Tanulmányok

Balogh Zsolt György, Polyák Gábor, Rátai Balázs, Szőke Gergely László

Munkahelyi adatvédelem a gyakorlatban

A PTE ÁJK IKJK és a göttingeni Georg-August Egyetem jogi karának társtanszéke 2011–2012. év folyamán közös, az Európai Unió által finanszírozott[1] projekt keretében vizsgálja a munkahelyi adatvédelem sajátos kérdéseit, azon belül kiemelten a munkahelyi ellenőrzés és a magánszféra konfliktusait. A kutatás egyik sarokköveként készült országjelentés célja a munkahelyi adatvédelem hatályos magyar szabályozásának és a szabályozás európai kontextusának bemutatása (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 megkülönböztessük a munkavállalók jogszerű megfigyelését az illegális adatgyűjtéstől. Ez a munkahelyi adatvédelemnek Magyarországon és az Európai Unióban egyaránt meghatározó problémaköre.

1. A HATÁLYOS JOGSZABÁLYOK RÖVID ÁTTEKINTÉSE

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

1.1. Nemzetközi és közösségi jogi források

1.1.1. Az ILO kódexe

A Nemzetközi Munkaügyi Szervezet (International Labor Organization, 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.[3] Nyilvánosságra hozatalát és terjesztését az ILO vezető testülete 1996 novemberében hagyta jóvá.

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.

1.1.2. 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.

1.1.3. Az Európai Unió kezdeményezései

Mindenekelőtt meg kell említenünk az általános adatvédelmi irányelvet, a 95/46/EC irányelvet, amelyet minden tagállamnak implementálnia kellett. A jogharmonizáció eredményeként az adatvédelem alapvető elvei minden tagállamban azonosak. A távközlés területén a 2002/58/EC irányelv 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.[4] A szociális partnerek (munkavállalói és munkáltatói szervezetek) reakciói szintén az ILOC-ra hivatkoztak. Az EUROCADRES (Council of European Professional and Managerial Staff)[5] hangsúlyozta, hogy a közösségi jogi szabályozás nem tükrözheti kizárólag a munkavállalók érdekeit, hanem a munkáltatók, a munkavállalók és a munkavállalói képviseletek együttműködésén kell alapulniuk.[6] Az UEAPME (European Association of Craft, Small and Medium-sized Enterprises)[7] azt az álláspontot képviselte, hogy az ILOC alapján kidolgozott nem kötelező magatartási kódexek alkalmazása megfelelő megoldás lenne.[8]

1.2. Hazai 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-jén lépnek 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 (a továbbiakban: Avtv.) volt. Az Országgyűlés 2011. június 11-én új adatvédelmi törvényt[9] fogadott el, ami néhány területen lényeges válto-

Balogh Zsolt György egyetemi docens, a PTE ÁJK Informatikai és Kommunikációs Jogi Tanszékének és Kutatóintézetének vezetője. Polyák Gábor egyetemi docens, az Infokommunikáció és Jog főszerkesztője. Rátai Balázs tudományos munkatárs a PTE ÁJK Informatikai és Kommunikációs Jogi Kutatóintézetében. Szőke Gergely László tudományos munkatárs a PTE ÁJK Informatikai és Kommunikációs Jogi Kutatóintézetében.

zásokat hozott. Szintén releváns jogforrás a Munka Törvénykönyve[10]; 2012. július 1-én új Munka Törvénykönyve lép hatályba[11].

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 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.

A munkahelyi adatvédelem területén a legnagyobb nehézséget ugyanakkor éppen a hiányos, sőt hiányzó ágazati szabályozás jelenti, vagy legalábbis jelentette.

2012. július 1-jétől 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.

1.3. Önszabályozás

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.[12]

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 Mt.-ben rögzített szabályoktól csak annyiban térhet el, amennyiben a munkavállalóra kedvezőbb feltételt állapít meg [Mt. 13. § (3) bek.]. 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. Lásd pl.:

1. A Mol Nyrt. kollektív szerződése (22.2. pont alatt) a munkavállaló általi rendkívüli felmondás okai között felsorolja azt az esetet, amikor a munkáltató megsérti a munkavállaló személyiségi jogait. 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) bek. b) pontja]

A kollektív szerződések utolsó, országos, átfogó elemzése 2008-ban készült a Szociális és Munkaügyi Minisztérium megrendelésére.[13] 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.

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. 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.

