

A privacy védelme a munkahelyen

Szabó Máté Dániel — Székely Iván*

Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1832, Fax: (36 1) 463-4035
e-mail: szabomat@szabomat.hu, szekelyi@ceu.hu

Absztrakt

A munkahely olyan környezet, ahol a munkavállaló a munkaidejét, munkaerejét, kreativitását a munkáltatója által meghatározott célok megvalósítására fordítja, ugyanakkor nem válik személyiség nélküli robottá, nem adja fel személyes integritását, sőt magánéletének egyes eseményei is szükségképpen a munkahelyen történnek. Emiatt a munkahely mintegy gyűjtőhelye a különféle privacy- és adatvédelmi problémáknak, jogok és érdekek ütközésének. A tanulmány¹ először a privacy-védelem és az adatvédelem magyarországi sajátosságait elemzi, rámutatva a bírósági jogérvényesítés csekély súlyára és az adatvédelmi biztos joggyakorlatának fontosságára, majd a munkahelyi privacy védelmének problémáit az adatvédelmi biztos vizsgálataiból és állásfoglalásaiból válogatva, ügyismertetések segítségével mutatja be. Az ismertetett ügyek négy csoportját a munkaerő-felvétellel, a munkavégzés ellenőrzésével, a munkavállalók személyiségének elemzésével kapcsolatos, illetve az ésszerű adatkezelési cél nélküli esetek alkotják. A tanulmány záró fejezetében a szerzők a magyarországi munkahelyi privacy helyzetének általános értékelését adják, kitérve a politikai rendszerváltás által indukált társadalmi átalakulásokra és a hatalmi viszonyok változásaira egy olyan tágabb kontextusban, ahol a munkahely része az információs és egyben hatalmi játéktérnek.

* Dr. Szabó Máté Dániel, jogász, adatvédelmi szakértő, a BME GTK Információ- és Tudásmenedzsment Tanszék külső előadója. Dr. Székely Iván, társadalmi informatikus, adatvédelmi szakértő, a BME GTK Információ- és Tudásmenedzsment Tanszék docense.

¹ A tanulmány alapjául szolgáló kutatást a Nyílt Társadalom Archivum támogatta.

1. A privacy-vel kapcsolatos jogérvényesítés jellegzetességei

A munkahelyi privacy² védelmének tapasztalatait összegző írás elején magyarázatot igényel e jogvédelem két jellegzetessége. A jogesetek ismertetésében egyrészt igen erősen összemosisódik a privacy és az adatvédelem fogalomrendszere, a privacy védelme a személyes adatok védelmének eszközrendszerével történik. A másik szembeszökő jellegzetessége a hazai privacy-védelemnek, hogy az ezzel kapcsolatos bírósági ítéletek száma igen csekély, és ez nemcsak a munka világában van így. A jogérvényesítés lehetséges módjai közül a jogukat érvényesíteni kívánó személyek, akik úgy érzik, megsértették jogaikat, választhatnak, és választásukat nagyban befolyásolják a jogérvényesítésre szolgáló intézmények jellemzői. Általánosságban elmondhatjuk, hogy azok, akik úgy érzik, megsértették magánszférájukat, ritkán fordulnak bírósághoz.

Az első jellegzetesség alkotmányjogi és alkotmány-történeti okokra vezethető vissza. A privacy védelméhez nagymértékben kapcsolódó személyes adatok védelméhez való jognak az Alkotmány alapjogi katalógusában való megjelenése³ a rendszerváltozás idején különös jelentőséggel bírt, az állam mindenhatósága és mindent látó volta lebontásának egyik eszköze volt, hogy alkotmányi szinten biztosították a polgárok számára az átláthatatlanságot. A személyes adatok védelméhez való jog alkotmányi szinten történt biztosítását egy igen szigorú adatvédelmi szabályozás⁴ követte, amely az önrendelkezési jog koncepcióját tette magáévá, és egyaránt vonatkozott a magán és az állami adatkezelőkre, nem zárta ki hatályát a magánemberek adatkezelési tevékenységére nézve sem. Széles körben határozta meg a személyes adatok fogalmát, így alkalmassá vált a polgárokkal kapcsolatos mindenfajta ismeretszerzés, megfigyelés, más módon történő háborgatás visszaszorítására. A szigorú szabályozás betartásának ellenőrzésére, a polgárok panaszainak kivizsgálására és orvoslására pedig a jogalkotó létrehozott egy hatékony intézményt, az adatvédelmi biztos és hivatala feladata az adatvédelem szabályainak érvényesülése felett való őröködés. Emellett a jogalkotó megnyitotta a bírói utat is az adatvédelmi szabályok megsértésének esetére, sőt, az adatalányok jogvédelmét különleges garanciákkal igyekezett elősegíteni, amelyekről a későbbiekben még szólunk. Az elmúlt tíz évben tapasztaltak azt mutatták, hogy a magánszféra megsértése esetén az adatvédelmi jog és az adatvédelmi biztos tud a maga speciális eszközeivel jogvédelmet biztosítani.

² A magyar nyelvben a *privacy* szónak nincs pontos megfelelője, többnyire „magánélet”-nek fordítják, ami az eredeti jelentésénél szűkebb, és csupán a személyes intimitások körét jelöli. A privacy a személyes magánszféra egészét, integritását jelölő fogalom, amelynek ma meghatározó eleme a személyes adatok feletti önrendelkezés.

³ A személyes adatok védelmét biztosító 59. § (1) bekezdés az Alkotmány 1989-ben történt átfogó módosításakor került az alaptörvénybe.

⁴ A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

A magánszférához való jog egyébként az Alkotmányban külön nem nevesített jog, az emberi méltósághoz való jogból, mint általános személyiségi jogból levezetett alapjog, amelynek védelmét a jogrendszer egyes ágaiban sajátos eszközökkel látta jónak megvalósítani a jogalkotó. A magánszféra elleni legsúlyosabb cselekmények büntetőjogi elismerését számos büntetőtörvényi tényállás jelenti, a személyiség polgári jogi védelmét pedig a Polgári Törvénykönyvben megfogalmazott általános és egyes nevesített személyiségi jogok biztosítása valósítja meg. Az Alkotmány adatvédelmi szakaszának végrehajtására megalkotott adatvédelmi törvény azonban ezeknél hatékonyabb jogvédelmet kínál, és általánosságban elmondható, hogy az Alkotmány alapjogi katalógusában a személyes adatok védelméhez való jog a normatív szinten legjobban és legpontosabban definiált alapjog.

A magyar adatvédelmi jog — az európai trendnek megfelelően — az általános törvény-szektorális törvény szabályozási modelljét követi, amelyben az adatvédelem legfontosabb elveit, a személyes adatok védelméhez való jog korlátozásának feltételeit, védelmének garanciáit egy úgynevezett általános törvényben találjuk. E törvény általában nem tartalmaz kifejezett felhatalmazásokat adatkezelésre. Az egyes adatfajtákra, illetve adatkezelőkre kötelező rendelkezéseket, az ő adatkezelésükre vonatkozó felhatalmazásokat a szektorális törvények tartalmazzák. Ilyen törvények nélkül az általános törvényben foglaltak nem érvényesülhetnek megfelelően, az abban elvi szinten megfogalmazottak csak minimális mértékben valósulnak meg a gyakorlatban. Szektorális szabályozás elsősorban egyrészt a különösen érzékeny adatok kezelésére feljogosított, másrészt a nagyszámú érintett adatait kezelő vagy olyan adatkezelőkre nézve szükséges, amelyek a velük szemben kiszolgáltatott helyzetben lévők személyes adatait kezelik. Annak ellenére, hogy a munkáltató oldalán az információs hatalom túlsúlya, illetve a munkavállaló számára hátrányos, egyenlőtlen kommunikációs helyzet e szektort az információs szabadsá jogok érvényesülése egyik kritikus területévé teszi, tehát kifejezetten indokolt lenne adataik kezelésére nézve speciális törvényi garanciákat meghatározni, a jogrendszerben a munkavállalók privacy-jét vagy személyes adataikat nem védi szektorális törvény.⁵ Sem a munka világát kódexként szabályozó Munka Törvénykönyve, sem más szektorális jogszabály nem szól a munkavállalók privacy-jének védelméről, a Munka Törvénykönyve jószerivel egyetlen adatkezelési normája csupán a munkaerő-felvétellel kapcsolatban határoz meg egy szabályt, amikor a következőképpen rendelkezik: a munkavállalótól csak olyan nyilatkozat megtevéle vagy adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely személyiségi jogait nem sérti és a munkaviszony létesítése

⁵ Az első adatvédelmi biztos, Majtényi László ezért tekinti súlyos mulasztásnak, hogy a hazai szektorális adatvédelmi jogalkotás nem fordít kellő figyelmet e terület szabályozására. *Az adatvédelmi biztos beszámolója, 1997.* 93. oldal.

szempontjából lényeges tájékoztatást nyújthat.⁶ Ez a rendelkezés tehát nem tesz mást, mint az adatvédelem célhoz kötöttségi elvét konkretizálja egy meghatározott élethelyzetre, valamely munkakör betöltésére jelentkező pályázók közüli választásra. Speciális szabályozás hiányában⁷ az adatvédelem általános szabályai alkalmazandók a munka világában történő adatkezelésre, és a fentebb kifejtettek alapján a privacy-védelem jelentős részére is.

A másik jellegzetesség a bírósági jogérvényesítés gyakorlati jelentőségének csekély volta. Az Alkotmány szerint az alapvető jogok megsértése miatt keletkezett igények, továbbá a kötelességek teljesítésével kapcsolatban hozott állami döntések elleni kifogások bíróság előtt érvényesíthetők.⁸ A bíróságok azonban e rendelkezés alapján alapjogi bíraskodást nem folytatnak, vagyis közvetlenül és kizárólag az Alkotmányra hivatkozva hatósági határozatok, intézkedések ellen nem lehet sikerrel rendes bírósághoz fordulni. A rendes bíróságok helyett az alapjogokat közvetett módon, vagyis azáltal védik, hogy az azokat is érvényesítő jogszabályokat — így például az egyes alapvető jogokról szóló külön törvényeket, a Polgári Törvénykönyvet vagy a Büntető Törvénykönyvet — alkalmazzák.⁹ A bíróságok, mivel direkt alapjogi bíraskodást nem folytatnak, igen ritkán alkalmazzák közvetlenül az Alkotmányt, így ritka az is, hogy ítéleteikben alaptörvényi rendelkezéseket, alapjogokat értelmeznének. Sajátos következménye a privacy-védelem több jogágban való, párhuzamos megvalósulásának, hogy a bíróságok nem szívesen alkalmazzák az Alkotmány rendelkezéseit közvetlenül kibontó adatvédelmi törvényt sem, általában idegenkednek az alkotmányjogi szabályok alkalmazásától is, sokkal szívesebben alkalmazzák a sokkal alacsonyabb szintű védelmet biztosító Polgári Törvénykönyvet, amelyben otthonosabban mozognak. És bár mind az adatvédelmi törvény, mind a Polgári Törvénykönyv oltalmazza a személyiséget a személyes adatok védelme útján, más dogmatikával, így más eredménnyel teszi. A polgári jogi értelemben vett adatvédelem hagyományos személyiségi jogként, védelmi jogként fogja fel az adatvédelmet, vagyis a Ptk. alapján védeni kell a személyiségi jogokat a jogosulatlan megismerés ellen. Alkotmányjogi értelemben viszont ez a jog aktív, önrendelkezési jog, az adatvédelmi törvény pedig ebben a szellemben készült. Ez utóbbi jogi tartalom magasabb szintű jogvédelmet nyújt az egyén számára.

Az adatvédelmi szabályok e ritka alkalmazása sem mutat egységes bírói jogértelmezést. A személyes adatok védelmével kapcsolatos bírósági ítéletek igen gyakran egymásnak

⁶ 77. § (1) bekezdés.

⁷ Az igazsághoz hozzátartozik, hogy a munkajogban vannak adatvédelmi tartalmú egyéb rendelkezések is, ám ezek nagyon speciális élethelyzetekre, zömmel egészségügyi adatkezelésre vonatkoznak.

⁸ 70/K. §.

⁹ *Az Alkotmány magyarázata*. Budapest, 2003, KJK-KERSZÖV Jogi és Üzleti Kiadó. 707–709. oldal. Halmi Gábor és Tóth Gábor Attila (szerk.): *Emberi jogok*. Budapest, 2003. Osiris Kiadó. 224–225. oldal.

ellentmondó következtésekre jutnak ugyanazon szabályok értelmezésekor, így a ritka adatvédelmi ítékezés is meglehetősen kiszámíthatatlan. A lassú és költséges, valamint a tapasztalatok szerint kiszámíthatatlan bírói út helyett a polgárok jogvédelemért elsősorban az adatvédelmi biztoshoz fordulnak, aki az adatvédelmi szabályok általános szinten megfogalmazott rendelkezéseit, amelyek inkább elvek, mint megszokott normatív rendelkezések, értelmezi, és joggyakorlatának eredménye egy olyan esetjog, amely a jogalanyok számára irányt mutat a jogszabályok alkalmazása tekintetében. Az adatvédelmi biztos gyakorlata tehát a bíróságok jogalkalmazását pótló esetjoggá vált az elmúlt évtizedben.¹⁰

A munka világában megfigyelhető szellős adatvédelmi szabályozás szintén magyarázatul szolgál arra, hogy miért nincsen a munkahelyi adatkezelés tárgyában jogerős bírói ítélet. A kiszolgáltatott munkavállaló valószínűleg „munkajogi mankókkal” is ódzkodna a pereskedéstől. A kemény munkajogi adatkezelési szabályozás hiánya látsen bátorítást jelent az erőfölényben levő munkáltatónak és a munkaügyi ellenőrzést sem ösztökéli a terület vizsgálatára.¹¹

Míndezek alapján a munkahelyi privacy-védelmi esetek ismertetésénél az adatvédelmi biztos joggyakorlatára koncentrálunk, tekintettel arra, hogy nincs olyan nyilvános bírósági jogeset, amely alkalmas lenne az elemzésre.

