MUNKAHELYI ADATVÉDELEM

NEMZETI JELENTÉS – MAGYARORSZÁG

SZERZŐK

Dr. Szőke Gergely László

Dr. Balogh Zsolt György

Dr. Polyák Gábor

Dr. Rátai Balázs

A projekt az Európai Unió "Fundamental Rights and Citizenship" programjának társfinanszírozásával valósul meg.

2012. JANUÁR

TARTALOMJEGYZÉK

1. BEVEZETÉS ÉS HÁTTÉR

1.1. A kutatás célja és módszertana

Az országjelentés fő célja a munkahelyi adatvédelem hatályos magyar szabályozásának és a szabályozás európai kontextusának bemutatása. Az elkészült országjelentések alapján összehasonlítjuk továbbá a magyar és a német szabályozást. Célunk tehát a jelenlegi helyzet feltérképezése és leírása – a következtetések levonása és a módosító javaslatok megfogalmazása a kutatás következő fázisának feladata.

Nem foglalkozunk az egyes munkavállalókat érintő minden adatvédelmi kérdéssel. Kutatásunk a technikai megfigyelés szabályozására irányul, annak érdekében, hogy megkülönböztessük a munkavállalók jogszerű megfigyelését az illegális adatgyűjtéstől. Ez a munkahelyi adatvédelemnek Magyarországon és az Európai Unióban egyaránt meghatározó problémaköre.

A hatályos jogszabályokon túl összefoglaljuk a kapcsolódó joggyakorlatot is. Megvizsgáljuk az adatvédelmi biztos kapcsolódó ajánlásait, valamint a kapcsolódó bírósági gyakorlatot. A kutatás tárgyát képezik továbbá a jogi szakirodalom, valamint az önszabályozás esetleges forrásai.

Az adatvédelem, a magánélet védelmének alapvető koncepcionális kérdéseit összefoglaló fejezetek után a különböző technikai megfigyelési eszközökre vonatkozó magyar szabályozást elemezzük. Maga a szabályozás jellemzően nem tesz különbséget technológiák alapján, így a különböző technológiákra nagyrészt azonos szabályok alkalmazandók. Az ismétlések elkerülése végett így egyes csak más alfejezetekre utalnak. A technológiák szerinti felosztást azért választottuk, mert az adatvédelmi biztosi és a bírósági döntések is egy-egy technológiára irányulnak. A projekt során összeállítandó magatartási kódex várhatóan szintén technológia-specifikus előírásokat fog tartalmazni.

1.2. A hatályos jogszabályok rövid áttekintése

E fejezetben a munkahelyi adatvédelem hatályos nemzetközi, európai és magyar szabályozását tekintjük át.

1.2.1. Nemzetközi és közösségi jogi források

1.2.1.1. Az ILO kódexe

A Nemzetközi Munkaügyi Szervezet[1] (a továbbiakban ILO) kezdeményezésével és támogatásával elkészült egy magatartási kódex,[2] amely átfogóan foglalkozik a munkavállalók személyes adatainak védelmével. A kódexhez készült egy hitelesített, a szövegbe ágyazott kommentár is. Nyilvánosságra hozatalát és terjesztését az ILO vezető testülete 1996 novemberében hagyta jóvá.

[1] International Labor Organization, ILO
[2] ILO Code of Practice, 1997, a továbbiakban ILOC

A kódex 2. pontja szerint a kódex kizárólag iránymutatásként szolgál, kötelező erővel nem bír. Azt is rögzíti, hogy a kódex „nem helyettesíti a nemzeti jogszabályokat, szabályzatokat, nemzetközi munkaügyi standardokat. Felhasználható a jogalkotás, a szabályzat-alkotás, a kollektív szerződések, a munkahelyi előírások, a szakpolitika és a gyakorlati mércék előmozdítására." A kódex a köz- és magánszektorra, illetve a manuális és az automatizált adatkezelésre egyaránt kiterjed. Munkavállaló alatt a jelenlegi és korábbi munkavállalókat és alkalmazottakat érti.

1.2.1.2. Az Európa Tanács megközelítése

Az 1980-as években az Európa Tanács az adatvédelem nemzetközi szabályozásában élenjáró szervezet volt. Az egyéneknek a személyes adatok automatizált kezelésével szembeni védelméről szóló, 1981. január 28-án elfogadott egyezmény (a továbbiakban Egyezmény) az adatvédelem egyik korai és átfogó dokumentuma. Az ET számos speciális területen is megfogalmazott ajánlásokat, a kutatásunkat érintően ilyen az R (89) 2 számú ajánlás a foglalkoztatási célú személyes adatok védelméről. Ez a korai dokumentum számos témakört érint és jelentős hatást gyakorolt a későbbi tagállami jogalkotásra.

1.2.1.3. Az Európai Unió kezdeményezései

Mindenekelőtt meg kell említenünk az általános adatvédelmi irányelvet, a 95/46/EC irányelvet,[3] amelyet minden tagállamnak implementálnia kellett. A jogharmonizáció eredményeként az adatvédelem alapvető elvei minden tagállamban azonosak. A távközlés területén a 2002/58/EC irányelv[4] előírásai alkalmazandók.

Meg kell említenünk, hogy az Európai Bizottság 1999-ben konzultációt kezdeményezett a munkavállalók személyes adatainak EU-szintű védelmének szabályozásáról. Az előterjesztett javaslatok nagyrészt az ILO kódexén alapultak.[5] A szociális partnerek (munkavállalói és munkáltatói szervezetek) reakciói szintén az ILOC-ra hivatkoztak. Az EUROCADRES[6] hangsúlyozta, hogy a közösségi jogi szabályozás nem tükrözheti kizárólag a munkavállalók érdekeit, hanem a munkáltatók, a munkavállalók és a munkavállalói képviseletek együttműködésén kell alapulniuk.[7] Az UEAPME[8] azt az álláspontot képviselte, hogy az ILOC alapján kidolgozott nem kötelező magatartási kódexek alkalmazása megfelelő megoldás lenne.[9]

[3] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
[4] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)
[5] European Commission: Second stage consultation, p. 6.
[6] Council of European Professional and Managerial Staff, www.eurocadres.org
[7] European Commission: Second stage consultation, p. 20.
[8] European Association of Craft, Small and Medium-sized Enterprises, www.ueapme.com
[9] European Commission: Second stage consultation, p. 3.

1.2.2. Nemzeti jogalkotás

A munkahelyi adatvédelem olyan komplex terület, amelyre vonatkozóan számos jogszabály tartalmaz előírásokat. A magyar jogszabályi háttér éppen változóban van, több releváns törvény módosult már vagy módosul a közeljövőben; ezek várhatóan 2012. január 1-én léptek hatálya. E módosítások elemzésére a kutatás következő fázisaiban kerül sor.

A munkahelyi adatvédelemmel kapcsolatban a hatályos Alkotmány és az új Alaptörvény meghatároz néhány alapvető jogot, amelyek megalapozzák a magánélet védelmét. Az adatvédelem első alapvető kódexe a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi CXII. törvény[10] volt. Az Országgyűlés 2011. június 11-én új adatvédelmi törvényt[11] fogadott el, ami néhány területen lényeges változásokat hozott. Szintén releváns jogforrás a Munka Törvénykönyve;[12] 2012. július 1-én új Munka Törvénykönyve lép hatályba.[13]

A közszektorban az alkalmazottak személyes adatainak védelmét további rendelkezések is érintik, de ezek egyike sem tartalmaz a technikai megfigyelésre vonatkozó előírást; e jogszabályok a kutatásnak nem tárgyai.

A magánszféra védelmének más vonatkozásait, mint a képmás a hangfelvétel védelme, illetve a levéltitok védelme, a polgári és a büntető törvénykönyvek szabályozzák.

1.2.3. Önszabályozás[14]

A tudományos publikációk számos esetben felvetik azt a lehetőséget, hogy a munkahelyi adatvédelem kérdését az érintettek az önszabályozás keretében oldják meg, például kollektív szerződések, magatartási kódexek vagy egyéb belső szabályozás útján. Eddigi kutatásaink azt mutatják, hogy ez inkább elméleti lehetőség, mintsem napi gyakorlat.

A munkáltatónak és a szakszervezeteknek lehetőségük van arra, hogy a munkáltató ellenőrzési joga gyakorlásának módját és feltételeit, valamint ennek során a személyes adatok kezelésének feltételeit kollektív szerződésben, mégpedig annak normatív részében szabályozzák. Ez a jogosítvány az Mt. 30.§ a) pontjából következik. Kollektív szerződés szabályozhatja a munkavállalók személyes adatainak védelmével és adatvédelmével összefüggő jogokat és kötelezettségeket, így rögzítheti azt is, hogy milyen módon gyakorolhatja a munkáltató a felügyeleti, ellenőrzési jogát a technikai eszközök használata során. A kollektív szerződéses szabályozás előnye, hogy lehetőséget nyújt arra, hogy a konkrét munkahely sajátosságainak megfelelően pontosítsák az Mt. és az Atv. szabályait.[15]

A kollektív szerződéses adatvédelmi szabályozásnak azonban fontos korlátját jelenti, hogy egyrészt nem lehet ellentétes az Mt., az Atv. és a Ptk. rendelkezéseivel, másrészt pedig az

[10] A továbbiakban: Avtv.
[11] 2011. évi CXII. törvény az információs önrendelkezésről és az információszabadságról, a továbbiakban új adatvédelmi törvény vagy új Avtv.
[12] 1992. évi XXII. törvény a Munka Törvénykönyvéről (Mt.)
[13] 2012. évi I. törvény a munka törvénykönyvéről (Új Mt.)
[14] E fejezet elkészítése Kovács Erika kutatásban való közreműködése segítségével készült.
[15] Arany Tóth, 2008a, pp. 307-308.

Mt.-ben rögzített szabályoktól csak annyiban térhet el, amennyiben a munkavállalóra kedvezőbb feltételt állapít meg.[16] Az Mt. azonban nem tartalmaz sem a technikai eszközök munkavállaló általi használatának ellenőrzésére vonatkozó szabályozást - kivéve a távmunkát végzőket - sem pedig a munkáltatói ellenőrzés módjára vonatkozó általános szabályt, így nehezen értelmezhető a munkavállalóra kedvezőbb feltétel kitétel.

A kutatás keretében mintegy 30 kollektív szerződést vizsgáltunk különböző iparágakban, illetve különböző méretű vállalkozásoknál. A kollektív szerződések egyáltalán nem tartalmaznak olyan jellegű szabályt, ami a munkavállaló e-mail-, GPS-, internet-, és telefonhasználatának szabályozására, annak ellenőrzésére vagy kamerás megfigyelésére vonatkozik. Ezek a szerződések semmilyen modern technológiai eszköz használatára és annak ellenőrzésére nem tartalmaznak szabályokat.

A kollektív szerződések viszonylag gyakran rögzítik, hogy a munkavállaló általi rendkívüli felmondás oka lehet a munkáltató által a munkavállaló személyiségi jogainak megsértése:

1) A Mol Nyrt. kollektív szerződése a munkavállaló általi rendkívüli felmondás okai között felsorolja azt az esetet, amikor a munkáltató megsérti a munkavállaló személyiségi jogait (22.2. pont). Ez a kitétel nyilvánvalóan vonatkozhat arra az esetre, amikor a munkáltató a munkavállaló engedélye vagy akár tudomása nélkül betekint az e-mailes levelezőrendszerébe, internethasználatába vagy kamerával megfigyeli.
2) A Dunaferr társaságcsoport kollektív szerződése a munkavállaló általi rendkívüli felmondás okaként megnevezi azt az esetet, amikor a munkáltató a munkavállalót emberi méltóságában megalázza (3.8.1. pont).
3) Az Agrow GP kollektív szerződése is rögzíti, hogy a munkavállaló rendkívüli felmondással megszüntetheti a munkaviszonyát, ha a munkáltató emberi méltóságában nyilvánosan megalázza (37.3. c) pont).
4) A Magyar Posta kollektív szerződése azt rögzíti, hogy a munkavállaló rendkívüli felmondással megszüntetheti a munkaviszonyát, ha a munkáltatói jogkört gyakorló a személyiségi jogait, illetve emberi méltóságát megsérti (13. § (3) b) pont).
5) Az MTI Zrt. kollektív szerződése is kimondja a munkavállaló rendkívüli felmondási jogát, amennyiben a munkáltató a munkavállalót emberi méltóságában megalázza, zaklatja (IV. fejezet, 1. b) pont).

A kollektív szerződések utolsó, országos, átfogó elemzése 2008-ban készült a Szociális és Munkaügyi Minisztérium megrendelésére.[17] Ennek során 20 ágazatra kiterjedően összesen 304 kollektív szerződést vizsgáltak. Ez a tanulmány részletesen elemezte a kollektív szerződések tartalmi elemeit ágazatonként és összesítve is. A tanulmány semmilyen utalást nem tesz arra vonatkozóan, hogy a kollektív szerződések tartalmaznának olyan rendelkezéseket, amelyekre kutatásunk irányult. Ez a tény is alátámasztja, hogy a kutatásunk témáját nem tárgyalják a kollektív szerződések.

[16] Mt. 13.§ (3)
[17] Fodor/Nacsa/Neumann, 2008

Lehetséges és elképzelhető, hogy néhány vállalat belső egyoldalú munkáltatói utasításban rögzíti a munkavállalók által használt technikai eszközökkel kapcsolatos szabályokat, ami esetleg, akár áttételesen tartalmazhat adatvédelmi rendelkezéseket. Ezt a gyakorlatot egy cég jelezte felénk. Ezek a belső szabályzatok tipikusan kizárólag belső használatra készülnek és nem hozzáférhetőek. A belső szabályzatok egyoldalú, a munkáltató részéről kiadott normák, amelyek alakításába a munkavállalóknak nincs befolyásuk és ezért ezek csak a joggyakorlás módját rögzíthetik, annak jogszabályban rögzített szabályait azonban nem korlátozhatják.

1.3. A magánszféra védelmének magyarországi keretei[18]

1.3.1. Alkotmányos háttér

Az Alaptörvény – követve a jogirodalomban kialakult többségi álláspontot[19] – közös bekezdésben említi az információs alapjogokat: a személyes adatok védelmét és a közérdekű adatok nyilvánosságát. A korábbi szerkezeti megoldás előnye ugyanakkor az volt, hogy rámutatott az információs alapjogok kapcsolódásaira egyfelől a kommunikációs jogok, másfelől az emberi méltóság irányában. Az információs alapjogok összetartozásának hangsúlyozása természetesen e kapcsolódásokat nem írja fölül.

Az Alaptörvény nevesíti, hogy e két alapvető jog érvényesülését sarkalatos törvénnyel létrehozott független hatóság ellenőrzi.

Megjegyezzük, hogy az adatvédelemre és az információszabadságra vonatkozó szabályozás eddig teljes mértékben 2/3-os szabályozási tárgykör volt.[20] Az új Alaptörvény alapján azonban – a jogszabály indokolásának hallgatása mellett, és alkotmányjogi érvekkel nehezen indokolhatóan – már kizárólag a hatóságra vonatkozó szabályozás minősül olyan tárgykörnek, amely 2/3-os parlamenti döntést igényel, az adatvédelemre és információszabadságra vonatkozó tartalmi szabályozás azonban nem.

Az Alkotmánybíróság – részletesen a személyi szám használatának alkotmányellenességéről szóló, sokszor félreértett határozatában kifejtve – a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként, hanem annak aktív oldalát is figyelembe véve információs önrendelkezési jogként értelmezi. „Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás

[18] E fejezet során a kiemelt források mellett támaszkodtunk a Polyák/Szőke, 2011 és a Szőke 2010 tanulmányok megállapításaira is.
[19] Majtényi, 2003, pp. 577-635., Balogh/Földes/Jóri/Székely 2004, pp. 47-66., Drinóczi, 2004.
[20] Alk. 59. § (2), 61. § (3), 2010. július 7-től 61. § (5)

módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek."[21]

1.3.2. Általános és ágazati adatvédelmi szabályozás

A személyes adatok védelmének törvényi szabályozására 1992-ben került sor. A magyar jogalkotó az információs önrendelkezési jogot és az információszabadságot ugyanabban a törvényben, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló, többször módosított 1992. évi LXIII. törvényben szabályozta.

2011. július 11-én az Országgyűlés elfogadta az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt. A jogszabály 2012. január 1-től felváltja és hatályon kívül helyezi az adatvédelem és információszabadság hatályos szabályozását: a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt és az elektronikus információszabadságról szóló 2005. évi XC. törvényt. Az új adatvédelmi törvény egyike azoknak a sarkalatos törvényeknek, amelyek az új Alaptörvény elfogadása kapcsán készültek, készülnek 2011 év folyamán.

Az új adatvédelmi törvény – bár nagymértékben támaszkodik a korábbi szabályozásra, és számtalan rendelkezést szó szerint átvesz a hatályos törvényekből – számos ponton módosítja is a korábbi szabályozást, és teljesen átalakítja az adatvédelem felügyeleti rendszerét.

A tanulmány nagyrészt az új szabályozás elemzését tartalmazza, egyúttal rámutatva a jelentősebb változásokra.

Az adatvédelem szabályozása természetesen nem oldható meg egyetlen törvényben. Az állami, gazdasági és egyéb szervezetek számtalan tevékenységükhöz kapcsolódóan, számtalan különböző célból kezelik az egyének személyes adatait. Az Avtv. a minden adatkezelés során figyelembe veendő általános követelményeket és garanciákat határozza meg, amiket azonban az adott adatkezelés sajátosságaira koncentráló, az általános szabályokat konkretizáló ágazati adatvédelmi jogszabályok egészítenek ki.

A munkahelyi adatvédelem területén a legnagyobb nehézséget ugyanakkor éppen a hiányos, sőt hiányzó ágazati szabályozás jelenti, vagy legalábbis jelentette. A munkaviszonyt szabályozó, 2012. június 30-ig hatályos Munka törvénykönyve egyáltalán nem tartalmazott adatvédelmi rendelkezést. A munkáltatói adatkezelés feltételeit teljes egészében a joggyakorlat határozta meg, ami komoly jogbizonytalansághoz vezetett.

2012. július 1-től új munkajogi kódex szabályozza a munkaviszonnyal összefüggő kérdéseket. Az új kódex néhány általános rendelkezést tartalma a munkáltatók ellenőrzésével és megfigyelésével kapcsolatban, amelyeket a tanulmány későbbi részeiben mutatunk be.

