósága érdekében a szabályozás a magánszemélyekénél szűkebb körben engedje meg a közfeladatot ellátó személyek magánszférájának védelmét; b) szűkítse az üzleti titok védelmét a közpénzeket érintő ügyletek körében; c) a környezeti adatok nyilvánosságát legalább olyan széles körben garantálja, mint az Aarhus-i Egyezmény.

A munkabizottsági tervezethez számos információs biztos és meganynyi civilszervezet juttatta el a véleményét és a javaslatait. Ezek nyomán az ET Emberi Jogi Bizottsága az egyezmény eredetileg 2008 januárjára tervezett elfogadását áprilisra halasztotta, további időt és lehetőséget adva a tagállamoknak a javaslat alaposabb megfontolására. *(1964/H/2007)*

Közérdekű adatok az önkormányzatok kezelésében

Ahogy az adatvédelmi biztos működése óta mindig, az információszabadságot érintő ügyek harmada ebben az évben is az önkormányzatok működésének nyilvánosságával volt kapcsolatos. A panaszok zöme változatlanul az önkormányzatok üléseinek és dokumentumainak, illetve az önkormányzat által kötött szerződéseknek a nyilvánosságát, valamint az önkormányzatok adatszolgáltatási gyakorlatát kifogásolta.

Az önkormányzati képviselőktől, polgármesterektől származó beadványok arra engednek következtetni, hogy sokak számára továbbra sem egyértelmű egészen, hogy az adatvédelmi biztosnak csak korlátozott lehetősége van az önkormányzati képviselőket, az egyes önkormányzati bizottságokat és szerveket megillető tájékozódási jogot vizsgálni. Korábban számtalanszor kifejtettük, hogy a biztos hatásköre csak a személyes adatok védelmével és a közérdekű adatok kezelésével összefüggő ügyekre terjed ki, vagyis azokra, ahol az egyének az Alkotmányban garantált információszabadsághoz való jogukat kívánják érvényesíteni. Az önkormányzati bizottságok és a feladatkörükben eljáró képviselők információkhoz való jogát az Ötv. alapján kell megítélni, a biztos ilyen esetekben csak annyiban foglalhat állást, amennyiben azok a személyes adatok védelmét, illetőleg a közérdekű adatok nyilvánosságát érintik, azaz amennyiben e szervek és személyek a közérdekű adatok megismerésének jogával kívánnak élni.

A képviselők és önkormányzati szervek, mint közfeladatot ellátó szervek vagy személyek tájékoztatáshoz fűződő joga tehát megkülönböztetendő az információszabadság érvényesülésétől. A közérdekű, illetve közérdekből nyilvános adatokat Avtv. 19. és 20. §-ai alapján ugyanúgy megismerhetik, mint minden más állampolgár. Személyes adatokat pedig az Avtv.-nek mindenki másra is érvényes szabályai szerint ismerhetnek meg, azaz ha erről törvény rendelkezik, vagy az érdekelt az adatok kiadásához hozzájárult. *(93/P/2007)*

Továbbra is gondot okoz az önkormányzatokban a zárt ülések elrendelése, illetve a zárt ülésen hozott döntések nyilvánossága. Számos állásfoglalásban leszögeztük, hogy az önkormányzatoknak alapvetően átláthatóan kell működniük, a nyilvánosság korlátozására esetükben csak nagyon szűk, törvények által meghatározott körben van lehetőség.

Egy panaszos azzal fordult a biztoshoz, hogy jóllehet a tárgyalt napirendi pont érintettje volt, a városi önkormányzat képviselő-testü-

letének bizottsági ülésére nem hívták meg, ezért nem tudott nyilatkozni, hogy a kérdés nyilvános tárgyalásába beleegyezik-e. A biztos a válaszában utalt arra, hogy az ügyben az Ötv. 12. § (4) bekezdésében foglaltak az irányadóak. Ezek szerint a képviselő-testület zárt ülést tart többek között választás, kinevezés, vezetői megbízatás adása, illetőleg állásfoglalást igénylő személyi ügy tárgyalásakor (illetve a képviselő-testület bizottsága ezen döntések előkészítésekor). A zárt ülés megtartásához a törvény egy további feltételt is fűz: zárt ülést csak akkor lehet elrendelni, ha az érintett a nyilvános tárgyalásba nem egyezik bele. Azaz az érintett számára biztosítani kell a nyilatkozás lehetőségét. E nyilatkozat megtételéhez azonban az érintettnek tudnia kell, milyen ügyben, mely személyes adatai feltárására kerülhet sor. Az információs önrendelkezési jogból következően a képviselő-testület kötve van az érintett nyilatkozatához, azt nem bírálhatja felül, az érintett rendelkezési jogát nem vonhatja el. Amennyiben az érintett nyilatkoztatására nem kerül sor, illetve nem nyilatkozik, a képviselő-testületnek zárt ülést kell tartania. A képviselő-testületi ülés zárttá minősítése nem tekinthető abszolút érvényűnek, nem vezethet az érintett információs önrendelkezési jogának csorbításához sem. Amennyiben tehát az érintett a zárt ülést követően a nyilvános üléshez való hozzájáruló nyilatkozatát pótolja, avagy a zárt ülés tartását kérő nyilatkozatát visszavonja, akkor a zárt képviselő-testületi ülés őt érintő része a továbbiakban nyilvános ülésnek tekintendő.
(1468/P/2007)

Gyakori panasz, hogy az önkormányzatok az Avtv.-ben és más törvényekben meghatározott kötelességük ellenére nem, vagy csak vonakodva adják ki, illetve teszik megismerhetővé az általuk magánszemélyekkel és gazdasági társaságokkal kötött szerződéseiket.

Egy település jegyzője például azzal a kérdéssel fordult a biztoshoz, hogy a számlák adatait tartalmazó számlanyilvántartó könyvek másolatát megkaphatja-e kérésére egy települési képviselő. A biztos válaszában kifejtette, hogy az Avtv. 19. §-ának (1)-(2) bekezdése arra kötelezi az önkormányzatokat mint közfeladatot ellátó szerveket, hogy biztosítsák feladataikra vonatkozóan, de különösen az önkormányzati költségvetésre és annak végrehajtására, az állami és önkormányzati vagyon kezelésére, a közpénzek felhasználására és az erre kötött szerződésekre, a piaci szereplők, a magánszervezetek és – személyek részére különleges vagy kizárólagos jogok biztosítására vonatkozóan a közvélemény pontos és gyors tájékoztatását, illetve ezeket az adato-

kat közzé- vagy más módon hozzáférhetővé tegyék. Az Avtv. célja, hogy az önkormányzat pénzügyei, gazdálkodása átlátható, nyomon követhető legyen. A közérdekű adatok megismerése előtt csak meghatározott törvényi korlátok állhatnak (Avtv. 19. § (3) bekezdése), illetve azok a személyes adatok nem ismerhetők meg, amelyek olyan személyekre vonatkoznak, akik nem gazdasági tevékenységük keretében kerülnek pénzügyi kapcsolatba az önkormányzattal (pl. szociális segélyezés, munkabér-kifizetés, munkavégzéshez kapcsolódó egyéb juttatás kifizetése, önkormányzati bérlakás bérének megfizetése). Az Avtv. 19. §-a, valamint a Polgári Törvénykönyv 81. §-a szerint is az önkormányzati költségvetés terhére – az önkormányzattal szerződő fél gazdasági tevékenysége keretében – kötött szerződésekre vonatkozó adatok nyilvánosak. Azok a magánosok és gazdálkodó szervezetek, akik, illetve amelyek az állammal vagy önkormányzattal bármiféle üzleti kapcsolatba kerülnek, kötelesek gazdasági tevékenységük adatainak nyilvánosságra kerülését eltűrni, mégpedig olyan mértékig, hogy a közvagyonnal való gazdálkodás, a közpénzek felhasználása ellenőrizhető legyen. Vagyis az önkormányzattal kötött polgári jogi szerződés adatai közérdekű adatok, és üzleti titokra hivatkozással sem zárhatóak el a nyilvánosság elől. Mindezek alapján a számlák, a számlanyilvántartó-könyv másolatai nyilvánosak. Az önkormányzat pénzügyeiről bárki – akár ilyen mélységben is – tájékozódhat. *(48/K/2007)*

Egy másik panaszos azt kérdezte az adatvédelmi biztostól, hogy kaphat-e másolatot a Kerületi Építési Szabályzat és Szabályozási Tervről (KSzT), illetve az ennek mellékletét képező munkarész anyagáról. A biztos válaszában kifejtette, hogy az KSzT alapjául szolgáló dokumentáció az önkormányzat kezelésében lévő, a személyes adat fogalma alá nem eső – titokká nem minősített, vagy minősülő – adatokat tartalmaz, azaz a dokumentáció adatai közérdekű adatok. Megállapította továbbá, hogy az „előkészítő anyagok, tervek" megismerése az önkormányzat törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását nem veszélyezteti, vagyis az adatok nem minősülnek döntést előkészítő adatnak, így a kérdéses iratok kiadásának törvényi akadálya nincs. Sőt, a vizsgálat megállapította azt is, hogy a panaszos által kért iratmennyiség másolása nem ró aránytalan terhet az adatkezelőre, mivel a kérdéses dokumentumok az iratanyagból leválaszthatók. *(1869/P/2007)*

Szintén gyakran kérdéses, hogy az önkormányzat tulajdonában lévő, önkormányzati feladatot ellátó gazdasági társaságnak van-e adatszolgáltatási kötelezettsége.

> Ezzel kapcsolatban egy panaszos abban kérte a biztos állásfoglalását, hogy egy önkormányzati tulajdonban lévő gazdasági társaság szerződései közérdekű adatoknak tekinthetők-e, illetve nyilvánosak és hozzáférhetőek-e. A válasz szerint: ha az önkormányzati tulajdonban lévő gazdasági társaság az Ötv.-ben, vagy egyéb jogszabályban meghatározott közfeladatot lát el, akkor az általa kezelt adatok körére az Avtv. közérdekű adatok nyilvánosságára vonatkozó rendelkezései alkalmazandók. *(1528/K/2007)*

A panaszok arra utalnak, hogy az önkormányzati adatkezelési gyakorlatban változatlanul nehézséget okoz a közérdekből nyilvános adatok körének meghatározása, egyebek mellett például az, hogy milyen mértékig tekinthető ilyen adatnak egy önkormányzati képviselő vagy a polgármester tevékenységével kapcsolatos adata.

> Egy panaszos beadványában az önkormányzati képviselők által leadott szavazatok nyilvánosságára, illetőleg a képviselők javadalmazására kérdezett rá. A biztos válaszában hivatkozott az Avtv. 19. §-ának (4) bekezdésére, mely szerint: ha törvény másként nem rendelkezik, közérdekből nyilvános adat az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy feladatkörével összefüggő személyes adata, továbbá egyéb, közfeladatot ellátó személy e feladatkörével összefüggő személyes adata. Ezen adatok megismerésére e törvénynek a közérdekű adatok megismerésére vonatkozó rendelkezéseit kell alkalmazni. Ha törvény kivételt nem tesz, közérdekből nyilvános adatnak minősül tehát a képviselő e minőségében tett valamennyi megnyilatkozása, cselekedete, illetve a tevékenységéért az önkormányzat költségvetéséből kapott tiszteletdíja, egyéb juttatása is. A korábbi gyakorlattal ellentétben ma tehát nem azt kell vizsgálni, hogy az önkormányzati képviselő feladatkörével összefüggő mely személyes adata nyilvános, hanem azt, hogy e személyes adatok között van-e olyan, amelyet valamely törvényi rendelkezés alapján nem lehet nyilvánosságra hozni, amelynek nyilvánosságra kerülését az érintett nem köteles tűrni. *(43/P/2007)*

Az Ötv. alapján az önkormányzati képviselő testületek működésének döntő része a nyilvánosság előtt zajlik, bárki által megismerhető. Más

szabályok (mindenek előtt az Avtv. és a Ket.) irányadók ugyanakkor az egyedi hatósági és egyéb ügyekben eljáró önkormányzati hivatalokra. Ez utóbbiak eljárásának nagyobb része értelemszerűen nem nyilvános, a közérdekű adatigénylés elutasítása során megalapozottan hivatkozhatnak például az Avtv. 19/A. §-ára, azaz a döntés-előkészítő adatok védelmére.

> Egy fővárosi önkormányzati képviselő abban kérte a biztos állásfoglalását, hogy jogszerűen járt-e el a Főpolgármesteri Hivatal Városüzemeltetési és Vagyongazdálkodási Főpolgármester-helyettesi Irodájának vezetője, amikor a 4-es metró projekt EU támogatási kérelmének megalapozására készült költség-haszon elemzést, annak döntés-előkészítő jellege miatt nem hozta nyilvánosságra. A biztos vizsgálata megállapította, hogy a 4-es metró beruházás EU támogatási kérelmének megalapozására készült költség-haszon elemzés része annak a dokumentációnak, amelynek alapján döntés születik a kérelemnek a brüsszeli hatóságokhoz történő benyújtásáról. A 4-es metró beruházással kapcsolatos támogatási kérelem előkészítése összetett folyamat, melyben közreműködőként több szerv is részt vesz, a végső döntést pedig a Kormány hozza meg. A költség-haszon elemzést is magában foglaló támogatási kérelem addig nem tekinthető tehát kész dokumentációnak, amíg arról a Kormány nem dönt. A Főpolgármester-helyettesi Iroda vezetője ugyanakkor tévesen hivatkozott arra, hogy a költség-haszon elemzés egészen a brüsszeli döntésig elzárható a nyilvánosság elől, hiszen a Kormány határozatával a pályázati kérelem véglegessé válik, ettől az időponttól tehát valamennyi azt megalapozó dokumentum nyilvános. *(1897/P/2007)*

Munkánkban egyelőre nem játszott számottevő szerepet az elektronikus információszabadságról szóló 2005. évi XC. törvényben (továbbiakban: Eitv.) előírt, az önkormányzatokra vonatkozó közzétételi kötelezettségek vizsgálata, hisz e törvény csak 2008. július 1-től kötelez minden önkormányzatot. Az önkormányzati dokumentumok internetes közzétételével kapcsolatos kérdések ugyanakkor már 2007-ben is több beadványban felmerültek.

> A főváros egy kerületének jegyzője azzal a kérdéssel fordult a biztoshoz, hogy nyilvánosságra hozhatóak-e az önkormányzati bizottságok döntései a honlapon. Ezzel kapcsolatban az állásfoglalás megállapította, hogy az Avtv. 19. §-ának (1) és (2) bekezdése szerint a helyi önkormányzati feladatot ellátó szerv vagy személy az önkormányzati vagyon kezelésére, a közpénzek felhasználására és az erre kötött szerző-

désekre vonatkozóan köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását. Kötelesek továbbá közzé- vagy hozzáférhetővé tenni a gazdálkodásukra vonatkozó adatokat. A bizottságok döntései azonban tartalmazhatnak magánszemélyekre vonatkozó személyes adatokat is. Ilyen esetekben az érintettek személyes adatainak védelmére (pl. anonimizálás útján) figyelemmel kell lenni nemcsak az adatigénylés iránti kérelem teljesítésekor, hanem a dokumentumok internetes közzétételekor is. *(911/K/2007)*

A két információs jog konfliktusa

A 2006 évről szóló beszámolóban már hangsúlyoztuk, hogy az Avtv.-nek a közfeladatot ellátó személyek adatainak nyilvánosságáról rendelkező, 2005 júniusától hatályos új szabálya csak az első fontos lépés a két jog: az adatvédelem és az információszabadság régóta megoldatlan konfliktusának rendezése érdekében.

E rendelkezés szerint: „Ha törvény másként nem rendelkezik, közérdekből nyilvános adat az (1) bekezdésben meghatározott szervek feladat- és hatáskörében eljáró személy feladatkörével összefüggő személyes adata, továbbá egyéb, közfeladatot ellátó személy e feladatkörével összefüggő személyes adata. Ezen adatok megismerésére e törvénynek a közérdekű adatok megismerésére vonatkozó rendelkezéseit kell alkalmazni." A 2006-ban e tárgykörben kiadott adatvédelmi biztosi ajánlás *(1234/H/2006)* nyomatékosan felhívta a figyelmet arra, hogy az Avtv. idézett módosítása a közfeladatot ellátó személyek igen széles körének (így például a köztisztviselők, a közalkalmazottak, az ügyészek, a bírók, az igazságügyi alkalmazottak, a fegyveres szervek hivatásos állományú tagjai, a Magyar Honvédség hivatásos katonái) jogviszonyát szabályozó törvények korrekciója nélkül értelmetlenné válik.

Felkértük a Miniszterelnöki Hivatalt vezető minisztert, hogy a hatáskörrel rendelkező miniszterekkel együtt vizsgálja felül a közfeladatot ellátó személyek jogállását rendező törvényeket, és az Avtv.-vel való összhang megteremtése érdekében kezdeményezze a szükséges módosításokat. A felülvizsgálatra, a szükséges törvénymódosításokra mindezidáig annak ellenére nem került sor, hogy az illetékes minisztériumok a saját működésük kapcsán maguk is nap mint nap megoldhatatlan helyzetekbe kerülnek. Az egyre szaporodó ügyek világosan jelzik, hogy az Avtv. új 19. § (4) bekezdé-

sének értelmezése az érintett jogalkalmazó szervek körében nem egységes, az adatvédelmi biztos pedig pusztán jogértelmezéssel a hiányzó szabályokat nem pótolhatja. Ez annál is kevésbé vállalható, mivel két egyenrangú alkotmányos jog konfliktusáról van szó.

2007-ben részben maguk az adatkezelők, részben panaszosok különösen nagy számban fordultak hozzánk beadvánnyal a feladatkörükben eljáró közalkalmazottak, köztisztviselők, rendészeti alkalmazottak adatainak nyilvánossága ügyében. Ezeket részletesen az önkormányzatokról és a rendőrségről szóló alfejezetben ismertetjük.

A korrupció elleni harc és a nyilvánosság

Miért is fontos az információszabadság törvénybe iktatása? A kérdésre sokféle válasz ismert. Ezek közül ma talán a leggyakoribb, hogy a közszféra átláthatóságát biztosító szabályok nélkül reménytelen a korrupció elleni harc. Feltehetőleg ez a felismerés vezetett ahhoz, hogy a korrupcióellenes feladatokról szóló 1037/2007. (VI. 18.) Korm. határozat a felállítandó 18 fős Antikorrupciós Koordinációs Testület (Testület) egyik tagjaként a közszféra átláthatóságával 12 éve „hivatásszerűen" foglalkozó adatvédelmi biztos delegáltját nevezte meg.

A 2007 szeptemberében megalakult testület legfőbb feladata egy hosszú távú korrupcióellenes stratégia, valamint egy rövidebb időszakra szóló cselekvési program kidolgozása. A Testület munkájának segítése érdekében 2007 októberében az adatvédelmi biztos delegáltjának kezdeményezésére és vezetésével a Testület további hat tagjának (az Igazságügyi és Rendészeti Minisztérium, a Miniszterelnöki Hivatal, az Állami Számvevőszék, a Közbeszerzések Tanácsa delegáltja, a Társaság a Szabadságjogokért és a magyar Transparency International képviselője) részvételével felállt az Átláthatósági Munkacsoport, mely feladatául tűzte a) annak feltárását, hogy a közügyek nyilvánosságára vonatkozó hatályos szabályok megfelelően szolgálják-e a korrupció elleni küzdelmet; mely területeken és milyen jogszabálymódosításokra van szükség; b) annak feltárását, hogy a nyilvánosságra vonatkozó hatályos szabályok milyen módon érvényesülnek a gyakorlatban; milyen (szakmai, financiális, szemléleti) okok akadályozzák a közérdekű adatok nyilvánosságának gyakorlati érvényesülését; milyen intézkedések (eseti vagy rendszeres szakmai képzések, az intézmény-finanszírozás

módosítása, stb.) indokoltak; valamint c) annak feltárását, hogy milyen szerepet játszik a média a korrupció elleni harcban, milyen korlátai vannak az oknyomozó újságírásnak Magyarországon és milyen intézkedések szükségesek e téren.

A Munkacsoport javaslatára 2007 végéig a Testület két kérdésben fogadott el határozatot:

1. Az Antikorrupciós Koordinációs Testület 2007. december 13-i ülésén a korrupció elleni harc és az oknyomozó újságírás kapcsolatát illetően megállapította, hogy az újságírókat ma gyakran és esetenként indokolatlanul fenyegeti büntetőeljárás titoksértés miatt. E fenyegetés is egyik oka lehet annak, hogy a sajtó nem tud elég hatékony szerepet játszani a korrupciógyanús ügyek feltárásában. Ezért a Testület egyetértett abban, hogy a készülő, a Büntető Törvénykönyv módosítását is magában foglaló, új titoktörvényben a jogalkotó differenciált szabályozást fogadjon el. Az újságírókat kizárólag akkor fenyegessék büntetőjogi szankciók a szándékosan elkövetett súlyos titoksértés miatt, ha büntetőeljárás során bizonyítást nyer, hogy az információk titokban tartásához súlyosabb érdekek fűződnek, mint a nyilvánosságra hozatalukhoz. A Testület felkérte a polgári nemzetbiztonsági szolgálatokat irányító tárca nélküli minisztert, hogy vizsgálja ki: az újságírókkal szemben kezdeményezett büntetőeljárással párhuzamosan vagy azt követően milyen eljárások folytak a titoktartási kötelezettségüket megsértő köztisztviselők ellen az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény hatálybalépése óta, és a vizsgálat eredményéről tájékoztassa a Testületet.

2. Az Antikorrupciós Koordinációs Testület 2007. december 13-i ülésén egyetértett abban, hogy az igazságszolgáltatás átlátható működése a korrupciós ügyekben különösen fontos. E nélkül a közvéleménynek nincs módja ellenőrizni, hogy a feltárt korrupciós ügyekben milyen eljárások nyomán milyen döntések születtek. Ma részben alacsonyabb szintű, egymással össze nem hangolt normák határozzák meg az igazságügyi tájékoztatás szabályait, valamint az eljáró szervek működésének nyilvánosságát. Ezért a Testület felkéri az igazságügyi és rendészeti minisztert, hogy tekintse át az igazságszolgáltatás átlátható működését akadályozó okokat. Ezt követően pedig tegyen javaslatot egy olyan, teljes körű törvényi szabályozásra, amely egyaránt biztosítja az igazságszolgáltatási szervek tevékenységének átláthatóságát, működésük kutathatóságát, a személyes adatok védelmét és a sajtó szabadságát.

A rendőrség tevékenységének átláthatósága

Ebben az évben a korábbiakat jócskán meghaladó számú panasz és konzultációs kérdés érkezett a biztos irodájához a rendőrség tevékenységének nyilvánosságával kapcsolatban. A beadványok részben a rendőrség, mint intézmény, részben pedig a rendőri vezetők tevékenységét érintették. A rendőrség a törvényekben meghatározott állami feladatokat ellátó szervezet, a működésével összefüggő dokumentumok, adatok nyilvánosságának megítélése a hatályos jogszabályok alapján általában egyértelmű. A közfeladatot ellátó személyek tevékenységére vonatkozó adatok nyilvánosságának jogi rendezetlensége miatt a rendőrök, rendőri vezetők tevékenységének nyilvánosságáról ez korántsem mondható el.

Miként ezt a múlt évi és a jelen beszámoló is több helyen jelzi: a közfeladatot ellátó személyekre vonatkozó új szabályozásnak az Avtv.-be történő beépítésekor elmaradt a kapcsolódó törvények módosítása. Egyebek mellett nem módosultak a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény (továbbiakban: Hszt.) adatszolgáltatási, nyilvánossági szabályai, holott ennek és több hasonló törvénynek a módosítására a biztos már 2006 őszén javaslatot tett, ám észrevételeinket nem vették figyelembe, miként 2007-ben, a Hszt. átfogó módosításakor sem.

Az egyik ügyben a rendőrség az egyik rendőri szakszervezet adatkérésének teljesíthetőségével kapcsolatban fordult a biztoshoz: ki kell-e adniuk az érdekképviseleti hovatartozásra vonatkozó összesített adatokat? A biztos válaszában kifejtette, hogy a tagnyilvántartási összesített adatok nem minősülnek az Avtv. 2. §-ának 1. pontja szerinti személyes adatoknak, hiszen konkrét természetes személyekkel nem hozhatók kapcsolatba. A szakszervezeti tagdíj levonására vonatkozó adatok a rendőrség, mint közfeladatot ellátó szerv kezelésében lévő adatok, és ebből következően közérdekű adatok. Emiatt nem megalapozott az adatkezelőnek az az érvelése, hogy a szakszervezeti tagságra utaló információk nem a rendőrség feladat- és hatáskörére, fő tevékenységére vonatkoznak, hanem a tagdíjlevonással, a munkajogi védelem biztosításával, a munkaidő-kedvezmény elszámolásával, mint járulékos tevékenységgel illetve munkaügyi feladatokkal kapcsolatosak, melyeket minden munkáltatónak el kell végeznie. Az Avtv. 19. §-ának (3) bekezdése szerint a közfeladatot ellátó szerveknek lehetővé kell tenniük, hogy a kezelésükben lévő közérdekű adatot bárki meg-

ismerhesse, kivéve, ha törvény ezt korlátozza. A szakszervezeti reprezentativitásra, taglétszámra vonatkozó adatok esetén ilyen korlátozásról nem beszélhetünk, tehát ezek az Avtv. 20. §-a szerinti rendben megismerhetőek. Amennyiben a tagdíjlevonási adatok összesített formában nem léteznek az adatkezelőnél, de az összeállítás nem okoz aránytalan többletmunkát, a közfeladatot ellátó szervtől elvárható, hogy a kérést teljesítse. *(512/K/2007)*

Egy másik ügyben egy panaszos azt kifogásolta, hogy az elismert és később kifizetett szabálysértési bírság után a szabálysértési hatóság nem adta ki számára az ügyében helyszínen intézkedő hatósági személy nevét, illetve a helyszínen készített fénykép másolatát. A biztos álláspontja szerint a szabálysértésekről szóló 1999. évi LXIX. törvény 47. § (2) bekezdése alapján az eljárás alá vont személy az ügy iratait az eljárás bármely szakaszában megtekintheti, azokról másolatot kérhet, illetve készíthet. Így az eljárás lezárultát követően is, mégpedig nemcsak ezen rendelkezés, hanem az Avtv. 12. § (1) bekezdése alapján is. A felügyelő intézkedésére vonatkozó információ, így egy adott időpontban és helyen eljáró felügyelő neve, azonosító száma pedig az Avtv. 19. §-ának (4) bekezdése szerint közérdekből nyilvános adat. *(1535/P/2007)*

A rendőrséget érintő legtöbb panaszt és kérdést kiváltó ügy ebben az évben a 2006. október 23-i események rendőri kezelését vizsgáló úgynevezett Papp-bizottság jelentésével volt kapcsolatban, elsősorban a rendőrök felelősségre vonásának adatait, személyük azonosíthatóságát érintette.

Az első ügyben egy civil szervezet fordult a biztoshoz a Papp-bizottság jelentése, illetve a büntetés-végrehajtási intézményekben elkövetett jogsértések vizsgálatát lezáró jelentés nyilvánosságával kapcsolatban. Az ügyben több konzultációra is sor került annak érdekében, hogy a közérdekű adatok nyilvánosságához való jog a rendőrség gyakorlatában a jövőben maradéktalanul érvényesüljön. Az érintett szervek a biztosi eljárás nyomán a jelentéseket nyilvánosságra hozták, ám azok nem teljes szövegét, csupán „a döntés megalapozását szolgáló adatoktól, illetve a személyes adatoktól megfosztott" változatát. A biztos felhívta a figyelmet arra, hogy a személyes adatok közül azok, amelyek a büntetés-végrehajtási szervezet személyi állományával hozhatók kapcsolatba, az Avtv. 19. § (4) bekezdése alapján nyilvánosak lehetnek. A döntés megalapozását szolgáló adatok kapcsán pedig az Avtv. 19/A. § (2) bekezdésében foglaltakra hivatkozott, mely szerint a döntés megalapozását szolgáló adat megismerésére irányuló igény a döntés meg-

hozatalát követően akkor utasítható el, ha az adat megismerése a szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztetné. A megkeresést követően az országos parancsnok azt a választ adta, hogy nyilvánosságra hozott jelentésen kívül másik nem készült, és a jelentésből csak azon személyes adatokat törölték, amelyek nem minősülnek közérdekből nyilvánosnak, illetve az Avtv. 19. § (2) bekezdése alapján olyan adatokat, melyek nyilvánosságra kerülése a büntetés-végrehajtás törvényes működési rendjét, így különösen a biztonságos őrzést veszélyeztetné. A biztos további intézkedést nem tudott tenni, ám ígéretet tett arra, hogy ezen éves beszámolóban fel fogja hívni az Országgyűlés figyelmét arra, hogy a jövőben a hasonló esetek gyors és hatékony vizsgálatokkal, illetve a nyilvánosság teljes körű tájékoztatásával megelőzhetők. *(1248/P/2007)*

A Papp-bizottság jelentésével kapcsolatos másik panaszban a beadványozó újságíró azt sérelmezte, hogy kérése ellenére a rendőrség nem nevezte meg a jelentésben elmarasztalt rendőröket, rendőri vezetőket, illetve nem nevezte meg a kódneveken szereplő személyeket; továbbá nem adott arra vonatkozó információkat, hogy e személyeket felelősségre vonták-e és milyen formában.

A biztos álláspontja szerint a rendőrök neve az Avtv. 19. § (4) bekezdése, valamint a Hszt. 203. § (3) bekezdése alapján nyilvános adat. A rendőri vezetők felelősségre vonását illetően ugyancsak a Hszt.-ből kell kiindulni, mely a személyügyi nyilvántartás adatkörei között sorolja fel a fegyelmi eljárásokra vonatkozó adatokat – a fegyelmi fenyítés nemét, hatályát, illetve a mentesítés tényét. A fegyelmi eljárással összefüggő adatok esetében a Hszt.-nek a személyügyi nyilvántartásból való adatszolgáltatásra vonatkozó szabályait kell figyelembe venni. A fegyelmi eljárással kapcsolatos adatokat e szerint csak a Hszt.-ben tételesen felsorolt személyek vagy szervek részére lehet kiadni. Ez az ügy ismét rávilágított arra, hogy a közfeladatot ellátó személyek feladatkörével összefüggő adatainak nyilvánosságára vonatkozó hatályos szabályok rendezetlenek. Ezért a biztos ismételten felhívta az igazságügyi és rendészeti miniszter figyelmét arra, hogy a rendészeti szervek tagjainak adatkezelésére vonatkozó szabályokat sürgősen felül kell vizsgálni, és összhangba kell hozni az Avtv. szabályaival. *(1522/P/2007)*

A 2006 őszi zavargások idején intézkedő rendőrök azonosíthatóságának hiányával kapcsolatos panasszal összefüggésben a biztosi állásfoglalás azon véleménynek adott hangot, hogy az állam sosem „arc nélkül" intézkedik. Minden egyes határozat, intézkedés mögött az állampolgár számára ismert kilétű ügyintéző, vezető áll, akinek feladatkörével összefüggő személyes adata Avtv. 19. § (4) bekezdése alapján közérdekből nyilvános adat. A Hszt. 203. § (3) bekezdése szerint pedig a fegyveres szervek hivatásos állományába tartozók személyügyi nyilvántartásából a fegyveres szerv megnevezése, a név, beosztás, rendfokozat és a kitüntetésre vonatkozó adat az érintett hozzájárulása nélkül is nyilvánosságra hozható. Ezekre tekintettel a rendőrség köteles minden állományába tartozó intézkedését visszakereshető módon nyomon követni, és az intézkedő rendőr nevéről későbbi kérés esetén (ha a helyszínen a rendőr nem azonosítható) az érdeklődőt tájékoztatni.

A jogállam követelményeinek megfelelően a törvényességet védő rendőrség és a közterületen erőszakosan fellépők között markáns határvonalat kell húzni. Amikor vétlen állampolgárokat bántalmaztak azonosíthatatlan kilétű rendőrök, az állam maga lépte át ezt a határvonalat. A biztos hangsúlyozta, hogy az állami szervek nem kerülhetnek olyan helyzetbe, hogy ne tudják azonosítani a saját állományukba tartozókat. Ezen az sem változtat, ha a rendőr nem visel azonosítót. Az azonosító viselésének mellőzése az állampolgár számára lehetetlenné teszi a vele szemben fellépő rendőr kilétének megállapítását, de nem szünteti meg a rendőrség azon kötelezettségét, hogy minden egyes intézkedés kapcsán meg tudja nevezni, hogy az ügyben ki járt el. Nem csak a fegyveres szervek hierarchikus működésétől idegen az a jelenség, hogy a rendőrség nem tud számot adni arról, hogy ki járt el adott helyen és időben, hanem a közérdekből nyilvános adatok megismeréséhez fűződő jog gyakorlását is kizárja. *(1824/P/2007)*

A rendőrökről készült fényképfelvételek világhálón történő nyilvánosságra hozatalával kapcsolatos ügyben a biztos kifejtette, hogy azt az álláspontot foglalta el, miszerint intézkedő rendőr nem tekinthető közszereplőnek, intézkedése pedig nem minősül közszereplésnek. A jelenlegi jogszabályi környezetben a rendőr hozzájárulásának hiányában arcképe nem hozható nyilvánosságra. Amennyiben valaki úgy véli, hogy bűncselekményt örökített meg, úgy a felvétel helye az ügyészségen, és nem a világhálón van. Ennek megfelelően jogellenes,

ha intézkedő rendőrök felismerhető arcképmását azinterneten közzéteszik. *(1848/K/2007)*

A bíróságok működésének nyilvánossága

Évről évre több beadvány tárgya, hogy a bíróságok tevékenységének mely része ismerhető meg, működésük mennyiben átlátható, és a velük kapcsolatos, illetve általuk kezelt adatok, információk nyilvánosak-e. Újra és újra tájékoztatást kérnek az emberek arról, hogy a tárgyalás nyilvánossága és a személyes adatok védelme hogyan egyeztethető össze, készíthető-e a tárgyaláson hang- és képfelvétel, és az közzétehető-e.

A bíróság tárgyalása – fő szabály szerint – nyilvános. A bíróság a tárgyaláson hozott határozatát akkor is nyilvánosan hirdeti ki, ha a tárgyalásról a nyilvánosságot kizárta. Tehát a nyilvánosság elvének érvényesülése folytán a nyilvános bírósági tárgyaláson bárki megjelenhet, a tárgyalást meghallgathatja. Azonban különbséget kell tenni a nyilvános tárgyalás nyilvánossága és a teljes akta nyilvánosság között. Az, hogy a tárgyaláson jelen lévők megismerhetik az eljárásban részt vevők különféle személyes adatait, tudomást szerezhetnek velük kapcsolatos információkról, nem jelenti egyúttal azok felhasználásának jogát vagy az ügyiratokba való betekintési jogosultságot.

A tárgyalás nyilvánossága ellenére az eljárás során keletkezett iratok és az iratban szereplő adatok nem nyilvánosak, mivel az iratokba történő betekintést és a másolatkészítést jogszabály korlátozza. A tárgyalás nyilvánosságának elve nem keletkeztet jogot továbbá a tárgyaláson elhangzottak szabadon történő rögzítésére, majd a felvételek szabad felhasználására. *(1016/K/2007)* Viszont fontos közérdek a bíróságok ítélkezési tevékenységének ellenőrizhetősége. A bíróságok működésének megismerhetőségében nagy előrelépést jelentett az Eitv., mely nemcsak a bíróságok működésével kapcsolatos közérdekű adatok, hanem a Legfelsőbb Bíróság és az ítélőtáblák határozatainak közzétételét is előírta.

Nem volt egyértelmű azonban, hogyan is kell a közzétételi kötelezettségnek eleget tenni, sőt az sem, hogy a bírósági határozatok egyáltalán közérdekű adatnak tekintendőek-e. Az Országos Igazságszolgáltatási Tanács hivatalvezetőjének kérésére igyekeztünk elősegíteni a törvényi rendelkezések megfelelő végrehajtását. Megjegyzendő, hogy a törvény terve-

zetének véleményezése során és a korábbi beszámolóban is – miközben üdvözöltük a törvény elfogadását – utaltunk a jogszabályi rendelkezésekkel kapcsolatos hiányosságokra.

A biztosi álláspont szerint a bíróságok természetesen közfeladatot ellátó szervek, és a bírói joggyakorlatra, jogalkalmazásra vonatkozó információk, így az anonimizált határozatok is a közérdekű adatok körébe tartoznak. Az Eitv. nem szabályozza, kinek a feladata a határozatok anonimizálása, és azt sem, hogy kit terhel az ezzel együtt járó felelősség. Ez annál is inkább fontos kérdés, mert az anonimizálás nem pusztán egy formalizált, technikai művelet, hanem az adatkezeléssel kapcsolatos, az adatok nyilvánosságra hozataláról szóló döntés. A szabályozásból nem állapítható meg, hogy az adatok közlésére köteles szerv adatkezelőnek vagy adatfeldolgozónak tekintendő-e, illetve viseli-e az anonimizálásért való felelősséget (saját maga anonimizál vagy a más szerv által végzett anonimizálást jóváhagyja). Az Eitv. szerint a közzétett bírósági határozattal együtt közzé kell tenni azokat az egyéb határozatokat, melyeket a közzétett bírósági határozattal felülbíráltak vagy felülvizsgáltak. Azonban a törvény nem ad világos iránymutatást arra, hogy az adat előállítása, keletkezése, valamint a közzététele közötti adatkezelési műveletet melyik határozat esetében mely szervnek kell elvégeznie. A bírósági határozatok szerkesztése, anonimizálása, közzététele az adott határozatot hozó bíróság illetve a bíróság elnökének feladata.

Kérdéses maradt, hogy a bíróság által felülvizsgált, nem bíróság által hozott határozatokat az azokat kiadó szervnek, a „közzétevő" bíróságnak vagy az OIT Hivatalának kell anonimizálnia. Az Igazságügyi és Rendészeti Minisztérium álláspontja szerint mindez nem okoz jogalkalmazási problémát, és az OIT Hivatalának kötelezettsége, hogy valamennyi közokiratot anonimizált formában közzétegye. A biztosi állásfoglalás szerint azonban ez a törvényből egyáltalán nem következik egyértelműen, és ha ez is volt a jogalkotói szándék, akkor az erre irányuló jogalkotás nem felel meg a normavilágosság követelményének. Az anonimizálás nem csupán a közzététel egy módja, hanem egy önálló, felelősséggel járó kötelezettség, vagyis nem irreleváns, ki anonimizálja az iratokat. A jogalkotónak kell az egyes szervezetek feladatait és felelősségi körét pontosan definiálni, mert ezáltal biztosítható a jogszabályok megfelelő végrehajtása, és ezáltal segíthető elő a jogbiztonság. *(1102/K/2007, 1665/P/2007, 1944/K/2007, 2155/K/2007)*

Szintén bírói kezdeményezésére született állásfoglalás arról, hogy nyilvános-e a peres ügyek lajstroma, és teljesítendő-e a bíróság által a peres felek és jogi képviselőik nevére, a per tárgyára, a pertárgyértékre vonatkozó adatigénylés.

A vizsgálat során egyértelműen megállapítható volt, hogy az adatigénylésben megjelölt adatkörből a folyamatban lévő gazdasági perekre vonatkozó összesített számadatok – akár a per tárgya, a pertárgyérték szerinti bontásban – közérdekű adatok, és e vonatkozásban az adatkérés teljesítendő. Bonyolultabb kérdés azonban, hogy a peres felek adatai mennyiben tekintendőek nyilvánosnak, egy adott perrel kapcsolatos információk, iratok mikor, milyen mértékben és kik által ismerhetőek meg, ugyanis a bíróságok által kezelt adatok megismerése, a bírósági eljárás nyilvánossága egy nagyobb kérdéskör részét jelentik. Az Avtv. fogalmi rendszerében egy adat vagy nyilvános, vagy nem nyilvános. A bíróságok eljárásában azonban a tárgyalás nyilvánosságának elve az adatnyilvánosság értelmezését nehezebbé teszi.

> A bírósági eljárások menete feloszthatő tárgyalási, valamint a tárgyaláson kívüli szakaszra, ezeken belül pedig nyilvános és nem nyilvános dokumentumokat, adatokat különböztethetünk meg. A tárgyalás szakaszában a tárgyaláson elhangzottak és az ítélethirdetés nyilvános (nem nyilvános tárgyaláson csak az ítélethirdetés publikus). A bírósági tárgyalás nyilvánosságáról, mint az eljárás egyik garanciális alapelvéről – az emberi jogok és az alapvető szabadságok védelméről szóló egyezmény és az Alkotmány alapján – a polgári perrendtartásról szóló törvény (Pp.) rendelkezik. A Pp. szabályai a magántitokhoz és a személyes adatok védelméhez való jogot korlátozzák, amikor – meghatározott kivételekkel – a tárgyalás és az ítélethirdetés nyilvánosságát rögzítik.
>
> A nyilvános bírósági tárgyaláson megjelenő érdeklődők különféle adatokat, információkat ismerhetnek meg, ebből nem következik azonban az ügyben érintett személyek jogainak teljes kiüresedése. Különbséget kell tenni a tárgyalás nyilvánossága, valamint a teljes aktanyilvánosság között. További kérdés, hogy a tárgyaláson megjelentek az ott megismert információkat hogyan használhatják fel (pl. kép- és hangfelvétel), különös tekintettel a sajtóra. A tárgyalási szakaszhoz tartozik még a tárgyalási jegyzék nyilvánosságának kérdése, mely az adatvédelmi biztos álláspontja szerint egyfajta „korlátozott" nyilvá-

nosságot jelent. (Tájékoztatási céllal a tárgyalások megkezdése előtt kell kifüggeszteni).

A tárgyaláson kívüli szakasz adatainak megismerését főként az iratbetekintési jog szabályozása szerint kell megítélni, és itt merül fel az is, hogy az ügyszakok, ügycsoportok szerinti lajstromozás, ezen belül a peres ügyek lajstroma megismerhető-e bárki által. Erre vonatkozóan a bíróságok eljárását szabályozó jogszabályok nem adnak kifejezett iránymutatást, és nincs olyan rendelkezés, mely a folyamatban lévő perekben a peres felek nevével együtt a per főbb adatainak nyilvánosságát mondaná ki, illetve tiltaná – jogi személyek esetében – a nyilvánosságot. A nyilvánosság egy bizonyos körben a fentiekben elmondottakból levezethető, így például a közfeladatot ellátó szervek vonatkozásában a nyilvánosság a folyamatban lévő perekre is értendő, mivel az Avtv. 19. §-a alapján a szerv peres ügyeivel kapcsolatos adatok, mint a tevékenységükre vonatkozó közérdekű adatok, nyilvánosak. Továbbá egyes ügyek már a per megkezdése előtt a sajtó által nyilvánosságra kerülhetnek. Azon perek esetében pedig, amelyekben tárgyalást tartottak, a tárgyalási jegyzék által érvényesül egyfajta nyilvánosság. *(780/K/2007)*

Amint korábban több alkalommal, ezen ügy kapcsán is jeleztük az igazságügyi és rendészeti miniszternek, hogy indokoltnak tartjuk a bírósági adatkezelés külön jogforrásban való részletesebb szabályozását úgy, hogy a szabályozás minden szereplő jogait és kötelezettségeit kellő mértékben figyelembe vegye. A bíróságok által kezelt adatok megismerése, a bírósági eljárás nyilvánossága mint egy összetett és különféle szempontokból jogértelmezést igénylő jogterület az adatvédelmi biztosi gyakorlatban hosszú évek óta rendszeresen felmerül. A személyes adatok védelme, a közérdekű adatok nyilvánossága, a sajtószabadság, a kutatás szabadsága, valamint a tárgyalás nyilvánosságának elve olyan alkotmányos jogok, illetőleg elvek, melyeknek együtt, egymásra tekintettel kell érvényesülniük.

A közpénzek átláthatósága

Az információszabadság-ügyek jelentős részét teszik ki kezdettől fogva azok az esetek, amelyekben vitatott, hogy az állami/önkormányzati szektor és a magánszféra között létrejött szerződések nyilvánosak-e. A szerződések nyilvánosságával foglalkozó beadványok a legkülönfélébb kérdéseket

érintették. Állást kellett foglalni például állami tulajdonú erdőrészlet magánkézbe adásával összefüggő csereszerződés *(1372/K/2007)*, a közszolgálati műsorszolgáltató által kötött szerződések *(1509/P/2006, 1028/K/2007)*, minisztériumi megrendelésre készült „háttértanulmányok" *(699/K/2007)*, egyszerű bérleti szerződések *(489/P/2007)*, a földalap-kezelő szerv által lebonyolított földértékesítési szerződések *(469/P/2007)*, közalapítványnak juttatott céltámogatásról szóló szerződések *(670/P/2007)*, gabonaraktárak intervenciós szerződéseinek nyilvánosságáról. *(758/K/2007)*

> Tipikus kérdés a közszolgáltatást végző, közvetlenül vagy közvetetten önkormányzati tulajdonú gazdasági társaságok működésével kapcsolatos szerződések nyilvánossága. E társaságok különféle szervezeti formában, különféle tulajdoni viszonyok között általában részben vagy teljesen közfeladatot látnak el, esetleg vállalkoznak is, mindezek ellenére tűrniük és biztosítaniuk kell a tevékenységükre vonatkozó nyilvánosságot, amint ezt a biztos az állásfoglalásaiban kifejtette. *(712/K/2007, 372/P/2007)*

Továbbra is jellemző, hogy a szerződések megismerését az adatkezelő állami vagy önkormányzati szervek üzleti titokra való hivatkozással tagadják meg. A már sokszor kifejtett alaptétel, hogy nem minden, a gazdasági tevékenységhez kapcsolódó üzleti információ tekinthető egyben üzleti titoknak, csak az, amelynek titokban maradásához a jogosultnak jogszerű érdeke fűződik. A hatályos joganyagban több olyan üzleti adatfajta létezik, amelynek nyilvánosságát, sőt kötelező közzétételét fontos közérdekre tekintettel jogszabály elrendeli. Ezekben az esetekben az információk titokban maradásához természetesen nem fűződik jogszerű érdek. Ilyenek például a gyógyszer-forgalmazási adatok, a környezeti (légszennyezési és zajártalomra vonatkozó) adatok, vagy a távhő szolgáltatási adatok. *(2133/K/2207, 372/P/2007, 1767/P/2007, 323/P/2007)*

Egy panaszos a Nemzeti Infrasturktúra Fejlesztő Zrt. (Zrt.) és egy konzorcium között az Mo autóút egy szakaszának kivitelezésére létrejött vállalkozási szerződés tartalmát szerette volna megismerni, azonban adatkérését arra hivatkozással tagadták meg, hogy a szerződés tartalma üzleti titok, nem tekinthető közérdekű adatnak.

> A biztos az állásfoglalásában leszögezte, hogy a Zrt. a gyorsforgalmi úthálózat építéséért felelős, állami tulajdonban álló gazdasági társaság, mely közfeladatot lát el. Az államháztartásról szóló törvény meg-

határozott szerződéses adatok közzétételére vonatkozó kötelezettséget ír elő, e kötelezettségnek a GKM, illetve a Zrt. eleget is tesz. E szabály azonban nem értelmezhető úgy, hogy a szerződések adataiból csak e szűk adatkör nyilvános, a többi információ pedig üzleti titokként elzárható lenne a nyilvánosság elől.