2. Ügyismertetések

A munkahelyi privacy-védelemmel kapcsolatos jogesetek áttekintésekor a jogeseteket négy témakör köré csoportosítottuk. A csoportosítás alapja a munkáltatók sajátos célja. Először azokat az ügyeket tekintjük át, amelyek a munkaerő-felvétellel kapcsolatosak, amelyek esetében a leendő munkavállalók privacy-jének megsértése a munkáltató azon célja elérése érdekében történik, hogy a számára legkedvezőbb tulajdonságokkal rendelkező személyt válassza a jelentkezők közül. A munkáltatók sokféleképpen próbálják ellenőrizni, mivel töltik el a dolgozók a munkaidejüket, a második esetkörben ezekkel az ügyekkel foglalkozunk. A harmadik ügýtípust a már munkaviszonyban álló alkalmazottak személyiségének mélyreható, esetleg a múltban történt események munkáltató általi felderítésének céljával elvégzett vizsgálatával kapcsolatos ügyek jelentik. Végül olyan privacy-sértő munkáltatói intézkedésekkel foglalkozunk, amelyeknek indokául nem tudunk ésszerű célt megjelölni.

¹⁰ Sólyom László: Az ombudsman „alapjog-értelmezése” és „normakontrollja”. In: Majtényi László (szerk.): *Az odaátra nyíló ajtó — The Door onto The Other Side*. Adatvédelmi Biztos Irodája, Budapest, 2001. 95. oldal.

¹¹ Schiffer András: Az egészségügyi adatkezelés anomáliái a munka világában. In: Szabó Máté Dániel (szerk.): *Védett adataink*. Társaság a Szabadságjogokért, Budapest, 2003.

2.1. Munkaerő-felvétel

A polgárok privacy-jét sértő cselekmények jelentős része a munka világában nem a már fennálló munkaviszony keretében történik, hanem a munkavégzésre irányuló jogviszony létrehozatala előtt álló, valamely állásra pályázó személyek jogainak megsértésével kapcsolatos. Az ügyeket áttekintve általában a következő kérdések merülnek fel: milyen személyes adatokat kérhet a munkáltató a leendő alkalmazottjától, milyen körülmények között kell azokat tárolni, illetve mi lesz a felvett személyes adatok sorsa a munkaviszony létrejötte vagy annak meghiúsulása esetén. Az első kérdésre a legnehezebb választ adni, mert a kérhető információk körét csak az adott munkakör ismeretében, esetenként lehet meghatározni. A Munka Törvénykönyvének már említett rendelkezése szerint a munkavállalótól csak olyan nyilatkozat megtétele vagy adatlap kitétele kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely személyiségi jogait nem sérti, és a munkaviszony létesítése szempontjából lényeges tájékoztatást nyújthat. Ez nem más, mint egy célhoz kötöttségi szabály, konkretizálja az adatvédelem általános célhoz kötöttségi elvét. A munkáltatóknak joguk van ahhoz, hogy az egyes munkakörökre olyan személyeket alkalmazzanak, akik egyrészt rendelkeznek a szükséges képesítésekkel, másrészt — ha bizalmas, nagy felelősséggel járó munkakörrel van szó — olyan háttérrel bírnak, amely a lehetséges kockázati tényezőket kizárja, vagy legalábbis csökkenti azokat. A munkavállalók kiválasztásakor ezért a munkáltatóknak számos személyes adatra lehet szükségük. A törvény nem rögzíti pontosan a munkáltatók által kezelhető adatok körét, az Mt. már idézett rendelkezése azonban határt szab az adatkezelésnek, összhangban az adatvédelmi törvény által meghatározott célhoz kötöttség elvével.

2.1.1. Fejvadász cégek adatkezelése

Magyarországon is elmúlt már az az idő, amikor a munkaerőt kereső cégek táblákon, hirdetésekben maguk jelölték meg a betöltésre váró pozíciókat, majd az álláskeresőknak nem volt egyéb dolguk, mint bizonyítványukkal felkeresni a „személyzetist” és munkába állni. Az utóbbi években, ahogyan más európai országokban, úgy Magyarországon is az álláskereső és a munkaerő-kereső közé iktatódott a HR-vállalkozások (fejvadászok) egyre terebélyesedő piaca. A fejvadász cégek különféle tesztek alapján vizsgálódnak — többek között — az álláskeresők verbális intelligencia fokáról, kockázatvállalási hajlamáról, várható lojalitásáról.¹² Elterjedt gyakorlat, hogy a fejvadász cég az álláskeresők kartotékjait úgymond készletezi, s a kívánt célra megszerkesztett adatbázisként kínálja fel jól fizető és munkaerőt kereső ügyfeleinek. Nem utolsósorban, a fejvadász szakmai kompetenciájára

¹² Ép személyiség, mint alkalmazási feltétel. *Népszabadság*, 2001. november 30.

van bízva, hogy az álláskeresőről nyert személyiségkép hány, és melyik cégvezető asztalán landol.¹³

A munkajogi szabályozás ezzel a változással nem tart lépést, nem vesz tudomást a HR-piac differenciálódásáról. A munkajogi kódex egyetlen adatkezelési szabálya kifejezetten a munkaerő-felvételre vonatkozik, de csak a törvény kommentárja hívja fel a figyelmet arra, hogy adatkérő a munkáltató mellett a fejevadász is lehet, így a 77. § rájuk is vonatkozna.¹⁴ Az álláskereső személy által absztrakt módon körülírt keresett munkakör és a lehetséges munkáltató által megadott, betöltendő pozíció adat-szükséglete nem feltétlenül esik egybe. A fejevadász cégek sok esetben nem is hagyományos közvetítő funkciót töltenek be, hanem tanácsadóként működnek közre egy adott munkáltatónál, az ott felvételre jelentkezettek „szűrésében”.

Ebben a körben tipikus az az eset, amelyben egy álláspályázatra jelentkező személy néhány órával a felvételi beszélgetése után meggondolta magát a pályázati szándékát illetően, nem kívánt már az állásra pályázni, ezért a munkáltató által a beszélgetés alatt készített, személyes adatait tartalmazó feljegyzést visszakérte, kérését azonban nem teljesítették. Az interjú során az anyagi helyzetére és a lakáskörülményekre vonatkozó kérdéseket is feltettek a pályázónak, és ezeket is rögzítették. A cég jogi képviselője ebben az esetben azzal védekezett, hogy a személyes adatokat tartalmazó papírlapot az adatok felvevőjének azért nem állt módjában visszaadni, mert az más, álláshirdetésre jelentkező személyekre vonatkozó információkat is tartalmazott, az adatok felvételére és tárolására pedig az esetleges újbóli meghallgatás, illetve a munkaszerződés későbbi megkötése céljából került sor. Az adatvédelmi biztos felszólította a céget a feljegyzések megsemmisítésére, ezt teljesítették is. A biztos felhívta továbbá a cég képviselőjének figyelmét arra, hogy a személyes meghallgatás során kért, az anyagi helyzetre és a lakáskörülményekre vonatkozó személyes adatok kezelése ellentétes a célhoz kötöttség elvével. A biztos ugyanakkor felhívta a panaszos figyelmét arra, hogy az adatok átadása önkéntes, így hasonló helyzetben jogában áll azok szolgáltatását megtagadni.¹⁵

2.1.2. A hazugságvizsgáló használata

A munkavállaló magánszférájába a munkáltató részéről történő beavatkozás egyik legdurvább esete az, amikor a munkáltató hazugságvizsgáló készüléket alkalmaz a munkavállalók megbízhatóságának ellenőrzésére. Az adatvédelmi biztos által vizsgált

¹³ Schiffőr András: i.m.

¹⁴ A Munka Törvénykönyvének 77. §-ához fűzött kommentár. Villányiné dr. Bárány Anikó: Kommentár a Munka Törvénykönyvéről szóló 1992. évi XXII. törvényhez. *Complex CD Jogtár*.

¹⁵ 828/A/1999.

ügyekből kiderül, hogy a hazugságvizsgáló egyik felhasználási területe az újonnan felveendő, a munkakörre pályázó személyek megbízhatóságának vizsgálata. Ebben az esetben a leendő munkáltató vagy a pályázati feltételek között teszi közzé a hazugságvizsgálaton való részvételt, vagy nem így tesz, nem mint feltételt határozza meg a vizsgálatot, azt csak lehetőségként kínálja fel, de értelemszerűen választása arra a pályázóra esik majd, aki megfelelő eredménnyel ment át a vizsgán. A leendő munkáltató ezzel a rá nézve nagyobb veszélyforrást, a nagyobb humán kockázatot jelentő személyeket kívánja kiszűrni, valamint azokat, akik eleve azon szándékkal akarnak elhelyezkedni valamely munkakörben, hogy ott jogellenes cselekményeket követhessenek el. A hazugságvizsgáló készülékkel történő vizsgálatot mint szolgáltatást nyújtó cégek ez utóbbi célra hivatkoznak a poligráf civil alkalmazása létjogosultságának egyik bizonyítékaként, nevezetesen arra, hogy bűnmegelőző hatása van: ha a bűnelkövetésre hajlamos személyek nem kerülnek a bűnelkövetés számára kedvező pozícióba, kisebb az esélye annak, hogy bűncselekményt követnek el. Ez kétségtelen, bár azok a leendő munkáltatók, akik a vizsgálat elvégzéséért e cégeknek fizetnek, ezt saját érdekeik védelme, és nem az összбűnözés csökkentése érdekében teszik. A munkáltatónak joga van — bizonyos korlátok között persze — védeni saját érdekeit, nem feladata azonban a bűnmegelőzés, ez az eredmény ezért az ő tekintetében önmagában nem teszi jogszerűvé a poligráf alkalmazását.¹⁶

Egy hazugságvizsgálatot sérelmező beadvány alapján lefolytatott eljárásában kiadott állásfoglalásában az adatvédelmi biztos megengedhetőnek tartotta a betöltetlen munkakörre jelentkezők esetében a kockázati vizsgálat elvégzését, mivel ők valóban szabadon dönthetnek arról, alávetik-e magukat egy ilyen vizsgálatnak, vagy sem.¹⁷

2.1.3. Pszichológiai tesztek

A munkakörre jelentkezők magánszférájába való mély behatolásnak más módja is kiderül a biztos eseteiből. Az egyik hipermarket-lánchoz felvételre jelentkezőknek — egyebek mellett — vad- és háziállatok, mértani idomok, mitológiai alakok és mesefigurák képei közül kellett eldönteniük, hogy „mi tetszik és miért”. A pályázók által adott válaszokat elküldték a külföldi anyavállalathoz, ahonnan egy pszichológus az igen-nem válaszok mellett olyasmiket fűzött hozzá a szakvéleményhez, hogy az illető „megbízhatatlan” vagy „nem becsületes”. Az adatvédelmi biztos vizsgálata kiderítette, hogy a pályázóktól beszerzett írásbeli hozzájárulás dacára hiányzott a kiszolgáltatott helyzetben lévő

¹⁶ 661/H/2000.

¹⁷ 354/A/2000. A munkáltatók által megrendelt hazugságvizsgálatokra a későbbiekben még visszatérünk.

álláskeresőék tájékoztatott beleegyezése, mivel nem tájékoztatták őket előre arról, hogy kik és milyen szempontok alapján fogják értékelni a tesztet.¹⁸

2.1.4. A pályázók orvosi vizsgálata

Az alkalmazottak kiválasztásakor a munkáltatóknak nemcsak egyéni preferenciáik vagy a jelöltek megbízhatósága alapján kell dönteniük, a munkavédelmi szabályok szerint a munkáltató csak a munkára alkalmas személyt alkalmazhatja, az egészségügyi megfelelésről pedig előzetes, illetve időszakonkénti orvosi vizsgálat alapján kell dönteni. Szellemi munkát végzők esetében azonban ezeknek a szabályoknak nem sok értelme van, hiszen az ő munkavégzésük általában nem jár káros fizikai és vegyi hatásokkal vagy fokozott balesetveszéllyel. Az adatvédelmi biztoshoz érkeztek olyan beadványok, amelyekben a panaszosok egy-egy központi közigazgatási szervnél a jogi előadói munkakör betöltésének feltételül szabott, széles körű adatgyűjtést, illetve orvosi vizsgálatot sérelmeztek. Az adatok között valóban vannak olyanok, amelyek felvétele indokolatlan lehet. Az irodai munkára jelentkezők azt kifogásolták, hogy a foglalkozás-egészségügyi orvos az erre a célra szolgáló adatlapon olyan adatokat is feljegyzett, amelyek a munkakörük betöltéséhez szükséges egészségügyi alkalmasság megítéléséhez nem voltak szükségesek.