2. AZ ADATKEZELÉS JOGALAPJA

A munkahelyi adatvédelem, illetve ellenőrzés szabályozásának kulcskérdése, hogy a munkáltató, mint adatkezelő honnan nyeri az adatkezelési felhatalmazást. A munkavállalók, mint érintettek számára a jogalap egyértelmű meghatározása az információs önrendelkezési jog minimum-garanciája. Ennek ellenére sem a jogalkotás, sem a jogalkalmazás nem tudott eddig megnyugtató választ adni e kérdésre.

2.1.1.1. 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.[14]

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.[15] 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."[16]

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 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.[17] 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 [10. § (1) bek.]. 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.

2.1.1.2. 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.

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".[18] 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,[19] az azonban így is kétséges, hogy a hazai adatvédelmi szabályozás kiállná-e a közösségi jog próbáját.[20]

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,[21] 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 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[22] – a jogalkotó nem határozta meg kellő pontossággal.[23]

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.[24] 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 szin-

te 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.

2.1.1.3. 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,[25] 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 nyilvánvaló munkavégzésre. (Abszurdan széles jogértelmezéssel azt is mondhatjuk, hogy a munkás által jól-rosszul elkészített munkadarab is az ő személyes adata.)"[26]

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.[27] 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.

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.

3. A KUTATÁSI TERÜLET MEGHATÁROZÁSA – A MUNKAHELYI ADATVÉDELEM ALAPJAI

3.1. 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.[28]

3.2. 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.

A régi Mt. kifejezetten nem rendelkezik az ellenőrzési jogról, de a szakirodalom általánosan hivatkozik a munkáltató felügyeleti/ellenőrzési jogosultságára.[29] 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".[30] 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.[31] Kiss György szerint a munka feletti felügyelet jogkör a konkretizálási jogtól (az utasítás adás jogától) nem választható el.[32] Az utasításra vonatkozóan az Mt. kimondja: a munkavállaló a munkát a munkáltató utasítása szerint köteles ellátni.[33] Emellett a munkáltató jogosult ellenőrizni az általa rendelkezésre bocsátott eszközök használatát is.

A szakirodalom általánosan hivatkozik a munkáltató felügyeleti/ellenőrzési jogosultságára. A felügyeletre vonatkozó szabály szükségszerűen feltételezi személyes adatok kezelését, így akár törvényi felhatalmazás is lehet.

3.3. Az ellenőrzés határai

3.3.1. 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.

3.3.2. Adatvédelmi előírások a Munka Törvénykönyvében 2012. július 1-je előtt

Az 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.[34] 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.

3.3.3. Adatvédelmi előírások a Munka Törvénykönyvében 2012. július 1-je után

Az új Munka Törvénykönyve a munkahelyi adatvédelem területén érzékelhető változást jelent. Kifejezetten rendelkezik a munkáltató által gyakorolható ellenőrzés feltételeiről (11. §). 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.

Az új Munka Törvénykönyve a munkahelyi adatvédelem területén érzékelhető változást jelent. Kifejezetten rendelkezik a munkáltató által gyakorolható ellenőrzés feltételeiről, és van adatvédelmi relevanciája a munkavállaló személyhez fűződő jogai tiszteletben tartására irányuló kötelezettségnek.

Szintén van adatvédelmi relevanciája a munkavállaló személyhez fűződő jogai tiszteletben tartására irányuló kötelezettségnek (9–10. §). 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 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.

3.4. Kölcsönös függőség

3.4.1. 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.[35]

3.4.2. 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 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.«[36]

4. 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.

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 fel-

hatalmazott 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.

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 esetében 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.

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.

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.[37]

5. AZ ELEKTRONIKUS LEVELEZÉS ELLENŐRZÉSÉNEK SZABÁLYOZÁSA

Az e-mail-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 e-mail magáncélú használatának feltételei általában nagymértékben tisztázatlanok.

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

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 e-mail megírásával egyúttal adatkezelési hozzájárulást is ad.[38]

Ezt a megkülönböztetést a későbbi állásfoglalások is megismétlik, és újból hangsúlyozzák a hozzájárulás kérdését: ha a munkavállaló tájékoztatást kapott a munkáltató által gyakorolt ellenőrzés lehetőségéről, az e-mail megismeréséhez való hozzájárulás már az e-mail megírásával megadottnak tekintendő.[39]

Egy 2006-os állásfoglalás szerint a munkáltató betekinthet a hivatali e-mailekbe, 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.[40]

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.[41] 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 e-mail 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.[42]

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.