A biztos hangsúlyozta, hogy az autópálya-építési szerződések, mint közfeladatot ellátó szerv által, közpénz-felhasználásról, közérdekű tevékenység tárgyában kötött szerződések alapvetően nyilvánosak, és kizárólag azon adatok kezelhetők üzleti titokként, amelyek titokban maradásához a Ptk. szerint az érintetteknek valóban jogszerű érdeke fűződik. A vizsgálat megállapította, hogy a szerződés szövegében üzleti titoknak tekinthető információ nem volt. A biztos a szerződéskötésre, illetve a szerződések nyilvánosságára vonatkozó gyakorlat felülvizsgálatára kérte a Zrt-t. Végül mind a GKM, mind a Zrt. elfogadta az adatvédelmi biztosi álláspontot az egyedi adatigénylést és az általános gyakorlatot illetően egyaránt. *(1786/A/2006)*

A közpénzeket érintő ügyek másik fontos területe a különféle pályázati eljárásokban kezelt adatok nyilvánossága. Az adatvédelmi biztosi gyakorlatban kezdettől fogva egyértelmű, hogy a győztes pályázatot bárki megismerheti. Ennek indoka, hogy a nyilvánosság kontrollja segítheti elő, hogy a közjavak elosztása során a törvényesség és a gazdaságosság szempontjai érvényesüljenek. A pályázati eljárás átláthatósága, mint közérdek megelőzi az üzleti titok védelmének magánérdekét is. A pályázati dokumentációk azonban esetenként tartalmazhatnak személyes adatokat, üzleti titkokat és egyéb védendő információt.

A pályázati adatok szélesebb körének megismerhetőségét javasolta a biztos a Nemzeti Civil Alapprogrammal (NCA) kapcsolatban. Az NCA civil szervezetek – társadalmi szervezetek, alapítványok - számára, azok működéséhez és tevékenységéhez biztosít központi költségvetési támogatást. Az NCA, illetve szervei közfeladatot ellátó szervek, ezért a működésükre vonatkozó információk közérdekű adatnak tekintendőek. A civil szervezetek – bár tevékenységük társadalmilag hasznos és fontos – nem tekintendőek az Avtv. szerinti közfeladatot ellátó szerveknek. Kivételt jelentenek ez alól azok a szervezetek, melyek jogszabály által meghatározott közfeladatot látnak el (pl. egyes közalapítványok). Ebből következően a nem közfeladatot ellátó szervekre – így a társadalmi szervezetekre, alapítványokra vonatkozó adatok – nem közérdekű adatok. Viszont a rájuk vonatkozó jogi szabályozás

bizonyos adatkörben – így a nyilvántartásba vételt, a pályázati döntéseket illetően – biztosítja a nyilvánosságot. Törvény elrendeli az NCA Tanácsa és Kollégiumai döntéseinek közzétételét, de nem rendelkezik az egyes pályázatok és azok dokumentációjának megismerhetőségéről. Azonban ezek nyilvánossága is indokolt lehet, mert ez a jogszabályban meghatározott nyilvános adatkör bővítése a pályázati eljárás és a döntések tisztaságát, a közpénzek felhasználásának átláthatóságát szolgálja. *(442/P/2007)*

Cégadatok és nyilvánosság

A közelmúltban több vizsgálat érintette a Cégközlöny adatainak felhasználását. Egy beadványozó arról kért állásfoglalást, hogy ezek az adatok rögzíthetőek-e, másolhatóak-e, korlátozás nélkül felhasználhatóak-e. Egy másik beadványozó vitatta annak jogszerűségét, hogy a Cégközlöny szerzői jogi védelem áll, és ezért sem részben, sem egészben nem másolható, nem továbbítható. A Cégközlöny az Igazságügyi és Rendészeti Minisztérium ma már kizárólag CD-formátumban elérhető hivatalos lapja, mely egyebek mellett tartalmazza az új cégek adatait, az adatokban bekövetkezett változásokat, a gazdálkodó szervezetek átalakulási közleményeit, a céghirdetményeket, a csődeljárásról, felszámolásról szóló bírósági határozatokat.

A Cégközlöny közzététele a cégnyilvántartás nyilvánosságát biztosító kötelezettség. A vizsgált kérdés az, hogy ha a Cégközlöny adatai nyilvánosak, akkor jogszerű-e a továbbfelhasználás, másolás tilalma, és jogszerű-e, hogy ha valaki céginformációhoz kíván jutni, akkor a Cégközlönyt nem csekély ellenérték fejében meg kell vásárolnia, ráadásul úgy, hogy az adatok kötelező közzétételének költségét az adatot szolgáltató cégek már megfizették. Alkotmányunk nemcsak a közérdekű adatok megismerésének jogát, hanem azok terjesztésének jogát is deklarálja. Jelenleg a CD-formátumban elérhető Cégközlöny licencszerződése a szoftver egyedi használatát biztosítja, azt tilos másolni, módosítani, mivel – a kiadó, illetve a szerkesztő szerint – a kiadvány szerzői jogi védelem alá tartozik.

Az ügy vizsgálatának lezárását követően ajánlás született. Az ebben foglaltak szerint nem indokolt és jogilag nem megalapozott a jogszabályban előírt közfeladatként előállított adatbázisok/dokumentumok szerzői jogi védelem alá helyezése. A Cégközlöny készítése és nyilvánosságra hozatala – az adatok felhasználást lehetővé tevő rendszerezése, adatbázisba rendezése

– közfeladat. E közfeladat ellátása közérdek – például a piaci forgalom biztonsága, jogbiztonság – érvényesülését szolgálja. A szolgáltató állam eszméjéből következően az államnak biztosítania kell az adatok könnyű elérhetőségét, egyszerűbb felhasználhatóságát, ezáltal is elősegítve a jogérvényesítést. Mindezt nem előzhetik meg sem az állam fiskális szempontjai, sem a Cégközlönyt előállító Magyar Hivatalos Közlönykiadó üzleti érdekei. Az álláspont szerint jogilag nem megalapozott, ha a szerkesztő, illetve a kiadó szerzői jogi jogosultságokra tart igényt, és korlátozza az adatok másolását, továbbítását. Mindez nem értelmezendő úgy, hogy a Cégközlönyért nem kérhető semmiféle díjazás, és a cégnyilvánosság nem feltétlenül teljes ingyenességet jelent. Méltányolható az adatok kezelőjének azon érdeke, hogy a sokszorosítás költségei megtérüljenek, a költségtérítés azonban nem foglalhat magába egyéb díjelemet. Összefoglalva az ajánlást: a jogszabályban előírt közfeladatként előállított adatbázisokat nem illetheti meg a szerzői jogi védelem. Ezért felkértük az igazságügyi és rendészeti minisztert, hogy vizsgálja felül Cégközlöny szerzői jogi védelem alá helyezésének megalapozottságát, a Cégközlöny adatai felhasználhatóságát, és tegye meg a szükséges intézkedéseket e kérdések rendezése érdekében. *(80/K/2007, 1663/K/2007)*

C. Az adatvédelmi biztos jogalkotással kapcsolatos tevékenysége

A korábbi évekhez hasonlóan idén is a jogalkotással kapcsolatos tevékenységünk számszerű adatait vesszük sorra, majd ezt követi a jogszabályvéleményezés és a jogi szabályozási kezdeményezéseink ismertetése. Válogatnunk és csoportosítanunk kell a bemutatásra szánt ügyeinket. A kiválasztott tervezetek tárgyalhatók például a hivatalunkhoz érkezés sorrendjében, vagy aszerint, hogy melyik minisztérium felelősségi körébe tartozott a jogszabály előkészítése. Mégsem így csoportosítjuk az ügyeket, mert a puszta időrendnél fontosabbak a tervezetek összefüggései, és mert az adatvédelmi biztos jogalkotással kapcsolatos tevékenységének nem a kormányzati szervekkel való kapcsolattartás a lényege, hanem az adatvédelem és az információszabadság elősegítése. Ezért külön-külön tárgyaljuk a személyes adatok védelme, illetve a közérdekű adatok nyilvánossága szempontjából értékelendő szabályozási elképzeléseket, problémákat és észrevételeinket, ezen belül a tervezetek tartalmi-, logikai szempontok szerinti csoportosítására törekedve. Ettől a szerkesztési elvtől csak az átfogó, kódex-jellegű szabályozást előkészítő tervezetek, így különösen az új Polgári Törvénykönyv esetében tér el e beszámoló.

Statisztika

Jogforrások szerinti összesítés

	2005	2006	2007
Törvény	130	48	99
Kormányrendelet	111	103	196
Miniszteri rendelet	158	127	244
Országgyűlési határozat	(Nincs adat)	1	0
Kormányhatározat	43	21	56
Egyéb	46	26	38
Összesen	488	326	634

A fenti adatsorok alapján szembeötlő a véleményezendő tervezetek számának jelentős növekedése, amely az előző évihez képest összességében közel kétszeres, de a korábbi maximumhoz, a 2005-ös adathoz képest is nagyjából egyharmadnyi.

A fenti táblázatban összesített 634 tervezethez még hozzá kell számítani azt a 82-t, amely a több fordulós egyeztetés során átdolgozott szöveggel érkezett ismételt véleményezésre, nem is szólva a jogalkotással kapcsolatos, hivatalból indított vizsgálatokról. Az összesen 716 jogszabálytervezet és az ahhoz kapcsolódó hivatalos levelezés 517 ügyiratban mintegy 400 Megabyte adatot, továbbá öt és fél folyóméternyi iratállományt tesz ki.

A növekedés okait vizsgálva megállapítható, hogy idén nőtt a jogalkotás volumene, például az előző évi 133 törvényhez és 365 kormányrendelethez képest 178 törvény és 410 kormányrendelet megalkotására került sor. A véleményezésre megküldött tervezetek számának növekedése meghaladja a kihirdetett jogszabályok számának növekedését, ami vélhetően annak tudható be, hogy a kormányzati jogszabály-előkészítő tevékenység az év utolsó harmadában volt a legintenzívebb, azonban az ebben az időszakban véleményezett tervezetek egy részének kihirdetésére csak jövőre fog sor kerülni.

Információs ágak szerinti összesítés

Az Adatvédelmi Biztos Irodájánál vizsgált állampolgári panaszokra és a konzultációs ügyekre általában igaz, hogy egy konkrét problémával, megválaszolandó kérdéssel találkozunk, amely könnyen karakterizálható aszerint, hogy melyik, az adatvédelmi biztos feladatköréhez tartozó alapjoggal mutat összefüggést. A véleményezett jogszabálytervezetek információs alapjogok szerinti csoportosítása korántsem ilyen egyszerű, hiszen a jogszabályok néhány kivételtől eltekintve – amilyen például az Avtv. – nem kifejezetten valamely alkotmányos előírás érvényre juttatása céljából jönnek létre, hanem azért, mert az államnak a jogi szabályozás eszközével kell rendeznie valamely életviszonyt vagy életviszonyokat. A jogszabály szabályozási tárgykörének meghatározásakor általában az azonos vagy összetartozó életviszonyok egységes jogszabályi rendezése a fő szempont, és ezt inkább csak kiegészíti a többi elméleti, jogi rendszertani megfontolás. Ezért esetleges, hogy valamely véleményezendő jogszabálytervezet a személyes adatok védelmével, vagy a közérdekű adatok nyilvánosságával, vagy mindkét

alapjoggal mutat összefüggést, már ha egyáltalán tartalmaz az adatvédelmi biztos által vizsgálandó rendelkezést.

Külön dilemmát okoz a véleményezett jogszabálytervezetek alapjogok szerinti besorolásánál, hogy a közérdekből nyilvános adatok nyilvánosságának előmozdítása is az adatvédelmi biztos feladatkörébe tartozik. Személyes adatok is tartoznak a közérdekből nyilvános adatok közé. Az ilyen személyes adatok kezelésére vonatkozó jogszabályt egyszerre kell a személyes adatok védelme és a közérdekből nyilvános adatok nyilvánossága szempontjából megítélnünk. Nem elméleti, hanem gyakorlati, ügyviteli szempontok alapján soroljuk azonos csoportba a közérdekű adatok nyilvánosságával és a közérdekből nyilvános adatok nyilvánosságával kapcsolatos tervezeteket.

A fentieket előrebocsátva megállapítható, hogy 2007-ben a véleményezett tervezeteknek körülbelül 72 százaléka elsősorban a személyes adatok védelmével kapcsolatban volt vizsgálandó, míg a fennmaradó mintegy 28 százaléka a közérdekű adatok nyilvánosságával vagy a közérdekből nyilvános adatok nyilvánosságával.

Havonkénti összesítés

Jan.	Feb.	Már.	Ápr.	Máj.	Jún.	Júl	Aug.	Szept.	Okt.	Nov.	Dec.
41	39	51	50	48	58	32	34	45	110	57	69

A korábbi évekhez hasonlóan az év utolsó negyedének hónapjaiban érkezett a legtöbb tervezet.

Előterjesztő minisztériumok szerinti összesítés

EüM	FVM	GKM	HM	IRM	KüM	KvVM	MeH	OKM	ÖTM	PM	SZMM	Más szerv
116	16	72	2	69	13	96	20	83	33	57	43	14

(Az Igazságügyi és Rendészeti Minisztérium minden törvénytervezet társelőterjesztője, azonban a táblázat IRM rovatában csak azon tervezetek adatai szerepelnek, amelyek előkészítéséért az IRM az első helyen felelős.)

A fentiek szerint látszólag az EüM és a KvVM az adatkezeléssel kapcsolatos jogszabályok legnagyobb kibocsátója. Ez azonban csak részben igaz. A KvVM-ben előkészített tervezetek egy részének véleményezése valóban fontos számunkra, minthogy a környezeti adatokhoz való hozzáférés szabályozása a közérdekű adatokhoz való jog kiemelt figyelmet érdemlő részterülete, azonban emellett szép számban érkeznek a KvVM-ből olyan előterjesztések is, amelyek még közvetett összefüggésben sincsenek az információs alapjogokkal. 2007-ben a KvVM-ből érkezett a legtöbb olyan tervezet, amelyet feltehetőleg tévedésből küldtek meg az adatvédelmi biztoshoz. Bár az ilyen tervezetek véleményezése feleslegesen szaporítja a munkánkat, ehhez azt is hozzá kell tenni, hogy más jogalkotási eljárási hibák sokkal veszélyesebbek az alapvető jogokra. Ezen a ponton említést érdemel az Egészségügyi Minisztérium 2007-es jogszabály-előkészítő tevékenysége, amelyet azért kell kritikával illetnünk, mert véleményünk szerint az egészségügyi-egészségbiztosítási jogszabályok gondosabb előkészítést igényelnének. 2007-ben számos alkalommal kellett kifogásolni a méltatlanul rövid véleményezési határidőket és az elektronikus információszabadságról szóló törvény jogszabály-előkészítésre vonatkozó szabályainak megszegését.

> Az adatvédelmi biztos a jogszabály-előkészítési eljárás hiányosságaival kapcsolatos kifogásait a tervezetekről írt állásfoglalásaiban jelezte *(például 141/J/2007, 350/J/2007, 2185/J/2007, 2219/J/2007, 2221/J/2007)*. Az egészségügyi pénztárakról és a kötelező egészségbiztosítás természetbeni ellátásai igénybevételének rendjéről szóló törvénytervezet esetében azonban a törvényjavaslat benyújtását követően az Országgyűlés Egészségügyi Bizottsága elnökének is jelezte, hogy véleménye szerint a közigazgatási egyeztetés során nem teljesült az a törvényi követelmény, mely szerint a véleményadás határidejét az előkészítőnek úgy kell megállapítania, hogy a véleményező megalapozott véleményt adhasson, és azt a tervezet előkészítésénél figyelembe lehessen venni. *(2082/J/2007)*

Meglepő, hogy még 2007-ben, jóval az elektronikus információszabadságról szóló törvény hatálybalépése után is szinte mindegyik minisztériumból jelentős számban érkeznek olyan tervezetek, amelyeknek „Nem nyilvános!" jelölése ellentétes a jogszabály-előkészítés nyilvánosságára vonatkozó szabályokkal. Ez ugyanúgy kifogásolandó, mint a közigazgatási egyeztetésre bocsátott jogszabálytervezetek elektronikus közzétételének törvénysértő elmulasztása.

A határidők

A jogszabálytervezet véleményezési határidejét az annak előkészítéséért felelős miniszter vagy államtitkár, szakállamtitkár határozza meg a jogalkotási törvény és a vonatkozó egyéb állami normák figyelembevételével. 2006. márciusa óta állnak rendelkezésre részletes, elemzésre alkalmas adatok. Ezek szerint 2006. március – december közötti időszakban átlagosan 5,84 munkanap jutott egy tervezet véleményezésére. 2007-ben ez az időtartam átlagosan 5,38 munkanapra csökkent. Nem lehet általános érvénnyel kimondani, hogy mennyi idő szükséges egy tervezet véleményezéséhez, tekintettel arra, hogy a jogszabálytervezetek terjedelmüket, bonyolultságukat tekintve igen eltérőek, ezért elég csak a nyilvánvalóan túl rövid véleményezési határidőkről szólni: 2007-ben 68 esetben állt rendelkezésre egy munkanap, vagy annál rövidebb idő a tervezetről való állásfoglalásra. Ez a 716 tervezetnek mintegy 9,5 százaléka.

Összefoglalás, következtetések

A jogalkotással kapcsolatos ügyszámunk a 2006-os visszaeséstől eltekintve az ezredforduló óta folyamatosan nő, azonban az idei ügyszám ilyen mérvű növekedése nem volt előre látható. Egy adat a növekedés arányainak érzékeltetésére: 2007 októberben 125 (110 új és 15 átdolgozott) tervezet érkezett véleményezésre, míg 2000-ben az egész évben összesen 136.

Örvendetes, hogy a minisztériumok 2007-ben az előző évhez képest ritkábban mulasztották el tervezetek egyeztetését az adatvédelmi biztossal. Erre abból lehet következtetni, hogy 2006-hoz képest jobban nőtt a véleményezett tervezetek száma, mint a kihirdetett jogszabályoké.

Munkánk feltételeit idén legfőképp az befolyásolta, hogy jelentősen nőtt az ügyszám (különösen ősztől), ugyanakkor feszítettebbé vált a jogszabályelőkészítés tempója. A jogalkotással kapcsolatos feladataink tehát növekedtek, azonban az Adatvédelmi Biztos Irodája hivatali apparátusának létszáma nem nőtt, hanem csökkent. Több körülmény jelzi, hogy az adatvédelmi biztos munkaszervezete teljesítőképessége határai közelébe jutott:

- A jogalkotással kapcsolatban hivatalból indított vizsgálatok száma 2007-ben nem követte a véleményezett, illetve a kihirdetett jogszabályok számának 2006 óta tapasztalt növekedését.

- Sajnálatos módon az előző évhez képest érzékelhetően többször fordult elő az előterjesztő által meghatározott véleményadási határidő túllépése.
- Le kellett mondani a kihirdetett jogszabályok folyamatos monitorozásáról, mert kötelező feladataink ellátása mellett erre már nem volt lehetőség. Emiatt nem állnak rendelkezésre adatok arról, hogy milyen arányban fogadták el az adatvédelmi biztos szabályozással kapcsolatos észrevételeit és javaslatait.

Tevékenységünk eredményességi indikátorainak kidolgozása tehát a jövő feladata. A törvényalkotás figyelemmel kísérését mindazonáltal továbbra is folyamatosan végezzük. 2007-ben 116 adatkezeléssel összefüggő törvényjavaslatot regisztráltunk, ebből 80 törvényjavaslat sorsát kísértük figyelemmel, de csak néhány esetben vált szükségessé, hogy az adatvédelmi biztos észrevételeivel és javaslataival az Országgyűlés illetékes szakbizottságához forduljon. E javaslatokat a beszámoló jogalkotási kezdeményezésekről szóló részében ismertetjük.

A jogszabálytervezetek véleményezése - adatvédelem

Az egészségügyi ellátási és a társadalombiztosítási reform

Az egészségügyi ellátórendszer és általában az egészségbiztosítási rendszer reformja erőltetett ütemű jogszabály-kibocsátást igényelt – ez utóbbiról már volt szó az ügyeink szektorális statisztikai elemzéséről szóló részben. A reformok tartalmáról csak annyiban tisztünk állást foglalni, amennyiben azok a személyes adatok védelmével és a közérdekű adatok nyilvánosságával összefüggnek. Ilyen összefüggések márpedig bőven akadnak. Tapasztalataink szerint az intézményrendszer reformja olyan kedvezőtlen hatásokkal járhat a személyes adatok védelmére, amelyeket a jogalkotó nem látott előre, vagy nem ismert fel teljesen.

> Az egyes, az egészségügyet érintő kormányrendeleteknek a vizitdíj és a kórházi napidíj bevezetésével kapcsolatos módosításáról szóló kormány-előterjesztés véleményezése során azt kifogásolta az adatvédelmi biztos, hogy a vizitdíj visszatérítési kérelmet a jegyzőnél kell előterjeszteni, a kérelemhez csatolva az igénybevett szolgáltatásokról kiállított nyugtát, illetve számlát. Így fennáll a veszélye annak, hogy az

érintett egészségi állapotával kapcsolatos bizalmas információk illetéktelen kezekbe jutnak. *(20/J/2007)*

A megszűnő és átalakuló kórházak egészségügyi dokumentációjának sorsára vonatkozó adatvédelmi biztosi vizsgálat eredményét összefoglaló ajánlás *(903/H/2007)* egyebek mellett felhívta az egészségügyi minisztert arra, hogy az adatvédelmi törvényben előírtaknak megfelelően hozzon létre, vagy jelöljön ki a dokumentáció kezelésére országos hatáskörű intézményt és készítse elő az átadandó dokumentáció kezelésére való törvényi felhatalmazásra vonatkozó szabályozás tervezetét. A szakminisztérium az ajánlásban foglaltakra válaszul példás gyorsasággal megküldte az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény módosításáról szóló tervezetet, amely rendelkezik az egészségügyi dokumentációk sorsáról, bár a tervezett szabályozás decentralizált archiválási modellt vázolt fel. Az egészségügyi dokumentációval kapcsolatos szabályozási igény tényének elfogadása mindenképp értékelendő, azonban kifogásolni kellett, hogy a tervezett normaszöveg sem a dokumentációt átvevő szerv lehetséges szervezeti formáját nem határozta meg, ahogy azt sem hogy az adatot átvevő szerv milyen egyéb feladatokat láthat még el az iratok tárolásán és kezelésén kívül. Így az intézményfenntartók egyedi döntésükkel tulajdonképpen bármilyen jogi személyt bevonhatnak az egészségügyi ellátóhálózatba és egészségügyi adatkezelővé tehetik azt. Az állásfoglalás szerint fennáll a lehetősége, hogy költségtakarékossági okból arra alkalmatlan adatkezelőkhöz kerülnek a különleges adatokat tartalmazó egészségügyi dokumentációk. *(2185/J/2007)*

Az előbbi eset kapcsán közbevetve megjegyezzük, hogy nem az egészségügy az egyetlen olyan terület, amelynél az átszervezések kapcsán fontos adatok „rossz kézbe" kerülésétől kell tartani. A *1859/J/2007* számú ügyben azt kifogásoltuk, hogy a Rendőrségről szóló törvény módosítása meg kívánja nyitni az utat a rendőrségi adatállományok feldolgozásának nem állami szervhez történő kiszervezése előtt.

A száz százalékban állami, illetve helyi önkormányzati tulajdonú közhasznú vagy gazdasági társasági formában működő aktív fekvőbeteg szakellátást biztosító egészségügyi szolgáltatók 2007. évi létszámcsökkentésének költségvetési támogatásáról szóló kormányrendelet tervezete szerint a Magyar Államkincstár a támogatásokról szóló értesítést név szerint részletezett adatszolgáltatással kiegészítve továbbítja az egészségügyi miniszter és a pénzügyminiszter számára, noha nekik

> nincs teendőjük a személyes adatokat tartalmazó listákkal. A kormányrendeleti szinten előírni kívánt, készletező adatgyűjtésre vonatkozó észrevételünk nyomán az előterjesztő ígéretet tett a kifogásolt adattovábbítás elhagyására. *(527/J/2007)*

A reform előtörténetéhez tartozik, hogy az adatvédelmi biztos 2004-ben beadvánnyal fordult az Alkotmánybírósághoz, az Irányított Betegellátási Modell adatkezelési rendelkezéseivel szemben. Az Alkotmánybíróság 36/2007. (VI. 6.) AB határozata nem fogadta el a beadvány érveit, azonban azt megállapította, hogy jogbiztonságot, valamint a személyes adatok védelméhez való jogot sértő – mulasztásban megnyilvánuló – alkotmányellenes helyzet keletkezett azáltal, hogy az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, valamint a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény, az ellátásszervezők által történő adatkezelésre vonatkozó tájékoztatással összefüggésben nem alkotta meg mindazokat az eljárási szabályokat, amelyek biztosítják, hogy az érintett adatai kezelésének megtiltásáról az adattovábbítást megelőzően nyilatkozhasson. Az Alkotmánybíróság 2007. december 31-ig adott időt a mulasztás pótlására.

A egészségbiztosítási reformintézkedések adatvédelmi értékelésének még nem jött el az ideje, mert a közigazgatási egyeztetés során megismert normatervezet az Országgyűléshez való beterjesztést megelőzően és azt követően is megváltozott, és még a beszámoló készítésekor sem tekinthető véglegesnek, továbbá a törvényhez tartozó nagyszámú végrehajtási rendelet tartalma sem ismert. A tervezett szabályozásnak jelenleg több homályos pontja van, olyannyira, hogy az egészségügyi pénztárakról és a kötelező egészségbiztosítás természetbeli ellátásai igénybevételének rendjéről szóló T/4221. számú törvényjavaslat alapján nem lehetett pontosan meghatározni, hogy a törvény értelmében mely szervek tekintendők társadalombiztosítási szervnek és melyek nem. *(2082/J/2007)*

A szakazonosítók kezelése

Az eddig ismertetett jogeseteink nem érintik az állami feladatellátás szervezeti reformjának alkotmányosságát és a reformok irányát, hanem csak bizonyos kapcsolódó adatvédelmi elvárásokra – például a normavilágosság követelményeinek megfelelő adatkezelési szabályozás, vagy a személyes

adatok biztonságos tárolásának előírása – mutatnak rá. Van azonban olyan, a személyes adatok védelméhez tartozó követelmény, amelynek érvényesítése az állami szervezetalakítást is befolyásolhatja.

Az Alkotmánybíróság 46/1995. (VI. 30) AB határozatának indoklása mutatott rá, hogy az Alkotmányból a személyes adatok felhasználását illetően – az alapjogi védelem szempontjait érvényesítve – a célhozkötöttség elve, és az osztott információs rendszerek alkotmányos követelménye határozható meg. A nevezett AB határozat nyomán született meg a személyi azonosító jel helyébe ágazatspecifikus szakazonosítókat léptető 1996. évi XX. törvény, amely pontosan meghatározza, hogy milyen állami feladatok ellátásához melyik szakazonosító használható. A törvény elhatárolja egymástól a három szakazonosító – a TAJ szám, az adóazonosító jel és a személyi azonosító – alkalmazási területét, kizárva a szakazonosítók összekapcsolásának lehetőségét. Éppen ezért lehetséges adatvédelmi veszélyforrásnak tekintünk minden olyan szabályozási elképzelést, amely a szakazonosítók használatának kiterjesztésére irányul, vagy gyengítené a szakazonosítók elkülönítésére vonatkozó előírások érvényesülését.

2006-ban az egyes pénzügyi tárgyú törvények módosításáról szóló 2006. évi CXXXI. törvény előkészítése során az adatvédelmi biztos súlyos aggodalmát fejezte ki az adóhatóság TAJ szám kezelésére való felhatalmazása miatt. Végül a törvénymódosítást nem lehetett megakadályozni, mert az előterjesztő Pénzügyminisztérium informatikai szükséghelyzetre hivatkozott *(1726/J/2006)*. Idén a Szociális és Munkaügyi Minisztérium kért állásfoglalást az adatvédelmi biztostól a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény módosításáról szóló törvénytervezetről. A véleményezendő tervezet szerint a munkáltató részéről történő éves konszolidált adatszolgáltatás az állami adóhatósághoz kerül. A biztos válaszában emlékeztetett arra, hogy az adóhatóság „szerepidegen" feladata ellentétbe kerülhet az osztott információs rendszerek alkotmányos elvével. *(1593/J/2007)*

Az egészségügyi pénztárakról és a kötelező egészségbiztosítás természetbeli ellátásai igénybevételének rendjéről szóló törvény tervezetét egyebek mellett azért kellett kifogásolni, mert a tagszervezőt is felhatalmazza a TAJ szám kezelésére. *(2082/J/2007)*

A szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról szóló 2007. évi I. törvénnyel, valamint a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló 2007. évi II. törvénnyel összefüggő egyes kormányrendeletek

módosításáról szóló kormányrendelet tervezete több idegenrendészeti eljárásban is elő kívánta írni, hogy a kérelmező bocsássa az eljáró hatóság rendelkezésére a személyi azonosítóról és a lakcímről szóló hatósági igazolványának másolatát. Ezt azért kellett kifogásolni, mert a másolaton szereplő személyi azonosító olyan szervhez kerülhetne, amely az 1996. évi XX. törvény alapján nem jogosult annak kezelésére. *(847/J/2007)*

A szabálysértési jogsegélyről szóló törvény közigazgatási egyeztetésre bocsátott tervezete szerint szabálysértési jogsegély ügyben mind a személyi azonosító, mind a társadalombiztosítási azonosító jel továbbítható külföldre. Ez az előírás elsősorban nem is az osztott információs rendszerek követelménye miatt volt kifogásolandó, hanem a célhozkötött személyes adatkezelés követelménye miatt, hiszen a nevezett szakazonosítók külföldön, más államok hatóságai által nem használatosak. *(312/J/2007)*

Az elmúlt évi beszámoló is felhívta a figyelmet arra, hogy egyre több adat és adatkezeléssel kapcsolatos jogkör koncentrálódik az állami adóhatóságnál. A fenti ügyeink között is van olyan, amely ezt a megállapítást támasztja alá. Ismeretes, hogy az adóhatóság szerepet kap a társadalombiztosítási jogviszony-ellenőrzések lefolytatásában is. Érthető, ha a kormányzat egységes, hatékony pénzügyi ellenőrző szervezetet kíván kiépíteni, azonban azt is szem előtt kell tartani, hogy az 1996. évi XX. törvény nem teszi lehetővé a szakazonosítót használó adózási, illetve társadalombiztosítási adatkezelések összekapcsolását. Nem tudható, hogy hosszabb távú koncepcióba illeszkedik-e az adóhatóság újabb és újabb hatáskörökkel való felruházása, azonban bármilyen további hatáskör-bővítés előtt elvi síkon tisztázni kellene, hogy hogyan és mennyiben egyeztethető össze az állami adóhatóság adatkezelési felhatalmazásainak bővítése az osztott információs rendszerek követelményével.

Elektronikus kormányzat

A közigazgatás korszerű informatikai hátterének kiépítése hosszú távú, bonyolult és költséges folyamat, amelynek csak egyik lényeges eleme a technikai, pénzügyi és szervezési feltételek biztosítása mellett a jogi szabályozás. A célkitűzések és a mindenkori feladatok nem törvényben öltenek testet, hanem elsősorban kormányhatározatokban. E határozatok az állami

irányítás egyéb jogi eszközei közé tartoznak, melyek véleményezése nem az adatvédelmi biztos törvényben nevesített feladata. Ennek ellenére helyeselhető, hogy az előkészítők rendszeresen kikérik az adatvédelmi biztos véleményét a különféle fejlesztési koncepciókról és a hasonló, a Kormány döntését igénylő tervezetekről, mert így idejekorán rá lehet mutatni a személyes adatok védelme szempontjából kifogásolható elképzelésekre.

Az E-közigazgatás 2007-2010 stratégiáról szóló előterjesztésről adott adatvédelmi biztosi állásfoglalás üdvözölte, hogy a dokumentum elegendő figyelmet szentel a személyes adatok védelmének, de utalt arra, hogy a központi elektronikus Ügyfélkapu bizonyos interakciók megvalósítására jelenleg nem megfelelő és további fejlesztések szükségesek a biztonságos személyazonosítás megvalósítása érdekében *(2270/J/2007)*. A problémákat a Központi Elektronikus Szolgáltató rendszerről szóló előterjesztésről adott vélemény *(892/J/2007)* és az egészségügyi miniszternek szóló levél *(511/K/2007)* részletezi.

Az E-közigazgatás 2010 Programtervben említett állampolgári közműrendszer kapcsán a rendszert felhasználók szerepköreinek konzisztens azonosításáról esik szó. Bár ennek mibenléte a tervezetben nincs kifejtve, emlékeztetünk arra, hogy az adatvédelmi biztos korábban egy hasonló elképzelés kapcsán leszögezte: nem lehet cél az állampolgárok különféle jogosultságainak központi nyilvántartását és elektronikus ellenőrzését végző rendszer létrehozatala. *(2270/J/2007)*

A Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek működésének, biztonsági előírásainak, informatikai katasztrófatervének, eszköz- és vagyonmentésének szabályozásáról szóló előterjesztés kapcsán több fordulós egyeztetést folytattunk az Elektronikus Kormányzat Központ (EKK) munkatársaival a Központi Rendszerben kialakított elektronikus állampolgári fórum működéséről. E fórumban bárki kifejtheti a véleményét közéleti kérdésekről, például a kormányzat és a közigazgatás működésével kapcsolatban. A fórum használatát a Központi Rendszerben regisztrált felhasználók számára biztosítják, tehát a hozzászólók személyazonosítása lehetséges. A fórumot fenntartóktól kapott tájékoztatás szerint azért nem akarták lehetővé tenni a névtelen hozzászólásokat, mert biztosítani kívánták a Központi rendszer, mint kritikus infrastruktúra védelmét, továbbá nem tartják kívánatosnak az anonim fórumokon esetleg kialakuló durva hangnemet, végül biztosítani akarták a jogi fellépés lehetőségét a törvény által büntetendő tartalmú hozzászólásokkal szemben. A fórumon való hozzászólás nem kötelező

és minden felhasználó megfelelő tájékoztatást kap a fórum igénybevételének feltételeiről.

Az EKK álláspontját tiszteletben tartva rámutatunk arra, hogy az EKK – mint kormányzati szerv – olyan, önként megadott adatok birtokába jut, amelyekből következtetni lehet a felhasználók egyik legérzékenyebb különleges adatára, a politikai véleményére. Nincs tudomásunk arról, hogy bárki is ezen adatok eredetitől eltérő célú felhasználását tervezné, mégis fel kell hívni a figyelmet arra, hogy egyre több, állami, önkormányzati szerv hoz létre politikai vélemények befogadására alkalmas elektronikus fórumot. *(418/J/2007)*

A közigazgatásban használt elektronikus személyazonosítási rendszerről adott állásfoglalás nem értett egyet azzal, hogy a központi ügyfél-azonosítási rendszer használatát az állami informatikai rendszereken kívül az egyéb nagy szolgáltató rendszerek, például a tömegközlekedés számára is megnyissák. Az a gondolat azonban üdvözlendő, hogy ki-ki maga dönthessen arról, kívánja-e az általa igényelt azonosító eszköz kontaktus nélküli leolvashatóságát. A tervezett eszközök és azonosítási módok bevezetése lehetőleg ne kötelezően, hanem egyéni kérésre, az érintett számára maximális rendelkezési lehetőséget és alternatívát biztosítva történjen. *(2419/J/2007)*

Nem az elektronikus közigazgatás témaköréhez tartozik, mégis itt érdemes megemlíteni, hogy az önkéntes kölcsönös biztosító pénztárakról, illetve a magánnyugdíjpénztárakról szóló egyes kormányrendeletek módosításáról szóló tervezet egyeztetése során is azt javasoltuk, hogy a személyes adatokat tartalmazó elektronikus pénztári kártya igénybevétele opcionális legyen, továbbá biztosítani kell az érintettek jogát ahhoz, hogy a kártyán tárolt adataikhoz közvetlenül hozzáférjenek.

Az elektronikus azonosítás problémájának aktualitását érzékelve 2007 decemberében ajánlás született az elektronikus ügyintézés során történő azonosítás adatvédelmi követelményeiről. Az ajánlás egy lehetséges modellt kínál az elektronikus azonosítás magánélet-barát megvalósítására, elfogadva, hogy létezhet más jó megoldás is. *(2581/H/2007)*

A rendvédelmi szervezetek adatkezelése

2007-ben a rendvédelmi tárgyú jogszabálytervezetek többsége a schengeni csatlakozással és a rendőrség-határőrség integrációjával kapcso-

latban készült. A schengeni csatlakozás története a beszámoló nemzetközi ügyekről szóló fejezetében szerepel. Itt a következőket emeljük ki:

A Rendőrségről szóló 1994. évi XXXIV. törvény módosítására irányuló tervezetben üdvözlendő az igazoltatás szabályainak módosítása, az igazoltatás során felvett adatok túl hosszú tárolási idejének csökkentése. Az Avtv. szerint az érintettet megillető tájékoztatási jogra, illetve a közérdekű adatok igénylésére vonatkozó szabályok szerint bárki tájékoztatást kérhet az igazoltatásának okáról, a felvett adatokról és azok továbbításáról. Az állásfoglalás javasolja a rendőrségi térfigyelő kamerák elhelyezésének korlátozását, mert túl általános az a felhatalmazás, amely értelmében a rendőrség közterületen bárhol, bármikor, bárkit megfigyelhet. A magánszféra nem szűkíthető le a magánlakásra, és az egyénnek közterületen is joga van arra, hogy bizonyos térben megfigyelés nélkül tartózkodhasson és mozoghasson. Az adatvédelmi biztos álláspontja szerint csak azok a közterületek vonhatók folyamatos képrögzítéssel megfigyelés alá, ahol ez a közbiztonság érdekében igazolhatóan szükséges. Fontos még, hogy bárki egyszerűen tájékozódhasson arról, hogy hol vannak közterületi megfigyelő eszközök elhelyezve. A szabályozás módosításának előkészítése során indokolt a civil szervezetekkel való konzultáció. *(1859/J/2007)*

Az egyes büntetőjogi tárgyú törvények módosításáról szóló törvény tervezetének egyik érzékeny pontja szintén a büntetés-végrehajtás rendészeti célú elektronikus megfigyelő eszközeinek használata volt, mivel a tervezett módosítás felhatalmazást kíván adni az ilyen eszközök büntetés-végrehajtási intézeten kívüli telepítésére is. Az adatvédelmi biztos a készülő törvénymódosítás kapcsán tájékoztatta az Igazságügyi és Rendészeti Minisztérium szakállamtitkárát azokról az ABI-nál folyó vizsgálatokról is, amelyek olyan adatvédelmi problémákat tártak fel, amelyek büntetőjogi tárgyú jogszabály módosításával orvosolhatók. Ezekről a jogalkotási kezdeményezéseinkről szóló részben még lesz szó. *(1855/J/2007)*

A hatályos jogban a rendvédelmi szervek titkos információgyűjtő tevékenységét az adott szervezetekre vonatkozó törvények párhuzamosan szabályozzák. A titkosszolgálati eszközök és módszerek bűnüldözési célú alkalmazásáról szóló törvénytervezet a szabályozási párhuzamosságok felszámolását és a joganyag egységesítését kívánta elérni. Ez alkalmat adott a titkos információgyűjtéshez kapcsolódó adatvédelmi garanciák újragondolására. Az adatvédelmi biztos az állásfoglalásában többek között javasolta a titkos információgyűjtés alá

vonható személyek körének pontosabb meghatározását és a titkos információgyűjtés céljának megvalósulásához nem szükséges adatok törlésére vonatkozó szabályok szigorítását. Tiszteletben tartjuk a jogalkotónak azt a döntését, hogy a nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének szabályozását ezúttal nem vonja a felülvizsgálat körébe. *(1941/J/2007)*

Nemzetközi elvárás alapján bevezetendő jogkorlátozó szabályok

2007-ből több olyan jogkorlátozásra irányuló szabályozási tervezet is említést érdemel, amelyek megalkotását nem annyira hazai társadalmi viszonyok rendezésére irányuló szabályozási igény tette szükségessé, mint inkább nemzetközi kötelezettség, megállapodás, vagy legalábbis elvárás.

Az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvénytervezet a személyes adatok védelme szempontjából annyiban előrelépés, hogy a korlátozó intézkedésekhez kapcsolódó adatkezelés szabályozását törvényi szintre emeli. Az előterjesztés első változata a vagyoni korlátozó intézkedések végrehajtását bűnmegelőzési intézkedésnek tekintve a rendőrségi törvény bűnmegelőzési adatkezelési szabályainak alkalmazását kívánta előírni. Az adatvédelmi biztos rámutatott, hogy a törvény alkalmazása során a rendőri tevékenység nem azonosítható a bűnmegelőzéssel és nem is illenek rá a bűnmegelőzési adatkezelési szabályok, ezért az utalásos szabályozási technika nem megfelelő. Ezután az előterjesztő az adatvédelmi biztos javaslatának megfelelően koncepcionálisan átdolgozta az adatkezelésről szóló részt. *(891/J/2007)*

Ugyancsak nemzetközi elvárásnak megfelelően kellett szigorítani a pénzmosás és a terrorizmus megelőzésére és megakadályozására szolgáló pénzügyi ellenőrzési szabályokat. Az adatvédelmi biztos állásfoglalása 14 észrevételt és javaslatot fogalmazott meg a törvénytervezettel kapcsolatban. Egyebek mellett rámutatott arra, hogy az „összefüggő ügyletek" pontatlan törvényi meghatározása és a szabályok helytelen alkalmazása miatt a pénzintézetek egy része feleslegesen követeli meg az ügyfélazonosítást olyan esetekben, amikor a néhány ezer forintos átutalások címzettjei például a közüzemi szolgáltatók. A tervezet nem körvonalazta megfelelően, hogy a pénzügyi szolgáltatók milyen körben kötelesek az adatok és az ügyfél által tett nyilatkozatok ellenőrzésére. A biztos álláspontja szerint sérti a személyes adatok védelmét, hogy az érintettek olyankor sem kaphatnak tájékoztatást a

pénzmosás gyanújáról tett bejelentésről, ha az utóbb alaptalannak bizonyul. *(764/J/2007)*

A CXXXVI. számon kihirdetett törvényben változatlanul maradt az érintett tájékoztatási jogát sértő szabály, ezért az adatvédelmi biztos a törvény végrehajtási rendeletében, a pénzügyi szolgáltatók által elkészítendő belső szabályzat kötelező tartalmi elemévé javasolta tenni azt, hogy az érintett ügyfél adattörlésre és helyesbítésre irányuló kérelmét olyankor is érdemben meg kell vizsgálni, és a törvényes feltételek fennállása esetén teljesíteni kell, ha a kérelem eredményéről az érintett nem tájékoztatható. *(2552/J/2007)*

Európa szerte heves társadalmi vitákat váltanak ki az elektronikus hírközlési adatok megőrzésére kötelező szabályok. Hazánknak is jogharmonizációs kötelessége volt az Európai Parlament és az Európai Unió Tanácsa által elfogadott, a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról szóló 2006/24/EK irányelv nemzeti jogba történő átültetése. A jogharmonizációs célú törvény előkészítésének 2007-ben többször is nekifutott a Gazdasági és Közlekedési Minisztérium.

Az adatvédelmi biztos a törvénytervezet véleményezése során felhívta a figyelmet a 95/46/EK Irányelv 29. cikke alapján létrehozott adatvédelmi munkacsoport véleményére. A munkacsoport szerint a forgalmi adatok megőrzése sérti az egyént megillető magánélet tiszteletben tartásához, valamint a közlés bizalmasságához és a személyes adatok védelméhez való jogot, melyet az emberi jogokról szóló európai egyezmény biztosít. A tagállamok a terrorizmus és a szervezett bűnözés elleni küzdelem jegyében nem fogadhatnak el bármilyen, általuk szükségesnek vélt intézkedést. Az adatok megőrzésére ezért csak az irányelvben meghatározott célból kerülhet sor, de csak az e célra minimálisan szükséges adatkörben, az egyéb célra megőrzött adatoktól elkülönítve és csak meghatározott bűnüldöző szervek számára hozzáférhetővé téve.

A törvénytervezet egyeztetése során a fenti szempontok érvényesítésére törekedtünk, mert meggyőződésünk, hogy hazánkban az állampolgárok biztonságának megőrzéséhez nem szükséges az irányelvben foglaltak valamiféle túlteljesítése. A törvénytervezet véleményezése több fordulóban, írásban és szekértői megbeszéléseken történt. Az egyeztetés során problémaként jelentkezett, hogy a terve-

zet sem az egyes adatkezelési célokat, sem az azokhoz rendelt adatköröket nem határozta meg, és határolta el megfelelően. Az adatok megőrzési határideje is ellentmondásos volt. Például kérdéses, hogy miért kellene megőrizni a sikertelen hívások adatait is, noha az irányelvből ilyen tartalmú szabályozási kötelezettség nem következik. Az azonban előrelépésként értékelhető, hogy az átdolgozott tervezet nem a lehetséges maximális adatmegőrzési időt kívánja előírni, hanem csak egy évet. *(17/J/2007, 1926/J/2007)*

A fenti felsorolás nem teljes. A 2007-es nemzetközi indíttatású, korlátozó jellegű tervezetek közé tartozik még például a Közösség területére belépő, illetve a Közösség területét elhagyó készpénz ellenőrzéséről szóló, 2005. október 26-i 1889/2005/EK európai parlamenti és tanácsi rendelet végrehajtásáról szóló törvény tervezete *(142/J/2007)*, vagy a tagállamok és harmadik országok közötti légiközlekedési szolgáltatásokra vonatkozó megállapodások tárgyalásáról és végrehajtásáról szóló 2004. április 29-i 847/2004/EK európai parlamenti és tanácsi rendelet 5. cikkében foglalt eljárási szabályok megállapításáról szóló Korm. rendelet tervezete. *(979/J/2007)*

Az Adatvédelmi Biztos Irodája 2007-es, nemzetközi vonatkozású jogalkotással kapcsolatos tevékenysége kapcsán meg kell említeni a kétoldalú szociális egyezmények előkészítésében való részvételünket – ezek az egyezmények a fenti példáktól eltérően természetesen nem korlátozó jellegűek. Észrevételekkel és javaslatokkal segítettük a koreai, a boszniai és hercegovinai, a montenegrói, az ukrán és a macedón partnerekkel kötendő szociális biztonsági egyezmények előkészítését, továbbá részt vettünk a szociális biztonsági egyezmények végrehajtására szolgáló igazgatási megállapodás modelljének kidolgozásában. *(5/J/2007, 161/J/2007, 1937/J/2007, 2034/J/2007, 2218/J/2007, 2692/J/2007)*

Az állami támogatások

Az állam által nyújtott különféle támogatásokhoz kapcsolódó adatkezelésről készülő szabályozási tervezetek vizsgálata mind a személyes adatok védelme, mind a közérdekű adatok nyilvánossága – a közpénzek felhasználása – szempontjából szükséges. A beszámolónak ebben a részében a támogatások adatvédelmi szempontú megítéléséről lesz szó.