Az egyik beadványozó arról számolt be, hogy az új munkáltatója utasításának megfelelően elment a munkahelyén megszervezett orvosi vizsgálatra. A várószobában vették fel a személyazonosító adatait, ott, ahol rajta kívül többen várakoztak. A várószobában a nővér íróasztalán több betegkartont látott, amelyet — ha a nővér kis időre távozott a helyiségből — bárki meg tudott nézni. A vizsgálat során a panaszostól az orvos megkérdezte és feljegyezte a következőket: testmagasság, testsúly, a családban milyen szív-, érrendszeri, emésztési, daganatos stb. megbetegedések voltak, beteg szülője hány éves, mikor lett beteg, jár-e nőgyógyászhoz, szed-e fogamzásgátló tablettát, vannak-e nőgyógyászati problémái. Az orvos ezt követően megvizsgálta a panaszos szemét, megmérte a vérnyomását, meghallgatta a tüdejét és a szívét, majd vérkép- és vizeletvizsgálatra küldte azzal, hogy a leleteket neki hozza vissza. A vizsgálat indokálta azt mondta, hogy „legalább ennyi adat legyen róla”. A panaszosnak végül alá kellett írnia a következő nyilatkozatot: „Eltitkolt betegségem nincs”.

Az adatvédelmi biztos a beadványok alapján vizsgálni kezdett. Az egyeztetés során a bepanaszolt munkáltatók az adatkezelés jogalapjául a munkaköri, szakmai, illetve személyi

¹⁸ 736/A/2000.

higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló rendeletet¹⁹ jelölték meg. Eszerint a munkaköri alkalmassági vizsgálat annak megállapítása, hogy egy meghatározott munkakörben és munkahelyen végzett tevékenység által okozott megterhelés a vizsgált személy számára milyen igénybevételt jelent, és annak képes-e megfelelni. Előzetes munkaköri alkalmassági vizsgálatot kell végezni a munkáltató által foglalkoztatni kívánt személynél a munkavégzés megkezdését megelőzően. A rendelet előírásának megfelelően a panaszosok is részt vettek kinevezésükkor, illetve egy-két héttel azt követően a vizsgálaton, amely keretén belül a rendelet mellékletében meghatározott „*Munkavállaló egészségügyi törzslapja*” című nyomtatványt töltötték ki. A munkáltatói jogok gyakorlóját az orvos csupán az összegző véleményéről tájékoztatta, az egészségügyi adatokat tartalmazó adatokat azonban rögzítette és megőrizte.

Az adatvédelmi törvényben meghatározott célhoz kötöttségi szabályok, valamint az egészségügyi adatok kezeléséről és védelméről szóló törvény²⁰ szerint az egészségügyi és személyazonosító adat kezelésének célja lehet a munkavégzésre való alkalmasság megállapítása, de a törvényben megjelölt adatkezelési célokból csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósításához elengedhetetlenül szükséges. A rendelet viszont — a törzslapon — igen széleskörű adatszolgáltatási kötelezettséget ír elő, amely nem felel meg az adatvédelem fenti elveinek. Az adatlap számos olyan adatfajtát tartalmaz, amely a munkakörök legtöbbjénél nem szükséges a kívánt cél eléréséhez, tehát a munkaköri alkalmasság megítéléséhez: az apa, anya és testvérek szív- és érrendszeri, légzőszervi, daganatos, emésztőszervi, anyagcserével összefüggő, pszichiátriai megbetegedései; a dohányzásra és az alkoholfogyasztásra (fajtájára, mennyiségére, abbahagyás évére), a sportolásra és az étkezési szokásokra vonatkozó adatok; jogosítvánnyal, katonai szolgálattal összefüggő, fogazattal kapcsolatos és még sok más adat. Számos adat felvétele indokolt bizonyos munkakörök esetében, de más munkakörök esetében nem. A beadványozók mint jogi referensek esetében a munkaköri alkalmasság megítélése tárgyában a látószervek egészségére vonatkozó adatokon kívül — mivel számítógéppel dolgoznak — szinte valamennyi adat kérése indokolatlan, és ezért a célhoz kötöttségi szabályokkal ellentétes. A rendelet szerint az adatlapon az érintettnek nyilatkoznia kell arról, hogy eltitkolt betegsége nincs. A rendelet ezzel azt eredményezi, hogy a munkavállaló az egészségi állapotára vonatkozó valamennyi adatot szolgáltatni köteles a munkáltató által megbízott orvos részére, enélkül munkavégzésre irányuló jogviszonyt nem létesíthet. Az adatlap olyan személyek különleges adatait is tartalmazza továbbá, akik a munkavégzésre irányuló

¹⁹ A munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet.

²⁰ Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény.

jogviszonynak nem alanyai (anya, apa, testvér). Mivel ők egyértelműen azonosíthatók, az ő személyes adataiknak is védelmet kell élvezniük. A rendelet által előírt adatlap az ismertetett tartalmi okokon túl formai okok miatt sem felel meg az adatvédelmi követelményeknek. A rendelet (illetve az adatlap) ugyanis különleges adatok kezelését írja elő: az érintettek egészségi állapotára, valamint kóros szenvedélyére vonatkozó adatokét.

Ebben az ügyben tehát nem a munkáltató eljárására volt visszavezethető a jogsérelem, hanem a jogszabály nem megfelelő voltára. A rendelet mellett, hogy nem megfelelő jogforrási szinten írt elő kötelező adatkezelést (ezt csak törvényben lehet megtenni), tartalmilag is alapjogsérelmet idézett elő. Az adatvédelmi biztos megállapította, hogy a rendelet azon rendelkezése, amely a munkába állás előtt kötelezővé teszi az alkalmassági vizsgálatot, önmagában nem ellentétes a személyes adatok védelméhez való joggal. A vizsgálat során a rendelet által előírt adatfelvétel azonban jelenlegi formájában jogsértő. Egyrészt azért, mert a célhoz kötöttség elvét figyelmen kívül hagyva rendkívül széles adatszolgáltatási kötelezettséget ír elő a munkavállaló számára, amely az adatfelvétel céljának eléréséhez az esetek többségében nyilvánvalóan nem szükséges adatokra és más személyek adataira is kiterjed. Másrészt az adatkezelést elrendelő jogszabály jogforrási szintje sem megfelelő. Mindezek alapján az adatvédelmi biztos kezdeményezte az egészségügyi miniszternél a foglalkozás-egészségügyi jogszabályok olyan módosítását, amely eredményeképpen — megfelelő szintű jogforrás — a foglalkozás-egészségügyi orvos részére csak olyan adatok szolgáltatását írja elő, amelyek az adott munkakör betöltésére való alkalmasság megítéléséhez szükségesek. A miniszter ugyanakkor nem tartotta szükségesnek a változtatást. Időközben mégis történt jogszabálymódosítás, amely szerint a véleményező orvos csak az alkalmasság elbírálásához szükséges vizsgálatokat végzi el, és az egészségügyi törzslap más rovatait áthúzza.²¹

Említést érdemel az egészségügyi miniszternek a vitában felhozott azon érve, hogy nem okozhat problémát a túlzott mértékű adatgyűjtés, hiszen a foglalkozás-egészségügyi orvos amúgy is titoktartásra kötelezett. Az adatvédelmi biztos válasza erre az érve elvi jelentőségű: az adatkezelés jogellenes voltát nem oldja meg a foglalkozás-egészségügyi orvos titoktartási kötelezettsége, a titoktartási kötelezettség ugyanis nem ad felhatalmazást arra, hogy az orvos bármilyen adatot kérhessen, illetőleg az érintett bármilyen adat szolgáltatására kötelezhető legyen. Az adatvédelmi jogszabályokat az orvos is köteles betartani.²²

²¹ E mondatot beiktatta: 80/2003. (XII. 23.) ESzCsM rendelet. Hatályos: 2004. január 22-től.

²² 270/A/2000, 759/A/2000, 359/A/2001.

2.2. A munkavégzés ellenőrzésével kapcsolatos ügyek

A munkáltatók minden kétséget kizáróan jogosan várják el, hogy az általuk megfizettet munkaidőt az alkalmazottak munkavégzésre fordítsák. A munkaviszonyból következő munkavégzési kötelezettség teljesítésének ellenőrzésére is természetesen joguk van. Az ellenőrzési lehetőségeik korláta azonban ott húzódik, ahol az alkalmazottak emberi jogai kezdődnek, azaz a munkáltató az ellenőrzéseivel nem sértheti a dolgozók alapvető jogait. Sajnos még nem ez az általános szemlélet. A munkáltató úgy véli, a munkavégzés ellenőrzése körében bármit megtehet. Nem szabad azonban megfeledkezni arról, hogy a munkaszerződés aláírásával a munkavállaló csak munkaerejét és munkaidejét „adja el”, a személyiségét nem. Az ember megmarad embernek akkor is, ha másnak dolgozik, szuverén egyén marad, nem rabszolgája munkáltatójának, csupán alkalmazottja. És mivel ember marad, megilletik alapvető jogai mindenkivel, még a munkáltatóval szemben is. A munkáltató tehát ellenőrizheti, de ez nem jelenti azt, hogy ellenőrzése körében bármit megtehet, nem sértheti a munkavállaló alapvető jogait. Ahogy nem kényszeríthető az alkalmazott ostrommal munkavégzésre, úgy nem ellenőrizhető a munkája a magánszférához való jogának megsértésével sem.

A munkavégzés ellenőrzésének hagyományos módja a munkateljesítmény értékelése. Az utóbbi időben azonban a dolgozók megfigyelése az, ami tipikussá kezd válni, különböző technikai eszközökkel igyekeznek a munkáltatók szemmel tartani — akár a szó szoros értelmében is — az alkalmazottakat. Itt említhető a dolgozók megfigyelése kamerarendszeren keresztül, vagy elektronikus levelezésük, telefonhívásaik, számítógéphasználatuk, internetezésük ellenőrzése, figyelemmel kísérése.

2.2.1. Elektronikus levelezés magánügyben

Az adatvédelmi biztosnak az ilyen ügyekben meghozott döntései többnyire általánosítható megállapításokat tartalmaznak: a munkavállalók megfigyeléséről az adatvédelmi biztos igyekszik olyan állásfoglalásokat hozni, amelyekből nemcsak a konkrét vizsgálatával érintettek, hanem mások is megismerhetik a követendő szabályokat.

Ha a munkáltató személyes használatra adta a számítógépet, akkor — az adatvédelmi biztos ügyeiből leszűrhetőek szerint — az azon tárolt személyes jellegű anyagokat nem ismerheti meg az érintett hozzájárulása nélkül. Természetesen abban az esetben, ha a munkavállaló a számítógépet visszaadja a munkáltatójának, akkor törölnie kell a magánjellegű fájlokat, ha nem akarja, hogy a számítógép új birtokosa azokat megismerje, ennek hiányában az adatok

megismeréséhez hozzájárulását megadottnak kell tekinteni, mivel azokat ő maga adta át a munkáltatónak.²³

A munkáltató által biztosított elektronikus levelezés tekintetében az adatvédelmi biztos a joggyakorlatában különbséget tesz a munkavállaló személyes használatára adott, esetleg a nevét vagy nevének töredékét is tartalmazó, valamint az olyan e-mail címek között, amelyek a cég ügyeinek intézését szolgálják, és nem egy-egy munkavállaló személyéhez kötöttek. Ez utóbbiakon folytatott levelezésbe a munkáltató betekinthez, még akkor is, ha e címen valamelyik — a postafiókhoz hozzáférő munkavállaló — magánjellegű levelezést is folytatott, hiszen azt a munkavállaló ennek tudatában tette. A személyes, csak az érintett munkavállaló (illetve a rendszergazda) számára hozzáférhető e-mail címen folytatott levelezést pedig adatvédelmi szempontból ugyanúgy kell megítélni, mint a hagyományos személyes levelezést és telefonálást. Mint ahogy a munkáltató az érintettek hozzájárulása nélkül nem ismerheti meg a munkavállalója részére a céghez érkező küldemények tartalmát, azokat nem tarthatja vissza, illetve nem semmisítheti meg, és a telefonbeszélgetéseit sem hallgathatja le, ugyanúgy nem jogosult a személyes e-mail címre érkező és az onnan elküldött levelek tartalmának megismerésére, azok továbbítására vagy törlésére sem mindaddig, amíg ahhoz az érintett hozzájárulását nem adja.²⁴

Van a munkahelyi e-mailezés ellenőrzésének jogszerű módja is. Az adatvédelmi biztoshoz fordult egyik beadványozó arról számolt be, hogy az őt foglalkoztató bank a dolgozói elektronikus levelezését ellenőrzi. Ezt abból tudta meg, hogy egy ismerőse által küldött levele helyett a következő értesítést kapta: „Üzenetet kapott, melyet tartalma miatt nem kaphat meg.” Ebből arra következtetett, hogy a munkavállalók levelezését tartalmilag is ellenőrzi, ráadásul cenzúrázzák is, a címzettekhez való eljutását akadályozzák. Az adatvédelmi biztos konzultált a bank vezérigazgatójával, tanulmányozta a vonatkozó ügyviteli utasításokat, belső szabályzatokat, és a következőket állapította meg.

A bank elektronikus levelezőrendszere deklarálta és elsődlegesen üzleti célokat hivatott szolgálni, azonban a hivatalos levelezésen felül a dolgozóknak módjában áll magánjellegű levelezést is folytatni. Minden banki dolgozó névre szóló, egyedi e-mail címmel rendelkezik, ezek a címek mutatják, hogy hivatali címről van szó (keresztnev.vezeteknev@cegnev.hu). A leveleket csak a címzett olvassa. Minden elektronikus levél vírusellenőrzésen és tartalmi ellenőrzésen megy keresztül. A tartalmi ellenőrzés automatikus, és kizárólag a levélhez csatolt melléklet típusát (program, kép-, hang-fájl) ellenőrzi, tehát a levél szövegére vonatkozóan semmiféle ellenőrzés nem

²³ Lásd például: 772/A/2000, 841/K/2002.