Az adatvédelmi szabályozás mellett a magánszféra védelmének más eszközei is elérhetők a magyar jogrendszerben. A Polgári Törvénykönyv a jóhírnévhez, a képmáshoz és a hangfelvételhez, illetve a magán- és levéltitokhoz való jog mellett nevesítve tartalmazza a személyes adatok védelméhez való jogot.

[21] 15/1991. (IV. 13.) ABH

Az adatkezelési előírások megsértése a legsúlyosabb esetekben büntetőjogi következményt is maga után vonhat; erről a tanulmány utolsó fejezetében lesz szó.

1.3.3. A magyar adatvédelmi szabályozás főbb elemei

1.3.3.1. A személyes adat fogalma

Az új Avtv. egyik jelentős változása a személyes adat fogalmának módosítása. A hatályos Avtv. szerint személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

Az új Avtv. külön határozza meg az érintett fogalmát, amely a 3. § 1. pontja szerint bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy. A személyes adat az új törvény alapján az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Kizárólag a fenti fogalmak összevetése alapján a személyes adat fogalma a hatályos fogalommal azonos, az új törvény egy másik szakasza – szerkezetileg erősen vitatható megoldásként – az adatvédelem alapelvei között azonban rögzíti, hogy a „személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.”[22] Ez egyértelmű elmozdulás a személyes adatok abszolút értelmezésétől a relatív értelmezés felé.

A személyes adat abszolút és relatív értelmezésének középpontjában az adat és az érintett közötti kapcsolat helyreállíthatóságának, azaz az érintett közvetett azonosíthatóságának kérdése áll. A (szélsőségesen) abszolút értelmezés szerint személyes adatnak minősül egy adat, ha az adat és a személy közötti kapcsolat elvileg megteremthető. Amennyiben tehát az érintett akár több különböző adatkezelőnél lévő adatok segítségével, több lépésben, különböző technikai eljárásokkal,[23] de végül is azonosítható, akkor – függetlenül attól, hogy az adott adatkezelőnek van-e tényleges vagy jogszerű lehetősége erre – az adatot személyes adatnak kell tekinteni. Ez az értelmezés a személyes adat fogalmát igen tágra szabja.

A relatív értelmezés szerint egy adat személyes adat jellegét az adatkezelő szempontjából kell vizsgálni: amennyiben az adatkezelő ténylegesen nem képes az általa kezelt adatokat az

[22] Új Avtv.4. § (3)
[23] Például titkosított adatok dekódolásával.

érintetthez kötni, úgy az adat e vonatkozásban (ezen adatkezelőnél) nem minősül személyes adatnak.[24]

A hazai adatvédelmi biztosi gyakorlat – kisebb kilengésekkel – ezidáig a személyes adat fogalmának abszolút értelmezés mellett foglalt állást: „minden olyan adat személyes adat, amely természetes személlyel kapcsolatba hozható […] tekintet nélkül arra, hogy a kapcsolat csak több lépésben építhető fel, illetve arra, hogy a kapcsolat megteremtésére valamely adatkezelő önmagában nem képes".[25] A kódolt „adatok annál az adatkezelőnél is személyes adatnak minősülnek, amelynek informatikai rendszere nem alkalmas azok értelmezésére."[26] Az uralkodó abszolút értelmezést azonban – néhol ellentmondást is tartalmazó állásfoglalásokkal – a rendszámok személyes adat jellegének elemzése kapcsán az adatvédelmi biztos többször is megtöri.[27]

Az Avtv. új szövegezése ugyanakkor egyértelmű elmozdulást jelent a személyes adatok abszolút értelmezése felől a (akár szélsőségesen) relatív értelmezés felé. A törvényszövegben található, az „adatkezelő rendelkezik azokkal a technikai feltételekkel" kitétel arra utal ugyanis, hogy amennyiben az adatkezelő nem képes az adat és az érintett kapcsolatát helyreállítani, úgy nem személyes adatot kezel. Ugyanakkor az érintett fogalmának, – és ezen keresztül a személyes adat fogalmának is – továbbra is részeleme a közvetett azonosítás lehetősége. Amint azt korábban említettük, a szélsőségesen abszolút és relatív értelmezés között számtalan árnyalt megközelítés lehetséges, és a törvényszöveg is teret enged a különböző jogértelmezések számára, azaz a joggyakorlat – elsősorban az új hatóság – feladata lesz a személyes adat és az azonosíthatóság szempontjait részletesen kidolgozni, figyelembe véve az adatvédelmi irányelv rendelkezéseit is.

1.3.3.2. Adatkezelő, adatfeldolgozó

Nem hozott változást az új Avtv. az adatkezelő/adatkezelés, illetve az adatfeldolgozó/adatfeldolgozás fogalmaiban. Az adatkezelés az adatokon végzett bármely művelet vagy a műveletek összessége, függetlenül az alkalmazott eljárástól.[28] Adatkezelés többek között – a törvény példálózó felsorolásában – az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Az a természetes személy vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza, és e döntéseket – maga vagy egy adatfeldolgozó megbízásával – végrehajtja, az adatkezelő.[29]

Az adatkezelési műveletekhez kapcsolódó technikai feladatok – az alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől független – elvégzése az adatvédelmi törvény

[24] Majtényi, 2006. pp. 110-113., Jóri, 2005, pp. 101-104.
[25] Jóri, 2005, p. 163.
[26] Jóri, 2005, p. 111.
[27] Jóri, 2005, p. 110., Majtényi, 2006, p. 110.
[28] Új Avtv. 3. § 10.
[29] Új Avtv. 3. § 9.

szerint adatfeldolgozásnak minősül.[30] Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából személyes adatok feldolgozását végzi, az adatfeldolgozó.[31] Az adatkezelő és az adatfeldolgozó közötti megbízási jogviszonyból következően az adatfeldolgozó az adatkezelő utasításainak megfelelően végzi a tevékenységét, ő maga az adatkezelést érintő érdemi döntést nem hozhat, további adatkezelőt nem vehet igénybe.[32] Felelőssége a saját tevékenységi körén belül a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért áll fenn. Az általa az érintettnek okozott kárért az érintettel szemben az adatkezelő felel.

1.3.3.3. Az adatkezelés jogalapja

1.3.3.3.1. Önkéntes és kötelező adatkezelés

A korábbi Avtv. alapján az adatkezelés jogalapja a munkaviszony területén csakúgy, mint máshol, kizárólag az érintett hozzájárulása vagy a törvény felhatalmazása lehetett. Ezen egyszerűnek látszó rendszer gyakorlati megvalósulását nagymértékben nehezítette, hogy az Mt., illetve a munkaviszonyt szabályozó más törvény nem rendelkezett adatkezelési felhatalmazásról. E szabályozási környezetből – elsőre legalábbis – az következne, hogy az adatkezelés kizárólag az érintett hozzájárulásán alapulhat. Ez a gyakorlatban lényegében kivitelezhetetlen. Az adatkezelés jogalapja a vizsgált adatkezelések mindegyikére irányadó, a későbbi fejezetekben ezért az esetleges sajátosságok bemutatása mellett csak utalunk az itt elmondottakra.

Az adatvédelmi törvény alapján a hozzájárulás – amelynek meghatározása az új törvényben nem változik – az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Az érintett kérelmére indult eljárásban a szükséges adatainak kezeléséhez való hozzájárulását vélelmezni kell. Erre a tényre az érintett figyelmét fel kell hívni. Az érintett a hozzájárulását az adatkezelővel írásban kötött szerződés keretében is megadhatja a szerződésben foglaltak teljesítése céljából. Ebben az esetben a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbítását, adatfeldolgozó igénybevételét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.[33]

Az egyik legfontosabb általános probléma a hozzájárulás önkéntességének kérdése. A munkavállaló alapvetően egzisztenciálisan függő helyzete, a munkáltató információs és gazdasági hatalmi túlsúlya sok esetben megkérdőjelezi a hozzájárulás önkéntességét. A munkaerő felvételi eljárás során az önkéntesség gyakrabban valós, bár a munkaerő-piaci

[30] Új Avtv. 3. § 17.
[31] Új Avtv. 2. § 18.
[32] Új Avtv. 10. §
[33] Avtv. 3. § (6), (7)

túlkínálat miatt egyfajta kiszolgáltatottság e folyamat során is jellemző lehet.[34] Ugyanakkor – és a munkavállalók ellenőrzése során ez különös jelentőséggel bír, egy fordított kiszolgáltatottság is egyre inkább jellemző: a modern technikai eszközöknek köszönhetően nincsenek biztonságban a munkáltató különböző adatai, a munkavállalók egyes információk illetéktelen személyes számára történő átadásával igen komoly károkat tudnak okozni. „Az informatikai korban a munkáltató kiszolgáltatottsága sem elhanyagolható új elemekkel bővül. Az a munkáltatói tapasztalat is valós, amely szerint »az ellenség belülről támad«, ez a félelem a modern informatikai eszközök általános birtoklása körülményei között indokolt is."[35]

A munkajog területén el kell határolni a munkaviszonyt megelőző, és a munkaviszony alatt történő adatkezelés jogalapjára vonatkozó kérdéseket.

A munkaviszonyt megelőző adatkezelés során az érintett önkéntessége tehát a szakirodalom által általában nem vitatott. Az adatkezelés jogalapja ez esetben az érintett hozzájárulása, amely kifejeződhet írásbeli, szóbeli vagy ráutaló magatartásban. Az Avtv. uralkodó – de korántsem egyértelmű – biztosi értelmezésében az érintett kérelmére indult eljárásban vélelmezett adatkezelési hozzájárulás kapcsán az eljárás kifejezést tágan kell értelmezni, az alatt nem csak jogilag formalizált eljárást, de az érintett által kezdeményezett egyéb ügyleteket is érteni kell.[36] Így egy álláspályázatra való jelentkezés véleményünk szerint ilyen ügyletnek minősül.

Az új Mt. a hozzájárulás kérdésével kapcsolatban tartalmaz néhány formális garanciát. A törvény szerint a munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyhez fűződő jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.[37] Az új Mt. azt a további fontos garanciát is tartalmazza, hogy a munkavállaló személyhez fűződő jogáról rendelkező jognyilatkozatot, így értelmezésünk szerint adatkezelési hozzájárulást is, érvényesen csak írásban tehet. A személyhez fűződő jog, többek között a személyes adatok védelméhez való jog korlátozásának módjáról, feltételeiről és várható tartamáról a munkavállalót előzetesen tájékoztatni kell.

1.3.3.3.2. Adatkezelés érdekmérlegelés alapján

A munkaviszony fennállása alatt azonban az adatkezelés jogalapja véleményünk szerint alapvetően nem a hozzájárulás. A hozzájárulás ugyan a fent említett esetekben megtörténhet a szerződés aláírásával, amennyiben a szerződés tartalmaz minden szükséges információt és a hozzájárulás tényét. Erre a gyakorlatban ritkán kerül sor, ráadásul a munkaviszony során több olyan adatkezelési művelet és cél is felmerülhet, amelyet a szerződés megkötésekor a felek még nem láttak előre. Természetesen amennyiben a fenti feltételek teljesülnek, a megfelelő tartalmú munkaszerződés értelmezhető adatkezelési hozzájárulásként.

[34] Arany Tóth, 2004b, pp. 15-17., Majtényi, 2006, p. 332., Hartai, 2003, p. 46.
[35] Majtényi, 2006, p. 333.
[36] Jóri, 2005, pp. 187-188.
[37] Új Mt. 10. § (1)

Emellett is lehetséges valamely jogszerű célból a munkavállaló hozzájárulásával személyes adatokat kezelni, az önkéntességet azonban megkérdőjelezhető, így annak meglétét egy jogvitában nagyon körültekintően kell vizsgálni.

Az új Avtv. talán legjelentősebb újdonsága az adatkezelési jogalapok bővítése. A korábbi adatvédelmi törvény kizárólag két – az új szabályozási környezetben is rendelkezésre álló – esetben tette lehetővé a személyes adatok kezelését: ha ehhez az érintett hozzájárult, vagy ha ezt törvény, illetve törvény felhatalmazása alapján, az abban meghatározott körben helyi önkormányzat rendelete elrendelte. JÓRI ANDRÁS szerint ez „az Avtv.-vel kapcsolatos alkalmazási nehézségek legtöbbjének – közvetlen vagy közvetett módon – okozója”.[38] Az információs önrendelkezési jog ilyen következetes érvényesítése Európában is egyedülálló, ugyanakkor e szabályozás a jogalkalmazói gyakorlatban csak meglehetősen rugalmas jogértelmezéssel volt hozzáilleszthető a felmerülő problémákhoz, és az európai közösségi joggal való összhangja is vitatható volt. Az Európai Bíróság ugyan nem zárta ki, hogy a tagállamok az adatkezelés feltételeit az irányelvben foglaltaknál szigorúbban határozzák meg,[39] az azonban így is kétséges, hogy a hazai adatvédelmi szabályozás kiállná-e a közösségi jog próbáját.[40]

Az adatvédelmi irányelv 7. cikkének f) pontja szerint személyes adatok kezelhetők többek között abban az esetben is, ha az adatkezelés az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendű az érintettnek a magánélet tiszteletben tartásához való joga. Az érdekmérlegelés jelentősen kitágítja a jogszerű adatkezelések körét, és egyúttal szükségszerűen bizonytalanabbá is teszi azok határait. A hozzájárulás és a törvényi felhatalmazás az érintett számára elvileg minden esetben előzetesen ellenőrizhetővé és átláthatóvá teszi az adatkezelés feltételeit. Ehhez képest az érdekmérlegelés akár az érintett tudta nélkül is alapot adhat a személyes adatok kezeléséhez, és minden esetben csak utólag, alapvetően szubjektív szempontok alapján dönthető el, hogy az adatkezelő valóban helyesen mérlegelte-e a szemben álló érdekeket, azaz jogszerű volt-e az adatkezelés. A felmerülő viták eldöntése a jogalkalmazóra is nagyobb felelősséget ró.

Mindezzel együtt az érdekmérlegelés, mint adatkezelési jogalap megjelenése indokolt mértékű rugalmasságot hoz a szabályozásba, és világos helyzetet teremt számos, jelenleg jogsértő, de jogkövetkezmény nélkül maradó adatkezelés számára. Ilyen jogsértések állhattak elő többek között a munkáltató adatkezelési gyakorlatában, amikor pontosan meghatározott jogalap nélkül ellenőrizte a munkavállalók tevékenységét,[41] a munkáltatók, oktatási intézmények által az intézményben dolgozók, tanulók részére nyújtott távközlési szolgáltatásokhoz kapcsolódó adatkezeléseknél, az oknyomozó újságíró tevékenységében, amikor valamely ügy felderítése kifejezetten az érintett akarata ellenére történik, vagy éppen a szerződés megszűnését követően az elévülési időn belül a szerződésből eredő károk

[38] Jóri, 2005, p. 163.
[39] Jóri, 2005; Majtényi, 2006, pp. 89-90.
[40] Jóri szerint az Avtv. eltérései nem okoznak a közösségi joggal való összeütközést (ld. Jóri, 2005, p. 32.). Álláspontunk szerint ez egyáltalán nem egyértelmű.
[41] Majtényi, 2006, p. 336., Szőke, 2009

érvényesítéséhez kapcsolódóan. Sőt számos, formálisan jogsértő adatkezelés jogi helyzetét tisztázhatja a rendelkezés olyan kötelező adatkezelések esetében, amelyek törvényi feltételeit – a korábbi és az új szabályozás egyaránt szigorú és részletese előírása ellenére[42] – a jogalkotó nem határozta meg kellő pontossággal.[43]

Az adatvédelmi törvény sajátossága ugyanakkor, hogy az érdekmérlegelést nem az adatvédelmi irányelv szóhasználatában, nem általános jogalapként határozza meg. A törvény szerint egyrészt akkor van helye érdekmérlegelésen alapuló adatkezelésnek, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, másrészt akkor, ha a személyes adat felvételére eredetileg az érintett hozzájárulásával került sor, és az adatkezelés az eredetitől eltérő célból, további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően folytatódik.[44] Ezekben az esetekben az adatkezelés jogszerű, ha az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll. Jogszerű az adatkezelés akkor is, ha az az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges. Utóbbi esetben a jogalkotó gyakorlatilag vélelmezi, hogy az adatkezelő érdeke előbbre való az érintett érdekeinél.

A magyar szabályozás tehát továbbra sem általános jogalapként határozza meg az érdekmérlegelést, hanem két esetben, a hozzájárulás beszerzésének lehetetlensége, illetve a már az adatkezelő birtokában lévő adatoknak az eredeti hozzájárulást meghaladó kezelése esetén. Annak értelmezésével, hogy milyen esetekben lehetetlen, illetve túlzottan költséges a hozzájárulás beszerzése – megvalósul-e ez akkor is, ha az érintett, ellenérdekeltsége miatt, nem ad hozzájárulást, vagy csak ennél szűkebb, objektív körülmények elégítik ki a törvényi feltételeket –, a joggyakorlat jelentős mértékben befolyásolni fogja e jogalap jelentőségét. Az adatvédelmi irányelv alapján ehhez képest akkor is jogszerű az adatkezelés, ha az adatkezelő meg sem próbál hozzájárulást szerezni.

A törvényi feltétel megfogalmazása során a jogalkotó feltehetően hangsúlyozni akarta a hozzájáruláson alapuló adatkezelés elsőbbségét, amit azonban éppen a másik érdekmérlegelési jogalap von kétségbe. Az eredetitől eltérő célból történő adatkezelés, bár az irányelvi rendelkezés kétségtelenül magában foglalja e lehetőséget – sőt akár a hozzájárulás beszerzésének lehetetlensége is értelmezhető úgy, hogy az magában foglalja ezt az esetet is – mégis jelentős kockázat az információs önrendelkezési jog szempontjából. Az érintett ebben az esetben ugyanis éppen arra számíthat, hogy az adatkezelő a birtokában lévő adatok kezelését nem folytatja. A célhoz kötöttséget, mint az Alkotmánybíróság által az információs önrendelkezési jog legfontosabb garanciájaként meghatározott adatkezelési korlátot, e rendelkezés kiüresíti, a célhoz kötöttség megsértésének bizonyítása legalábbis szinte lehetetlenné válik. Másrészről viszont a jogalkalmazói gyakorlat olyan értelmezést is kialakíthat, amely szerint az érdekmérlegelés egyik legfontosabb szempontja az adatkezelés célja, így akár gyakorlati szempontból fel is értékelődhet a célhoz kötöttség elve.