A 2006-os beszámoló szólt a lakosság energiafelhasználásának szociális támogatásáról szóló 231/2006. (XI. 22.) Korm. rendeletre vonatkozó

adatvédelmi biztosi kifogásokról. Az észrevételek nyomán a szociális és munkaügyi tárca előkészítette az egyes szociális tárgyú törvények módosításáról szóló törvény tervezetét (2007. évi CXXV. törvény), amely a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény 54/D. §-ába iktatta az energiafelhasználási támogatás adatvédelmi biztos által hiányolt szabályait *(870/J/2007)*. A törvényi szabályozást követően új kormányrendelet készült a törvényben foglaltak végrehajtására. Ez a 2007. november 1-jén hatályba lépett 289/2007. (X. 31.) Korm. rendelet a lakossági vezetékes gázfogyasztás és távhőfelhasználás szociális támogatásáról *(1965/J/2007)*. Az új szabályok alkalmazását is figyelemmel kísérjük. Az első tapasztalatok szerint az új szabályozás általában megfelelő, azonban előre nem látható problémaként jelentkezett, hogy a hőelosztásos mérést használó társasházakban a támogatás jogszerű igénybevételének ellenőrzéséhez olyan lakások hőfelhasználásáról is adatokat kell gyűjteni, amelyekben élők nem részesülnek energiaár támogatásban.

Az egészségkárosodott személyek szociális járadékairól szóló Korm. rendelet tervezetének véleményezése során a biztos azt állapította meg, hogy a törvényi felhatalmazást nélkülöző, elsődleges jogalkotói jogkörben megalkotott kormányrendelet lesz, amely különleges adatok kezelését is elő kívánja írni. Bár a tervezett normaszöveg több helyen utalt a társadalombiztosítási nyugellátásról szóló törvényre, egyértelmű, hogy nem annak végrehajtási rendeletéről van szó, így a törvény adatkezelési szabályai sem vonatkoztathatók a vizsgált kormányrendelet tervezetre. Az adatvédelmi biztos állásfoglalásában jelezte: nem vállalhatja annak ódiumát, hogy hátrányos helyzetben élő emberek azért ne juthassanak a nekik járó járadékhoz, mert ez erről szóló jogszabály adatvédelmi kifogás miatt nem hirdethető ki, azonban rendkívül fontosnak tartja az adatkezelés törvényi hátterének mielőbbi rendezését. A szakminisztérium államtitkára válaszlevelében ígéretet tett erre. *(2322/J/2007)*

A felsőoktatásban résztvevő hallgatók juttatásairól és egyes térítésekről szóló kormányrendelet tervezete szerint a hallgató szociális helyzetének megítéléséhez „figyelembe lehet venni különösen" a hallgató által is lakott közös háztartásban élők számát, jövedelmi és vagyoni helyzetét. Az adatvédelmi biztos emlékeztetett arra, hogy ő és hivatali elődje a hasonló – nemcsak az oktatásban előforduló, szociális alapú – támogatások elbírálásával kapcsolatban kezdettől azon az állásponton volt, hogy a rászorultság elbírálásához nem elengedhe-

tetlenül szükséges a vagyoni helyzetre vonatkozó adatok kezelése. *(38/J/2007)*

Oktatási és kulturális célú adatkezelés

Az Oktatási és Kulturális Minisztérium jogszabály-előkészítő tevékenysége mindenképp említést érdemel, hiszen 2007-ben a minisztériumok között a harmadik legtöbb, összesen 83 adatkezeléssel kapcsolatos tervezetet bocsátottak egyeztetésre.

A közoktatásról szóló 1993. évi LXXIX. törvény módosításáról szóló előterjesztésről adott biztosi állásfoglalásunk összefoglalóan megállapítja, hogy a közoktatásban egyre nagyobb mennyiségű adatot gyűjtenek össze, amely nem felel meg az adatminimalizálás követelményének. Az adatvédelmi biztos kifogásolta a pályakövetési rendszer egyes adatkezelési szabályainak félreérthető megfogalmazását, így az anonim adatszolgáltatás és a személyes adatok továbbításának összemosását is. *(577/J/2007)*

A felsőoktatásról szóló 2005. évi CXXXIX. törvény módosításáról szóló törvény tervezetét szinte pontosan ugyanazokkal a kritikai észrevételekkel kellett illetni, mint az előbb vázolt közoktatási törvénymódosítást. A felsőoktatási törvény módosításánál még szembeötlőbb volt az adatgyűjtés kiterjesztése és az adatbázisok számának növekedése, amely készletező, szükségtelenül párhuzamos adatgyűjtéseket elrendelő rendszer kiépülésének lehetőségét vetíti előre. *(628/J/2007)*

A Deák Ferenc ösztöndíjról és a Klebersberg Kúnó ösztöndíjról szóló kormányrendelet-tervezetek egyeztetése során az ösztöndíjban részesülők névsorának közzétételét kifogásolta az adatvédelmi biztos. *(580/J/2007, 732/J/2007)*

A munka világa

Ügyeink következő csoportjában az a közös, hogy olyanok – köztisztviselők, hivatásos állományú katonák, rendvédelmi dolgozók, közalkalmazottak vagy a Munka Törvénykönyve szerint munkát vállalók, esetleg kamarai tagsághoz kötött hivatást gyakorlók – adatainak védelmében léptünk fel, akik gyenge érdek- és jogérvényesítő pozícióban vannak a jogviszony másik pólusán lévő szervvel szemben.

A köztisztviselők jogállásáról, a közalkalmazottak jogállásáról és a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról, valamint a Magyar Honvédség hivatásos és szerződéses állományú katonáinak jogállásáról szóló törvények módosításáról szóló előterjesztés köztisztviselőkre vonatkozó fejezetével kapcsolatban, a biztoshoz korábban érkezett panaszok tömege alapján arra kellett felhívni a figyelmet, hogy nem elégséges, ha a törvény általában lehetőséget ad a pályáztatás során a közelebbről meg nem határozott kompetencia vizsgálatokra és „egyéb kiválasztási módszerek, eljárások" alkalmazására. Fontos, hogy a felvételi vizsgálatok lefolytatása megfelelő, részletes szabályozás alapján történjék. *(205/J/2007)*

Az előbbi törvénytervezetben ellentmondásosak voltak a pályázatok adatainak megőrzésére vonatkozó szabályok. A pályázati iratok kezelése nem csak a köztisztviselők esetében problematikus, hanem a közalkalmazottaknál is. A közalkalmazottak jogállásáról szóló törvény nem tartalmaz részletes pályáztatási adatkezelési szabályokat, ezért az adatvédelmi biztos a törvény ágazati végrehajtási rendeleteibe javasolta beépíteni a pályázati dokumentációk sorsát megfelelően rendező szabályokat. Az adatvédelmi biztos 2007-ben az egészségügyi, a szociális, valamint gyermekjóléti és gyermekvédelmi, továbbá a környezetvédelmi és vízügyi ágazati végrehajtási rendeletekhez tett ilyen észrevételt. *(1508/J/2007, 1570/J/2007, 1639/J/2007, 2607/J/2007)*

A kormányzati személyügyi igazgatási feladatokat ellátó szerv által lefolytatott pályáztatás rendjéről, annak szervezéséről és lebonyolításáról, a toborzási adatbázisról, valamint a pályáztatási eljáráshoz kapcsolódó nyilvántartásról szóló kormányrendelet tervezete szerint az irányított beszélgetés keretében felmérhető a pályázó személyisége. Az adatvédelmi biztos arra figyelmeztetett, hogy az elbeszélgetésnek lehet ugyan járulékos hozadéka a pályázó személyiségével kapcsolatos szubjektív benyomások szerzése, azonban az eljárás nem válhat valamiféle személyiségtesztté, mert így olyan eszköz kerülne a pályáztatók birtokába, amely messze túlmutatna az adatkezelés eredeti, törvényes célján. *(2531/J/2007)*

A Magyar Könyvvizsgálói Kamaráról, a könyvvizsgálói tevékenységről, valamint a könyvvizsgálói közfelügyeletről szóló törvény tervezete szerint nem vehető fel a kamara tagjai körébe, aki az életmódja vagy magatartása miatt a könyvvizsgálói hivatás gyakorlásához szükséges közbizalomra érdemtelen. Az adatvédelmi biztos szerint ez az előírás csak abban az esetben fogadható el, ha a törvény pontosan, a célhozkötött adatkezelés követelményére tekintettel meghatározza,

hogy mely adatkezelő, milyen forrásból származó, kire vonatkozó és milyen fajtájú személyes adatok felhasználásával vizsgálhatja a jelentkező életvitelét és magatartását. *(586/J/2007)*

A katonai szolgálati viszony méltatlanság címén történő megszüntetésének eljárási szabályairól szóló HM rendelet tervezete a fegyelmi eljárás rendjéhez sok tekintetben hasonlóan kívánta szabályozni a méltatlansági eljárás rendjét. Lényeges különbség azonban, hogy míg a fegyelmi eljárás szabályait a törvény meghatározza, addig a méltatlansági eljárásról szinte csak egy végrehajtási rendeletalkotási felhatalmazás található a törvényben. A hiányzó adatkezelési szabályok miniszteri rendeleti úton nem pótolhatók és a méltatlansági eljárásról szóló rendelet nem terjesztheti ki magára a fegyelmi eljárás törvényi szabályainak hatályát. *(1891/J/2007)*

Az új Polgári Törvénykönyv

Az új polgári jogi kódex előkészítése több éves folyamat, amely 2007-ben még nem zárult le. Az Igazságügyi és Rendészeti Minisztérium februárban, majd októberben bocsátotta közigazgatási és társadalmi egyeztetésre a normaszöveg tervezetét. A törvény előkészítői az első szövegváltozathoz tett adatvédelmi biztosi észrevételek közül többet elfogadtak, illetve időközben párhuzamosan olyan törvénymódosítások indultak el, amelyek a további javaslataink egy részét – például jogi személyekre vonatkozó nyilvántartások nyilvánosságával kapcsolatos kifogást vagy a házassági vagyonjogi nyilvántartás szabályozására vonatkozó észrevételt – okafogyottá tették.

Az új Ptk. átdolgozott tervezetében elsősorban az üzleti titok újraszabályozását kellett kifogásolni. A Polgári Törvénykönyv 2003 óta hatályos szövege megnyugtatóan rendezte az üzleti titok védelme és a közérdekű adatok nyilvánossága közötti korábbi konfliktust. Az eltelt négy év tapasztalatai alapján nem szükséges a módosítás. A know-how védelmét a mai rendelkezések is biztosítják. A javaslat a kérdés szabályozásának mai, áttekinthető – a közérdekű adat és az üzleti titok fogalmát világosan szétválasztó – logikáját megbontja, ezáltal a javasolt szöveg megértésén fáradozó jogalkalmazót is komoly megpróbáltatásnak teszi ki. Különösen áll ez a jogi védelem alatt álló és a jogi védelem alatt nem álló üzlet titok, azaz közérdekű adat fogalmának megkonstruálására. Ez feloldhatatlan dilemma elé állítja az adatkezelőt: vagy jogosulatlanul hozzáférhetővé teszi a jogi

védelem alatt álló üzleti titkot, kártérítési pert, netán büntetőeljárást kockáztatva, vagy törvénysértően megtagadja egy jogi védelem alatt nem álló üzleti titok kiadását, ezzel közigazgatási pert, illetőleg ugyancsak büntetőeljárást kockáztatva.

Szintén problematikusnak tekintjük a tulajdoni lap nyilvánosságával kapcsolatos szabályokat. A tervezet értelmében az ingatlan-nyilvántartási tulajdoni lap tartalma korlátozás nélkül megismerhető; azt bárki személyazonosítás nélkül, internetes honlapon, térítésmentesen megtekintheti. Álláspontunk szerint a tulajdoni lapon feljegyzett jogosultak adataira vonatkozó adatszolgáltatás csak olyan adatigénylők számára teljesíthető, akiket megfelelően azonosítottak. Azt javasoltuk, hogy az eljáró szerv naplózza az adatigénylőket és a hozzáférhetővé tett személyes adatokat. Ez azért szükséges, mert az Avtv. szerint a természetes személynek joga van a reá vonatkozó adatszolgáltatásokról való tájékoztatásra, és ez a jog olyankor is megilleti, ha az ingatlan-nyilvántartásban tárolt személyes adatai bárki számára hozzáférhetők. Az adatszolgáltatások nyilvántartása feltehetőleg segíthet kiszűrni az úgynevezett „ingatlan-maffia" jellegű bűncselekmények elkövetői által kezdeményezett adatlekérdezéseket is.

A fenti észrevételeken kívül javasoltuk még az új Polgári Törvénykönyv fogalomhasználatának összhangba hozását az Avtv. terminológiájával. *(237/J/2007)*

Az adatvédelmi biztos jogköre

Az információs alapjogvédelem intézményi oldalához hozzátartozik, hogy az adatvédelmi biztos hatékony jogi eszközökkel rendelkezzen törvényben meghatározott feladatai ellátásához, ezért helyénvaló a beszámolóban számot adni az adatvédelmi biztos jogkörét érintő szabályozási tervezetekkel kapcsolatos álláspontunkról.

A határterületről, valamint a határátkelőhely területére határátlépés céljából történő belépésről és tartózkodás szabályairól szóló kormányrendelet közigazgatási egyeztetése során az adatvédelmi biztos nem tartotta helyes megoldásnak, hogy a nevében eljáró munkatársai vizsgálat céljából csak előzetes időpont-egyeztetést követően léphessenek be a határátkelőhelyekre. Az országgyűlési biztosok számos vizsgálatának hitelességét és az esetleges jogsértések eredményes fel-

tárását éppen az ellenőrzések váratlansága biztosítja. A tervezett korlátozás nincs összhangban az Avtv.-vel. *(1970/J/2007)*

A katonai nemzetbiztonsági szolgálatok objektumaiba történő belépés rendjéről szóló HM rendelet a nemzetbiztonságról szóló 1995. évi CXXV. törvény (továbbiakban: Nbtv.) szabályai alapján teszi lehetővé az adatvédelmi biztos belépési és adatmegismerési jogának gyakorlását. Az Nbtv. az adatvédelmi biztos nemzetbiztonsági szolgálatokat érintő eljárására az állampolgári jogok országgyűlési biztosának az 1993. évi LIX. törvényben (továbbiakban: Obtv.) meghatározott jogosítványait rendeli alkalmazni, amelyekhez képest csak korlátozott többletjogosítványokat biztosít. Így az Nbtv. összességében korlátozza az adatvédelmi biztos jogosítványait a nemzetbiztonsági szolgálatokkal kapcsolatos eljárása során. Ez a szabályozási konstrukció lényegében változatlan az Nbtv. hatályba lépése óta, ugyanakkor az adatvédelmi biztos jogköre és eljárásának szabályai azóta többször megváltoztak. Az Európai Unióhoz történő csatlakozás során a jogharmonizációs törvénymódosítás az adatvédelmi felügyelő hatóság jogköreivel ruházta fel az adatvédelmi biztost. Ez után a 2005. évi XIX. törvény az adatvédelmi biztos eljárása és intézkedései tekintetében az Obtv.-t rendelte alkalmazni az Avtv.-ben meghatározott eltéréssel. E változtatások ellentmondást idéztek elő az Nbtv. és az Avtv. között.

Koncepcionális szinten abban ragadható meg az ellentmondás, hogy az adatvédelmi biztos hatósági jogkörével ellentétesek a korlátozások. A tárgyi jog szintjén abban mutatkozik ellentmondás, hogy az Avtv. 24/A. §-a az adatvédelmi biztos eljárására és intézkedéseire kizárólag az Obtv. szabályait rendeli alkalmazni, az Avtv.-ben meghatározott eltérésekkel. Ez a norma nem teszi lehetővé, hogy más törvény – például az Nbtv. – speciális szabályokat állapítson meg az adatvédelmi biztos eljárására és intézkedéseire. A kollízió törvényhozási úton oldható fel. *(1351/J/2007)*

A titkosszolgálati eszközök és módszerek bűnüldözési célú alkalmazásáról szóló törvény előkészítése során javasoltuk egyértelművé tenni: a titkos információgyűjtés során keletkezett adatok megismerésének korlátozása nem vonatkozik a feladatkörében eljáró adatvédelmi biztosra. *(1941/J/2007)*

A Rendőrségről szóló törvény módosítása a rendőrségi adatfeldolgozás kiszervezésének jóváhagyásában szánt volna szerepet az adatvédelmi biztosnak. Ezt a biztos visszautasította, annál is inkább,

mert egyáltalán nem értett egyet azzal, hogy a rendőrségi adatok privát adatfeldolgozók birtokába kerüljenek. *(1859/J/2007)*

2007. októberében átirat érkezett a Külügyminisztériumból, amelyben felkérték a biztost a magyar - moldovai idegenrendészeti kormányközi megállapodás adatkezelési részének megszövegezésére. Válaszában elhárította a felkérést, mert annak teljesítése nehezen lenne összeegyeztethető a független adatvédelmi biztos alkotmányos szerepkörével. *(2008/J/2007)*

A jogszabálytervezetek véleményezése - a közérdekű adatok nyilvánossága

Nem lehet fontosságuk alapján pontos rangsorba állítani a közérdekű adatok nyilvánosságával kapcsolatos, 2007-ben véleményezett tervezeteket. Az mindenesetre megállapítható, hogy az adatnyilvánosság iránti közérdeklődés megélénkült, mert a társadalmat irritáló korrupciós ügyek egyik lehetséges ellenszere a közpénzek felhasználásának jobb ellenőrizhetősége. Az is tapasztalható, hogy a környezet állapotáért való aggodalom fokozott elvárásokat támaszt a környezeti adatok hozzáférhetősége iránt. Indokolt ezért először ezekkel a kérdéskörökkel kapcsolatos adatvédelmi biztosi állásfoglalásokról beszámolni. Ezt követi azoknak a fontos törvénytervezeteknek – például a közigazgatási hatósági eljárási kódex novellája, vagy a minősített adatok védelméről szóló törvény tervezete – az ismertetése, amelyek egy-egy szabályozási területen lényegesen befolyásolhatják az információszabadság érvényesülését. Ezek közé sorolható még az új Polgári Törvénykönyv tervezete – különösen az üzleti titok és a közérdekű adatok nyilvánosságának kapcsolata miatt. Erről már volt szó a beszámolóban *(237/J/2007)*, ezért nem szükséges ismétlésbe bocsátkozni. Végül felhívjuk a figyelmet arra, hogy a jogalkotási kezdeményezésekről szóló, ezután következő alfejezet nagyobb része olyan adatvédelmi biztosi javaslatokat ismertet, amelyek a közérdekű adatok nyilvánosságának előmozdítását célozzák.

A közpénzek felhasználásának átláthatósága

Már a 2006. évi beszámolóban is kitértünk arra, hogy egyértelmű törvényi szabályokra van szükség az uniós források felhasználásának

megismerhetővé tétele érdekében. Idén az egyes törvények fejlesztéspolitikai tárgyú módosításáról szóló törvény tervezete az uniós támogatások átláthatósága érdekében új rendelkezéssel kívánta kiegészíteni az Avtv.-t.

> Egyértelmű az, hogy az uniós források felhasználásának nyilvánosságát növelni kell. A javasolt megoldás azonban több szempontból sem volt szerencsés. Az előterjesztésből nem derült ki, milyen adatok nyilvánosságát kívánja biztosítani. Nem derült ki, milyen megfontolások indokolják a még el nem bírált, illetve a vesztes kérelmek nyilvánosságát. A biztos úgy vélte, a jogalkotói cél elérésére jobb megoldás volna az államháztartásról szóló 1992. évi XXXVIII. törvény módosítása, illetve kiegészítése. *(914/J/2007)*

> A Betegjogi, Ellátottjogi és Gyermekjogi Közalapítvány Alapító Okiratának módosításáról szóló előterjesztés véleményezése során arra kellett emlékeztetni, hogy a Közalapítványnak, mint kiemelkedően közhasznú tevékenységet folytató, közfeladatot ellátó szervezetnek maradéktalanul meg kell felelnie az adatvédelmi törvény közérdekű adatok hozzáférhetővé tételére vonatkozó szabályainak. A Közalapítvány kezelésében lévő közérdekű adatok megismerését nem lehet előzetes időpont-egyeztetéshez kötni és a Közalapítvány székhelyén történő adatbetekintésre korlátozni. Az sem elégséges, ha közfeladatot ellátó szerv a honlapján csak a „legfontosabb" közérdekű adatait teszi közzé. Fontos, hogy a közfeladatot ellátó szerv tevékenységére, működésére vonatkozó összes közérdekű adat könnyen és a lehető legteljesebb formában elérhető legyen az érdeklődők számára. *(1405/J/2007)*

A környezeti adatok nyilvánossága

A környezeti adatokhoz való jog megkerülhetetlen alapdokumentuma a környezeti ügyekben az információhoz való hozzáférésről, a nyilvánosságnak a döntéshozatalban történő részvételéről és az igazságszolgáltatáshoz való jog biztosításáról szóló Aarhusban, 1998. június 25-én elfogadott Egyezmény, melyet a 2001. évi LXXXI. törvény hirdetett ki. Erre, valamint az Aarhusi Egyezménnyel összhangban megalkotott környezetvédelmi törvényre hivatkozva utasítottuk el, hogy az ENSZ Éghajlatváltozási Keretegyezménye és annak Kiotói Jegyzőkönyve végrehajtási keretrendszeréről szóló törvény tervezete szerint a törvény szabályozási körébe tartozó adatok közül csak az összesített adatok legyenek bárki számára hozzáférhetők.

Álláspontunk szerint a törvény szabályozási körébe tartozó minden adat közérdekű adat. Ezt az előterjesztő elfogadta. *(395/J/2207)*

A környezeti zaj- és rezgés elleni védelem szabályairól szóló kormányrendelet tervezete az érintett ingatlantulajdonosokra korlátozta volna a zaj- és rezgésvédelmi intézkedési terv tervezetébe történő betekintés jogát. A biztos, a környezet védelmének általános szabályairól szóló 1995. évi LIII. törvény környezeti adatok nyilvánosságára vonatkozó szabályai alapján, nem látta indokoltnak ezt. A környezethasználó közüzemnek biztosítania kell, hogy az általa okozott környezetterheléssel, környezet igénybevétellel, valamint környezetszennyezéssel összefüggő adatokról kérelemre bárki tájékoztatást kaphasson. *(1112/J/2007)*

A bányászatról szóló 1993. évi XLVIII. törvény végrehajtásáról szóló 203/1998. (XII. 19.) Korm. rendelet módosításáról szóló Korm. rendelet véleményezése során szintén azt kellett kifogásolni, hogy a tervezet az adatokhoz való hozzáférést az „érintett nyilvánosság" számára kívánta biztosítani. Az „érintett nyilvánosság" angol jogi szaknyelvből átemelt fogalma idegen az Avtv. fogalmi rendszerétől és a kormányrendeletben való használata nem segítené elő a jogbiztonság érvényesülését. Ennél is súlyosabb kifogás, hogy sem az Avtv., sem az Aarhusi Egyezmény, sem a környezetvédelmi törvény nem engedi meg a környezeti információkhoz való hozzáférés érdekeltséghez kötését. *(2665/J/2007)*

A védett természeti területek és értékek nyilvántartásáról szóló 13/1997. (V. 28.) KTM rendelet módosításáról szóló KvVM rendelet tervezete nem volt teljesen összhangban az adatvédelmi törvény rendelkezéseivel, mert a közérdekű adatok szolgáltatását a „közléssel kapcsolatban felmerült költségek" megtérítéséhez kötötte. Az Avtv. a közérdekű adatról készített „másolat készítésével kapcsolatban felmerült költségek megtérítéséről" rendelkezik. A KvVM szakállamtitkára elfogadta az adatvédelmi biztos észrevételét és módosították a tervezet kifogásolt részét. *(1203/J/2007)*

Hozzáférés a közigazgatási hatósági eljárásban kezelt közérdekű adatokhoz

A környezeti adatok nyilvánosságával kapcsolatban eddig ismertetett ügyeink mindegyike egyszersmind azt is példázza, hogy mennyi problémával jár a közigazgatási hatósági eljárásban, illetve a közigazgatási hatósági

nyilvántartásokban kezelt közérdekű adatokhoz való hozzáférés szabályozása, illetve a jogalkalmazás.

A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (továbbiakban: Ket.) 69. §-ának (6) bekezdése – a korábbi eljárási törvény szigorú iratbetekintési szabályait némiképp finomítva – meghatározott ügycsoportokban a hatóság által meghozott döntések nyilvánosságát írta elő. Ez a megoldás az információszabadság szempontjából bizonyos előrelépést jelentett, mert enyhítette a korábbi szigort, mely kizárólag az ügyfélnek biztosított jogot a hatósági ügyek iratainak megismeréséhez. A megoldás azonban nem oldotta fel az Avtv. és a Ket. közötti ellentmondást, csupán az első lépést tette meg annak érdekében, hogy az államigazgatási ügyekben általában is érvényesülhessen a 32/1992. (V. 29.) AB határozatban kifejtett elv: „a közérdekű információkhoz való szabad hozzáférés lehetővé teszi a választott népképviseleti testületek, a végrehajtó hatalom, a közigazgatás jogszerűségének és hatékonyságának ellenőrzését, serkenti azok demokratikus működését".

A Ket. hatálybalépése óta eltelt időszak jogalkalmazási tapasztalatai a szabályozás korrekciójának szükségességét vetették fel. Világossá vált, hogy a nevezett rendelkezésben több helyen is szereplő bizonytalan jogfogalmak („a lakosság jelentős részét érintő", „a jogokat közvetlenül érintő", „a környezet állapotát jelentősen befolyásoló") nem elégségesek a jogalkalmazó orientálására és az évtizedek óta alkalmazott hatósági gyakorlat megváltoztatására. A bárki számára hozzáférhetővé teendő döntések felsorolása sem teljes. Hiányzik a listáról a pénzügyi döntések nyilvánossága, noha ez a terület fokozottan ki van téve a korrupciós veszélynek. Indokolt lenne kiegészíteni a felsorolást a jogi személyekkel, jogi személyiség nélküli szervezetekkel és az egyéni vállalkozóknak a vállalkozásával kapcsolatban lefolytatott hatósági ellenőrzés keretében hozott, jogsértést és szankciót megállapító határozatokkal. A nyilvánosságra hozatal ugyanis a jogsértéstől visszatartó erővel bírhat és jogkövető magatartásra ösztönözhet. Hasonló előírások több közigazgatási jogszabályban (például fogyasztóvédelmi, adózási) találhatók, azonban garanciális jelentősége volna, ha a Ket. általánosságban is kimondaná. Ugyancsak fontos, hogy a törvény egyértelművé tegye: a környezeti információk nyilvánossága nem csorbítható a Ket.-re hivatkozva.

Amellett, hogy javaslatot tettünk a Ket. 69. § (6) bekezdésében foglaltak korrekciójára, felvetettük a Ket. nyilvánosságra vonatkozó szabályai átfogó felülvizsgálatának szükségességét. A Ket. szóban forgó rendelkezése nincs összhangban az Avtv.-vel, pontosabban a Ket. a közfeladatot ellátó szervek igen széles körének közérdekű adatkezelését illetően „felülírja" a közérdekű adatok megismeréséhez fűződő alkotmányos jogot szabályozó Avtv.-t. A közérdekű adatok megismeréséhez fűződő alkotmányos jog szabályozása körében nem az Avtv.-t kell egy eljárási törvényhez igazítani, hanem fordítva. Javasoltuk a szakértői egyeztetés megkezdését a minden bizonnyal alaposabb előkészítést igénylő módosítás megalapozásához. *(1169/J/2007)*

A minősített adatok védelméről szóló törvény

Hosszú évek óta vajúdik a minősített adatok védelméről szóló törvény előkészítése. Lassan összeszámolni is nehéz lesz, hány különböző koncepciót és szabályozási tervezetet készítettek a Belügyminisztériumban, majd a feladatot átvevő Miniszterelnöki Hivatal Nemzetbiztonsági Irodájánál. A 2005-ben az Országgyűlés elé terjesztett, majd később visszavont törvényjavaslat helyett új törvénytervezet készült, amelyet az előterjesztő 2007-ben több fordulóban, írásban, illetve népes értekezleteken egyeztetett *(1607/J/2007)*. Közben a törvénytervezet jelentősen átformálódott. A változások dokumentálása vagy akár csak a viták során képviselt adatvédelmi biztosi álláspont részletes ismertetése a felmerült kérdések bonyolultsága miatt túlmutat a beszámoló terjedelmi korlátain, ezért csak néhány fontosabb kérdésre koncentrálunk.

Az első ilyen lényeges szabályozási csomópont az információszabadság és a titokvédelem összeütközésének alkotmányos szabályozása. Helyes, hogy a véleményezésre bocsátott tervezet a minősítő feladatává tette azt, hogy a titkosításhoz fűződő érdekek mellett az adatok nyilvánosságához fűződő közérdeket is hivatalból tárja fel és vegye figyelembe. Ez az elv következetesen érvényesítendő a minősítés felülvizsgálata és a titoksértés büntetőjogi szankcionálása során is. A tervezett normaszöveg azonban nem volt kiforrott. A közérdekre való utalás ugyanis nehezen értelmezhető az alapjogi korlátozás alkotmányossági tesztjének dogmatikai rendszerében. Emellett kifogásolható volt az is, hogy csak az adatok nyilvánosságához fűződő „lényegesen nagyobb" közérdek fennállása esetén maradhat el a minősítés. Ha összemérhető az adatok titkosításához és a nyilvános-

ságához fűződő érdek, akkor az a helyes, ha törvény egyszerűen annak enged érvényesülést, amelyik erősebb. Szinte megoldhatatlan probléma elé állítja a jogalkalmazókat, ha nem egyszerűen azt kell mérlegelniük, hogy az államérdekkel szemben álló érdek, illetve jog nagyobb-e, hanem azt, hogy az lényegesen nagyobb-e az államérdeknél.

Újonnan felismert problémaként jelezte az adatvédelmi biztos, hogy ha a minősített iratot a minősítés érvényességi idejének lejárta előtt selejtezni lehet, akkor az abban lévő közérdekű adatok megismerhetőségét véglegesen kizárják, így a közérdekű adatokat az állampolgárok elől véglegesen elvonják. Ez hasonlóképp alkotmánysértő lehet, mintha az adatot végtelen időre minősítenék. A biztos javasolta, hogy a törvény zárja ki a minősített iratok selejtezését. Fontos, hogy a minősítés érvényességének megszűnése és az iratok selejtezése között biztosan legyen egy olyan időszak, amikor az iratok rendelkezésre állnak a tudományos kutatás és a közérdekű adatok megismerése számára. Ezt ki kellene egészíteni azzal, hogy a minősítők rendszeresen, például évente tegyék közzé az általuk minősített, érvényes minősítéssel rendelkező iratok mennyiségét.

Koncepcionális változást jelentett, hogy az egyeztetések nyomán a korábbi hosszú titokköri lista helyett a szöveg 6 pontban 11 fajta védendő érdekkörbe tartozó adatok minősítését kívánta lehetővé tenni. Ez a szabályozási mód (nem konkrét adatfajták, hanem adattípusok meghatározása) követi a titokszabályozás nemzetközi gyakorlatát, ugyanakkor vizsgálandó, hogy nem áll-e ellentétben az Avtv. 1. § (3) bekezdésével. („E törvény szerint megengedett kivételt csak meghatározott adatfajtára és adatkezelőre együttesen lehet megállapítani.")

A minősítések bírósági felülvizsgálatával kapcsolatban az adatvédelmi biztos álláspontja az volt, hogy egy alkotmányos jog védelmével és az Avtv.-vel a kétfokozatú bírósági eljárás áll összhangban (Avtv. 17. § és 21. §). A bíróságnak mind alaki, mind tartalmi értelemben kell vizsgálnia a minősítést. Voltaképpen ezt a fajta – kétfokozatú – bírósági felülvizsgálatot írja elő ma is az Avtv. A tervezet újdonsága nem ez, hanem az, hogy minősített személyes vagy közérdekű adat igénylése esetén a minősítő soron kívül köteles a minősítés indokoltságát felülvizsgálni. Az Avtv. 21. § (2) bekezdéséből ma is következik a bíróságoknak az a kötelezettsége, hogy formai és tartalmi értelemben is vizsgálják a minősítést.

A minősített adattal való visszaélés Btk.-beli szabályozásánál az információszabadság garanciáinak szempontjából az a megoldás támo-

gatható, hogy a szabályozás mindenképpen legyen differenciált. Nem hagyható figyelmen kívül, hogy a közérdekű adatoknak nemcsak a megismerése, de a terjesztése is alkotmányos jog. A korlátozásra (és ennek egyik legkomolyabb formája a büntetőjogi szankcionálás) vonatkozó szabályokra is érvényesek ezért az alapjogi korlátozásra vonatkozó alkotmányos szabályok és alkotmánybírósági határozatok. Ezekre is tekintettel az helyénvaló, hogy a civil személy csak szándékos elkövetés esetén legyen büntethető, továbbá, hogy legyen büntethetőséget kizáró ok, ha a bíróság megállapítja, hogy a minősített adat nyilvánosságra hozatalához nyilvánvalóan nyomósabb érdek fűződött, mint a titokban tartáshoz, és a bíróság legyen köteles minden esetben vizsgálni a minősítés tartalmi és formai értelemben vett jogszerűségét, valamint hogy az elkövetéskor még fennálltak-e a minősítés indokai.

A törvénytervezet további sorsáról nincs információnk. Az előkészítés több éves elhúzódása nem jogosít túlzott reményekre az új titoktörvény gyors elfogadását illetően, pedig azt már régóta várják azok az állami tisztviselők, akik minősített adatokkal dolgozva a gyakorlatban tapasztalják meg a hatályos titokszabályozás gyengeségeit, amelyekről a korábbi beszámolók is szót ejtettek.

A döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló törvény

A törvény azt célozza, hogy a költségvetési szervek és a többségi állami tulajdonban lévő gazdálkodó szervezetek birtokában lévő adatvagyont – közérdekű adatokat, anonimizált személyes adatokat és egyedi statisztikai adatokat – fel lehessen használni az állami döntéseket megalapozó hatásvizsgálatokhoz. A közérdekű állami adatvagyon ilyen célú felhasználásának alkotmányosságához nem férhet kétség, de a személyes adatok anonimizálása erős adatvédelmi garanciákat igényel.

Az első törvénytervezet abból indult ki, hogy amennyiben az adatkezelés során a személyazonosító adatokat úgynevezett „hash" kódra cserélik ki, akkor ezáltal az adatok személyes jellege megszűnik. A hash kód olyan adat, amelyet a személyazonosító adatokból hoznak létre egyirányú leképezést megvalósító algoritmus alkalmazásával, amely a kiinduló adatokból mindig ugyanazt az egyedi kódot állítja elő, ám a kódból az eredeti adatok nem nyerhetők vissza.

Ezt a megközelítést elvetettük, mert a kiinduló személyes adatok és a hash kód képzési algoritmus ismeretében utóbb az „anonim" feldolgozás során nyert adatok és a természetes személy közötti kapcsolat helyreállítható, következésképp az adatok újra megszemélyesíthetők. Ha az érintett és az adatok közötti kapcsolat nem véglegesen, hanem csak ideiglenesen, feltételesen szűnik meg, akkor az adatok személyes jellege megmarad.

Az adatvédelmi biztos olyan garanciális előírásokat javasolt beépíteni a törvénybe, amelyekkel az adatok anonimizálása biztonságossá válik:

- A hash képzési algoritmus adatfeldolgozásonként egyedi legyen, megelőzendő az eltérő célú adatfeldolgozásokban keletkezett adatállományok összekapcsolhatóságát.

- A hash képzési algoritmushoz külső szerv ne férhessen hozzá és azt az adatfeldolgozás után töröljék.

- A fentiekből következik, hogy hash-képzést és az anonimizált adatállományok összekapcsolását olyan szervnek kell végeznie, amely nem azonos az adatkérővel, illetve az adatforrásokkal.

- Ne lehessen olyan leválogatást kérni, amely csoportismérv alapján egyébként is „megszemélyesíthető" adatokat eredményez. E javaslat nyomán került a tervezetbe két korlátozás: a legalább 100 fős leválogatási egyedszám előírása, illetve a legfeljebb kistérség pontosságú címadat.

A javasolt módosításokat beépítették a törvénytervezetbe és így a törvényjavaslat koncepcionálisan elfogadhatóvá vált. Az adatvédelmi biztos mindazonáltal törvényes jogkörében eljárva figyelemmel fogja kísérni a törvény alkalmazását és szükség esetén javaslatot fog tenni annak módosítására. *(472/J/2007)*

A törvényjavaslat Országgyűléshez való beterjesztését követően az adatvédelmi biztos az Országgyűlés Emberi jogi, kisebbségi, civil- és vallásügyi bizottságának elnökét tájékoztatta a törvénytervezet előkészítéséről, illetve később az egyik országgyűlési pártfrakció kérésére is kifejtette álláspontját a törvényjavaslatról. *(1085/Z/2007)*

A jogalkotással kapcsolatos kezdeményezések

Nem tervezhető előre, hogy milyen jogalkotási kezdeményezéseket kell tennünk, hiszen ezekre elsősorban az állampolgári beadványok kivizsgálása

nyomán kerül sor. Az adatvédelmi biztosnak nincs befolyása arra, hogy milyen panasszal fordulnak hozzá. Ha utólag esetleg mégis hasonlóságok, összefüggések fedezhetők fel a jogalkotási kezdeményezéseink között, az attól függ, hogy milyen adatkezelési, adatvédelmi szabályozási problémákat tekintettek sérelmesnek, megoldandónak a hozzánk fordulók.

Egy újságíró a 2006. október 23-i események rendőri kezelését vizsgáló úgynevezett Papp-jelentés kapcsán az adatvédelmi biztoshoz fordult, miután az ORFK Szóvivői Irodája megtagadta kérdéseinek megválaszolását. A panasz vizsgálata során a biztos arra a következtetésre jutott, hogy a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény személyügyi nyilvántartásra, valamint az adatok megismerésének rendjére vonatkozó szabályai nincsenek összhangban az adatvédelmi törvény közérdekből nyilvános adatokra vonatkozó szabályaival. A probléma eddig sem volt ismeretlen, amit a 2006-ban hasonló ügyben kiadott adatvédelmi biztosi ajánlás is bizonyít. A közfeladatot ellátó személyek feladatkörével összefüggő személyes adatai nyilvánosságára vonatkozó jogszabályok összhangjának megteremtéséről szóló ajánlás olvasható a honlapunkon. A biztos az ajánlás másolatának megküldésével kezdeményezte az igazságügyi és rendészeti miniszternél a törvényi kollízió feloldását *(1522/P/2007)*. Később ez a probléma több panasz és konzultáció kapcsán is felmerült, például egy, az október 23-i tüntetések idején hibázó rendőr fenyítésére vonatkozó adatkéréssel kapcsolatban. Ez a szabályozási probléma megoldásának időszerűségére mutat rá. *(2294/P/2007, 2454/K/2007)*

Egy állampolgár arra kívánt választ kapni, hogy milyen okból tagadja meg a levéltár és a gyámhivatal az édesapja anyakönyvi kivonatában szereplő utólagos bejegyzésbe való betekintést. A beadvány hivatalunk gyakorlatában szinte minden évben visszatérő problémát érintett, amelyre az éves beszámolók rendre felhívják a figyelmet. Gondolatmenetünk kiinduló pontja, hogy a közeli hozzátartozó anyakönyvi adatai az adatok megismerését kérő hozzátartozóval is kapcsolatba hozhatók, ezért az ő személyes adatai is, és ezt az adatok megismerésének szabályozásánál is figyelembe kellene venni. A hatályos jogszabályi rendelkezések alapján az érintett még a saját eredeti anyakönyvi adataiba sem tekinthet be. Indokolt és szükséges lenne tehát az anyakönyvi eljárásra vonatkozó szabályok átfogó módosítása, az Alkotmánnyal és az adatvédelmi törvénnyel való összhang megteremtése. *(1843/P/2007)*

Az Országos Igazságszolgáltatási Tanács (OIT) Hivatala az adatvédelmi biztos állásfoglalását kérte a Bírósági Határozatok Gyűjteménye közzétételének rendjével kapcsolatban. Az elektronikus információszabadságról szóló törvény nem szabályozza, hogy kinek a feladata a határozatok anonimizálása, illetve kit terhel az ezzel együtt járó felelősség. A törvény szerint a közzétételről az OIT Hivatalának kell gondoskodnia. Azonban a törvény nem ad világos iránymutatást arra, hogy az adat előállítása, keletkezése, valamint a közzététele közötti adatkezelési műveletet melyik határozat esetében mely szervnek kell elvégeznie, ezért a biztos a törvény megfelelő kiegészítését kezdeményezte. *(1102/K/2007)*

A Köztársasági Elnök Hivatalából érkezett állásfoglalás-kérés a köztársasági elnök kegyelmi döntéseinek nyilvánosságával kapcsolatban. A biztos a vonatkozó alkotmányos előírások és a kapcsolódó jogszabályok áttekintése után megállapította, hogy a köztársasági elnök kegyelmi jogkörének gyakorlásáról, e közfeladat ellátásáról való tájékozódáshoz, az egyéni kegyelmezési jog mint sajátos jogintézmény érvényesülésének a társadalom általi figyelemmel kíséréséhez, valamint a bírósági tárgyalás nyilvánossága elvéből következően elfogadható a személyes adatok szűk körének, így az érintett nevének és a rá vonatkozó kegyelmi döntésnek a nyilvánossága. Ez azonban nem jelentheti az ügy minden részletének nyilvánosságra kerülését. Az adatvédelmi biztos felajánlotta, hogy igény esetén kezdeményezi az állásfoglalásban foglaltaknak megfelelő jogszabály-módosítást.
(473/K/2007)

Egy beadvány kapcsán vizsgálta a biztos az Észak-dunántúli Környezet-, Természetvédelmi és Vízügyi Felügyelőség környezeti hatástanulmánnyal kapcsolatos adatkezelését. A környezeti hatásvizsgálati eljárásról szóló 314/2005. (XII. 25.) Korm. rendelet szerint a hatástanulmány elektronikus adathordozón is benyújtható. Egy hatástanulmány több ezer oldalas dokumentum is lehet, és hagyományos módon történő másolása igen nehézkes, indokolatlan munkaterhet és költséget ró a hivatalokra. Az engedélykérő, környezethasználó köteles ugyan tájékoztatás nyújtására, azonban nem feltétlenül érdekelt abban, hogy a hatástanulmányt részletekbe menően bárki megismerhesse, ezért előfordul, hogy a dokumentum könnyebb és alaposabb megismerését nem segíti, hanem csupán az általa kiemelt információkat hangsúlyozza. A biztos ezért a környezeti adatok megismerésére vonatkozó jog hatékonyabb érvényesülése érdekében javasolta, hogy ha a környezeti hatástanulmány egésze vagy egy része elektronikus

adathordozón készült, akkor e vonatkozásban a környezethasználóknak ne csak tájékoztatási, hanem elektronikus közzétételi kötelezettségük is legyen, továbbá szöveges részét elektronikus adathordozón legyen kötelező benyújtani. Ez egyszerűsítené az adatkérők jogainak érvényesítését is, és a jelentős költségkímélés sem elhanyagolható szempont. *(803/P/2007)*

A megszűnő és átalakuló kórházak egészségügyi dokumentációjának sorsára vonatkozó adatvédelmi biztosi vizsgálat eredményét összefoglaló ajánlásról már volt szó, így azt most nem ismételjük. *(903/H/2007)*

2007-ben is folyamatosan nyomon követtük a törvényalkotás működését. Több tucat törvényjavaslatot vizsgáltunk meg, ám csak néhány esetben került sor az Országgyűlés szakbizottságainak megkeresésére, ha az ügy súlya ezt feltétlenül szükségessé tette.

A biztos a közellátás biztonsága szempontjából kiemelkedő jelentőségű vállalkozásokat érintő egyes törvények módosításáról szóló T/3660. sz. törvényjavaslattal kapcsolatban az Alkotmányügyi, igazságügyi és ügyrendi bizottság elnökét kereste meg. Levelében helyesnek tartotta a gazdasági társaságok és egyéb szervezetek vonatkozásában a tulajdonosi, képviseleti jogosultságra, vezető tisztségviselői minőségre és felügyelő-bizottsági megbízásra vonatkozó adatokról való adatszolgáltatás lehetővé tételét az üzleti kapcsolatok átláthatósága érdekében. Ugyanakkor a személyes adatok védelméhez fűződő jog aránytalan, a szükséges mértéken túli korlátozásának nevezte a magánszemélyek különféle tulajdonosi jogosultságai összességének bárki által való megismerhetővé tételét. A tulajdonosi jogosítványok megismerhetősége elfogadható azokban az esetekben, amikor a tulajdonos jelentős befolyással bíró, döntéshozó személy, azonban a megjelölt körön túl – pl. kisrészvényesek vonatkozásában – nem helyes a tulajdonosi viszonyok átláthatóvá tétele, mivel nincs olyan, alkotmányosan elfogadható indok, amely a személyes adatok védelmének ilyen mértékű korlátozását szükségessé tenné.

A közigazgatási egyeztetés során több fordulóban véleményezett, a mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló törvény tervezetét a Kormány a T/2082. számon nyújtotta be az Országgyűléshez. Az előterjesztő minisztérium állásfoglalást kért az adatvédelmi biztostól arról a parlamenti vita során felmerült módosí-

tó javaslatról, amely szerint a normatív támogatásokkal kapcsolatos adatokat is közzé kellene tenni, valamint, hogy a támogatások odaítélésével kapcsolatos valamennyi adat nyilvános legyen.

A biztos válaszában támogatta, hogy a hivatalok a közpénzekkel kapcsolatos adatok minél szélesebb körét ne csak egyedi adatigénylésre, hanem pro-aktív közzététellel is megismerhetővé tegyék. Az agrártámogatással összefüggő adatok közzététele a hazai és uniós közpénzekkel való gazdálkodás áttekinthetőségét, ellenőrizhetőségét szolgálja. A kedvezményezettek egy része azonban magánszemély, a kezelt adatok egy része ennél fogva személyes adat. A közérdekű adatok nyilvánosságához és a személyes adatok védelméhez fűződő alkotmányos jogoknak egymásra tekintettel kell érvényesülniük. A közpénzek átláthatóságának nem feltétele, ezért nem is indokolt, hogy a támogatott nevének, regisztrációs számának, a támogatás céljának, jogcímének és összegének közzétételén túl a természetes személyek lakcímadata is nyilvánossá váljon. *(37/J/2007)*

Az egészségügyi pénztárakról és a kötelező egészségbiztosítás természetbeni ellátásai igénybevételének rendjéről szóló törvényjavaslatról az Országgyűlés Egészségügyi Bizottsága elnökének írt levél is megemlítendő a törvényalkotás nyomon követése során készített állásfoglalások között. E levélről már volt szó a beszámolóban. *(2082/J/2007)*

Néha előfordul, hogy szerencsés véletlen folytán, vagy a szabályozási igény azonos időben történő felismerése miatt mintegy összetalálkozik egymással a jogalkotási kezdeményezés és szakminisztériumból érkező szabályozási tervezet.

