ÁSVÁNYI ZSÓFIA

ADATVÉDELEM A FOGLALKOZTATÁSBAN – MIT MUTAT AZ ESETJOG?

DATA PROTECTION IN EMPLOYMENT – WHAT DOES CASE LAW SHOW?

A digitalizáció és a globalizáció összefonódása következtében soha nem látott mértékben került összeütközésbe egymással a munkáltató információhoz való joga és a munkavállaló magánélethez fűződő joga. Ezzel egyidőben olyan mennyiségű és jelentőségű új jogforrás, állásfoglalás és hatósági határozat született Európában és Magyarországon, amelyeket érdemes alaposabban górcső alá venni. A tanulmány fő célja megvizsgálni az Európai Unió Bírósága, az Emberi Jogok Európai Bírósága, valamint a magyar Kúria és a Nemzeti Adatvédelmi és Információszabadság Hatóság foglalkoztatást érintő esetjogát a szervezetek toborzás- és kiválasztási gyakorlata, valamint a munkavállalók munkaviszonnyal kapcsolatos ellenőrzése kapcsán. A tanulmány a dokumentumelemzés módszerével döntéseket elemez azért, hogy segítse az iránymutatást az állásra jelentkezők, illetve a munkavállalók magánszférájához fűződő joga és a munkáltató információhoz való joga között húzódó határvonal pontosabb megismeréséhez.

Kulcsszavak: **adatvédelem, munkaviszony, HRM, toborzás és kiválasztás, munkavállalók munkaviszonnyal kapcsolatos ellenőrzése**

The interlocking of digitalisation and globalization has led to an unprecedented conflict between the employer's right to information and the employee's right to privacy. Also, recent years have created a great number of significant new sources of legislation, case law decisions and official decisions both in Europe and in Hungary that deserve closer examination. The main aim of the study is to examine the employment case law of the Court of Justice of the European Union and the European Court of Human Rights, as well as the Hungarian Curia and the National Data Protection and Freedom of Information Authority, related to the recruitment and selection practices of organizations and the control of employees. The study is using the document analysis method to provide guidance regarding the demarcation line between jobseekers' and employees' right to privacy and the employers' right to information.

Keywords: **data protection, employment relationship, HRM, recruitment & selection, controlling employees**

Finanszírozás/Funding:
A szerző a tanulmány elkészítésével összefüggésben nem részesült pályázati vagy intézményi támogatásban.
The author did not receive any grant or institutional support in relation with the preparation of the study.

Szerző/Author:
Dr. Ásványi Zsófia, egyetemi adjunktus, Pécsi Tudományegyetem, (asvanyizs@ktk.pte.hu)

A cikk beérkezett: 2020. 07. 22-én, javítva: 2020. 09. 28-án, elfogadva: 2020. 11. 03-án.
This article was received: 22. 07. 2020, revised: 28. 09. 2020, accepted: 03. 11. 2020.

A digitalizáció behálózza életünk valamennyi színterét. Ahelyett, hogy a memória természetes szelekciós folyamata okán felejtenénk, és „elfelejtődnénk", a technikának köszönhetően digitális nyomaink sokszor akaratunktól függetlenül is megmaradnak. A „felejtés joga" („*right to be forgotten*") és a magánélet tiszteletben tartásához való jog („*right to privacy*") folyamatosan ütközésben van az információhoz való joggal. Mindez különösen igaz a foglalkoztatási kontextusra, amelyet természetéből fakadóan erőteljes alá- és fölérendeltség jellemez (Bankó, 2015), azaz a jogszabályi keretek megtartása mellett a munkáltatónak döntő befolyása van a munkajogviszony tartalmának alakítására. A „munkáltatói hatalom" természetéből fakadóan a munkáltató információhoz való jogának eszközei is szofisztikáltabbak és számosabbak annál, amivel a munkavállaló ténylegesen rendelkezik.

A munkaviszony természetét még összetettebbé teszi a tény, hogy ez egy pszichológiai töltetű jogviszony (Kiss, 2020), amelyben a szervezetek elkötelezett munkavállalókat keresnek. Az elkötelezettség munkavállalói motivációra gyakorolt pozitív hatásait ismerjük (Farkas et al., 2013, p. 16), ami könnyen elillan, ha a munkáltató az információhoz való jogának gyakorlása során érinti a munkavállaló magánéletét. A munka és a magánélet éles határvonalának ilyen módon történő megszüntetése a kiszolgáltatott helyzet felismeréséhez, végső soron a jogviszony pszichológiai vetületének sérüléséhez vezethet.

Bár egyedi szervezeti döntésekkel részben orvosolható a fenti probléma (Jarjabka & Lóránd, 2010), a munkavállalók személyes adatainak és magánéletük védelme vonatkozásában a jogalkotó nem hagyta magukra a munkáltatókat: európai szinten született meg az új generációs adatvédelmi szabályozás, amelynek időszámítása az Európai Unió tagállamaiban ténylegesen 2018. május 25-én kezdődött, az általános adatvédelmi rendelet (angol rövidítéssel: GDPR, továbbiakban: Rendelet) megjelenésével. A Rendelet jogi természetéből fakadóan tagállami átültetés nélkül, egységesen alkalmazandó a tagállami jogokban úgy a foglalkoztatásban, mint az élet valamennyi területén. A kötelező jogi norma különlegességét annak 88. cikke adja, amely lehetőséget teremt a tökéletes tagállami illesztésre, amellyel valamennyi tagállam, így Magyarország is élt. Előzetesen megállapítható, hogy a Rendelet, annak magyar specifikációiként is értelmezhető további magyar jogforrások (lásd részletesebben később), valamint a hozzájuk köthető mértékadó jogalkalmazási gyakorlatok együttesen szolgálják a természetes személyek, így a munkavállalók alapvető jogait és szabadságait és ezen belül különösen a személyes adataik és a magánélethez fűződő jogaik védelmét a munkahelyen.

A kutatás jellege, indokoltsága és módszerei

A tanulmány multidiszciplináris megközelítést alkalmaz. Bár a cím jogtudományi megközelítést vetít előre, a tanulmány kifejezetten a menedzsment, azon belül is az emberierőforrás-menedzsment, a munkajog és az adatvédelmi jog metszetét mutatja be.

A jogtudományon belül az infokommunikációs és az adatvédelmi jog igen nagy terjedelemben vizsgálja nemzetközi és magyar adatvédelem horizontális, valamennyi jogágra kiterjedő szabályozási kérdéseit. A munkajog ehhez képest specifikusan a foglalkoztatási jogviszonyokban (ágazati jogszabályként) végzi el a digitális világ és a magánszféra elhatárolását, ám annak elsősorban az európai uniós szabályoknak való megfelelését és a jogalkalmazás kérdéseit szem előtt tartva. Az emberierőforrás-menedzsment nemzetközi és hazai tudományos szakirodalma a digitalizációhoz kapcsolódóan elsősorban a mesterséges intelligencia foglalkoztatásreleváns területeit, a rugalmas foglalkoztatási formákat és a szervezeti Big Data stratégiák menedzsmentmegfontolásait elemzik.

Megállapítható, hogy a munkavállalók személyes adatainak védelme és a magánélethez való jog kizárólag a munkajog területe, ahonnan viszont hiányoznak a szervezeti HR-menedzsment aspektusai. Jelen tanulmány ezt a hiátust igyekszik betölteni azzal, hogy a jogesetekből levonható tanulságok alapján a HR-szakma tudományos és gyakorló képviselőinek is hasznosítható megoldásokat kínál.

Szem előtt tartva a folyóirat szakmai irányultságát, vizsgálatom általános célja feltárni az európai és magyar jogalkalmazás látókörébe került foglalkoztatással kapcsolatos adatvédelemi eseteket. Kutatási kérdéseim e célkitűzés mentén a következők. Tágabb értelemben: Milyen jogalkotási és jogalkalmazási keretrendszerben születnek európai szinten és Magyarország vonatkozásában a munkaviszonyt érintő adatvédelmi döntések? Szűkebb értelemben: Melyek az Európai Unió, az Európai Tanács, valamint a Kúria és a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) adatvédelmi döntései és iránymutatásai az állásba jutás (toborzás és kiválasztás) és a munkavállaló munkavégzés közben történő ellenőrzése kapcsán?

Nem képezik vizsgálatom tárgyát a munkahelyi adatvédelem további lehetséges területei, úgy mint távmunka, otthoni munkavégzés, munkavállalók biometrikus adatainak felhasználása, elektronikus dokumentumok kérdése, vagy a platform munkavégzés, amelyek egyben további kutatások témáim irányát is kijelölik.

A fenti kérdések megválaszolásához a dokumentumelemzés módszerét választottam. A vizsgált szervezetek hivatalos honlapján nyilvánosan elérhető keresőfunkcióval szűkítettem le a vizsgálatom tárgyát a foglalkoztatási tárgykörre, azon belül is a munkáltató toborzási és kiválasztási tevékenységére, valamint a munkavállalók munkaviszonnyal összefüggésben történő ellenőrzésére.