[42] Avtv. 3. § (3); új Avtv. 5. § (3)
[43] Jóri, 2005, pp. 164-165.
[44] Új Avtv. 6. § (1) és (5)

Új tartalmat nyer viszont az érintett tiltakozási joga, ami ilyen adatkezelések esetén is lehetőséget biztosít a kifogásolt adatkezelés megszűntetésének kezdeményezésére. Korábban ez a jogintézmény az érintett adattörlési joga mellett önálló jelentőséggel nem rendelkezett, most azonban olyan esetekben is lehető teszi az adatkezelés megszűntetését, amikor az érintett a törlési jogával nem élhet. Ugyanakkor nem egyértelmű az érintett tájékoztatásának szabályozása. Az adatkezelőt terhelő proaktív tájékoztatási kötelezettség nélkül az érintett tudomást sem szerez az adatkezelés tényéről. A törvény szerint az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.[45] Az érdekmérlegelésen alapuló adatkezelés szigorúan értelmezve egyik esetnek sem felel meg, ebből következően a tájékoztatási kötelezettség sem terjed ki rá. Mivel azonban formálisan természetesen maga a törvény teszi lehetővé az adatkezelő számára, hogy a megfelelő feltételek teljesülése esetén kezelje a személyes adatokat, ezért a fenti rendelkezés értelmezhető úgy is, hogy az adatkezelő az érdekmérlegelésen alapuló adatkezelés megkezdése előtt is köteles tájékoztatni az érintettet. Az információs önrendelkezési jog érvényesülését kizárólag az utóbbi értelmezés garantálja.

1.3.3.3.3. A munkaviszonnyal összefüggő adatkezelés jogalapja

A munkaviszonnyal kapcsolatos adatvédelmi kérdésekben ARANY TÓTH MARIANN már a korábbi jogszabályi környezetben is több alkalommal hivatkozott az érdekek mérlegelésének lehetőségére,[46] ez azonban jogalapként a szabályozás alapján nem volt elfogadható. A gyakorlatban az adatkezelési célok és az. Mt. egyes rendelkezései, mint adatkezelésre adott felhatalmazás során azonban egyfajta érdekmérlegelésre mégiscsak sor kerülhetett.

Az új szabályozás alapján a munkáltató minden olyan személyes adatot felhasználhat tetszőleges célra, amely az érintett hozzájárulása alapján került a birtokába. Ennél szélesebb adatkörre vonatkozóan azonban továbbra is önálló adatkezelési jogalapot kell felmutatni. Egy munkaszerződésben megadott felhatalmazás önmagában nem alapozza meg a hagyományos vagy elektronikus levelek tartalmának vagy a számítógép-használati adatoknak a megismerését, ha a hozzájárulás ezekre az adatokra nem terjed ki. Így összességében a munkáltatói ellenőrzési jogkör gyakorlásának továbbra is a hozzájárulás marad a jogalapja, és a rendelkezés várhatóan nem jelent érdemi előrelépést a munkajogi adatvédelem gyakorlatában. Ez egyúttal arra is rámutat, hogy a magyar szabályozás az adatfelvétel hozzájáruláshoz kötésével az irányelvhez képest jelentősen szűkíti a mérlegelés jogalapként való alkalmazását.

Máshonnan közelíti meg – látszólag a jogalap kérdésétől függetlenül – a kérdést MAJTÉNYI LÁSZLÓ. Véleménye szerint a „munkahelyen is megilleti az alkalmazottat a privacy védelme, ennek azonban ésszerű feltétele (noha ezt a szabályokból elég nehéz kiolvasni), hogy a védendő tevékenység magánéleti legyen, de pedig a céghez, annak tevékenységéhez köthető. A munkáltató nevében, illetve számára folytatott tevékenység felett, ha az adatvédelmet a józan ész fényében értelmezzük, a munkáltató rendelkezik”, „a munkahelyi privacyvédelem a munkavállaló magánéleti megnyilvánulásaira vonatkozik, nem pedig a közvetlen és

[45] Új Avtv. 20. § (1)
[46] Arany Tóth, 2004b, pp. 18-19.; Arany Tóth, 2008a

nyilvánvaló munkavégzésre. (Abszurdan széles jogértelmezéssel azt is mondhatjuk, hogy a munkás által jól-rosszul elkészített munkadarab is az ő személyes adata.)”[47]

MAJTÉNYI szavai arra engednek következtetni, hogy az adatvédelmi szabályozás hatályát, netán magát a személyes adat fogalmát a munkaviszony kapcsán csak a magánéleti megnyilvánulásokra kell kiterjeszteni – de a szerző maga is elismeri, hogy a szabályokból ez nehezen kiolvasható. Ugyanakkor a magánéleti / munkaviszonnyal kapcsolatos tevékenység elhatárolása a jövőben magától értetődő elhatárolási mércéje lehet az Mt. szektorális adatvédelmi szabályozásának; az új Mt. tartalmaz ilyen irányú rendelkezést.

A magunk részéről az adatvédelmi jog dogmatikai tisztaságát megtartva úgy véljük, hogy a munkáltató adatkezelésének jogalapja sok esetben az Mt. szakaszai lehetnek. Egyetértünk JÓRI ANDRÁS megközelítésével, amely szerint azon törvényi rendelkezések, amelyek nem közvetlenül adatkezelésről, csupán adatkezelést szükségképpen feltételező jogintézményről, hatáskör gyakorlásáról szólnak, szintén értelmezhetők adatkezelési felhatalmazásnak.[48] Így véleményünk szerint az Mt. egyes rendelkezései éppen ilyennek minősülnek, és azok adatkezelési felhatalmazásként való értelmezése teremti meg a jogalapot a személyes adatok kezelésére. E rendelkezések sok esetben meglehetősen általánosak, így ez esetben is – a fent említett megoldásokhoz hasonlóan – „bátor”, életszerűséget előtérbe helyező jogértelmezésre van szükség.

A szakirodalom általánosan hivatkozik a munkáltató felügyeleti/ellenőrzési jogosultságára. Ez tartalmilag „azt a jogot jelenti, hogy a munkáltató a munkajogviszony teljesítése körében ellenőrizze a munkavállaló magatartását, arra vonatkozóan tényeket állapítson meg, illetve a munkavállaló teljesítményét összevesse a jogviszonyban elvárhatóval. A munkavállaló a felügyeleti jog gyakorlását tűrni köteles”. A felügyeletre vonatkozó szabály szükségszerűen feltételezi személyes adatok kezelését, így akár törvényi felhatalmazás is lehet. Az irányítási/felügyeleti jogot ugyanakkor a régi Mt. kötelezettségként nevesíti: a munkáltató köteles a munkavállaló számára a munkavégzéshez szükséges tájékoztatást és irányítást megadni. KISS GYÖRGY szerint a munka feletti felügyelet jogkör a konkretizálási jogtól (az utasítás adás jogától) nem választható el. Az utasításra vonatkozóan az Mt. kimondja: a munkavállaló a munkát a munkáltató utasítása szerint köteles ellátni. Emellett a munkáltató jogosult ellenőrizni az általa rendelkezésre bocsátott eszközök használatát is.

Az Mt. munkajogviszony tartalmára vonatkozó szabályai véleményünk szerint olyan törvényi rendelkezések, amelyek nem közvetlenül adatkezelésről, de adatkezelést szükségképpen feltételező jogintézményről, hatáskör gyakorlásáról szólnak, és így ezek értelmezhetők adatkezelési felhatalmazásként.

Ugyanakkor a munkavállaló ellenőrzése során tekintetbe kell venni az adatkezelés kapcsán a célhoz kötöttség követelményét is, amelyet minden esetben körültekintően kell vizsgálni. Az adatvédelmi biztos számos konkrét esetben a munkavállaló hozzájárulásához kötötte az egyes ellenőrzési cselekményeket.

[47] Majtényi, 2006, p. 336.
[48] Jóri, 2005, pp. 164-165.

Az új Mt. a korábbi helyzethez képest jelentős előrelépést jelent. A törvény 11. §-a szerint a munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartása körében, és kizárólag e körben ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető. A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

A törvény egy általánosabb adatkezelési felhatalmazást is tartalmaz, amikor kimondja, hogy a munkavállaló személyhez fűződő joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyes adatok védelme, mint a Ptk.-ben is nevesített személyhez fűződő jog tehát a munkajogi szabályozás alapján is egyfajta érdekmérlegelés tárgya lehet. A törvény rögzíti, hogy a munkavállaló a személyhez fűződő jogáról általános jelleggel előre nem mondhat le.

1.3.3.4. Az adatkezelés garanciái

A személyes adatok kezelésének legfontosabb garanciája továbbra is az, hogy arra minden esetben pontosan meghatározott, jogszerű cél teljesítése érdekében kerüljön sor. „A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, »készletre«, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes.”[49]

A célhoz kötöttség garanciáját a törvény összetett követelményként fogalmazza meg:

- személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet;[50]
- a célhoz kötöttségnek az adatkezelés minden szakaszában teljesülnie kell, azaz az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelési célnak;[51]
- csak az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas személyes adat kezelésére kerülhet sor;[52]
- az adatkezelés nem haladhatja meg a cél megvalósulásához szükséges mértéket és időtartamot;[53]
- ha az adatkezelés célja megszűnt, akkor a személyes adatot törölni kell;[54]
- a célhoz kötöttség technikai garanciájaként az adattárolás módjának alkalmasnak kell lennie arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.[55]

Az adatvédelmi törvény a kezelt adatok minőségére vonatkozó követelményként határozza meg, hogy azok felvétele és kezelése legyen tisztességes és törvényes.[56] A tisztességes adatkezelés követelménye a törvényesség mércéjénél szigorúbb, pontos tartalma azonban

[49] 15/1991. (IV. 13.) ABH
[50] új Avtv. 4. § (1)
[51] új Avtv. 4. § (1)
[52] új Avtv. 4. § (2)
[53] új Avtv. 4. § (2)
[54] új Avtv. 17. § (2) d)
[55] új Avtv. 4. § (4)
[56] Avtv. 4. § (1)

általános érvénnyel nem határozható meg. Az adatminőség követelményeként a törvény előírja továbbá, hogy a kezelt személyes adatok legyenek pontosak, teljesek és ha szükséges, időszerűek.[57] Ennek teljesülése nélkül az adatkezelés célja nem teljesíthető, és az érintett számára a pontatlan adatok kezelése jelentős érdeksérelmet okozhat.[58]

1.3.3.5. Az érintett jogai az adatkezeléssel kapcsolatban

Az Avtv. személyes adatainak kezelésével kapcsolatban sajátos jogokat biztosít az érintettek részére,[59] amelyek az adatkezelés egész folyamatában biztosítják az információs önrendelkezési jog érvényesítésének lehetőségét. Az érintett jogait kizárólag törvény korlátozhatja, az adatvédelmi törvényben meghatározott közérdekű célokból.[60]

- Az érintettet nem csak az adatfelvételkor kell tájékoztatni az adatkezelés lényeges körülményeiről, hanem azokról az adatkezelés során is *tájékoztatást kérhet*. Az adatkezelő köteles a kérelem benyújtásától számított a lehető legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a kért tájékoztatást. Költségtérítést csak akkor állapíthat meg, ha a tájékoztatást kérő az adott évben azonos területre vonatkozó tájékoztatási kérelmet már benyújtott.[61] Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.
- Az érintett kérheti a valóságnak meg nem felelő személyes adatai *helyesbítését*. Ha a hiányos vagy téves adat jogszerűen nem korrigálható, akkor azt – törvény eltérő rendelkezése hiányában – törölni kell. Az adatkezelő megjelöli az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.
- A kötelező (törvényen alapuló) adatkezelések kivételével az érintett bármikor kérheti személyes adataink *törlését*, és ezzel az adatkezelés megszüntetését. Az adattörlés az adatok felismerhetetlenné tételét jelenti oly módon, hogy a helyreállításuk többé nem lehetséges. A törlésre irányuló kérelemnek nem feltétele, hogy az adatkezelés jogellenes legyen. Az adatvédelmi biztos a sajtó gyakorlatában felmerült kifogásokra reagálva megerősítette, hogy az adatkezelőnek nincs mérlegelési joga a kérés teljesítését illetően.

---

[57] Avtv. 4. § (1)

[58] A törvény az adatminőség elvének részeként írja elő azt, a célhoz kötöttséggel kapcsolatban már tárgyalt követelményt, amely szerint az adatok tárolása módjának alkalmasnak kell lennie arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani [Avtv. 7. § (1) c)].

[59] új Avtv. 14-19. §

[60] Ezek a közérdekű célok az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, illetve az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából – beleértve minden esetben az ellenőrzést és a felügyeletet is –, továbbá az érintett vagy mások jogainak védelme érdekében.

[61] A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

Törlés helyett az adatkezelő zárolja a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.

- Az adatvédelmi törvény az érintett részére biztosítja továbbá a *tiltakozás* jogát. A tiltakozás az érintett olyan nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri. E jogával az érintett különösen akkor élhet, ha – a kötelező adatkezelés kivételével – a személyes adatok kezelése kizárólag az adatkezelő jogának vagy jogos érdekének érvényesítéséhez szükséges, valamint ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik. Az adatkezelő – az adatkezelés egyidejű felfüggesztésével – a tiltakozást köteles a kérelmet legfeljebb 15 nap alatt megvizsgálni, és annak eredményéről a kérelmezőt írásban tájékoztatni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést megszüntetni és az adatokat zárolni.[62] A személyes adat nem törölhető, ha az adatkezelést törvény rendelte el, azonban a tiltakozással érintett adat nem továbbítható más adatkezelő részére.

1.3.3.6. Adatvédelmi biztos, adatvédelmi hatóság

A személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében a korábbi adatvédelmi törvény létrehozta az adatvédelmi biztos intézményét. Az adatvédelmi biztos egyrészt az egyéni jogérvényesítés sajátos fóruma volt, másrészt olyan jogvédelmi intézmény, amely egyéni kezdeményezés nélkül is eljárhatott.

Az új szabályozás kétségkívül legtöbb vitát kiváltó eleme az adatvédelem és információszabadság felügyeleti rendszerének újraszabályozása. A szabályozás lényege, hogy – megtartva több adatvédelmi biztosi jogosítványt – új hatósági jogkörökkel és bírságolási joggal kiegészülve felügyeleti hatóság, a Nemzeti Adatvédelmi és információszabadság Hatóság jött létre, amelynek elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi ki. Az új hatóság 2012. január 1-i felállítása miatt az adatvédelmi biztos intézménye a jelenlegi adatvédelmi biztos mandátumának mintegy félidejénél megszűnt.

Az adatvédelmi biztos jelentős jogfejlesztő szerepet töltött be, amely szerepet elvileg az új hatóság is átvehet. Többek között a munkahelyi adatvédelem területén is jól látható volt, hogy az adatvédelmi biztos ajánlásai a gyakorlatban normaként érvényesültek,[63] azokat az adatkezelők magatartásuk alakításánál figyelembe vették.

Az adatvédelmi hatóság feladatairól és eljárásairól a tanulmány utolsó fejezetében bővebben írunk.

[62] A tiltakozási jog gyakorlása sértheti azok jogát vagy jogos érdekét, akik a személyes adatokhoz az adatkezelőtől adattovábbítás útján jutnak (adatátvevő). Az új Avtv. ezért biztosítja az adatátvevő részére, hogy az adatokhoz való hozzájutás érdekében bírósághoz forduljon.
[63] Sólyom, 2001, pp. 89-90.

1.4. A kutatási terület meghatározása – a munkahelyi adatvédelem alapjai

1.4.1. A köz- és magánszektor eltérő szabályozása

A köz- és a magánszektor adatkezelésére vonatkoznak ugyan eltérő szabályok, a technikai eszközök használatára és ellenőrzésére vonatkozó speciális szabályok hiánya miatt azonban mindkét szektorra ugyanazon elveket és előírásokat kell alkalmazni. Sem a joggyakorlat, sem a tudományos publikációk nem különböztetik meg a két szektort.[64]

1.4.2. A munkáltatónak a munkavállaló ellenőrzéséhez fűződő érdeke

Általánosságban megállapítható, hogy a munkavállalónak legitim érdeke fűződik a munkavállaló tevékenységének ellenőrzéséhez; ezt az érdek számos munkajogi előírásban visszaköszön.

Az Mt. kifejezetten nem rendelkezik az ellenőrzési jogról, de a szakirodalom általánosan hivatkozik a munkáltató felügyeleti/ellenőrzési jogosultságára.[65] Ez tartalmilag „azt a jogot jelenti, hogy a munkáltató a munkajogviszony teljesítése körében ellenőrizze a munkavállaló magatartását, arra vonatkozóan tényeket állapítson meg, illetve a munkavállaló teljesítményét összevesse a jogviszonyban elvárhatóval. A munkavállaló a felügyeleti jog gyakorlását tűrni köteles”.[66] A felügyeletre vonatkozó szabály szükségszerűen feltételezi személyes adatok kezelését, így akár törvényi felhatalmazás is lehet. Az irányítási/felügyeleti jogot ugyanakkor az Mt. kötelezettségként nevesíti: a munkáltató köteles a munkavállaló számára a munkavégzéshez szükséges tájékoztatást és irányítást megadni.[67] KISS GYÖRGY szerint a munka feletti felügyelet jogkör a konkretizálási jogtól (az utasítás adás jogától) nem választható el.[68] Az utasításra vonatkozóan az Mt. kimondja: a munkavállaló a munkát a munkáltató utasítása szerint köteles ellátni.[69] Emellett a munkáltató jogosult ellenőrizni az általa rendelkezésre bocsátott eszközök használatát is.

1.4.3. Az ellenőrzés határai

1.4.3.1. A jogszerű ellenőrzés és a jogszerűtlen megfigyelés közötti határ

Ha kutatásunk alapvető célját szeretnénk összefoglalni, azt mondhatnánk, hogy kísérletet teszünk a munkavállalók jogszerű ellenőrzése és jogszerűtlen megfigyelése közötti határ kijelölésére. A fentiek szerint a munkáltatónak jogos érdeke fűződik a munkavállalók ellenőrzéséhez, ez azonban nem terjed ki a munkavállalók magánéletének folyamatos technikai megfigyelésére. Ahogy erről szó lesz, az egyik fő probléma a különböző technikai eszközök hivatali és magánjellegű használatának, illetve a munkavállalók hivatali és magánjellegű magatartásának elkülönítése.