A térfigyelő rendszerekkel kapcsolatos vizsgálatok tapasztalatai alapján az adatvédelmi biztos kezdeményezte az igazságügyi és rendészeti miniszternél, hogy intézkedjék a rendőrség kezelésében lévő közterületi megfigyelő rendszerek jogszerű működtetése érdekében. Ha a miniszter megítélése szerint a rendőrség képrögzítési lehetőségére vonatkozó törvényi szabályok ma már nem megfelelőek, akkor járjon el azok módosítása érdekében. A kezdeményezést követően nem sokkal érkezett a hivatalunkhoz a Rendőrségről szóló törvény módosításáról szóló tervezet, amely e terület újraszabályozását is előirányozta. Az adatvédelmi biztos javaslatait így be lehetett csatornázni a törvénymódosítás előkészítésébe. *(1722/H/2007)*

Az egyes büntetőjogi tárgyú törvények módosításáról szóló törvény véleményezésre küldött tervezete lehetőséget kínált a panaszbeadványok

kivizsgálásának tapasztalatait összegző büntetőjogi tárgyú szabályozási javaslataink megtételére:

Egy állampolgár a folyamatban lévő büntetőügyében, minősített adatokra vonatkozó vallomástétel kapcsán fordult a biztoshoz. Az adatvédelmi biztos eljárásának ez esetben törvényi akadálya volt, azonban a vonatkozó jogszabályok hivatalból történő áttekintése után az a következtetés adódott, hogy a büntetőeljárásról szóló törvény hatályos előírásai csak részlegesen szabályozzák a minősített adat büntetőeljárásban történő megismerését és felhasználását. A törvény 2002-es novellája megfelelően szabályozta a büntetőeljárás irataiban található államtitok és szolgálati titok megismerését, azonban nem vonja szabályozási körébe a szóban közölt minősített adat megismerését és felhasználását, így az lényegében a minősítő döntésétől függ. Az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény 17. §-a diszkrecionális jogkört biztosít a minősítő számára titoktartási kötelezettség alóli felmentés megadására – ez már önmagában is alkotmányossági aggályokat vet fel. A titoktartás alóli felmentés megtagadása sértheti a terhelt védekezéshez, illetve védelemhez való jogát. A biztos az észrevételekről tájékoztatta az Igazságügyi és Rendészeti Minisztérium szakállamtitkárát. *(1855/J/2007)*

A büntetőjogi tárgyú törvénymódosítás kapcsán arra is felhívta a figyelmet, hogy a tapasztalatok szerint a Btk. 177/A. §-ban szabályozott „visszaélés személyes adattal" törvényi tényállása nem megfelelő, amióta a jelentős érdeksérelem a bűncselekmény alapesetének tényállási eleme lett. Ezt a problémát korábban az 1650/J/2006-2. számú állásfoglalás részletezte. *(1855/J/2007)*

A közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet módosításáról szóló kormányrendelet tervezetének véleményezése során javasolta a biztos a hivatalhoz érkező küldemények felbontására és érkeztetésére vonatkozó szabályainak módosítását. Egy állampolgári panasz kivizsgálása nyomán tudott, hogy a korábbi iratkezelési szabályozás előírta a közfeladatot ellátó szervhez érkező, névre szóló, megállapíthatóan magánjellegű küldemények felbontás nélkül címzetthez továbbítását. Ez, a személyes adatok védelme szempontjából kedvező szabály sajnos 2005-ben kimaradt a módosítandó kormányrendeletből, ezért a biztos kezdeményezte annak megfelelő kiegészítését. Ezt az előterjesztő elfogadta. *(1493/J/2007)*

D. Államtitok és szolgálati titok

A korábbi beszámolókban a minősített adatokkal kapcsolatos tevékenységről szóló rész az Információszabadság fejezet része volt. Több oka is van, hogy a korábbi szerkesztési elvekkel szakítva idén külön fejezetet szánunk tevékenységünk e területének. Egyrészt a minősített adatok védelmét nemcsak a közérdekű adatok nyilvánosságával, hanem a személyes adatok védelmével szembeállítva is vizsgálnunk kell, minthogy a titokvédelem mindkét alapvető jogot korlátozhatja. Másrészt, 2007-ben folyt néhány olyan, minősített adatot érintő vizsgálat az Adatvédelmi Biztos Irodájában, amely akár a szélesebb nyilvánosság érdeklődésőre is számot tarthat, és amelyeknek fontosságukra tekintettel indokolt külön fejezetet szentelni. Előbb azonban néhány szó a szolgálati titokköri jegyzékekről.

A szolgálati titokköri jegyzékek

Meglehet, hogy utolsó alkalommal számolunk be az adatvédelmi biztos által véleményezett szolgálati titokköri jegyzékekről, ugyanis a hatályos titoktörvény (az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény) helyébe léptetni tervezett törvény a szolgálati titok kategóriát és így a szolgálati titokköri jegyzékeket megszünteti, bár még nem tudható, hogy a törvényhez tartozni fog-e egységes minősített adatköri jegyzék, vagy a törvényalkotó lemond a minősíthető adatfajták felsorolásáról.

2007-ben a következő szolgálati titokköri jegyzék tervezeteket véleményezte az adatvédelmi biztos:

- A Magyar Kereskedelmi Engedélyezési Hivatal szolgálati titokköri jegyzékéről szóló közlemény *(370/J/2007)*,
- Az Oktatási és Kulturális Minisztérium szolgálati titokkörének megállapításáról szóló OKM rendelet *(430/J/2007)*,
- A Rendőrség szolgálati titokköri jegyzékének kiadásáról szóló 2/2004. (I. 13.) ORFK utasítás módosításáról szóló ORFK utasítás *(706/J/2007)*,
- A Magyar Nemzeti Bank szolgálati titokköri jegyzékéről szóló 1/2005 (MK 1.) MNB közlemény kiegészítéséről szóló közlemény *(962/J/2207)*,
- A Szociális és Munkaügyi Minisztérium szolgálati titokkörének megállapításáról szóló SZMM utasítás *(1280/J/2007)*,

- A Vám- és Pénzügyőrség szolgálati titokköri jegyzéke *(1284/J/2007)*,
- A Rendőrség szolgálati titokköri jegyzéke – a határőrség integrációja után alkalmazandó szolgálati titokköri jegyzék *(2589/J/2007)*,
- Az Állami Számvevőszék szolgálati titokköri jegyzéke *(2609/J/2007)*.

A véleményezett tervezetekről általában megállapítható, hogy azok olyan adatfajtákat sorolnak fel, amelyekbe tartozó adatok megfelelhetnek a szolgálati titok törvényi ismérveinek. A jegyzékek néhány pontjánál felmerült, hogy az azokhoz tartozó adatok inkább az államtitok törvényi meghatározásának felelnek meg, mintsem a szolgálati titokénak, azonban e pontokat mégsem kifogásoltuk, tudván, hogy az államtitok minősítéshez irányadó szempontok szigorúsága miatt néha az ilyen, elismerten védendő adatokat csak a szolgálati titokká minősítéssel lehet a szükséges védelemben részesíteni. Ez egyébként az információszabadság szempontjából már csak azért sem kifogásolandó, mert a szolgálati titkok esetében a jogkorlátozás lehetséges időtartama rövidebb, mint az államtitok esetében.

Több szolgálati titokköri jegyzéknél tapasztalt törekvés a közfeladatok ellátásáról, illetve a különféle támogatásokról kötendő szerződések titkosításának lehetővé tétele. Megfelelő indokolás nélkül nem fogadható el, hogy az ilyen dokumentumok általában elzárhatók lennének a nyilvánosság elől. A közpénzek támogatási szerződések keretében történő felhasználásának ellenőrizhetőségéhez közérdek fűződik, ezért csak bizonyos területeken – ilyen lehet például a honvédelem, a rendvédelem vagy a gazdaságstratégia – , kivételesen kerülhet szóba a titokminősítés. A hatályos titoktörvény az Avtv. 19. §-ának (2) bekezdésre utalva korlátozza a közfeladatot ellátó szervek gazdálkodására vonatkozó adatok szolgálati titokká minősítését.

A másik típushiba a szakzsargon használata a védendő adatfajták meghatározásánál. A szolgálati titokkör elsősorban a minősítőknek szól, azonban egyszersmind az információkorlátozás határait kijelölő előírás, ezért az információszabadság és a jogbiztonság érdekében egyaránt fontos, hogy közérthető legyen. Nem szerencsés, ha a jegyzék olyan fogalmakat használ, amelyek csak a beavatottak számára érthetők.

Az olajügyek

2007-ben ismét a közérdeklődés fókuszába kerültek a 90-es évek úgynevezett olajszőkítési ügyei. Az év közepén kormányzati döntés született az olajbűncselekmények felderítése során keletkezett iratállomány felülvizsgálatára, anonimizálására és a törölt minősítésű iratok elektronikus közzétételére. Az iratállomány felmérésére és a felülvizsgálat szervezésére az iratbirtokos szervek, illetve azok jogutódai szakértőiből álló kormányzati munkacsoport jött létre. Az első híradások szerint szeptemberre tervezték a terjedelmes és bonyolult iratanyag felülvizsgálatának végrehajtását. Már felülvizsgált és anonimizált iratok ősz óta rendszeresen kerülnek fel az iratbirtokos szervek honlapjaira.

Az ügy iránti társadalmi érdeklődést tapasztalva, kezdettől hivatalból figyelemmel kísértük a történéseket, eredetileg azzal az elképzeléssel, hogy 2007 őszén, az iratfelülvizsgálat befejeztét követően tájékoztatást kérünk a munkabizottság tevékenységéről, és megvizsgáljuk a fenntartott minősítésű iratanyag minősítésének jogszerűségét. Az iratok felülvizsgálata azonban elhúzódott és időközben több, az iratok hozzáférhetőségével kapcsolatos kérés, megkeresés érkezett hozzánk.

Elsőként említendő az Országgyűlés Hivatala főosztályvezetőjének kérése, amely az Országgyűlés Hivatalánál, az Országgyűlés irattárában és levéltárában tárolt, az olajügyek és a szervezett bűnözés között az esetleges korrupciós ügyek feltárására létrehozott korábbi országgyűlési vizsgálóbizottság működése során különböző forrásokból a bizottsághoz érkezett iratanyag vizsgálatára irányult.

> A nevezett bizottság jelentés benyújtása nélkül fejezte be tevékenységét. A bizottság nyilvános üléseinek jegyzőkönyve bárki számára hozzáférhető, azonban a bizottsághoz érkezett nagy mennyiségű – mintegy 29 doboznyi – irat jogi státusza kérdéses volt. A biztos munkatársai soron kívüli helyszíni vizsgálat során megállapították, hogy a vizsgált iratállomány forrását, jellegét és tartalmát tekintve rendkívül heterogén. Némelyik irat állami szervektől vagy magánszemélyektől származik, és van olyan is, amelynek forrása ismeretlen. Az iratokban található adatok minősége, megbízhatósága nem állapítható meg. Az iratokat ügyviteli nyilvántartásba vették, azonban nagy részüket nem használták fel a bizottság működése során.

Az iratok hozzáférhetővé tételének lehetőségével kapcsolatban több, egymással néhol nehezen összeegyeztethető jogi megfontolást kell egyszerre érvényesíteni. Először arra kell rámutatni, hogy az országgyűlési vizsgálóbizottság által végzett személyes adatkezelés jogalapja rendezetlen volt. Bár a bizottság tevékenysége fő szabályként a nyilvánosság előtt zajlott, e nyilvánosság nem terjeszthető ki automatikusan a bizottsághoz érkezett, ám a bizottság működése során fel nem használt, nyilvános ülésen nem tárgyalt iratokra. Az ilyen iratok kérés nélküli közzétételére jogi kötelezettség nincs. Ezen iratok hozzáférhetővé tételéről adatigény esetén az iratok tartalmának megvizsgálása alapján kell egyedi döntést hozni:

- Kérésre az Avtv. szabályai szerint hozzáférhetővé kell tenni az iratokban található közérdekű adatokat. Az ilyen adatok nyilvánossága nem korlátozható a döntés megalapozását szolgáló adatokra vonatkozó szabályok szerint, mert a vizsgálóbizottság feladata nem döntéshozatal volt, azonban az egyéb törvényi korlátokat – például a minősített adatok védelme, az üzleti titok stb. – figyelembe kell venni.

- Az iratokban található személyes adatok csak az érintett kifejezett hozzájárulása esetén továbbíthatók és hozhatók nyilvánosságra. Nincs szükség a hozzájárulásra, ha a személyes adat közérdekből nyilvános. Ilyen lehet például törvény eltérő rendelkezésének hiányában a közfeladatot ellátó szervek feladat- és hatáskörében eljáró személy feladatkörével összefüggő személyes adata, továbbá egyéb, közfeladatot ellátó személy e feladatkörével összefüggő személyes adata. Az érintett hozzájárulásának hiányában az adatok csak anonimizáltan hozhatók nyilvánosságra. Anonimizálás alatt nemcsak a névadat törlése értendő, hanem minden olyan adat törlése, amely alapján a védendő adat rekonstruálható, illetve az érintett azonosítható.

- A bizottsághoz érkezett állampolgári bejelentések bizalmas voltának fenntartása több okból is fontos. A bejelentő adatai éppúgy védendők, mint bárki másé. Ezen túl nyomós közérdek fűződik ahhoz, hogy az országgyűlési vizsgálóbizottság iránti közbizalom fennmaradjon és a bizottsághoz tett bejelentés miatt senkit ne érjen hátrány. Végül, de nem utolsó sorban figyelembe kell venni, hogy a bizottság vizsgálata bűncselekményekre irányult. Amennyiben az elkövetők tudomást szereznének arról, hogy ki, milyen bejelentéssel élt velük kapcsolatban, akkor akár évek múltán is bosszút állhatnak vagy „elhallgattathatják" a terhelő tanút. *(1308/K/2007)*

Több kérdés és kérés is érkezett az üggyel kapcsolatban a sajtó munkatársaitól. A Magyar Újságírók és -Készítők Európai Szövetségének elnöke azt kezdeményezte, hogy soron kívül vizsgáljuk meg az iratok titkosításának jogszerűségét és lehetőség szerint kezdeményezzük az iratok, illetve azok egyes részeinek nyilvánosságra hozatalát, továbbá szükség szerint tegyünk javaslatot olyan jogszabályi módosításokra, amelyek kizárják a nyilvánosság indokolatlan korlátozásának lehetőségét.

> Az adatvédelmi biztos válaszában azt a tájékoztatást adta, hogy az iratfelülvizsgálat előrehaladását hivatalból figyelemmel kíséri. 2007 augusztusában megkereste a munkabizottság tevékenységét felügyelő dr. Szilvásy György minisztert, akitől tájékoztatást kért az iratok felülvizsgálatáról. A miniszter felkérte arra, hogy segítse az iratok felülvizsgálatát. A biztos munkatársai megkezdték a problémák felmérését az iratbirtokos szervezeteknél. A nagy mennyiségű iratanyag kormányzati munkacsoporttal párhuzamos tételes felülvizsgálatát azért nem tartja szükségesnek, mert annak nagy részét feltehetőleg egyébként is nyilvánosságra fogják hozni. Arra azonban ígéretet tett, hogy ha a vizsgálata olyan jogsértést állapít meg, amely közérdeklődésre tarthat számot, akkor soron kívül a nyilvánossághoz fog fordulni. *(1268/P/2007)*

Az elmúlt időszakban a biztos munkatársai több esetben személyesen tájékozódtak az iratfelülvizsgálat menetéről és december folyamán írásban kértük a munkabizottság tagjait, hogy számoljanak be a munka előrehaladásáról. Az olajügyekhez kapcsolódó iratok mintegy 80 százaléka a rendőri szervek kezelésében van, ezért az Igazságügyi és Rendészeti Minisztérium az ősz folyamán értekezletet szervezett a Nemzeti Nyomozó Iroda – mint az ORFK Központi Bűnüldözési Igazgatóság jogutódja – kezelésében lévő minősített iratanyag felülvizsgálatának megvitatására, amelyen az Adatvédelmi Biztos Irodájának munkatársai is részt vettek. Az értekezleten elhangzottak kapcsán állásfoglalás született, mely az iratfelülvizsgálat gyakorlati problémáit megismerve elő kívánta segíteni, hogy a törvényes keretek között minél teljesebben érvényesülhessen az iratok nyilvánossága.

Az állásfoglalás szerint továbbra is fenntartható azon iratok minősítése, amelyeknél jelenleg is fennáll a nyilvánosság korlátozásához fűződő bűnüldözési vagy nemzetbiztonsági érdek. A minősítés abban az esetben is fenntartható, ha az a titkos információgyűjtés erői, eszközei és módszerei

érdekében igazolhatóan szükséges, ám ez gondos eseti mérlegelést igényel. Nincs törvényes lehetőség ismételt titokminősítésre, ha az iratállomány felülvizsgálata során megállapítást nyer, hogy valamely, korábban minősített irat minősítése időközben megszűnt. Azokat az iratokat, amelyek minősítését nem tartják fenn, a minősítés megszüntetésére utaló jelzéssel kell ellátni. Ha ugyanis az állami szervek minősített iratnak látszó, de valójában törölt minősítésű iratokat tennének közzé, az zavarhoz és jogbizonytalansághoz vezethetne.

Felmerült, hogy a Rendőrségről szóló törvény 63. §-ának (3) bekezdése a megszüntetett minősítésű iratok közzétételét kizárja. Az Rtv. hivatkozott bekezdése azonban a titkos információgyűjtés alapján tett intézkedések és az abban érintettek adatainak nyilvánosságra hozatalát zárja ki. A korlátozás tehát a titkos információgyűjtés alapján tett rendőri intézkedésekkel, és nem magával a titkos információgyűjtéssel kapcsolatban áll fenn. E törvényhely kiterjesztő értelmezése azért sem lenne elfogadható, mert a feltétlen érvényesülést követelő, az egyedi körülményeket figyelmen kívül hagyó, meghatározatlan időtartamú nyilvánosságkorlátozó jogszabályok alkotmányosan kifogásolhatók.

A tapasztalatok majd az iratfelülvizsgálat befejeztével összegezhetők. 2007 történéseiről a következők állapíthatók meg:

Az iratok nyilvánosságra hozataláról hozott döntés az információszabadság érvényesülését előmozdító fontos kormányzati kezdeményezés, amely találkozik a társadalom részéről érzékelhető elvárással. A munka elhúzódik, azonban ez az iratok nagy mennyiségével indokolható. Az iratok felülvizsgálata szakszerűen, képzett szakemberek bevonásával zajlik. A közzétett adatok köre nem szükségképp azonos azzal, amelyet közérdekű adatkérés esetén hozzáférhetővé kellene tenni az adatigénylő számára, ami azonban elfogadható, tekintettel arra, hogy a közzétételre nem törvényi kötelezettség, hanem kormányzati elhatározás alapján kerül sor. Nincs a birtokunkban olyan információ, amely szerint a közzéteendő adatokat bárki is politikai vagy egyéb érdek alapján szelektálná.

Az anonimizálás utólag felismert kedvezőtlen velejárója, hogy a nevek törlése lehetetlenné teszi a közzétett iratokon belüli, és az iratok közötti logikai összefüggések rekonstruálását. Ha sor kerül még valaha hasonlóan bonyolult irategyüttesek közzétételére, akkor az anonimizálást lehetőleg úgy kell majd végrehajtani, hogy a névadatok helyébe kódnév – például „A61215

úr" vagy „K97378 Kft." - kerüljön. Így a védendő adatok titokban tartása mellett is megőrizhetők az iratok logikai összefüggései.

Sajtó, civil szervezetek

Az adatvédelmi törvény nem tesz különbséget a közérdekű adat megismerését kérő adatigénylők között, mégis indokolt kitüntetett figyelemmel kezelni a sajtó munkatársai és a civil szervezetek adatvédelmi biztoshoz eljuttatott beadványait, mert azok a tapasztalatok szerint gyakorta fontos, közérdekű ügyekben lépnek fel.

Internetes újság munkatársa kért állásfoglalást az adatvédelmi biztostól, mert a Honvédelmi Minisztériumnál a minősített adatok védelmére hivatkozva nem adtak választ a honvédség titkos objektumainak hozzávetőleges számára és az azokban folyó tevékenység jellegére vonatkozó kérdéseire. Az ügy kivizsgálása során a biztos a Honvédelmi Minisztérium képviselőivel tisztázta, hogy a kérdések nem egyes objektumokra és az azokban folyó tevékenységre vonatkozó, valóban védendő adatokra vonatkoznak, ezért a HM Kommunikációs és Toborzó Főosztályának vezetője elküldte a kért adatokat az adatvédelmi biztoshoz, aki továbbította azokat az adatkérőhöz. A biztos felhívta arra a HM illetékesének a figyelmét, hogy a jövőben a minősített adatra vonatkozó adatkérés teljesítésének elutasítása helyett lehetőség szerint törekedjenek részleges, minősített adatot nem tartalmazó válaszadásra, hiszen ez utóbbi eljárás van összhangban a közfeladatot ellátó szervek törvényes tájékoztatási kötelezettségével. *(1416/P/2007)*

Egy másik újságíró azt panaszolta, hogy a Honvédelmi Minisztériumban államtitokra hivatkozva megtagadták a Nemzeti Döntéshozó Személy kilétére vonatkozó adatkérését. A minisztériumban nem sikerült az adatkérés nyomára akadni, ezért a biztos hivatalból folytatta a vizsgálatot. A Honvédelmi Minisztérium államtitkára azt a tájékoztatást adta, hogy a Nemzeti Döntéshozó Személy a honvédelmi miniszter vagy az általa kijelölt személy. Az adat minősítése 2005-ben megszűnt. A Nemzeti Döntéshozó Személy a honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény 132. § -ának szabályai szerint dönt arról, hogy nyitható-e figyelmeztető vagy megsemmisítő tűz az ország légterében tartózkodó légi járműre. Az ügyben folytatott vizsgálat lezárult, mert a minisztérium hozzáférést biztosított a közérdekből nyilvános adathoz. *(1731/T/2007)*

Egy újság szerkesztőségéből a Nemzetbiztonsági Szakszolgálat által rögzített telefonbeszélgetésről készített jegyzőkönyv egy részének jogszerű felhasználási lehetőségéről kértek tájékoztatást, az irat másolatát eljuttatva az Adatvédelmi Biztos Irodájához. Szomorú, de sajnos nem példátlan, hogy személyes adatokat és törvény által védett titkokat tartalmazó, tisztázatlan körülmények között megszerzett iratokat illetéktelen személyek a sajtóhoz továbbítanak vagy egyéb módon felhasználnak.

Első lépésként meg kellett állapítani, hogy az irat rendelkezik-e érvényes államtitok minősítéssel. Ha igen, akkor az adatvédelmi biztos ugyanúgy köteles feljelentést tenni államtitoksértés miatt, mint bárki más. A Nemzetbiztonsági Szakszolgálat útján a biztos megkereste azt a rendőri szervet, amelynél az adatokat minősítették. Tájékoztatásuk szerint az irat államtitok minősítése már megszűnt. A jegyzőkönyvet büntetőeljárásban használják fel, és már nem lehet kideríteni, hogy milyen úton-módon jutott el az iratmásolat a sajtóhoz. Az adatvédelmi biztos felhívta az iratot beküldő újságíró figyelmét arra, hogy a lehallgatási jegyzőkönyvben rögzített személyes adatok kezelésére csak az érintettek adhatnak hozzájárulást. A folyamatban lévő büntetőeljárásra tekintettel az érintettek hozzájárulása esetén is tisztázandó, hogy az iratok esetleges idő előtti közzététele nem sért-e bűnüldözési érdeket. *(1699/H/2007)*

Az Országgyűlés Honvédelmi és rendészeti bizottságának elnöke és a Nemzetbiztonsági bizottságának elnöke levélben kért állásfoglalást az adatvédelmi biztostól egy civil szervezet adatkérésével kapcsolatban. A jogvédő szervezet adatigénye az Országgyűlés Honvédelmi és rendészeti bizottságának, valamint Nemzetbiztonsági bizottságának birtokában lévő, már megszűnt minősítésű dokumentumok megjelölésére, tárgyára, a minősítő kilétére, a minősítés időpontjára és konkrét jogcímére, valamint érvényességi idejére, továbbá a minősítés megszűnésének okára vonatkozott. A kérés teljesítésének előkészítése során kétség merült fel azt illetően, hogy a közérdekű adatok megismerésének joga kiterjed-e a közfeladatot ellátó szervek alaprendeltetésén kívül eső, „nem érdemi" ügyviteli tevékenysége során kezelt közérdekű adatokra is.

Az adatvédelmi biztos válaszában nem tartotta lehetségesnek, hogy az adatkezelő aszerint mérlegeljen, hogy az adatkérés „érdemi" vagy „nem érdemi" tevékenységhez kötődő adatokra vonatkozik. A különbségtételnek ugyanis nincs törvényes alapja és egyébként sem lehetne egzakt módon elhatárolni, hogy a közfeladatok ellátása során

melyek az érdemi és melyek a nem érdemi tevékenységek. A közfeladatot ellátó szerv tájékoztatási kötelezettsége elvileg minden, a birtokában lévő közérdekű adatra kiterjed. Az adatigény teljesítése csak akkor utasítható el, ha az adat nyilvánosságát az Avtv.-vel összhangban törvény korlátozza. Az adatkezelő kötelessége, hogy a rendelkezésre álló adatokat megkeresse a birtokában lévő nyilvántartásokban és dokumentumokban, és az adatigénylő választása szerint közérthető tájékoztatást, illetve másolatot adjon. A másolatkészítésért – legfeljebb az azzal kapcsolatban felmerült költség mértékéig – állapítható meg költségtérítés, amelynek összegét az igénylő kérésére előre közölni kell. A törvényben meghatározott, legfeljebb 15 napos teljesítési határidő betartása kívánatos, ha azonban a kért adatok nagy mennyisége miatt ez nem lehetséges, akkor a határidő a teljesítéshez szükséges időtartammal meghosszabbodik. Ilyen esetben célszerű az adatigénylővel tisztázni, hogy igényt tart-e a több részletben történő teljesítésre.

Ha a kért közérdekű adatok feldolgozással állíthatók elő, akkor a megállapodásban nem köthető ki, hogy az adatkérő kizárólagos jogot nyer az előállított közérdekű adatok felhasználására. Ha a kért adatok rekonstruálása azért szükséges, mert bár a közfeladatot ellátó szerv jogszabály által előírt kötelessége lett volna a közérdekű adatok előállítása és kezelése, azonban ezt elmulasztotta, úgy az adatok utólagos előállításához szükséges adatfeldolgozásért nem kérhető díj. *(222/K/2007)*

2005-ben indult, de sajnos csak 2007-ben fejeződött be annak a panasznak a kivizsgálása, amelyben egy jogvédő szervezet azt kifogásolta, hogy több rendőri szervnél drograzziák okáról, a rendőri erők számáról és költségéről kértek tájékoztatást, azonban a kért közérdekű adatokat csak részben vagy egyáltalán nem kaphatták meg.

A Kecskeméti Rendőr-kapitányságnál időközben megszűnt az adatok szolgálati titok minősítése, így az adatvédelmi biztostól származó megkeresés után a közérdekű adatokat továbbították az adatigénylőnek. Az akció költségeire vonatkozó adat nem állt rendelkezésre, mert a razziához nem készült külön költségkimutatás. Az akcióterv csak az akcióban titokban, civil ruhában résztvevő rendőrök közvetlen költségeit – például belépőjegy – tüntette fel.

Az Avtv. szabályai szerint a közfeladatot ellátó szervek a feladatkörükbe tartozó ügyekben kötelesek elősegíteni és biztosítani a közvé-

lemény pontos és gyors tájékoztatását, azonban jogi úton kikényszeríthető tájékoztatási igény meghatározott, létező közérdekű adatokra állhat fenn. Az adatvédelmi biztos álláspontja szerint elvárható a közfeladatot ellátó szervtől, hogy a kért adatgyűjtést, adatfeldolgozást végezze el, ha ez nem jár aránytalan munkateherrel, amint erre az Európai Parlament és Tanács a közszféra információinak további felhasználásáról szóló 2003/98/EK irányelve utal. Az adatkezelő szervnek nem jelenthet túlzott terhet egyszerű műveletek végzése, viszont nem köteles jelentős munkateherrel, költséggel járó adatfeldolgozási, adatgyűjtési, rendszerezési feladatok elvégzésére és ezáltal új adatok előállítására. A vizsgált ügyben a teljes költségkimutatás utólag csak nehezen lenne elkészíthető, ezért az adatvédelmi biztos szerint erre a rendőri szerv nem kötelezhető.

A Budapesti Rendőr-főkapitányság államtitokra hivatkozva megtagadta a drograzziával kapcsolatos adatigény teljesítését, ezért az adatvédelmi biztos munkatársai a helyszínen, a rendőri szervnél vizsgálták az adatok minősítésének jogszerűségét és megalapozottságát. A vizsgálat megállapította, hogy a bűnügyi felderítés körében keletkezett iratok minősítése szükséges volt. A minősítés érvényessége formai és eljárási szempontból nem kérdőjelezhető meg. Az iratokat áttekintve az is megállapítást nyert, hogy a kért adatok titokban tartásához már nem fűződik közvetlen bűnüldözési érdek.

A vizsgált szerv részéről felhívták a figyelmet arra, hogy a kért adatok részadatok. Ha valamely ügyről bűnüldözési érdekből nem adhatnak teljes tájékoztatást, akkor a nyilvánossághoz eljutó részinformációk alapján hamis, negatív színben tűnhet fel a rendőri munkájuk. Az adatvédelmi biztos szerint annyiban megalapozott és méltányolandó ez az aggodalom, hogy a közérdekű adatok nyilvánossága elsősorban arra szolgál, hogy az állampolgárok valós és teljes képet kapjanak a közfeladatot ellátó szervek működéséről, márpedig részadatok birtokában e kép szükségképp hiányos, és esetleg torz is lehet. Ez azonban semmiképp sem lehet az adatkérés elutasításának indoka, mert ilyen adat-megtagadási jogcímet a törvény nem ismer. A közérdekű adatkérések kooperatív kezelése önmagában is javítja a közfeladatot ellátó szerv közmegítélését. Az egyeztetést követően Budapest rendőrfőkapitánya arról tájékoztatta az adatvédelmi biztost, hogy a közérdekű adatkérést teljesítették. *(718/A/2005)*

További, minősített adattal kapcsolatos vizsgálatok

Állampolgári beadvány hívta fel a figyelmet arra, hogy az Országgyűléshez a J/3166. számon benyújtott, a honvédelmi politika 2006. évi megvalósításáról, a Magyar Honvédség felkészítéséről, állapotáról és fejlesztéséről szóló jelentés szolgálati titok minősítésű. Megkerestük az irat minősítőjét – a Honvédelmi Minisztérium főosztályvezetőjét – és javasoltuk, hogy készítsék el a jelentés minősített adatot nem tartalmazó kivonatát, hiszen abban feltehetőleg a honvédség helyzetének köz általi megismerését segítő adatok vannak. A minősítő azt a választ adta, hogy a jelentés az országgyűlési képviselők információs igényének megfelelően készült, azonban a honvédelmi tárca rendszeres tájékoztatást ad a jelentés által érintett, a nagyobb nyilvánosság érdeklődésére számot tartható kérdésekről, ezért a jelentés rövidített, nyilvános változatának megjelentetése nem szükséges. Az ügy apropóján meg kívánjuk vizsgálni a Honvédelmi Minisztérium közérdekű tájékoztatási gyakorlatát. A vizsgálat jelenleg folyamatban van. *(1099/P/2007)*

Ugyancsak minősített adatokkal függ össze, hogy az Országgyűlés Nemzetbiztonsági Bizottságának elnöke arról kért állásfoglalást, milyen típusú információk megismerésére jogosult a 2003. évi III. törvény végrehajtásának ellenőrzésére alakult, Kenedi János által vezetett szakértői bizottság. Kizárólag a hatályos jogszabályok értelmezésével válaszoltuk meg a kérdést, hiszen nem rendelkezünk áttekintéssel a szóban forgó iratanyagról.

> A főbb megállapítások: A szakértői bizottság feladatait az állambiztonsági iratok átadása teljesítésének értékeléséről szóló 190/2007. (VII. 23.) Korm. rendelet határozza meg. Eszerint a szakértői bizottság feladata lényegében az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról szóló 2003. évi III. törvény egyes rendelkezései teljesülésének ellenőrzése. A szakértői bizottság tehát olyan adatokat jogosult megismerni, amilyen adatok megismerésére egy közfeladatot ellátó állami szerv tagjai kormányrendeleti úton felhatalmazhatók. Személyes adatok megismerésére, kezelésére kormányrendeleti úton nem adható felhatalmazás. Államtitok vagy szolgálati titok esetén a minősítő vagy a titokbirtokos szerv vezetője dönt a betekintési engedély megadásáról. A rendelet hatálya alá tartozó dokumentumok esetlegesen fellelhetők nem a Kormány alárendeltségébe tartozó szerveknél is. E szervek esetében kétséges, hogy az adatkezelés kormányrendelettel előírható volna. Az állásfoglalás teljes szövege az adatvédelmi biztos honlapján olvasható. *(1905/K/2007)*

Végül megemlítjük, hogy az Adatvédelmi Biztos Irodájánál több olyan ügy van folyamatban, amelyekben rendvédelmi szervnél szolgálati jogviszonnyal kapcsolatban keletkezett, minősített adatok érintett általi megismerhetőségét vizsgáljuk. Ezekről az ügyekről szükség szerint a 2008-as beszámolóban szólunk majd.

III. NEMZETKÖZI ÜGYEK

A nemzetközi ügyeink közül 2007 legfontosabb eseménye tagadhatatlanul Magyarország csatlakozása a schengeni rendszerhez. A (hat éves) nemzetközi munka összegzéseként azonban szót érdemel, hogy Irodánk az elmúlt években milyen egyértelműen pozitív megítélést vívott ki magának nemzetközi színtéren: nyugat-európai kollégáink egyenrangú partnerként kezelnek, Kelet-Európában ugyanakkor egyfajta minta modellnek tekintik a magyar rendszert. Ezt a nemzetközi tanácskozásokon, konferenciákon a szlovén, szlovák, horvát és lengyel adatvédelmi hatóságok vezetői mindig is kiemelik.

Jó hírünknek köszönhető, hogy Moldávia is a magyar adatvédelmi gyakorlatot tekinti mintaértékűnek a jövőre felálló moldáv Információs Központ kialakításánál. Bár még csak a jogszabály - előkészítés és a szervezetépítés tervezési fázisánál tartanak, 2007 novemberében egy négy fős delegáció a moldáv információs fejlesztési miniszterhelyettes vezetésével – és a magyar Külügyminisztérium támogatásával – hivatalos látogatást tett nálunk. Három napon keresztül intenzív szakmai továbbképzések és megbeszélések során próbáltuk átadni tapasztalatainkat a személyes adatok védelmének gyakorlati megvalósításáról. Ez persze csak a kezdete egy hosszú távú és – remélhetőleg – mindkét fél számára sikeres kétoldalú együttműködésnek.

A nemzetközi munkát bemutató fejezetben szó esik még az európai adatvédelmi hatóságok hatáskörének esetleges jövőbeli fejlődési irányát jelző Európai Adatvédelmi Címkéről, a harmadik országokba történő adattovábbítások általános felvetéseiről, természetesen bővebben Schengenről, az ehhez kapcsolódó magyar vízumkiadási gyakorlat külföldi helyszíneken történő ellenőrzési tapasztalatairól, a Visa Waiver Programról, a Prümi Szerződéshez való csatlakozásról, valamint a Váminformációs Rendszer, az EURODAC és az Europol nyilvántartásainak nemzetközi és nemzeti felügyeletéből fakadó ellenőrzések megállapításairól. Beszámolunk az Európai Unió adatvédelmi biztosaiból álló, úgynevezett 29-es Adatvédelmi Munkacsoport ezévi munkájának fontos eredményeiről, külön is kiemelve a személyes adat fogalmának elemzéséről szóló munkacsoporti véleményt.

Végül érdekes információk olvashatók az Európai Unió bel- és igazságügyi együttműködésének fontos szereplőiként számontartott munkacsoportok információs jogokat érintő munkájáról, a Rendőrségi Munkacsoport és Telekommunikációs Munkacsoport 2007-es tevékenységéről és egy információ-technológiával foglalkozó nemzetközi konferenciáról.

EuroPriSe projekt (European Privacy Seal – Európai Adatvédelmi Címke)

A németországi Schleswig-Holstein tartomány adatvédelmi hatósága irányította figyelmünket a EuroPriSe kezdeményezésre. A német hatóság a EuroPriSe-hoz hasonló regionális projekt keretében már több mint 40 címkét (Gütesiegel) ítélt oda (például a szociális és munkaügyi igazgatás, a Windows Update Service és a WGA for Windows XP részére). 2007. novemberében több munkatársunk részt vett Bécsben egy ezzel foglalkozó nemzetközi munkaértekezleten is.

Az EuroPriSe kísérleti projekt célja az Európai Adatvédelmi Címke bevezetése, mely alkalmas eszköz lehetne annak igazolására, hogy egy informatikai termék vagy egy információ-technológián alapuló szolgáltatás elősegíti az adott terméknek vagy szolgáltatásnak az európai adatvédelmi szabályozással összhangban történő használatát. Az adatvédelmi címke tehát nem azt tanúsítaná, hogy egy termék vagy szolgáltatás konkrét alkalmazása az adatvédelmi jogszabályoknak megfelel, hanem azt, hogy a termék vagy szolgáltatás az adatvédelmi jogszabályoknak megfelelően használható.

Az adatvédelmi címke bevezetése – megfelelő garanciák mellett – számos előnnyel járna mind a fogyasztók és az adatvédelmi hatóságok, mind pedig az informatikai termékek gyártói számára. A fogyasztók számára egyértelművé tenné, hogy az adott termékben vagy szolgáltatásban adatvédelmi szempontból megbízhatnak, csökkentené a hatóságok ellenőrzési terheit, és piaci előnyhöz juttatná a címkével rendelkező termékeket.

A címke kibocsátását megelőző eljárásnak két szakasza van: először jogi és informatikai szakértők értékelik a terméket vagy szolgáltatást, majd egy független hitelesítő testület (adatvédelmi hatóság) hitelesíti a szakértők által készített jelentést. A szakértőknek több feltételnek is meg kell felelniük (legyenek függetlenek a gyártótól, rendelkezzenek megfelelő szakmai

képesítéssel és gyakorlattal stb.) ahhoz, hogy felvételt nyerjenek a szakértői listára, amelyet a gyártók és forgalmazók a EuroPriSe projekt honlapján érhetnek el. Az informatikai termék vagy szolgáltatás értékelését a szakértőknek a EuroPriSe katalógusban felsorolt szempontok alapján kell elvégezniük. Az értékelési szempontokat négy csoportba sorolták:

- alapvető kérdések,
- az adatkezelés jogalapja,
- technikai és szervezési intézkedések,
- az érintettek jogai.

Az egyes csoportok tehát több vizsgálati szempontot, és mindegyik szemponton belül több kérdést tartalmaznak (például az adatkezelés jogalapjának értékelésekor 15 szempontot kell megvizsgálni és egy szemponthoz akár 5-10 megválaszolandó kérdés is tartozhat). A vizsgálati szempontok a 95/46/EK adatvédelmi irányelvben, a 2002/58/EK e-adatvédelmi irányelvben és a 2006/24/EK adatmegőrzési irányelvben lefektetett követelményekhez igazodnak. A szakértőknek iránymutatásul szolgálnak az Európai Bíróság határozatai és a 29-es Adatvédelmi Munkacsoport véleményei a jogszabályok értelmezésekor. Mivel az Európai Adatvédelmi Címke azt nem tanúsítja, hogy a termék/szolgáltatás a nemzeti adatvédelmi törvényeknek is megfelel, az azoknak való megfelelést nem kell vizsgálniuk a szakértőknek. Az értékelési szakasz végén a szakértők egy jelentést készítenek, amely alapján a gyártó eldöntheti, hogy érdemes-e a terméket benyújtania a hitelesítő hatósághoz.

Az eljárás második szakaszában a hitelesítő hatóság (adatvédelmi hatóság) értékeli a jogi és az informatikai szakértő jelentését és dönt arról, hogy megkapja-e a termék a címkét. A hatóság vizsgálja a jelentés következetességét, teljességét és módszertanát, valamint biztosítja az eljárások egységességét. Az elutasító döntést a hatóság nem hozza nyilvánosságra, viszont értesíti a többi tagállam adatvédelmi hatóságait. Ha pozitív döntés születik, akkor a projekt honlapján közzétesznek egy rövid jelentést. Az információtechnológia gyors fejlődése miatt a címke csak 2 évig érvényes.

Az Európai Unió által finanszírozott projekt jelenleg a kísérleti szakaszban tart, 8 országból 9 tag – köztük a francia és a spanyol adatvédelmi hatóságok – részvételével. Az Európai Bizottság 2008 második felében

értékeli majd a projekt eredményességét és dönt arról, hogy bevezeti-e az Európai Adatvédelmi Címkét.

Irodánk – sok más adatvédelmi hatósághoz hasonlóan – érdeklődik a projekttel kapcsolatban, végső döntést azonban a kísérlet tapasztalatainak birtokában és az Európai Bizottság értékelése után hozunk.

Adattovábbítás harmadik országokba

A globalizáció és a terrorizmus elleni harc következményeként egyre gyakoribb jelenség, hogy hazai adatkezelők az Európai Gazdasági Térségen (EU tagországok, valamint Izland, Norvégia és Liechtenstein) kívüli, úgynevezett harmadik országokba továbbítanak személyes adatokat. A harmadik országok közül az Amerikai Egyesült Államokba irányuló adattovábbítások a leggyakoriabbak. A gyakran ismétlődő konzultációs kérdések miatt az év elején egy részletes tájékoztatóban ismertettük az adatvédelmi törvény vonatkozó rendelkezéseit (9. §), azok értelmezését, és Irodánk gyakorlatát a harmadik országokba irányuló adattovábbításokkal kapcsolatban. Emellett meg kell említeni az Egyesült Államokban adatvédelmi feladatokat ellátó Szövetségi Kereskedelmi Bizottság (Federal Trade Commission) képviselőinek látogatását. A találkozó kiváló alkalom volt az információcserére a két ország különböző adatvédelmi szabályozásának sajátosságairól.

Az Amerikai Egyesült Államokba a hazai adatkezelők általában két okból továbbítanak adatokat:

Az első ok az amerikai hatóságok adatkérése. Az Amerikai Belbiztonsági Minisztérium az utas-nyilvántartási adatokat gyűjti a légitársaságoktól az USA-ba utazó utasokról. Az Egyesült Államok Értékpapír- és Tőzsdefelügyelete a külföldi korrupt eljárásokra vonatkozó amerikai törvény és az értékpapír tőzsdéről szóló törvény alapján gyűjt adatokat hazai cégekről – tudomásunk szerint a Pénzügyi Szervezetek Állami Felügyeletén keresztül – kölcsönös jogsegély alapján. Az Egyesült Államok Pénzügyminisztériuma pedig közvetve gyűjt adatokat magyar bankoktól, a nemzetközi átutalásokat lebonyolító SWIFT cég USA-beli adatbázisából való adatkérésekkel, a terrorizmus finanszírozását felderítő program keretében. Ezen adattovábbítások csak az érintettek hozzájárulása vagy törvényi felhatalmazás alapján lehetnek jogszerűek, a törvényi felhatalmazás esetén pedig további

feltétel, hogy megfelelő legyen a személyes adatok védelmének szintje a harmadik országban. A megfelelő védelem biztosítását az USA hatóságai egyoldalú kötelezettség-vállalásokban vagy az EU-val kötött megállapodásokban vállalják. A hazai cégek kötelesek minden esetben tájékoztatni az érintetteket az adattovábbításról.

Az adattovábbítások második jellemző köre a multinacionális vállalatcsoportok magyar „leányvállalatainak" adatszolgáltatása az „anyacég" részére. Egy multinacionális vállalatcsoporton belüli, azaz a tagok közötti adattovábbítás legegyszerűbb módja, ha a vállalatcsoporton belül globálisan, tehát minden tagnál földrajzi elhelyezkedésre tekintet nélkül, kialakítják a személyes adatok megfelelő védelmét. A vállalatcsoport kötelezi tagjait (Kötelező Erejű Vállalati Szabályokkal, a továbbiakban BCR) egy egységes adatvédelmi szint kialakítására, amely egy minimum szintnek, de európai mércével mérve még megfelelőnek minősül. Ettől persze pozitív irányba el lehet (és el is kell) térni, ha a tag országának törvényei szigorúbbak.

2007-ben tovább egyszerűsödött a BCR-ek alkalmazása, mivel a 29-es munkacsoport elfogadott egy standard jelentkezési lapot, amelyet a cégek az adatvédelmi hatóságokhoz nyújthatnak be a BCR jóváhagyására irányuló eljárásban. Irodánk ennek hatására több BCR-t is kapott külföldi adatvédelmi hatóságoktól (a cég európai központjának székhelye szerinti ország adatvédelmi hatósága lesz az úgynevezett vezető hatóság, aki koordinálja az eljárást) véleményezésre. Annak ellenére azonban, hogy a tagállamok együttműködésére a munkacsoport kialakított egy eljárást, a határidőket is lefektetve, eddig csak egyetlen ügyben született meg a hatóságok közös döntése.

Ugyan a BCR-ek szerepét a 2006-os beszámoló már bemutatta és a 29-es Adatvédelmi Munkacsoport fejezetén belül később részletesen is szó esik róla, néhány fontos jellemzőt most is szeretnénk kiemelni. A BCR-ekben lefektetett szabályok nem alkalmazhatók, ha azoknál a nemzeti adatvédelmi szabályozás szigorúbb. Minden BCR-nek tartalmaznia kell azt a kitételt, amely szerint annak szabályai csak akkor vonatkoznak a vállalatcsoport tagjára, ha az adott országban nincs szigorúbb rendelkezés hatályban. Ebből is látható, hogy a BCR-ek valójában a vállalatcsoport olyan tagjainál bírnak jelentőséggel, amelyek megfelelő adatvédelmi szinttel nem rendelkező harmadik országban találhatók. Különösen fontos vizsgálni, hogy a BCR tartalmazza-e azt a kötelezettség vállalást, amely szerint egy harmadik

országbeli adatkezelő az érintett kérelmére az érintett országában (az adatexportáló országban) vagy abban az EU tagállamban fordulhat az adatvédelmi hatósághoz vagy bírósághoz, ahol a vállalatcsoport központja van. Ez a kötelezettségvállalás nagy jelentőséggel bír, mivel legtöbb esetben egy ország adatvédelmi szintjét részben azért nem tartja megfelelőnek az EU, mert ott külföldiek nem érvényesíthetik adatvédelmi jogosultságaik sérelméből származó igényüket. A BCR-ek fontos részét képezik a vállalások gyakorlati megvalósulását biztosító intézkedések is (pl. külső és belső auditok).