Az Európai Unió Bírósága ítélkezési gyakorlatának tárházából kulcsszavas kereséssel kizárólag előzetes döntéshozatali eljárásokat vizsgáltam, amelyek közül (2019-ig mintegy 10.500 lezárt ügyből) kettő kapcsolódott a tárgykörhöz, míg az Emberi Jogok Európai Bírósága „HUDOC" adatbázisának szintén kulcsszavas keresőjét alkalmazva hat vonatkozó ügyet találtam. Egy Alkotmánybírósági határozat és három bírósági határozat (BH) mellett, a Kúria színes és számos ítélkezési gyakorlatából mindösszesen egy állásfoglalást (MK 122. számú állásfoglalás), három elvi bírósági határozatot (EBH) és kettő döntést találtam, amely az általam vizsgált témakörhöz kapcsolódott. Mivel adatvédelemre szakosított szervről van szó, az összes vizsgált szerv közül a NAIH gyakorlatában találtam a legtöbb tárgyra vonatkozó döntést: a honlapon 2012 óta éves bontásban vezetett 271 darab hatósági határozat és végzés közül húszat.

Adatvédelem és munkajog az Európai Unió, az Európa Tanács és Magyarország jogforrási rendszerében

Az adatvédelem szakirodalmának egy jelentős ágát képezik azok a tanulmányok, amelyek e jogág evolúciós fejlődését adják. A történelmi hűség kedvéért megemlítem, hogy az első magánszféra-védelemmel foglalkozó tanul-

mány, Warren & Brandeis (1890) sokat hivatkozott cikke a Harvard Law Review hasábjain jelent meg, „The Right to Privacy" címmel. A tanulmány egyes elemeit és hatását elemzi például Jóri (2009), Majtényi (2006), Sólyom (1983).

A jelenlegi, harmadik generációs adatvédelem (Majtényi, 2003; Jóri, 2005; Hegedűs, 2013) életre hívása a globalizáció és a digitalizáció összekapcsolódásának eredménye. Bár az adatvédelem történeti gyökerei nem régiek, annak mégis több korszakát különbözteti meg a szakirodalom. A legszélesebb körben elfogadott álláspont szerint az első generációs szabályok a 70-es években alakultak ki, és az állami, számítógépes (legalább részben automatizált) nyilvántartásokkal szemben igyekezett valamilyen védelmet kialakítani az állampolgárok számára. A második generációs szabályok a 80-as, 90-es években jelentek meg, és már nem csak az automatizált, de a papíralapú nyilvántartásokat is a szabályozás hatálya alá vonták (Jóri, 2009). Így érkeztünk el a harmadik generációs szabályokhoz, amelyet Hegedűs (2013) szerint egy következő – negyedik – generációs szabályozás is követ, amelyre meglátása szerint jellemző lesz az önszabályozás, az Internettel kapcsolatban megjelenő adatvédelmi kérdések és a magánszférát erősítő technológiák („*right to disconnect*") megjelenése. Mint sok más kategorizálást, az adatvédelmi korszakváltások határait, vagy éppen azt, hogy az egyes jogforrások megjelenése pontosan melyik generációba tartozik, érdemes némi fenntartással kezelni. Szőke (2013) szerint a korszakolásnál valójában nagyobb jelentősége van az egyes szabályozások főbb jellemzőit és azok fejlődési tendenciáit kutatni.

Európai jogforrások

Ezt szem előtt tartva a továbbiakban azon tanulmányok legfontosabb megállapításait elemzem, amelyek az Európai Unió és az Európa Tanács által alkotott, a foglalkoztatásban releváns adatvédelmi jogszabályi kereteket és az azok által felvetett problémákat vizsgálják. Hogy az egyes tanulmányok mely joganyag részletekbe menő kritikai elemzését tartalmazzák, értelemszerűen attól függ, hogy mikor íródott. Megfigyelhető, hogy egy-egy nagyobb horderejű európai vagy magyar jogalkotási aktus, a publikációk sűrűsödését vonja maga után.

Általánosságban elmondható, hogy az EU más nemzetközi szervezetekhez képest meglehetősen későn szánta rá magát adatvédelmi jogalkotásra, így mintegy „kihagyva" az első szabályozási hullámot (Szőke, 2013). A 1980-as évek nemzetközi szintű jogalkotási eredményeit, az OECD-irányelvek (a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvek) és az Európa Tanács 108. számú Egyezmény elfogadását követően ugyanis az volt az uralkodó álláspont, hogy az Egyezményhez való csatlakozás megoldja a közösségi harmonizáció kérdését is. A jogalkotási és ennek megfelelően a publikációs késlekedés legfontosabb oka Szőke (2013) szerint abból fakadt, hogy a jogalkotás során két egymással ellentétesnek tűnő érdek között kellett egyensúlyt teremteni. El kellett fogadni egyrészt azt, hogy a (személyes) adatok hatékony felhasználása és ezek szabad áramlása az információs társadalom kiépítésének és a közös gazdasági térség kialakításának egyik kulcsa, másrészt azt is el kellett ismerni, hogy a személyes adatok védelme az egyének magánszféra-védelmének fontos eszköze, és biztosítani kellett ennek a magas szintű védelmét az EU tagállamaiban, illetve európai polgárok adatai esetén lehetőleg azon kívül is. Végül a 1995-ben készült el a sok kompromisszumot tartalmazó *95/46/EK irányelv* (Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról), amely egyébként a második generációs jogalkotás legfőbb európai eredménye. A legtöbb nemzetközi és hazai elemző elismerte az irányelv eredményeit (Korff, 2002; Bennett & Grant, 1998; Jay & Hamilton, 1999; Jóri, 2009). Kiemelték, hogy az irányelv lefektette a globális digitális társadalom alapvető fogalmait, a rendelkezések alkalmazhatósága alapján nem tett különbséget a közszféra és a magánszektor adatkezelői között (lévén az állam, Nagy Testvér mellett a Kis Testvér, az üzleti szféra adatéhsége is megnőtt), és hatálya mind az automatizált, mind a manuális adatkezelésekre kiterjed. Mivel azonban a 80-as évek végére kialakult dogmatikai alapokra épült, hosszú távon tartalmilag nem volt kellően hatékony.

Kereken húsz évvel ezelőtt, amikor 2000-ben a nizzai csúcstalálkozón a tagállamok aláírták az *Alapjogi Chartát*, önállóan nevesített alapjogként szabályozták a személyes adatok védelméhez fűződő jogot (8. cikk). Ez egyértelműen az alapjogi védelem megerősödését mutatta. Az adatvédelmi jog helye tovább erősödött az EU-n belül, amikor a *Lisszaboni Szerződés* (2009) kötelező jogi kötőerővel ruházta fel az Alapjogi Chartát és közvetlen alapjogvédelemben részesítette személyes adatok védelme tárgykört.

A második generációs adatvédelmi korszak jellegzetességeit számos tanulmány vizsgálta. E körben az információs önrendelkezési jog (az adatalany maga határozhat arról, hogy adatait más személyekkel vagy szervezetekkel megismerteti-e vagy sem) kifejezetten gazdag publikációs eredményt keletkeztetett (Szőke, 2013; Balogh, 2011; Majtényi, 2010; Jóri, 2009). Népszerű és sokat idézett Mayer-Schönberger (1997, p. 232) szemléltetése, aki szerint az információs önrendelkezési jogon alapuló adatvédelem „fogatlan papírtigrisnek", a „felső középosztály játékszerének" bizonyult. Érzékletesen írja le azt a helyzetet, amelyben az információs önrendelkezési joggal élve az egyén hozzájárulása a személyes adatok kezelésének legfontosabb jogalapja – a gazdasági erőfölényben, jobb alkupozícióban lévő adatkezelőkkel szemben az adatalany általában meg is adja a hozzájárulást, azaz valójában az adatvédelem nem érvényesül a magánszférát védő mechanizmusként.

Az adatvédelmi reform (harmadik generációs szabályozás előfutára) Európában 2012-re vált sürgető kérdéssé. Soha nem látott mértékben megnőtt a globális szintű adatmegosztás és adatgyűjtés, valamint egyre jellemzőbbé vált, hogy a magánszemélyek személyes információkat, adatokat tettek mindenki számára elérhetővé (Európai Bi-

zottság, 2012). A reform egyik eredményeként lépett hatályba a GDPR Rendelet (2016/679 rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről), amely 2018. május 25-től az EU összes tagállamában hatályos. Jogi természetéből fakadóan a Rendelet közvetlenül (átültetés nélkül) alkalmazandó és közvetlenül hatályosul a tagállami jogokban. Mindemellett a *88. cikke* lehetőséget ad a tagállamoknak a finomhangolásra. Ezek a módosítások a rendelethez képest sem szigorúbb, sem megengedőbb szabályozást nem eredményezhetnek, pusztán a pontosítást szolgálhatják. Ezen felül a tagállamok egy tárgykörben, a 9. cikk szerinti különleges adatok (biometrikus adatok, genetikai adatok és egészségügyi adatok) vonatkozásában állapíthatnak meg saját szabályokat. Bár jelentős számú tudományos szakirodalmi hivatkozás nem keletkezett a korábbi 95/46/EK irányelv 29. cikke alapján létrejött *adatvédelmi munkacsoport* „Key Provisions" alcsoportjára, mindazonáltal tevékenysége ma is jelentős hatást gyakorol a személyes adatok foglalkoztatással összefüggő kezelésére, és néhány megállapítására a módszertani részben utalni fogunk (Adatvédelmi munkacsoport, 2017; Adatvédelmi munkacsoport, 2014).

Az adatvédelmi jog egy speciális ágát képezi azon tanulmányok köre, amelyek az *Európa Tanács* jogalkotó tevékenységét elemzik. Az Európa Tanács 108. számú adatvédelmi egyezménye (1981) korának legjelentősebb adatvédelmi dokumentuma és egészen 1995-ig, az EU adatvédelmi irányelvének elfogadásáig az egyetlen kötelező erejű, nemzetközi szintű jogforrása. Az egyezmény tartalmáról részletes elemzést kínál Balogh (1998), Jóri (2009), Hegedűs (2013). Az Európa Tanács kifejezetten a foglalkoztatásra vonatkozó ajánlását 1989-ben adta ki először, majd azt 2015-ben felülvizsgálta.