---

[64] Ez alól egy lényeges kivétel van, amit a levelezés ellenőrzésénél ismertetünk.
[65] Kiss, 2005, p. 180., Bankó/Berke/Kiss, 2004, p. 89., Arany Tóth, 2008a, p. 235.
[66] Bankó/Berke/Kiss, 2004, pp. 89-90.
[67] Mt. 102. § (2) b)
[68] Kiss, 2005, p. 180.
[69] Mt. 104. § (1)

1.4.3.2. Adatvédelmi előírások a Munka Törvénykönyvében 2012. július 1-e előtt

A régi Mt. 3. § (4) bekezdésének, amely szerint a munkáltató a munkavállalóra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet. A 77. § (1) alapján a munkavállalótól csak olyan nyilatkozat megtétele vagy adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely személyiségi jogait nem sérti, és a munkaviszony létesítése szempontjából lényeges tájékoztatást nyújthat.

A Munka Törvénykönyve a távmunka ellenőrzésére vonatkozóan tartalmaz néhány további előírást. A törvény szerint a munkáltató indokolt esetben ellenőrizheti a távmunkát végző munkavállaló munkavégzési kötelezettségének teljesítését. Az ellenőrzés során a munkáltató nem tekinthet be a távmunkát végző munkavállalónak a munkavégzéshez használt információtechnológiai és informatikai eszközön tárolt, a munkaviszonyból származó jogokkal és kötelezettségekkel össze nem függő adataiba. A munkáltató meghatározhatja, hogy a munkavégzéshez általa biztosított információtechnológiai és informatikai, illetve elektronikus eszközt a távmunkát végző munkavállaló mely tevékenységre nem használhatja. Az e tilalom betartásának ellenőrzéséhez szükséges adat a munkaviszonyból származó kötelezettséggel összefüggő adatnak minősül.[70] Ez az előírások az ellenőrzés megfelelő kereteit biztosítják, de kizárólag a távmunkára alkalmazhatók.

Összességében megállapítható, hogy a hatályos munkajogi szabályozás meglehetősen kevés adatvédelmi előírást tartalmaz, aminek következtében a munkajogi jogviszonyokra az adatvédelmi törvény általános rendelkezéseit kell alkalmazni.

1.4.3.3. Adatvédelmi előírások a Munka Törvénykönyvében 2012. július 1-e után

Az új Munka Törvénykönyve a munkahelyi adatvédelem területén érzékelhető változást jelent. Kifejezetten rendelkezik a munkáltató által gyakorolható ellenőrzés feltételeiről.[71] E szerint s munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete – munkaviszonyon kívüli tevékenysége – nem ellenőrizhető. További kötelezettségként előírja a törvény, hogy a munkáltatónak előzetesen tájékoztatnia kell a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

Szintén van adatvédelmi relevanciája a munkavállaló személyhez fűződő jogai tiszteletben tartására irányuló kötelezettségnek.[72] A célhoz kötöttség elvét fogalmazza meg az az előírás, ami szerint a munkavállaló személyhez fűződő joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. Ezzel összhangban megtiltja a törvény a munkavállaló személyhez fűződő

[70] Mt. 192/G. § (3) és (6)
[71] új Mt. 11. §
[72] új Mt. 9-10. §

jogairól való általános jellegű, előzetes lemondást. Szintén a célhoz kötöttség biztosítéka, hogy a munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyhez fűződő jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

Az adatkezelő tájékoztatási kötelezettségeként is értelmezhető az a rendelkezés, ami szerint a személyhez fűződő jog korlátozásának módjáról, feltételeiről és várható tartamáról a munkavállalót előzetesen tájékoztatni kell. Kifejezetten is előírja a törvény, hogy a munkáltató köteles a munkavállalót tájékoztatni személyes adatainak kezeléséről. Az általános adatvédelmi szabályokhoz képest szigorúbb követelmény, hogy a munkavállaló személyhez fűződő jogáról rendelkező jognyilatkozatot érvényesen csak írásban tehet.

Az adattovábbítás korlátozásaként a törvény előírja, hogy a munkáltató a munkavállalóra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet. A munkaviszonyból származó kötelezettségek teljesítése céljából a munkáltató a munkavállaló személyes adatait ugyanakkor adatfeldolgozó számára átadhatja. Erről a munkavállalót előzetesen tájékoztatni kell.

Mindezzel együtt az új Mt. sem hozott létre valódi, az adatkezelési célokat és feltételeket pontosan meghatározó ágazati adatvédelmi szabályozást. Jelentős előrelépés ugyanakkor az adatkezelés jogalapjának a korábbihoz képest egyértelműbb meghatározása, a munkahelyi ellenőrzés lehetőségének törvényi megteremtése. A fennmaradó hiányosságok kitöltésében fontos szerepe lehet az adatvédelmi hatóságnak, és fontos szerepük lesz a belső szabályozásoknak. Különösen a nagyobb munkáltatóknak érdemes a jogbiztonságot növelő magatartási kódexet elfogadniuk.

1.4.4. Kölcsönös függőség

1.4.4.1. A munkavállaló függő helyzete: önkéntes-e a hozzájárulás?

Amint azt fent már kifejtettük, az egyik legfontosabb általános probléma a hozzájárulás önkéntességének kérdése. A munkavállaló alapvetően egzisztenciálisan függő helyzete, a munkáltató információs és gazdasági hatalmi túlsúlya sok esetben megkérdőjelezi a hozzájárulás önkéntességét. A munkaerő felvételi eljárás során az önkéntesség gyakrabban valós, bár a munkaerő-piaci túlkínálat miatt egyfajta kiszolgáltatottság e folyamat során is jellemző lehet.[73]

1.4.4.2. A „függő” munkáltató: megakadályozható-e szigorú ellenőrzés nélkül fontos és értékes információk eltulajdonítása?

Ugyanakkor – és a munkavállalók ellenőrzése során ez különös jelentőséggel bír, egy fordított kiszolgáltatottság is egyre inkább jellemző: a modern technikai eszközöknek köszönhetően nincsenek biztonságban a munkáltató különböző adatai, a munkavállalók egyes információk illetéktelen személyes számára történő átadásával igen komoly károkat tudnak okozni. „Az

[73] Arany Tóth, 2004b, pp. 15-17., Majtényi, 2006, p. 332., Hartai, 2003, p. 46.

informatikai korban a munkáltató kiszolgáltatottsága sem elhanyagolható új elemekkel bővül. Az a munkáltatói tapasztalat is valós, amely szerint »az ellenség belülről támad«, ez a félelem a modern informatikai eszközök általános birtoklása körülményei között indokolt is."[74]

[74] Majtényi, 2006, p. 333.

2. A MUNKAHELYI MEGFIGYELÉS JOGI SZABÁLYOZÁSA

Mielőtt részletesen vizsgáljuk a munkahelyi megfigyelés egyes eszközeire vonatkozó szabályozást és a kapcsolódó adatvédelmi biztosi és bírósági, gyakorlatot, le kell szögeznünk, hogy azok – értelemszerűen – a jelenleg hatályos jogi környezeten alapulnak. Az új munka törvénykönyvének 2012. július 1-i hatálybalépésével több ponton történhet változás, a kódex egyik legfontosabb újdonsága éppen a munkavállalók ellenőrzésének jogalapjához kapcsolódik. E fejezet megállapításaiból egyértelműen látható, hogy az adatvédelmi biztos eddigi gyakorlata a hozzájárulás elvén alapul, vagyis a munkahelyi megfigyelés valamennyi típusa csak a munkavállaló hozzájárulásával folytatható. Kérdéses, hogy e kiindulópont az új jogszabály alapján is tartható-e. Az adatvédelmi biztosi gyakorlat bemutatását ugyanakkor mindenképpen szükségesnek tartjuk, mivel az nagyrészt kialakította a jogszerű megfigyelés feltételeit és korlátait, és ezek az új jogszabály életbe lépését követően – a megfigyelés jogalapjának változása esetén is – alkalmazhatóak maradnak.

2.1. A hagyományos levelezés szabályozása

A hagyományos levelek ellenőrzése adatvédelmi szempontból azért releváns, mert a levél tartalma, illetve megírásának, elküldésének és fogadásának körülményei – a címzett és a feladó neve, címe, az elküldés és a kézbesítés dátuma, a feladás helye, stb. – személyes adatok. A munkahelyi levelezés ráadásul nem is csak az adott munkavállaló személyes adatait érinti, hanem a címzettét, aki a munkáltatóval adott esetben semmilyen jogviszonyban nem áll. Az ellenőrzési jog kialakítása során a legfontosabb probléma a hivatali és a magánjellegű levelek megkülönböztetése: míg az elsőre kiterjed a munkáltatói ellenőrzési jog, utóbbira nem. E két kategória megkülönböztetése a gyakorlatban nem mindig egyértelmű. A kapcsolódó joggyakorlat elsősorban az ebből eredő nehézségekhez kapcsolódik.

2.1.1. Jogalkotás

A levelezés ellenőrzésének sajátos polgári jogi és büntetőjogi korlátai is vannak. A Polgári Törvénykönyv szerint személyhez fűződő jogok sérelmét jelenti a levéltitok megsértése.[75] Ez megvalósul a levél tartalmának jogosulatlan megismerésével. A levéltitok védelme nem korlátozódik a papíron, hagyományos postai úton továbbított küldeményekre, hanem kiterjed az elektronikus úton továbbított küldeményekre is.

A Büntető Törvénykönyv szerint levéltitok megsértésének vétsége miatt büntetendő az, aki másnak közlést tartalmazó zárt küldeményét, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja.[76] A büntetőjogi védelem tehát kiterjed minden „közlést tartalmazó zárt küldeményre”, annak tartalmától függetlenül. A küldemény zártsága a tényállás megvalósulási feltétele. A küldemény felbontásának minősülhet minden olyan cselekmény, amely alkalmas a küldemény tartalmának

[75] Ptk. 81. § (1)
[76] Btk. 178. §

megismerésére. A levéltitok-sértés csak akkor minősül bűncselekménynek, ha kifejezetten a küldemény tartalmának megismerésére irányul. Szintén a levéltitok-sértés tényállásának keretében vonandó felelősségre az, aki távközlési berendezés útján továbbított közleményt kifürkész. Távközlési eszköz minden olyan eszköz, amely elektronikus jeltovábbítást tesz lehetővé. A „kifürkészés" – lehallgatás – minden olyan cselekményt magában foglal, ami a távközlési úton továbbított küldemény jogosulatlan megismerésére irányul. A foglalkozás vagy közmegbízatás felhasználásával elkövetett, valamint a jelentős érdeksérelmet okozó levéltitok-sértés súlyosabban büntetendő. Ez a munkáltató magatartásának megítélésében is irányadó.

A közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet a küldemények felbontásával és érkeztetésével kapcsolatban úgy rendelkezik, hogy a szervhez érkezett küldeményt a címzett, a központi iratkezelést felügyelő vezető által írásban felhatalmazott személy, a szervezeti és működési szabályzatban meghatározott szervezeti egység dolgozója, vagy automatikusan az iratkezelési szabályzatban meghatározott elektronikus rendszer bonthatja fel. Felbontás nélkül dokumentáltan a címzettnek kell továbbítani azokat a küldeményeket

a) amelyek „s. k." felbontásra szólnak,
b) amelyeknél ezt az arra jogosult személy elrendelte.

Ezen esetekben a küldemények címzettje köteles gondoskodni az általa átvett hivatalos küldemény iratkezelési szabályzat szerinti iktatásáról. Korábban a rendelet további esetként akkor is a címzettet jelölte meg a küldemény felbontására kizárólag jogosult személyként, ha a küldemény névre szóló és megállapíthatóan magánjellegű volt. A jogalkotó ezt az előírást törölte, ugyanakkor az adott szervet hatalmazta fel arra, hogy a névre szóló küldemények kezeléséről az iratkezelési szabályzatában rendelkezzen. A megoldás alkotmányos szempontból aggályos, de az iratkezelési szabályzat elkészítése során az adatvédelmi biztosi gyakorlat nem hagyható figyelmen kívül.

2.1.2. Az adatvédelmi biztos gyakorlata

Az adatvédelmi biztos gyakorlata a magánjellegű és hivatalos levelek megkülönböztetésében azt a szigorú értelmezést követi, hogy „ha a hivatalba érkező névre szóló, megállapíthatóan magánjellegű levelek estében kétség merül fel, akkor azt garanciális okokból a címzettel nyittassák fel, ami után kiderülhet, hogy a levél hivatalos vagy magánjellegű, iktatni kell vagy sem." Hasonló megfogalmazást tartalmaz egy későbbi állásfoglalás is: „a munkavállalónak címzett levelet akkor lehet például postabontóban felbontani, ha a levél címzéséből, külső megjelöléséből egyértelműen kiderül, hogy az hivatalos tárgyú". A biztosi álláspont szerint tehát a hivatalos jellegnek kell megállapíthatónak lennie, és kétség esetén a magánjelleget kell vélelmezni. Abban az esetben, ha mégis magánjellegű levelet nyit fel a munkáltató, a küldeményt vissza kell zárni, és jelezni kell rajta, hogy ki és mikor bontotta fel.

Az adatvédelmi biztos szerint a munkahelyről küldött levél tartalmát a munkáltató teljes körű ellenőrzési joggal rendelkezik, mivel azt munkaidőben, a munkáltató által rendelkezésre bocsátott eszközökkel írta.[77]

2.1.3. Bírósági gyakorlat

A témakört érintő bírósági gyakorlatot nem ismerünk.

2.1.4. Tudományos publikációk és álláspontok

HEGEDŰS BULCSÚ az adatvédelemi biztosi gyakorlatot azzal egészíti ki, hogy annak előírása, hogy a munkavállaló a munkahelyi címén ne folytasson magánjellegű levelezést, nem teremt jogalapot a magánlevelek felbontására, mivel a levél küldőjének a munkahelyi előírásokat nem kell ismernie.[78]

2.1.5. Önszabályozás

Ide kapcsolódó forrást nem találtunk.

2.2. Az elektronikus levelezés ellenőrzésének szabályozása

Az email-írás a munkafolyamat gyakori része, a hivatalos kommunikáció az egyes feladatok teljesítésének fontos része. Az email ugyanakkor személyes adat is, függetlenül a kommunikáció hivatalos vagy magánjellegétől. Ráadásul nem csak a munkavállaló személyes adata, hanem a szervezeten kívüli levélíróé vagy címzetté is, akire nézve a munkáltató szabályzatainak alkalmazhatósága legalábbis kérdéses. A gyakorlatban az elektronikus eszközök és az email magáncélú használatának feltételei általában nagymértékben tisztázatlanok.

2.2.1. Jogalkotás

Speciális előírások nem szabályozzák az elektronikus levelezést, az általános adatvédelmi, munkajogi és polgári jogi szabályok irányadók.

2.2.2. Az adatvédelmi biztos gyakorlata

Az adatvédelmi biztos gyakorlata meglehetősen állásfoglalást tartalmaz az elektronikus levelezéssel kapcsolatban, a gyakorlat azonban nem teljesen konzisztens.

A gyakorlat különbséget tesz a küldött és a fogadott levelek között. Az adatvédelmi biztos szerint a munkáltatónak sokkal szélesebb ellenőrzési joga van a munkavállaló által küldött emailek esetében, mivel a munkavállaló az email megírásával egyúttal adatkezelési hozzájárulást is ad.[79]

Ezt a megkülönböztetést a későbbi állásfoglalások is megismétlik, és újból hangsúlyozzák a hozzájárulás kérdését: ha a munkavállaló tájékoztatást kapott a munkáltató által gyakorolt

[77] ABI, 120/A/2004
[78] Hegedűs, 2006a, p. 48.
[79] ABI, 120/A/2004, ABI, 1543/A/2004

ellenőrzés lehetőségéről, az email megismeréséhez való hozzájárulás már az email megírásával megadottnak tekintendő.[80]

Egy 2006-os állásfoglalás szerint a munkáltató betekinthet a hivatali emailekbe, amelyeket a munkavállaló feladatainak ellátásával kapcsolatban küldtek vagy fogadtak, a munkáltató utasításai szerint. Ilyen esetben is biztosítani kell azonban harmadik személyek magánélethez való jogát. A dokumentum nem utal a munkavállaló hozzájárulásának szükségességére.[81]

Későbbi gyakorlatában az adatvédelmi biztos megerősítette a hozzájárulás szükségességét, és megállapította, hogy az emailek kezeléséhez (ide értve azok megismerését is) mind a küldő, mind a címzett hozzájárulását meg kell szerezni.[82] E megállapítás azon a feltevésen alapul, hogy ebben az esetben az adatkezelésnek nincs speciális, törvényi jogalapja, így az kizárólag hozzájárulás alapján történhet. Hangsúlyoznunk kell, hogy a hozzájárulás önkéntessége egy munkajogi jogviszonyban erősen kérdéses, és ha elfogadjuk, hogy a hozzájárulás valóban egy önkéntes nyilatkozat, a munkavállaló a hozzájárulását feltehetően nem fogja megadni olyan esetben, amikor valamit titkolni akar a munkáltató elől, és az ellenőrzésnek súlyos következményei lehetnek.

Az ajánlás azt is megállapítja, hogy a munkáltatónak minden munkavállalót tájékoztatnia kell az ellenőrzés szabályairól, és ebben az esetben a munkavállalónak számolnia kell az ellenőrzés lehetőségével. Az állásfoglalás egyértelműen nem tartalmazza, de utal arra, hogy a hozzájárulás már az email megírásával megadottnak tekintendő.