A tudományos publikációk mindenekelőtt rögzíti, hogy az e-mailekre is kiterjed a levéltitok védelme, és az adatvédelmi követelmények minden olyan esetben irányadók, amikor az e-mail címzése vagy tartalma egy meghatározott természetes személyhez köthetők – az esetek többségében ez a feltétel teljesül.[43]

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.[44] 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.[45] 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 e-mail tartalmát csak akkor ismerheti meg, ha az üzenet egy hivatali e-mail-címre érkezett, és az ellenőrzés minden érintett hozzájárulásával történik; a munkavállaló hozzájárulása megadottnak tekintendő, ha tud az ellenőrzés lehetőségéről.[46]

A tudományos publikációk aszerint is különbséget tesznek, hogy az emailt a munkavállaló vagy külső harmadik személy írta.[47] A különbségtétel az adatvédelmi biztos gyakorlatán alapul, amivel néhány szerző egyetért[48], mások pedig nem: Arany Tóth szerint az emaileket az érintettek státuszától függetlenül azonos vagy nagyon hasonló védelemnek kell megilletnie.[49] 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[50] adatvédelmi rendelkezéseit is figyelembe kell venni.[51] Azzal ugyan egyetértünk, hogy a hírközlési adatvédelmi előírások figyelembe vétele hasznos, azt azonban rögzítenünk kell, hogy a munkáltató nem minősül elektronikus hírközlési szolgáltatónak, akkor sem, ha sajátos hozzáférés-, email- és hostszolgáltatóként 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.

6. 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.

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.[52] 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.[53]

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.

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.[54] Az ellenőrzés ahhoz nem biztosít jogalapot, hogy a munkáltató a számítógépen tárolt bármilyen magánjellegű dokumentumot megismerjen.[55]

Tilos a munkavállaló tudta nélkül telepített kémprogramokkal figyelni a számítógép használatát. Az adatvédelmi biztos 2005. évi állásfoglalása szerint ez olyan titkos információgyűjtésnek minősül, ami alapvetően csak bírói engedéllyel végezhető.[56] Az adatvédelmi biztos állásfoglalásában kimondta, hogy a munkavállalók számítógép használatának, internetfelhasználásának, 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 egy 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 végzett 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 az Alkotmánybíróság által megfogalmazott azon követelmény, miszerint az érintett személy adatai kezelését jogosult átlátni, az azzal kapcsolatos jogait pedig jogosult érvényesíteni.[57]

7. 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.[58]

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.[59]

A biztos azt is hangsúlyozza, hogy az internet-használat ellenőrzésére a munkavállaló hozzájárulása alapján kerülhet sor, amely hozzájárulás megfelelő tájékoztatáson alapul.[60] Későbbi döntéseiben a biztos e feltételeket megerősítette.[61] 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.[62]

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.[63]

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.[64] 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.[65]

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.[66]

Ha a munkavállaló számára megengedett a magáncélú internet-használat, akkor a munkáltató nem ellenőrizheti a meglátogatott oldalakat.[67] 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.[68]

A kamerák használata a személyes adatok nagymennyiségű kezelést generálja. Ez igaz a munkavállalók személyiségprofiljának létrehozására is.

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[69], mi azonban továbbra is úgy gondoljuk, hogy a munkáltató nem alanya e szabályozásnak.[70]

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.[71] Valóban rendelkezésre állnak ugyan ilyen privacy-barát megoldások, valószínűleg azonban gyakorlati alkalmazásuk nehézkes és nem is jellemző.

8. A TELEFONHASZNÁLAT ELLENŐRZÉSE

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

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. A telefonhasználat minden esetben magában foglalja a személyes adatok kezelését, így az általános adatvédelmi szabályok szintén alkalmazandók. A telefonhasználathoz kapcsolódó adatkezelés az adatvédelmi biztos gyakorlatában visszatérő probléma.

Az adatvédelmi biztos gyakorlata a következőkben foglalható össze:

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.

Ugyanezen szabályok irányadók arra az esetre, ha a személyi jövedelemadóra vonatkozó előírások különbséget tesznek a hivatali és a magáncélú telefonhasználat adóztatásában.

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.

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.

9. 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.

A kamerás megfigyelésre vonatkozóan nincs külön munkajogi szabályozás.[72] 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.