A Rendelet horizontális (munkajogra is kiterjedő) hatálya okán nem találunk kifejezetten adatvédelmi tárgyú európai munkajogi joganyagot. Az Európai Unió „munkajoga" néhány kollektív munkajogi intézménytől eltekintve (2009/38/EK irányelv az Európai üzemi tanácsokról, 2002/14/EK irányelv a munkavállalók tájékoztatásáról és a velük folytatott konzultációról) kifejezetten az individuális relációkra összpontosít, azon belül is elsősorban az atipikus jogviszonyokra, a munkavédelemre, a munkáltató strukturális átalakítása esetén szükséges eljárásokra és a munkavállalók egyes munkakörülményeire (Kiss, 2001). Legaktuálisabban az EU munkajogi jogalkotási aktivitásában az átlátható és tisztességes munkafeltételek (2019/1152 EU irányelv) és a munka és a magánélet közötti egyensúly megteremtése állnak (2019/1158 EU irányelv), mindkét irányelv esetén egyébként 2022. augusztusi tagállami implementációs kötelezettséggel.

Összefoglalásként megállapítható, hogy az európai adatvédelmi jogalkotás az Európai Unió és az Európa Tanács keretein belül párhuzamosan, mégis egymással összhangban zajlott az elmúlt évtizedekben. A jogfejlődés eredményeként mára az EU elsődleges és másodlagos jogforrásai, valamint az Európa Tanács kötelező és nem kötelező jogi aktusai biztosítják az adatvédelem horizontális kereteit, lefedve az élet valamennyi érintett színterét, így a foglalkoztatást is – erre irányuló külön európai munkajogi rendelkezés nélkül. A hatályos európai jogforrásokat az *1. táblázat* tartalmazza.

1. táblázat

A munkajogviszonyra (is) vonatkozó hatályos európai adatvédelmi jogforrások

Európai Unió		Európa Tanács
Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikke	**Adatvédelem a munkajogviszonyban**	Emberi Jogok Európai Egyezménye (1950)
Alapjogi Charta 7. és 8. cikk		Megújított 108. Egyezmény (2015)
95/46/EK irányelv 29. cikke alapján létrejött adatvédelmi munkacsoport ajánlásai és véleményei		Foglalkoztatásra vonatkozó 5. számú ajánlás (2015)
2016/679 Általános adatvédelmi rendelet, és annak 88. cikke		

Forrás: saját szerkesztés, felhasználva az Európai Unió Alapjogi Ügynöksége és az Európa Tanács kézikönyve (2019) megállapításait

Jogforrások Magyarországon

Magyarországon 1977-ben jelent meg a jogrendszerben a személyes adatok védelmére való első utalás: a régi Ptk. (1959. évi IV. törvény 83. §) a személyhez fűződő jogok között úgy rendelkezett, hogy a számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat, és a nyilvántartott adatokról tájékoztatást – az érintett személyen kívül – csak az arra jogosult szervnek vagy személynek lehet adni. Emellett rögzítette az érintett helyesbítéshez való jogát. A rendszerváltó jogalkotás körében 1989-ben a személyes adatok védelme és a közérdekű adatok nyilvánossága alapvető jogként bekerült az Alkotmányba és hatályba lépett a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Avtv.) és a kutatás szempontjából releváns munka törvénykönyvéről szóló 1992. évi XXII. törvény (továbbiakban: régi Mt.). Az adatvédelem szabályainak érvényesülését az akkori adatvédelmi biztos is felügyelte. 2012 fordulópontot jelentett az adatvédelemben, amikor mindkét törvény helyébe új, mai is hatályos joganyag lépett: az Avtv-t felváltotta a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.), a 2012. évi I. törvény a munka törvénykönyvéről (továbbiakban: új

Mt.), amely kereken húsz év után „nyugdíjba küldte" a régi Mt-t. Az Infotv. egyik legnagyobb változtatása az intézményi oldalon, hogy megszűntette az ombudsmani rendszert, és létrehozta az adatvédelmi felügyeleti hatóságként működő Nemzeti Adatvédelmi és Információszabadság Hatóságot (NAIH). A hatályos magyar jogrendszerben a horizontálisan (minden adatkezelési jogviszony tekintetében általánosan) alkalmazandó Infotv-hez kapcsolódik a munkajogviszonyt érintő ágazati törvény az Mt. (Kiss, 2020). Az Országgyűlés 2019 áprilisában, azaz egy évvel a Rendelet hatályba lépése után hajtott végre átfogó módosításokat az ágazati törvényekben (2019. évi XXXVI. törvény), így az Mt-ben is, amelyre a Rendelet 88. cikke adta meg a lehetőséget a tagállamok számára.

A Rendelet olyan kötelező norma, amelyet valamennyi tagállamnak egységesen, egyformán és közvetlenül kell megtartania. Az Infotv. valójában tehát csupán néhány anyagi jogi szabályt tartalmaz a rendelet hatálya alá tartozó adatkezelések esetére [Infotv. 2. § (2) bekezdés]. Ez azt is jelenti egyben, hogy a munkaviszonyban felmerülő adatkezelési kérdésekre Magyarországon az alábbi rendelkezések hatályosak:

a. *Rendelet szabályai így különösen*: GDPR-alapelvek (5. cikk), az adatkezelés célja és jogalapja (6. cikk), előzetes tájékoztatás és az érintetti jogok biztosítása (12–22. cikkek), adatkezelési és adatfeldolgozási tevékenységek belső nyilvántartása (30. cikk), az adatbiztonság és a beépített és alapértelmezett adatvédelem elvének biztosítása (24–25., 32. cikk), adatvédelmi incidens (33–34. cikk), egyes esetekben az adatvédelmi tisztviselő kijelölése (37–39. cikk),
b. *meghatározott körben az Infotv. általános szabályai* [Infotv. 2. § (2) bekezdés],
c. speciálisan az *Mt. 10-11. § valamint 11./A §-ok*, az alábbi tárgykörökben:
   1. munkaviszonnyal kapcsolatos okiratok bemutatása, másolása [Mt. 10. § (1)-(3) bekezdések],
   2. alkalmasságvizsgálatok [Mt. 10. § (4) bekezdés],
   3. munkavállalók tájékoztatása az adatkezelésről [Mt. 10. § (5) bekezdés],
   4. különleges adatok (természetes személyek egyedi azonosítását célzó biometrikus adatok úgy mint képmás, ujjlenyomat, íriszkép, aláírás dinamikájának elemzésén alapuló adat) és bűnügyi személyes adatok kezelése (erkölcsi bizonyítvány) [Mt. 11. §],
   5. munkavállaló munkaviszonnyal összefüggő magatartásának ellenőrzése [Mt. 11/A. §].

Összefoglalásként megállapítható, hogy a rendszerváltó alkotmányozás 1992-ben az EU szabályozási logikájától eltérően teremtette meg az adatvédelem alapjait Magyarországon: horizontális (Adatvédelmi törvény) és a foglalkoztatásra külön hatályos (régi Munka törvénykönyve) jogforrások formájában. Ez a szabályozási szerkezet él ma is, bár megújult tartalommal, elnevezésekkel és a téma fontosságát is jelölve – bővített intézményrendszerrel.

A hazai és európai jogforrási hierarchiából fakadóan a tagállami jog felett, a szubszidiaritás elve mentén – az EU adatvédelmi biztos intézménye és az uniós jog, valamint az Európa Tanács tagjaként az EJEE, a 108. sz. Egyezmény és az 5. számú ajánlás áll. Ezt a jogforrási keretrendszert szemlélteti a 2. táblázat, amely a következő fejezetben kifejtésre kerülő ítélkezési gyakorlatok koordinátarendszerét adja.

2. táblázat

A munkajogviszonyban releváns adatvédelmi jogforrások és hatóságok Magyarországon a rendszerváltástól napjainkig

EURÓPAI UNIÓ EUMSZ 16. cikk Alapjogi Charta 7. és 8. cikk Általános Adatvédelmi Rendelet Adatvédelmi munkacsoport Európai adatvédelmi biztos		**EURÓPA TANÁCS** Emberi Jogok Európai Egyezménye 108. Egyezmény Foglalkoztatásra vonatkozó 5. számú ajánlás
Magyarország Alaptörvénye		
Adatvédelmi törvények és intézmények 2011. előtt		**Adatvédelmi törvények és intézmények 2011. után**
1992. évi LXIII. törvény (Avtv.)	⇒ **Adatvédelem a munkajogviszonyban** ⇒	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
1992. évi XXII. törvény (régi Mt.)		2012. évi I. törvény a munka törvénykönyvéről (Mt.)
Adatvédelmi biztos		Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

Forrás: saját szerkesztés

Mit mutat az esetjog?, avagy az Európai Unió Bírósága, az Emberi Jogok Európai Bírósága esetjoga és a magyar joggyakorlat

Bár a kontinentális jogrendszerekben a precedensjog nem ismert, a nemzetközi és tagállami szinteken működő bíróságok jogalkalmazást egységesítő tevékenysége vitathatatlan. A továbbiakban az Európai Unió Bírósága

(*Court of Justice of the European Union*) és az Európa Tanács mellett működő Emberi Jogok Európai Bíróságának (*European Court of Human Rights)* foglalkoztatást érintő adatvédelemi tárgyú ítélkezési vívmányait elemzem.