Ugyanebben az állásfoglalásában a biztos azt is kimondja, hogy a munkáltatónak joga van ahhoz, hogy a „munkavállalójától azt kérje, hogy a beérkező, illetőleg a kimenő hivatalos tárgyú elektronikus leveleket számára nyomtatott formában adja át". „A kizárólag munkavégzés céljából átadott e-mail postafiók ellenőrzése kapcsán a munkáltatónak joga van arra, hogy a postaládában lévő e-mailek fejlécének megtekintése után – ahol szerepel a küldő és a fogadó személye, e-mail címe, a levél megnevezése, a küldés időpontja, a levél mérete – egy konkrét levél kiadását kérje a munkavállalótól." Ez esetben a másik fél levéltitkára hivatkozva a levél átadása megtagadható, de ekkor a munkavállaló munkajogi szankciókkal számolhat.[83]

Véleményünk szerint a hivatalos célú levelezés esetén az e-mail tartalmának ellenőrzéséhez csak a másik fél hozzájárulása szükséges, a munkavállalóé nem, mivel az adatkezelés jogalapját ez esetben a munkáltató Mt-ben foglalt felügyeleti jogának gyakorlására vonatkozó szabályok adják. Ha ugyanis a munkavállaló hozzájárulása az adatkezelés jogalapja, ez a hozzájárulás jogkövetkezmény nélkül visszavonható. A gyakorlatban ez a koncepció nem működhet.

2.2.3. Bírósági gyakorlat

A témakört érintő bírósági gyakorlatot nem ismerünk.

[80] ABI, 1722/A/2004
[81] ABI, 1393/K/2006
[82] ABI, 40/K/2006
[83] ABI, 40/K/2006

2.2.4. Tudományos publikációk és álláspontok

A tudományos publikációk mindenek előtt rögzíti, hogy az emailekre is kiterjed a levéltitok védelme, és az adatvédelmi követelmények minden olyan esetben irányadók, amikor az email címzése vagy tartalma egy meghatározott természetes személyhez köthetők – az esetek többségében ez a feltétel teljesül.[84]

A releváns szakirodalmi álláspontok szerint az email tartalma két személyhez kapcsolódik, így mind a küldő, mind a címzett személyes adatának minősül, akkor is, ha valamelyikük a munkáltató szervezetén kívüli személy. Ilyen esetben az adatkezelés jogalapja csak a szervezeten kívüli személy hozzájárulása lehet.[85] E harmadik személy – megfelelő tájékoztatáson alapuló – hozzájárulásának beszerzése a gyakorlatban korántsem egyszerű.

Szintén fontos kérdése a szakirodalmi forrásoknak az elektronikus levél hivatali vagy magán jellegének meghatározása. A magánlevelezést a munkáltató nem ellenőrizheti, kivéve, ha ahhoz a munkavállaló és az érintett harmadik személy is hozzájárul.[86] Álláspontunk szerint a hozzájárulás tényén túl egy további követelménynek is teljesülnie kell: a magánjellegű emailek ellenőrzése csak jogszerű cél érdekében történhet. A gyakorlatban a magánjellegű levelezés ellenőrzésének általában nincs jogszerű célja, kivéve a hivatali és a magán levelezés elkülönítése érdekében történő ellenőrzést. A tudományos álláspontok szerint a munkáltatónak az email tartalmát csak akkor ismerheti meg, ha az üzenet egy hivatali email-címre érkezett, és az ellenőrzés minden érintett hozzájárulásával történik; a munkavállaló hozzájárulása megadottnak tekintendő, ha tud az ellenőrzés lehetőségéről.[87]

A tudományos publikációk aszerint is különbséget tesznek, hogy az emailt a munkavállaló vagy külső harmadik személy írta.[88] A különbségtétel az adatvédelmi biztos gyakorlatán alapul, amivel néhány szerző egyetért,[89] mások pedig nem: ARANY TÓTH szerint az emaileket az érintettek státuszától függetlenül azonos vagy nagyon hasonló védelemnek kell megilletnie.[90] Azzal ugyan egyetértünk, hogy az emailek minden típusára azonos elvek alkalmazandók, az adatvédelmi biztos által is alkalmazott különbségtétellel azonban egyetértünk. A levél tartalmának megismerése ugyanis más-más jogalap alapján történik a munkavállaló és a külső fél által írt email esetében. Azt is hozzá kell tenni azonban, hogy a különbségtétel a gyakorlatban meglehetősen nehéz.

Végül ARANY TÓTH MARIANN azt is felveti, hogy az elektronikus adatokhoz kapcsolódó forgalmi adatok kezelése során az elektronikus hírközlési jog[91] adatvédelmi rendelkezéseit is figyelembe kell venni.[92] Azzal ugyan egyetértünk, hogy a hírközlési adatvédelmi előírások

[84] Gálik/Polyák, 2005, p. 212., Arany Tóth, 2008a, p. 267., Hegedűs, 2006a, p. 47.
[85] Arany Tóth, 2008a, p. 268., Hegedűs, 2006a, p. 48.
[86] Arany Tóth, 2008a, p. 271., Hegedűs, 2006a, pp. 48-49., Majtényi, 2006, pp. 345-346.
[87] Arany Tóth, 2008a, pp. 269-270., Hegedűs, 2006a, pp. 48-49.
[88] Más szóval munkahelyen belüli kommunikációról van-e szó, vagy a munkahely és harmadik fél közötti kommunikációról.
[89] Hegedűs, 2006a, p. 48.
[90] Arany Tóth, 2008a, p. 270.
[91] 2003. évi C. törvény az elektronikus hírközlésről
[92] Arany Tóth, 2008a, pp. 272-273.

figyelembe vétele hasznos, azt azonban rögzítenünk kell, hogy a munkáltató nem minősül elektronikus hírközlési szolgáltatónak, akkor sem, ha sajátos hozzáférés-, email- és host-szolgáltatóként tevékenykedik. Ez azért okoz nehézséget, mert az e tevékenységgel összefüggésben keletkező személyes adatok nem kapcsolódnak a munkajogi jogviszonyhoz, kezelésük jogi feltételei ezért tisztázatlanok. A munkáltató elektronikus hírközlési szolgáltatói státuszával kapcsolatban sem az adatvédelmi biztos, sem a szakirodalom nem tett érdemi megállapításokat.

Összességében az e-mail ellenőrzésére vonatkozó biztosi joggyakorlatot és szakirodalmat kissé ellentmondásosnak érezzük, amelynek oka elsősorban a jogalap kérdésének tisztázatlansága.

2.2.5. Önszabályozás

Ide kapcsolódó forrást nem találtunk.

2.3. A számítógép-használat szabályozása

A számítógép-használat során számos személyes adat keletkezik. Ezek közé nem csak a számítógépen tárolt személyes dokumentumok tartoznak, hanem a számítógépre telepített, azon futtatott programok listája, az egyes szoftverek használatával kapcsolatos adatok. A munkáltatói ellenőrzés a munkáltató által rendelkezésre bocsátott eszközök használatának ellenőrzésére terjed ki, de adott esetben – például a munkáltató bizalmas információinak védelme érdekében – indokolt lehet a munkavégzésre használt, a munkáltató tulajdonában lévő eszköz ellenőrzése is. Az adatvédelmi jogi gyakorlatban az ellenőrzési jogkör szélessége és az adatok személyes jellegének megállapítása mellett az ellenőrzés módja is problémaként merült fel.

2.3.1. Jogalkotás

Speciális előírások nem szabályozzák a számítógép-használatot, az általános adatvédelmi, munkajogi és polgári jogi szabályok irányadók.

2.3.2. Az adatvédelmi biztos gyakorlata

Az Internet és számítógép használatának ellenőrzésének megítélése során – törvényi szabályozás hiányában – ismét csak az adatvédelmi biztosi joggyakorlatból indulhatunk ki. Ennek értelmében a munkáltató akkor jogosult a munkavállaló számára rendelkezésre bocsátott számítógép használatát ellenőrizni, ha ahhoz az érintett hozzájárult.

Az adatvédelmi biztos gyakorlata szerint a munkavállaló részére átadott számítógépen tárolt programokat, adatokat a munkáltató csak akkor ellenőrizheti, ha az eszközt kizárólag munkavégzés céljából adta át, és a munkavállalók által birtokolt programok installálását tiltotta. A tájékoztatás mellett az adatok kezeléséhez szükséges az érintett munkavállalók hozzájáruló nyilatkozatának a beszerzése is. Az ellenőrzés fogalma a számítógépen tárolt adatok megismerését takarja. Az egyes számítógépeken tárolt programok listájának elkészítése önmagában is személyes adatok kezelésének minősül, és az ellenőrzés eredményének továbbítása vagy nyilvánosságra hozatala is csak az érintett hozzájárulásával

történhet.[93] 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.[94]

Ennek kapcsán is figyelembe kell venni a célhoz kötöttség követelményét: amennyiben az ellenőrzést végző személy olyan adatokat talál, amely a munkával nem összeegyeztethető, akkor az ellenőrzés célja megvalósult, és fel kell szólítani a munkavállalót ezek eltávolítására. Az ellenőrzés arra terjedhet ki, hogy az ellenőrzést végző személy megállapítsa, hogy tiltott programok, fájlformátumok – például zenei, vagy film fájlok – találhatók-e az adattárolón. Ennek észlelésén túl azonban a filmfájlokba nem jogosult betekinteni, zenei anyagokat nem jogosult meghallgatni, mivel ez már túlnyúlik az ellenőrzéssel járó jogkörön.[95] Az ellenőrzés ahhoz nem biztosít jogalapot, hogy a munkáltató a számítógépen tárolt bármilyen magánjellegű dokumentumot megismerjen.[96]

Tilos a munkavállaló tudta nélkül telepített kémprogramokkal figyelni a számítógép használatát. Az adatvédelmi biztos 2005-s állásfoglalása szerint ez olyan titkos információgyűjtésnek minősül, ami alapvetően csak bírói engedéllyel végezhető.[97] Az adatvédelmi biztos állásfoglalásában kimondta, hogy a munkavállalók számítógép használatának, internet-felhasználásának, továbbá munkahelyi magatartásának az ellenőrzésére léteznek olyan, a gyakorlatban kialakult megoldások, amelyek nem sértik vagy korlátozzák az érintettek személyiségi jogait. A kémprogramok használata ezért aránytalan korlátozás.

A számítógép-használat ellenőrzésének sajátos kérdése merült fel akkor, amikor agy németországi vállalat magyar leányvállalatának munkatársa azzal a kérdéssel fordult az adatvédelmi biztoshoz, hogy az anyavállalat utasítására jogszerűen telepíthető-e olyan program a dolgozók számítógépeire, mellyel a német központban lényegében minden, a számítógépen tárolt adatot, azon végezett műveletet ellenőrizhetnének. Állásfoglalásában a biztos arra mutatott rá, hogy a munkáltatói jogkört gyakorló személy adatfeldolgozónak minősül, az anyavállalat pedig a tényleges adatkezelőnek. Ezzel a megoldással lényegében a munkáltatói jogosultság a Magyarországon bejegyzett gazdasági társaságtól a magyar joghatóság alá nem tartozó anyavállalathoz kerülne, mely alapvetően ellentétes a munkavállalók jogainak védelmével, tekintettel arra, hogy a német székhelyű anyavállalat által meghozott döntésekre a magyar joghatóság nem terjed ki. Az adatkezelésnek ez a magyar joghatóság alóli „kihúzása” akkor is sérti az érintettek személyes adatok védelméhez való jogát, ha azok az adatkezeléshez a hozzájárulásukat formailag megadták. Sérül ugyanis

[93] ABI, 866/A/2006-3.
[94] ABI, 772/A/2000, ABI, 841/K/2002
[95] ABI, 866/A/2006-3.
[96] ABI, 531/A/2004
[97] ABI, 1012/K/2005

az Alkotmánybíróság által megfogalmazott azon követelmény, miszerint az érintett személy adatai kezelését jogosult átlátni, az azzal kapcsolatos jogait pedig jogosult érvényesíteni.[98]

2.3.3. Bírósági gyakorlat

A témakört érintő bírósági gyakorlatot nem ismerünk.

2.3.4. Tudományos publikációk és álláspontok

Hegedűs Bulcsú az adatvédelmi biztos gyakorlatát elemezve a fentieket a következő megállapításokkal egészítette ki:

- a magánjellegű fájlok esetében nem csak azok megismerése, de azok másolása vagy törlése is jogellenes; a munkáltató csak azt követően rendelheti el a fájlok törlését, hogy eredménytelenül felszólította a munkavállalót azok eltávolítására;
- a számítógép ellenőrzését lehetőség szerint nem manuálisan, hanem automatizált formában kell történnie.[99]

2.3.5. Önszabályozás

Ide kapcsolódó forrást nem találtunk.

2.4. Az internet és a közösségi hálózatok használatának szabályozása

Az internet használata számos munkavállaló számára elengedhetetlen a feladatai teljesítéséhez, az interneten elérhető információk jelentősen előmozdíthatják a munkavégzést. Másrészről azonban nagy a kockázata annak, hogy a munkavállalók a munkaidőben saját céljaikra használják az internetet. Az internet-használat ellenőrzése ezért fontos a munkáltató számára, ez ugyanakkor a munkavállalók magánszférájának megsértését is jelentheti.

A közösségi oldalak használata, mint a Facebook, szintén felvethet adatvédelmi és munkajogi kérdéseket. Egy negatív hangvételű üzenet, de akár kárt is okozhat a munkáltató hírnevének. Az üzenet közzétételének időpontjából az is kiolvasható továbbá, hogy a munkavállaló munkaidőben a közösségi oldalakat használta. E kérdések a magyar gyakorlatban és szakirodalomban még nem igazán merültek fel, egy tanulmány kivételével, amely a közösségi hálózatok munkajogi vonatkozásait vizsgálja.[100]

2.4.1. Jogalkotás

Speciális előírások nem szabályozzák az elektronikus levelezést, az általános adatvédelmi, munkajogi és polgári jogi szabályok irányadók.

[98] ABI, 2511/K/2007
[99] Hegedűs, 2006b, pp. 82-83.
[100] Horváth/Gelányi, 2011 A közösségi hálózatok általános adatvédelmi kérdéseit a magyar szakirodalom is tárgyalja (ld. Polefkó, 2010-2011) de a munkahelyi adatvédelem kérdései egyelőre nem jelentek meg.

2.4.2. Az adatvédelmi biztos gyakorlata

Az adatvédelmi biztos mindenekelőtt számos határozatában megállapította, hogy az IP-cím és a meglátogatott honlapok címe, a honlap letöltésének időpontja és egyéb adatai személyes adatok, mivel valamely meghatározott természetes személyhez köthetők.[101]

A biztos azt is hangsúlyozza, hogy az internet-használat ellenőrzésére a munkavállaló hozzájárulása alapján kerülhet sor, amely hozzájárulás megfelelő tájékoztatáson alapul.[102] Későbbi döntéseiben a biztos e feltételeket megerősítette.[103] Ha a magáncélú internet-használat tilos, és a munkavállalót tájékoztatták az ellenőrzés lehetőségéről, akkor a munkavállaló valamely honlap letöltésével egyúttal hozzájárulását is adja az adatkezeléshez.[104]

Az internet-használat ellenőrzése nem engedélyezett, ha a munkáltató lehetővé teszi az internet magáncélú használatát. Ha csak a hivatali használat engedélyezett, akkor az ellenőrzés jogszerűségének feltétele, hogy a munkáltató az ellenőrzés lehetőségéről tájékoztatja a munkavállalót. A meglátogatott honlapok titkos ellenőrzése tilos.[105]

2.4.3. Bírósági gyakorlat

Az internet-használat ellenőrzésével kapcsolatban bírósági ítélet nem született. Van azonban egy említésre méltó bírósági ítélet, amelyben a bíróság azt vizsgálta, hogy a számítógép és az internet magáncélú használata lehet-e rendkívüli felmondási ok. Az érintett munkavállaló többek között erotikus oldalakat látogatott meg, saját és kollégája számítógépét egyaránt felhasználva. A Legfelsőbb Bíróság szerint e magatartás tekinthető a munkaszerződés súlyos megsértésének, mivel a magáncélú használatot a munkáltató megtiltotta, így a cselekmény szolgálhat rendkívüli felmondás indokaként.[106] Az ítélet ugyanakkor nem foglalkozik azzal a kérdéssel, hogy a munkáltató hogyan jutott a meglátogatott oldalakra vonatkozó adatok birtokába, és hogy ez az adatgyűjtés jogszerű volt-e vagy sem.[107]

2.4.4. Tudományos publikációk és álláspontok

A tudományos publikációk mindenekelőtt különbséget tesznek a hivatali és a magáncélú internet-használat között. Általánosságban a munkáltató jogának tekintik az internet-használat feltételeinek meghatározását. A gyakorlatban azonban e feltételek sokszor tisztázatlanok, és a munkavállaló a munkáltató „hallgatólagos beleegyezésével” használhatja magáncélra az internetet.[108]

---

[101] ABI, 693/K/1998, ABI, 750/A/2004, ABI, 1598/K/2004. Meg kell említenünk, hogy ezek az adatok nem minden esetben köthetők egy meghatározott természetes személyhez. Mind a magyar, mind az európai megközelítés azon a feltevésen alapul azonban, hogy az IP-cím meghatározott természetes személyhez köthető.
[102] ABI, 531/A/2004
[103] ABI, 800/K/2008
[104] ABI, 1767/K/2006
[105] ABI, 570/A/2001
[106] BH2006. 64.
[107] A munkavállaló beismerte az erotikus oldalak látogatását – a bíróságnak ezért nem kellet az adatgyűjtés körülményeivel foglalkoznia.
[108] Arany Tóth, 2008b, pp. 170-171.

Ha a munkavállaló számára megengedett a magáncélú internet-használat, akkor a munkáltató nem ellenőrizheti a meglátogatott oldalakat.[109] Ha kizárólag a hivatali internet-használat megengedett, a munkáltató a használatot kontrollálhatja, de ebben az esetben is csak akkor, ha ehhez a munkavállaló hozzájárult, és őt az ellenőrzés lehetőségéről tájékoztatták. A további adatvédelmi alapelveket, mint például az arányosság, szintén figyelembe kell venni.[110]

A meglátogatott oldalak tartalmán túl más forgalmi adatok ellenőrzésének is lehet jelentősége (például a túl nagy forgalom a tartalmak illegális letöltésére és szerzői jogi jogsértésre utalhat). A forgalmi adatok kezelésének feltételeit általánosan alkalmazható szabályozás nem tisztázza. ARANY TÓTH felveti ugyan az elektronikus hírközlési szabályozás alkalmazását,[111] mi azonban továbbra is úgy gondoljuk, hogy a munkáltató nem alanya e szabályozásnak.[112]

A tudományos publikációk az ellenőrzés helyett a magáncélú internet-használat egyéb módon történő korlátozását javasolják, mint például bizonyos tartalmak kiszűrése vagy a megtekinthető oldalak körének pontos meghatározása.[113] Valóban rendelkezésre állnak ugyan ilyen privacy-barát megoldások, valószínűleg azonban gyakorlati alkalmazásuk nehézkes és nem is jellemző.