²⁴ A számos ügy közül egy pár példa: 839/A/2000, 795/K/2002, 756/K/2002, 105/A/2003, 571/K/2003.

történik. A hivatalos és a magánlevelezés ugyanazon technikai szűrőrendszeren keresztül történik. A szűrőprogram minden olyan levelet megállít (és csak azokat), amelyek vírusosak, futtatható programot, képet, filmet vagy hangot tartalmaznak. A bank ezzel a működéséhez nem szükséges állományok bekerülésének lehetőségét, valamint a szerzői jogvédelem alá eső programok és más szellemi alkotások jogosulatlan felhasználásának lehetőségét kívánja csökkenteni. Egy-egy levél megállításáról a címzett azonnal értesítést kap a következő szöveggel: „Üzenetet kapott, amelyet tartalma miatt nem kaphat meg.”

A levelek megállítása ugyanakkor nem jelenti azt, hogy azokat a címzettek nem kaphatják meg. A vírusos levelek kivételével ugyanis a címzettek minden levelet megkaphatnak. Azokról a levelekről, amelyeket a levélszűrő rendszer megállított, a címzett értesítést kap, amely tartalmazza a fenti mondaton kívül a feladóját és címét. Ezek alapján a címzett el tudja dönteni, hogy a levelet kéri-e vagy sem. Amennyiben az informatikai belső ügyfélszolgálatától kéri a levél továbbítását, úgy minden esetben megkapja azt. Ilyen esetben szelektálás nélkül minden levél továbbításra kerül. Azok a kimenő levelek, amelyek azonnali továbbítása — méretük miatt — nagyban leterhelné a levelezőrendszert, később, a munkaidő befejezése után kerülnek továbbításra, így a levelezőrendszer kellő sávszélességgel tudja fogadni a bejövő leveleket. A levelekben ilyenkor sem történik semmi tartalmi változtatás. A bank ugyanakkor megsemmisít (töröl) minden olyan levelet, amely vírusos tartalma miatt veszélyezteti a rendszer biztonságos működését.

Mindezekekről a feltételekről a bank tájékoztatta a dolgozókat. A dolgozók a munkaszerződés aláírásával elfogadják a bank belső szabályzatait, amelyek közül több is tartalmazza az elektronikus levelezés módját, feltételeit. A munkaszerződés utolsó bekezdése előírja a banki szabályok betartását. Ezen kívül a bank által használt elektronikus levelezőrendszer részletes információt ad a levelezőrendszer használatáról, feltételeiről. Ezen felül a banki intranetre való első bejelentkezéskor a felhasználónak el kell fogadnia egy nyilatkozatot arról, hogy a vonatkozó belső rendelkezéseket, szabályokat ismeri. A bank összes szabályzata, folyamatleírása a dolgozók számára elektronikus és hagyományos módon is elérhető, a bank tehát több módon igyekszik megismertetni a levelezőrendszer használatának feltételeit a dolgozókkal.

Tekintettel azonban arra, hogy a beadványozó esetében a tájékoztatás nem bizonyult elegendőnek, hiszen a beadványa félreértésen alapult, az adatvédelmi biztos kezdeményezte a bank vezetőjénél, hogy a levél megállításáról szóló értesítés hívja fel a címzett figyelmét arra is, hogy a megállított levelet milyen feltételekkel kaphatja meg. A biztos megállapítása szerint egyébként a bank eljárása nem sérti a munkavállalók személyes adatok védelméhez való jogát.²⁵

²⁵ 660/A/2002.

2.2.2. Az internet-használat ellenőrzése

Az a tény, hogy ki milyen internet-oldalakat és milyen gyakorisággal tekint meg, személyes adatnak minősül. Az adatvédelmi biztos — hasonlóan az elektronikus levelezés ellenőrzésével kapcsolatban tett megállapításokhoz — különbséget tesz aszerint, hogy a munkáltató az internet használatát kizárólag munka céljából engedélyezi, vagy lehetővé teszi a magáncélú használatot is. Amennyiben a munkavállaló az internet használatát csak a munka végzése céljából engedélyezi, lehetősége van ennek ellenőrzésére. Ezt azonban csak akkor teheti meg, ha a dolgozók figyelmét előzetesen felhívta az internet használatának korlátozására, és az utólagos ellenőrzés lehetőségére. Abban az esetben, ha a munkavállalók úgy férhetnek hozzá az internethez, hogy előzetesen nem kaptak ilyen tartalmú tájékoztatást — esetleg a munkáltató kifejezetten hozzájárult a magáncélú használatához —, az internet-használatra vonatkozó adatokat, így a látogatott oldalak címét a munkáltató nem ismerheti meg. Ha mégis vizsgálja az internet használatát, és erről kimutatást készít vagy készíttet, jogellenes adatkezelést végez.²⁶

2.2.3. A munkavállaló telefonhívásainak ellenőrzése

A munkahelyi telefonról kezdeményezett hívások listázásával kapcsolatos ügyekből az derül ki, hogy az adatvédelmi biztos szerint a munkáltató ezzel nem ellenőrizheti a telefon használatát. Mind a hívó, mind a hívott fél személyes adatának minősül ugyanis az, hogy az adott időpontban beszélgetést folytattak, és azt egymással tették. Személyes adat tehát az, hogy egy munkavállaló egy meghatározott telefonszámot hív, és személyes adat az is, hogy a hívott fél valamilyen kapcsolatban áll a hívó féllel. Tekintettel arra, hogy a hívott fél hozzájárulásának beszerzése gyakorlatilag nem lehetséges, a híváslista készítése még a munkavállalók hozzájárulása esetén sem lenne jogszerű. A költségek csökkentése azonban más módon jogszerűen is elérhető. Egyik lehetséges megoldás lehet a magáncélú beszélgetések tiltása, illetve annak céljára nyilvános (érmével működő vagy kártyás) telefonok elhelyezése a munkahelyen. Egy másik — a munkáltatók körében is kedvelt — megoldás az, hogy a munkavállalók számára meghatározott összegig biztosítják a telefonálás lehetőségét, e kereten belül a becsült hivatalos telefonálási szükségletnél magasabb összeget határoznak meg, ahhoz hozzáadják a munkavállaló számára engedélyezett magáncélú beszélgetéseknek megfelelő azon értéket, amelyet a munkáltató "ajándékoz" munkavállalói számára. A hivatalos beszélgetéseknek megfelelő összeg becslését segíti, ha a vidékre vagy külföldre irányuló hívásokat csak meghatározott

²⁶ Például: 790/K/2001, 795/K/2002.

készülékekről engedélyezik. Az így meghatározott kereten felüli telefonhívások díjának megfizetésére a munkavállalót kötelezik.²⁷

2.2.4. Globális helymeghatározó rendszer (GPS) mint a munkavállalók ellenőrzésének eszköze

Az adatvédelmi biztos egy esetben állást foglalt egy területi képviselőként dolgozó munkavállaló beadványa alapján a munkáltató által, autó nyomkövetésével történő megfigyeléssel kapcsolatban. A munkáltató műholdas helymeghatározó rendszerrel figyelte, mire használja a munkavállaló a használatába adott cégautót. Az adatvédelmi biztos megállapításai szerint az, hogy valaki mikor merre megy, hol áll meg, autójával mennyi benzint fogyaszt, az az ő személyes adata. A cégautó használatának munkáltató által történő ellenőrzése jogszerűségének megítélésekor különbséget kell tenni aszerint, hogy a munkáltató személyes használatra vagy kizárólag a munkavégzés céljára adta-e a munkavállalónak az autót. Amennyiben a munkáltató a személyes használatot nem engedélyezi, az autó használatát ellenőrizheti, de erről, illetőleg az ellenőrzés módjáról tájékoztatnia kell a munkavállalót. Az autó minden ezt követő olyan használata, amely nem a munkavégzést szolgálja, úgy jut a munkáltató tudomására, hogy a munkavállaló erről tud, és az adatkezeléshez tulajdonképpen hozzá is járul. Más a helyzet akkor, ha az autót személyes használatra adta a munkáltató, az tehát nemcsak a munkavégzés céljára használható. Az adatkezeléshez adott megfelelő hozzájárulás hiányában ebben az esetben is csak törvény rendelkezése alapján ellenőrizhető az autó használata. A Munka Törvénykönyve felhatalmazást ad a munkáltató számára bizonyos adatkezelésekre, így például arra is, hogy a munkavégzésre fordított időt nyilvántartsa. Ebben a tekintetben tehát a munkáltató által a műholdas követőrendszer segítségével felvett adatok egy részének kezelésére jogalapot biztosít. E törvényi felhatalmazás azonban bizonyosan nem jogosítja fel a munkáltatót arra, hogy például a pontos útvonalat kövesse. A cégautóval ellátott munkavállalót úgy tájékoztatták, hogy a műholdas megfigyelőrendszer célja az autólopás kivédése. Ezen cél eléréséhez pedig nem elengedhetetlen a munkavállaló autóval megtett útjainak folyamatos ellenőrzése, rögzítése, ezért az ilyen adatkezelés ellentétes az adatvédelmi törvény célhoz kötöttségi szabályaival. Ez a cél úgy is elérhető lenne, ha a járműhasználatot nem figyelnék, a követő-rendszer csak az autó ellopása esetén lépne működésbe.²⁸

²⁷ Példák erre az ügytípusra: 764/K/2000, 674/K/2002, 803/K/2002.

²⁸ 117/A/2002.

2.2.5. Kamera a munkahelyen

Érdemes az adatvédelmi biztos számtalan munkahelyi kamerarendszerrel kapcsolatos ügyének közös megállapításait összegezni. Általánosságban megállapítható, hogy speciális szabályozás hiányában csak az általános adatvédelmi szabályok alkalmazhatók erre a kérdésre nézve is. Az adatvédelmi biztos általában a munkavégzés ellenőrzésére nem tartja megengedhetőnek a kamerarendszer üzemeltetését, azt kizárólag biztonsági céllal tartja bevezethetőnek.

Az adatvédelmi biztos szerint törvényi meghatározások alapján a képfelvevő, -rögzítő berendezések által felvett és tárolt felvételek — amennyiben azon a személyek felismerhetők, azonosíthatók — személyes adatokat tartalmaznak, ezért az ilyen berendezések működtetése adatkezelésnek minősül. Ilyet pedig csak akkor lehet tenni, ha a felvételen megjelenő személyek ehhez hozzájárulnak, vagy törvény megengedi a felvételek készítését. A felvételek készítése adatvédelmi problémákat vet fel, hiszen a felvételek a megfigyelt eseményeket, és ezzel egyes személyek adott helyen való jelenlétét, magatartását, tevékenységét — azonosítható és a későbbiekben visszakereshető módon — rögzítik, tárolják. Személyes adatokat is tartalmazó felvételek rögzítése és meghatározott ideig történő tárolása pedig csak az adatvédelmi szabályok betartásával lehet jogszerű. A képfelvevő, -rögzítő berendezések telepítése, működtetése során figyelemmel kell lenni arra a rendelkezésre, amely szerint „a személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait — ha törvény kivételt nem tesz — az adatkezeléshez fűződő más érdekek, ideértve a közérdekű adatok nyilvánosságát is, nem sérthetik.” Az üzleti vagy a biztonsági érdekek igen erősek lehetnek, az adatvédelmi biztos szerint azonban nem hagyható figyelmen kívül, hogy ezen érdekek érvényesítése a képfelvevő, -rögzítő berendezések használata során az Alkotmány által biztosított emberi jog sérelmével valósul meg. Az érintettek személyes adatainak védelméhez való jogát sértő felvétel készítését ezért — törvényi felhatalmazás hiányában — ilyen érdekek nem tehetnek indokolttá.

Ha külön törvényi felhatalmazás nem rendelkezik a képfelvétellel megvalósuló adatkezelésről, az adatvédelmi követelményeknek csak azok a képfelvevő, -rögzítő berendezések felelnek meg, amelyek esetében az érintetteket (például látogatókat, ügyfeleket, vendégeket, dolgozókat, az adott területen megjelenő más személyeket) tájékoztatják a képfelvevő rendszer működéséről, és külön felhívják arra a figyelmet, hogy a berendezés (meghatározott célból és esetekben) rögzíti a képeket, továbbá az adatkezelő arról is tájékoztatást ad, hogy a rögzítésre mikor kerül sor, az milyen célt szolgál, és a felvételeket hol és meddig őrzik. Az érintett személyek a képfelvétel rögzítéséhez nyilatkozattal (írásban vagy szóban), vagy ráutaló magatartással (például a kamerával

megfigyelt területen való megjelenéssel) kell, hogy hozzájárulásukat adják a felvételek készítéséhez, az érintetteknek lehetőségük kell, hogy legyen gyakorolni az adatkezeléssel összefüggésben őket megillető jogait: tájékozódhatnak adataik kezeléséről, és — a korábbi hozzájárulásukra tekintet nélkül — azokat bármikor törölthetik. A felvételt készítő és az érintett személy azonos információk helyzetét biztosítani kell, azaz vita esetén a felvételt az érintett személy is felhasználhatja. Az adatvédelmi biztos szerint a személyiségi jogok sérelmét jelenti, ha — törvényi felhatalmazás nélkül — rejtetten működtetnek ilyen berendezéseket. Egy üzletben csak abban az esetben rögzíthetők a berendezések által közvetített, személyazonosításra alkalmas képek, ha — a rögzítés céljának, módjának, a felvételek tárolási idejének és helyének, valamint az adatkezelő szervezet ismeretében — az érintettek egyértelműen hozzájárultak, illetve hozzájárulhatnak személyes adataik kezeléséhez. Amennyiben — törvényi felhatalmazás hiányában — olyan közterületen vagy nyilvános magánterületen történik képrögzítéssel megfigyelés, amelyet a személyes adataik kezeléséhez hozzájárulni nem szándékozik is kénytelenek felkeresni, vagy ott megjelenni, akkor lehetővé kell tenni, hogy az érintettek kérésére a rájuk vonatkozó felvételeket soron kívül töröljék.