Az Európai Unió Bírósága és az Emberi Jogok Európai Bírósága ítélkezési gyakorlata

Az adatvédelemmel foglalkozó jogászok gyakori témája (Szőke, 2014; Jóri, 2009; Mészáros, 2017) az *Európai Unió Bírósága* (továbbiakban: EUB) ítélkezési gyakorlata, amelynek munkajogi adatvédelmi döntéseit az EUB hivatalos honlapjának keresője és a „Tematikus adatlapok" kereső felület segítségével igyekeztem feltárni. A vizsgált döntések előzetes döntéshozatali eljárások és mindösszesen két ügynek van foglalkoztatási relevanciája, bár egyik sem a munkaerő-felvételhez vagy a munkavállalók munkaidőben történő megfigyeléséhez kapcsolódik. *Lindqvist ügyben* (2003) kimondta a bíróság, hogy amennyiben magánszemélyeket egyértelműen beazonosító személyes adatok felkerülnek az Internetre, az a „személyes adat részben vagy egészben automatizált módon való kezelését" jelenti, ugyanakkor nem minősül annak harmadik országba történő továbbításának (ebben az ügyben egy svéd önkéntes tett fel szintén önkénteseket beazonosító személyes adatokat az internetre). *Worten ügyben* (2013) az EUB ugyan személyes adatnak minősítette a munkavállalók munkaidő-adatait, de azt is kimondta, hogy a munkáltatónak, mint a személyes adatok kezelőjének kötelezettsége, hogy a munkafeltételek ellenőrzésére hatáskörrel rendelkező nemzeti hatóságok részére azonnali hozzáférést biztosítson a munkaidő-nyilvántartáshoz.

A magyar foglalkoztatási gyakorlatokra is jelentős hatása van az Európa Tanács mellett működő *Emberi Jogok Európai Bírósága* (továbbiakban: EJEB) ítélkezési gyakorlatának, amely az európai munkajogi adatvédelem jelentős bástyájának tekinthető. Az elmúlt években az EJEB több olyan esetben is eljárt, amelyek a munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzéséhez kapcsolódtak és nagy nemzetközi visszhangot keltettek. A munkaerő-biztosításhoz kapcsolódó esetet azonban itt sem találtam. Az EJEB fokozatos, de következetes ítélkezési gyakorlatát a munkavállalók ellenőrzése tárgykörben a következő ügyek mentén dolgozta ki.

Az EJEB *Halford v. United Kingdom* (1997) ügyben kimondta, hogy mind az üzleti célú, mind az otthonról lebonyolított telefonhívások az Emberi Jogok Európai Egyezménye (továbbiakban: EJEE) 8. cikk 1. pontja szerinti magán- és családi élet tiszteletben tartásához való jog fogalmai alá tartoznak. A munkáltató előzetes figyelmeztetés nélkül tehát nem jogosult a munkavállaló (az ügyben egy angol rendőrnő) hivatali és magántelefonját lehallgatni.

A *Copland kontra Egyesült Királyság* (2007) ügy kiterjesztette a fenti ügy tárgykörét az e-mail- és internethasználatra is. A munkáltató titokban, vagyis előzetes tájékoztatás vagy vonatkozó munkáltatói szabályzat hiányában nem jogosult a munkavállaló telefon-, e-mail- és internethasználatát nyomon követni, mert ezek mindegyike az EJEE 8. cikk szerinti védelmében részesülnek.

A *Bărbulescu kontra Románia ügy* (2017) nagy magyar sajtónyilvánosságot kapott (Hegyeshalmi, 2017; hrportal.hu, 2017; nepszava.hu, 2017), és hozzá kapcsolódóan több jogértelmezést segítő szakmai írás is született (Rózsavölgyi, 2018; Kállai, 2017). Az ítélet alapvető jelentősége abban áll, hogy meghatározta azokat a szempontokat, amelyeket a nemzeti bíróságoknak figyelembe kell venniük annak értékelése során, hogy a munkáltató ellenőrzési, fegyelmi jogkörének gyakorlása jogszerű-e. Az ügy olyan alkalmazottra (Bărbulescu) vonatkozik, akinek munkaszerződését a munkáltató felmondta, miután a munkavállalók internetes kommunikációját megfigyelte és megállapította, hogy Bărbulescu magáncélokra (is) felhasználta a vállalati erőforrásokat, például a Yahoo Messengert. Az azóta Bărbulescu-tesztnek is nevezett szempontrendszer a következő kérdések megválaszolását várja a tagállami bíróságoktól:

a. A munkavállalót értesítette-e előzetesen a munkáltató a megfigyelésről?
b. Milyen széles körű volt a megfigyelés, és mennyire avatkozott bele a munkavállaló magánéletébe?
c. Milyen jogos indokok alapján történt a megfigyelés?
d. Elegendőek lettek volna-e a munkáltató részéről kevésbé tolakodó módszerek?
e. Milyen következményekkel járt a megfigyelés a munkavállalóra nézve, és valóban a legsúlyosabb szankció szükséges-e?
f. Voltak-e megfelelő biztosítékok a munkavállaló számára, így például panasztételi lehetőség a megfigyeléssel kapcsolatban?

Sipka & Zaccaria (2018) kiemeli, hogy a Bărbulescu ügynek van egy másik igen lényeges aspektusa is: a munkavállaló magánadatai (magánélete) abban az esetben sem ellenőrizhetők, ha a magáncélú eszközhasználatot a munkáltató kifejezetten kizárta. Tehát egy munkaeszköz utasítástól eltérő használata eredményezhet munkajogi következményeket (fegyelmi eljárás, munkaviszony-megszüntetés), de a munkavállalói szabályszegés még ebben az esetben sem jogosíthatja fel a munkáltatót arra, hogy a tárolt magánadat tartalmát megismerje.

A munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzése tárgykörben ki kell térni az EJEB legutóbbi döntésére, a *Libert kontra France* ügyben hozott döntésre (2018). A Bărbulescu ügytől eltérően itt éppen az volt a kérdés, hogy a munkáltató ellenőrzési joga az átadott eszközök vonatkozásában meddig terjed ki. Az ítélet kulcseleme, hogy csupán az a munkáltatói ellenőrzési cselekmény sérti az EJEE 8. cikkét, amely a munkavállaló által egyértelműen „magán" jelöléssel ellátott adatokra vonatkozik. Az alapügyben eljáró Francia Semmítőszék ugyanis különbséget tett a „magán" (private) és a „személyes" (personal) adatok között: a kettő közül csak a „magán" (private) élvezi a 8. cikk védelmét. A bíróság érvelése szerint a „személyes" (personal) adat kevéssé szenzitív, és lehet a munkavállaló személyéhez kötődő, de a munkavégzéssel összefüggésben álló adat is (munkahelyi elérhetőség, teljesítménymutatók, szakmai besorolás). A kettő adattípus éles elhatárolása a gyakorlatban persze nem mindig egyér-

telmű, a felek közötti vita is ebből eredt. Az is kiolvasható az ítéletből, hogy a „magán" jelöléssel ellátott adatok sem élveznek abszolút védettséget: ha a munkáltató által biztosított eszközön kerülnek tárolásra, akkor a munkavállaló jelenlétében nem tilos az ezekbe történő betekintés. A célhoz kötöttség viszont minden munkáltatói betekintés esetén követelmény: olyan adatokba és dokumentumokba semmilyen módon nem tekinthet be a munkáltató, amelyek egyértelműen nem a munkaviszony céljával, rendeltetésével függnek össze (Sipka & Zaccaria, 2018).

Az EJEB a munkavállaló munkaviszonnyal összefüggő magatartásának megfigyelése körében a *Köpke kontra Németország* ügyben (2010) rejtett videokamerás megfigyeléssel összefüggésben kimondta, hogy amennyiben a munkáltatók alkalmazni kívánnak munkavállalókat ellenőrző kamerás megfigyelést, akkor igazolniuk kell azt a jogos érdeket, amely szükségessé teszi a rejtett kamera alkalmazását.

Ezt a döntést fejleszti tovább az EJEB a *López Ribalda és társai kontra Spanyolország* (2019) ügyben, amikor átülteti a Bărbulescu-teszt lépéseit a munkáltatók munkahelyi kamerás megfigyelési intézkedéseire:

a. Munkavállaló előzetes értesítése: Csak a jelentős köz- vagy magánérdekek védelmére vonatkozó nyomós követelmény igazolhatja az előzetes tájékoztatás hiányát.
b. A megfigyelés mértéke: tilos a megfigyelés a fokozottan védett helységekben (mosdók, öltözők). Az előzőnél alacsonyabb, de még magas védelemben részesülhetnek a körülhatárolt, nyilvánosság számára nem hozzáférhető helyiségek (saját iroda). A munkatársak és a vásárlók számára nyitva álló, vagy belátható területeken jóval kevesebb privátszférára számíthat az alkalmazott.
c. Megfigyelés indokoltsága: Nem elfogadható a rejtett kamerás megfigyelés általában azért, mert felmerülhet a lopás, vagy más munkavállalói jogellenesség legkisebb gyanúja. Ugyanakkor a súlyos kötelességszegés elkövetésének ésszerű gyanúja, valamint a készlethiány jelentős mértéke (lopás miatt) elegendő oknak minősülhet a rejtett kamerás megfigyeléshez különösen abban az esetben, ha ez a munkáltató zökkenőmentes működését veszélyezteti és felmerül több alkalmazott összehangolt fellépésének gyanúja is.
d. Kevésbé tolakodó módszerek alkalmazása: Mivel a konkrét ügyben a megfigyelés tíz napig tartott és a felvételeket szűk kör láthatta, a magánéletbe való beavatkozás nem volt súlyosnak tekinthető és más hatékony módszer nem állt a munkáltató rendelkezésére a tulajdonjogának védelme érdekében.
e. A megfigyelés következményeinek vizsgálata továbbra is szükséges.
f. Megfelelő munkavállalói biztosítékok (panasztétel lehetősége) úgyszintén szükségesek.