Az adatvédelmi törvény szerint a megfelelő védelem biztosítása (akár BCR által) csak akkor feltétele az adattovábbításnak, ha az adattovábbítást törvény teszi lehetővé. Az érintettek hozzájárulásán alapuló adattovábbításoknak nem feltétele az, hogy a harmadik országban megfelelő szintű legyen az adatok védelme. Ez különösen aggasztó munkavállalói adatok továbbításakor, mivel a munkavállalói hozzájárulás önkéntessége kétségbe vonható a függőségi helyzet miatt. Ezért megnyugtatóbb megoldás lenne, ha a Munka Törvénykönyve megadná a törvényi felhatalmazást a BCR-ek alapján történő adattovábbításhoz. A Szociális és Munkaügyi Minisztériumnál a kezdeményezésünket pozitívan fogadták.

Az adattovábbítások e második csoportjával kapcsolatban meg kell említeni, hogy több tagállamban is egyre gyakoribb jelenség, hogy a leányvállalatoknak a „pre-trial discovery" eljárás keretében kell személyes adatokat küldeniük USA-beli anyacégük részére. A „pre-trial discovery" az amerikai perjogra jellemző eljárás és a tárgyalás előkészítő szakaszában a lehetséges bizonyítékok összegyűjtését jelenti, akár az ellenféltől is. Az amerikai cégek egyre nagyobb nyomásnak vannak kitéve, hogy az EU-ban található „leányvállalataik" által tárolt adatokat is a szemben álló fél rendelkezésére bocsássák. Az amerikai cégek 90 százaléka érintett az eDiscovery-ben, amely az elektronikusan tárolt információk átadására irányul. Magyarország és az USA is részese a polgári és kereskedelmi ügyekben külföldről történő bizonyítás-felvételről szóló Hágai Egyezménynek, amely a polgári ügyekben a részes államok bíróságai között történő együttműködést szabályozza. Az egyezmény nem kötelezi a hazai cégeket a megkeresések teljesítésére, sőt az egyezményhez tett fenntartásunk alapján az Igazságügyi és Rendészeti Minisztérium is teljesítés nélkül visszaküldi a „pre-trial discovery" keretében történő megkereséseket a megkereső államnak.

A személyes adatok megfelelő védelmét egy harmadik országbeli adatkezelő gyakran az Európai Bizottság modell szerződéseinek alkalmazásával demonstrálja. 2007-ben a 29-es Munkacsoporthoz javaslat érkezett az Európai Bizottság 2002/16/EK határozatában szereplő modell-szerződés módosítására. A módosítás biztosítaná a lehetőséget arra, hogy a harmadik országbeli adatfeldolgozó további adatfeldolgozót vegyen igénybe. Felhívtuk a figyelmet arra, hogy az Avtv. jelenlegi szabályai szerint az adatfeldolgozó nem vehet igénybe alfeldolgozót.

Schengeni csatlakozás

Az állampolgárok számára az Európai Unióhoz történő csatlakozás legszembetűnőbb bizonyítéka az államhatárok útlevél, személyi igazolvány felmutatása nélküli átlépésének lehetősége 2007. december 21-től. A belső határok lebontását a tagállamok rendvédelmi szerveinek fokozott együttműködése teszi lehetővé, így kompenzálva a határok eltörléséből adódó lehetséges biztonsági kockázatokat.

Az együttműködést, a tagállamok közötti adatcserét elősegítendő és a külső határokon az egységes határellenőrzés érdekében alakították ki a Schengeni Információs Rendszert (Schengen Information System – SIS). A rendszer a schengeni államok által rögzített adatokat tartalmazza. Az adatbázisban szerepelnek a beutazási és tartózkodási tilalom alatt álló harmadik országbeli személyek adatai; a letartóztatandó és európai elfogatóparancs alapján átadásra kerülő személyek adatai; eltűnt személyek adatai; bírósági eljárásban keresett személyekre (büntetőeljárásban bíróság által idézett személyekre, büntetés letöltésére felhívott személyekre, tanúkra) vonatkozó adatok; személyekre és tárgyakra vonatkozóan leplezett megfigyelés vagy célzott ellenőrzés céljából kiadott jelzések; lefoglalandó vagy büntetőeljárásban bizonyítékként felhasználandó tárgyakra vonatkozó adatok. Az adatvédelmi elveknek megfelelően (főszabályként) az érintettnek joga van tájékoztatást kapni arra vonatkozóan, hogy milyen rá vonatkozó adatokat tárolnak a SIS-ben; kérheti a hibás adatok törlését, kijavítását, továbbá bírósághoz vagy az illetékes hatósághoz fordulhat kérve az adatok javítását, törlését vagy kártérítés megállapítását.

A SIS-szel kapcsolatos legfontosabb tudnivalókról az állampolgárok számára tájékoztató kiadvány készült, részletes információk pedig honlapunkon is olvashatóak.

A SIS-t tagállami nemzeti rendszerek és a Strasbourgban található központi rendszer alkotják. A rendszer felépítésének sajátosságát követi a rendszer ellenőrzése. A nemzeti rendszer felügyeletét a tagállam adatvédelmi hatósága látja el, a központi rendszer ellenőrzése a tagállamok adatvédelmi hatóságainak képviselőiből álló Közös Felügyelő Hatóság feladata. Hazánkban a nemzeti rendszer független felügyeletéért az adatvédelmi biztos felelős. Ennek megfelelően vett részt Irodánk a 2007. december 21-i csatlakozást megelőző – elsősorban jogalkotási jellegű – előkészületi feladatokban, ahogy az a korábbi évek beszámolóiból is kitűnik.

A SIS alkalmazása szükségszerűen együtt jár személyes adatok kezelésével, ezért elengedhetetlen volt a törvényi szintű szabályozás. A törvényelőkészítő munkák során az első egyeztető tárgyalások határideje csúszott, így a normaszöveg első változatát csak 2007 március végén kaptuk meg rövid válaszadási határidővel. Több, mint húsz pontból álló észrevételt tettünk, és aktívan részt vettünk a törvénytervezet munkacsoporton belüli vitájában is. Sajnos az elfogadott, a Schengeni Végrehajtási Egyezmény keretében történő együttműködésről és információcseréről szóló 2007. évi CV. törvény – többszöri észrevételünk ellenére – 2007 végéig adós marad a SIS nemzeti részét képező N.SIS -hez tartozó adatbázisok adatkezelőjének meghatározásával. Ez alapvető gátját képezte – az egyébként régóta esedékes – Adatvédelmi Nyilvántartásba történő bejelentkezésnek is. A törvényhez kapcsolódó kormányrendelet és az ezzel összefüggő IRM rendelet előkészítő munkálataiba sajnálatos módon, felkérés hiányában nem állt módunkban részt venni.

További – sürgősen megoldandó – probléma, hogy az adatvédelmi biztosnak felügyeleti jogai gyakorlásához a nyilvántartási rendszerhez technikai értelemben is hozzá kellene tudni férnie, de a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatal az N.SIS adatbázishoz történő csatlakozást biztosító berendezések rendelkezésre bocsátásával ugyancsak adósunk.

Mivel a schengeni térséghez történő csatlakozás 2007. december 21-én megtörtént, és az eddig „próbaüzemben" működő rendszer „éles üzeművé" vált, ezért a törvényes rend maradéktalan betartása érdekében soron kívül

kellene gondoskodni a fenti intézkedésekről, ellenkező esetben a rendszer működése nem minősíthető törvényesnek.

Az adatvédelmi biztos három éve megfigyelőként vesz részt a Közös Ellenőrző Hatóság (Joint Supervisory Authority Schengen) ülésein. Ez év tavaszán a Közös Ellenőrző Hatóság két vizsgálatot indított, a Schengeni Végrehajtási Egyezmény (SVE) 99. és 111. cikkére vonatkozóan. Az Ellenőrző Hatóság elnökének kérésére a megfigyelő státuszban lévő tagállamok is megválaszolták a leplezett figyelés vagy célzott ellenőrzés céljából bevitt figyelmeztető kérdésekre és az érintettek bírósághoz vagy az illetékes hatósághoz való fordulásának jogára vonatkozó kérdéseket, átgondolva az SVE gyakorlati megvalósításának tagállami lehetőségeit.

Konzulátusok ellenőrzése

Magyarország teljes jogú schengeni tagságának előkészületeként 2006-ban kezdődött a magyar konzulátusok vízumkiadásának adatvédelmi ellenőrzése, amely az idén a szentpétervári, a kisinyovi, a shanghaji és a hong-kongi konzulátusok, valamint a taipeji Magyar Kereskedelmi Iroda ellenőrzésével folytatódott.

A beszámolóban a szentpétervári és az ázsiai jelentéseket összefoglalva, a kisinyovi vizsgálatról készült jelentést részleteiben adjuk közre. Ennek oka, hogy a kisinyovi magyar konzulátuson nyitották meg az Európai Unió első közös vízumkérelem-átvevő központját (Common Application Centre – CAC). A konzulátusokon folytatott adatvédelmi vizsgálatok során azt ellenőrizzük, hogy a konzulátusok kizárólag a jogszabályban előírt, a vízumkérelem elbírálásához valóban szükséges adatokat kérjék a kérelmezőktől és a jogszabályban rögzített módon kezeljék a kérelmezők személyes adatait. Minden esetben ellenőrizzük a papíralapú iratok irattározásának rendjét és azt, hogy a kérelmezőket megfelelő módon tájékoztatják-e személyes adataik kezelésének miként jéről.

Kisinyov

Ellenőrzés a közös vízumkérelem-átvevő központban – a nem magyar vízumkérelmek átvétele, kiadása

A Bizottság felvetésére, hogy mely állam konzulátusa vállalja el a Moldáviában konzulátussal nem rendelkező tagállamok vízumkérelmének átvételét, Magyarország vállalkozott. A magyar felajánlás eredményeként a CAC-hoz több tagállam is csatlakozott.

A közös vízumkérelem-átvevő központ 2007. április 12-én kezdte meg működését, ettől kezdve veszik át a magyar vízumkérelmek mellett az osztrák, a szlovén és a lett vízumkérelmeket, a dán vízumkérelmeket május 21-étől kezdődően gyűjtik. A közös vízumkérelem-átvevő központ az egyes érintett tagállamok és a Magyar Köztársaság között megkötött kétoldalú megállapodások alapján működik. A központ átveszi a vízumkérelmeket, az adatokat és dokumentumokat továbbítja a célország konzulátusának és a visszaérkezett vízumokat kiadja a kérelmezőknek. Szükség esetén, például interjúra történő meghíváskor felveszi a kapcsolatot a kérelmezővel. A tagállamoknak a vízumkérelem elbírálásához kapcsolódó gyakorlata különböző. Vannak olyan tagállamok, amelyek a vízumkérelmezőtől több igazolást, dokumentumot kérnek és ezek alapján döntenek, a kérelmező személyét ellenőrizve. Van olyan tagállam, mint Lettország, ahol a lett meghívó fél ellenőrzésére fektetik a hangsúlyt, és magának a kérelmezőnek az ellenőrzése kevésbé szigorú. A CAC minden esetben az érintett tagállam előírásaira tekintettel jár el.

A központ munkatársai átveszik a kérelmezőtől a vízumkérelmet és a szükséges dokumentumokat, és ellenőrzik, hogy minden hiánytalanul került-e benyújtásra. A kérelmeket elektronikus úton és papíralapon is továbbítják. Az osztrák és dán kérelmeket a bukaresti konzulátusokra, a szlovén és a lett kérelmeket pedig Kijevbe küldik meg. Az elektronikus úton továbbított adatok szűkebb adatkörre vonatkoznak. Az útlevél leolvasó segítségével a rendszerbe bevitt fénykép, személyes adatok és az útlevél adatai, továbbá az ügyfél lakcíme kerül elektronikusan továbbításra. A kérelmeket hetente gyorspostával küldik meg az illetékes konzulátusoknak, illetve a kijevi lett konzulátusnak csak a kérelem szkennelt változatát küldik meg. A postára adásig a kérelmeket elkülönítve, elzárva tárolják.

Az adatok elektronikus elküldését követően a számítástechnikai rendszer egy táblázatban generálja a következő adatokat: nyilvántartási szám, a kérelem beérkezése, a kérelem státusza és a kérelmező vezeték- és keresztneve; további személyes adat nem marad a rendszerben. A vízum kiadását követően ez a nyilvántartás is törlésre kerül. A központ működése során szükségessé vált a kérelmező elérhetőségének rögzítése, mert esetenként személyes interjúra kell hívni a kérelmezőt a döntéshozó konzul kérésének megfelelően. Ezért a vízumkérelem nyomtatvány első oldalát az elérhetőségi adatokkal lefénymásolják és ez a másolat Kisinyovban marad a vízumkérelem-átvevő központban. Javasoltuk, hogy a vízum kiadását és a költségek elszámolását követően ezt a fénymásolatot semmisítsék meg.

A kérelmek benyújtásakor a kérelmezők román és orosz nyelvű nyilatkozatot írnak alá, mely alapján hozzájárulnak ahhoz, hogy adataikat a közös vízumkérelem-átvevő központ kezelje, továbbá hozzájárulnak adataik külföldre történő továbbításához. A vizsgálat során kértük, hogy ezt a nyilatkozatot egészítsék ki azzal, hogy milyen célból kerülnek továbbításra az adatok. Kérésünknek megfelelően a nyilatkozatot még a vizsgálat során módosították.

A vízumkérelmezők tájékoztatása megfelelő. A világhálón a www.cac.md címen található román és orosz nyelven tájékoztatás a vízumkérelmek benyújtásának feltételeiről államok szerinti tagolásban, továbbá a központ munkarendjéről, az ügyintézési tudnivalókról. Ezen kívül automata telefonos információs rendszeren keresztül is megismerhetők a szükséges tudnivalók a nap 24 órájában, továbbá a konzulátuson fali hirdetőkön tájékozódhatnak az érdeklődők.

Természetesen azonosításra alkalmatlan módon statisztikákat készítenek a központ munkájára vonatkozóan. Ezek alapján 2007. április 12-e és május 21-e között 167 magyar, 152 osztrák, 122 lett és 10 szlovén kérelmet vettek át Kisinyovban.

A magyar vízumkérelmek feldolgozása

A Magyar Köztársaság külképviseletein a vízumkiadásnál a külföldiek beutazásáról és tartózkodásáról szóló 2001. évi XXXIX. törvény (továbbiakban: Idtv.) és a végrehajtására kiadott rendeletek rendelkezéseire tekintettel jártak el. A pontosság érdekében megjegyezzük, hogy az Idtv.-t a vizsgálatot követően a harmadik országbeli állampolgárok beutazásáról és tartózkodá-

sáról szóló 2007. évi II. törvény hatályon kívül helyezte. 2007. július 1-től az eljárás és az adatkezelés szabályait az új törvény határozza meg.

A magyar vízumkérelmek kapcsán elmondható, hogy az ügyintézés nagyrészt megegyezik a korábbi vizsgálatok során megismert ügyintézéssel. A kisinyovi konzulátuson is megfigyelhető az egyes adminisztratív fázisok elkülönülése. A vízumkérelmeket és a vízumkérelem elbírálásához szükséges dokumentumokat a helyi alkalmazottak veszik át a kérelmezőtől. Ezt követően az adatok felvitele a Konzuli Információs Rendszerbe (KIR) a magyar vízumadminisztrátorok feladata. A konzulátuson dolgozók a KIR azon részéhez férnek hozzá, melyhez munkájuk elvégzéséhez jogosultsággal bírnak. A magyar konzulátusra kiküldött rendszergazda a jogosultsági beállításokat szükség szerint haladéktalanul módosítani tudja. Vízumkérelmet utazási irodán keresztül a konzulátus nem fogad el, a kérelmeket kevés kivételtől eltekintve személyesen kell leadni.

A vízumkérelmek leadásakor a kérelmezők leadják útlevelüket, a kitöltött vízumkérelmet és egyéb szükséges dokumentumot. A vízumkérelmek átvételét követően az útlevél adatait útlevél leolvasó segítségével felviszik a KIR-be. Ha a beolvasás nem tökéletes, akkor manuálisan rögzítik az adatokat. A vízumkérelem elbírálásához szükséges további, az útlevélben nem szereplő adatokat szintén manuálisan rögzítik (erre példa az egészségbiztosítás időtartama). Az adatbevitelt és a vízumdíj számlázását követően egy, a képernyőn megjelenő ablakban tájékoztatás jelenik meg arra vonatkozóan, hogy a vízumkérelmező adatai szerepelnek-e a beutazási és tartózkodási tilalom alatt állók jegyzékében (tiltónévjegyzék) és az elveszett útiokmányok adatbázisában. A tiltónévjegyzékben és az elveszett úti okmányok adatbázisában keresni nem lehet, egy-egy ügyhöz kapcsolódóan jelez találatot a rendszer, vagy jelzi, hogy az adott személy nem szerepel az adatbázisban.

A KIR a vízumkérelmezők adatait a Külügyminisztériumon keresztül a Bevándorlási és Állampolgársági Hivatalba (BÁH) továbbítja. A jogszabályban meghatározott esetekben a vízumkérelem ügyében nem a konzulátuson születik döntés, hanem a rendszerben továbbított adatok alapján a BÁH dönt a kérelem ügyében. A moldáv állampolgárok esetében főszabály szerint a vízumkérelem elbírálása központi hatáskörben a BÁH-nál történik a Vízumrendészeti kézikönyv 5. sz. melléklete alapján.

Az Idtv. 79. § (2) értelmében a vízumkérelmek és a kiadott vízumok alapján a külföldi adatait a központi adatkezelő szerv (BÁH) a vízum

érvényességi idejének lejártát követő öt évig, az illetékes idegenrendészeti hatóság (konzulátus) a vízum érvényességi idejének lejártát követő egy évig kezeli. A kérelmeket és a benyújtott dokumentumokat a D vízumkérelmek és az elutasított kérelmek kivételével irattárban őrzik. Az irattárban 2006-ban és 2007-ben benyújtott vízumkérelmeket találtunk az ellenőrzés alkalmával, az elutasított kérelmek a 2003-as évtől kezdődően vannak meg az irattárban. A korábban benyújtott, elutasított kérelmeket a vonatkozó rendelkezések alapján megsemmisítették.

A vízumkérelmezők tájékoztatása megfelelő. Az Interneten, automata telefonos tájékoztatási rendszeren és a konzulátuson keresztül is megszerezhető a szükséges információ román és orosz nyelven. A vizsgálat összegzéseként megállapítható, hogy a Magyar Köztársaság kisinyovi konzulátusán a vízumkiadás során az adatkezelés, adatvédelem megfelel a jogszabályi előírásoknak, a közös vízumkérelem-átvevő központ pedig kifejezetten úttörő szerepet lát el, amely során az adatvédelmi normákat maradéktalanul sikerült megvalósítani.

A Közös Ellenőrző Hatóság ülésén beszámoltunk a Kisinyovban végzett vizsgálatról. A vizsgálatról készített jelentést megküldtük a CAC-ban résztvevő többi tagállam adatvédelmi hatóságának is.

Szentpétervár

2007 áprilisában vizsgáltuk a szentpétervári főkonzulátuson a vízumügyintézés gyakorlatát. A vízumkiadás során az adatkezelés, adatvédelem a következő két ajánlás figyelembevételével megfelel a jogszabályi előírásoknak.

A főkonzulátuson kamerák figyelik az épület azon részeit, ahol az ügyfelek megfordulnak, erre több helyen is felhívják az ügyfelek figyelmét. Jelenleg a felvételeket nem rögzítik. Tanácsos lenne a felvételek rögzítése az esetleges visszaélések, ügyféli praktikák – amire más külképviseleten már volt példa – elkerülése érdekében. A felvételek rögzítésének adatvédelmi szempontból nincs akadálya abban az esetben, ha erről tájékoztatják az ügyfeleket, továbbá, ha a felvételeket bizonyos idő elteltével törlik.

Mivel az alagsori irattári helyiség egyben raktározási célokat is szolgál, ezért kértük, hogy a helyiségbe belépéssel rendelkezők körét azokra az alkalmazottakra korlátozzák, akik az irattári anyagokat kezelhetik.

Shanghaj, Hong Kong, Taipej

Tajvan államiságát a Magyar Köztársaság nem ismeri el, ezért nincs a két állam között hivatalos kapcsolat. Ez az oka annak, hogy Tajvanon nem működik konzulátus. A tajvani Magyar Kereskedelmi Iroda fő feladata a kétoldalú kapcsolatok fejlesztése, kiemelten a kereskedelmi együttműködés bővítése, ugyanakkor az Iroda intézi a Tajvanról hazánkba látogatók beutazásával és tartózkodásával kapcsolatos feladatokat is.

A vízumkérelmek száma az ázsiai régióban folyamatosan növekszik. Shanghajban az elmúlt két évben megkétszereződött a vízumkérelmek száma. Hong Kongban nem oly jelentős a vízumkérelmek száma, de az elmúlt két évben a növekedés 30 százalék volt. Az elmúlt években a tajvani Kereskedelmi Iroda által kiadott vízumok száma nem nőtt jelentős mértékben: Tajvanon évente 12.000 vízumot adnak ki.

Az adatvédelmi vizsgálat megállapította, hogy a Magyar Köztársaság shanghaji és hong kongi főkonzulátusán és a tajvani Kereskedelmi Irodában a vízumkiadás során folytatott adatkezelési, adatvédelmi gyakorlat a következő ajánlások figyelembevételével megfelel a jogszabályi előírásoknak.

A külképviseletek jelenleg a KIR-nek csak ahhoz a részéhez férnek hozzá, csak azoknak a vízumkérelmezőknek az adatait látják, akik az adott külképviseleten nyújtották be kérelmüket. A Külügyminisztérium tervei között szerepelt a KIR olyan fejlesztése, hogy az adatbázisba bevitt kérelmezői adatokhoz ne csak az a konzulátus férhessen hozzá, amelyik az adatokat bevitte, hanem az adott országban található valamennyi magyar konzulátus. Ez az elképzelés adatvédelmi szempontból nem kifogásolható és a konzulátusok munkáját megkönnyítené, ezért javasoltuk, hogy ezt a fejlesztést a kínai magyar külképviseleteken is valósítsák meg. A kijevi konzulátuson elvégzett vizsgálathoz hasonlóan, ebben az esetben tanácsos lenne a konzulátuson alkalmazottak munkaszerződésébe belefoglalni, hogy a biztonsági kamerák munkavégzés közben felvételt készítenek róluk. A munkavállalók aláírásával hozzájárulásuk a felvételek készítéséhez megadottnak tekinthető.

Elutasító döntés esetén a shanghaji konzulátus a kérelmező által benyújtott összes dokumentumot megküldi a Bevándorlási és Állampolgársági Hivatal (BÁH) regionális központjába. Ilyen gyakorlatot az eddigi vizsgálatok során nem tapasztaltunk és – kivételes estektől eltekintve – nem is szükséges, hogy a dokumentumokat akár eredeti formában, akár másolat-

ban a konzulátus továbbítsa a BÁH-nak. Adatbiztonsági okokból is célszerűbb az adatokat a konzulátuson tárolni. A helyi konzuli együttműködés keretében a konzulátusok közötti személyes adat átadására vonatkozóan nincs jogszabályi felhatalmazás. Ezért ezt a gyakorlatot, bár elképzelhető, hogy a konzulátusokon folyó munkát megkönnyíti, kértük, hogy a jövőben ne folytassák.

Az Amerikai Egyesült Államok vízummentességi programjának kiterjesztése (Visa Waiver Program)

A Külügyminisztérium 2007 májusában szervezett szakmai megbeszélést az Amerikai Egyesült Államok vízummentességi programjának magyar állampolgárokra történő kiterjesztésének lehetőségéről. A megbeszélésen elmondtuk, majd később ezt írásban is megerősítettük, nincs akadálya annak, hogy a Visa Waiver Program keretében az amerikai fél megkapja az ellopott, elveszett úti okmányokra vonatkozó adatokat. Ezeknek az adatoknak egy részét az Interpolon keresztül jelenleg is ellenőrizni tudják az amerikai hatóságok. A Schengeni Információs Rendszer kialakítása során kiépítendő, az ellopott, elveszett úti okmányok központi adatbázisához történő hozzáférés kizárólag eseti jelleggel elfogadható. Szintén elképzelhető a körözési információkhoz történő hozzáférés megvalósítása, meghatározott bűncselekmények vonatkozásában, eseti alapon. Szükséges azonban az adatlekérdezésekre vonatkozó szabályok kétoldalú megállapodásban történő szabályozása és a megállapodás törvényben történő kihirdetése.

A Visa Waiver Program kapcsán megkerestük nemzetközi partnereinket, akik arról tájékoztattak, hogy a többi tagállamban az adott ország ez ügyben illetékes hatóságai nem kérték a nemzeti adatvédelmi hatóságok szakmai véleményét a program előkészítése során.

A Prümi Szerződéshez való csatlakozás

Belgium, Németország, Spanyolország, Franciaország, Luxemburg, Hollandia és Ausztria 2005. május 27-én írták alá a „határon átnyúló együttműködés fokozásáról, különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció leküzdése érdekében" létrejött szerződést (Prümi Szerződés), melynek célja a Schengeni Megállapodás bevezetésével

keletkezett biztonsági deficit kiegyenlítése volt. Ennek megfelelően a résztvevő országok fokozzák a határon átnyúló együttműködésüket a terrorizmus elleni harc, a határon átnyúló bűnözés és az illegális migráció területén, különös tekintettel a kölcsönös információ cserére. Ennek fő eszközei a DNS profil, az ujjnyomat és a gépkocsi nyilvántartás adatainak kölcsönös felhasználása, hangsúlyozva, hogy az úgynevezett nemzeti kapcsolattartó egységen (National contact point) keresztül történő adatváltásnál az egyes országok nemzeti joganyagának előírásait kell figyelembe venni.

A Prümi Szerződéshez történő magyar csatlakozás előkészítő munkái 2006–ban kezdődtek, erről a tavalyi beszámolóban már volt szó. Az egyik lényeges megállapítás az volt, hogy a magyar csatlakozás törvényhozási munkái során ki kell jelölni a bűnügyi nyilvántartásról és a hatósági erkölcsi bizonyítványról szóló, 1999. évi LXXXV. törvényben (továbbiakban: Bnytv.) is szereplő daktiloszkópiai és fénykép, valamint a DNS nyilvántartás adatkezelőjét. Mindkét nyilvántartás a Bűnügyi Szakértői és Kutatóintézet (BSZKI) szervezeti keretében működik, de a Bnytv. által meghatározott bűnügyi nyilvántartást üzemeltető (kezelő) szervezet jelenleg a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala. Ezért a két szervezet viszonyában adatvédelmi szempontból szükségessé vált a feladatmegosztás (adatkezelő-adatfeldolgozó) tisztázása, melyre a 2007-ben befejeződött vizsgálatunk tett pontot. Ellenőriztük a BSZKI-ban folytatott daktiloszkópiai rendszer adatkezelését, a 2007 márciusában megtartott helyszíni ellenőrzés célja pedig a DNS-profil nyilvántartás adatkezelésének átvilágítása volt.

A Bnytv. előírása alapján külön adatbázisban tárolják az egyes mintákhoz tartozó személyes adatokat és a minták laboratóriumi vizsgálatával nyert DNS-profilokat. A két adatbázist egy közös azonosító kód alapján lehet egymáshoz rendelni, mely csupán mutató szerepet tölt be, semmilyen következtetés nem vonható le belőle az adattartalomra vonatkozóan.

A törvényben szereplő gyanúsítotti minták feldolgozásának leginkább labormunka-igényes, ennek következtében „bérmunkaként" költségtakarékosan kiadható részét anonimizált formában a Genoid Molekulárbiológiai Kutató, Gyártó és Egészségügyi Szolgáltató Kft. (Genoid Kft.) végzi. A Genoid Kft. a 2005. évben kiírt közbeszerzési eljárás keretében (a megfelelő auditáció birtokában) három éves időtartamra elnyert pályázat alapján kapott erre a tevékenységre megbízatást, mint egy kifejezetten erre a

tevékenységre szakosodott, a szükséges eszközökkel felszerelt minősített laboratórium. A munka minőségét a Genoid Kft.-nél dolgozó igazságügyi szakértő ellenőrzi, felügyeli. A minták anonimizálását a Genoid Kft.-nek történő továbbítás előtt a BSZKI végzi, a minták megjelölése vonalkóddal történik, melyre az adott minta feldolgozás során történő automatizált nyomon követése miatt is szükség van.

A Genoid Kft.-nél végzett tevékenység jelenti az Intézet szakértői munkájának alapját, mert az itt meghatározott DNS-profil, mint alapadat kerül be a DNS-profil adatbázisba. A Genoid Kft.-nél alkalmazott biztonsági eljárások részben a minősített laboratóriummal szemben támasztott követelmények, részben a munka speciális jellege által megkívánt módon alakulnak.

Az adatvédelmi törvény értelmező rendelkezései szerint ez a tevékenység szerződés keretében végzett adatfeldolgozó tevékenységnek minősül, melyet az adatkezelő megbízásából végez az adatfeldolgozó. A Belügyminisztérium Központi Gazdasági Főigazgatósága, mint megrendelő, és a megrendelő részéről közreműködő szervezeti egység, a BSZKI által a Genoid Kft.-vel kötött „Vállalkozási szerződés" másolatát áttekintve megállapítható, hogy az összhangban van a közbeszerzési eljárásban kiírt feltételekkel, azonban az adatfeldolgozásra vonatkozóan csak nagyon általános előírásokat tartalmaz. Ezért javasoltuk, hogy a Genoid Kft.–vel az adatfeldolgozásra vonatkozó megbízási szerződést soron kívül kössék meg. Ebben a szerződésben kell pontosan szabályozni a DNS-profil feldolgozásával kapcsolatos eljárási szabályokat, az egyes szereplők adatkezeléssel kapcsolatos jogait, kötelezettségeit, különös tekintettel a minták anonimitására.

A BSZKI végzi a személyes adathoz nem kötött helyszíni bűnjelmintákból a DNS profilok meghatározását, a már ismert profilokkal történő összehasonlítását, azaz a tulajdonképpeni szakértői munkát. Ennek keretében külföldi megkeresések esetén az intézet ad szakértői véleményt, illetve szükség esetén a magyar megkereséseket az intézet kezdeményezi a külföldi partnereknél. Azonosítás esetén az eredmény a minta azonosító kódjának megismerése. Hazai megkeresés esetén az azonosító kód alapján állapítják meg a kérdéses személy kilétét a személyi adatbázisban, külföldi megkeresés esetén az azonosítás tényét közlik az azonosítást kérő szervezettel, de a szóban forgó személy adatait csak jogsegély egyezmény keretében adják meg.

A helyszíni vizsgálat során ezeket a folyamatokat – a lehetőségekhez képest – megtekintettük, ideértve a név-adatokkal beérkezett minták érkeztetését, az adatok személyes adatbázisba történő rögzítését és az anonimizálás folyamatát.

Az itt szerzett tapasztalatok megerősítették azt a korábbi véleményünket, hogy a DNS-profil adatbázisnál alkalmazott adatkezelés – az adatfeldolgozói szerződés megkötésének függvényében – megfelel a törvény által előírt szabályoknak. Mivel a szakértői munka jelenti az adatbázis működtetésének alapját – ezt a tényt a Belügyminisztérium közjogi helyettes államtitkára, Dr. Sípos Irén 2004. május 12-én kelt levelében is hangsúlyozta –, a BSZKI adatkezelő tevékenységet folytat, amely során több, ehhez kapcsolódó adatfeldolgozást végző szervezettel működik együtt. Az adatkezelői státusz megerősítése azonban természetszerűleg együtt jár olyan kötelezettségekkel is, melyek a Bnytv. 46. §-ban szereplő adatszolgáltatásra és az érintett állampolgárok 49. § (4) bekezdésében szereplő tájékoztatására vonatkoznak.

A vizsgálat eredményéről tájékoztattuk az Igazságügyi és Rendészeti Minisztérium vezetőjét is, aki ígéretet tette arra, hogy a Bnytv. jövőben esedékes általános felülvizsgálatánál megállapításainkat figyelembe veszik.

Sajnálatos módon erre a felülvizsgálatra a 2007. évben nem került sor, pedig az Országgyűlés 2007. szeptember 17-én elfogadta a Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között a határon átnyúló együttműködés fokozásáról, különösen a terrorizmus, a határon átnyúló bűnözés és az illegális migráció leküzdése érdekében létrejött Szerződés (Prümi Szerződés) kihirdetéséről, valamint ehhez kapcsolódóan egyes törvények módosításáról szóló 2007. évi CXII. törvényt, mely 2007. december 1-jén lépett hatályba.

Az EURODAC vizsgálat

Az Európai Közösségek tagállamainak egyikében benyújtott menedékjog iránti kérelem megvizsgálására illetékes állam meghatározása érdekében 1990. június 15-én Dublinban aláírták az erről szóló egyezményt (továbbiakban: a dublini egyezmény). Az egyezmény előírásai értelmében meg kell állapítani a menedékjogot kérelmező személyek és a Közösség külső határa-

inak jogellenes átlépése miatt letartóztatott személyek azonosságát, valamint lehetővé kell tenni annak ellenőrzését, hogy az illegálisan az adott tagállam területén tartózkodó külföldiek kértek-e menedékjogot valamely másik tagállamban.

A személyek pontos azonosításának alapjául a Európai Közösségek tagállamai az ujjnyomatok összehasonlítását választották. Az erre szolgáló rendszer EURODAC néven került kialakításra a Tanács 2725/2000/EK rendelete alapján. Az itt meghatározott rendszer egy központi egységből áll, amely az ujjlenyomatadatok számítógépes központi adatbázisaként működik, és a tagállamok, valamit a központi adatbázis közötti elektronikus adatátvitelt szolgálja. Az Eurodac rendszer tehát egyrészt a menedékjogot kérelmező személyek azonosítására, másrészt a menedékjog elbírálásában eljáró ország meghatározására szolgál. A rendszer alkalmazása ennek megfelelően bonyolult jogi és eljárási feladatokat lát el.

Az Európai Adatvédelmi Biztos, Peter Hustinx úr kezdeményezésére lefolytatott – a tagállamoknak továbbított kérdőíves – vizsgálat összefoglaló jelentését az EURODAC Felügyelő Koordinációs Csoport 2007 júliusában adta ki. Ennek főbb megállapításai a következők:

1. A különleges keresések témakörében nagyszámú keresést hajtottak végre, ezeket azonban nagyrészt tévedésből végezték (például a rendszerhez történő egyéb hozzáférés nehézsége miatt vagy oktatási célból).

2. Az Eurodac rendelettől eltérő, egyéb célra történő lehetséges alkalmazás, azaz a célhozkötöttség elvének tiszteletben tartása területén a vizsgálat nem állapított meg hiányosságot. Az a tény, hogy az adatvédelmi hatóságok még nem kaptak panaszt ezzel kapcsolatban, szintén megerősíti ezt az értékelést (azonban óvatosan kell bánnunk ezzel a következtetéssel, tekintettel a menedékért folyamodók Eurodac-hoz kapcsolódó jogi ismereteik hiányára).

3. A felelősségek szétválasztásánál a jelentés megállapította, hogy míg az alapelv önmagában nem is problémás, az alkalmazása igen. Nem fordulhat elő, hogy a legfőbb adatkezelő nem azonosítható, a legbonyolultabb felépítésű tagállamok esetében azonban maguk az adatvédelmi hatóságok kérték, hogy az adatkezelő személyét közöljék velük. Ennek a kérdésnek a pontosítása Magyarországon is az elkövetkező időszak fontos feladatát képezi.

4. Az ujjnyomatok technikai minőségével kapcsolatban jelenleg az adatok 6 százalékát utasítják el rossz minőség miatt; az elmúlt évben is ez volt a helyzet. Általános megállapítás, hogy az optikai szkennerek, mint például a „live scanner" alkalmazása sokkal hatékonyabb, mint a tintás ujjlenyomatvétel. Az optikai szkennerek esetén a minőségi hibákat azonnal jelzi a berendezés, ezzel összhangban a tintás ujjnyomatvételi lapok esetén magasabb az elutasítás aránya, mint ez elektronikus lapoknál. Az ujjnyomatok technikai minőségét egyaránt befolyásolja az alkalmazott technikai berendezések színvonala, illetve az ujjnyomatvételt végző személyzet rendszeres oktatása. Ezen a téren Magyarország – a jelentés megállapításaitól függetlenül – új eszközök rendszerbe állításával bővíti az elektronikus ujjnyomatbeviteli kapacitását, másrészt rendszeres képzéssel, továbbképzéssel és helyszíni konzultációval segíti az ujjnyomatok vételének minőségi javítását.

Az Európai Adatvédelmi Biztos, mint az EURODAC rendszer központi egység felügyelő szervezetének vezetője, az előbb említett – tagállami – vizsgálat mellett, a központi egységre vonatkozó részletes biztonsági auditot is végrehajtott. Az Eurodac rendszere a központi egységből, a rendszer működését garantáló egységből, valamint a felhasználói egységekből áll. A szóban forgó vizsgálat a központi egységet érintette, és nem terjedt ki a központi egység és a tagállamok közötti hálózat működésére. A vizsgálat magában foglalta a központi infrastruktúra, személyzeti, szervezeti és technológiai kérdések vizsgálatát annak érdekében, hogy meg lehessen állapítani, vajon a rendszer továbbra is eleget tesz-e az Eurodac rendeletben foglalt követelményeknek, illetve a biztonsági intézkedések megfelelnek-e a jelenlegi legjobb gyakorlatnak. A vizsgálat azzal a megállapítással zárult, hogy az alkalmazott biztonsági intézkedések, valamint az intézkedések alkalmazásának módja magas szintű védelmet garantál. Ugyanakkor a rendszer bizonyos elemei és a szervezeti biztonság gyenge pontokat is tartalmaz.

NEBEK - EUROPOL Nemzeti Iroda

Magyarország 2001-ben, az újonnan csatlakozó országok közül elsőként, együttműködési megállapodást kötött az Europollal, amelynek teljes jogú tagjává az Európai Unióhoz történt csatlakozás után három hónappal vált. Az Europol Egyezményt a 2006. évi XIV. törvény hirdette ki.

Az Europol célja, hogy a tagállamok közötti rendőrségi együttműködés keretében javítsa a tagállamok illetékes hatóságainak eredményességét és együttműködését a nemzetközi bűnözés súlyos formáinak megelőzése és leküzdése terén. Az Europol az úgynevezett „egyablakos elv" alapján működik: meghatározott feladatokat egy kijelölt központi hatóság lát el a tagállamban, amely a hazai koordináció mellett az uniós szervezettel való kapcsolattartásért is felelős, azaz közvetítő szerepet tölt be. Az „egyablakos elv"-nek való megfelelés céljából az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény hozta létre az Országos Rendőr-főkapitányság szervezetében a Nemzetközi Bűnügyi Együttműködési Központot (NEBEK), mely 2002. januárban kezdte meg működését. A törvény hatálya kiterjed az Europol-lal, az Interpol-lal, a Schengeni Információs Rendszerben (SIS), az Európai Csalásellenes Hivatallal (OLAF), valamint a két- és többoldalú nemzetközi szerződések keretében vagy az európai közösségi jogi normák alapján megvalósuló bűnügyi együttműködésre és információcserére.

Az Europol Egyezmény értelmében a tagállamoknak ki kell jelölniük egy független nemzeti adatvédelmi ellenőrző hatóságot, amelynek egyik feladata az Europollal történő információcsere során a személyes adatok kezelésének és továbbításának hazai jog szerinti ellenőrzése. E feladatot Magyarországon – a 2006. évi XIV. törvényben előírtaknak megfelelően – az adatvédelmi biztos látja el.

A 2007-ben végrehajtott adatvédelmi ellenőrzéseink során nyolc, véletlenszerűen kiválasztott, az Europol-lal történt adatcserét tartalmazó ügyet vizsgáltunk, s az alábbiakat állapítottuk meg:

1. Egy kiadatással kapcsolatos ügyben az érintettet olyan nyilvántartásban is lekérdezték, amely az adott ügy intézéséhez nem volt szükséges – ez rutinszerű (cél nélküli) lekérdezésre utal.

2. Az Europolnál működik egy Interpol-összekötő is. Egy tőle származó, telefonszám-ellenőrzést kérő ügyben az érintettek adatait a hazai nyilvántartásokban ellenőrizték, találat nem volt, de a megkeresésre nem válaszoltak. Céltól eltérő adatkezelésre utal, hogy a telefonszám-felsorolásban szereplő ország-előhívó számok alapján magyarországi szám nem volt. Az ugyanezen ügyben érkezett további adatokat és információkat nem ellenőrizték, nem elemezték, és nem továbbították egyetlen olyan hazai nyomozóhatóságnak

sem, amely érdeklődhet az eset iránt. Az adattárolás célja sem azonosítható annak fényében, hogy sem elemzés, sem hazai szervnek való továbbítás nem történt.

3. Gyakori hiányosság, hogy az adatkérésből hiányzik vagy az adatkérés célja, vagy a jogalapja, esetenként mindkettő. E mulasztás az adatkezelés jogszerűségének ellenőrizhetőségét akadályozza.

4. Az évek óta folyó ügyek egy iktatószámon futnak, s esetenként több száz alszámot tartalmaznak. Az ügyeket nem strukturálják bűncselekmény, személy, vagy más szempont szerint, ezért nehezen áttekinthetőek, ami nemcsak az adatvédelmi ellenőrzést, hanem a munkavégzést – így az elemzést is – megnehezíti.

Egy ilyen, 2003 óta tartó ügyben találtunk egy távközlési szolgáltatónak küldött adatkérést, amelyben az adatkérés jogalapjaként egy elérhetetlen megállapodásra hivatkoztak. További jogalapként a 29/1996. számú BM rendelet volt megjelölve, amely azért volt hibás, mert ez a rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 15/1994. BM rendeletet módosította, és sem az alaprendeletben, sem a módosításban nem szerepel a NEBEK, mivel az nem nyomozó hatóság. Ugyanebben a levélben a NEBEK élni kívánt azzal a törvény adta lehetőséggel, hogy az érintett tájékoztatáshoz fűződő jogát bűnüldözési érdekből korlátozza, ám elvétette a jogszabályra hivatkozást: a rendőrségi törvény olyan szakaszára hivatkozott, amelyet az Alkotmánybíróság két hónappal azelőtti hatállyal megsemmisített.

5. Az Europollal folytatott információcsere során mind az Europol, mind a hazai jogszabályok előírásai alapján különböző jelöléseket kell alkalmazni, amelyekkel egyrészt az információ és forrása megbízhatóságát, másrészt az információ felhasználhatóságát minősítik. Adatvédelmi szempontból ez utóbbinak van jelentősége. Sajnálatos módon mind a hazai, mind a külföldi hatóságoktól érkező adatkérések, illetve az azokra adott válaszok többségéről vagy hiányoznak a jelölések, vagy pontatlanok. Az előző pontban említett ügyben például az egyik adatkérésen szerepelt egy kezelési kód, de a részleteket, azaz a továbbítás célját, a további felhasználási engedélyeket és korlátozásokat már nem jelölték meg.

6. 2007 novemberében üzembe állították a NEBEK új elektronikus iktatórendszerét. A MonDoc nevű program elkészítését egyrészt az eddigi iktatórendszer hiányosságai, másrészt a schengeni csatlakozásból adódó

többletfeladatok számítógépes támogatása indokolta. Az egyik adatvédelmi ellenőrzésünk során megkezdtük a program „tesztelését". A program első ránézésre bonyolult, a funkciógombok mérete és elhelyezése nem igazán felhasználóbarát, az egyes műveletek elvégzése körülményes és időigényes, emiatt az a benyomásunk alakult ki, hogy a program használatával az ügyintézési idő jelentősen meghosszabbodik.

A korábbi rendszer egyik hibájaként értékeltük, hogy a küldő szervezeti egység nevét nem legördülő menüből kellett kiválasztani, hanem be kellett gépelni. A gépelési hibák miatt egy szervezeti egység neve legalább két, de eseténként 5-6 formában szerepelt a rendszerben, ami a küldő szerv szerinti visszakeresést nehezítette. A szabad begépelési lehetőség a MonDoc rendszerben is adott, emiatt a lekérdezés továbbra is összetett feladat marad (valamennyi formációt egyenként kell lekérdezni, hogy végül összeálljon a szervezeti egység teljes iratanyaga).

Megnéztük az egyik irat naplóadatait is: az egyes műveletek elnevezései miatt nem tudtuk megállapítani, hogy valójában mi történt a vizsgált elektronikus irattal.

7. Végül, de nem utolsósorban két örvendetes tény: elkészült az egyes országos nyilvántartásokhoz történő hozzáférési jogosultsággal rendelkezők nyilvántartása, ezzel együtt új, ellenőrizhetőbb eljárási rendet vezettek be a jogosultsági ügyintézésben, továbbá a munkaállomásokat leválasztották az internetről, amivel komoly adatbiztonsági kockázatot hárítottak el.

Váminformációs Rendszer (CIS)

A Európai Unió tagországainak vámügyi együttműködése során az információcsere hatékonyságának elősegítése érdekében a tagállamok és a Bizottság által egyformán hozzáférhető automatizált Váminformációs Rendszert (CIS) hoztak létre, melynek első és harmadik pilléres jogi alapját az 515/97/EK rendelet és az 1995. június 26-i Egyezmény teremtette meg. A CIS a megállapodások értelmében az Európai Csalásellenes Hivatal (OLAF) keretében működik, és ez a szervezet a felelős a CIS technikai megvalósításáért, működtetéséért és karbantartásáért.

A CIS egy központosított rendszer, melynek egyik legfőbb jellemzője, hogy a tagállam által kijelölt illetékes nemzeti hatóság (Magyarországon a Vám- és Pénzügyőrség) közvetlen adatbeviteli lehetőséggel rendelkezik. A

nemzeti adatbázisban szereplő adatok központi rendszerbe történő rögzítését csak *„jóváhagyó"* (*„authorizer"*) jogosultsággal rendelkező végezheti, aki a rögzítés során vizsgálja a bevitt adatok pontosságát, jogszerűségét és az adatvédelmi szabályok érvényesülését. A bevitt adatokat bármelyik regisztrált felhasználó lekérdezheti. A felhasználói jogosultság megadása a *„jóváhagyó"* által aláírt formanyomtatvány alapján az OLAF-nál történik. A központi rendszerben tárolt adatokat évente felülvizsgálják.

A CIS adatállomány első- és harmadik pilléres adatokat is tartalmaz, ezért a rendszer adatvédelmi felügyelete többrétű:

- az első pillér adatkörébe tartozó ügyek esetében a tagállami adatbázist a nemzeti adatvédelmi ellenőrző hatóság, az OLAF-nál lévő központi adatbázist az európai adatvédelmi biztos és az OLAF belső adatvédelmi felelőse ellenőrizheti;
- a harmadik pillér adatkörébe tartozó ügyek esetében a tagállami adatbázist a nemzeti adatvédelmi ellenőrző hatóság, európai szinten pedig a közös adatvédelmi ellenőrző hatóság (Customs Joint Supervisory Authority – Customs JSA) felügyeli.