Ezen eseten túlmenően egy munkahelyen — elsősorban biztonsági, vagyonvédelmi célból — a felvételek akkor rögzíthetők, ha ott a felvétel készítésének idején a kamerát üzemeltető személyen vagy megbízottjain kívül más jogszerűen nem tartózkodhat. A rögzített képek tárolási idejét (a törlési határidőt) úgy kell megválasztani, hogy a felvételek megőrzésére csak addig kerüljön sor, ameddig arra a — berendezést működtető szervezet által — meghatározott cél megvalósulásához feltétlenül szükség van; az érintettek jogainak érvényesítése érdekében — kifejezett kérésükre — az adatkezelés eredeti céljához szükségesnél hosszabb törlési határidő is megállapítható. Az érintettek jogainak érvényesítése érdekében lehetővé kell tenni, hogy — a korábbi hozzájárulására tekintet nélkül — bárki kérhesse a személyével összefüggő felvételek törlését.²⁹

2.2.6. Kamera az Adatvédelmi Biztos Irodájában

A munkahelyi kamerás megfigyeléssel kapcsolatos ügyek egyike meglehetősen különlegesnek számít annyiban, hogy a bepanaszolt rendszer az Adatvédelmi Biztos Irodájának is otthont adó Országgyűlési Biztosok Hivatalában működik. A beadványozók — akik az adatvédelmi biztost, mint munkáltatójukat panaszolták be az adatvédelmi biztosnál — szerint a hivatal területén a kamerák jogellenesen működtek, mivel a dolgozók hozzájárulását a rendszer üzembe helyezéséhez senki nem kérte, és működött az az

²⁹ A megfigyelés, adatgyűjtés céljából üzemeltetett képfelvévő, -rögzítő berendezésekkel kapcsolatos adatvédelmi biztosi ajánlás, 2000. december 20., 475/H/2000.

érintettek kifejezett ellenérzése ellenére is. Sérelmezték, hogy a megfigyelőrendszer üzembe helyezésekor csupán egy meglehetősen szűkszavú tájékoztatást kaptak a dolgozók a kamerákkal kapcsolatban, miszerint *"a hivatal területén a fölépcsőházból nyíló ajtók nincsenek zárva, ezért a hivatal egész területét biztonsági kamera figyeli, az adatvédelem és a személyiségi jogok védelmét szem előtt tartva. Ugyanígy kamera figyeli a ház külső területét is."* A vizsgálat során az adatvédelmi biztos megállapította, hogy a rendszer üzemeltetésének a célja a hivatal dolgozóinak megfelelő védelme és a vagyonvédelem, konkrétan annak megakadályozása, hogy idegenek engedély nélkül tartózkodhassanak a hivatal területén. A közvetített képeket a portaszolgálat figyeli. A képeket sem a vizsgálat idején, sem korábban nem rögzítették. A kamerák nincsenek elrejtve, egyszerű szemrevételezéssel is — mind az épületen belül, mind az utcán közlekedők által — jól észlelhetők. A biztos megállapításai szerint a portán található monitorokon a személyek pontosan beazonosíthatók, arcuk jól felismerhető. A megfigyelt folyosószakaszokon dolgozóknak, illetve a velük kapcsolatban lévőknek nincs tényleges választási lehetőségük, hogy elkerülik-e a megfigyelt szakaszt, vagy más irányban közlekednek. Az épületbe érkezőket hosszú ideig nem is tájékoztatták figyelemfelhívó táblák a kamerák működéséről. Az adatvédelmi biztos állásfoglalása szerint a megfigyelés alapul szolgálhat akár szenzitív adatok megismerésére is, tehát indokolt az érintettek fokozott védelme még akkor is, ha a kamerák által közvetített képeket azok rögzítése nélkül, közvetlenül a monitorokon kísérik figyelemmel. Ahhoz ugyanis, hogy egy információ személyes adat legyen, nem kell az érintett nevét és egyéb adatait ismerni, elegendő, ha a természetes személy meghatározható az információ alapján. Az adatvédelmi biztos szerint azonban ha a kamerák által közvetített képeket a rendszer nem rögzíti, nem szükséges az érintettek hozzájárulása. Kifogásolhatónak tartotta ugyanakkor, hogy a kamerák felállításáról nem tájékoztatták előzetesen a dolgozókat, így nem tudhatták rögzítik-e és tárolják-e a kamerák által sugárzott képet. A kamerák beüzemelésével egyidejűleg a bejáratnál — jól látható és olvasható helyre — fel kellett volna szereltetni egy tájékoztató táblát, amely felhívja az érkezők figyelmét a kamerák működtetésére. Az országgyűlési biztosok e tárgyban adatkezelési szabályzatot fogadtak el, amely időközben hatályba lépett.³⁰

2.3. Amikor a munkáltató nyomoz

Egyes munkáltatók szeretik maguk felderíteni azokat, a jogaikat vagy érdekeiket sértő cselekményeket, amelyeket feltehetően az alkalmazottaik követtek el ellenük. Cégek vezetői, személyzeti kérdésekben döntéseket hozó munkatársai szembekerülnek az alkalmazottak megbízhatóságának kérdésével, ha azok olyan munkaköröket töltenek be, amelyekben nagy értékű árucikkkel vagy fontos információkkal foglalkoznak. A vezetők,

³⁰ 94/A/2002.

munkáltatók — érthetően — minél többet szeretnének megtudni az emberekről, akikre vagyonukat bízják, ha lehetséges, akár gondolataikat, szándékaikat is látni kívánják. Ha pedig magánnyomozók és személyzeti tanácsadók olyan szolgáltatást kínálnak nekik, amelynek segítségével — állításuk szerint — az őszinteség mérhető, és tényfeltáró vagy megbízhatósági vizsgálatot ígérnek pszichológiai tesztek vagy akár hazugságvizsgáló készülék alkalmazásával, azt természetesen elfogadják, a szolgáltatást saját biztonságuk érdekében igénybe veszik. A hazugságvizsgálat azonban a vizsgált személyek alapvető emberi jogait érinti, ezért szükséges, hogy a jog valamilyen módon reagáljon rá.

Ezekben az esetekben nem az alkalmasság megítéléséről van szó, hanem arról, hogy vagy azért, mert már történt valami jogellenes a cégnél, vagy azért, mert a vezetés fél egy ilyen esemény bekövetkeztétől, megpróbálják felderíteni, hogy kik azok, akik elkövethettek, vagy elkövethettek ilyen cselekményeket.

2.3.1. Pszichológiai tesztek

1998. folyamán az Adó- és Pénzügyi Ellenőrzési Hivatal elnöke elrendelte, hogy a hivatal vezető beosztásban lévő tisztviselőinek irányított személyiségvizsgálaton kell átesniük egy személyzeti tanácsadó cég közreműködésével. A panaszos szerint „a személyiségvizsgálattal nyerhető információk felhasználása irányítási, munkaszervezési célokra súlyosan sérti az APEH köztisztviselőinek személyiségi jogait, miután köztisztviselői jogviszonyukba nem személyiségük teljességével, hanem annak a szaktudásuk köré szervezett és a hivatal számára szükséges készségeivel és adottságaival léptek. Ez jogviszonyuk alapja”. A hivatal elnöke viszont azzal védekezett, hogy a vizsgálat célja a „humánkapacitás feltérképezése”, és „a felmérés nem kérdőjelezi (nem kérdőjelezheti) meg az érintettek szakmai/munkajogi alkalmasságát.” A felmérés kiterjedt volna a teljes vezetői állományra (a hivatal vezetése, hivatali főosztályvezetők, főosztályvezető-helyettesek, osztályvezetők, megyei igazgatók és személyi titkárok) – összesen mintegy 120 főre. A felmérésben való részvétel deklaráltnan nem lett volna kötelező, az elnök szerint a részvétellel kapcsolatos döntése miatt senkit hátrány nem érhet. A felmérés úgynevezett irányított készség- és képességvizsgálattal történt volna, ami kifejezetten meghatározott tulajdonságok felderítésére irányul. A vizsgálatban részleges anonimitást biztosítottak volna, vagyis az eredmények személyhez történő társítását, az adatok összekapcsolását kizárólag hivatal elnöke végezhette volna el. A vizsgálat képességvizsgálati teszt, intelligenciateszt, grafológiai kontrollvizsgálat, célzott interjú, egyéb személyes információk felhasználásával történt volna. Mint kiderült, a vizsgálatot végző cég a tesztkiértékelő lapokat nem adta volna át a megbízónak, hanem csak az eredmények alapján készített szakvéleményt, amely kifejezetten a vizsgálati célul kitűzött képességkimutatást szolgálja.

A köztisztviselők munkajogi jogállásáról szóló jogszabály³¹ az átlagosnál jobban védi ezen személyek privacy-jét munkáltatóikkal szemben: a törvény egyenesen kizárja a törvényben felsorolt adatok körén túlmutató adatgyűjtést, még az érintett hozzájárulásával is. Ez a törvény tehát pontosan meghatározza, hogy a közigazgatási szervek — mint munkáltatók — a köztisztviselőkről milyen személyes adatokat gyűjthetnek és tarthatnak nyilván. Ezeken túlmenően pedig megtiltja az adatkezelést. A köztisztviselők munkájának értékelésére, képességeik felmérésére a törvény meghatároz egy értékelési módszert, az azonban nem foglal magában olyan irányított személyiségvizsgálatot, mint amelyet az adóhivatalnál elrendeltek.

Az adott esetben az önkéntes részvétel kizárt volt, a vizsgálat megállapította, hogy az érintetteket felszólították a személyiségvizsgálaton való megjelenésre. Az adatvédelmi biztos a vizsgálatot lezáró ajánlásában úgy foglalt állást, hogy ilyen személyiségvizsgálatra irányuló eljárás azzal a feltétellel minősülhet jogszerűnek, ha biztosítják a teljes önkéntességet és anonimitást, tehát a hivatal elnöke sem jogosult a vizsgálati eredményeket a vizsgált személlyel összekapcsolni. Ilyen vizsgálatoknak pedig természetesen már nem lehet a célja egyéni következtetések levonása, csupán a hivatal általános racionalizációja, a munka szervezésének segítése, hiszen a vizsgálati eredmények csak összesítve ismerhetők meg a hivatal vezetője számára.³²

2.3.2. Poligráf, mint nyomozási eszköz a munkáltató kezében

A legdurvább nyomozási eset az, amelyben a munkáltató hazugságvizsgáló készülék segítségével nyomoz. Ez pedig egyre több alkalommal fordul elő. Az egyik nagyvállalatnál összességében igen nagy értékben elkövetett lopások felderítése (és kétségkívül a továbbiak megakadályozása) céljából a dolgozók igen széles körének (860-ból 100–120 dolgozót érintően) hazugságvizsgálattal egybekötött „kockázatelemzését” határozták el. A tervezett vizsgálatnak csak egy részét folytatták le, mert az adatvédelmi biztos eljárása nyomán a vállalat vezetője a vizsgálatot leállította. Az adatvédelmi biztosnak az ügyben kialakított álláspontját azóta több hasonló ügyben hangoztatva számos ilyen vizsgálatot sikerült leállítani.

A büntetőeljáráson kívül, a múltbéli események felderítése céljából a munkáltató által végzett hazugságvizsgálat jogszerűségéről, és az ilyen vizsgálat eredményének a büntetőeljáráson kívül való felhasználhatóságáról szóló ügyben elsőként át kellett tekinteni,

³¹ A köztisztviselők jogállásáról szóló 1992. évi XXII. törvény, a továbbiakban: Ktv.

³² 95/A/1998.

hogy a hazugságvizsgáló készülékekkel egyáltalán milyen mértékben foglalkozik a magyar jog. A büntetőeljárás törvény nem tartalmaz rendelkezést a vallomások hazugságvizsgáló készülékkel való ellenőrzésre vonatkozóan,³³ noha a bírói gyakorlat néhány éve figyelembe veszi az ilyen vizsgálat eredményét. A szabad bizonyítás elvének megfelelően nem tekinti döntő bizonyítéknak: a büntetőeljárásban szabadon felhasználható minden olyan bizonyítási eszköz és bizonyíték, amely a tényállás megállapítására alkalmas lehet. A hatóságok ezeket egyenként és összességükben szabadon értékelik, és ezen alapuló meggyőződésük szerint bírálják el. A büntetőeljárásban azonban nem hagyható figyelmen kívül, hogy olyan eljárási garanciák érvényesülnek, amelyek ellensúlyozzák az eljárás alá vont személy hatóságokkal szembeni kiszolgáltatott helyzetét. A rendőrség által is csak szigorú feltételek teljesülése esetén végezhető hazugságvizsgálat. A rendőrségről szóló törvény szerint a Rendőrség csak büntetőeljárásban, vagy körözött személy felkutatásakor ellenőrizheti ilyen műszerrel az érintettet, és csak akkor, ha ahhoz az érintett előzetesen írásban hozzájárul.³⁴ A jogalkotó a hazugságvizsgáló alkalmazhatóságának szűk körű meghatározására törekszik, amikor a poligráfot bűnfelderítő eszközként határozza meg, amikor nemzetközi forgalmát korlátozza, a Magyar Köztársaság vámterületére történő behozatalát engedélyhez köti.