3. táblázat

A munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzése az Európai Unió Bírósága és az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatának tükrében

Ügy neve	Ítélet keletkezése	Ítélet jelentősége
EURÓPAI UNIÓ BÍRÓSÁGA (Előzetes döntéshozatali eljárások)		
Lindqvist ügy	2003	Magánszemélyek és az őket egyértelműen beazonosító személyes adatok internetre kerülése „személyes adat részben vagy egészben automatizált módon való kezelését" jelenti.
Worten ügy	2013	Bár a munkaidőadat személyes adatnak minősül, a munkáltatónak, mint a személyes adatok kezelőjének kötelezettsége, hogy a munkafeltételek ellenőrzésére hatáskörrel rendelkező nemzeti hatóságok részére azonnali hozzáférést biztosítson a munkaidő-nyilvántartáshoz.
EMBERI JOGOK EURÓPAI BÍRÓSÁGA (EJEE 8. cikk vizsgálata)		
Halford ügy	1997	A munkáltató előzetes figyelmeztetés nélkül nem jogosult a munkavállaló *hivatali és magántelefonját* lehallgatni.
Copland ügy	2007	A munkahelyen folytatott telefonbeszélgetéseken túl az *e-mailek és az internethasználat* nyomon követéséből származó információk is a 8. cikk szerinti védelemben részesülnek.
Bărbulescu ügy	2017	– A munkáltató egyértelműen elfogadott és elismert joga, hogy a munkavállalót ellenőrizze és ennek keretében megismerje a számítógépen tárolt, munkaviszonnyal kapcsolatos adatokat. – *Ennek jogszerűségi feltétele: Bărbulescu-teszt.* – A munkavállaló magánadatai (magánélete) abban az esetben *sem ellenőrizhetők*, ha a magáncélú eszközhasználatot a *munkáltató kifejezetten kizárta.*
Libert ügy	2018	– *Célhoz kötöttség elve*: minden munkáltatói betekintés esetén követelmény, hogy az egyértelműen összefüggésben legyen a munkaviszony céljával, rendeltetésével. – A munkavállaló által kifejezetten *„magán" jelöléssel ellátott és a munkáltató eszközein levő adatainak* ellenőrzésére a munkáltató csak a munkavállaló jelenlétében jogosult, figyelembe véve a célhoz kötöttség elvét is.
Köpke ügy	2010	Kamerás megfigyelés esetén a munkáltatónak *igazolnia kell azt a jogos érdeket*, amely szükségessé teszi a kamera alkalmazását.
López Ribalda és társai ügy	2019	*Bărbulescu-teszt kiterjesztése a munkavállalók videokamerás megfigyelésének esetére.*

Forrás: saját szerkesztés

Az EUB és az EJEB által kimunkált esetjog legfontosabb megállapításait a 3. táblázat foglalja össze.

Magyar esetek katalógusa

A munkaerő-ellátáshoz és a munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzéséhez kapcsolódó döntéseket az európai esetjogi résztől eltérően nem a döntés kibocsátója alapján, hanem tárgykör szerinti csoportosításban vizsgáltam. Ennek oka a határozatok, állásfoglalások és tájékoztatók számossága, amelyek lényegi tartalmi elemeit fűztem egybe az egyes munkajogi adatvédelmi szituációk elemzésekor.

A vizsgált tárgykörök katalogizálása előtt lényeges kiemelni, hogy függetlenül az ügy tartalmától, a munkáltatói adatkezeléssel kapcsolatos alapvető elvárás a jogszerűség és a Rendeletben, az Infotv-ben, valamint az Mt-ben lefektetett általános alapelveknek való megfelelés:

a. *Célhoz kötöttség elve:* a munkáltatónak minden adatkezeléséhez célt kell rendelnie. Azaz személyes adat csak akkor kezelhető, ha az adat kezelése nélkül a munkaviszony létesítése, fenntartása, megszűnése nem lenne lehetséges.

4. táblázat

Vizsgált munkahelyi adatkezelési szituációk és a hozzájuk köthető hivatalos szerv által kiállított dokumentumok összefoglaló táblázata

Munkahelyi szituáció	Kibocsátó	Ügyszám
Adatkezelés a toborzás és kiválasztás során		
Anonim álláshirdetések	NAIH / Adatvédelmi biztos	NAIH-1159-15/2015/H. NAIH-608/2013/H 167/A/2006-3.
Pályázók közösségi oldalon levő profiljának megtekintése	NAIH NAIH Tájékoztató (2016)	NAIH/2016/4386/2/V
	Adatvédelmi munkacsoport (2017)	
Alkalmasságvizsgálatok	NAIH Tájékoztató (2016)	
Referencia-ellenőrzés	NAIH	NAIH/2016/4386/2/V
Hazugságvizsgáló (poligráf) alkalmazása	Kúria	EBH2013. M. 9.
Visszajelzés a kiválasztási döntésről	NAIH Tájékoztató (2016)	
Pályázatok, önéletrajzok megőrzése	NAIH Tájékoztató (2016)	
	Európa Tanács (2015)	
Munkavállalók munkaviszonnyal összefüggő magatartásának ellenőrzése		
Kamerás megfigyelés	NAIH / Adatvédelmi biztos	NAIH/2019/2466 NAIH/2018/2466/2/K NAIH/2018/3295/H NAIH/2015/3355/H NAIH-1941/2013/H NAIH-4001-6/2012/V 1805/A/2005–3 ABI–97/2010/P
	Kúria	EBH 296/2000
	Alkotmánybíróság	36/2005. (X. 5.) AB határozat
Céges e-mail-fiók ellenőrzése	NAIH / Adatvédelmi biztos	NAIH/2019/769 NAIH/2019/51/11 879/A/2005–3
Céges laptop ellenőrzése	NAIH	NAIH/2015/1402/H NAIH-421-19/2013/H.
Céges telefon ellenőrzése	Kúria	LB Mfv.I.10.397/2018.
Munkaidőben történő internethasználat ellenőrzése		BH2006. 64
GSP rendszer alkalmazhatósága	NAIH / Adatvédelmi biztos	NAIH-42-6/2013/V 1664/A/2006–3
Munkahelyi alkohol- és drogteszt alkalmazása	Kúria	MK 122. számú állásfoglalás LB Mfv.I. 10.939/1999 EBH 1999/47. BH2006. 64. BH2000. 432. ABI–687/2010/K

Forrás: saját szerkesztés

b. *Szükségesség-arányosság elve:* Az alkalmazott eszköznek alkalmasnak kell lennie a cél elérésére, de csak a szükséges mértékű adatkezeléssel járhat (pl. időben korlátozott) és az ellenőrzés csak a munkával összefüggésben történhet. A munkavállalók magánélete nem ellenőrizhető.
c. *Megfelelő jogalap az adatkezeléshez*: A munkahelyi adatkezelés során alapvetően három jogalap jöhet szóba, amely közül a munkáltatónak választania kell: az érintett hozzájárulása (önkéntesség), törvényi felhatalmazás, illetve a munkáltató jogos érdekén alapuló adatkezelés. (A Rendelet 6. cikke összesen hat lehetséges jogalapot ismer, a munkaviszonnyal összefüggésben valójában a fenti három a legjellemzőbb.) Korábban utaltam rá: mivel a munkaviszonyt erős alá-fölérendeltség jellemez, a munkavállalói hozzájárulás jogalapként csak akkor jöhet szóba, ha valódi választási lehetőség áll az érintett rendelkezésére, és nem áll fenn negatív következmény veszélye a hozzájárulás megtagadása esetén. E helyen utalok arra is, hogy a munkáltatói jogos érdek, mint jogalap esetén a munkáltatónak el kell végeznie az érdekmérlegelési tesztet (részletesen lásd: Adatvédelmi Munkacsoport, 2014). Ilyenkor az adatkezelő mérlegre teszi egyrészt a saját vagy egy tőle független harmadik személy jogos érdekét, valamint az érintett magánszférájából, vagy más alapvető jogaiból származó védelméhez fűződő jogait, érdekeit, és amennyiben az első érdekkör felülírja a másodikat, az adatkezelés jogszerű lesz, amennyiben nem, úgy az adott adatkezelés nem kezdhető meg. A jogos érdek önmagában sokféle lehet, így a munkáltató gazdasági érdekei, hatékonyságnövelés, kutatás-fejlesztés, szervezeti fejlesztés, új folyamatok kialakítása, biztonsági intézkedések, visszaélés-megelőző rendszerek, statisztikai adatgyűjtés, de akár a hatékony napi működés is ide tartozhat.
d. *Munkavállalók előzetes tájékoztatása*: Az előzetes és megfelelő tájékoztatás kötelezettségének központi eleme az Infotv. 20. § (2) bekezdése, amely felsorolja azokat az alapvető adatkezelési körülményeket, amelyekről az adatkezelőnek tájékoztatást kell nyújtania. Amennyiben a munkáltató technikai eszközzel kíván ellenőrzést végezni úgy az nem lehet titkos, arról a munkavállalókat előzetesen tájékoztatni kell. A munkahelyi adatkezelésekkel összefüggésben továbbá az is kiemelten fontos, hogy a munkáltató szervezetén belül ki férhet hozzá a személyes adatokhoz.