Magyarországon a nemzeti adatvédelmi ellenőrző hatóság feladatát az adatvédelmi biztos látja el, aki 2006 nyara óta tagja a közös adatvédelmi ellenőrző hatóságnak és 2007 tavaszától a Customs JSA alelnökévé választották.

2006 júniusában a Customs JSA úgy döntött, hogy valamennyi tagállamban egységes adatvédelmi ellenőrzést kell tartani, ezt a vizsgálatot az elmúlt évi beszámolóban részletesen ismertettük.

2007. június 13-14-én a JSA által kinevezett négy fős ellenőrző csoport vizsgálta a CIS működését és az adatbázisát. A Magyarország, mint tagország által bevitt adatok között hibát észlelt, amiről 2007. július 2-án tájékoztattak minket, és – 2007. július 20.-i határidővel – kérték a hibás adatmegadás okának kivizsgálását. 2007 júliusában az Adatvédelmi Biztos Irodájának munkatársai helyszíni ellenőrzést tartottak, melynek során kiderült, hogy egy arra jogosult vámhatóság egy gépjármű határon történő belépése során végzett ellenőrzésénél illegális rejtekhelyet fedezett fel a rakodótérben. Ez a rejtekhely a vizsgálat idején üres volt, de feltételezhető, hogy más esetekben bűncselekmény elkövetésére használták. Az erre vonatkozó adatokat és a gépjármű vezetőjének adatait rögzítették és továbbították a

magyar hatóságok a CIS-be. Ennek során a gépjárművezető személyes adatainak rögzítésénél került sor hibás adatrögzítésre, mivel születési dátuma helyére az adatrögzítés dátuma került megadásra. Ez véleményünk szerint a rögzítő program bizonyos hiányosságaira is felhívja a figyelmet. Az ellenőrzés során megtekintettük az adatrögzítés alapjául szolgáló ügyiratot, az adott esetre vonatkozóan megvizsgáltuk az adatkezelés szabályainak betartását.

A vizsgálat során a rendelkezésünkre álló ügyiratból megállapítható volt a hiányzó születési adat, melyet az arra jogosult tisztviselő jelenlétünkben kijavított az adatbázisban, és melynek eredményéről lekérdezés keretében személyesen is meggyőződtünk. A vizsgálat eredményről a kért határidőre tájékoztattuk a JSA titkárát.

Részvételünk a 29. cikk alapján létrehozott adatvédelmi munkacsoport tevékenységében

A munkacsoport a tagállamok nemzeti adatvédelmi felügyelő hatóságainak vezetőiből, biztosaiból álló, független tanácsadó szerv, melynek munkájában 2007-ben is aktívan részt vett Irodánk. Szinte minden megtárgyalt témához hozzájárultunk álláspontunk ismertetésével, ezzel szerepet (és felelősséget) vállalva a munkacsoport véleményeinek, munkaanyagainak elkészítésében.

A tagságunkból származó feladatainkat két csoportba lehet sorolni: az ülések előtti előkészítő és az azokat követő végrehajtási feladatokra. Az előkészítő folyamatban való aktív részvételt kiváló lehetőségnek tartjuk arra, hogy hangot adjunk adatvédelmi szabályozásunk sajátosságainak, prioritásainknak és megosszuk tapasztalatainkat a többi tagállammal. A munkacsoportnak gyakran uniós jogszabálytervezetekről kell állást foglalnia, így alkalmunk van arra, hogy ne csak azok átültetésekor, hanem már megalkotásukkor is kinyilvánítsuk véleményünket.

A munkacsoport véleményeinek előkészítése információgyűjtést jelent a tagállamok adatvédelmi hatóságaitól egy adott problémával kapcsolatban a nemzeti adatvédelmi szabályozásról, a kiadott állásfoglalásokról vagy arról, hogy mi a tagállamok álláspontja egy adatvédelmet érintő uniós jogszabály- vagy egyéb tervezetről. A kéthavonta tartott üléseken a tagál-

lamok ütköztetik véleményeiket, majd kialakítanak egy közös álláspontot, ezáltal előmozdítva az adatvédelmi irányelv egységes alkalmazását.

Fontosnak tartjuk a munkacsoport anyagainak elfogadását követően a közvélemény gyors tájékoztatását, ezért az ülésekről szóló sajtóközlemények és az elfogadott dokumentumok fordítását honlapunkon el lehet érni. Gyakorlatunkban figyelembe vesszük a véleményekben foglaltakat, főként, ha jogértelmezési problémák merülnek fel, vagy egy új probléma megoldása előtt állunk.

A munkacsoport tevékenységét 2007-ben a terrorizmus elleni küzdelem jegyében történő túlzott adatgyűjtés és adattovábbítás problémája, ezen belül különösen az USA és az EU különböző adatvédelmi szintjeinek közelítését célzó megállapodások értékelése dominálta. 2007-ben megkezdődött a keresőprogramok adatvédelmi kérdéseinek vizsgálata, amely jelentős visszhangot keltett a sajtóban is.

Emellett kiemelt figyelmet szentelt a munkacsoport a személyes adat fogalmáról szóló anyagának is, amely eddigi egyik legfontosabb lépése az egységes jogalkalmazás megteremtése terén.

A munkacsoport 2007-ben a következő véleményeket és munkaanyagokat fogadta el:

1/2007 sz. vélemény a bűnüldöző, a vám- és az egyéb biztonsági hatóságok munkájában alkalmazott felderítési technológiákról szóló zöld könyvről (WP 129):

Az Európai Bizottság 2006-ban fogadta el a bűnüldöző, a vám- és az egyéb biztonsági hatóságok munkájában alkalmazott felderítési technológiákról szóló zöld könyvet (általános problémafelvetés és alternatív javaslatok bemutatása) (COM(2006) 474), melynek célja az érdekelt felek közötti vita ösztönzése volt. A téma adatvédelmi vonatkozásainak köszönhetően a Bizottság a munkacsoportot is meghívta, hogy vegyen részt a dokumentummal kapcsolatos konzultációban.

A munkacsoport hangsúlyozta, hogy a felderítési technológiák példa nélküli megfigyelést tesznek lehetővé és felhívja a Bizottság figyelmét az adatvédelmi biztosok „megfigyelt társadalomról" szóló konferenciáján elfogadott közleményére. A közlemény arra figyelmeztetett, hogy a megfigyelésnek lehetnek pozitív következményei is, azonban ellenőrzés hiányá-

ban, túlzott mértékű, láthatatlan alkalmazásuk magánéletünket már nem csak befolyásolják, hanem aláássák bizalmunkat, megnövelik a társadalmi kirekesztődés esélyét. A technológiák önmagukban nem feltétlenül jelentenek problémát, ha az adatvédelmi jogszabályoknak egyébként megfelelnek. Elengedhetetlen például, hogy az emberek figyelmét felhívják alkalmazásukra.

Általános kifogás, hogy a zöld könyv felderítési technikákra vonatkozó definíciója nem elég pontos és részletes, általánosságban beszél „felderítési technikákról". Ez nem fogadható el, különbséget kell tenni az egyes technológiák között és világosan meg kell határozni azok adatkezelési céljait. Nem elegendő indok az alapvető jogok korlátozására az adott felderítési technika hasznossága: kényszerítő társadalmi szükségletet kell kielégítenie ahhoz, hogy jogszerűen korlátozza a magánélet tiszteletben tartásához való alapvető jogot.

Kifogásolható továbbá, hogy a zöld könyv egyenlőség jelet tesz a „terrorizmus" és „a bűnözés egyéb formái" közé. A vélemény végül néhány adatvédelmi alapelvre hívja fel a Bizottság figyelmét: meg kell határozni a személyes adatok gyűjtésének célját, csak ezen cél eléréséhez szükséges adatokat lehet begyűjteni, amelyeket csak a szükséges ideig szabad megőrizni.

Munkadokumentum az elektronikus egészségügyi nyilvántartásban (EHR) tárolt egészségügyi adatok kezeléséről (WP 131):

A munkadokumentum iránymutatást ad az egészségügyi adatok kezelésére vonatkozó jogszabályok értelmezéséhez, valamint áttekinti az elektronikus egészségügyi nyilvántartások kialakításának adatvédelmi feltételeit és a rendszerekbe beépítendő garanciákat.

Az EHR-rendszerek elsődleges célja az, hogy egy adott személyről összegyűjtsék az egészségi állapotára vonatkozó összes, hosszú távon feltehetőleg jelentőséggel bíró adatot. A rendszer biztosítja, hogy egy jövőbeli kezelés esetén rendelkezésre álljanak a lényeges információk, ezáltal megnövelve a kezelés sikerének esélyét. Ugyanakkor jelentős kockázatot rejt magában, hogy a felhasználók egy lényegesen szélesebb köre tud a rendszeren keresztül a betegek egészségügyi adataihoz hozzáférni.

Az orvosi nyilvántartásokban szereplő minden adat különleges, szenzitív adat, függetlenül attól, hogy nem közvetlenül a beteg egészségi állapotára vonatkozik (például a kórházba kerülés ideje és egyéb adminisztratív adatok). A betegtől nem kérhető általános jövőbeni adatkezelési hozzájárulás. Nem kell a beteg hozzájárulását kérni az adatkezeléshez, ha az létfontosságú érdekeinek védelméhez szükséges, azonban ez a kivétel csak életmentő kezelések esetén alkalmazható. A munkacsoport a továbbiakban elemzi az egészségügyi adatok kezelésének a beteg hozzájárulásán kívüli másik két jogalapját is: az egészségügyi szakemberek általi és a fontos közérdekből történő feldolgozást.

Az EHR működésének egyik legfontosabb garanciája a beteg önrendelkezésének tiszteletben tartása. A fokozott kockázatot rejtő adatok (pl. pszichiátriai vagy abortusszal kapcsolatos adatok) kezelését a beteg előzetes hozzájárulásához kellene kötnie („opt-in"), egyéb esetekben pedig biztosítani kell a kimaradás lehetőségét („opt-out"). Fontos lenne, hogy a beteg megtilthassa a kezelése során rögzített adatainak közlését más egészségügyi szakemberekkel. Foglalkozni kell továbbá az EHR-rendszerből történő teljes kivonulás lehetőségével is. Elengedhetetlen a betegek és szakemberek megbízható azonosítása és hitelesítése, a jelszavas hitelesítés helyett a munkacsoport az elektronikus aláírást ajánlja.

Differenciálni kell a hozzáférési jogokat és kategóriákat, a betegek számára pedig biztosítani kell a jogot, hogy megtagadhassák a hozzáférést az EHR-ben szereplő adataikhoz. Meg kell fontolni a „zárt boríték" alkalmazásának lehetőségét, azaz az aktán belül bizonyos adatokat úgy kellene elkülöníteni, hogy azokhoz csak az érintett kifejezett hozzájárulása esetén lehetne hozzáférni (kinyitni a borítékot).

Az EHR-rendszerek egyéb célú felhasználását meg kell tiltani, eszerint a kezelésen és egészségügyi igazgatáson kívüli célból nem lehet felhasználni a betegek adatait. Tehát például magán biztosító társaságok megbízásából vagy egy peres ügyben szakértői minőségben az orvosok ne férhessenek hozzá az EHR-rendszerhez.

A munkacsoport további garanciákként sorolja fel, hogy csak releváns információkat tartalmazzon az EHR-rendszer és csak a szükséges ideig; továbbá az adatbiztonság követelményét (pl. az adatvédelem biztonságát javító technológiák – PET – alkalmazása, hozzáférések naplózása); a rendszer átláthatóságának biztosítását (pl. a betegek tájékoztatása ingyenes,

könnyen használható elérési pontok felállításával, ahonnan a betegek ellenőrizhetik aktájukat).

Végül ki kell alakítani az ellenőrzés eljárásait, valamint garantálni kell a betegek kártérítéshez való jogát adataik helytelen vagy jogosulatlan felhasználása esetére. A tagállamoknak tisztázniuk kell a felmerülő felelősségi kérdéseket például arra az esetre, ha a hozzáférés technikai okból hiúsul meg, vagy az egészségügyi szakember nem tanulmányozza megfelelő mélységben a beteg aktáját az EHR-ben.

Vélemények az utas-nyilvántartási adatok továbbításáról

2007-ben a munkacsoport három véleményében is foglalkozik az utas-nyilvántartási adatok (PNR adatok) továbbításának kérdésével. Februári véleményében még a 2006-os ideiglenes EU-USA PNR megállapodáshoz kapcsolódóan fogalmazta meg légitársaságoknak, utazási irodáknak címzett iránymutatásait az utasok tájékoztatását illetően. 2007 nyarán ez a megállapodás hatályát vesztette, így újabb megállapodás született az EU és az USA között, melyről az 5/2007 sz. véleményében fejti ki kritikáját a munkacsoport. Az év végére pedig elkészült az európai PNR rendszerről szóló javaslat. A javaslat elfogadása esetén a légifuvarozóknak a terrorizmus és szervezett bűnözés elleni harc céljából már nem csak az USA Belbiztonsági Minisztériuma számára kellene továbbítani az utasok PNR adatait (USA-ba, az USA-ból vagy azon keresztül utazók adatait), hanem az európai hatóságok számára is (az Európai Unióba és az onnan repülő légi utasok PNR adatait). A munkacsoport 11/2007 sz. véleményében elemzi az Európai Bizottság EU PNR rendszerre vonatkozó javaslatát.

2/2007 sz. vélemény az utasok tájékoztatásáról - PNR-adataik továbbításáról az Amerikai Egyesült Államok hatóságai felé (WP 132):

Az Amerikai Egyesült Államok és az Európai Unió 2006-ban kötött megállapodása alapján a légitársaságok kötelesek az USA Belbiztonsági Minisztériuma (DHS) számára elektronikus hozzáférést biztosítani az USA-ba, az USA-ból vagy azon keresztül utazók utasnyilvántartási (PNR) adataihoz. Az Európai Unió adatvédelmi irányelve és a nemzeti adatvédelmi törvények is előírják az adatkezelőknek az érintettek tájékoztatásának kötelezettségét. Azonban a munkacsoport úgy véli, hogy a légitársaságok,

utazási irodák és számítógépes helyfoglalási rendszerek nem teljesítik kielégítő módon e kötelezettségüket. A megfelelő tájékoztatási gyakorlat előmozdítása érdekében a vélemény részletes útmutatást ad arról, hogy kinek, mikor, hogyan és milyen tartalmú tájékoztatást kell nyújtania a transzatlanti utasok részére. A munkacsoport két modell tájékoztatót is mellékelt véleményéhez.

Az érintetteket elsősorban annak a légitársaságnak kell tájékoztatnia, amely a repülőjegyet eladja. Ha a jegyet egy utazási irodán keresztül vásárolják, akkor annak kell az utasokat tájékoztatni adataik továbbításáról. Számítógépes helyfoglalási rendszereken keresztül történő vásárlás esetén e rendszerek kötelesek tájékoztatást nyújtani. Mindhárom esetben még a jegyvásárlás előtt eleget kell tenni a tájékoztatási kötelezettségnek. A jegy átadásakor meg kell ismételni a tájékoztatást, mivel nem biztos, hogy az utas vette saját magának a jegyet.

Utazási irodában történő jegyvásárláskor legalább a rövid tájékoztatót át kell adni az utas részére. Ha további információt kér, akkor a hosszabb tájékoztatót is a rendelkezésére kell bocsátani. Telefonos vásárlás esetén fel kell olvasni a rövid tájékoztatót az utas részére és kérésére meg kell adni a hosszabb tájékoztató elérését. Ha interneten történik a vásárlás, akkor a rövid tájékoztatónak automatikusan kell megjelennie, például felugró ablak formában. A rövid tájékoztatónak fel kell ajánlania a hosszú tájékozatóhoz tartozó linket.

5/2007 vélemény az Európai Unió és az Amerikai Egyesült Államok között az utas-nyilvántartási adatállomány (PNR) adatainak a légi fuvarozók általi feldolgozásáról és az Egyesült Államok Belbiztonsági Minisztériuma részére történő továbbításáról létrejött újabb megállapodásról (WP 138):

2007 júliusában az Európai Unió újabb megállapodást kötött az Amerikai Egyesült Államokkal a PNR adatok DHS részére történő továbbításáról. Az ideiglenest felváltó új megállapodás több részből áll: a megállapodás, a DHS garanciákat tartalmazó levele és az EU azon válasza alkotják, amelyben a PNR-adatok védelmének szintjét megfelelőnek minősíti az Egyesült Államokban.

A munkacsoport elismeri, hogy a megállapodás megakadályozta a jogbizonytalanság kialakulását, azonban véleménye szerint a megállapodás

adatvédelmi szintje elégtelen, sőt, még a korábbi megállapodás gyengének minősített adatvédelmi szintjét sem éri el. Sajnálatos továbbá, hogy az EU nem konzultált egyetlen adatvédelmi szervvel sem, mielőtt megfelelőnek ítélte a megállapodásban foglalt adatvédelmi biztosítékokat.

Az adattovábbítás céljai megegyeznek az előző megállapodásban foglalt, túl általánosan fogalmazott célokkal: 1) a terrorizmus és a hozzákapcsolódó bűncselekmények; 2) egyéb súlyos bűncselekmények, beleértve a transznacionális jelleget öltő szervezett bűnözést; 3) a fent említett bűncselekmények okán kiadott elfogatóparancs elől vagy őrizetből történő szökés. Az előző megállapodásban is említett felhasználási lehetőségeket, melyek alapján a PNR adatokat bármely büntetőeljárásban, vagy egyéb, az USA törvényei által előírt esetben felhasználhatták, az új megállapodás már az adattovábbítás céljai között sorolja fel.

A PNR-adatok átvételére jogosult DHS egységeket nem jelöli meg pontosan az új megállapodás. Ezek az egységek továbbadhatják az adatokat a DHS-en belüli „harmadik hivataloknak", az USA egyéb hatóságainak és külföldi kormányhatóságoknak is. Újbóli továbbításra csak esetenkénti mérlegelés alapján volt mód, az új megállapodásban sajnos már nem szerepel ez a nehezítő feltétel.

A látszat ellenére nőtt a továbbítandó adatelemek száma. Ugyan az új megállapodás csak 19 adatcsoportot nevez meg a korábbi 34 adatelemmel szemben, de a csoportok az eredeti lista 33 elemén kívüli újabb elemeket is tartalmaznak. A DHS nemcsak a listán szereplő adatokat, hanem különleges esetekben olyan adatokat is felhasználhat, amelyek a légitársaságok foglalási rendszerében szerepelnek, a listán azonban nem.

Az adattovábbítás nemcsak az utasokat, hanem más személyeket is érint (munkáltató, családtagok).

Különleges adatok nem szerepelnek a továbbítandó adatok listáján, ennek ellenére a DHS bizonyos körülmények között felhasználhat különleges adatokat is. Az új megállapodás szerint a DHS szűrné ki őket, de a munkacsoport szerint ezt a légitársaságoknak kellene elvégezni, méghozzá az adattovábbítás előtt.

Kifogásolható, hogy a légitársaságok véleményét a DHS nem hallgatja meg, az adatátadó rendszerek műszaki követelményeit egyedül a DHS határozza meg.

Az átadási rendszerre való áttérés 2004 óta halasztódik. Az új megállapodás 2008. január 1-jét jelölte meg határidőként.

Az adatok megőrzésének idejét a már eredetileg is aránytalanul hosszú három és fél évről tizenöt évre hosszabbította meg a DHS. Hét évig tárolják az adatokat egy aktív adatbázisban, majd további nyolc évig nyugvó, használaton kívüli státuszban. A két hozzáférési időszak között azonban adatvédelmi szempontból nincs különbség.

11/2005 sz. vélemény a PNR adatok bűnüldözési célra történő felhasználásáról szóló tanácsi kerethatározat-tervezetről (WP 145):

A javaslat az Európai Unióba és onnan repülő légi utasok jelentős mennyiségű személyes adatainak gyűjtését kívánja megvalósítani. A javaslat újabb mérföldkő egy európai megfigyelt társadalom felé a terrorizmus és szervezett bűnözés elleni harc jegyében. Nem csak a gyanú alatt állók, hanem minden ártatlan utas utazási szokásainak rekonstrukcióját tenné lehetővé évekre visszamenőleg. A munkacsoport főbb kritikái a következők: a PNR adatok gyűjtésének hatékonyságát és szükségességét még senki sem támasztotta alá; a PNR adatoknál szűkebb körű előzetes utasinformációs adatokon (API adatok) túli adatgyűjtés elengedhetetlenségét nem igazolja a tervezet; a különleges adatokat az adatkezelőnek, tehát a légifuvarozóknak kellene kiszűrni a bűnüldöző szerveknek való továbbítás előtt; minden légifuvarozónak az átadási (push) eljárást kellene alkalmazni; az adatok megőrzésének ideje aránytalanul hosszú; a javaslat adatvédelmi szabályozása elégtelen, az érintettek jogait és az adatkezelők kötelezettségeit nem fekteti le.

1/2007. sz. ajánlás a Kötelező Erejű Vállalati Szabályok jóváhagyására irányuló egységes jelentkezési lapról (WP 133):

A 95/46/EK adatvédelmi irányelv szerint az EU tagállamaiból csak akkor lehet személyes adatot harmadik országba továbbítani, ha a harmadik országban biztosított az adatok megfelelő szintű védelme vagy az adatkezelő megfelelő adatvédelmi garanciákat teremt. A Kötelező Erejű Vállalati Szabályok (Binding Corporate Rules, a továbbiakban: BCR) alkalmazása az utóbbi feltételt szolgálja, azaz egy vállalatcsoport demonstrálhatja velük, hogy a csoporton belüli adattovábbítások tekintetében megteremtette a megfelelő adatvédelmi garanciákat.

Az ajánlásban a munkacsoport egy olyan minta-jelentkezési lapot tesz közzé, amelyet a vállalatok az adatvédelmi hatóságokhoz nyújthatnak majd be BCR-jük jóváhagyása céljából.

A jelentkezési lap első része a jelentkező vállalatcsoportról gyűjt szervezeti jellegű információkat, a második rész „háttéranyag" címmel szisztematikusan megvizsgálja, hogy a jelentkezést benyújtó vállalatcsoportnál teljesülnek-e a BCR-ekkel szemben korábban megfogalmazott követelmények (van-e kötelező ereje a BCR-nek a vállalatcsoporton belül és az érintettek felé, kit terhel a bizonyítási teher, a gyakorlatban hogyan érvényesülnek a BCR szabályok, van-e elfogadott audit program stb.). A kérdések következő csoportja az adatkezelésről és az adatok útjáról gyűjt információt. Végül az adatvédelmi garanciákról kell számot adnia a vállalatnak.

3/2007. sz. vélemény a diplomáciai és konzuli képviseletek számára kibocsátott, a vízumokra vonatkozó Közös Konzuli Utasításnak a biometrikus adatok bevezetésével, valamint a vízumkérelmek fogadása és feldolgozása megszervezésének rendelkezéseivel kapcsolatos módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (COM(2006)269 végleges) (WP 134):

A Közös Konzuli Utasítás (KKU) azokat a minimumszabályokat határozza meg, amelyeket a tagállamok konzuli képviseleteinek be kell tartani a vízumok kibocsátása során. A KKU módosításának célja, hogy a vízumkérelmezők biometrikus adatainak kötelező gyűjtéséhez jogalapot teremtsen. A begyűjtött biometrikus adatokat a Vízuminformációs Rendszerben (VIS) tárolnák az EU tagállamai. A VIS-ről és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendelet (a továbbiakban VIS-rendelet) azonban még nem került elfogadásra.

A munkacsoport már két véleményében is kifejtette álláspontját, de most ismét kétségét fejezi ki egy átfogó EU-adatbázis szükségességét illetően. Mivel a közös vízumpolitika a közösségi jog hatálya alá tartozik, a VIS-nek meg kell felelnie a 95/46/EK adatvédelmi irányelvnek, az abban lefektetett szükségesség és arányosság alapelveinek is. Így felmerül a kérdés, hogy az arányosság elvét nem sérti-e a több millió biometrikus azonosító begyűjtése. Felül kellene vizsgálni azt a javaslatot is, amely szerint a nemzetbiztonsági hatóságok hozzáférhetnének a VIS-hez.

A VIS-rendeletben – és nem a KKU módosításáról szóló rendeletben – kellene lefektetni az adatminőségre, az intézkedések arányosságára, és az adatvédelmi biztosítékokra vonatkozó rendelkezéseket, valamint a központi VIS-ben tárolt adatok kategóriáit, az ujjlenyomatvételre kötelezett, illetve az alól mentesülő személyek kategóriáit, az adat megőrzésre, valamint az ujjlenyomatot adni nem képes személyekre vonatkozó rendelkezéseket.

Nem fogadható el, hogy csak a hat év alatti gyerekek mentesülnek az ujjlenyomat-adási kötelezettség alól, és hogy az idős személyekre nem vonatkozik a kivétel; az Eurodac adatbázishoz hasonlóan csak a 14 és 80 év közötti személyeket kellene kötelezni ujjlenyomat szolgáltatására.

Mivel a lakosság 5 százalékát nem lehet nyilvántartásba venni, mert nincs olvasható ujjlenyomata, vagy fogyatékossága miatt nem tud ujjlenyomatot adni, ezért kiegészítő eljárások segítségével biztosítani kell, hogy ilyen esetekben az ujjlenyomat hiánya miatt ne utasítsák el a vízumkérelmet.

A munkacsoport kifejezetten ellenzi a biometriai azonosítók gyűjtésének kiszervezését külső szolgáltatókhoz; ha nincs mód ennek elkerülésére, akkor biztosítani kell a feldolgozás szigorú felügyeletét, és hogy a felelősség a tagállam illetékes vízumhatóságainál maradjon.

4/2007 sz. vélemény a személyes adat fogalmáról (WP 136):

A munkacsoport a dokumentumot az eddig elfogadott egyik legjelentősebb véleményének tartja, ezért külön is felhívjuk a figyelmet arra, hogy honlapunkon az állásfoglalás szövege magyarul és angolul teljes terjedelemben szerepel.

A vélemény célja a tagállamok körében egy egységes személyes adat fogalom kialakítása, azaz példákkal illusztrálva iránymutatás az egységes jogalkalmazáshoz. Az elemzés a személyes adat fogalmának négy építőkövén alapul: ”azonosított vagy azonosítható”, „természetes személyre”, „vonatkozó”, „bármely információ”. Ezen elemek szorosan összefonódnak és együttesen határozzák meg, hogy az információ személyes adat-e.

1. Első elem: „bármely információ”

Az információ jellegére tekintettel az anyag megjegyzi, hogy bármilyen állítás egy személyről lehet személyes adat. Nem számít, hogy az állítás objektív vagy szubjektív. A szubjektív állítások leggyakrabban a banki

szférában, biztosítóknál vagy a munkaviszonnyal kapcsolatban fordulnak elő (példák: „Titus megbízható adós", „Nem várható Titus közeli elhalálozása", „Titus jó munkaerő és előléptetést érdemel"). Ahhoz, hogy az állítás kimerítse a személyes adat fogalmát, az sem szükséges, hogy az információ igaz vagy bizonyított legyen.

Az információ tartalma bármi lehet: nem csak a magánéletre, családi életre, hanem bármilyen munkakörülménnyel, gazdasági vagy társas viselkedéssel kapcsolatos tevékenységre vonatkozó adat. Személyes adat közlésének számít, ha a gyógyszergyárakkal valaki közli azonosított vagy azonosítható orvosok gyógyszerfelírási szokásait. A személyes adat fogalma lefed bármilyen formátumú és bármilyen adathordozón tárolt információt. Például:

- telebank szolgáltatás igénybevételénél felvétel készül az ügyfél hangjáról, miközben utasításokat ad a banknak,
- a térfigyelő kamerával készített felvételek is személyes adatnak minősülnek, ha az egyének felismerhetők a felvételen.

A munkacsoport itt fontosnak tartotta megjegyezni, hogy az emberi szövetminták (vérminta stb.) csak a biometrikus adatok forrásai, nem maguk a biometrikus adatok (példa: az ujjlenyomat biometrikus adat, de az ujj maga nem számít biometrikus adatnak).

2. Második elem: „vonatkozó"

Általában az egyénről szóló információ az egyénre „vonatkozónak" tekinthető. Azonban számos olyan helyzetet is lehet említeni, amikor ez nem dönthető el egyértelműen, mert mondjuk az adatok által közvetített információ elsősorban tárgyakra vonatkozik és nem egyénekre.

Példa: egy meghatározott ház értéke tárgyról szóló információ – ha kizárólag arra használjuk, hogy szemléltessük a kerületben az ingatlan árakat, ha viszont az ingatlantulajdonos adófizetési kötelezettségének megállapítására használják, akkor már személyes adatnak tekinthető.

Csak akkor „vonatkozik" az adat egy egyénre, ha egy „tartalom" elem, vagy egy „cél" elem, vagy egy „eredmény" elem jelen van. Ahhoz, hogy az információról azt mondhassuk, hogy az adott személyre „vonatkozik", a három elem közül elég, ha az egyik jelen van (a három elem vagylagos, azaz

nem együttesen kell jelen lenniük). Tehát, ha a „tartalom" elem jelen van, akkor nem szükséges a „cél" vagy az „eredmény" elemek jelenléte.

A „tartalom" elem jelen van azokban az esetekben, ha az információ egy meghatározott személyről szól, függetlenül az adatkezelő vagy harmadik személyek céljától és attól is, hogy az információ az érintettre hatással van-e. Példa: az orvosi vizsgálat eredményei egyértelműen a betegről szólnak, azaz rá vonatkoznak.

A „cél" elem is felelős lehet azért a tényért, hogy az információ egy adott személyre „vonatkozzék". E „cél" elemet meglévőnek lehet tekinteni, amikor az adatot az esetet övező valamennyi körülményt figyelembe véve abból a célból használják fel vagy használják fel valószínűleg, hogy az egyén státuszát vagy viselkedését értékeljék, bizonyos bánásmódban részesítsék vagy befolyásolják.

A harmadik típusú „vonatkozás" az „eredmény" elem jelenléte esetén áll elő. Azok az adatok, amelyek felhasználása valószínűleg hatást fog gyakorolni egy meghatározott személy jogaira és érdekeire még akkor is személyes adatnak minősülnek, ha a „tartalmi" elem vagy a „cél" elem hiányzik. Nem szükséges, hogy a lehetséges eredmény jelentős hatás legyen. Elegendő, ha az egyént az adatfeldolgozás következtében eltérően kezelik másoktól.

3. Harmadik elem: „azonosított vagy azonosítható" (természetes személy)

Egy természetes személy akkor tekinthető azonosítottnak, amikor egy csoporton belül elkülönül a csoport többi tagjától. Akkor „azonosítható" valaki, ha ugyan még nem történt meg az azonosítás, de az lehetséges.

- „Közvetlenül" vagy „közvetve" azonosítható:

Egy személy neve a leggyakoribb közvetlen azonosítást lehetővé tevő azonosító. Ahol az azonosítás nem lehetséges a rendelkezésre álló azonosítók alapján, ott még fennállhat a közvetett módon – tipikusan a rendelkezésre álló azonosítók és más információ „egyedi kombinációi" útján – történő azonosítás lehetősége. Példa: egy korábbi, nagy érdeklődés által kísért bűnügyről újabb információt közöl a sajtó nevek vagy születési évek nélkül. Nem tűnik különösen bonyolultnak, hogy valaki további információhoz jusson hozzá a bűnügyben érintett személyek azonosítása céljából.

Nem kizárt, hogy valaki előkeresi az ügyről szóló korábbi újságcikkeket, amelyekben szerepelnek a bűnügyben érintettek nevei is. Tehát megalapozottnak tűnik, hogy az újabb újságcikkben (név nélkül) szereplő adatokat „azonosítható személyekre vonatkozó információnak" minősítsük, így személyes adatnak tekintsük őket.

A név nem mindig szükséges egy személy azonosításához. Példa: a webforgalmat figyelő eszközök lehetővé teszik, hogy meghatározzák egy számítógép viselkedését, a gép mögött pedig a felhasználóét. A felhasználó személyiségét össze lehet rakni a részletekből: nevének, címének ismerete nélkül besorolható társadalmi-gazdasági, pszichológiai, filozófiai és egyéb kategóriákba. Az egyén azonosításának lehetősége többé már nem feltétlenül jelenti neve megállapításának képességét.

- Az azonosítás eszközei:

Az adatvédelmi irányelv is különös figyelmet szentel az „azonosíthatóság" fogalmának, amikor úgy fogalmaz, hogy *„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"*. Ez azt jelenti, hogy egy pusztán hipotetikus lehetőség nem elegendő ahhoz, hogy valakit azonosíthatónak tekintsük: ha minden olyan módszert figyelembe vettünk, amit az adatkezelő vagy más személy valószínűleg felhasználna, és az azonosítás nem lehetséges, vagy a lehetőség elhanyagolható, akkor az adott személyt nem tekinthetjük azonosíthatónak. Az azonosítás lehetőségének megállapításánál figyelembe kell venni az azonosítás költségét, az adatkezelő által várt előnyt, az egyének érdekeit, a szervezési működési zavar kockázatát (lásd titoktartási kötelezettségek megszegése), a lehetséges technikai hibákat, a technikának nem csak a jelenlegi állását, hanem a várható, az információ feldolgozásának ideje alatt történő fejlődését is (ha mondjuk 10 évre tervezik az adatok megőrzését, akkor az adatkezelőnek számítania kell arra, hogy a kilencedik évben lehetővé válik az azonosítás, ezáltal személyes adattá minősítve az információt). Példa: gyógyszerkísérleti adatok esetében, ha kórházak vagy orvosok betegeik egészségügyi adatait továbbítják egy cég számára gyógyszerkísérletekhez, a betegek neveit azonban nem, csak a véletlenszerűen hozzájuk rendelt sorozatszámokat; és az adatok semmiféle többlet információt nem tartalmaznak, amelyek kombinációjával az azonosítás lehetővé

válna; valamint a betegek neve az orvos kizárólagos birtokában maradnak és minden olyan jogi, technikai és szervezési intézkedést megtettek, ami megakadályozza a betegek azonosítását vagy azonosíthatóvá válását, akkor az adatvédelmi hatóságok ezt úgy tekinthetik, hogy a gyógyszer cégnek nem áll rendelkezésére olyan módszer, amit valószínűleg felhasználna az érintettek azonosítására.

Amikor az információ kezelésének célja kifejezetten az egyének azonosítása, akkor feltételezhető, hogy az adatkezelőnek megvannak, vagy meglesznek azok a módszerei, amelyeket „valószínűleg felhasznál majd az érintett azonosítására". Az előbbiekben leírtak különösen relevánsak a kamerával történő megfigyelés esetén: az adatkezelők gyakran érvelnek úgy, hogy csak kis százalékban történik meg a rögzített személyek azonosítása és ezért a néhány azonosítástól eltekintve nem történik adatkezelés. Azonban a kamerás megfigyelés célja minden esetben az, hogy ha az adatkezelő szükségesnek tartja, akkor azonosíthassa a videofelvételeken látható személyeket. Ezért a teljes alkalmazást adatkezelésnek kell tekinteni, még akkor is, ha a gyakorlatban néhány felvett személy nem azonosítható.

- Pszeudonimizált adatok:

A pszeudonimizálás a személyazonosság elrejtését jelenti. Pszeudonimizált adatokat elsősorban kutatáshoz és statisztikákhoz használnak. A pszeudonimizálás lehet visszafelé követhető (ilyenkor azok a személyek, akikre vonatkozik az információ közvetve azonosíthatónak tekinthetők), de el lehet úgy is végezni, hogy az újbóli azonosítás ne legyen lehetséges.

- Kódolt adatok:

A kódolás a pszeudonimizálás klasszikus esete (lásd nem összesített adatok statisztikai célokra). A kódolt adatok használata általános a gyógyszerkísérletek klinikai fázisában. A betegekhez, vizsgálati eredményeikhez az az egészségügyi szakember/kutató rendeli a kódot, aki teszteli a gyógyszereket a betegeken. A gyógyszercég csak kódolt formában kapja az eredményeket a kutatótól, mivel számára a bio-statisztikai eredmények a relevánsak. A kutató külön tárolja a kódhoz tartozó kulcsot, ami a kóddal jelölt beteg azonosítására szolgál. A kutató köteles megőrizni a kulcsot, mivel előfordulhatnak olyan esetek, amikor szükség lehet a betegek azonosítására, mivel kiderül, hogy a tesztelt gyógyszer veszélyes. Ilyen esetekben a

betegek azonosítása nem csak megtörténhet, hanem meg kell történnie bizonyos körülmények fennállása esetén, ezért az azonosítást beépítették az adatkezelés céljai és eszközei közé, tehát ebben az esetben a kódolt adatok személyes adatnak minősülnek. Ha viszont a kutatás más területein vagy ugyanazon projekt más területein az újra azonosítás lehetősége nincs beépítve a protokollokba, akkor a kódolt adat kezelésére nem vonatkozik az adatvédelmi irányelv.

- Anonim adatok:

Anonim adatnak minősül minden olyan információ, amely olyan személyre vonatkozik, aki nem azonosítható az adatkezelő vagy bárki más által minden olyan módszer figyelembevételével, amit az adatkezelő vagy más valószínűleg felhasználna az említett személy azonosítására. Az, hogy valaki azonosítható-e az adatok alapján a körülményektől függ, tehát minden esetre külön-külön kell elemeznünk, hogy valószínű-e az azonosítás. Ez különösen fontos olyan statisztikai információ esetén, amikor annak ellenére, hogy az információ összesített adatként szerepel, mégis lehetséges az azonosítás, mivel a kiindulási minta nem elég nagy. Statisztikai felméréseknél a töredék információk kombinációja valósulhat csak meg, mert a statisztikusok számára általános kötelezettség, hogy csak anonim adatokat közölhetnek összesített adatok formájában. Ha úgy tűnik, hogy egy elemzési szempont azonosításhoz vezethet az egyének egy csoportján belül, akkor akármilyen nagy is az a csoport (mondjuk csak egy orvos van egy 6000 fős városban), a szempontot törölni kell a felmérés szempontjai közül.

4. Negyedik elem: „természetes személy"

Az irányelv által biztosított védelem természetes személyekre, azaz élő emberekre vonatkozik. Mivel a polgári jog szerint a halottak már nem számítanak természetes személynek, így a rájuk vonatkozó információ sem tekinthető személyes adatnak. A vélemény azonban felsorol néhány esetet, amikor a holtak adatai közvetve védelemben részesülnek. Azonban a tagállamok dönthetnek úgy is, hogy nemzeti adatvédelmi jogszabályuk hatálya a halottakra is kiterjedjen. A meg nem született gyermekek adatainak védelme attól függ, hogy az adott tagállam jogszabályai milyen álláspontot képviselnek a meg nem született gyermekek jogi védelmével kapcso-

latban általában. A jogi személyekre viszont nem terjed ki az adatvédelmi irányelv által biztosított védelem.

Végül a IV. pontban a vélemény azt a helyzetet elemzi röviden, amikor az adat (valószínűleg) kívül esik a személyes adat definícióján (elhunyt személy adatai, meg sem született magzat adatai stb.).

1/2007 sz. beszámoló az első közös végrehajtási intézkedésről: értékelés és következő lépések (WP 137):

Az Európai Bizottság 2003-ban felhívta a munkacsoportot, hogy fontolja meg szektorális vizsgálatok indítását uniós szinten, az első ilyen jellegű vizsgálat 2006-ban a magán egészségbiztosítási szektort érintette. Egy standard kérdőívet kellett a nemzeti hatóságok által kiválasztott biztosító társaságoknak kitölteni, mely alapján 2007-ben sor került a tagállamonkénti, összehasonlító értékelésre.

A biztosítók minden tagállamban feldolgoznak személyes információt és egészségügyi adatot, a legtöbb tagállamban pénzügyi adatokat, biztosítás történeti adatokat, és a családtagokra vonatkozó információt is, hat tagállam biztosítótársaságai pedig genetikai adatokat is kezelnek. Az adatfeldolgozás leggyakoribb célja szinte minden tagállamban a szerződések intézése és a kockázatértékelés, de néhányukban előfordul a direkt marketing és statisztikai célú feldolgozás is. Az adatgyűjtés és feldolgozás leggyakoribb jogalapja a hozzájárulás, azonban nem tisztázott, hogy az mindig önkéntes és megfelelő tájékoztatáson alapul-e, valamint kétséges az érintettek megfelelő tájékoztatása is.

8/2007 sz. és 9/2007 sz. vélemények a személyes adatok védelmének szintjéről a Feröer-szigeteken és Jersey-ben (WP 141 és WP 142):

Feröer-szigetek és Jersey harmadik országoknak számítanak, mivel nem tagjai az Európai Gazdasági Térségnek. A munkacsoport a Feröer-szigetek és Jersey adatvédelmi szintjének megállapításához a következő alapelvek jelenlétét vizsgálta a két ország adatvédelmi törvényeiben:

- célhozkötöttség,
- adatminőség és arányosság,
- átláthatóság,
- adatbiztonság,

- az adatokhoz való hozzáférés joga, helyesbítés joga, tiltakozás joga,
- újbóli adattovábbítás korlátozása,
- különleges adatokkal, direkt marketinggel és automatizált döntésekkel kapcsolatos további alapelvek megléte.

Vizsgálta továbbá azt is, hogy a következő eljárási/végrehajtási mechanizmusokat alkalmazzák-e a két országban:

- a jogkövetés kielégítő szintjének biztosítása,
- az érintettek támogatása,
- megfelelő jogorvoslat a kárt szenvedett feleknek.

A munkacsoport arra a következtetésre jutott, hogy mindkét ország adatvédelmi törvénye tiszteletben tartja a fent említett alapelveket és érvényesülnek a szükséges eljárási/végrehajtási mechanizmusok. Hiányosságokat csak Jersey esetében fogalmaz meg: a személyes adat fogalmának szűkebb meghatározása, az átláthatóság és az adatvédelmi biztos szűkebb hatáskörét kifogásolja. Azonban mindkét véleményében hangsúlyozza a munkacsoport, hogy a megfelelő adatvédelmi szint eléréséhez a harmadik országoknak nem kell az irányelv által lefektetett minden követelménynek megfelelni.

További, a 29-es Munkacsoport tevékenységével összefüggő témák:

- Biometrikus azonosítással ellátott úti okmányok

A 29-es Adatvédelmi Munkacsoport által készített, az előbbiekben már említett felmérés kapcsán informálódtunk a biometrikus azonosítók jelenlegi hazai alkalmazásról, melynek során a következőket állapítottuk meg:

A magyar útlevél-kiadási gyakorlat alapja a külföldre utazásról szóló 1998. évi XII. törvény, melyet – a biometrikus azonosítókra tekintettel – módosított a 2006. évi XXI. törvény (végrehajtási kormányrendeletek: 101/1998. (V.22.) Korm. rendelet és 197/2006. (IX.27.) Korm. rendelet). Magyarországon 2006. szeptember 1-től biometrikus azonosítót (fényképet) tartalmazó útlevelet ad ki a hatóság. Az új útlevél adattárolásra alkalmas elektronikus eszközt – chipet – tartalmaz, mely lehetővé teszi az útlevél

adatoldalának elektronikus formában történő rögzítését. Az okmányirodákban készülnek el az igénylőkről a digitális fényképek, az útlevél adatlapjára pedig lézergravírozással felkerülnek az adatok (személyazonosító adatok, kérelmező aláírása és fényképe), ezzel ezek láthatóvá válnak. Az adatlap adattartalma digitalizálás után az útlevél adattárolásra alkalmas elektronikus eszközébe is rögzítésre kerül. Mivel ez az adatsor nem tartalmaz új információt, ezért az elektronikus eszköz adattartalmát külön nem tárolják, azaz erről a gyártás után a kiállító hatóságnak és más hivatalnak sincs információja.

Az üres tároló eszközbe tehát az útlevél előállítás során történik az adatok beírása. Ekkor a tároló eszköz „nyitott" állapotban van. Minden kész útlevelet ellenőriznek, amikor az útlevél kitöltéséhez megadott, az útlevélbe nyomtatott, és az elektronikusan tárolt adatokat összevetik. Amennyiben hibátlan a kitöltés, és ez megegyezik a tárolt adatokkal, akkor a „nyitott" tárolóeszköz lezárásra kerül. Ezután a tárolt adatokat már többet nem lehet megváltoztatni. Amennyiben ezt mégis megkísérlik, a tárolóeszköz megsemmisíti a tárolt adatokat, és többé nem lehet használni az eszközt.

A kiadott útlevelek adattartalmát az arra feljogosított szervezetek (elsősorban határőrizeti szervek) ellenőrizhetik. Ez az ellenőrzés csak az útlevélben tárolt adatok alapján lehetséges, mivel ezek az adatok ebben a formában máshol nincsenek eltárolva. Amennyiben az útlevél tulajdonosa meg kíván győződni az útlevelében elektronikusan tárolt adatok helyességéről, úgy ezt kérésére az okmányirodában nézheti meg, mivel itt áll rendelkezésre az elektronikusan tárolt adatok kiolvasására alkalmas eszköz. Amennyiben a kérésre történt adatellenőrzés során hibát fedez fel az útlevél tulajdonosa, akkor illetékmentesen és soron kívül új, a helyes adatokat tartalmazó útlevelet állít ki részére a hatóság.

Magyarország, a Tanács 2004. december 13-i 2252/2004/EK rendelete és a Bizottság 2006. június 28-i 2909. határozata alapján 2009. július 1-vel tervezi az útlevél biometrikus azonosítói közé felvenni az ujjnyomatokat. Ebben az esetben az ujjnyomatok (egy, vagy két ujj) képe nem kerül tárolásra, csak azok kódját rögzítik az okmányirodában. A kódot az okmányt kitöltő hatóság részére továbbítják, mely az útlevél elektronikus adattároló eszközében azt rögzíti. Egyéb helyen a továbbiakban már nem tárolják ezt az adatot.

- A személyes adatok Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi feldolgozása

Az előző évi beszámolóban szerepel, hogy a személyes adatok Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi feldolgozásával kapcsolatos európai aggályokat 2006-ban kezdte vizsgálni az EDPS és a 29-es Munkacsoport. Akkor az Európai Unió független adatvédelmi felügyelő hatóságai a bankszektort érintő jelentős kérdéssel kapcsolatban közös véleményt fogalmaztak meg.

A SWIFT pénzügyi üzenetek feldolgozásával foglalkozó, belgiumi székhelyű szervezet, mely pénzügyi adatokat továbbít tömeges méretekben az USA hatóságaihoz. A SWIFTNet FIN nyilvántartási rendszere alapján az európai központtal párhuzamosan működik egy annak tökéletes tükörképét alkotó adatbázis az Egyesült Államokban is. 2001. szeptember 11-e után a terrorizmus elleni harc keretében arra utasították az amerikai hatóságok (Pénzügyminisztérium (UST) Külföldi Vagyontárgyakat Ellenőrző Osztálya (OFAC)) a SWIFT-et, hogy az európai nemzetközi tranzakciókat is tartalmazó amerikai adatbázist adják át nekik. Ezt a kérést a SWIFT kénytelen volt teljesíteni, a nemzetközi pénzátutalások kezelésére szolgáló SWIFT-hálózatban gyűjtött és feldolgozott személyes adatokat tehát 2001 vége óta továbbítják az UST-hez.