A büntetőeljáráson kívül pedig elsősorban a munkáltatók használják a poligráfot munkavállalóik, illetőleg a leendő munkavállalóik ellenőrzése céljából úgy, hogy a vizsgálat elvégzésével egy biztonságtechnikai, magánnyomozó, vagy pszichológiai szaktanácsadó céget bíznak meg. A munkahelyen elkövetett bűncselekmények felderítése esetében a munkáltatók kísérletet tesznek az elkövetői kör meghatározására.

Az adatvédelmi biztos állásfoglalása szerint a bűncselekmények felderítése és üldözése nem a munkáltató, hanem az arra hivatott szervek, a nyomozóhatóságok, az ügyészség és a független bíróság feladata. Egy gazdasági társaságnak nem állhatnak rendelkezésére a múltban történt események felderítésére olyan eszközök, amilyenekkel a bűnüldöző szervek rendelkeznek. A valamennyi dolgozóra vagy a dolgozók nagy hányadára kiterjedő vizsgálat ráadásul nem pusztán a munkavállalók személyes adatok védelméhez való jogát sérti, hanem emberi méltóságukat is, mert ellenőrzésükkel indokolatlanul széles körre terjesztik ki a „gyanúsítottak” körét. Így a dolgozók olyan helyzetbe kerülnek, amelyben úgy érzik, tisztáznuk kell önmagukat, és valódi akaratok ellenére is vállalják a vizsgálatban való részvételt. A biztos érvelése szerint egy jogállamnak meg kell találnia azokat az eszközöket, amelyek alkalmasak a bűncselekmények megelőzésére, és egyszersmind indokolt mértékben korlátozzák az egyének alapvető jogait. Még ennek elmaradása vagy

³³ Az azóta hatályba lépett új büntetőeljárás törvény már szól a poligráfós vizsgálatról, azonban csak a terhelttel összefüggésben, amikor úgy rendelkezik, hogy a vizsgálat elvégzése a terhelt hozzájárulásával történhet.

³⁴ A Rendőrségről szóló 1994. évi XXXIV. törvény 41. §-a.

nem kielégítő működése esetén sem lenne támogatható az, hogy az állampolgárok és a nem bűnmegelőzésre és -üldözésre hivatott szervezeteik maguk vegyék kezükbe az ilyen ügyeik megoldását, önhatalmúlag pótolva ezzel a feltételezetten vagy valóban ellátatlanul maradó állami feladatokat megvalósítását.

A poligráfós vizsgálat során a vizsgált személy személyes adatait hozza a vizsgálatot végző tudomására — legalábbis egy részében — akaratától függetlenül. Az egyik ilyen szolgáltatást nyújtó cég tájékoztatója szerint a „polygraph (hazugságvizsgáló) megfelelő alkalmazásával 98%-os megbízhatósági mutató érhető el. A polygraph olyan speciális készülék, amellyel egyszerre több élettani paraméter vizsgálható, és a vizsgálat során létrejött eltérések számítógépes adatfeldolgozással megbízhatóan regisztrálhatók, értékelhetők és tárolhatók”. Nyilván azért mondható el e módszerről, hogy megbízható, mert a vizsgált személyek akaratukkal nem tudják befolyásolni azt, hogy a kérdésfeltevést követően milyen információkkal látják el a készüléket és azon keresztül a vizsgálót. Az adatvédelmi törvény személyesadat-definíciója szerint a személyes adatok fogalmi körébe tartoznak nemcsak a vizsgálat során feltett kérdésekre a vizsgált személy által adott válaszok, hanem állításainak igaz vagy hamis voltára vonatkozó adatok is. Ezeket az adatokat a készülék és a vizsgáló észleli, rögzíti, értékeli, tehát adatkezelést végez. Személyes adatot kezelni csak az érintett hozzájárulásával, vagy törvény, illetőleg szűkebb körben önkormányzati rendelet felhatalmazása alapján lehet. Mivel jogszabály nem hatalmazza fel sem a munkáltatót, sem a megbízása alapján tevékenykedő biztonsági céget erre az adatkezelésre, azt e cég csak az érintett hozzájárulásával teheti.

Az Alkotmánybíróság állandó gyakorlatában az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jogot — annak aktív oldalát is figyelembe véve — információs önrendelkezési jogként értelmezi. Az egyén önrendelkezési joga, vagy más szóval az autonómia tiszteletének, a személyiség tiszteletének elve szerint minden autonóm embernek joga van szabadon, saját értékei és élettervei szerint dönteni és cselekedni, és ennek a jognak csak mások hasonló jogai szabnak határt. Ennek megfelelően az adatkezeléshez adott hozzájárulás csak akkor nyújt megfelelő alapot a személyes adatok kezeléséhez, ha az az érintett kívánságának önkéntes, határozott és tájékozott kinyilvánítása. Az érintettől azonban ebben az esetben nem várható el a *határozott, tájékozott, és önkéntes* hozzájárulás, mivel akaratlanul nem tudja befolyásolni személyes adatainak átadását, és az a poligráf készülék használata folytán akarata ellenére is megtörténik. Az önkéntesség kizárt azért is, mert a dolgozók a vizsgálatban való részvétel, az együttműködés megtagadása esetén egzisztenciájukat veszélyeztetik. A munkavállalók ettől való félelme megalapozott abban az esetben is, ha a munkáltatónak valóban nem áll szándékában őt a vizsgálat eredményétől illetve a hozzájárulás megadásától függően elbocsátani vagy más munkakörbe áthelyezni.

Felmerülhet a kérdés, hogy miért nem engedi meg a jog bárki számára poligráfus vizsgálat elvégzését. Az adatvédelmi biztos szerint az Alkotmányban biztosított emberi méltósághoz való jog nem teszi ezt lehetővé. A poligráfus vizsgálat során a személyiségnek egy olyan mértékű „átvilágítása” történik, amelynek következtében az érintett emberi méltósága sérül. Ezért csak rendkívüli garanciák érvényesülése esetén van lehetőség e készülék alkalmazására, ezek egyike az, amely szerint csak meghatározott szervek, meghatározott indokokkal, szigorú feltételek teljesítése esetén végezhetnek ilyen vizsgálatot. Ez az oka annak is, hogy a poligráfokat a magyar jog büntfelderítő eszköznek tekinti, és mint ilyennek Magyarországra történő behozatalát engedélyhez köti.

Nyomozási céllal az adatvédelmi biztos a poligráf alkalmazását a büntetőeljáráson kívül elfogadhatatlannak tartotta, és intézkedése nyomán az érintett cégnél megszüntették a vizsgálatot.³⁵

Az ilyen típusú ügyekkel kapcsolatban az állapítható meg, hogy az egzisztenciális vagy más szempontból kiszolgáltatott helyzetet magában hordozó munkaviszonyban a hozzájárulás, mint az adatkezelés jogalapja általában nem fogadható el. A hozzájárulásnak ugyanis önkéntesnek kell lennie, ami abban az esetben, ha a munkáltató úgy teszi fel a kérdést, hogy „Hozzájárul-e? Igen, vagy igen?”, akkor a munkavállalónak nincs választása, hiszen számolnia kell az elbocsátással.

2.4. Egyéb, a munkavállalók privacy-jét érintő ügyek

A munkáltatók adatéhsége olykor kifürkészhetetlen. A fent ismertetett, privacy-sértő, információ-szerzési céljaikon kívül időnként nagyon speciális, esetleg értelmetlen adatgyűjtésbe kezdenek. Olyan adatokat kérnek el a munkavállalóiktól, amelyek kezelésének célja egy munkaviszonyban nehezen magyarázható, vagy akár az adatgyűjtés célja egyenesen kifürkészhetetlen.

Egy felháborodott munkavállaló azzal fordult az adatvédelmi biztoshoz, hogy munkahelyén megtiltották nemcsak a saját mobiltelefonok használatát, hanem azt is, hogy azokat a munkavállalók akár kikapcsolva is a munkahelyükre bevigyék. Az adatvédelmi biztos ezekkel a sérelmekkel hatásköre hiányában nem tudott foglalkozni, állást foglalhatott azonban a munkáltató azon intézkedésével kapcsolatban, amely szerint a munkavállalóknak a saját tulajdonukban lévő mobiltelefonjuknak nemcsak a számát, hanem az arról kezdeményezett hívások listáját is át kellett adniuk. Bizonyos készenléti jellegű

³⁵ 354/A/2000. Hasonló ügyek: 661/H/2000, 33/K/2002.

munkakörök esetében elképzelhető lehet, hogy a telefonszámra a munkáltatónak szüksége van, ha a munkavállaló önként adja a telefonszámát, akkor kezelheti is. Ugyanakkor az adatvédelmi biztos szerint elképzelhetetlen olyan cél, amelyre tekintettel a munkáltatónak szüksége lenne a munkavállaló által, a saját mobiltelefonján folytatott beszélgetések adataira, ezért azok kérését nyilvánvalóan ellentétesnek találta a célhoz kötöttség elvével.³⁶

Ehhez hasonló volt az az ügy, amely szerint a beadványozó munkahelyén mindenkitől elkérték a járművezetői engedély és az útlevél számát, függetlenül attól, hogy ki milyen munkakörben dolgozott. Az e személyes adatokat megadni nem kívánó dolgozókkal közölték, hogy nem kötelező ott dolgozni. Az adatvédelmi biztos szerint a célhoz kötöttség követelményével ezen adatkezelés is ellentétes volt.³⁷

2.4.1. A munkavállaló politikai múltjára irányuló adatgyűjtés

Speciális munkahelyen, speciális adatfajták gyűjtésével volt kapcsolatos az adatvédelmi biztosnak az a vizsgálata, amelyben a Magyar Honvédség parancsnokának azon titkos parancsával foglalkozott, amely szerint valamennyi katonai alakulatnak listát kellett készítenie azokról a ma is szolgálati viszonyban lévő személyekről, akik 1990. előtt a pártállami időszakban a Honvédségnél politikai helyettesként, párttitkárként, illetve a magasabb katonai szervezeteknél függetlenített politikai munkásként szolgáltak. A honvédelmi miniszter a beadványozó állításával szemben úgy nyilatkozott, hogy a Magyar Honvédség parancsnoka nem adott ki és nem is kapott titkos parancsot az 1990. előtti politikai szerepvállalásra vonatkozó adatgyűjtésre. A Magyar Honvédség parancsnoka viszont részletesen beszámolt a vizsgálatról. Előadta, hogy a vizsgálat célja a Honvédség stratégiai felülvizsgálatának, korszerűsítésének, egy modernebb, létszámában is kisebb, mobilabb és jobban finanszírozható, hadrafoghatóbb haderő kialakításának előkészítése volt. Az előkészítő munka során utasítást kapott a minisztertől, hogy a személyügyi szervekkel vizsgálta meg azt, hogy azok a jelenleg aktív vagy szolgálatot teljesítő tábormok és tisztek, akik 1990. előtt politikai tiszti vagy az akkori állampártban pártfunkciót töltöttek be, rendelkeznek-e azokkal a katonai szakmai végzettségekkel, amelyeket jelenlegi beosztásukhoz a törvény előír. A vizsgálat során az adatvédelmi biztos birtokába jutottak azok a listák, amelyek a parancsnak megfelelően készültek. Ezek „pártcsoportbizalmi”, „pártbizottsági tag”, „KISZ-bizottsági titkár”, „politikai helyettes” megjelölés szerepelt. A listákon azonban szakmai végzettségre, valamint szakmai előmenetelre utaló adatok nem voltak. Kiderült, hogy a listakészítést követően többek szolgálati viszonyát megszüntették.

³⁶ 429/A/2002.

³⁷ 174/A/2002.

Tekintettel arra, hogy a megkérdezett honvédelmi vezetők egymással ellentétes tartalmú nyilatkozatokat tettek, illetve nem tettek maradéktalanul eleget válaszadási kötelezettségüknek, az adatvédelmi biztosnak nem állt módjában megállapítani, kinek az utasítására készültek a vizsgálat tárgyát képező listák, azok létezése azonban bebizonyosodott.

Az adatvédelmi biztos vizsgálat megállapította, hogy az adatgyűjtés a megjelölt cél eléréséhez nem elengedhetetlen, arra nem is alkalmas, mégpedig két okból kifolyólag. Az adatgyűjtés kizárólag olyan személyekre korlátozódott, akik 1990. előtt politikai tisztí vagy pártfunkciót töltöttek be. A végzettség megléte szempontjából azonban irreleváns az érintettek politikai múltja, párttal való kapcsolata. A fent leírt célt csak teljes körű, tehát valamennyi tisztre kiterjedő adatgyűjtés szolgálta volna, ennek eredménye mutatta volna meg azt, hogy valóban mindenkinek megvan-e a szükséges végzettsége. A listák továbbá nem tartalmaztak információt arra vonatkozólag, hogy az azon szereplő korábbi politikai tisztek vagy korábban pártpolitikai tevékenységet folytató személyek milyen szakmai végzettséggel rendelkeznek. Ennek következtében a listák teljességgel alkalmatlanok voltak a megjelölt cél elérésére, akár egyetlen személy szükséges szakmai végzettsége meglétének megállapítására is. Az adatvédelmi biztos ezért az adatgyűjtést jogellenesnek találta, és felszólította a Magyar Honvédség vezetőit, hogy a törvénytelenül készített listákat — az érintettek tájékoztatásával egyidejűleg — haladéktalanul semmisítsék meg.³⁸ Az ügy nagy visszhangja mutatja, hogy a politikai múlt a különleges adatok közül is az érzékenyebbek közé tartozik.