A 4. táblázat az általam vizsgált munkahelyi adatkezelési szituációk összefoglalását tartalmazza, amelyek a munkáltató toborzási és kiválasztási tevékenységéhez, valamint a munkavállalók munkaviszonnyal összefüggésben történő ellenőrzéséhez kapcsolódnak. Ezek a szervezetek HR-tevékenységei során rendszeresen felmerülő helyzetek, amelyeket az adatkezelés jogszerűségének szemszögéből vizsgálok. A táblázat harmadik oszlopában az alábbi szervek által kibocsátott dokumentumok találhatók:

1. Alkotmánybírósági határozatok (AB),
2. Kúria döntések, állásfoglalások (MK), elvi bírósági határozatok (EBH), bírósági határozatok (BH),
3. NAIH tájékoztató, ajánlás, határozat és Adatvédelmi biztos (2012 előtti ügyek) beszámolói és határozatai,
4. Egyes esetekben a fentieket megerősítették az Európa Tanács és az Adatvédelmi munkacsoport által kiadott ajánlás és vélemény.

Következtetések és megfontolások a szervezeti emberierőforrás-menedzsment gyakorlatok számára

A tanulmány korábbi fejezeteinek tartalma alapvetően azt a célt szolgálta, hogy a Magyarországon működő munkáltatók emberierőforrás-menedzsment területen dolgozó szakemberei számára is pontosan kirajzolódjon az a jogszabályi környezet amelyben, a munkaviszonyban releváns adatvédelmi szabályok alkalmazása szükséges és indokolt. A továbbiakban az európai és magyar esetjogból kiolvasható következtetéseket foglalom össze, amelyek a szervezeti HR-szakemberek számára támpontot jelenthetnek az egyes HR-funkciók jogkövető kialakításához és fenntartásához.

Emberierőforrás-biztosítás (toborzás és kiválasztás)

A hatékony emberierőforrás- vagy személyzetbiztosítást sokan tartják a szervezeti siker kritikus tényezőjének (Karoliny, Ásványi, & Bálint, 2017). A személyzetbiztosítás nemcsak a szervezeti kiválóság és a költségkontroll egyik eszköze, de az egyik olyan funkció is egyben, ahol az adatvédelemnek nagy jelentősége van. A jelöltek adatainak megfelelő védelme megfelelő garanciákat kell, hogy kapjon a toborzás és kiválasztás teljes folyamata során.

A toborzási tevékenység során az *anonim álláshirdetések* kapcsán merül fel problémaként az, hogy az állást meghirdető munkáltató jogos megfontolásból nem kívánja felfedni a kilétét, így az állásra jelentkező pályázó valójában nem tudja, hogy ki minősül az Infotv alapján adatkezelőnek és így kinél tudja érvényesíteni jogait. Ebben a gyakorlatban rendkívül egyenlőtlen helyzetben vannak a felek, hiszen míg az érintettek jelentkezésük elküldésével azonnal „kiadják magukat", minden személyes adatukat megismeri az álláshirdetést feladó munkáltató, addig a munkáltató egyáltalán nem ad semmilyen tájékoztatást a személyéről, ezáltal is fokozva a munkavállalók kiszolgáltatottságát, és a munkáltató információs fölényét. Az adatvédelmi biztos már 2006-os ajánlásában is kifejtette, hogy az álláshirdetésekben a hirdetést feladó személynek meg kell adnia azokat az adatokat (cím, telefonszám), amelyek alapján az érintett megfelelő tájékoztatást kaphat arról, hogy személyes adatait kinek küldi meg. Ha a hirdetést feladó olyan jellegű személyes adatokat is kér, mely kezelésének célja nem egyértelmű (kézzel írt önéletrajz), a jelentkező tájékoztatást kérhet az adatok kezelésének céljáról (ABI 167/A/2006). A NAIH tájékoztatójában (2016) kifejti, hogy alapvetően nem fogadható el a munkáltatók részéről az anonim álláshirdetések feladása, mivel az esetek túlnyomó többségében ezzel aránytalanul sérül a je-

lentkezők információs önrendelkezési joga. Ezért a munkáltatók csak különösen indokolt, rendkívüli esetben, és akkor is legfeljebb korlátozott mértékben (például egy rövid, átmeneti időtartamig) élhetnek az anonim álláshirdetések gyakorlatával. Ugyancsak az anonim álláshirdetések kapcsán a NAIH a profession.hu állásportál gyakorlatának elemzése után arra a következtetésre jutott, hogy mind az állásportál üzemeltetője, mind az álláshirdetés feladója adatkezelőnek minősül. Az adatvédelmi biztos ajánlásával szemben a NAIH egy megengedőbb gyakorlatot is elfogadhatónak tart: ha az állásportálon az anonim hirdetésre jelentkezés előtt a jelöltek egy „checkbox" kipipálásával maguk dönthetnek arról, hogy egy munkáltató felé továbbíthatók-e az adataik vagy sem, ez az elfogadható előzetes tájékoztatási gyakorlatnak megfelel. Ezzel együtt biztosítani kell az érintettek számára, hogy élhessenek a törléshez való joggal, ezáltal pedig az adatkezelő pontos kilétének felfedésére sincs feltétlenül szükség.

A kiválasztási eljárás során érdemes azt is megvizsgálni, hogy mit mutat az európai és magyar esetjog a *jelentkező közösségi oldalakon elérhető profiljának* felhasználásáról a kiválasztási eljárásban. A NAIH és a 29. cikk szerinti adatvédelmi munkacsoport is azt az álláspontot osztja, hogy bizonyos feltételekkel ez a gyakorlat megengedett, mert egyfelől mindenki maga állítja be, hogy az általa megosztott tartalmat ki láthatja, másrészt nem életszerű azt elvárni a munkáltatóktól, hogy ne tekintsék meg a nyilvános tartalmakat. Ahhoz, hogy ez a gyakorlat jogszerű legyen, az alábbi feltételeknek meg kell valósulniuk (NAIH, 2016, Adatvédelmi munkacsoport, 2017):

a. tájékoztatni kell a jelentkezőket (álláshirdetésben) a közösségi oldalak megtekintésének lehetőségéről,
b. csak a munkaviszony létesítése szempontjából releváns adatokat lehet megismerni (a munkaviszony létesítése szempontjából nem lényeges adat a magánéletre, párkapcsolatra, családi életre, vallásra vonatkozó adat),
c. az adatok megismerése csak a nyilvánosan elérhető adatokra terjedhet ki, a leendő munkavállaló sem más ismerőse útján nem kérhet információkat nem nyilvános profiladatokról, sem azt nem kérheti a munkavállaltól, hogy jelölje barátnak a szélesebb körű hozzáférés érdekében,
d. a munkáltató nem jogosult arra, hogy a jelentkező profiloldalát mentse, tárolja vagy más számára továbbítsa.

A megfelelő számú és kvalitású jelölt toborzása után a szerveztek kiválasztási eljárását is átszövi az adatkezelési tevékenység. Az Mt. 10. § (4) bekezdése alapján a munkavállalóval szemben olyan *alkalmasságvizsgálat* alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő (jogalap ilyenkor a jogi kötelezettség teljesítése), vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges (a jogalap az érdekmérlegelés). A NAIH (2016) gyakorlata alapján részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, és a vizsgálat milyen eszközzel, módszerrel történik. Az eredmények megismerhetősége is korlátozott: azt csak a vizsgált munkavállaló, illetve a vizsgálatot végző szakember ismerheti meg, különösen, mivel abból akár olyan következtetés is levonható, amely maga az érintett munkavállalók számára sem volt ismert. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez, de a vizsgálat részleteit, és annak teljes dokumentációját nem ismerheti meg. Amennyiben a munkáltató szakembere végzi a vizsgálatot, az érdekmérlegelés (a választott módszernek alkalmasnak kell lennie a cél elérésére, a munkaviszonnyal kapcsolatos releváns adatot lehet kapni a teszttel, szükséges annak elvégzése) és a belső feladatmegosztás alapján dönthető el, hogy pontosan mely szereplő mely adat megismerésére jogosult.

Amennyiben a munkáltató teszteket alkalmaz a kiválasztás során, akkor figyelemmel kell lennie arra, hogy munkaalkalmassági (képesség- vagy készséget mérő) tesztek mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitölthetők a munkavállalókkal. Más megítélés alá esnek azonban a pszichológiai tesztlapok: az egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében kötelezően kitölthető a munkavállalók nagyobb csoportjával a személyiségjegyek kutatására alkalmas tesztlap, de csak akkor, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása (NAIH, 2016).

Ami a *referencia-ellenőrzés* gyakorlatát illeti: egy új munkáltató előzetes tájékoztatás, és az arra adott munkavállaló hozzájáruló nyilatkozata hiányában nem jogosult megkeresni a korábbi munkáltatót azért, hogy információkat gyűjtsön a jelentkezőről. Mindazonáltal a hozzájárulás megadásakor is előfeltétel a törvényes cél megléte (az általános információgyűjtés nem elégséges), ellenkező esetben jogellenes adatkezelés valósul meg (NAIH/2016/4386/2/V).