Az ilyen célú adattovábbítás (vagyis inkább adatmásolás, „tükrözés"), mely eltér az eredeti adatkezelési céltól, nincs összhangban az európai adatvédelmi szabályokkal, így a magyar szabályokkal sem. Megjegyzendő, hogy ugyanazon cég SWIFT Net File ACT újabban kifejlesztett szolgáltatása az adatvédelmi kritériumoknak már jobban megfelel.

A 29-es Adatvédelmi Munkacsoport és az egyes érintett (leginkább a belga) tagállamok hatóságainak tevékenysége, helyzetelemző vizsgálatai igen sikeresek voltak. A megfelelő adatvédelmi szint biztosítása terén jelentőséggel bír, hogy a SWIFT 2007 júliusában csatlakozott a Safe Harbour adatvédelmi egyezményhez.

Emellett a Bizottság és a Tanács Elnöksége, valamint a UST közös "jognyilatkozatot" tett, melyben az USA garanciát vállalt az EU-ból származó, a SWIFT által továbbított személyes adatok kezeléséért. A Bizottság a jognyilatkozatban szereplő elemekből felépülő jogi keretet elegendőnek találja az európai adatvédelmi jogok tiszteletben tartása és érvényesítése szempontjából.

A pénzügyi tranzakciók SWIFT szolgáltatásán keresztül történő adattovábbítások az érintettek hozzájárulásán alapulnak. A bankok minden olyan ügyfélnek kötelesek tájékoztatást nyújtani, aki a SWIFTNet Fin szolgáltatást használja nemzetközi pénzátutalás alkalmával, függetlenül attól, hogy a szolgáltatást online, telefonon vagy személyesen a bankban veszik-e igénybe.

Mindemellett a 29-es Adatvédelmi Munkacsoport egy hosszabb tájékoztató elkészítését is javasolja, amely részletes háttér információt tartalmaz a SWIFTNet Fin működéséről és az adattovábbítási műveletekről. A tájékoztatást meg kell adni minden egyes nemzetközi átutalás alkalmával, kivéve, ha az ügyfél már kapott tájékoztatást az adott tranzakcióval kapcsolatban (például amikor az ügyfél tartós megbízást ad a banknak ugyanazon átutalás többszöri megismétlésére). A tájékoztatás történhet azon a formanyomtatványon is, amelyen az ügyfelek a tranzakciót kérik, de történhet a bank honlapjának megfelelő pontján is. Annak érdekében, hogy az érintettek jogaikat megfelelően tudják gyakorolni, és a pénzügyi intézmények egységes gyakorlatot folytassanak a tájékoztatási kötelezettségük teljesítése terén, Közlemény született, illetve a Magyar Bankszövetséget kértük meg arra, hogy a tagjait informálja. Igen sajnálatos, hogy csak néhány bank vette a fáradságot, hogy az ügyfelei figyelmét felhívja a SWIFTNet Fin adattovábbításáról szóló tájékoztatóra.

Előrelépés azonban, hogy a SWIFT a közelmúltban lépéseket tett az átláthatóság, valamint a cég szerkezetének tervezett átalakítása érdekében. Ez alapján 2009-ig Svájcban kialakítanak egy új operációs központot is, ami azt jelenti, hogy az Európán belüli tranzakciókban szereplő személyes adatokat már nem az USA-ban található operációs központban fogják kezelni. Az EU-USA tranzakciókra ez nem vonatkozik, ezeket az adatokat továbbra is az USA-ban kezelik. Az egyéb nemzetközi, Európai Unión belüli és kívüli bankok közötti tranzakciók tárolási helye még nem eldöntött.

- Belső Piaci Információs Rendszer (Internal Market Information System – IMI)

A szakmai képesítések elismeréséről szóló 2005/36/EK irányelv és a belső piaci szolgáltatások szabad áramlásáról szóló 2006/123/EK irányelv az irányelvek hatékony végrehajtásának biztosítása érdekében a tagállamok

számára együttműködési kötelezettséget határoznak meg. Az együttműködés eszközeként egy internetes alapú szoftvert (IMI) kíván a Bizottság a tagállamok rendelkezésére bocsátani.

Tekintettel arra, hogy jelentős lesz a személyes adatokat érintő információcsere, a 29-es Munkacsoport Véleményt (7/2007) fogalmazott meg a Belső Piaci Információs Rendszerrel kapcsolatos adatvédelmi kérdésekről (WP 140).

Az IMI strukturált információáramlást biztosító szoftvere lehetővé teszi majd azt, hogy a tagállamok a belső piaci jogszabályok végrehajtásakor hatékonyabban tudnak napi szinten együttműködni. A szoftver a hatáskörrel és illetékességgel rendelkező hatóságok ügyintézőinek nevét és elérhetőségét is tartalmazza majd, és irányítószám szerinti kereséssel bármely tagállam ügyintézője megtalálja majd azt az illetékes ügyintézőt, aki az intézkedés során felmerült kérdésre válaszolni tud, illetve valamely adat, tény vagy jogviszony fennállásáról nyilatkozni tud. Az IMI a tagállamok illetékes hatóságai számára lehetővé teszi majd azt, hogy meghatározott közösségi jogszabályok végrehajtására vonatkozó strukturált kérdéscsoportok segítségével más tagállamok hatóságainak továbbíthassanak kéréseket. A tagállamok közötti hatékony információ-áramláshoz szükséges, hogy az architektúra bizonyos pontjain minden tagállamban álljon valaki. Ezek a pontok: a nemzeti IMI-koordinátor és a hatóságok ügyintézői.

Az IMI felépítését vizsgálva a 29-es Munkacsoport alapvetőnek találja, hogy a Bizottság által javasolt kérdések, menük olyan struktúrában jelenjenek meg, mely az irreleváns, aránytalan vagy harmadik felekhez kapcsolódó adatok gyűjtésének kockázatát minimalizálja. A bizottság és az illetékes hatóságok feladatait, felelősségét világosan meg kell határozni. A koordinátorok esetében ugyanezt várja el a Munkacsoport. Az adatmegőrzés idejét nemzeti szinten kell szabályozni azzal, hogy a Bizottság 6 hónapot irányzott elő erre. A jogi felhatalmazás tekintetében a nemzeti jogra nehezedik a felelősség.

Az IMI-t érintő adatvédelmi kérdésekről készített véleményében a Munkacsoport kifejezetten kérte, hogy bizottsági határozat állapítsa meg az IMI szereplőinek jogait és kötelezettségeit. Erről a Bizottság decemberben fogadott el határozatot.

Az Unió bel- és igazságügyi együttműködésének adatvédelmi kérdései

Ezen a területen a legfőbb döntéshozó szerv a Bel- és Igazságügyi Miniszterek Tanácsa (BIÜT). A BIÜT legfontosabb feladata a jogi aktusok jóváhagyása, valamint a közeljövő prioritásainak (téma, teendő) kijelölése. A BIÜT döntéseinek előkészítését egyrészt a Coreper (az EU-hoz akkreditált tagállami állandó képviselők bizottsága), másrészt a 36. cikk Bizottság (az elnevezés a létrehozó EK Szerződés-cikkre utal) végzi. A 36. cikk Bizottság (más néven CATS) a tagállamok egy vagy több magas rangú szakértőjéből áll, s a döntés-előkészítés mellett a büntetőügyekben folytatott rendőrségi-, és vámegyüttműködés koordinációja a feladata.

A CATS munkáját – egyebek mellett – az alábbi, szakértőkből álló munkacsoportok segítik:

- Europol Munkacsoport
- Szervezett Bűnözés Elleni Munkacsoport (Multidisciplinary Group on Organised Crime - MDG)
- Rendőrségi Együttműködés Munkacsoport (Police Cooperation Working Party - PCWP)
- Terrorizmus Elleni Munkacsoport (Working Party on Terrorism - TWG)

Az EU döntéshozatali mechanizmusában való magyar részvételről szóló hazai jogszabályok értelmében a fenti munkacsoportokban végzett munka koordinációjáért, a tárgyalási álláspont összeállításáért az Igazságügyi és Rendészeti Minisztérium (IRM) a felelős, amely az adatvédelmi biztost is felkérte az egyeztetésekben való részvételre. Sajnálatos módon a munkacsoporti anyagok véleményezésére az esetek többségében nagyon szűk – sokszor néhány órás – határidőt biztosítanak csak számunkra.

Europol Munkacsoport

Az Europol Munkacsoport egyetlen témája az Europol Egyezményt felváltó tanácsi határozat tervezete volt 2007-ben, mely magában foglalja az Egyezmény szövegét a három jegyzőkönyv módosításaival együtt, így például az Europol megbízatásának és feladatainak kibővítését a pénzmosással, a bűnmegelőzés területén történő segítségnyújtással, a

bűnügyi technikai és bűnügyi tudományos módszerekkel, a közös nyomozócsoportokban való részvétel lehetőségével és a tagállamok nyomozások lefolytatására vagy koordinálására való felkérésének lehetőségével, valamint az Európai Parlament jobb tájékoztatásával.

A tervezettel kapcsolatban észrevételeink többségét az IRM figyelembe vette a magyar tárgyalási álláspont elkészítésekor. Fenntartásaink vannak azonban a határozattervezet azon megfogalmazásával kapcsolatban, amely szerint az Europolhoz delegált tagállami összekötők a nemzeti jogszabályok alapján az Europol hatáskörén kívül eső bűncselekményekben is folytathatnak két- vagy többoldalú információcserét. A tagállami összekötők és az őket delegáló nemzeti egység közötti kommunikációt egy védett vonalon üzemelő levelező rendszer (InfoEx) biztosítja, amely az Europol tulajdonát képezi, az Europol informatikai felügyelete alatt működik, és az Europollal folytatott információcsere eszközéül szolgál. Más összeköttetés nem lévén a nemzeti egység és az összekötő között, az Europol hatáskörén kívül eső bűncselekményekben történő adatcserét is e rendszer segítségével lehet végrehajtani, ami felveti a céltól eltérő adatkezelés lehetőségét. Mivel az Europol elemzői szintén hozzáférnek az InfoEx rendszerhez, nem látjuk biztosítottnak azt sem, hogy az Europol kizárólag a hatáskörébe eső bűnügyi információkhoz juthasson hozzá. Tekintettel arra, hogy ezen aggályunk nem talált meghallgatásra, a tárgyalási álláspontba nem vették fel, a határozat magyar jogrendbe illesztése során külön figyelmet szentelünk a probléma rendezésének.

Ez év őszétől véglegesedni látszanak azon pontok, melyek az Europol informatikai rendszerének adatbázisairól (Europol Információs Rendszer, elemzési munkafájl, tárgymutató), új adatbázisok létrehozásának szabályairól, a kezelhető adatok köréről, az „adatgazdai" felelősségi körökről, az adatok tárolási/törlési határidejéről szólnak. Az e fejezetekhez fűzött szövegpontosító megjegyzéseinket azzal a céllal tettük meg, hogy a majdani határozat értelmezése (a különböző szövegváltozatok angol nyelvűek) és magyar jogrendbe ültetése könnyebb legyen, azokat azonban elhárították azzal, hogy a megfogalmazások utolsó átnézése során ezek a szempontok érvényesíthetők lesznek. A II. és III. fejezet szövegére hatással lehet az a harmadik pilléres adatvédelmi kerethatározat is, amely a bűnüldözési célú információcsere adatvédelmi alapelveit hivatott meghatározni, annak végleges tartalma és hatályba lépésének időpontja azonban egyelőre nem ismert.

Az uniós szervezetekkel és a harmadik országokkal/szervezetekkel folytatott együttműködés témájában – ezen belül a személyes és minősített adatok cseréjénél – szükségesnek tartjuk annak egyértelművé tételét, hogy az eljárási rendek között differenciálni kell. Az uniós szervezetek egy részére (például OLAF, Európai Központi Bank) érvényes a személyes adatok feldolgozása során az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv, illetve a 45/2001/EK rendelet, amely biztosítja a személyes adatok védelmének megfelelő szintjét. A harmadik országok és szervezetek esetében azonban egyrészt szükség van az adatvédelem megfelelő szintjének vizsgálatára azelőtt, hogy a konkrét adatcsere megindulna, másrészt célszerű megállapodást kötni az adatok átadás-átvételének, védelmének szabályairól. A szöveg véglegesítése valószínűleg megtörténik decemberben.

Várhatóan jövő év elején is folytatódik az V., azaz az adatvédelmi fejezet véleményezése. Üdvözlendőnek tartjuk, hogy a tanácsi határozatban helyet kapott az Europol adatvédelmi tisztviselő funkciója, bár a jelenlegi szövegváltozat szerint pontatlan a beosztás függetlenségét biztosító garanciák leírása.

Az V. fejezet tartalmazza az érintettek információs önrendelkezési joga gyakorlásának szabályait is. Más adatvédelmi fórumokon (például Rendőrségi Munkacsoport) kialakított álláspontunknak megfelelően javaslatot tettünk ezen eljárási rend egyszerűsítésére is. Jelenleg a bármely tagállamban beadható tájékoztatás-kérésre az Europol válaszol annak a tagállamnak a jogrendje szerint, amelyiknél a kérést benyújtották. Indokolatlannak tűnik azzal terhelni az Europolt, hogy 27 féle adatvédelmi jogszabályt úgy ismerjen, hogy problémamentesen teljesíthesse tájékoztatási kötelezettségét. Javaslatunk alapján a nemzeti jogszabályra utaló kifejezés törlésével kialakulna az Europolra vonatkozó egységes metódus, ami azonban nem jár az alkotmányos jogok sérelmével.

Szervezett Bűnözés Elleni Munkacsoport (Multidisciplinary Group on Organised Crime – MDG)

A Munkacsoport 2007-ben többek között foglalkozott:

- Az európai korrupcióellenes kapcsolattartói hálózat (EACN) + ENSZ korrupció elleni egyezménnyel (UNCAC),

- Fedett nyomozók alkalmazására vonatkozó tanácsi állásfoglalás előkészítésével és az úgynevezett
- Lőfegyver irányelv módosításával.

Ez utóbbiról bővebben is szólunk, mert az egyeztetések során vita alakult ki arról, hogy kötelező legyen-e egy központi, a fegyverek és tulajdonosaik adatait tartalmazó adatbázis létrehozása, mivel több tagországban decentralizált számítógépes rendszerrel oldották meg a fegyverek nyilvántartását. Magyarország e vitában nem volt érintett, mivel rendelkezik központi fegyver-nyilvántartással. Az Európai Parlament által elfogadott szöveg értelmében 2014. december 31-ig kell központosított vagy decentralizált fegyver-nyilvántartást létrehozni úgy, hogy ahhoz az illetékes bűnüldöző hatóságok hozzáférését biztosítani kell. Ezzel együtt a fegyverek „életciklusa" miatt módosították, azaz 10 évről 20 évre emelték a fegyverrel kapcsolatos adatok tárolási határidejét, illetve pontosították a tárolandó adatok körét (ezek többsége a fegyverre vonatkozik).

Az irányelv módosítása jó példával szolgál egy adatvédelmi szabályozási problémára. A módosítandó 91/477/EK irányelv egyebek mellett arról rendelkezik, hogy a tagállamoknak (kereskedőknek) nyilvántartást kell vezetniük az irányelv hatálya alá tartozó lőfegyverek azonosításához szükséges jellemzőkről (típus, gyártmány stb.), valamint a „szállító és a fegyvert megszerző személy" nevéről és címéről. Az irányelv azt is tartalmazza, hogy a tagállamok hatóságait tájékoztatni kell a bejelentéshez kötött lőfegyverek átruházásáról és átadásáról a fegyver azonosító adatain kívül az „azt megszerző személy azonosításához szükséges adatok feltüntetésével". Az irányelv leírja az egyik tagállamból a másikba történő szállítás esetén követendő eljárási rendet: eszerint a fegyveradatok mellett az eladó és a vevő nevét és címét az illetékes hatóságok tudomására kell hozni. Álláspontunk szerint ezen adatkezelések „igazgatási" célúak, ezért a tagállami adatvédelmi rendelkezések mellett figyelembe kell venni a személyes adatok vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv előírásait is.

Az irányelv módosításának egyik célja az illegális fegyvergyártás és -kereskedelem elleni küzdelem hatékonyságának növelése, amelyet az információcsere javításával kívánnak támogatni. Úgy véljük, problémás annak általános előírása, hogy az irányelv hatálya alatt végzett adatkezelés

és adattovábbítás során a 95/46/EK irányelvet kell alkalmazni, mert az imént említett cél bűnüldözési szempontú, ezért arra nem terjed ki a 95/46/EK irányelv hatálya. Célszerűbbnek tartottuk volna vagy valamelyik „harmadik pilléres" jogi eszköz módosítását, vagy egy új megfogalmazását azért, hogy a különböző célú adatkezelések és adattovábbítások jogszerűen történjenek, ezen észrevételünk azonban nem talált meghallgatásra, így az EP által megszavazott szövegváltozatban nem tesznek különbséget a kétféle cél szerinti adattovábbításra vonatkozó előírások során.

Hasonló, „pillérek közötti keveredés" tapasztalható a Schengeni Információs Rendszer, a Vízuminformációs Rendszer, a Váminformációs Rendszer és az Eurodac esetében is, ami a jogalkalmazók és az adatvédelmi ellenőrzést végzők munkáját megnehezíti, továbbá lehetővé teszi a célnak nem megfelelő adatkezelést.

Rendőrségi Együttműködés Munkacsoport (Police Cooperation Working Party – PCWP)

A Rendőrségi Együttműködés Munkacsoport 2007-ben az alábbi – számunkra – érdekes témákkal foglalkozott:

1. Eltűnt személyek és azonosítatlan holttestek adatbázisa

Az év elején arról tájékoztatták a PCWP-t, hogy az Interpol Közgyűlése szerint az eltűnt személyekről és az azonosítatlan holttestekről külön adatbázist kellene létrehozni, elsősorban a természeti katasztrófák utáni azonosítás megkönnyítése céljából. A PCWP e témában jelenleg nem látja szükségét – még a leendő Interpol-adatbázist kiegészítő jelleggel sem – egy uniós szintű központi adatbázis létrehozásának, azt azonban elképzelhetőnek tartják, hogy az esetleg meglévő tagállami adatbázisok közötti gyors és hatékony adatcserét előirányzó jogi aktus megfogalmazásáról tárgyaljanak később.

2. Bűncselekményekkel kapcsolatba hozható fegyverek nyomon követése

Elkészült a bűncselekményekkel kapcsolatba hozható fegyverek nyomon követését célzó adatcsere eljárási rendjének minimum követelményeit tartalmazó tanácsi ajánlás tervezete. Az ajánlás célja, hogy a tagállami

bűnüldöző hatóságok egységes elvek alapján és egységes formanyomtatványt használva hajtsák végre az információcserét azokban az esetekben, amikor nemzetközi (európai) együttműködés szükséges a fegyver eredetének vagy útjának megállapításához. Az ajánlás végén található az egységes formanyomtatvány, amelyet az információcsere során valamennyi tagállamnak alkalmaznia kell. A dokumentum véleményezése során észrevételt tettünk: az ajánlás nem egyértelmű a tekintetben, hogy az információcserére a tagállam kérelmére, az adatkérés céljának és jogalapjának feltüntetésével kerülhet sor. A formanyomtatvány – véleményünk szerint – olyan adattípusokat is tartalmaz, amelyek nem feltétlenül szükségesek az adatcsere céljának teljesüléséhez. Az ajánlás további „sorsáról" nincs információnk, feltehetően elnapolták a véglegesítését.

3. Nemzetközi vonatkozású labdarúgó meccsek biztonsága

A PCWP egész évben sokat foglalkozott a labdarúgó mérkőzések biztonságával. Egyik ülés során például Németország számolt be a 2006-os világbajnoksággal kapcsolatos rendőri tapasztalatokról, valamint Ausztria és Svájc a jövő évi Európa Bajnokság biztonsági előkészületeiről. Ősszel nemzetközi konferenciát szerveztek, ahol az olasz, a német, az angol, a portugál és a belga hatóságok mutatták be nemzeti megoldásaikat, valamint az EU és az UEFA törekvéseit ismertették. A tapasztalatok és igények összefoglalásaként elkészült egy munkaprogram, ami 19 célkitűzésre, ezen belül 60 intézkedésre tesz javaslatot. A munkaprogram egyik vitás pontja az a terv, amely szerint a „magas kockázatú szurkolókra" kiutazási tilalom lenne elrendelhető.

4. Gépjárművel kapcsolatos bűncselekmények visszaszorítása

Nemzetközi szakértők csoportja irányelv-javaslatot készített egy járműazonosító rendszer (Whole of Vehicle Marking – WOVM) bevezetésére. A javaslat alapján a 17 karakterből álló járműazonosítót a jármű valamennyi (fő)darabján feltüntetnék olyan – néhány EU-n kívüli országban már használt – technológiával (microdotting, azaz 0,5 mm-nél kisebb pontokból álló jelzés elhelyezése), hogy az azonosító nem távolítható el és nem módosítható, ugyanakkor egy olcsó eszközzel leolvasható. Az azonosító és a jármű tulajdonosa közötti kapcsolat megteremtését követően az

esetleg ellopott jármű akkor is visszajuttatható a tulajdonosának, ha azt különböző helyeken alkatrészekre bontva találják meg.

5. Speciális beavatkozó egységek együttműködése

A 2001. szeptember 11-i támadást követően az EU bűnüldöző hatóságainak speciális egységei életre hívták az úgynevezett ATLAS-hálózatot, amelynek keretében azóta számos szemináriumra, tanulmányútra, tananyagok cseréjére és közös gyakorlatozásra került sor. Az elmúlt évek túszdrámái és más különleges beavatkozást igénylő esetei rávilágítottak arra is, hogy az egyes tagállamoknak gyakran lenne szükségük más országok segítségére, amelyet célszerű lenne uniós jogi eszközbe foglalni. Ennek megfelelően elkészült a különleges beavatkozó egységek együttműködéséről szóló tanácsi határozat tervezete, amely a Prümi Szerződés vonatkozó részeit kiegészítve határozza meg a segítségnyújtás feltételeit (kérésre, felszerelés vagy szakértelem) és a másik tagállam területén való jelenlét általános szabályait (felelősség, költségek stb.).

A jogrendbe illesztés során figyelemmel kísérjük a közérdekű adatok nyilvánosságára (közvélemény tájékoztatása a más tagországból érkező kommandósokról, katasztrófa-elhárítókról stb.), valamint a személyes adatok kezelésére (érkező segítők, áldozatok adatai stb.) vonatkozó szabályok kialakítását.

6. Útlevél-adatok cseréje az Interpollal

A Tanács 2005/69/IB közös álláspontja arra kötelezi a tagállamokat, hogy a nemzeti adatbázisba, illetve a Schengeni Információs Rendszerbe (SIS) történő rögzítéssel párhuzamosan (az adatrögzítést követően) kicseréljék az Interpollal az ellopott, elveszett vagy jogellenesen használt kitöltött, illetve kitöltetlen útlevelek adatait (útlevélszám, kibocsátó ország, okmány típusa). Az adatcsere az Interpol ellopott útiokmányok adatbázisába való adattovábbítással valósul meg. A közös álláspont alapján átadott adatokhoz csak azok az Interpol-tagállamok férhetnek hozzá, amelyek biztosítják a személyes adatok megfelelő szintű védelmét. Lehetőség van arra is, hogy csak azok az Interpol-tagok kapjanak adatokat, amelyek viszonozzák azt, illetve a tagállamok megállapodhatnak az Interpollal szélesebb adatkör cseréjéről is. A jogi aktus előírja, hogy a nemzeti adatbázisban, illetve a SIS-

ben történő lekérdezést követően az Interpol adatbázisában is végre kell hajtani az adatellenőrzést. A közös álláspont a Bizottságot bízta meg az előírások végrehajtásának ellenőrzésével.

7. Közös ellenőrző pontok a schengeni térségben

A PCWP egyik ülésén a francia-spanyol határon működő közös ellenőrző pontokat mutatták be. Jelenleg négy – ebből azonban csak egy folyamatosan működődő – olyan határszakasz van, ahol a vám- és határellenőrzési feladatokat ellátó francia és spanyol munkatársak együtt teljesítenek szolgálatot. Az együttműködési központok számára az információcserét lehetővé tevő megállapodás alapján kétnyelvű informatikai hátteret alakítottak ki, amely szükség esetén lehetővé teszi, hogy a feladatok ellátásához szükséges információ négy órán belül rendelkezésre álljon. A központok segítik a más tagállami hatóságokkal és az Interpollal való együttműködést is. A francia elnökség idején (2008. II. félév) kiemelt téma lesz az ilyen típusú közös kapcsolattartó pontok működése. Tudomásunk szerint Hegyeshalomnál magyar-osztrák, Ártándnál pedig magyar-román közös kapcsolattartó pontok működnek, ahol az országok közötti együttműködési megállapodások alapján mind az információcsere, mind a közös járőrözések és ellenőrzések évek óta zajlanak.

Terrorizmus Elleni Munkacsoport (Working Party on Terrorism – TWG)

Kiemelt témák: a terrorizmus finanszírozása elleni küzdelemben „a listán" szereplő személyek pénzügyi helyzetének befagyasztása, „radikális hitszónokok" kitoloncolása, információcsere terrorista indíttatású emberrablásokról.

A terroristák internet-használata elleni kezdeményezés („Check the Web" - „Keress a Neten") célja a tagállamok és az Europol közötti együttműködés megerősítése azzal, hogy a nyílt internet-források elemzését-értékelését önkéntes alapon megosztják egymással. Az internet-használat jelentős szerepet játszik a terrorista szervezetek körében: toborzásra, kiképzésre (fegyver- és bombakészítési, taktikai tanácsok stb.), egyéb információk továbbítására használják.

A tagállamok együttműködésének megkönnyítése céljából az Europol létrehozott egy információs portált, amely több modulból áll:

- szakértői hálózat (tagállami kapcsolattartók, nyelvtudás, szakértelem);
- megfigyelt internetes oldalak címlistája;
- terrorista szervezetek nyilvános bejelentései (források összekapcsolásának elősegítése);
- elemzés-értékelés eredménye (párhuzamos munka elkerülése céljából).

Az Europol információs portáljának használatával a tagállamok elérhetővé tehetik egymás számára az információikat, illetve egy helyen megtalálhatók lesznek az EU-ban rendelkezésre álló ismeretek. Az egymás információihoz és eredményeihez való gyors és közvetlen hozzáféréssel elkerülhető a párhuzamos munkavégzés, illetve a kapcsolattartó személyek jegyzéke alapján egyszerűbbé válik az egyes feladatok összehangolása.

A „Keress a Neten" együttműködés eredményeit, hatékonyságát évente fogják értékelni. Ez annál is inkább üdvözlendő, mert a terrorizmus ellen – sokszor az emberi jogok kárára – csatasorba állított eszközök hatékonyságáról sajnos kevés konkrét elemzést olvashatunk.

A Rendőrségi Munkacsoport (Working Party on Police and Justice - WPPJ)

Az európai adatvédelmi biztosok konferenciája által felállított munkacsoport, mely különösen a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre vonatkozó nemzetközi dokumentumokat elemzi, dolgozza fel az éves európai adatvédelmi biztosi konferenciák (Spring Conferences) előkészítéseként.

Ahogy az már a 2006. évi beszámolóban is szerepelt, a magyar adatvédelmi biztos volt a Rendőrségi Munkacsoport elnöke az európai adatvédelmi biztosok 2006 tavaszán Budapesten megrendezett konferenciájától kezdődően a 2007 májusában Larnacában, Cipruson megtartott konferenciáig. A magyar elnöklés alatt a munkacsoport három dokumentumot készített elő, és terjesztette azokat a ciprusi tavaszi konferencia elé:

A rendvédelmi szervek tevékenysége során a hozzáférhetőség elvének alkalmazására vonatkozó közös állásfoglalás az Európai Unió és a nemzeti parlamentek jogalkotóinak kíván iránymutatást adni a rendvédelmi szervek együttműködése szabályrendszerének kialakításához. A közös állásfoglalás összefoglalásaként egy ellenőrzési listát állítottak össze, amely egyrészt összefoglalja a dokumentumot, másrészről a jogalkotókat segíti az adatvédelem szempontjából fontos kritériumok ellenőrzésénél.

A ciprusi tavaszi konferencia nyilatkozatot fogadott el a rendőrségi és igazságügyi együttműködés keretében, büntetőügyekben kezelt személyes adatok védelméről szóló kerethatározat tervezetre vonatkozóan. Az előző véleményekhez hasonlóan az adatvédelmi hatóságok most is hangsúlyozták a nemzeti szinten is megfelelő és harmonizált adatvédelmi követelmények alkalmazásának fontosságát. Ezen túlmenően a dokumentum a kerethatározat tervezetének kidolgozásakor követendő adatvédelmi elvek listáját is tartalmazza.

A konferencia döntött a Rendőrségi Munkacsoport átszervezéséről. Az Európai Unió harmadik pillérében, a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés területén egyre több olyan javaslat kerül napirendre, amely több figyelmet érdemel az európai adatvédelmi hatóságoktól. Rá kell mutatniuk a szabadságjogokat fenyegető kockázatokra, és megoldási javaslatokat kell nyújtaniuk az egyének jogainak hatékonyabb tiszteletben tartása érdekében. Ezzel egyidőben az Európai Parlament, a Tanács és a Bizottság is egyre gyakrabban fordul az adatvédelmi hatóságok képviselőihez és kéri ki véleményüket. A Rendőrségi és Igazságügyi Munkacsoport az európai adatvédelmi hatóságok tavaszi konferenciája nevében jár el, ha sürgős esetben a konferencia gyors válaszadására van szükség. A hatékonyság fokozása érdekében döntött úgy a tavaszi konferencia, hogy két éves időtartamra választja meg a munkacsoport elnökét és alelnökét.

A munkacsoport 2006 őszén három ízben hallatta hangját. Elsőként a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében kezelt személyes adatok védelméről szóló kerethatározat tervezetre vonatkozóan hívta fel a figyelmet arra, hogy a kidolgozás alatt lévő tervezetben biztosított védelem szintje nem lehet alacsonyabb, mint a jelenleg hatályos nemzetközi jogi dokumentumokban biztosított védelem szintje.

A Tanács tervei között szerepel, hogy az Europol egyezményt az egyezménnyel azonos tartalmú határozat váltsa fel. A határozattervezet adatvédelemről, adatbiztonságról szóló fejezetéhez a munkacsoport szövegszerű megoldási javaslattal állt elő.

A Bel- és Igazságügyi Tanács 2007 júniusában felhatalmazta a Bizottságot, hogy készítsen javaslatot a rendvédelmi szervek Eurodac-hoz történő hozzáférésére vonatkozóan a terrorista cselekmények és egyéb súlyos bűncselekmények megelőzése és felderítése során végzett feladataik során. A Bizottság több megbeszélést kezdeményezett a kérdés kapcsán, amelyre az adatvédelmi hatóságok képviselőit is meghívták. Legutóbb a Rendőrségi és Igazságügyi Munkacsoport levélben fordult a Bizottság alelnökéhez és adott hangot aggodalmának. A rendvédelmi szervek Eurodac-hoz történő hozzáférésével szembeni legfőbb érv az, hogy az adatbázist nem rendvédelmi célokra hozták létre. Eddig a Bizottság nem tudta kellőképpen igazolni a rendvédelmi szervek hozzáférésének szükségességét és azt sem sikerült még tisztázni, hogy milyen adatokat vetnének össze az Eurodac-ban tárolt adatokkal.

Telekommunikációs Munkacsoport (International Working Group on Data Protection in Telecommunications - IWGDPT)

A telekommunikációval foglalkozó nemzetközi adatvédelmi munkacsoport Berlinben tartotta 42. konzultációját 2007. szeptember 4-5-én.

A találkozón igen részletes és kimerítő tanulmány vázolta fel mindazokat a problémákat, amelyekkel az adatvédelemnek a digitális és interaktív televíziózásra való áttéréssel szembesülnie kell. A technológiai újításoknak köszönhetően a kommunikáció, a számítástechnika és tömegtájékoztatás jelenleg még elkülönült hálózatai egyetlen szélessávú adatátviteli rendszerben ötvözhetők. Ez az egységes adatátviteli rendszer komoly hatást gyakorol az adatvédelemre, hiszen a digitális szolgáltatások elképzelhetetlenek a felhasználók adatainak feldolgozása és gyűjtése nélkül.

A technológiai újításoknak köszönhetően egyre szélesebb körben használatosak a tömegközlekedésben az elektronikus jegyek. Az elektronikus díjfizetési rendszer az elektronikus kártya használatára épül, és előnye, hogy a vasúti, a földalatti és felszíni közlekedésben egyaránt alkalmazható. A rendszer az úgynevezett RFID technológiával is összekapcsolható. A kártya

chipje tartalmazza a közlekedés szempontjából lényeges információkat, és az utas személyes adatait. A találkozó résztvevői ajánlást fogadtak el, amelyben kifejtették, hogy a tömegközlekedési vállalatoknak és a közlekedési hatóságoknak egyértelmű tájékoztatást kell adniuk az utasoknak az adatkezelésről, minimalizálni kell a kezelt adatok körét, és az utasoknak alternatívát kell nyújtani az elektronikus rendszer mellett arra, hogy névtelenségbe burkolva is igénybe vehessék a tömegközlekedési eszközöket.

A találkozón szó esett a 29-es Munkacsoport és a Google Inc. között zajlott konzultációról, amely a Google adatkezelésének az uniós normákhoz való igazítását célozza.

A találkozó további témái voltak a „GoLog" internetes kereső, más webes szolgáltatások, és a Whois adatbázisok, a p2p (peer-to-peer) technológia használatával járó szerzői jogsérelmek, a számítástechnikai bűnözés elleni egyezmény, illetve a gépjárművek közlekedési eseményt rögzítő berendezéseinek adatvédelmi természetű problémái.

A munkacsoport megbeszélésén elhangzott, hogy szoros együttműködés szükséges az ISO-val a minőségügyi szabványok fejlesztése terén.

A találkozón ismertettük a hazai közoktatási intézményekben bevezetni tervezett biometrikus beléptető-rendszert, és a magyarországi piac- és közvélemény-kutatásban jelentős szerepet betöltő cég (Medián) új webaudit szolgáltatását (WebProfil). A webauditot érintő adatvédelmi vizsgálat még nem zárult le, a vizsgálat részletei az Internetről szóló fejezetben olvashatók.

Információ Biztonsági Megoldások Európai Konferenciája (ISSE/SECURE)

Az Információ Biztonsági Megoldások Európai Konferenciáját 1999-ben hozta létre az „eema" (IT szakemberek, üzletemberek és kormányzati szereplők független szervezete) és a TeleTrust Deutschland (non-profit szervezet, mely az információs és kommunikációs technológiák megbízhatóságát ösztönzi és támogatja). A Konferenciát 2007. szeptember 25-27. között Varsóban tartották meg.

A kommunikációs és információs hálózatok biztonsága egyre nagyobb figyelmet érdemel. A felmerülő problémák kezelésére újabbnál újabb stratégiákat szükséges kidolgozni. Ehhez a szakmai, illetve a különböző szektorok közötti együttműködés elengedhetetlen európai szinten. Ezen a

fórumon a közvetlen tapasztalatcserének köszönhetően naprakész információkkal szembesülhettünk: milyen irányba halad az információs biztonsági technika, milyen újabb jogi, technikai kihívásokkal kell szembenézni adatvédőként, információs jogokat hogyan kezelik, a gyakorlatban felmerülő veszélyek, a rendszerek fejlesztői és a biztonsági megoldásokat árusítók szerepvállalása, az információ biztonsággal foglakozó vezető szakembereket leginkább foglalkoztató praktikus kérdések.

Kiemelkedő fontossággal bírt, hogy a piacvezető cégek, felismerve az emberi tényezőnek az információ biztonsága megőrzésében játszott szerepét, érdekeltségét, jelentős energiát és pénzt áldoznak arra, hogy a biztonság védelme érdekében növeljék a munkavállalóik ismereteit. A tájékoztatáshoz kapcsolódóan különösen figyelemreméltó – és követendő – a fiatalok internet használatát kísérő veszélyekre való figyelemfelhívó lengyel tájékoztató kampány.

IV. AZ ADATVÉDELMI NYILVÁNTARTÁS ÉS AZ ELUTASÍTOTT KÉRELMÍEK NYILVÁNTARTÁSA

A. Adatvédelmi nyilvántartás

Az adatvédelmi biztos az Avtv. 24. § c) pontja szerint gondoskodik az adatvédelmi nyilvántartás vezetéséről. Az adatvédelmi nyilvántartás nyilvános, bárki számára megtekinthető, illetve a honlapunkon elektronikusan is elérhető.

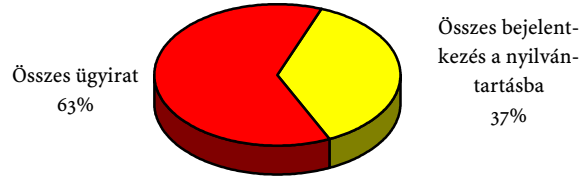
Az adatvédelmi nyilvántartás célja, hogy nyilvántartsa a Magyar Köztársaság területén folytatott adatkezeléseket. Az adatvédelmi nyilvántartás tartalmazza, hogy kik (mely adatkezelők), milyen célból, milyen jogalappal, milyen személyes adatokat, mennyi ideig kezelnek, az adatokat hova, milyen célból, milyen jogalappal továbbítják. A nyilvántartás, ha az adatkezelők bejelentési kötelezettségüknek eleget tesznek, átfogó képet ad arról, hogy a különböző adatkezelők által összegyűjtött adatokat kik, milyen célból használják fel.

A nyilvántartás célja elsősorban az érintettek tájékoztatása, különösen abban az esetben, ha információs önrendelkezési jogukat közvetlenül nem gyakorolhatják, ugyanakkor az adatkezelések jogszerűségének ellenőrzésére is szolgál. Azon bejelentések esetében, melyek hiányosak, felhívjuk az adatkezelőt a bejelentés kiegészítésére, módosítására. Ha egy adatkezelésről a bejelentés során kiderül, hogy az adatkezelő a megjelölt személyes adatok kezelésére, vagy továbbítására nem rendelkezik megfelelő jogalappal, vagy az adatokat az adatkezelés céljának elérésével nem törli, esetleg a cél eléréséhez szükségtelen adatokat is kezel, az adatvédelmi biztos, bár a bejegyzést nem tagadhatja meg, az adatkezelővel szemben, a bejegyzést megelőzően vizsgálatot indít. Természetesen, ha egy adatkezelésről megállapításra kerül, hogy jogellenes, az adatvédelmi biztos az adatkezelőt haladéktalanul felhívja a jogellenes adatkezelés megszüntetésére, így a nyilvántartásba bejegyzés mintegy okafogyottá válik.

Az adatvédelmi nyilvántartás deklaratív hatályú. Bár a bejelentés, mint jognyilatkozat az adatkezelőt köti, az adatvédelmi nyilvántartásba

történő bejegyzés nem jelent „engedélyt" az adatkezelésre. Az adatvédelmi ismeretek szélesebb körű elterjedésével párhuzamosan növekszik az adatkezelések adatvédelmi nyilvántartásba történő bejelentésének száma. Eddigi tapasztalataink szerint az adatkezelők az adatkezelés jogszerűségét az „adatvédelmi nyilvántartási szám megszerzésével, meglétével" kapcsolják össze. Nyomatékosan fel kell azonban hívnunk az adatkezelők, de leginkább az érintettek figyelmét arra, hogy nem az az adatkezelés jogszerű, amelynek van nyilvántartási azonosítója, hanem az, amely során az adatkezelő a személyes adatokat jogszerűen kezeli. A bejelentés önmagában nem teszi jogszerűvé az adatkezelést. Előfordulhat ugyanis, hogy az adatkezelés bejelentése során az adatkezelő megjelöl minden kötelezően bejelentendő adatot, azok meg is felelnek a törvényi követelményeknek – például ha az adatkezelő az adatkezelés jogalapjaként az érintett hozzájárulását jelöli meg – , de az adatkezelés nem a bejelentésnek megfelelően folyik, vagy ha például az adatkezelő a bejelentés során elmulasztja megjelölni, hogy az összegyűjtött adatokat harmadik személyekhez továbbítja.

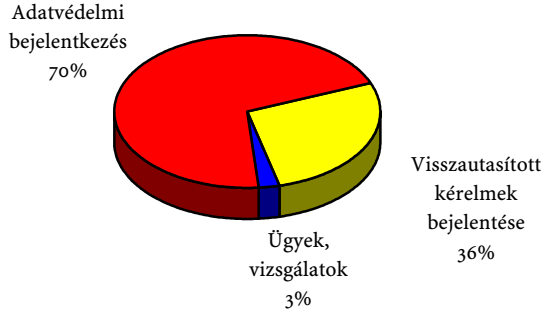
Az ABI tevékenységi körében az adatvédelmi nyilvántartás helyzete
2007 (%)



Az Avtv. 28. § (1) bekezdése rendelkezik az adatvédelmi nyilvántartás részletes szabályairól. A személyes adatokat kezelő adatkezelő köteles adatkezelési tevékenysége megkezdése előtt az adatvédelmi

biztosnak nyilvántartásba vétel végett bejelenteni az adatkezelés célját, az adatok fajtáját és kezelésük jogalapját, az érintettek körét, az adatok forrását, a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, az egyes adatfajták törlési határidejét, az adatkezelő, az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, valamint a belső adatvédelmi felelős nevét és elérhetőségi adatait.

Az ABI nyilvántartási tevékenységének megoszlása
a beérkezett nyilvántartási kérelmek alapján
2007 (%)



Az adatvédelmi nyilvántartásba történő bejelentések 2007. évi tapasztalatai

Az adatkezelők a bejelentést leginkább a honlapunkon megtalálható, és arról letölthető adatlapon teszik meg, bár a bejelentésnek az adatlap nem kötelező formája. Mivel nagyon sokféle adatkezelés folyik, az adatlap nem minden esetben nyújt a bejelentett adatkezelésről elegendő információt. Azon bejelentések esetében, amikor sokféle személyes adatnak, bonyolult rendszerben történő kezeléséről van szó, célszerűbb az Avtv. 28. §-ában megjelölt adatoknak az adatlap kitöltése mellett, az adatlapnál bővebb, az adatkezelés folyamatát is leíró bejelentése, mert

így jobban nyomon követhető, hogy mely adatkezelések kapcsolódnak össze, illetve az egyes adatbázisok között milyen adattovábbítás zajlik.

Az adatvédelmi nyilvántartásba történő bejelentés egy jognyilatkozat, melyet a jognyilatkozatra vonatkozó formai kritériumok megtartásával az adatkezelő szerv vagy személy köteles megtenni. Tapasztalataink szerint sokszor – különösen a reklám célú adatgyűjtések estében – nem az adatkezelő, hanem az adatfeldolgozással megbízott adatfeldolgozó a bejelentő. Ha az adatkezelő helyett az adatfeldolgozó jár el a bejelentés során, a bejelentéshez csatolni a Polgári Törvénykönyv, illetve a gazdasági társaságokról szóló törvény képviseletre vonatkozó szabályainak megfelelően a képviseleti jogosultságot igazoló okiratot (meghatalmazás, megbízás).

A bejelentést minden esetben (cégszerűen) alá kell írni. Ha valamely adatkezelés bejegyzése sürgős, (pl. népszavazás, népi kezdeményezésre irányuló aláírásgyűjtés) az Iroda fogadja a faxon, vagy e-mailen elküldött bejelentéseket is, ilyenkor a bejelentés feldolgozását a faxon, vagy e-mailen megküldött bejelentés alapján is megkezdjük, de az adatkezelésre vonatkozó nyilatkozatot, vagy bejelentőlapot ilyen esetben is szükséges aláírva, postán utólag megküldeni.

Az aláírás helye az adatlapon nincs megjelölve, de a bejelentőlap minden oldalának, vagy a kísérőlevélnek (melyhez a bejelentés folytatólagosan csatolva van) aláírásával a bejelentés hitelesíthető.

A bejelentést – tekintettel arra, hogy csak az aláírt nyilatkozat jegyezhető be a nyilvántartásba, valamint arra, hogy elektronikus aláírást fogadni nem tudunk – csak postai úton, vagy személyesen lehet megtenni.

Az adatkezelőt, illetve a hozzá tartozó adatkezelést a bejelentés alapján az Adatvédelmi Biztos Irodája nyilvántartásba veszi. A bejegyzésre vonatkozóan az Avtv. határidőt nem állapít meg A megküldött bejelentések bejegyzése attól függően történik, hogy az adott időben milyen mennyiségű bejelentés érkezik. Gyakorlati tapasztalatok azt mutatják, hogy a bejegyzés, illetve postázás körülbelül két hetet vesz igénybe. Mivel az adatvédelmi nyilvántartás az adatvédelmi biztos honlapján elérhető, az adatkezelő, illetve az adatkezelés bejegyzését követően a nyilvános adatbázisban azonnal megjelenik, így az adatvédelmi nyilvántartási azonosító ott már korábban is megtekinthető.

Az adatkezelés bejegyzéséről, illetve az adatvédelmi nyilvántartási azonosítóról az adatkezelőt értesítjük. Az Avtv. 29. § (1) bekezdése szerint a nyilvántartási számot az adatok továbbításánál, illetve nyilvánosságra hozásánál és az érintetteknek való kiadásakor kell feltüntetni. Általános gyakorlat, hogy az adatkezelők az adatvédelmi nyilvántartási azonosítót az érintettekkel való kapcsolattartás során minden dokumentumon, így az adatkezelési tájékoztatón is feltüntetik. Ezt a gyakorlatot, tekintettel arra, hogy az adatvédelmi nyilvántartás informatív jellegéből következően plusz tájékoztatást nyújt az érintetteknek, üdvözöljük.

Az Avtv. 3. § (1) bekezdése szerint személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény – vagy törvény alapján, az abban meghatározott körben önkormányzati rendelet – elrendeli. Az adatkezelések tehát a jogalap tekintetében kétfélék lehetnek, jogszabály által elrendelt, illetve az érintett hozzájárulásán alapuló adatkezelés.

Az Avtv. 28. § (2) bekezdése szerint a jogszabályban elrendelt adatkezelést a szabályozás tárgya szerint illetékes miniszter, országos hatáskörű szerv vezetője, illetőleg a polgármester, főpolgármester, a megyei közgyűlés elnöke köteles bejelenteni a jogszabály hatálybalépését követő 15 napon belül.

A jogszabályban elrendelt adatkezelések bejelentése – a törvény egyértelmű rendelkezése ellenére – esetleges. Ennek az lehet az oka, hogy egyrészt nagyon sok jogszabály rendelkezik adatkezelésről, mely adatkezelések bejelentése korábban sem volt teljes, másrészt a jogszabályváltozások során az adatkezelésekben bekövetkező változás bejelentése elmarad.