2.4.2. A vallásos vagy más meggyőződésre vonatkozó adatok kezelése a munkahelyen

A különleges adatok egy másik fajtája, a vallásos meggyőződésre vonatkozó adatok munkahelyen történő „kötelező” kezelése borzolta a kedélyeket 2001. folyamán. Az ilyen adatokat Magyarországon a történelmi tapasztalatok és jelenleg is ható politikai indulatok miatt az átlagosnál jobban szokás félteni. A Ktv. módosításával minden egyes köztisztviselőnek esküt kellett tennie, a törvény szerint pedig az eskü szövege az eskütevő meggyőződése szerint kiegészülhetett az „Isten engem úgy segítjen!” záradékkal. Az eskünek nemcsak szóban kellett elhangoznia, hanem írásban is meg kellett erősíteni, az esküokmányok elkészítése előtt pedig nyilatkoztatták a köztisztviselőket, hogy „istenes” vagy enélküli esküokmányt szeretnének-e aláírni. Sokan megfélemlítve érezték magukat, úgy érezték, elvárásnak kell eleget tenniük egyik vagy másik változat választásával.

³⁸ A Magyar Honvédségnél szolgálati viszonyban álló tisztek politikai múltjáról való adatgyűjtéssel kapcsolatos vizsgálat megállapításait összegző adatvédelmi biztos ajánlás. 2000. szeptember 14., 226/A/2000.

A jogszabály a meggyőződésnek megfelelő esküszöveg elmondását tette kötelezővé, így tulajdonképpen kötelezővé tette a meggyőződés kinyilvánítását. A törvény a lelkiismeret- és vallásszabadság korlátozását több tekintetben is megvalósította, a kinyilvánítás kötelezővé tétele mellett meghatározta annak körülményeit is: a meggyőződés megvallásának a munkáltatói jogok gyakorlója és a munkatársak előtt kellett történnie, szóban és írásban egyaránt nyilatkozni kellett. Mivel a záradék szövege a törvényben meghatározott, a nyilatkozat tartalma tekintetében is érvényesültek bizonyos korlátok, aki tehát nem Istenre, hanem istenekre, vagy akár nem is istenségre, hanem az Ősanyára akart esküt tenni, mert meggyőződése ezt diktálta, nem tehetta meg, illetőleg azt mondott, amit akart, de az írásbeli megerősítésen ez már nem szerepelhetett.

A lelkiismereti és vallásszabadság korlátozása mellett az ilyen módon meghatározott eskünek voltak adatvédelmi vonatkozásai is. Az, hogy az eskütevő elmondja-e esküje végén az „Isten engem úgy segítjen” záradékot, személyes adat. Nem is akármilyen, hanem különleges adat, mivel az érintett vallásos vagy más meggyőződésére utal, vagy legalábbis alkalmas arra, hogy abból valaki erre vonatkozó következtetést vonjon le. A közfelfogás szerint az esküjében foglaltakhoz a vallásos ember hívja segítségül Istent, az adatvédelmi törvény szerint pedig személyes adatnak kell tekinteni valamely adatból levonható, az érintettre vonatkozatható következtetést is, függetlenül annak valós vagy valótlan voltától. A záradék elmondása tehát akkor is a vallásos vagy más meggyőződésre utaló személyes adat, ha az eskütevő csak az esemény ünnepélyességének, fényének emelése céljából teszi azt hozzá a kötelező szöveghez, nemcsak a közfelfogás miatt, hanem azért is, mert maga a törvény rendelkezik úgy, hogy az eskütevő a meggyőződése szerint választhatja vagy hagyhatja el a záradékot. Bárhogy is dönt az eskütevő, akár záradékos, akár záradék nélküli az esküje, az eredmény mindenképpen a meggyőződésre vonatkozó adatnak a közigazgatási szerv, a főnök és a kollégák tudomására hozása: harmadik lehetőség, amely az adat titokban tartását tenné lehetővé, nincs. Ha nem teszi az esküje végére a záradékot, akkor ugyanis azt az adatot közli magáról, hogy meggyőződése szerint nem istenhívó. Ilyen különleges adatot viszont a köztisztviselőt foglalkoztató szerv nem kezelhet, még akkor sem, ha a köztisztviselő ehhez hozzájárul, történelmi okokból ugyanis a törvény úgy rendelkezik, hogy állami nyilvántartásba vallásos meggyőződésre vonatkozó adat nem vehető fel.

A törvény hatálybalépésének idején az adatvédelem helyzete sajátos volt: az Országgyűlés fél éven keresztül nem választott adatvédelmi biztost, helyette adatvédelmi ügyekben az állampolgári jogok országgyűlési biztosa járt el. Szerinte az eskü ilyen szabályozás mellett nem sértette az állampolgárok jogait, szerinte az „Isten engem úgy segítjen!” szövegrész választása és kinyilvánítása esetén sem tudhatja senki, hogy az az eskütevő miféle meggyőződését tükrözi, abból a bármely kívülálló által levont következtetés csak a saját szubjektív értékítéletét, lelkiismereti meggyőződését (sic!) tükrözi. Állásfoglalásának egy

másik részében ezzel szemben azt állapította meg, hogy az olyan esküokmányban, amely az eskütevő választásának megfelelően tartalmazza, vagy nem tartalmazza az „Isten engem úgy segítjen!” mondatot, különleges adat szerepel, mert általánosságban alkalmas lehet az érintett lelkiismereti meggyőződésére vonatkozó következtetés levonására is. Az ügyet azzal zárta, hogy nem kellett megsemmisíteni azokat az esküokmányokat sem, amelyek a köztisztviselő választása szerint tartalmazzák vagy mellőzik a záradékot.³⁹

Az ügy iránt érdeklődést tanúsító közvéleményt az eskünél csak ez az állásfoglalás osztotta meg jobban. Álláspontunk szerint, ha lett volna adatvédelmi biztos, másképpen oldódott volna meg ez az ügy. Megfelelő jogalap hiányában, sőt erre vonatkozó kifejezett tilalmat megfogalmazó rendelkezés mellett a közigazgatási szerv nem kezelheti a köztisztviselők vallásos vagy más meggyőződésre vonatkozó adatait. Az eskütevő nem válogathatja ki azokat a munkatársait sem, akik előtt szívesen feltárná meggyőződését. Ezért a szóban elmondott eskü esetében, amikor az eskütevő választ a kétféle szöveg közül, mindazok jogosulatlanul szereznek tudomást a meggyőződésről, akik az eseményen jelen vannak. Ha eltekintünk a szóbeli eskütétel problémáitól, és a továbbiakban az eskütétel írásban történő megerősítésére és arra szorítkozunk, hogy a megerősítést tartalmazó esküokmánynak mi lesz a sorsa, találhatunk olyan megoldást, amellyel a jogellenes adatkezelés elkerülhető. Amennyiben az eskü írásban történő megerősítését tanúsító esküokmány a törvény szövegének pontos átvételével, átmásolásával készül el, tehát mindenkire nézve azonos szöveget tartalmaz, nem készítenek záradékkal ellátott és záradék nélküli változatokat, a meggyőződésre utaló adat nem kerül jogellenesen a köztisztviselő személyi anyagába. Sok közigazgatási szervnél nem így készítették el az esküokmányt, hanem előre megkérdezték a köztisztviselőket, hogy záradékos vagy záradék nélküli változatot kérnek-e. Ahol kétféle esküokmány közül kellett választani, ott ma törvénytől függetlenül az emberek vallásos meggyőződésére vonatkozó adatait, az ilyen okmányokat a legjobb lenne megsemmisíteni. Ahol azonban az esküokmányon szereplő szöveget pontosan kimásolták a törvényből, így csak egyféle papír készült, álláspontunk szerint nem sértették meg az adatvédelem szabályait.⁴⁰

³⁹ 615/A/2001.

⁴⁰ Szabó Máté Dániel: Alkotmányossági kérdések a köztisztviselői eskü záradékával kapcsolatban. *Fundamentum*, 2002. 1. szám. 111–116. oldal.

3. A munkahelyi privacy helyzetének általános értékelése

A szerzők szakmai és magánéleti tapasztalatai alapján a munkahelyi privacy, illetve a munkavállalók személyes adatainak védelme jellemzésére nem alkalmas egyetlen jelző vagy egyetlen koherens leírás. Széles a skála: az alkalmazottaik személyiségét mintegy információs és pszichológiai rabszolgaságban tartó — csak közvetett bizonyítékokból ismerhető — vállalatoktól a személyiségi jogokat tiszteletben tartó munkahelyekig számos adatkezelői típussal találkozhatunk. Nagy általánosságban a helyzet — elsősorban a jogszabályi rendelkezések és az adatvédelmi biztos működése miatt — jobbnak tekinthető, mint a volt szovjet blokk számos országában, ugyanakkor tükrözi a legtöbb problémát, amivel a fejlett országok is küzdenek, tetézve a rendszerváltásból adódó speciális problémákkal.

Amint azt az ismertetett esetekből és a jogi helyzet általános áttekintéséből láhattuk, Magyarországon a jog erős garanciákat nyújt a munkavállalók személyes adatainak védelmére, annak ellenére is, hogy a munka világára vonatkozó szektorális adatvédelmi szabályozás hiányzik a magyar jogrendszerből. Az is látható, hogy az adatvédelmi biztos magas szakmai színvonalú gyakorlatával megfelelő védelmet nyújt a jogaikat érvényesíteni kívánó munkavállalóknak és mintegy pótolja a bírói gyakorlat hiányosságait.

Műfaji és terjedelmi korlátaink között természetesen nem volt célunk az összes ügytípust részletesen bemutatni; tanulmányunkban csupán a legfontosabb problémák, érvek és jogi állásfoglalások kiemelésére törekedtünk. Az ismertetett ügyek többsége — az adatvédelmi biztosi esetek sajátosságaiból adódóan — *panaszügy* volt (esetleg konzultációs ügy, amely valamely eldöntendő kérdésre, problémára irányult), ezekből tehát csak közvetett képet kapunk a munkahelyi adatvédelmi jogérvényesítés szintjére, és még közvetettebbet a magyarországi munkahelyi privacy általános helyzetére vonatkozóan.

A nemzetközi szakirodalomban a közelmúltban megjelent a magánélet, illetve a személyes adatok védelmének egyfajta pragmatikus megközelítése, amelynek központi eleme a privacy „ésszerű”, „elvárható” mértéke. E megközelítés számos vitatható elemet tartalmaz és alapvető értékek és jogok erodálásával fenyeget, ugyanakkor tükrözi a jogszabályi rendelkezések és az adatkezelési gyakorlat közötti ellentmondások feloldásának szükségességét. Meddig terjednek tehát a privacy „ésszerű”, „elvárható” határai a magyarországi munkahelyeken?

Az ésszerűség és elvárhatóság többféleképpen értelmezhető: jogi és társadalmi szempontból szükségképpen, de a mai adatkezelés közegében a technológiai szempont is egyre

fontosabbá válik.⁴¹ Ami a jogi megközelítést illeti, Magyarország, nem meglepően, az európai (most már európai uniós) adatvédelmi szabályozási modellt⁴² követi, amire korábban többször hivatkoztunk. A magyar adatvédelmi jog néhány vonatkozásban némiképp szigorúbb védelmet biztosít az Európa Tanács ill. az EU által megkövetelt minimumnál⁴³ (például ilyen volt az EU csatlakozás előtt a határátlépő adatáramlás feltételeire vonatkozó rendelkezés⁴⁴), de volt diktatúrák esetében a védelem magasabb szintje érhető és elvárható. Az ismertetett adatvédelmi biztosítási esetekben, a kevés bírói ítéletben és általában a jogi okfejtésekben az „elvárhatóság” fogalma nem játszik jelentős szerepet, bár implicit módon természetesen megjelenik bennük. Az adatvédelmi biztos vagy a bíró helyett a jól kidolgozott általános és szektorális jogszabályi rendelkezésekből⁴⁵ vezeti le álláspontját, illetőleg — elsősorban az adatvédelmi biztos esetében — saját állásfoglalásainak, ajánlásainak esetjogi természetű, jogfejlesztő sorára támaszkodik.

Vajon merevebb-e, és egyben a valóságtól elrugaszkodottabb-e ez a rendszer az amerikai adatvédelmi szabályozási felfogáshoz, vagy a *reasonable privacy* fogalmához képest? A Magyarországra (és egyben a régió rendszerváltó országaira) jellemző helyzet ismeretében nem így gondoljuk. Megítélésünk szerint párhuzamosan kell érvényesülnie a jogi és a társadalmi fejlődésnek: a világos, végrehajtható szabályok gyorsabb megszületésének és betartatásának, valamint a lassabb társadalmasodási folyamatnak, ami e szabályoknak a mindennapi életben releváns, „ésszerű” tartalmat ad, és ami idővel nemcsak a munkavállalók, hanem a munkaadók viselkedésére is kihat majd. Természetesen több folyamat hat egyidejűleg; a magánélet határai megváltoztak és folyamatosan változnak, azonban az ahhoz fűződő — a fejlett nyugati demokratikus társadalmak egyik pillérét jelentő — alapvető értékek feltehetően nem változnak, sőt a rendszerváltó országokban kissé megkésve szilárdulnak meg. Ezért az elmúlt másfél évtizedben kialakult felfogás, megújult jogrendszer, formálódó jogérvényesítési lehetőségek és gyakorlat helyett nem

⁴¹ Az alkalmazott adatkezelési technológia eleve meghatározza az információs privacy lehetőségeit, ráadásul működése általában nem ismert részleteiben az adatalanysok előtt.