Végül egy talán széles körben ismert tény: a kiválasztási eljárásban tilos a *poligráfos vizsgálat alkalmazása.* Az EBH2013. M.9. számú ügyben a Kúria megerősítette ezt az álláspontot, és rögzítette, hogy ez a fajta mérés még a munkavállaló beleegyezése esetén is személyiségi jogi jogsértést valósít meg, ezáltal sérelemdíj iránti igényt alapozhat meg.

A munkaerő-ellátási feladatlánc egyik lényeges, a munkáltatói márka megítélésére is komoly hatást gyakorló eleme a jelöltek számára történő visszajelzés. A jelentkezők információs önrendelkezési jogát az biztosítja a legmagasabb szinten, ha *visszajelzést kapnak* arról is, ha a munkáltató nem őt választotta az adott állásra. A NAIH (2016) álláspontja szerint a munkáltató részéről nem fogadható el az a gyakorlat, ha például az álláshirdetésben kiköti, hogy amennyiben az adott jelentkező nem kap külön értesítést, akkor a munkáltató nem vette fel a jelentkezőt az adott állásra.

Az álláshirdetésekre beérkezett önéletrajzok, pályázatok megőrzése kapcsán a NAIH (2016) arra az álláspontra

helyezkedett, hogy ha a munkáltató a jelentkezők közül kiválasztott egy személyt a meghirdetett állásra, akkor megszűnt az adatkezelés célja és az Infotv 17. § (2) bekezdés d) pontja alapján a ki nem választott jelentkezők személyes adatait törölni kell. Fennáll a törlési kötelezettség abban az esetben is, ha az érintett még a jelentkezés során meggondolja magát és visszavonja pályázatát. A NAIH (2016) és az Európa Tanács (2015) szerint az a jó gyakorlat a munkáltató részéről, ha a megőrzéshez a jelentkezők hozzájárulását kéri a felvételi eljárás lezárását követően úgy, hogy egyben megjelöli az adatkezelés célját és várható időtartamát.

A munkavállalók ellenőrzésére vonatkozó szabályok

A munkaviszony akkor tudja betölteni rendeltetését, ha a felek megfelelően tudják benne gyakorolni jogaikat és teljesíteni kötelezettségeiket. A munkáltatónak a munkavégzéshez szükséges irányítás nemcsak joga, hanem kötelezettsége is, tehát úgy kell a munkát szerveznie, hogy a munkavállaló munkáját megfelelően elláthassa. Ebben az alá- és fölérendeltségi jogviszonyban a munkáltatói jog körében tehát megjelenik az ellenőrzéshez való jog is, amelynek lényeges korlátja az Mt. 11/A. § (1) bekezdésének első mondata, amely szerint a munkavállaló csak a munkaviszonnyal összefüggő magatartása körében ellenőrizhető.

A legtöbb általam elemzett döntés a munkavállalók *kamerás megfigyeléséhez* kapcsolódott. Összhangban az Mt. 11/A. §-sal, mind az AB határozatból, mind a NAIH (NAIH-4001-6/2012/V) ajánlásából kiderül, hogy tilos a kamerás megfigyelés, az alábbi esetekben:

a. ha a kamera kizárólag egy munkavállalót és az általa végzett tevékenységét figyeli meg, ugyanis jogellenesnek tekinthető az olyan elektronikus megfigyelőrendszer alkalmazása, amelynek célja a munkavállalók munkahelyi viselkedésének a befolyásolása,
b. amennyiben a megfigyelés az emberi méltóságot sértheti (így különösen az öltözőkben, zuhanyzókban, az illemhelyiségekben vagy orvosi szobában, és az ahhoz tartozó váróban),
c. olyan helyiségben, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve (ez alól kivétel, ha van a helységben védendő tárgy, például étel-ital automata),
d. ahol a kamerás megfigyelés célja más, személyiségi jogok gyakorlását kevésbé korlátozó módszerrel (például biztonsági őr) is megvalósítható (1805/A/2005–3).

Ugyanakkor, ha a munkahely területén jogszerűen senki sem tartózkodhat (munkaidőn kívül vagy a munkaszüneti napokon), akkor a munkahely teljes területe (öltözők, illemhelyek, munkaközi szünetre kijelölt helyiségek) megfigyelhető. A munkáltató elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmazhat, közterület megfigyelésére nem.

A kamera alkalmazásához nem szükséges a munkavállalók hozzájárulását beszerezni, ugyanakkor a munkavállalókat erről előzetesen és írásban kell tájékoztatni (melyik kamerát milyen célból helyezte el, milyen területre irányul), továbbá írásos tájékoztatást kell adni az adatkezelés részleteiről is (részletesen lásd: ABI–2962/2010/P és NAIH, 2016). A rejtett kamera alkalmazása főszabályként tilos, ugyanakkor kivételesen, büntetőeljárásban az eset összes körülményének függvényében indokolt lehet (EBH2000. 296.). Végül lényeges, hogy a munkáltatónak ki kell kérnie az üzemi tanács véleményét azoknak a technikai eszközöknek az alkalmazásáról, amelyeket az ellenőrzés során igénybe vesz [Mt. 264. § (1) bek. *d)* pont].

A Rendelet fogalommeghatározásai alapján a munkahelyi *e-mail-fiók,* a munkavállaló rendelkezésére bocsátott *laptop*, illetve *telefon* adattartalma személyes adatnak, a személyes adaton elvégzett bármely művelet pedig adatkezelésnek minősül (továbbiakban ezeket az eseteket egyben vizsgálom). Ezért a munkáltatónak egy belső szabályzatot célszerű megalkotnia az e-mail-fiókok, számítástechnikai eszközök használatának, ellenőrzésének szabályairól, amelyben kitér arra, hogy használható-e magáncélokra az e-mail-fiók, illetve számítástechnikai eszköz (és ha igen, akkor milyen adatokat engedélyez és melyeket nem), melyek a biztonsági másolat készítésének szabályai, valamint melyek az e-mail-fiók és a számítástechnikai eszközök használatának részletes ellenőrzési szabályai (NAIH/2019/769/).

A NAIH továbbiakban ismertetett állásfoglalását a korábban részletezett Bărbulescu-tesztre tekintettel alakította ki. E szerint az ellenőrzés első lépéseként az e-mail-cím és a levél tárgyának az ellenőrzése is elegendő lehet, hiszen bizonyos esetekben már ebből is lehet látni azt, hogy az e-mail magáncélú-e. (Ha a munkáltató nem engedélyezi az e-mail-fiók magáncélú használatát, és az ellenőrzés pusztán arra terjed ki, hogy megállapítsa azt, hogy a munkavállalók betartották-e ezt a munkáltatói rendelkezést, akkor szintén elegendő az e-mail-cím tárgyának megtekintése.) A kialakult adatvédelmi gyakorlat szerint a munkáltató rendes körülmények között nem jogosult az e-mail-fiókban tárolt magánjellegű e-mailek tartalmát ellenőrizni még akkor sem, ha az ellenőrzés tényéről előzetesen a munkavállalókat tájékoztatta. Ezt követően kerülhet sor az e-mail-fiók használatának következő szintje szerinti, részletesebb ellenőrzésére, az e-mailek tartalmának ellenőrzésére. Főszabályként az ellenőrzés során biztosítani kell a munkavállaló jelenlétét. Ha ez nem lehetséges, akkor azonban egyrészt tájékoztatást kell nyújtani a munkavállaló számára a tervezett munkáltatói intézkedésről, másrészt lehetőséget kell biztosítani arra, hogy helyette meghatalmazottja vagy képviselője jelen legyen. Amennyiben ezek egyike sem lehetséges, akkor független harmadik személy bevonásával is hozzá lehet férni az e-mail-fiókhoz.

A *laptop* adattartalmának ellenőrzése esetén visszautalunk a Libert ügyben korábban kifejtettekhez: amennyiben a munkáltató engedélyezi a laptop magáncélú használatát, akkor a laptop merevlemezén a munkavállalónak szükséges azt egyértelmű jelzéssel elkülönítenie,

hogy mely adatok a személyes adatai. Ugyanis mind a laptopról készített biztonsági mentés során, mind a laptop ellenőrzése során a munkáltatónak kiemelt figyelmet kell fordítania arra, hogy a munkavállalók magánélettel kapcsolatos személyes adatait nem kezelheti.

A *munkahelyi telefonhasználat* ellenőrzését, a hívás-lista alkalmazását ellehetetleníti, hogy a hívott fél neve és telefonszáma is személyes adat, s míg a munkavállaló előzetes hozzájárulása beszerezhető, a hívott harmadik személyeké nem. Ezért ha a céges telefon magáncélra is használható, akkor a NAIH (2016) jó gyakorlatnak tekinti azt, ha a kimenő hívások két előhívóval vehetők igénybe: az egyik előhívó a hivatalos, a másik a magáncélú hívások során használható. A hivatalos hívások adatait a munkáltató megismerheti, a magáncélú hívások adatait nem. A telefonbeszélgetések lehallgatása tilos.

Amennyiben a munkáltató szabályzatban előre meghatározza, hogy mely honlapok megtekintését blokkolja a munkáltató informatikai rendszere, akkor ezzel jelentősen csökkenteni lehet annak esélyét, hogy az *internethasználat ellenőrzésére* egyáltalán sor kerüljön (Adatvédelmi munkacsoport, 2014; NAIH, 2016). Jó gyakorlat, ha a munkáltató ugyanebben a szabályzatban azt is rögzíti, hogy milyen munkáltatói érdekek miatt kerülhet sor az internethasználat ellenőrzésére, ki jogosult az ellenőrzés elvégzésére, azt milyen szabályok szerint lehet lefolytatni (fenti fokozatosság elvének betartása mellett), valamint milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak az ellenőrzés kapcsán. Ha a munkavállaló a tilalom ellenére magáncélból használja munkaidőben az internetet, az munkáltatói azonnali felmondást (BH2006. 64.) alapja lehet.