Problémát jelent például a regionális szervek adatvédelmi nyilvántartási átvezetése. Az átszervezést követően a regionális szervek az elődszervek bejelentéseit nem módosították, holott az Avtv. 29. § (2) bekezdése kötelezővé teszi minden olyan változás bejelentését, mely az adatvédelmi nyilvántartás adattartalmát érinti, így az adatkezelő megváltozását, átalakulását is. A változások, átalakulások nyomon követése az adatkezelők közreműködése nélkül szinte lehetetlen.

Ez a probléma egyébként az államigazgatás majd minden területére jellemző. Míg a magánszervek, cégek szervezeti átalakulásaikat (pl. cégnévváltozás, székhelyváltozás, átalakulás) elég nagy arányban bejelentik,

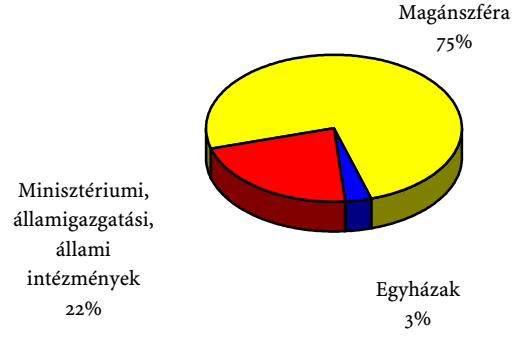
addig az állami és önkormányzati szervek (minisztériumoktól a helyi szervezeti egységekig) rendre elmulasztják a változás adatvédelmi nyilvántartásba történő bejelentését. Az elmúlt évekhez hasonlóan az állami és önkormányzati szervek 2007-ben kevés bejelentést teljesítettek annak ellenére, hogy jelentős számú adatkezelést is érintő jogszabálymódosítások történtek.

Kivételt csak a rendvédelmi szervek képeznek, melyek a személyes adatok kezelését érintő bejelentéseket rendre megküldik.

Az állami adatkezelők adatvédelmi nyilvántartásba történő bejelentését jól példázza, hogy az Igazságügyi és Rendészeti Minisztériummal valamint a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalával folytatott levelezés, illetve felhívásunk ellenére a Schengeni Információs Rendszert, az adatkezelő kilétének tisztázatlansága okán az adatvédelmi nyilvántartásba 2007 végéig még mindig nem jelentették be.

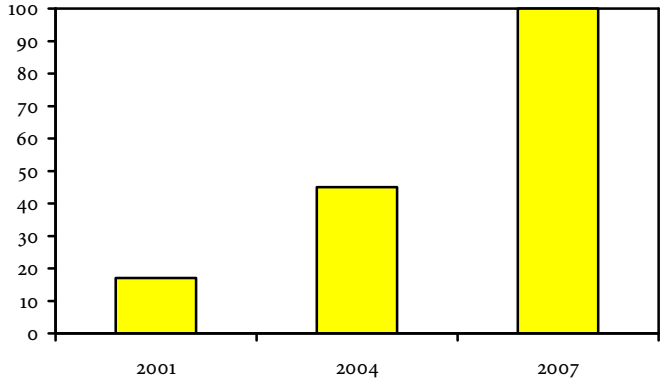
Meg kell azonban jegyezni, hogy az Avtv. 28. §-ának (2) bekezdésében meghatározott bejelentési kötelezettséget több bejelentésre kötelezett félreértett. Az, hogy a jogszabályban elrendelt adatkezelést a miniszter, illetve az országos hatáskörű szerv vezetője köteles bejelenteni, nem jelenti azt, hogy a bejelentést tevő az adatkezelő. Adatkezelő az a szerv, vagy személy, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja. Adatkezelő lehet ebből következően – függetlenül attól, hogy az adatvédelmi nyilvántartásba történő bejelentést ki teszi meg – valamely területi szerv is.

Főbb adatkezelői kategóriák
(önkormányzatok nélkül)
2007 (%)



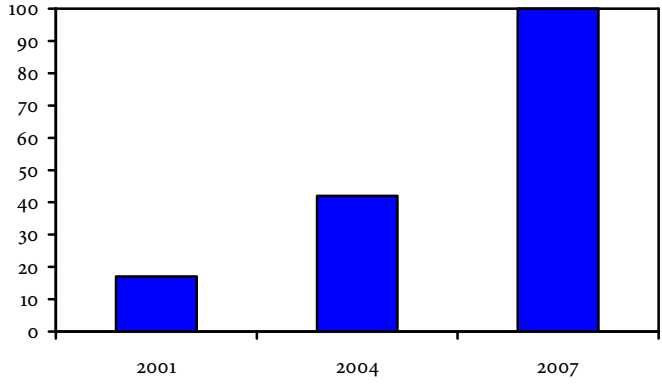
Tekintettel arra, hogy a közelmúltban az államigazgatási szervek tekintetében jelentős változások történtek, mely változások átvezetése az adatvédelmi nyilvántartásba nem történt meg, szükségesnek látjuk felhívni a minisztériumok és az országos hatáskörű szervek vezetőinek figyelmét az Avtv. 28. §-ának (2) bekezdésében szabályozott bejelentési kötelezettségre. Az adatvédelmi nyilvántartásba be kell jelenteni a jogszabályváltozások következtében létrejövő új adatkezeléseket, valamint az egyes adatkezelések esetében az adatkezelő személyében történő változást, illetve természetesen azt is, ha az adatkezelő megnevezése megváltozik. Be kell jelenteni az adatkezelésben bekövetkezett minden olyan változást is, amely a bejelentésben meghatározott adatkört érint. Így be kell jelenteni az adatkezelés céljában, a kezelt adatok fajtájában, az érintettek körében, az igénybevett adatfeldolgozó személyében történt változást. Be kell jelenteni továbbá azt is, ha az adatkezelés alapjául szolgáló jogszabály, így az adatkezelés jogalapja változik meg.

Bejelentkezett magánszféra
(adatkezelők)
2001-2007 (%)



Nagyon sok bejelentés érkezik a magánszféra adatkezelőitől. Továbbra is elsősorban a marketing tevékenységet végző szervek jelentették be a promóciós célú adatkezeléseket. Tovább nőtt az internetes adatgyűjtések, adatkezelések száma.

Bejelentkezett magánszféra
(adatkezelések)
2001-2007 (%)



Az érintettek hozzájárulásával történő adatgyűjtések esetében újra és újra felhívjuk az adatkezelők figyelmét az érintettek megfelelő tájékoztatásának fontosságára. Az adatvédelmi szabályok lehetővé teszik magánszemélyek, szervezetek, cégek részére személyes adatok gyűjtését, ha az adatgyűjtés konkrétan meghatározott célból történik, az adatkezelés csak a konkrét cél eléréséhez feltétlenül szükséges adatok gyűjtésére korlátozódik, az adatkezelő az összegyűjtött adatokat biztonságosan kezeli, tárolja, az adatkezelő az adatgyűjtést megelőzően az érintetteket az adatkezelés részleteiről megfelelően tájékoztatja. Az adatkezelő az adatgyűjtés megkezdése előtt tehát köteles az érintetteket az adatkezelés részleteiről megfelelően tájékoztatni, valamint adatkezelését az adatvédelmi nyilvántartásba bejelenteni.

Marketing, direkt marketing célú adatkezelések bejelentése

A reklámmal, marketinggel foglalkozó társaságok tapasztalataink szerint már sokkal jártasabbak az adatvédelmi kérdésekben, mint korábban. A reklám célú adatkezelések (promóciók) nagy részét a piacon jelen lévő marketing tevékenységgel foglalkozó cégek végzik,

többségében megbízási szerződés keretében. Ezek a cégek rengeteg promóciós adatgyűjtést, nyereményjátékot szerveznek a különböző termékeket és szolgáltatásokat megrendelő, használó személyek körének megkeresése érdekében. Az így létrejövő adatbázisok – a megbízástól függően – vagy a megbízottnál maradnak, vagy a megbízóhoz kerülnek, jellemzően további megkeresésekre történő felhasználás céljából.

Abban az esetben, ha a megbízás a promóció teljes lebonyolítására, az adatkezelés egészére vonatkozik, és a megbízó az adatokhoz nem fér hozzá, azokat semmilyen céllal nem kezeli, akkor a megbízó a szűken értelmezett adatkezelésben nem vesz részt. Ez esetben a megbízott az adatkezelő, aki az egyes adatkezelési műveletek elvégzéséhez adatfeldolgozót vehet igénybe. Ha azonban a megbízott cég „csak" adatfeldolgozóként vesz részt az adatkezelésben, az adatkezelésnek „csak" egy részét végzi, mint a személyes adatok gyűjtése, az érintettek részére küldemények postázása, az összegyűjtött személyes adatok azonban a megbízóhoz kerülnek, az adatbázis a megbízó birtokába kerül, az adatkezelő a megbízó szerv, míg a megbízott adatfeldolgozó a folyamatban. Az adatfeldolgozó cég ez esetben az Avtv. 4/A. § (2) bekezdése szerint tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe.

Az adatvédelmi nyilvántartásba bejelentési kötelezettsége az adatkezelőnek van. A bejelentést annak a személynek, szervnek kell megtennie, amely az adatkezelési folyamatban az adatkezelő, nem kell azonban külön bejelentést tennie az adatfeldolgozónak, őt bejelentése során az adatkezelő köteles az adatvédelmi nyilvántartásba bejelenteni. Az adatfeldolgozó a bejelentés ügyében csak az adatkezelő cég képviseletében, az adatkezelő által adott meghatalmazás, esetleg ilyen tárgyú megbízás birtokában járhat el.

Internetes adatkezelések bejelentése

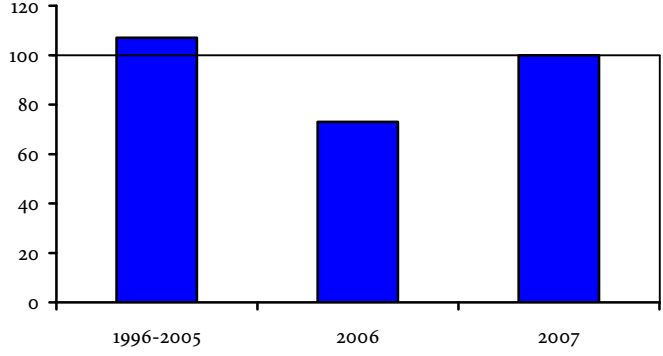
Az internet egyre nagyobb szerephez jut az emberek mindennapi életében, ezzel együtt egyre több személyes adat kerül fel a hálóra. Ha a felhasználó által megadott adatok (IP-cím, a felhasználó neve, e-mail címe, stb.) természetes személlyel összekapcsolhatóak, illetve kapcsolatuk a természetes személlyel helyreállítható, akkor személyes adatnak minősülnek. Az ilyen adatoknak a szerveren történő tárolása adatkezelésnek minősül, az adatkezelő ebben az esetben a szerver üzemeltetője. A

tartalom készítője oldalain általában csak olvasható információkat tesz közzé, és nem rögzít személyes adatokat, így nem adatkezelő. Ha azonban a felhasználó regisztrálja magát a weboldalon, akkor a tartalomszolgáltató is adatkezelővé válhat.

A weboldalakon a regisztráció önkéntes. Az adatkezelés jogszerűségének feltétele azonban, hogy az adatkezelő a regisztráció helyén megfelelő tájékoztatást nyújtson arról, hogy kik, milyen célból, mennyi ideig kezelik a regisztrált személyes adatait. Az adatkezelőnek biztosítania kell továbbá, hogy az érintett bármikor, legalább olyan egyszerűen, mint ahogy a regisztrációra is sor került, „leregisztrálhasson", vagyis kérje személyes adatainak az adott oldalról történő törlését.

Ha a honlap üzemeltetője elektronikus leveleket, hírleveleket is küldeni szeretne az oldalon regisztrált személyeknek, az Avtv. rendelkezésein túl az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény rendelkezéseire is figyelemmel kell lennie. A törvény szerint kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető elektronikus úton, levelezés során elektronikus hirdetés. Az elektronikus hirdető, az elektronikus hirdetési szolgáltató és az elektronikus hirdetés közzétevője köteles nyilvántartást vezetni azokról, akik számára bejelentették, hogy kívánnak elektronikus hirdetést kapni; nem küldhető elektronikus hirdetés annak, aki nem szerepel ebben a nyilvántartásban.

Internettel kapcsolatos adatkezelések száma
(%)



Az internetes adatkezeléseket az adatvédelmi nyilvántartásba be kell jelenteni. A bejelentési kötelezettség független attól, hogy az érintett hozzájárulásával történő adatkezelésről, vagy a törvény által elrendelt adatkezelésről van szó. Az Interneten történő adatgyűjtések esetén nagy figyelmet kell fordítani az érintettek megfelelő tájékoztatására, mivel a világhálón a megadott személyes adatok sokszor az érintett figyelmetlensége miatt olyan személyekhez, olyan helyekre is eljuthatnak, akikhez, illetve ahova az érintett azokat nem kívánta továbbítani. Körültekintően kell eljárni a különböző közösségi portálokon történő regisztráció során. Tekintettel arra, hogy a közösségi portálokon milyen sok személyes adatot, illetve sokszor különleges adatokat adnak meg a látogatók, különös figyelmet kell fordítani az érintettek egyértelmű és részletes tájékoztatására, illetve az adatok biztonságának biztosítására.

Továbbra is sok webáruház üzemeltetésével kapcsolatos adatkezelés bejelentése érkezik az Irodához. Webáruház üzemeltetése olyan szolgáltatás nyújtása az interneten, mely során személyes adatok gyűjtése, tárolása is történik. Az internetes áruházban történő vásárlással „szokványos", a kereskedelmi forgalomban megvalósuló adás-vétel jön létre. Ha

a személyes adatok felhasználása csak a konkrét vásárlással összefüggésben történik, úgy mint például számlázás, az adatkezelést nem kell az adatvédelmi nyilvántartásba bejelenteni, mivel az az Avtv. 30. §-ának a) pontjában szabályozott ügyfélkapcsolatnak minősül. A szolgáltatás nyújtásához szükségszerűen nem kapcsolódó adatkezelést (pédául adatok tárolása reklámanyag továbbítása céljából), illetve az egyéb célú adatkezelést (például fórum) azonban az adatvédelmi nyilvántartásba be kell jelenteni.

Az internetes adatkezelések során az adatkezelőknek különös figyelmet kell fordítani a gyerekek személyes adatainak védelmére. Személyes adatával mindenki saját maga rendelkezhet. Az egyes (felnőtt) családtagok nem adhatnak érvényes hozzájárulást egymás személyes adatainak kezelésére, míg kiskorú gyermekek esetében a személyes adatok kezeléséhez a szülő (törvényes képviselő) hozzájárulása szükséges. Az érintett adatkezeléshez való hozzájárulása egy jognyilatkozat, melyre a Ptk. rendelkezései irányadók. A Ptk. szerint tizennegyedik életévét be nem töltött kiskorú (cselekvőképtelen) nevében a törvényes képviselője jár el, tizennegyedik életévét betöltött kiskorú (korlátozottan cselekvőképes) esetében pedig a kiskorú nyilatkozatának érvényességéhez – ha jogszabály kivételt nem tesz – törvényes képviselőjének beleegyezése, vagy utólagos jóváhagyása szükséges. Bár a korlátozottan cselekvőképes kiskorú a törvényes képviselőjének közreműködése nélkül is megkötheti a mindennapi élet szokásos szükségleteinek fedezése körébe tartozó kisebb jelentőségű szerződéseket, tehet jognyilatkozatot, mégis előfordulhatnak olyan visszás helyzetek, amikor a kiskorú olyan ügylethez adja személyes adatainak (például képmás) kezeléséhez való hozzájárulását, amely a mindennapi élet szokásos jogügyletein túl mutat. Az adatkezelő felelőssége, hogy jogszerűen kezelje a személyes adatokat. Úgy gondoljuk, hogy a kiskorúak érdekeinek védelme érdekében az adatkezelő köteles – akár külön technikai módszer alkalmazásával is – biztosítani a személyes adatok kezeléséhez való hozzájárulás törvényességét.

Követelések kezelése céljából történő adatkezelések bejelentése

Az egyes adósságbehajtással foglalkozó cégekkel kapcsolatban nagyon sok beadvány érkezik a hivatalhoz. A követelésbehajtó cégek

adatátvételének jogalapja különböző lehet, attól függően, hogy az alapkövetelés jogosultja maga, vagy jogi képviselő útján próbálja érvényesíteni a követelést, engedményezi a követelést, esetleg az alapszerződésben foglaltak alapján ruházza át követelését adósságkezelő cégnek.

Mindegyik esetben szükséges azonban, hogy az adósságkezelő cég adatátvétele és adatkezelése vagy az érintett tájékozott hozzájárulásán, vagy valamilyen törvényi rendelkezésen alapuljon. Mivel a követeléskezelő, adósságbehajtó cég az érintettel nincs ügyfélkapcsolatban, a követelésbehajtás során megvalósuló adatkezelést az adatvédelmi nyilvántartásba be kell jelenteni. Meg kell jelölni a bejelentés során, hogy a követelésbehajtó konkrétan milyen személyes adatokat kezel, az adatokat milyen forrásból gyűjtötte, illetve meg kell jelölni az egyes megbízóktól származó adatgyűjtés, adatkezelés jogalapját.

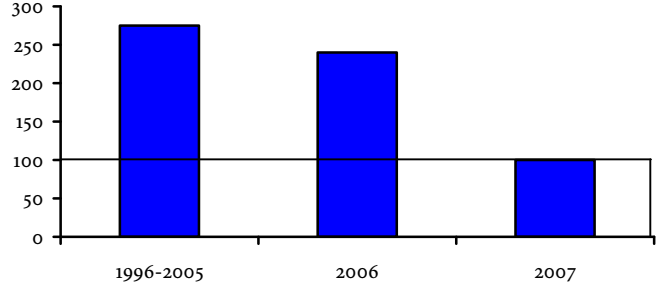
Aláírásgyűjtések bejelentése

2007-ben – ahogy az azt megelőző évben is – sok aláírásgyűjtés célú adatkezelés bejelentése érkezett. Az aláírásgyűjtés során személyes adatok kezelése történik, melynek alapja az Alkotmányban meghatározott petíciós jog, illetve az országos népszavazásról és népi kezdeményezésről szóló 1998. évi III. törvény, valamint a helyi önkormányzatokról szóló 1990. évi LXV. törvény. Az adatvédelmi nyilvántartásba minden aláírásgyűjtést be kell jelenteni, így a népszavazás, népi kezdeményezés célú, illetve a petíciós célú aláírásgyűjtéseket, adatkezeléseket is. Országos népi kezdeményezés, országos népszavazás esetén az Országos Választási Bizottság még az aláírásgyűjtő ívek hitelesítése előtt felhívja a kezdeményezőket az adatkezelés adatvédelmi nyilvántartásba történő bejelentésére, így a népszavazási, népi kezdeményezés célú aláírásgyűjtéseket az adatkezelők rendre bejelentik a nyilvántartásba. Bár korábban közleményben hívtuk fel az aláírásgyűjtők figyelmét az adatvédelmi nyilvántartásba való bejelentés kötelezettségére, még mindig sok olyan petíciós célú aláírásgyűjtésről szerzünk tudomást, melynek adatvédelmi nyilvántartásba történő bejelentését az adatkezelő elmulasztotta. A népszavazási kezdeményezéshez, népi kezdeményezés támogatásához kapcsolódó aláírásgyűjtés esetén a bejelentési kötelezettséget az Országos Választási Bizottság, illetve a helyi, területi választási iroda

vezetője hitelesítő döntését követően – a jogorvoslatra nyitva álló 15 napos határidő kezdetén – célszerű teljesíteni. Ez esetben az aláírásgyűjtő ív hitelesítő záradékkal történő ellátása idejére az adatvédelmi nyilvántartási azonosító – a hitelesítő záradékkal való elláthatóságtól függő hatállyal – kiadható a kezdeményezők részére. Egyéb aláírásgyűjtés esetén az adatvédelmi nyilvántartásba történő bejelentkezést követően kezdhető meg ez a tevékenység.

Aláírásgyűjtéssel kapcsolatos adatkezelések száma

(%)



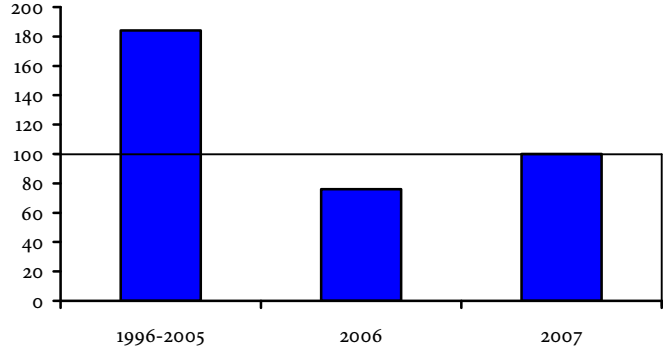
Az aláírásgyűjtés időszakában az adatkezelőt terhelő törvényi kötelezettségek teljesesítéséért az a személy felel, aki vagy amely az Országos Választási Bizottságnál kezdeményezte a kérdés, illetve az aláírásgyűjtő ív hitelesítését. Felelőssége mindazon személyekért fennáll, akik az aláírásgyűjtés szervezésében részt vesznek, a kitöltött aláírásgyűjtő íveket birtokolják, tárolják. Az adatvédelmi nyilvántartási számot az aláírásgyűjtés helyszínén is jól látható formában megtekinthetővé kell tenni.

Munkavállalói adatok továbbításának bejelentése

Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely az adatkezelővel munkaviszonyban álló személyek adatait tartalmazza. Be kell azonban jelenteni az adatkezelést, ha a munkáltató a munkavállalók személyes adatait más szervhez, vagy külföldre továbbítja. Szintén bejelentési kötelezettség alá esik a munka-

viszonnyal közvetlenül össze nem függő adatgyűjtés, így például a külföldi munkavállalók vízum ügyintézése, külföldi anyavállalathoz történő továbbítása, vagy munkavállalói részvényprogramhoz kapcsolódó adatkezelés.

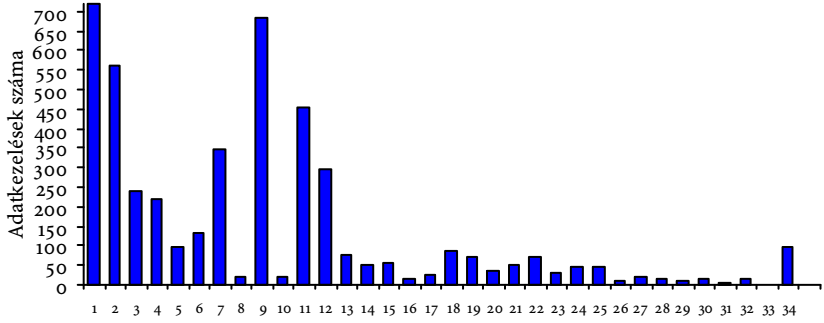
Munkavégzéssel kapcsolatos adatkezelések száma
(%)



Önkormányzatok helyi adatkezelései

Ebben az évben is folytatódott az utóbbi évek bejelentéseinek tendenciája, alacsony számú bejelentés érkezett az önkormányzatok részéről a bevezetett helyi adatkezelésekről. A tapasztalt jelenség oka valószínűleg az, hogy – amint ez az önkormányzatokat érintő vizsgálatokat bemutató fejezetben is olvasható – a helyi adatkezelések bonyolultsága ellenére sok önkormányzati tisztviselő nincs tisztában az adatkezeléssel összefüggő kötelezettségekkel.

A bejelentett helyi adatkezelések fajtái



1 iparűzési adó
2 magánszemélyek kommunális adója
3 vállalkozók kommunális adója
4 építményadó
5 telekadó
6 idegenforgalmi adó
7 gépjárműadó
8 föld bérbeadásából jövedelemadó
9 ebadó
10 behajtandó köztartozások
11 földbérlet
12 lakásépítési kölcsönök nyilvántartása
13 első lakáshoz jutók támogatása
14 marhalevél nyilvántartása
15 méhek vándoroltatása
16 belvízkár
17 mezőőri járulék
18 lakásbérlők
19 üzletek, működési engedélyek
20 közoktatás
21 gyermekvédelem
22 szociális igazgatás
23 sorkötelesek
24 vízközműfejlesztés
25 szemétszállítási díj
26 veszélyes állatok
27 sírbolt könyv
28 kitüntetések, díjak
29 gázközműberuházás
30 támogatások alapítványból
31 egyéni vállalkozói igazolványok
32 telepengedély
33 vízszolgáltatást igénybevevők
34 egyéb adatkezelések

Parkolási szolgáltatást nyújtó társaságok

A közúti közlekedési nyilvántartásról szóló törvény módosítását követően – mivel a módosítással a parkolási szolgáltatást nyújtó társaságok önállóan is igényelhetnek díj és pótdíj behajtása érdekében adatot a nyilvántartásból – megszűnt a bizonytalanság abban a kérdésben, hogy ki köteles az adatkezelést az adatvédelmi nyilvántartásba bejelenteni. A parkolási szolgáltatást nyújtó adatkezelők (bizonyos esetben adatfeldolgozók) az elmúlt évben sorra jelentették be adatkezeléseiket.

Kivételek az adatvédelemi nyilvántartásba történő bejelentési kötelezettség alól

A legtöbb kérdést továbbra is a bejelentés alóli kivételek okozzák. A bejelentési kötelezettség alá nem eső adatkezelések azért mentesülnek a bejelentési kötelezettség alól, mert az adatkezelés célja egyrészt az érintett számára ismert és az adatfelvétel közvetlenül tőle történik, másrészt célja az érintett személyes érdekén túlmutat, vagy ki sem kerül a személyes szférából. Némely kivétel esetében az adatkezelés szorosan kötődik az adatkezelő működéséhez, és a személyes adatok kezelése az érintettel fennálló jogviszonyhoz, vagy szolgáltatáshoz kapcsolódik, más esetekben a személyes adatok kezelése közérdeket szolgál, vagy a cél teljesüléséhez a személyes jelleg megőrzésére csak az adatkezelés meghatározott szakaszában van szükség.

A legtöbb problémát az Avtv. 30. §-ában meghatározott kivételek pontos értelmezése okozza. Ezen belül leginkább az a) pontban szabályozott ügyfélkapcsolatban álló személyek kifejezés értelmezhető nehezen a bejelentők számára. Az iroda gyakorlata szerint az ügyfélkapcsolat – mint a bejelentési kötelezettség alóli kivétel – akkor áll fenn, ha az adatkezelés az adatkezelő és az érintett között fennálló jogviszony szükségszerű eleme. Egy internetes portálon történő regisztrációval például önmagában nem jön létre jogviszony. A regisztráció céljának megfelelően azonban már létrejöhet olyan konkrét jogviszony, amely ügyfélkapcsolatot eredményez, így például webáruház működtetésével adás-vételi jogviszony. A jogviszony teljesítéséhez szükségszerűen kapcsolódó adatkezelést az adatvédelmi nyilvántartásba nem kell bejelenteni (például számlázás), be kell azonban jelenteni azt az adatkezelést, melynek

célja nem közvetlenül kapcsolódik a szolgáltatás nyújtásához (például fórum), illetve az olyan adatkezelést, amely a jogviszony teljesítésén túl mutat (például adatok tárolása reklámanyag továbbítása céljából).

Az Avtv. 30. § a) pontjában meghatározott kivételek között megjelölt esetekben is be kell jelenteni az adatkezelést az adatvédelmi nyilvántartásba, ha az adatokat az adatkezelő más személy, vagy szerv részére hozzáférhetővé teszi, nyilvánosságra hozza, vagy egyébként az eredetitől eltérő célra használja fel.

Az Avtv. 30. § b) pontjában szabályozott kivétellel kapcsolatban is voltak értelmezési problémák. Nem kell bejelenteni az adatvédelmi nyilvántartásba az olyan adatkezeléseket, amelyet az egyház, vallásfelekezet tagjairól, a tagok által az egyházban betöltött funkcióiról vezet. Be kell azonban jelenteni a támogatókról, adományozókról vezetett nyilvántartást.

Az adatvédelmi nyilvántartásba történő bejelentés alól mentesülő adatkezelések közül még problémát okoz az Avtv. 30. § j) pontjában szabályozott, a természetes személy saját célját szolgáló adatkezelés értelmezése. E tekintetben megszorítóan kell értelmezni a törvényt. Csak olyan adatkezelés minősül a természetes személy saját célját szolgáló adatkezelésnek, amely során az érintettek tudtával kerülnek személyes adatok az adatot kezelő birtokába, azokat az adatbirtokos csak magán célra kezelheti.

Az adatvédelmi nyilvántartás tartalmi összetétele

A 2007. év végén az adatvédelmi nyilvántartás az alábbi fontosabb adatkezelő kategóriák szerinti összetétellel jellemezhető:

Minisztériumi, államigazgatási, állami intézmények mint adatkezelők:	431	
adatkezeléseik:		1.377
A magánszférába tartozó adatkezelők:	1.459	
adatkezeléseik:		3.665
Önkormányzatok mint adatkezelők:	3.244	
törvény által elrendelt és helyi adatkezeléseik		29.854

Az Adatvédelmi Biztos Irodája informatikai rendszerének korszerűsítése

Az előző évi beszámolókban felhívtuk a figyelmet, hogy az elhasználódott számítástechnikai eszközök cseréje a adatvédelmi nyilvántartás, illetve az iktatási rendszer szolgáltatása biztonságának érdekében halaszthatatlanná vált.

A szükséges berendezések nagyobb része 2006-ban végül is leszállításra került, viszont a megújulást biztosító, új platformra való áttérést lehetővé tevő adatbázis kezelő szoftver beszerzése anyagi eszközök hiányában továbbra is meghiúsult.

Végül is a szükséges programrendszer 2006 év végén megrendelésre került, és 2007 I. félévében a várakozásnak megfelelően le is szállították.

Az operációs rendszer felváltásához és az ezzel kompatibilis adatbázis kezelő platformra váltáshoz szükséges feltételeket biztosító számítógépi (hardware) korszerűsítéseket a biztos informatikus munkatársai a 2007. évben folyamatosan végezték. Az Adatvédelmi Biztos Irodája számítóközpontjának elektro-mechanikai kialakítását is önerőből, saját szakembereivel végezte az iroda.

Az adatbázis fejlesztéséhez és üzemeltetéséhez saját fejlesztői hálózatot alakítottunk ki. E hálózat segítségével az adatbázis kezelő rendszer beérkezése után már lehetségessé vált a szoftver migrációs fejlesztések elkezdése.

Az adatvédelmi biztos megújított honlapja

Az üzemeltetési tapasztalatok

2006. január 2-ával egy megújult multimédiás honlap jelentkezett a http://abiweb.obh.hu/abi/ címen, mint az adatvédelmi biztos megújított honlapja. A honlap iránt érdeklődők széles körből kerültek ki, hiszen az adatvédelmi biztoshoz minden olyan magán-, vagy jogi személy fordulhat, aki Magyarország területén tartózkodik. Így elvileg mindenkihez szól, aki hazánkban tevékenykedik és rendelkezik bármilyen Internet hozzáféréssel.

Az iroda szakértői az elektronikus információszabadságról szóló 2005. évi XC. törvény (továbbiakban: Eisztv.) előírásainak megfelelően az új honlapon lehívható, interaktív kitöltést biztosító közérdekű adat igénylő űrlapot fejlesztettek ki. Ezen az elektronikus űrlapon a közérdekű adat iránti igény az Adatvédelmi Biztos Irodája honlapján keresztül (http://abiweb.obh.hu/abi/, www.obh.hu – Adatvédelmi Biztos) benyújtható.

A hozzánk eljuttatott vélemények azt tükrözik, hogy az olvasható információkat kiegészítő vizuális (grafikus és/vagy animációs) elemek alkalmazása tetszést aratott, miközben sikerült elérni, hogy a honlap navigációja egyértelmű, megjelenése egységes maradt, amit továbbra is az animációs elemekből épülő menüs megjelenés segít.

Továbbfejlesztettük azokat a lehetőségeket, amelyek biztosítják, hogy a honlap egyes főbb fejezeteiben és főmenü pontjaiban részenkénti, valamint az egészében összetett keresést is lehessen végezni. A 2007. év tapasztalatai is azt mutatják, hogy honlapunk szerkezetében is alkalmas a társadalom egyes rétegeiben a személyes adatok védelme valamint a közérdekű adatok nyilvánossága iránt megnyilvánuló különböző mélységű érdeklődés kiváltására.

Az új honlap látogatottsága 2007-ben

Egyre komolyabb szerepet tölt be a magyar államigazgatási ügyintézésben az elektronikus ügyintézés, így az Adatvédelmi Biztos Irodájának honlapja is egyre nagyobb látogatottságot kapott az elmúlt időszakban. Az adatkezelők adatvédelmi nyilvántartási bejelentkezési kötelezettségeinek teljesítése érdekében is használják a biztos honlapját mind a letölthető útmutató anyagok, mind a kitöltendő űrlapok lehívása tekintetében.

Ez tükröződik a honlap látogatottsági mutatóiban is. Míg a 2006 évben a honlap iránt 80.440 alkalommal érdeklődtek, addig az új tervezésű adatvédelmi biztosi honlapra a 2007. év folyamán lényegesen több rákérdezés történt. (A pontos szám meghatározása azért nehézkes, mert a mesterséges intelligencián alapuló, hálózati keresést segítő rendszerek (például Google) a napi meghatározhatatlan ráfutási gyakoriságukkal torzítják a hozzáférések tranzakciós számlálójának értékét.)

Az adatvédelmi biztos angol nyelvű honlapjának megújítása

A magyar nyelvet nem ismerő érdeklődők a honlap angol változatát látogathatták, aminek tartalma nem egyezik meg teljesen a magyar oldalakéval. A külső megjelenése is a magyar nyelvű honlap előző változatának megfelelő kialakítású volt. Mint már említettük, az adatvédelmi biztos honlapja a folyamatos fejlesztéseknek köszönhetően 2006-ban új külsővel és változatlan minőségű bővített szakmai tartalommal vált hozzáférhetővé az internetes látogatók számára. A 2007. évben ezt követte a honlap angol nyelvű változatának a magyar nyelvűhöz való közelítése.

Az új angol nyelvű honlap bejelentkező oldala az alábbi ábrán látható:

Az angol nyelvű honlap szerkesztése, külső megjelenésének kialakítása érdekében tanulmányoztuk más külföldi adatvédelmi felügyelő hatóságok honlapjait. Több szempontot tartottunk szem előtt a fejlesz-

tésnél azért, hogy könnyen, felhasználó-barát módon, mégis esztétikusan, és ami talán a leglényegesebb, az idegen nyelvet beszélő látogatók számára is a leghasznosabb információkkal feltöltve tegyük lehetővé a honlap olvasását. A fő elvként az szolgált, hogy követni és megtartani kellett a magyar honlap arculatát. Ehhez társult, hogy a honlap szerkezeténél olyan fő címeket, tartalmakat vettünk tekintetbe és helyeztünk el, amelyek tapasztalataink szerint segíteni fogják szakmabeli munkatársaink és minden érdeklődő személy, legyen az valamely állampolgár vagy gazdasági társaság, munkáját.

Az elektronikus iktatási rendszer (ELIK) továbbfejlesztése

Tevékenységünk átláthatósága, a vizsgált ügyek közérdekűsége, a biztosi tevékenységről történő beszámoltatási kötelezettségnek való árnyaltabb megfelelés érdekében az iroda szakértői folyamatos fejlesztői tevékenységgel bővítik az Elektronikus Iktatási Rendszer lehetőségeit. Az elkészített programoknak köszönhetően az aktát kísérő adatlap az eddigi kézi kitöltés helyett az iktatási rendszerből automatikusan készül el. Ezen túl kifejlesztettük az Adatvédelmi Biztos Irodájának digitális irattárát, mely a bejövő és a kimenő dokumentumok tárolására szolgál az iktatási rendszer hálózati szerverén.

B) Az elutasított kérelmek nyilvántartása

Az adatvédelmi biztos jogkörében eljáró állampolgári jogok országgyűlési biztosa 2007-ben, a Magyar Közlöny 186. számában megjelent felhívással fordult az adatkezelőkhöz, melyben a személyes adatok kezelésével kapcsolatos elutasított kérelmek és a közérdekű adatok megismerésére irányuló elutasított kérelmek bejelentésére hívta fel ismételten az adatkezelők figyelmét.

Személyes adat iránti kérelmek elutasítását minden adatkezelőnek, közérdekű adat iránti kérelmek elutasítását pedig a közfeladatot ellátó szerveknek kell bejelenteniük. A korábbi felhívásokban is felkértük az adatkezelőket, – annak ellenére, hogy a törvény ilyen kötelezést nem tartalmaz – hogy a teljesített kérelmekről is adjanak tájékoztatást, hiszen ennek ismeretében kísérhető figyelemmel az információszabadság alkotmányos jogának érvényesülése. A személyes adatok kezelésével kapcsolatos elutasított kérelmek esetében a törvény csak az érintett felé ír elő indoklási kötelezettséget, az adatvédelmi biztos felé nem. A közérdekű adatokra vonatkozó kérelmek elutasítása esetében ezzel szemben a törvény előírja, hogy az érintett írásbeli tájékoztatásán túl az adatkezelő köteles az éves jelentésében az adatvédelmi biztost értesíteni az elutasított kérelmekről, és annak indokairól. A részben teljesített kérelmek esetében is fennáll a jelentési kötelezettség a részben elutasított kérelemre, illetve annak indokára nézve.

Az elutasított kérelmek bejelentésére külön formanyomtatvány nincs. Az Avtv. rendelkezéseinek értelmében statisztikai adatokat kell az adatvédelmi biztosnak jelenteni, vagyis azt, hogy az elmúlt évben hány személyes adat iránti kérelem érkezett az adott adatkezelőhöz és ebből mennyit utasítottak el; illetve, hogy hány közérdekű adat iránti kérelem érkezett az adott szervhez és ebből mennyit utasítottak el, illetve mi volt az elutasítás indoka. Sajnos az évről évre ismétlődő felhívások ellenére még mindig kevés, és azon belül is sok pontatlan jelentés érkezik.

Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett, általa kezelt adatairól. A tájékoztatást az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban megadni. Az érintett tájékoztatását az adatkezelő csak a törvényben szabályozott esetekben tagadhatja meg. A tájékoztatás

megtagadása esetén az adatkezelő köteles az elutasítás indokát is közölni. *„Az elutasított kérelmekről az adatkezelő az adatvédelmi biztost évente értesíti."* (Avtv. 13. § (3) bekezdés)

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerveknek és személyeknek lehetővé kell tenniük, hogy a kezelésükben lévő közérdekű adatot bárki megismerhesse. A közérdekű adat megismerése iránt bárki – szóban, írásban vagy elektronikus úton – igényt nyújthat be. A közérdekű adat megismerésére irányuló igénynek az igény tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül kell eleget tennie az adatkezelőnek. Az igény teljesítésének megtagadásáról, annak indokaival együtt, 8 napon belül értesíteni kell az igénylőt. *„A fent említett szervek évente értesítik az adatvédelmi biztost az elutasított kérelmekről, valamint az elutasítás indokairól."* (Avtv. 20. § (9) bekezdés)

Személyes adatok kezelésével kapcsolatos elutasított kérelmek nyilvántartása.

2007-ben összesen 283.570 személyes adat iránti kérelmet nyújtottak be, 139 különböző adatkezelőhöz, ebből 1768 személyes adat iránti kérelmet utasítottak el.

2007-ben 100 önkormányzati szervhez összesen 40.207 személyes adat iránti kérelmet nyújtottak be, ebből 191 kérelmet utasítottak el.

	2005	2006	2007
Jelentést küldők száma	498	446	381
Személyes adat iránti kérelem	315.818	212.871	283.570
Elutasított kérelmek	168	422	1768

35 különböző állami szervhez 2007-ben összesen 95.439 személyes adatok iránti kérelmet nyújtottak be, ebből 1.567 kérelmet utasítottak el.

2007-ben a privát szférából 4 társaság jelentett adatkérést az adatvédelmi biztos számára, összesen 147.924 személyes adat iránti kérelmet, ebből 10 kérelmet utasítottak el.

Láthatjuk, hogy a jelentések számát tekintve szinte semmi változás nem történt az elmúlt évekhez képest. A jelentések számában mutatkozó bizonyos fokú csökkenést az okozta, hogy több állami szervtől központilag összesített jelentéseket kaptunk. Évről–évre ugyanazon adatkezelők tesznek eleget bejelentési kötelezettségüknek. A magán adatkezelők között csökkent a bejelentést tevők száma, így még mindig nagyon kevés jelentés érkezik a tényleges adatkezelői számhoz viszonyítva. Megfigyelhető továbbá, hogy az állami szervekhez érkezett személyes adat iránti kérelmek száma csökkent, az elutasítások száma viszont ennek ellenére megnégyszereződött.

Az elutasítás indokai között továbbra is leggyakoribb az illetékesség hiánya, illetve az, hogy a kérelmező nem saját adat megismerésére irányuló kérelmet nyújtott be. Sokszor azért történik a kérelem elutasítása, mert a kérelem pontatlan. Probléma lehet továbbra is az adatszolgáltatás fizikai teljesíthetősége. Ilyen például, hogy az érintett adatainak helyesbítésére irányuló kérelem azért nem teljesíthető, mert a kezelt adatok helyesek, vagy hogy a szerv a kérelmezővel kapcsolatban adatot nem kezel. Továbbra is számot adunk olyan elutasításokról, ahol az elutasítás indoka nemzetbiztonsági ok, illetve bűnüldözési ok.

Közérdekű adatok megismerésére irányuló elutasított kérelmek nyilvántartása.

2007-ben összesen 179.192 közérdekű adat megismerésére irányuló kérelmet jelentett be 62 adatkezelő, ebből 89 kérelmet utasítottak el.

	2005	2006	2007
Jelentést küldők száma	498	442	381
Közérdekű adatok megismerésére irányuló kérelmek	129.984	183.959	179.192
Elutasított kérelmek	25	466	89

40 önkormányzati szervhez 2007-ben összesen 4.789 közérdekű adat megismerésére irányuló kérelmet nyújtottak be, ebből 12 kérelmet utasítottak el.

22 különböző állami szervhez 2007-ben összesen 174.403 közérdekű adat megismerésére irányuló kérelmet nyújtottak be, ebből 77 kérelmet utasítottak el.

2006. január 1-jén lépett hatályba az elektronikus információszabadságról szóló törvény, melynek célja annak biztosítása, hogy a közvélemény pontos és gyors tájékoztatása érdekében a közérdekű adatokat elektronikus úton bárki számára személyazonosítás és adatigénylési eljárás nélkül, folyamatosan és díjmentesen közzétegyék.

Ez a tény a jelentések számát tekintve a közérdekű adatok megismerésére irányuló elutasított kérelmek tekintetében nem okozott jelentős változást. A majdnem azonos számú bejelentőhöz azonban az elmúlt két évben lényegesen nagyobb számú közérdekű adat megismerésére irányuló kérelem érkezett. Figyelemre méltó, hogy a kérelmek számának növekedése ellenére az elutasítások száma lényegesen csökkent 2006-hoz képest.

A közérdekű adatok megismerésére irányuló kérelmek elutasításának legfőbb indokai, hogy a kért adat az adatkezelő szerv kezelésében nem található, illetve, hogy a közérdekű adat belső használatra készült, vagy döntés-előkészítéssel összefüggő adat, vagy államtitokká minősített adat.

Az évről évre megismétlődő felhívások ellenére csak az adatkezelők egy része – rendszerint ugyanazok az adatkezelők – tesznek eleget törvényi kötelezettségüknek. Ennek következtében a bejelentett adatmennyiségből nem tudunk pontos következtetéseket levonni.

V. FÜGGELÉK

A 2006. évi beszámoló parlamenti fogadtatása

Az adatvédelmi biztos 2006. évi tevékenységéről szóló beszámolót a Magyar Köztársaság Országgyűlése 2007. április 25-ei ülésnapján 254 igen, 14 nem szavazattal, 53 tartózkodás mellett elfogadta.

Az iroda szervezete és gazdálkodása

Az Adatvédelmi Biztos Irodájánál – a 2007. december 31-i állapot szerint – 42 főállású és 3 mellékfoglalkozású munkatárs dolgozik. Az alábbiakban a 2007. év kiadásainkat mutatjuk be. (a közölt adatok ezer forintban értendőek)

Az Adatvédelmi Biztos Irodájának 2007. évi közvetlen működési kiadásai

Személyi kiadások:	
Illetmények	203.081
Jutalom	19.075
Jubileumi jutalom	6.875
Napidíj	1.943
Megbízási díj	4.080
Felmentés, végkielégítés	13.787
Költségtérítések	13.248
Egyéb juttatások	6.905
Személyi kiadások összesen	**268.994**
Munkáltatót terhelő járulékok	**82.554**
Dologi kiadások:	
Külföldi kiküldetés	6.603
Reprezentáció	1.306
Készletbeszerzés, telefonköltség	2.503
Gépkocsi üzemeltetés	3.013
Nyomda	1.032
Fordítás, lektorálás, megbízás	721
Áfa és egyéb kiadások	8.146
Dologi kiadások összesen:	**23.324**
Beruházási kiadások	**7.302**
Összes kiadás*:	**382.174**

* Az összes kiadás nem tartalmazza az Adatvédelmi Biztos Irodája általános üzemeltetési kiadásait, azok az országgyűlési biztosok közös Hivatalának kiadásaiban jelennek meg.

A beszámolóban előforduló jogszabály-rövidítések jegyzéke

- a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény: *Avtv., adatvédelmi törvény*
- a közúti közlekedési nyilvántartásról szóló 1999. évi LXXXIV. törvény: *Kknyt.*
- a Rendőrségről szóló 1994. évi XXXIV. törvény: *Rtv.*
- a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény: *Bvsztv.*
- a büntetőeljárásról szóló 1998. évi XIX. törvény: *Be.*
- az adózás rendjéről szóló 2003. évi XCII. törvény: *Art.*
- a hulladékgazdálkodásról szóló 2000. évi XLIII. törvény: *Hgt.*
- a helyi önkormányzatokról szóló 1990. évi LXV. törvény: *Ötv.*
- a nemzeti és etnikai kisebbségek jogairól szóló 1993. évi LXXVII. törvény: *Nektv.*
- a szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény: *Sztv.*
- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény: *Eüak.*
- a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény: *Ebtv.*
- a bűnügyi nyilvántartásról és a hatósági erkölcsi bizonyítványról szóló 1999. évi LXXXV. törvény: *Bnytv.*
- a Büntető Törvénykönyvről szóló 1978. évi IV. törvény: *Btk.*
- a Munka Törvénykönyvéről szóló 1992. évi XXII. törvény: *Mt.*
- a felsőoktatásról szóló 2005. évi CXXXIX. törvény: *Ftv.*
- az elektronikus hírközlésről szóló 2003. évi C. törvény: *Eht.*
- a biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény: *Bit.*
- a büntetések és az intézkedések végrehajtásáról szóló 1979. évi 11. törvényerejű rendelet: *Bvtvr.*
- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény: *Ltv.*
- a társasházakról szóló 2003. évi CXXXIII. törvény: *Tht.*

- az elektronikus információszabadságról szóló 2005. évi XC. törvény: *Eitv.*
- az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény: *Obtv.*
- a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény: *Ket.*