2.4.5. Önszabályozás

Ide kapcsolódó forrást nem találtunk.

2.5. A telefonhasználat ellenőrzése

A munkavállalók rendszerint ellenőrzik a munkáltatók telefonhasználatát, különösen akkor, ha ennek költségeit a munkavállaló viseli.

2.5.1. Jogalkotás

A munkavállalók telefonhasználatára nincs speciális jogszabály. Közvetve ugyanakkor szabályozza e kérdést a Ptk., az elektronikus hírközlési törvény, az Mt. és az adatvédelmi törvény.

A Ptk. védi a magántitkot, ide értve a kommunikáció bizalmasságát is, és a személyhez fűződő jogok között védi a hangfelvételt.

A telefonos hangszolgáltatások az elektronikus hírközlési törvény hatálya alatt is állnak, amely kifejezetten a munkaviszonyra vonatkozó rendelkezést nem tartalmaz. A szolgáltatót a törvény kötelezi arra, hogy a felhasználó hozzájárulása nélkül forgalmi és helymeghatározási adatokat ne tárjon fel.

Az Mt. a munkáltató részére lehetővé teszi a munkaeszközök használatának meghatározását, és ez magában foglalja a telefonhasználatot is.

[109] Arany Tóth, 2008b, p. 172.
[110] Hegedűs, 2006b, pp. 82-83.
[111] Arany Tóth, 2008b, p. 173.
[112] Ld. az elektronikus levelezésről szóló fejezetben.
[113] Arany Tóth, 2008b, p. 173., Hegedűs, 2006b, pp. 82-83., Jóri/Hegedűs/Kerekes, 2010, p. 288.

A telefonhasználat minden esetben magában foglalja a személyes adatok kezelését, így az általános adatvédelmi szabályok szintén alkalmazandók.

2.5.2. Az adatvédelmi biztos gyakorlata

A telefonhasználathoz kapcsolódó adatkezelés az adatvédelmi biztos gyakorlatában visszatérő probléma. A fontosabb állásfoglalások a következők:

- Munkavállalók telefon- és Internet használatának ellenőrzése.[114]
- A munkahelyi telefonhasználat ellenőrzése a személyi jövedelemadóról szóló törvény figyelembe vételével.[115]
- Állásfoglalás a köztisztviselő által kezdeményezett telefonhívások adatainak megismerhetőségéről.[116]

Az adatvédelmi biztos gyakorlata a következőkben foglalható össze.

1. A munkáltató jogosult ellenőrizni a munkavállalók telefonhasználatát, ugyanakkor nincs joguk hozzáférni a munkavállalók híváslistájához, és nincs joguk a hívott és fogadott számok listájának, illetve a hívások időtartamára vonatkozó adatok átadását követelni a hírközlési szolgáltatótól. A hívásokra vonatkozó adatok ugyanis a munkavállaló és a másik fél személyes adatai.
2. Ugyanezen szabályok irányadók arra az esetre, ha a személyi jövedelemadóra vonatkozó előírások különbséget tesznek a hivatali és a magáncélú telefonhasználat adóztatásában.
3. A biztos szerint a telefonhasználat költségeinek a munkáltató és a munkavállaló közötti megosztását egy előre meghatározott arány szerint célszerű megosztani, vagy a munkáltató által fizetett maximális összeg meghatározásával, így elkerülhető a hívások ellenőrzése.
4. Ha a hivatali és magáncélú hívások hívásonként szétválogatása nem elkerülhető, akkor ezt a válogatást kizárólag a munkavállaló végezheti. Ebben az esetben a munkavállaló a zárt borítékban megkapott hívások közül kiválogatja a hivatali hívásokat, és az egyéb hívott számokat olvashatatlanná teszi.

2.5.3. Bírósági gyakorlat

E témakörben nincs releváns bírósági gyakorlat.

2.5.4. Tudományos publikációk és álláspontok

Az adatvédelmi biztos által kialakított gyakorlat számos szakirodalmi elemzés tárgyát adta.[117]

ARANY-TÓTH szerint a munkavállalók elektronikus megfigyelésének szabályait a munkaviszonyra vonatkozó szabályok között speciális rendelkezésekkel kell szabályozni. E

[114] ABI, 1767/K/2006
[115] ABI, 1672/K/2006
[116] ABI, 3362/P/2009
[117] Ld. Székely/Szabó, 2005 pp. 129-130; Hartai, 2003 p. 48; Hajdú, 2005 pp. 172-173.

szabályozás megalkotása sürgető feladat, mert a hatályos szabályozás nem ad megfelelő iránymutatást a jogszerű adatkezelés feltételeiről, és a hozzájárulás önkéntessége a munkaviszony keretei között mindig kérdéses.[118]

2.5.5. Önszabályozás

Nincs releváns önszabályozási gyakorlat.

2.6. A kamerás megfigyelés szabályozása

A CCTV rendszerek telepítése és kiterjedt használata a hétköznapi élet számos területén általános jelenséggé vált az üzleti tevékenységtől a bűnmegelőzésen és a forgalom-figyelésen át a közbiztonság és a vagyonvédelem területéig. E rendszerek hardver és szoftver elemei egyre intelligensebbek, és a rendszerek terjedése az ipari társadalmak polgárainak magánéletére egyre nagyobb fenyegetést jelent. A CCTV kamerákra gyakran a Nagy Testvér szemeiként hivatkoznak.

A kamerák használata a személyes adatok nagymennyiségű kezelést generálja. Ez igaz a munkavállalók személyiségprofiljának létrehozására is. A munkáltató ellenőrzési és felügyeleti tevékenysége minden eszközt magában foglalhat, a bizalmas tudás és információ védelmében. Az egyes adatok személyes adatok megállapításán és az ellenőrzési jog terjedelmének meghatározásán túl a felügyelet módja az adatvédelmi szabályozás számára is komoly problémát jelent.

2.6.1. Jogalkotás

A kamerás megfigyelésre vonatkozóan nincs külön munkajogi szabályozás.[119] Így csak az általános szabályokra hivatkozhatunk, és kísérletet tehetünk a kamerás megfigyelésre vonatkozó megfelelő következtetések levonására. Az adatvédelem alapelveit az adatvédelmi biztos értelmezte különböző állásfoglalásaiban.

2.6.2. Az adatvédelmi biztos gyakorlata

A jogszerű kamerás megfigyelés körüli viták legkritikusabb pontja a megfigyelés céljának meghatározása. Az üzleti életben és a munka világában a legfontosabb adatkezelési cél a tulajdonvédelem és a munkavállalók védelme. A másik kritikus pont a képfelvételek sorsa. A valós idejű rendszerek esetében a műszaki vagy a biztonsági személyzet figyeli a kamera képeit. Ez a működési mód azonban nagyon ritka. A jelenlegi CCTV rendszerek háttértárolóval vannak felszerelve, és a képfelvételek hosszabb-rövidebb ideig megőrzésre kerülnek. Ez a magánszférára nézve nagyobb kockázatot jelent.

A munkahelyi video-megfigyelés csak törvényes célból fogadható el, és a céltól eltérő adatkezelés minden esetben jogsértő. Az adatvédelmi biztos hangsúlyozza, hogy a felvételek korlátozás nélküli rögzítése és tárolása törvénysértő. A munkavállalókat tájékoztatni a kamera-rendszer telepítéséről, és meg kell határozni annak célját. A tájékoztatásnak arra is ki

[118] Arany Tóth, 2008a, pp. 305-306.
[119] Arany Tóth, 2008a, p. 277.

kell terjednie, hogy a felvételeket rögzítik- és tárolják-e. A munkavállalónak joga van a róla készült felvételeket megnézni és ellenőrizni.[120]

A megfigyelés és a video-felvétel akkor jogszerű, ha a munkavállaló megfelelően tájékozott, és az adatkezeléshez hozzájárulását adta.[121] A rejtett kamerák használata ezért a munkavállalók magánéletének súlyos megsértését jelenti.[122]

2.6.3. Bírósági gyakorlat

A bírósági határozatok tárában 2007 óta összesen 8 olyan ítélet található, amely a munkahelyi kamerás megfigyelés szempontjából valamilyen módon releváns. Ezek az esetek jogszerűtlen felmondásokhoz vagy a munkavállalók diszkriminációjához kapcsolódtak. Eddig egyetlen munkavállaló sem fordult bírósághoz a kamerák munkahelyi telepítése vagy használata miatt. Ennek következtében nem áll rendelkezésünkre kifejezett bírósági ítélet az ilyen rendszerek jogszerű használatának feltételiről. A kapcsolódó esetek mindegyikében bizonyítékként használták a felek a felvételeket, és a bizonyíték jogszerűségét sem a felek, sem a bíróság nem vitatta.[123]

2.6.4. Tudományos publikációk és álláspontok

A munkahelyi kamerás megfigyelés jogi kereteit vizsgáló szerzők többnyire az adatvédelmi biztos által kialakított gyakorlatot foglalják össze, valamint az egyes állásfoglalások értelmezéséhez nyújtanak segítséget. MAJTÉNYI a munkahelyi privacy alapproblémájának tekinti a kamerázást, és kiemeli, hogy alkalmazása csak akkor lehet indokolt, ha az arányban áll a védendő értékekkel, és megfelelően tájékoztattak minden érintettet a megfigyelés körülményeiről.[124] Az érdekek megfelelő mérlegelésével kapcsolatban ARANY TÓTH szerint figyelembe kell venni a kamerák üzemeltetésének időtartamát, időpontját, valamint a megfigyeltek számát is egyes esetekben, mivel azok alapvetően befolyásolják a kamerázás indokoltságát. Kiemeli, hogy a munkavállaló egyéniesített megfigyelése, és minden rejtett kamerás megfigyelés jogellenes.[125] A dolgozók megfigyeléssel kapcsolatos tájékoztatása szerinte megfelelően részletes kell, hogy legyen, így például a felvételek munkáltatói döntéshozatalban betöltött szerepét, a jogorvoslati lehetőségeket is ismertetni kell. Emellett a munkavállalói érdekképviseleti szervek szerepe véleménye szerint nem kellően hangsúlyos, funkcióik a területen még nem alakultak ki megfelelően.[126]

HEGEDŰS arra hívja fel a figyelmet, hogy a kamerarendszerek telepítése – a jogi megítéléstől sokszor függetlenül – egyre gyakoribb a munkahelyeken, mivel egyszerűen kezelhetőek, és alacsony áron elérhetőek. Gyakran a vagyonvédelem mellett munkaügyi ellenőrzés céljából is

[120] ABI, 461/A/1998
[121] ABI, 475/H/2000
[122] Arany Tóth, 2008a, p. 289.
[123] Az ügyek listája: Fővárosi Munkaügyi Bíróság - 5.M. 394/2007/12.; Veszprémi Munkaügyi Bíróság - 2.M.341./2006./8.; Miskolci Munkaügyi Bíróság - 8.M.1286/2005/19.; Fővárosi Munkaügyi Bíróság - 31.M.3189/2002/55.; Pécsi Munkaügyi Bíróság - 3.M.1763/2005/15.; Nyíregyházi Munkaügyi Bíróság - 1.M.687/2005/12.
[124] Majtényi, 2006, pp. 347-348.
[125] Arany Tóth, 2008, pp. 287-289.
[126] Arany Tóth, 2008, pp. 294., 311.

használják őket a munkáltatók, amit azonban semmilyen érdek nem támaszt alá, mivel a tartós megfigyeltség érzete személyiségváltozást eredményezhet.[127] A kamerás megfigyelés állampolgárokra gyakorolt hatása kapcsán megállapítható, hogy bár számos vizsgálat és tanulmány készült e témában, azok jelentősen eltérő eredményekre jutottak, általános tendenciák lényegében nem vonhatóak le.[128]

2.6.5. Önszabályozás

Egy kollektív szerződés – a Budapesti Közlekedési Zrt.-nél - említi az adatvédelmi szabályok betartásának szükségességét, kifejezetten a munkavállalókról készített felvételekkel kapcsolatban. A BKV Zrt. kollektív szerződésének 2. sz. mellékletének 3. pontja „a járművezetők ellenőrzése szabályozásának leírása" címet viseli. 3.1. pontja leírja az ellenőrzés során követendő általános irányelveket. Ez a fejezet a következő szűkszavú és tartalmilag semmitmondónak tekinthető szöveget tartalmazza: „A fényképezőgéppel és videokamerával végzett ellenőrzések során kiemelt figyelmet kell fordítani a személyiségi jogok védelmére és az adatkezelési törvényben foglaltakra. Az elkészített felvételeket csak az ellenőrzés dokumentálására és a személyiségi jogok figyelembevételével balesetmegelőző anyagokban szabad felhasználni."

2.7. Az RFID használatának szabályozása

A rádiófrekvenciás azonosítás[129] (a továbbiakban: RFID) olyan technológia, amely rádióhullámokat használ valamely elektronikus jel, ún. RFID címkékből származó jelek továbbítására. A címke egy meghatározott tárgyhoz van hozzárendelve. A jeleket megfelelő vevőkészülék értelmezi, és ez alapján azonosítja és nyomon követi az adott tárgyat.

Az RFID technológia születését jelentős viták és kritikák kísérték a magánszféra védelmezőinek oldaláról. A két legfontosabb adatvédelmi fenntartás a következő:

Mivel az adott tárgy birtokosa nem feltétlenül van tudatásban az RFID címke alkalmazásának, és a címkék távolról is leolvashatók az érintett tudta nélkül, lehetővé válik az érintett hozzájárulása nélkül rá vonatkozó érzékeny adatok gyűjtése.

Ha a címkézett tárgy megvásárlása során a vevő bankkártyával vagy valamely pontgyűjtő-kártyával fizet, akkor közvetve, az adott tárgy egyedi azonosítóján keresztül a vevő személyazonossága is megállapíthatóvá válik.

Az Európai Unió 2009. május 12-én ajánlást fogadott el a magánéletnek az RFID területén alkalmazandó garanciáiról.[130] Az ajánlás szerint a tagállamoknak biztosítaniuk kellene, hogy az RFID üzemeltetők átfogó adatvédelmi tesztet végeznek a rendszer üzembe helyezése előtt. Az RFID üzemeltetők a teszt eredményeit a megfelelő hatóság részére átadják.

[127] Jóri/Hegedűs/Kerekes 2010, p. 286. Ld. még 35/2002. (VII.19.) ABH
[128] Szőke 2011, p. 204.
[129] Radio-frequency identification
[130] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 2011, p. 3.

2.7.1. Jogalkotás

Az RFID technológiát a magyar jogban kizárólag a frekvenciagazdálkodás körében említik jogszabályok, amelyeknek adatvédelmi vonatkozása nincs.

2.7.2. Az adatvédelmi biztos gyakorlata

Nincs releváns joggyakorlat.

2.7.3. Bírósági gyakorlat

Nincs releváns bírósági gyakorlat

2.7.4. Tudományos publikációk és álláspontok

Nincs releváns szakirodalom.

2.7.5. Önszabályozás

Nincs releváns önszabályozási gyakorlat.

2.8. A biometrikus azonosítók szabályozása

A biometrika olyan technológiákat foglal magában, amelyek alkalmasak arra, hogy meghatározott, az adott egyénre kizárólagosan jellemző sajátosságok és fizikai jellemvonások alapján azonosítsanak egyéneket. Bármely fiziológiai és/vagy magatartási jellemző alkalmazható biometrikus jellemzőként, feltéve, hogy megfelel az alábbi követelményeknek:

- Univerzalitás: minden személy rendelkezik az adott jellemzővel;
- Megkülönböztető jelleg: az adott jellemzőalapján bármely két személy megfelelően megkülönböztethető egymástól;
- Folytonosság: az adott jellemző megfelelő mértékben állandó;
- Gyűjthetőség: az adott jellemző kvalitatív módon mérhető;[131]

A biometrikus azonosító egy olyan mintafelismerő rendszer, amely a működése során biometrikus adatokat gyűjt az érintettről, a gyűjtött adatokból előállít egy személyes jellemzőt, és e jellemzőt összehasonlítja az adatbázisban lévő mintákkal. A rendszer a biometrikus adatokat négy lépésben gyűjti és kezeli:

- leolvassa valamely fizikai jellemzőt,
- e jellemzőt digitális kóddá konvertálja,
- a kódot egy adatbázisban tárolja,
- az adatbázis és a digitális kód alapján később az érintett azonosítható.

A biometrikus rendszer két módon működhet: ellenőrző és azonosító módban.

Az ellenőrző módban a rendszer a biometrikus adat és a korábban összegyűjtött biomertikus adatok összehasonlításával igazolja valamely személy identitását. A nem biometrikus ellenőrző rendszerek PIN-kód, felhasználói név vagy jelszó használatát jelentik. Amikor

[131] McGuire, 2000, pp. 441, 444.

például a felhasználó a jelszavát megadja egy számítógépnek, a számítógép egy-az-egyben összehasonlítást végez annak megállapítására, hogy a hozzáférést igénylő a megfelelő felhasználó-e. Az ellenőrzést rendszerint pozitív azonosításra használják, ahol a cél annak kizárása, hogy több személy használja ugyanazt az identitást.[132]

Az azonosítási módban működő biometrikus rendszer az érintettet az adatbázisban szereplő összes felhasználóval való összehasonlítás alapján ismeri fel. Ebben az esetben a rendszer egy-a-többhöz típusú összehasonlítást végez. Az azonosítási módot általában negatív azonosításhoz használják, ahol a cél annak megakadályozása, hogy ugyanazon személy több identitást alkalmazzon. Ez az eredmény kizárólag biometrikus adatok kezelésével érhető el.[133]

2.8.1. Jogalkotás

A biometrikus adatok kezelésére vonatkozó legfontosabb jogszabály a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII törvény. Más jogszabályok visszautalnak e törvényre, és további előírásokat nem állapítanak meg. A munkajogi jogviszonyokra vonatkozóan nincs a biometrikus adatok gyűjtését és kezelését szabályozó jogszabály.