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 kell terjednie, hogy a felvételeket rögzítik- és tárolják-e. A munkavállalónak joga van a róla készült felvételeket megnézni és ellenőrizni. *(461/A/1998)*

A megfigyelés és a videofelvétel akkor jogszerű, ha a munkavállaló megfelelően tájékozott, és az adatkezeléshez hozzájárulását adta *(475/H/2000)*. A rejtett kamerák használata ezért a munkavállalók magánéletének súlyos megsértését jelenti.[73]

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 feltételeiről. A kapcsolódó esetek mindegyikében bizonyítékként használták a felek a felvételeket, és a bizonyíték jogszerűségét sem a felek, sem a bíróság nem vitatta.

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."*

10. AZ RFID HASZNÁLATÁNAK SZABÁLYOZÁSA

A rádiófrekvenciás azonosítás (radio-frequency identification, 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 tudatában 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. [74] 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.

11. 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

A biometrikus azonosító egy olyan mintafelismerő rsz, 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 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.

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.

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 *(ABI-1454/ 2010/K)*. 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 *(ABI-926/2010/H)*.

12. 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.

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.

A munkavállalók GPS vagy GSM technológia segítségével történő nyomon követése az adatvédelmi biztos gyakorlatában visszatérő probléma. A biztos gyakorlata a következő megállapításokkal foglalható össze:

A természetes személy földrajzi pozíciója személyes adat. A jármű pozíciója a járművet használó személy személyes adata. Ha a munkáltató helymeghatározó eszközt telepít a munkavállaló által használt járműbe vagy mobiltelefonba, akkor adatkezelővé válik. 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. Kizárólag az érintett hozzájárulása lehet az adatkezelés jogalapja.

A természetes személy földrajzi pozíciója személyes adat. A jármű pozíciója a járművet használó személy személyes adata.

Kizárólag azok a munkavállalók ellenőrizhetők helymeghatározó eszközökkel, akiknek a munkája ezt szükségessé teszi, és a megfelelő munkavégzés ellenőrzése más módon nem megoldható. 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.

Jegyzetek

1 A projekt az Európai Unió „Fundamental Rights and Citizenship" programjának társfinanszírozásával valósul meg. További információ: www.pawproject.eu

2 An ILO code of practice – Protection of workers' personal data, International Labour Office, Geneva, 1997, (a továbbiakban: ILOC, kódex)

3 A továbbiakban: ILOCCom

4 Second stage consultation of social partners on the protection of workers' personal data, p. 6,

5 www.eurocadres.org

6 Second stage consultation of social partners on the protection of workers' personal data, p. 20

7 www.ueapme.com

8 Second stage consultation of social partners on the protection of workers' personal data, p. 3

9 2011. évi CXII. törvény az információs önrendelkezésről és az információszabadságról (Új Avtv.)

10 1992. évi XXII. törvény a Munka Törvénykönyvéről (Mt.)

11 2012. évi I. törvény a Munka Törvénykönyvéről (Új Mt.)

12 Lásd Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, Bába Kiadó, Szeged 2008. pp 307–308.

13 Fodor T. Gábor – Nacsa Beáta – Neumann László: Egy és több munkáltatóra kiterjedő hatályú kollektív szerződések összehasonlító elemzése, Budapest, 2008.