⁴² Az európai és amerikai modell eltéréseinek egy lehetséges megközelítésére lásd Székely I.: Adatvédelem és nyilvánosság. In: Lajtha Gy. (szerk.): *Távközlő hálózatok és informatikai szolgáltatások*. Hírközlési és Informatikai Tudományos Egyesület, Budapest 2002. Online kiadás. <http://www.hte.hu/onlinekonyv.html>

⁴³ Magyarország 1994-ben aláírta, 1997-ben ratifikálta az Európa Tanács adatvédelmi egyezményét (ETS No. 108), 2000-ben megkapta a magyarországi adatvédelem megfelelő szintjéről szóló európai bizottsági határozatot (Commission Decision on the adequate protection of personal data provided in Hungary, 2000/519/EC), 2004 májusától pedig az Európai Unió tagjává vált, így vonatkozik rá az EU adatvédelmi direktívájának (95/46/EC) hatálya.

⁴⁴ Avtv. 9. § (1993. végéig hatályos szöveg): „Személyes adat az országból — az adathordozótól vagy az adatátvitel módjától függetlenül — külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adata nézve teljesülnek.”

⁴⁵ Igaz, hogy fentebb éppen a munka világában hiányoltuk e szektorális szabályokat.

tartanánk helyesnek egy pragmatikusabb, az elvárhatóságon, ésszerűségen, illetve az önszabályozáson alapuló rendszer bevezetését.

A helyzet megértéséhez érdemes az információs viszonyokat a hatalmi viszonyok szempontjából vizsgálni, egy olyan tágabb kontextusban, ahol a munkahely része az információs és egyben hatalmi játéktérnek.

Mint közhelyszerűen ismert, az információ hatalom, s a rendszerváltás utáni új információs rezsim e hatalom újraelosztását, demokratizálását jelentette, mind a közinformációk hozzáférhetősége terén, mind a személyes adatok feletti önrendelkezés biztosítása terén. A rendszerváltás körüli időkben az információs jogok iránti igény szorosan összefüggött a szabadság iránti igénnyel, és az információs jogok a közfelfogásban az alapvető emberi jogok és szabadságok részévé váltak.⁴⁶ Bár az Alkotmánybíróság metaforája szerint⁴⁷ az emberi jogok érvényesítése egyirányú utca, ahol nincs helye a visszafordulásnak, mégis a konszolidáció éveiben egyes információs jogok érvényesíthetősége beszűkült, a közigazgatás haszonelvű és hatékonyság-elvű törekvései egyre többször ütköznek az információs privacy-t biztosító rendelkezésekkel, s a technikai modernizációval ismét az „igazgatandó” társadalom, a kényelmet a biztonság és az önrendelkezés elé helyező polgár víziója kerül előtérbe. E jelenség része az állami és magánszektor információkezelőinek összefogása a mindinkább fogyasztóvá váló állampolgárral szemben.

Nemcsak az információ, a pénz is hatalom, s a rendszerváltás egyúttal a tőke újraelosztását is jelentette, pontosabban egy megkésett eredeti tőkefelhalmozódást, a régió többi rendszerváltó országában történetekhez hasonlóan. E folyamat része volt a tömeges privatizáció,⁴⁸ s létrejöttek az új üzleti és egyben információkezelő monopóliumok. Bár voltak egyes kezdeményezések a korábbi rendszerben felhalmozódott anyagi javak demokratizálására is (lásd munkavállalói részvényprogramok), a folyamat egésze az anyagi javak új birtokosai és a birtoklásból kimaradtak státusának erőteljes polarizációjához vezetett. Számos munkahely került át a magánszektorba, ahol egyúttal új munkahelyek és munkakörök teremtődtek: a javak új birtokosai munkaadókká, a birtoklásból kimaradtak munkavállalókká váltak. A magánszektorban viszont — a közszektorral és az új nyilvánossággal ellentétben — nem volt jog-biztosítási (köztük: információs

⁴⁶ A fejlett Nyugat lelkesen üdvözölte e fejleményeket; ennek egyik szakmailag is hiteles példája David H. Flaherty, Brit Columbia (Kanada) korábbi adatvédelmi és információszabadság biztosának üzenete, amely saját, 1995–1996. évi jelentésének előszavába is bekerült. Lásd: http://www.oipcbc.org/publications/annual_reports/1997AR/comm97.html Magyar fordításban: *Az adatvédelmi biztos beszámolója 1997*, 424–425. old.

⁴⁷ Idézi az adatvédelmi biztos, lásd <http://abiweb.obh.hu/adatved/magyar/1998/M043-127-1.htm#3.1.1> vagy <http://abiweb.obh.hu/adatved/magyar/b032.htm>

⁴⁸ Ennek során az anyagi javakkal együtt gyakran az információvagyon is magánkébe került.

jog-biztosítási) hullám, itt rögtön az új kapitalizmus szabadossága érvényesült, ami a munkavállalók érdekérvényesítő képességét és egyben információs státusát korlátozó trendekben is megnyilvánult.

Megítélésünk szerint ez az egyik alapvető oka, hogy az aktuális munkahelyi privacy problémák zöme Magyarországon az üzleti szektor munkáltatóinál tapasztalható.⁴⁹ A rendszerváltás munkahelyekre gyakorolt hatásai is itt érvényesültek és érvényesülnek a legmarkánsabban: ilyen hatásokkal jártak a klasszikus kapitalizmus megkésett jelenségei, az amúgy is hitelét veszített szakszervezeti mozgalom hanyatlása (gyakorlatilag kizárása egyes új üzleti szektorokból), valamint egyes nyugati beruházó cégek meggyőződése, mely szerint az új demokráciákban a dolgozók jogérvényesítő igénye és képessége kisebb, mint Nyugaton, ezért itt olyan technikák alkalmazása is megengedhető, amelyek fejlett országokban már nem szalonképesek.

Ehhez járul a kései eredeti tőkefelhalmozás után bekövetkezett élesedő verseny, valamint az ezt kísérő „egyfaktoros” gondolkodásmód, ami a piac- és profitszerzést abszolutizálja és a „korszerű” vállalatiirányítási stratégiák bevezetésével mind a dolgozót, mind az ügyfelet egyszerű közgazdasági elemnek tekinti.

E trendekbe jól illik a modern human resource management technikák divatja: a már említett pszichológiai tesztek készítése, a fejtudás cégek szerepének növekedése, valamint a korszerűnek tekintett, technokratikus és algoritmizált vállalatiirányítást követő cégek azon gyakorlata, hogy munkavállalóikat érdekérvényesítő képességük és kommunikációs lehetőségeik szempontjából igyekeznek atomizálni. E törekvések szigorú (esetenként kétséges jogszerűségű) munkaszerződésekben tükröződnek, amelyek egyik célja, hogy legalizálják a munkahely személyesadat-kezelési gyakorlatát.

Nem elszigetelt tapasztalat, hogy a munkavállalók félnek adatvédelmi jellegű panaszukat artikulálni, nyilvánosságra hozni, még inkább az adatvédelmi biztoshoz vagy bírósághoz fordulni. Kiszolgáltatott helyzetükből adódóan — amit paradox módon egy átlagosnál magasabb fizetés is megerősíthet — tartanak állásuk elvesztésétől, munkáltatójuk retorzióitól, esetleg nem hivatalos (és nem legális) feketelistára kerülésüktől, ami megnehezíti későbbi elhelyezkedésüket. E tanulmány egyik társszerzőjének gyakorlatában fordult elő egy olyan eset, hogy egy egyetemi diákja kérésére titkos találkozót kellett megszerveznie a diák ilyen munkahelyen dolgozó szülője és az adatvédelmi biztos között,

⁴⁹ Természetesen a közszektor egyes sajátos adatvédelmi problémái, mint például a politikai vagy ügynök-múlttal kapcsolatos adatok felhasználása sem elhanyagolhatók.

mert csupán az adatvédelmi biztossal való konzultáció tényének kiderülése is az állás elvesztésével fenyegetett.

Ellentétes-e tehát a jogszabályokból és az adatvédelmi biztos ajánlásaiból tükröződő helyzet a valósággal? Vajon csak azért ilyen erős a szimbolikus védelem, mert a valóságos helyzet olyan rossz? Szerencsére ez nem állítható: az adatvédelmi jog — legalább is általános szinten — beépült a köztudatba, és bár számos adatkezelő csak fő tevékenységének értelmetlen korlátozását látja benne, az adatvédelmi biztos ajánlásait általában elfogadják. Azok a munkavállalók, akik magánéletükben érzékenyek privacy-jukra, munkahelyi jogaikkal is általában tisztában vannak, s bár nem mindig merik és akarják érvényesíteni e jogokat, ez mégis valamelyest korlátozza a munkaadó, illetve a vezetőség információs hatalmát, mozgásterét a munkavállaló adatainak kezelésében.

Az információs privacy mértéke, annak „ésszerű” volta nemcsak jogértelmezés kérdése, függvénye az adatkezelő felfogásának és az adatalányok elvárásainak, érzékenységének egyaránt. 1989–90 fordulóján (tehát a rendszerváltás turbulens időszakában) készült Magyarország és a régió első és feltehetően mindmáig egyetlen átfogó adatérzékenységi vizsgálata: tanulmányai szerint az adatalányok általában tájékozottak és gyanakvók az adataikkal való visszaélések tekintetében, ugyanakkor engedelmes adatszolgáltatók. Feltehetően e kép a munkahelyek adatkezelési helyzetére is érvényes. A vizsgálat további jelentős megállapítása, hogy az adatfelvétel idején a magyar lakosság 16 százaléka szignifikánsan érzékenyebb volt adatai sorsát illetően és jelentős adatvédelmi tudatosságot árult el; ugyanakkor e sajátosság semmilyen értékelhető összefüggést nem mutatott a szokásos demográfiai változokkal. Ez a megállapítás arra utalt, hogy az információs önrendelkezés igénye nem az ismert társadalmi szereposztások szerint oszlik meg, hanem egy sajátos dimenziót képvisel. Sajnos, azóta nem volt mód hasonló részletességű vizsgálat elvégzésére, amely az adatkezelési szintéren a rendszerváltás óta bekövetkezett jelentős változásokat feltárná.

Felértékelődőben van az adatvédelmi auditálás gyakorlata, bár az adatkezelők többnyire csak valamilyen probléma, kritika, rossz publicitás, avagy a felügyeleti szerv ellenőrzésének veszélye esetén fordulnak külső szakértőkhöz. Ugyanakkor jól jellemzi a munkahelyi privacy helyzetét és megítélését, hogy az ilyen auditálások általában csak az ügyfelek vagy harmadik személyek adatainak kezelésére terjednek ki, a dolgozókéra nem.

Fontos változások léptek hatályba 2004 januárjában az adatvédelmi törvény módosításával: az adatvédelmi biztos hatósági jellegű jogosítványokat kapott, ellenőrzési, szankcionálási jogköre — összhangban az EU követelményeivel — jelentősen kibővült. Az új rendelkezések belső adatvédelmi felelősök kinevezését, illetve megbízását teszik

kötelezővé országos hatósági, munkaügyi vagy büntügyi adatállományt kezelő, illetve feldolgozó szervezeteknél, pénzügyi szervezeteknél, valamint távközlési és közüzemi szolgáltatóknál.⁵⁰ Noha az új felelősök feladatai főként az ügyfelek és harmadik személy adatainak kezelésére irányulnak, működésük vélhetően jótékony hatást gyakorol majd a munkahelyi privacy alakulására is. Szerepük mindazonáltal nem lesz irigylésre méltó, kissé hasonlóan a belső ellenőrökéhez: egy technokrata, profitorientált közegben könnyen a kerékkötőt láthatják működésükben.

Az új információs és kommunikációs technológiák Magyarországon is egyre meghatározóbb szerepet játszanak a személyes adatok, így a munkavállalók személyes adatainak kezelésében is. Az informatikus (a személyesadat-kezelő rendszerek tervezője és működtetője) alapesetben mindig az erősebb fél — esetünkben a munkaadó — természetes szövetségese: tőle kapja a megbízást, az anyagi ellenszolgáltatást, benne látja karrierje lehetőségeit. Ezért a kifejlesztett rendszerek általában egyoldalúan a megbízó érdekeit és értékrendjét tükrözik, s kevés az olyan, munkavállalói adatokat kezelő, a munkavállalókat korrekt módon, a jogszerű kereteken belül maradván ellenőrző informatikai rendszer, amely az üzleti célokat és érdekeket egy korszerű adatvédelmi szemlélettel párosítva érvényesíti.

A szerzők azonban némileg optimisták az oktatás hatásainak megítélésében (maguk is egyetemi oktatók a tárgyalattal összefüggő területeken): a tág értelemben vett adatvédelem és az információs privacy oktatása több szinten jelen van a magyar oktatási kínálatban, az egyetemi szaktárgyaktól a rövid tanfolyamokig. E fórumokon nemcsak jogászok, hanem adatkezelők, államigazgatási és üzleti vezetők, belső adatvédelmi felelősök és informatikusok is részt vesznek, s ennek eredményeképpen legalább is tudatában vannak a legfontosabb alapelveknek, szabályoknak és gyakorlati megoldásoknak, még akkor is, ha nem mindenkor törekednek azok betartására és érvényesítésére.

Az oktatásnak azonban hosszabb távú hatásai is vannak: az adatvédelmi biztos jogpropagátori tevékenységével, a sajtó és az egyelőre nem túl jelentős civil szektor segítségével a személyes adatok — s ezen belül a munkavállalói személyes adatok — korrekt kezelése az általános adatkezelési etika részévé válik, s ennek már tapasztalhatók a gyakorlati jelei.

⁵⁰ Belső adatvédelmi felelősök állítását korábban is előírták egyes szektorális jogszabályok, így például az egészségügyi adatok kezelése terén, az új szabályozás azonban jelentősen kibővíti a kötelezettek körét és meghatározza a belső adatvédelmi felelősök feladatait.