2.8.2. Az adatvédelmi biztos gyakorlata

Az elmúlt években az adatvédelmi biztos kevés ügyben foglalkozott a biometrikus azonosítókkal, és ezek az ügyek rendszerint a bűnügyi nyilvántartással foglalkoztak; ezek az ügyek a kutatás szempontjából nem relevánsak. A biometrikus adatok kezelésére vonatkozó általános megállapításokat tartalmazó állásfoglalásában a biztos a lehető legkevesebb adat kezelésének elvét erősítette meg. A biztos hangsúlyozza, hogy a több egyenértékű adatkezelési módszer közül az adatkezelő köteles azt választani, amelyik az információs önrendelkezési jog legkisebb sérelmét vagy korlátozását okozza, és a lehető legkevesebb adat kezelését eredményezi.[134] Egy másik ügyben az adatvédelmi biztos aláhúzta, hogy az érintettet a biometrikus adatok kezeléséről mindig megfelelően tájékoztatni kell. Ezen adatok kezelése a biztos szerint csak kivételes feltételek teljesülése esetén megengedett.[135]

2.8.3. Bírósági gyakorlat

Nincs releváns bírósági gyakorlat e tárgykörben.

2.8.4. Tudományos publikációk és álláspontok

Nincs releváns szakirodalom.

2.8.5. Önszabályozás

Nincs releváns önszabályozási gyakorlat.

---

[132] Jain/Prabhakar/Ross, 2004
[133] Betzel, 2005, p. 520.
[134] ABI, 1454/K/2010
[135] ABI, 926/H/2010

2.9. A GPS és GSM technológia használata a munkavállaló földrajzi helyének meghatározására

A GPS és a GSM technológia használható a munkavállalók mozgásának figyelemmel kísérésére. A leggyakoribb adatvédelmi probléma a munkavállalók járműveibe szerelt GPS-eszközökhöz kapcsolódnak. A mobiltelefonba épített GPS-eszközök és a kapcsolódó mobil alkalmazások időnként szintén okoznak adatvédelmi problémákat. A mobiltelefonok helymeghatározási célú alkalmazása a GPS-szel azonos kérdéseket vet fel.

2.9.1. Jogalkotás

A magyar jogrendszerben a GPS és GSM technológiához kapcsolódó speciális szabályozás nincs. A mobiltelefonok segítségével gyűjtött helymeghatározási adatok kezelés ugyanakkor az elektronikus hírközlési törvény hatálya alá tartozik, amelynek 156. § (13) és (14) szerint az értéknövelt szolgáltatás nyújtásához szükséges helymeghatározási adatok kezelése esetén a szolgáltató köteles a felhasználót tájékoztatni a kezelt adatok típusáról, az adatfeldolgozás céljáról, időtartamáról, továbbá arról, hogy az adatokat szükséges-e harmadik fél számára továbbítani, és a felhasználóval kapcsolatos helymeghatározási adatokat kizárólag a felhasználó hozzájárulása esetén dolgozhatja fel, olyan mértékben és időtartamig, amely szükséges az értéknövelt szolgáltatás nyújtásához.

2.9.2. Az adatvédelmi biztos gyakorlata

A munkavállalók GPS vagy GSM technológia segítségével történő nyomon követése az adatvédelmi biztos gyakorlatában visszatérő probléma. A legfontosabb kapcsolódó ajánlások a következők:

- Állásfoglalás a SIM-kártya cellainformációinak útján történő földrajzi helymeghatározásról a munkavállalók esetében;[136]
- Állásfoglalás munkavállaló mobiltelefonjába szerelt helymeghatározó rendszer működtetéséről;[137]
- Állásfoglalás a munkavállaló tartózkodási helyének mobiltelefon cellainformációi alapján történő ellenőrzéséről;[138]
- Állásfoglalás a munkáltató által gépjárműbe szerelt GPS nyomkövető rendszer alkalmazásáról;[139]
- Állásfoglalás munkavállaló mobiltelefonjába szerelt GPS rendszerről;[140]
- Állásfoglalás egy multinacionális cég által bevezetett GPS rendszerről;[141]
- Személykövető rendszer működtetésének adatvédelmi feltételei;[142]

A biztos gyakorlata a következő megállapításokkal foglalható össze:

[136] ABI, 920/K/2006
[137] ABI, 663/P/2009
[138] ABI, 1092/P/2009
[139] ABI, 415/K/2009
[140] ABI, 636/K/2009
[141] ABI, 857/K/2009
[142] ABI, 922/2/2010

1) A természetes személy földrajzi pozíciója személyes adat. A jármű pozíciója a járművet használó személy személyes adata.
2) Ha a munkáltató helymeghatározó eszközt telepít a munkavállaló által használt járműbe vagy mobiltelefonba, akkor adatkezelővé válik.
3) A munkavállalók helymeghatározási adatainak kezelésére törvény nem ad felhatalmazást. Helytelen az az értelmezés, amely szerint az Mt. 103. § (1) bekezdése megfelelő jogalapot biztosít az ilyen adatok kezeléséhez.[1] Kizárólag az érintett hozzájárulása lehet az adatkezelés jogalapja.
4) Kizárólag azok a munkavállalók ellenőrizhetők helymeghatározó eszközökkel, akiknek a munkája ezt szükségessé teszi, és a megfelelő munkavégzés ellenőrzése más módon nem megoldható.
5) A munkavállalók nyomon követése kizárólag munkaidőben megengedett. Az adatvédelmi biztos számos esetben tett ajánlást arra, hogy a munkáltatók biztosítsák a munkavállalók részére a helymeghatározó eszközök kikapcsolásának lehetőségét.

2.9.3. Bírósági gyakorlat

Nincs releváns bírósági gyakorlat.

2.9.4. Tudományos publikációk és álláspontok

A szakirodalom forrásai alapvetően az adatvédelmi biztos gyakorlatát foglalják össze.[143]

2.9.5. Önszabályozás

Nincs releváns önszabályozási gyakorlat.

[143] Székely/Szabó, 2005, p. 130., Jóri/Hegedűs/Kerekes, 2010, pp. 289-290.

3. A MUNKAHELYI ADATVÉDELMI SZABÁLYOK MEGSÉRTÉSÉNEK KÖVETKEZMÉNYEI

Az adatvédelmi követelmények megsértése esetére a jogalkotó mind reparatív, mind represszív jellegű szankciókat kilátásba helyez. Mivel az adatvédelmet a Ptk. a személyhez fűződő jogok közé sorolja, ezért azzal kapcsolatban az általános polgári jogi szankciók is igénybe vehetők. Az adatvédelmi törvény ugyanakkor az általánostól eltérő kárfelelősségi mércét tartalmaz. Az adatvédelem szabálysértési jogi és büntetőjogi következményeit olyan ún. keretténállások szabályozzák, amelyek a magatartás jogellenes jellegét az általános és az adott adatkezelésre vonatkozó ágazati adatvédelmi rendelkezések alapján rendelik meghatározni.[144]

3.1. Az adatvédelmi törvényen alapuló jogkövetkezmények

3.1.1. Bírósági jogérvényesítés

Az adatvédelmi törvény az érintett jogainak érvényesítéséhez bírósági utat biztosít. Amennyiben az adatkezelő az érintettet korlátozza jogainak gyakorlásában, akkor az érintett a jogait bírósági úton is érvényesítheti. A bírósági eljárásra vonatkozó rendelkezések az érintett részére kedvező helyzetet teremtenek, többek között a bizonyítási kötelezettség megállapításával. A bizonyítási eljárás általános szabályaival szemben nem az érintett, hanem az adatkezelő köteles bizonyítani azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel. Ha a bíróság a kérelemnek helyt ad, az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, törlésére, az érintett tiltakozási jogának figyelembevételére kötelezi. A bíróság elrendelheti ítéletének nyilvánosságra hozatalát, ha azt az adatvédelem érdekei és nagyobb számú érintett jogai megkövetelik.

Az Avtv. az adatvédelmi követelmények megszegésével okozott károkért viselt felelősséget az általános polgári jogi felelősségnél szigorúbban szabályozza. A törvény szerint az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt köteles megtéríteni. A felelősség alól kizárólag akkor mentesül, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.[145] Nem kell megtéríteni a kárt annyiban, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

3.1.2. Az adatvédelmi biztos

A korábbi adatvédelmi törvény a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében létrehozta az adatvédelmi biztos intézményét. Az adatvédelmi biztost az Országgyűlés választotta hat évre. Jogállást a korábbi

[144] Ld. EBH2002. 613.
[145] Ez a szabályozás az adatkezelő felelősségét a Ptk. ún. veszélyes üzemi kárfelelősségi mércéje szerint szabályozza (Ptk. 345. §).

adatvédelmi törvény és az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény határozza meg.

Az adatvédelmi biztos figyelemmel kísérte a személyes adatok védelmének és a közérdekű adatok nyilvánossága érvényesülésének feltételeit. Ennek keretében egyéni bejelentés alapján vagy – ha az adott ügyben bírósági eljárás nincs folyamatban – hivatalból ellenőrizte az Avtv. és az adatkezelésre vonatkozó más jogszabályok megtartását. Egyéni bejelentéssel bárki az adatvédelmi biztoshoz fordulhatott, ha véleménye szerint személyes adatainak kezelésével, a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogainak gyakorlásával kapcsolatban jogsérelem érte, vagy annak közvetlen veszélye fennáll, kivéve, ha az adott ügyben bírósági eljárás van folyamatban.

Jogellenes adatkezelés észlelése esetén az adatvédelmi biztos a következők szerint, nem hatósági jogkörben járt el:

- az adatkezelőt az adatkezelés megszüntetésére szólította fel, ami alapján az adatkezelő haladéktalanul köteles volt megtenni a szükséges intézkedéseket, és erről 30 napon belül írásban tájékoztatni az adatvédelmi biztost,
- tájékoztathatta a nyilvánosságot eljárásának megindításáról, a jogellenes adatkezelés (adatfeldolgozás) tényéről, az adatkezelő (adatfeldolgozó) személyéről és a kezelt adatok köréről, valamint az általa kezdeményezett intézkedésekről, meghozott határozatokról,
- ha az adatkezelő vagy adatfeldolgozó a személyes adatok jogellenes kezelését (feldolgozását) nem szüntette meg, az adatvédelmi biztos határozatban elrendelhette a jogosulatlanul kezelt adatok zárolását, törlését vagy megsemmisítését, megtilthatta a jogosulatlan adatkezelést vagy adatfeldolgozást, továbbá felfüggeszthette az adatok külföldre továbbítását,
- az adatkezelő, az adatfeldolgozó vagy az adatkezeléssel érintett személy az adatvédelmi biztos határozatának felülvizsgálatát jogszabálysértésre hivatkozással kérhette a bíróságtól, amely a felülvizsgálat során a polgári perrendtartásról szóló törvénynek a közigazgatási perekre vonatkozó szabályai szerint jár el.

Az adatvédelmi biztos feladatkörében a fentieken túl általános jelleggel, valamint meghatározott adatkezelő részére ajánlást bocsáthatott ki. Az adatkezelő köteles a részére kibocsátott ajánlásra harminc napon belül érdemben válaszolni.[146]

3.1.3. A Nemzeti Adatvédelmi és Információszabadság Hatóság

Az új adatvédelmi törvény kétségkívül legtöbb vitát kiváltó eleme az adatvédelem és információszabadság felügyeleti rendszerének újraszabályozása. A szabályozás lényege, hogy – megtartva több adatvédelmi biztosi jogosítványt – új hatósági jogkörökkel és bírságolási joggal kiegészülve felügyeleti hatóság jön létre, amelynek elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi ki. Az új hatóság 2012. január 1-i felállítása miatt az

[146] Gálik/Polyák 2005, pp. 226-227.

adatvédelmi biztos intézménye a jelenlegi adatvédelmi biztos mandátumának mintegy félidejénél megszűnik.

A létrejövő hatóság autonóm államigazgatási szerv, amelynek elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi. A kinevezés módja a jelenlegi modellhez képest egyértelmű visszalépés: az országgyűlés kétharmadának szavazatával megválasztott adatvédelmi biztoshoz képest a hatóság elnöke kevésbé lehet független tisztség. A szervezetrendszerrel kapcsolatban több rendelkezés is biztosítja a formális függetlenséget: Az elnök megbízása meglehetősen hosszú időre, kilenc évre szól, és a visszahívás feltételei korlátozottak és pontosan körülhatároltak. Az újraválaszthatóság lehetősége ugyanakkor nagymértékben rontja a hosszú kinevezési idő függetlenséget erősítő hatását. A törvény az elnökjelölttel szemben részletes összeférhetetlenségi szabályokat és szakmai követelményeket határoz meg, melyek nem különböznek lényegesen a hatályos, adatvédelmi biztosra vonatkozó szabályoktól.

A hatóság elnökének munkáját az általa határozatlan időre kinevezett elnökhelyettes segíti, amely felett az elnök gyakorolja a munkáltatói jogokat. Az elnökhelyettesre vonatkozó kinevezési feltételek és összeférhetetlenségi szabályok megegyeznek az elnökre vonatkozó szabályokkal. Mind az elnököt, mind a helyettesét vagyonnyilatkozat-tételi kötelezettség terheli.[147] A hatóság elnöke – meghatározott végzettséggel és gyakorlattal rendelkező – vizsgálókat nevezhet ki a köztisztviselői létszám legfeljebb húsz százalékáig.[148] A vizsgáló más köztisztviselőhöz viszonyított speciális jogállását, feladatait sem a törvényszöveg, sem az indokolás nem részletezi.

A törvény részletesen meghatározza a hatóság feladat- és hatásköreit és egyes hatásköröknél részletezi az eljárási szabályokat.

Az új Avtv. 52. §-a szerint a hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok (közérdekből nyilvános adatok) megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll. A hatóság – néhány kivételtől eltekintve – köteles a vizsgálatot lefolytatni,[149] az eljárás során a jelenlegivel lényegében azonos vizsgálati jogkörök illetik meg.[150]

A vizsgálat szabályozásával – az indokolás szerint is[151] – lényegében a korábbi ombudsman jellegű hatásköröket kívánta a jogalkotó átmenteni, és külön is rögzíti, hogy a hatóság vizsgálata nem minősül közigazgatási hatósági eljárásnak, arra a Ket. szabályait nem kell alkalmazni.[152]

---

[147] Új Avtv. 46-47. §§
[148] Új Avtv. 51. § (1)
[149] A vizsgálat lehetséges elutasításának oka lehet továbbra is pl. az, ha az ügyben bírósági eljárás van folyamatban. A további szabályokat ld. 53. § (2)-(3)
[150] Új Avtv. 54. §
[151] Új Avtv. indokolás az 52. §-hoz
[152] Új Avtv. 52. § (2)

A vizsgálat végeztével – 2 hónapon belül – a hatóság felhívhatja az adatkezelőt a jogsérelem orvoslására, amelynek megtételéről, vagy arról, hogy az abban foglaltakkal nem ért egyet, az adatkezelő 30 napon belül köteles a hatóságot tájékoztatni. Amennyiben ez nem vezet eredményre, úgy a hatóság ajánlást tehet a szerv felügyeleti szervének,[153] nyilvános jelentést készíthet az ügyről illetve adatvédelmi hatósági eljárást kezdeményezhet vagy titokfelügyeleti hatósági eljárást kezdeményezhet.[154] E két hatósági eljárást egyébként a hatóság felhívás és/vagy ajánlás kibocsátása nélkül is kezdeményezheti.

A hatóság ugyancsak a vizsgálat eredményeként ajánlást tehet jogszabály módosítására is, amennyiben a jogsérelem vagy annak közvetlen veszélye a jogi szabályozás hiányosságára vagy fölösleges, nem egyértelmű rendelkezésére vezethető vissza.[155]

Az új szabályozási környezet alapján nem egyértelmű, hogy a hatóság indíthat-e hivatalból olyan vizsgálatot (vagy bármilyen elnevezéssel illetett eljárást), amelynek eredményeként ajánlást bocsát ki. Az adatvédelmi biztos eddigi története során számos alkalommal indított hivatalból vizsgálatot egy-egy terület speciális adatvédelmi kérdéseit vizsgálva, melynek célja az volt, hogy az adott területen az adatkezelők orientálására átfogó ajánlás szülessen. Ez összességében nagyban hozzájárult ahhoz, hogy egy-egy területen következetes adatvédelmi gyakorlat alakulhasson ki. A 38. § (4) bekezdés c) pontja alapján a hatóság jogosult általános jelleggel vagy meghatározott adatkezelő részére ajánlást kibocsátani, de ennek részletei a vizsgálatról szóló szabályok között csak részben található meg. A vizsgálat keretében ugyanis kizárólag kérelemre indult eljárásban, és csak jogszabály módosítására irányuló, vagy a vizsgált adatkezelő felettes szerve számára bocsátható ki ajánlás, de kifejezetten az adatkezelő számára nem! A jogszabály módosítására irányuló ajánlásban természetesen számos általános jellegű megfontolást is tehet a hatóság, de a vizsgálat szabályozása alapján erre is csak kérelemre kerülhet sor. Ráadásul az említett – általános jellegű, szektorokat átfogó, sokszor tudományos igényű – ajánlások kiadására a két hónapos határidő biztosan nem elegendő.

Véleményünk szerint a helyes értelmezés az, ha a 38. § (4) bekezdés c) pontja alapján – különösen, mivel e szakasz a jelenlegi egyik legfontosabb hatáskör szó szerinti átvétele – a hatóság is rendelkezik majd azzal az ombudsmani jellegű hatáskörrel, hogy hivatalból indított eljárásban átfogó ajánlást bocsáthasson ki.