14 Avtv. 3. § (6), (7)
15 Ez általános vélekedés a szakirodalomban, lásd Arany Tóth Mariann: Munkáltatói felelősség a jogellenes adatkezelésért a munkaerő-felvételi eljárásban, Munkaügyi Szemle, 2004/1. pp 15–17., Majtényi, László: Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága, Complex, Budapest, 2006, p. 332., Hartai Győző: Adatvédelem a munkahelyen, Munkaügyi szemle, 2003/1, p. 46.
16 Majtényi: i. m. p. 333.
17 Jóri András: Adatvédelmi kézikönyv, Osiris, Budapest, 2005, pp. 187–188.
18 Jóri András: i. m. p. 163.
19 Case C-101/01 (Lindqvist). Az ügyről ld. Jóri András: im.; Majtényi László: i. m. pp. 89–90.
20 Jóri szerint az Avtv. eltérései nem okoznak a közösségi joggal való összeütközést (lásd Jóri András: i. m. p. 32.). Álláspontunk szerint ez egyáltalán nem egyértelmű.
21 A jogértelmezés nehézségeiről ld. Majtényi László: i. m. p. 336.; Szőke Gergely László: [Első oldal], Infokommunikáció és Jog, 2009. december
22 Avtv. 3. § (3); új Avtv. 5. § (3); részletesen lásd később.
23 Erről ld. Jóri András: i. m. pp 164–165.
24 Új Avtv. 6. § (1) és (5) bek.
25 Arany Tóth Mariann: Hozzájárulás a munkáltatói adatkezeléshez a munkajogviszonyban, Munkaügyi Szemle, 2004/11. pp 18–19.
26 Majtényi László: i. m. p. 336.
27 Jóri András: i. m. pp. 164–165.
28 Ez alól egy lényeges kivétel van, amit a levelezés ellenőrzésénél ismertetünk.
29 Kiss György: Munkajog, Osiris, 2005, p. 180., Bankó Zoltán–Berke Gyula–Kiss György: Bevezetés a munkajogba, JUSTIS, Budapest, 2004, p. 89., Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, Bába és Társai, Budapest, 2008, p. 235.
30 Bankó Zoltán–Berke Gyula–Kiss György: i. m. pp. 89–90.
31 Mt. 102. § (2) bek. b) pont.
32 Kiss György: i. m. p. 180.
33 Mt. 104. § (1) bek.
34 Mt. 192/G. § (3) és (6) bek.
35 Ez általános vélekedés a szakirodalomban, ld. Arany Tóth Mariann: i. m. pp. 15–17., Majtényi László: i. m. p. 332., Hartai Győző: i. m. p. 46.
36 Majtényi László: i. m. p. 333.
37 120/A/2004.
38 120/A/2004, 1543/A/2004
39 1722/A/2004
40 1393/K/2006
41 40/K/2006
42 40/K/2006.
43 Gálik Mihály–Polyák Gábor: Médiaszabályozás, KJK-KERSZÖV, Budapest, 2005, p. 212.; Arany Tóth Mariann: A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor, Infokommunikáció és Jog 2008/4; Hegedűs Bulcsú: A munkahelyi hagyományos és elektronikus levelezés ellenőrzése, Munkaügyi szemle 2006/1. p. 47.
44 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, p. 268., Hegedűs Bulcsú: i. m. p. 48.
45 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, p. 271., Hegedűs Bulcsú: i. m. pp. 48–49., Majtényi László: i. m. pp. 345–346.
46 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, pp. 269-270, Hegedűs Bulcsú: i. m. pp. 48–49.
47 Más szóval munkahelyen belüli kommunikációról van-e szó, vagy a munkahely és harmadik fél közötti kommunikációról.
48 Hegedűs Bulcsú: i. m. p. 48
49 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, p. 270
50 Az elektronikus hírközlésről szóló 2003. évi C. törvény.
51 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, pp. 272–273.
52 866/A/2006-3.
53 772/A/2000, 841/K/2002.
54 866/A/2006-3.
55 531/A/2004.
56 1012/K/2005.
57 2511/K/2007.
58 Horváth, Linda–Gelányi, Anikó: Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései, Infokommunikáció és Jog 2011/2.
A közösségi hálózatok általános adatvédelmi kérdéseit a magyar szakirodalom is tárgyalja (ld. Polefkó, Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből, Infokommunikáció és Jog 2010/3.) de a munkahelyi adatvédelem kérdései egyelőre nem jelentek meg.
59 693/K/1998, 750/A/2004, 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.
60 531/A/2004
61 800/K/2008
62 1767/K/2006
63 570/A/2001
64 BH 2006/64.
65 A munkavállaló beismerte az erotikus oldala látogatását – a bíróságnak ezért nem kellet az adatgyűjtés körülményeivel foglalkoznia.
66 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor, pp. 170–171.
67 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor, p. 172.
68 Hegedűs Bulcsú: i. m. 82–83.
69 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor, p. 173.
70 Lásd az elektronikus levelezésről szóló fejezetben.
71 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor p. 173, Hegedűs Bulcsú: A munkahelyi számítógép és internet ellenőrzésével kapcsolatos gyakorlat, Munkaügyi Szemle 2006/7–8. pp. 82–83., Jóri, András–Hegedűs, Bulcsú–Kerekes, Zsuzsa (szerk.): Adatvédelem és információszabadság a gyakorlatban, Complex, Budapest, 2010, p. 288.
72 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, p. 277.
73 Arany Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban, p. 289.
74 Privacy and Data Protection Impact Assessment Framework for RFID Applications, 2011, p. 3.