Akár a vizsgálat eredményeként, akár vizsgálati eljárás nélkül is a hatóság adatvédelmi hatósági eljárást indít, ha valószínűsíthető a személyes adatok jogellenes kezelése, és a jogellenes adatkezelés

- személyek széles körét érinti,
- különleges adatokat érint, vagy
- nagy érdeksérelmet vagy kárveszélyt idézhet elő.[156]

[153] A felügyeleti szerv számára a jogsérelemre való közvetlen felhívás nélkül is tehet ajánlást.
[154] Új Avtv. 56, 58. §§
[155] Új Avtv. 57. §
[156] Új Avtv. 60. § (4)

A hatóság e feltételek fennállása nélkül is indíthat hatósági eljárást, ha a személyes adatok védelméhez fűződő jog érvényesítése érdekében.[157]

A hatósági eljárásra a Ket. szabályait az új Avtv-ben meghatározott eltérésekkel kell alkalmazni; az ügyintézési határidő két hónap. Az eljárás kizárólag hivatalból indítható, az akkor sem minősül kérelemre indult eljárásnak, ha bejelentésen alapuló vizsgálat előzte meg.[158]

Az adatvédelmi hatósági eljárásban szankciórendszere részben átveszi a jelenlegi – nagyrészt az EU adatvédelmi irányelvén alapuló – jogkövetkezményeket, kiegészítve a bírságolás lehetőségével. A hatóság határozatban

- elrendelheti a valóságnak nem megfelelő személyes adat helyesbítését,
- elrendelheti a jogellenesen kezelt személyes adatok zárolását, törlését vagy megsemmisítését,
- megtilthatja a személyes adatok jogellenes kezelését vagy feldolgozását,
- megtilthatja a személyes adatok külföldre továbbítását,
- elrendelheti az érintett tájékoztatását, ha azt az adatkezelő jogellenesen tagadta meg,
- 100.000 Ft-tól 10.000.000 Ft-ig terjedő bírságot szabhat ki,[159]
- valamint a hatóság elrendelheti a határozat – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt az adatvédelem érdekeinek, illetve nagyobb számú érintett jogainak védelme ezt megköveteli.[160]

A bírság összegével kapcsolatban megjegyezzük, hogy a kiszabható legnagyobb összeg európai összehasonlításban és egyes adatkezelőkkel: például multinacionális cégekkel szembeni visszatartó erőt figyelembe véve is meglehetősen alacsony. Ennek indokáról az törvény indokolása hallgat; vélhetően a bírságolási lehetőség újdonságára tekintettel állapított meg a jogalkotó viszonylag alacsony összegeket.

A hatóság másik nevesített hatósági jellegű, Ket. szabályai szerint lefolytatott eljárása a titokfelügyeleti hatósági eljárás, amely akkor indítható, ha a bejelentésen alapuló vizsgálat alapján vagy egyébként valószínűsíthető, hogy a nemzeti minősített adat minősítése jogellenes. Ezen eljárást szintén minden esetben hivatalból indítja meg a hatóság, akkor is, ha az eljárást vizsgálat előzte meg.[161]

Az eljárás eredményeként a hatóság a minősítésére vonatkozó jogszabályok megsértésének megállapítása esetén a minősítőt a minősítés szintjének, illetve érvényességi idejének a megváltoztatására, vagy a minősítés megszüntetésére hívhatja fel. A minősítő a határozat bírósági felülvizsgálatát hatvan napon belül kérheti. A bíróság eljárására a közigazgatási

[157] Új Avtv. 60. § (1)
[158] Ekkor azonban a bejelentőt az adatvédelmi hatósági eljárás megindításáról, illetve befejezéséről értesíteni kell. Ld. új Avtv. 60. § (1)-(3), (5)
[159] A hatóság a bírság kiszabása során figyelembe veszi a jogsértéssel érintettek körének nagyságát, a jogsértés súlyát és a jogsértés ismétlődő jellegét. Új Avtv. 61. § (4)
[160] Új Avtv. 61. § (1)-(3)
[161] Új Avtv. 62. §

perekre vonatkozó rendelkezéseke kell alkalmazni azzal, hogy a bíróság az ügyben zárt tárgyaláson, soron kívül jár el.[162]

Végül meg kell említeni, hogy a hatóság pert indíthat az adatkezelővel szemben a közérdekű adatokkal és a közérdekből nyilvános adatokkal kapcsolatos jogsértés miatt. A per során alkalmazandó különös eljárási szabályok közül kiemelendő a bizonyítási teher megfordulása: azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani.[163]

A fent részletezett eljárások mellett a hatóság

- javaslatot tehet az adatvédelmet és információszabadságot érintő jogszabályok megalkotására, illetve módosítására, valamint véleményezi a feladatkörét érintő jogszabályok tervezetét,
- általános jelleggel vagy meghatározott adatkezelő részére ajánlást bocsát ki;
- véleményezi a közfeladatot ellátó szerv tevékenységével kapcsolatosan az e törvény szerint közzéteendő adatokra vonatkozó különös, illetve egyedi közzétételi listákat;
- megszervezi a belső adatvédelmi felelősök konferenciáját;
- adatvédelmi nyilvántartást vezet,
- meghatározza az adatvédelmi auditálás szakmai szempontjait;
- az adatkezelő kérelmére adatvédelmi auditot folytathat le.
- tevékenységéről minden év március 31-ig beszámol az Országgyűlésnek.[164]

3.2. Munkajogi szankciók

A munkajogi felelősséggel kapcsolatban először tisztázandó, hogy a kár a munkaviszony létrejötte előtt – a felvételi, kiválasztási eljárásban – vagy azután következett be. A Munka Törvénykönyve tartalmaz speciális kárfelelősségi szabályokat, amelyek kifejezetten a munkaviszony keretében okozott károkra vonatkoznak. A munkaviszony létrejöttét megelőző károkozás az általános polgári jogi, illetve az adatkezeléssel összefüggésben az általános adatvédelmi[165] szabályok szerint érékelendő.[166]

A munkaviszony fennállta alatt bármely fél által okozott károkra, ide érve a munkáltat által az adatkezelési szabályok megsértése miatt okozott kárt is, a munkajogi felelősségi szabályok alkalmazandók.

Az új Mt. szerint a munkáltató köteles megtéríteni a munkavállalónak a munkaviszonnyal összefüggésben okozott kárt. Mentesül a felelősség alól, ha bizonyítja, hogy a kárt az ellenőrzési körén kívül eső olyan körülmény okozta, amellyel nem kellett számolnia és nem

[162] Új Avtv. 63. § (1)-(3)
[163] Új Avtv. 64. § (3)
[164] Új Avtv. 38. § (3)-(4)
[165] Arany Tóth, 2004a
[166] Kiss, 2005, p. 285.

volt elvárható, hogy a károkozó körülmény bekövetkezését elkerülje vagy a kárt elhárítsa, vagy akkor, ha a kárt kizárólag a károsult elháríthatatlan magatartása okozta.[167]

A hatályos munkajogi és az adatvédelmi szabályozás – szemben az Mt. korábbi felelősségi szabályaival – összhangban van egymással, mindkettő a munkáltató, mint adatkezelő fokozott felelősségéből indul ki.

3.3. Egyéb szankciók

3.3.1. Polgári jogi jogkövetkezmények

A Ptk. A személyek polgári jogi védelme cím alatt, A személyhez fűződő jogok című alfejezetben rendelkezik a személyiség polgári jogi védelmének feltételeiről és eszközeiről.[168] Ahogy erről korábban szó volt, a magánszféra védelme a személyhez fűződő jogok körében több rendelkezésnek is tárgya.

A személyiségvédelem polgári jogi eszközei elsősorban az elszenvedett sérelem kiküszöbölését, helyreállítását szolgálják. A személyhez fűződő jogok megsértésének egyes polgári jogi jogkövetkezményei attól függetlenül igénybe vehetők, hogy a jogsértő felróható – azaz jellemzően vétkes vagy rosszhiszemű – magatartást tanúsított-e. Ilyen objektív szankció

- a jogsértés megtörténtének bírósági megállapítása;
- folyamatos vagy ismétlődő jogsértés esetén a jogsértés abbahagyására kötelezés és a további jogsértéstől való eltiltás;
- elégtétel adása nyilatkozattal vagy más megfelelő módon, szükség esetén a jogsértő részéről vagy költségén az elégtételnek megfelelő – azaz a jogsértéssel azonos mértékű – nyilvánosság biztosításával (erkölcsi jóvátétel);
- a sérelmes helyzet megszüntetése, a jogsértést megelőző állapot helyreállítása a jogsértő részéről vagy költségén, továbbá a jogsértéssel előállott dolog megsemmisítése, illetőleg jogsértő mivoltától megfosztása.[169]

A polgári jogi jogkövetkezmények másik része felróhatósághoz kötött, azaz alkalmazásuknak akkor van helye, ha a jogsértő nem úgy járt el, ahogy az az adott helyzetben általában elvárható.[170] Felróható magatartással szemben kártérítés követelhető, illetve közérdekű bírság kiszabására kerülhet sor.[171]

3.3.2. Büntetőjogi jogkövetkezmények

A Btk. Visszaélés személyes adattal című tényállása egyes adatvédelmi követelmények súlyosabb megszegésével szemben büntetőjogi szankciók alkalmazását rendeli.[172] A bűncselekményt az követi el, aki a személyes adatok védelméről vagy kezeléséről szóló

[167] új Mt. 166. §
[168] Ptk. 75-85. §§
[169] Ptk. 84. § (1)
[170] Ptk. 339. § (1)
[171] Ptk. 84. § (1)-(2)
[172] Btk. 177/A.

törvényi rendelkezések megszegésével, jogtalan haszonszerzés céljából vagy jelentős érdeksérelmet okozva

- jogosulatlanul vagy a céltól eltérően személyes adatot kezel,
- az adatok biztonságát szolgáló intézkedést elmulasztja,

Az érintett tájékoztatására vonatkozó kötelezettség megszegése is bűncselekmény, ha az jelentős érdeksérelmet okoz (ebben az esetben tehát a jogtalan haszonszerzés nem tényállási elem).

A jelentős érdeksérelem tényállási feltételként történő megjelenése szűkre szabja a büntetőjogi eszközök alkalmazhatóságát. Súlyosabban büntetendő a különleges személyes adatokkal való visszaélés, valamint hivatalos személyként, közmegbízatás felhasználásával, vagy jogtalan haszonszerzés végett elkövetett bűncselekmény.

4. FORRÁSOK

4.1. Szakirodalmi források

Arany Tóth, Mariann (2004a): Munkáltatói felelősség a jogellenes adatkezelésért a munkaerő-felvételi eljárásban, Munkaügyi szemle, 1. szám

Arany Tóth, Mariann (2004b): Hozzájárulás a munkáltatói adatkezeléshez a munkajogviszonyban, Munkaügyi szemle, 11. szám

Arany Tóth, Mariann (2008a): A munkavállalók személyes adatainak védelme a magyar munkajogban, Bába és Társai, Budapest

Arany Tóth, Mariann (2008b): A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor, Infokommunikáció és Jog, 4. szám

Balogh, Zsolt György – Földes, Ádám – Jóri, András – Székely, Iván (2004): Adatvédelem és információszabadság, Fundamentum, 4. szám

Bankó, Zoltán – Berke, Gyula – Kiss, György (2004): Bevezetés a munkajogba, JUSTIS, Budapest

Betzel, Margaret (2005): Privacy Year in Review: Recent Changes in the Law of Biometrics, I/S: A Journal of Law and Policy for the Information Society, 2-3. szám

Drinóczi, Tímea (2004): Az információszabadság elhelyezkedése az alapjogi rendszerben, különös tekintettel a más alapjogokkal való kapcsolatára, Infokommunikáció és Jog, 5. szám

Fodor T., Gábor – Nacsa, Beáta – Neumann, László (2008): Egy és több munkáltatóra kiterjedő hatályú kollektív szerződések összehasonlító elemzése, Szociális és Munkaügyi Minisztérium, Budapest

Gálik, Mihály – Polyák, Gábor (2005): Médiaszabályozás, KJK-Kerszöv, Budapest

Hajdú, József (2005): A munkavállalók személyiségi jogainak védelme, Pólay Elemér Alapítvány, Szeged

Hartai, Győző (2003): Adatvédelem a munkahelyen, Munkaügyi szemle, 1. szám

Hegedűs, Bulcsú (2006a): A munkahelyi hagyományos és elektronikus levelezés ellenőrzése, Munkaügyi szemle, 1. szám

Hegedűs, Bulcsú (2006b): A munkahelyi számítógép és internet ellenőrzésével kapcsolatos gyakorlat, Munkaügyi szemle, 7-8. szám

Horváth, Linda – Gelányi, Anikó (2011): Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései, Infokommunikáció és Jog, 2. szám

Jain, Anil K. – Prabhakar, Salil – Ross, Arun (2004): An Introduction to Biometric Recognition, 14 IEEE Transactions On Circuits And Systems For Video Technology: Special Issue On Image-And Video-Based Biometrics, 4. szám, http://biometrics.cse.msu.edu/JainRossPrabhakarCSVT-vl5.pdf [27.04.2005].

Jóri, András (2005): Adatvédelmi kézikönyv, Osiris, Budapest

Jóri, András – Hegedűs, Bulcsú – Kerekes, Zsuzsa (eds.) (2010): Adatvédelem és információszabadság a gyakorlatban, Complex, Budapest

Kiss, György (2005): Munkajog, Osiris

Majtényi, László (2003): Az információs jogok. In: Halmai, Gábor – Tóth, Gábor Attila (Eds.): Emberi Jogok, Osiris, Budapest, pp. 577-637.

Majtényi, László (2006): Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága, Complex, Budapest

McGuire, Lisa Jane (2000) Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up You Privacy, Akron Law Review, 3. szám

Polefkó, Patrik (2010): Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (1. rész), Infokommunikáció és Jog, 3. szám

Polyák, Gábor – Szőke, Gergely (2011): Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései. In.: Drinóczi, Tímea (ed.): Magyarország új alkotmányossága, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs, pp. 155-178.

Sólyom, László (2001): Az ombudsman „alapjog értelmezése" és „normakontrollja", In.: Az odaátra nyíló ajtó, Adatvédelmi Biztos Irodája, Budapest

Székely, Iván – Szabó, Máté Dániel (eds.) (2005): A privacy védelme a munkahelyen, In.: Szabad adatok, védett adatok, BME GTK Információ és Tudásmenedzsment Tanszék

Szőke, Gergely László (2009): [Első oldal], Infokommunikáció és Jog, 6. szám

Szőke, Gergely László (2010): Privacy Protection (Book chapter). In.: Rátai, Balázs – Homoki, Péter – Polyák, Gábor – Schvéger, Judit – Szemes, Balázs – Szőke, Gergely László – Tasnádi, Sándor – Tóth, András: *Cyber Law in Hungary*, Kluwer Law International, The Netherlands

Szőke, Gergely László (2011): Közterületi kamerázás az Európai Unióban, JURA, 2. szám

4.2. Az adatvédelmi biztos esetei

ABI, 461/A/1998
http://abiweb.obh.hu/abi/index.php?menu=aktualis/archivum/ajanlasok&dok=9278
[10.05.2011.]

ABI, 693/K/1998
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1998/M/1/1&dok=693_K_1998
[10.05.2011.]

ABI, 917/K/1998
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1999/M/1/1&dok=917_K_1998
[10.05.2011.]

ABI, 475/H/2000
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/M/1/1&dok=475_H_2000 [10.05.2011.]

ABI, 772/A/2000
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/III/1/2/1&dok=beszamolok_2000_III_A2 [10.05.2011.]

ABI, 570/A/2001
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=570_A_2001 [10.05.2011.]

ABI, 127/K/2003
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/M/1&dok=127_K_2003 [10.05.2011.]

ABI, 1472/A/2003
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/II/1/2&dok=beszamolok_2003_IIA3 [10.05.2011.]

ABI, 120/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/2 [27.05.2011]

ABI, 531/A/2004
http://abiweb.obh.hu/abi/index.php?menu=munkaugy&dok=11861 [27.05.2011]

ABI, 750/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/6 [24.05.2011]

ABI, 1543/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/2 [27.05.2011]

ABI, 1598/K/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/6 [24.05.2011]

ABI 1722/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2005/M/4/1&dok=1722_A_2004 [27.05.2011]

ABI, 1012/K/2005
http://abiweb.obh.hu/abi/index.php?menu=munkaugy&dok=11866 [24.05.2011]

ABI, 40/K/2006
http://abiweb.obh.hu/abi/index.php?menu=munkaugy&dok=11871 [27.05.2011]

ABI, 559/A/2006
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=559_A_2006-3&nyomtat=1 [15.05.2011]

ABI, 866/A/2006
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=866_A_2006-3 [24.05.2011]

ABI, 920/K/2006
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=920_K_2006-2&nyomtat=1 [15.05.2011]

ABI, 1393/K/2006
http://abiweb.obh.hu/abi/index201.php?menu=munkaugy&dok=1393_K_2006-5 [24.05.2011]

ABI, 1664/A/2006
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2007&dok=1664_A_2006-8&nyomtat=1 [15.05.2011]

ABI, 1672/K/2006
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=1672_K_2006-3&nyomtat=1 [15.05.2011]

ABI, 1767/K/2006
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=1767_K_2006-3&nyomtat=1 [15.05.2011]

ABI, 2511/K/2007
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=2511_K_2007-3 [27.05.2011]

ABI, 800/K/2008
http://abiweb.obh.hu/abi/index.php?menu=internet1&dok=800_K_2008-3 [27.05.2011]

ABI, 415/K/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=415_K_2009-3&nyomtat=1 [15.05.2011]

ABI, 636/K/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=636/K/2009-3&nyomtat=1 [15.05.2011]

ABI, 663/P/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=663/P/2009-3&nyomtat=1 [15.05.2011]

ABI, 857/K/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=857/K/2009-3&nyomtat=1 [15.05.2011]

ABI, 1092/P/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=1092_P_2009-6&nyomtat=1 [15.05.2011]

ABI, 3362/P/2009 http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=3362/P/2009-3&nyomtat=1 [15.05.2011]

ABI, 922/2/2010
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2010&dok=ABI-922-2_2010_K&nyomtat=1 [15.05.2011]

ABI, 926/H/2010
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2011&dok=ABI-1642-9_2011_H [20.09.2011]

ABI, 1454/K/2010
http://abiweb.obh.hu/abi/beszamolok/2010/beszamolo_2010.pdf [15.05.2011]

4.3. Bírósági joggyakorlat

15/1991. (IV. 13.) ABH

35/2002. (VII.19.) ABH

BH2001.269

BH2006.64

Fővárosi Munkaügyi Bíróság, 5.M. 394/2007/12.;

Fővárosi Munkaügyi Bíróság, 31.M.3189/2002/55.;

Miskolci Munkaügyi Bíróság, 8.M.1286/2005/19.;

Nyíregyházi Munkaügyi Bíróság, 1.M.687/2005/12.

Pécsi Munkaügyi Bíróság, 3.M.1763/2005/15.;

Veszprémi Munkaügyi Bíróság, 2.M.341./2006./8.;

4.4. Egyéb felhasznált dokumentumok

ILO Code of Practice – Protection of workers' personal data, International Labour Office, Geneva, 1997

European Commission: Second stage consultation by social partners on the protection of workers' personal data, http://ec.europa.eu/social/BlobServlet?docId=2504&langId=en [12.03.2011.]

Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12th January 2011, http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf [10.09.2011.]