A *GPS navigációs rendszer* által tárolt adat a gépjárművet vezető személyes adatának is minősül, minthogy annak alapján következtetéseket lehet levonni a munkavállalóra (például mikor, milyen útvonalon haladt a munkavállaló, mennyi idő alatt milyen távolságot tett meg). A GPS alkalmazását ezért logisztikai célból javasolja alkalmazni a NAIH (2016), vagyis annak a jármű helyzetének a meghatározására kell szolgálnia, nem pedig a munkavállaló követésére. Ennek fényében elfogadható a munkáltató részéről az, ha a rendszer alkalmazásának célja, hogy egyes munkakörök (futár vagy fuvarozó) esetében hatékonyabban szervezze meg a munkafolyamatokat, vagy ha a gépjármű szállítmánya vagy maga a gépjármű, annak értéke ezt kifejezetten indokolja. Jogszerűen alkalmazható GPS akkor is, ha a munkavállalók életének, testi épségének a megóvása a cél (például konfliktuszónán keresztül történő szállítás esetén). Ezek alapján egyértelmű: a munkaidőn kívüli időszakban, vagy az otthoni munkavégzés idején történő nyomon követés, mivel adatkezelési célja nincs, jogellenes. Az adatvédelmi biztos továbbá olyan kapcsolóberendezés használatát javasolja, amely megakadályozza a munkavállaló magánéletének ellenőrzését (1664/A/2006–3).

Az Mt. 52. § (1) bekezdése kifejezetten előírja, hogy a munkavállaló köteles a munkáltató által előírt helyen, időben és munkára alkalmas állapotban megjelenni, a munkáltató kötelezettségei között pedig szerepel a biztonságos munkavégzés körülményeinek megteremtése (Mt. 51. §). Ebben a körben merülhet fel, hogy a munkáltató jogosult *alkohol- vagy drogtesztet alkalmazni a munkavállalók körében*. A Legfelsőbb Bíróság már 1999-ben kimondta, hogy a munkáltató kizárhatja a munkahelyi alkoholfogyasztást (LB Mfv. I. 10.939/1999) és e szabály megszegése esetén a rendkívüli felmondás is jogszerű (Mfv. E. 10.741/2002/1). Az MK 122. számú állásfoglalása pedig azt is rögzíti, hogy ha a munkavállaló az alkoholtól befolyásolt állapotának ellenőrzésére irányuló vizsgálatot megtagadja, ez önmagában is alkalmas lehet hátrányos jogkövetkezmény alkalmazására. A közreműködést megtagadó munkavállaló a munkavégzéstől eltiltható, és emiatt jogszerű a munkabérének a megvonása is az eltiltás időtartamára. Az alkoholos befolyásoltság ellenőrzése azonban nem sértheti az érintett személyiségi jogait, az ellenőrzési jog gyakorlása nem lehet rendeltetésellenes (így nem lehet sem általános vagy naponta többszöri gyakorlat, valamint arra jogosult személy kell hogy elvégezze, vagyonőr nem). Ennek biztosítására célszerű az érdekmérlegelési teszt előzetes elvégzése.

A kábítószer-fogyasztásra vonatkozó személyes adatok különleges adatoknak minősülnek, így az adatkezeléshez szükséges a törvény kifejezett rendelkezése vagy az érintett önkéntes, egyértelmű, tájékozott beleegyezésen alapuló írásos felhatalmazása. Az irányadó bírói gyakorlat értelmében az önhibából eredő kábítószer-fogyasztás következtében előállt zavart állapot önhibából eredő bódult állapotnak minősül (BH2000. 432.). A munkavállalók alkoholos befolyásoltságának témájában kialakított, a kábítószer-fogyasztásra analógiával alkalmazható gyakorlat szerint a munkáltatói ellenőrzésben való közreműködés a munkavállaló munkaviszonyból eredő kötelezettsége (MK 122. számú állásfoglalás). A drogtesztet csak megfelelő végzettséggel rendelkező személy irányítása alatt lehet végezni.

Következtetések, lehatárolások és további kutatási irányok

Az adatvédelem, a munkajog és az emberierőforrás-menedzsment közös metszetét vizsgáló tanulmány szakirodalmi áttekintése alapvetően a tárgykör európai és magyar jogforrási rendszerének áttekintését tartalmazza. A feltárt források között azonban nincs olyan, amely kifejezetten a munkaviszonyban alkalmazott HRM-gyakorlatok számára nyújtana egyértelmű iránymutatást, így szükségét láttam annak, hogy feltárjam az esetjogban született döntéseket. Az empirikus kutatás az Európai Unió Bírósága, de főként az Emberi Jogok Európai Bírósága, valamint a magyar bíróságok és adatvédelmi hatóság(ok) döntéseit vizsgálta. Mivel a témakör széles, a dokumentumelemzést leszűkítettem a szervezetek toborzási és kiválasztási tevékenysége, illetve a munkavállalók munkaviszonyhoz kapcsolódó ellenőrzése során felmerülő adatvédelmi szituációkra.

Az eredmények alapján meglehetősen tiszta kép rajzolódik ki arra vonatkozóan, hogy a HR szakmai gyakorlatait mely pontokon szükséges illeszteni az új adatvédel-

mi elvárásokhoz. Az EJEB döntéseiből kiinduló, de azt tovább gondoló NAIH-döntésekből és állásfoglalásokból összefoglalóan az alábbi megállapítások tehetők.

A munkavállalók személyes adatainak kezelése során a munkáltatónak mindig figyelemmel kell lennie az adatvédelem alapvető elveire, függetlenül attól, hogy milyen technikát alkalmaz (telefon, e-mail, laptop, internet, kamera, internet, közösségi oldalak) a jelöltek vagy a munkavállalók mérésére, vagy ellenőrzésére vonatkozóan. Sőt, az analóg és az elektronikus közlések is ugyanolyan megítélés alá esnek.

Az adatkezeléshez szükséges jogalap kiválasztásakor a munkavállaló jóváhagyása nem lesz megfelelő, kivéve, ha azt a munkavállalók vagy jelöltek hátrányos következmények nélkül visszautasíthatják (például önéletrajz és pályázati anyagok megőrzése). Esetenként hivatkozni lehet a szerződés teljesítésére vagy a jogos érdekre, feltéve, hogy az adatkezelés a törvényes cél érdekében feltétlenül szükséges, és megfelel az arányosság elvének. Amennyiben valamely adatkezelésre nincs jogszabályi kötelezettség, túlmutat a munkaszerződés teljesítésén, és elsősorban a munkáltató érdekkörében merül fel az adatkezelés szükségessége, az érdekmérlegelés lehet a megfelelő jogalap.

A jelölt és a munkavállaló mindig csak a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, a jelölt és a munkavállaló magánélete ugyanakkor védett.

Az állásra jelentkezőknek és a munkavállalóknak érdemi és előzetes tájékoztatást kell nyújtani az alkalmazott alkalmasság-vizsgálatról, megfigyelésről, vagy ellenőrzésről, ugyanakkor nem szükséges tőlük ezek elvégzéséhez előzetes hozzájárulást kérni.

A munkavállalók munkaviszonnyal kapcsolatos ellenőrzése során a Bărbulescu-teszt lépései és a fokozatosság elve szerint kell eljárnia a munkáltatónak.

Végül célszerű a munkáltatónak belső szabályzatot alkotnia a számítástechnikai eszközök munkahelyi használatának és ellenőrzésének szabályairól. Ebben érdemes részletesen meghatározni, hogy használható-e magáncélokra az adott eszköz, ha igen, akkor milyen adatok engedélyezettek és melyek nem. Amennyiben a magáncélú használatot a munkáltató engedélyezi, úgy ezeket az adatokat milyen jelzéssel (például: „Magán" és pontosan hol) kell a munkavállalónak ellátnia és tárolnia, továbbá hogy melyek a biztonsági másolat készítésének szabályai; mely honlapok látogathatók munkaidőben; valamint melyek az e-mail-fiók és számítástechnikai eszközök használata ellenőrzésének részletes szabályai.

Felhasznált irodalom

Adatvédelmi munkacsoport (2014). *06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról.* WP 217, Brüsszel.

Adatvédelmi munkacsoport (2017). *2/2017. sz. vélemény a munkahelyi adatkezelésről*, WP 249, Brüsszel.

Állam- és Jogtudomány Különszám (2017). Az Európai Emberi Jogi Egyezmény 25 éve Magyarországon. *Állam- és Jogtudomány, 58*(4).

Balogh Zs. Gy. (1998). *Jogi informatika.* Budapest – Pécs: Dialog Campus.

Balogh Zs. Gy (2011). Közterületi térfigyelés és adatvédelem. *Vezetéstudomány, 42*(5), 26-35.

Bankó, Z. (2015). A munkáltatói hatalom korlátai a munkaviszony megszüntetése során – a felmondási tilalmak és korlátozások a magyar munkajogban. *JURA, 21*(2), 5-10.

Bankó Z. & Szőke G. (2016). *Issues of the Digital Workplace: Situation in Hungary.* Budapest: JurInfo Kiadó.

Barakonyi, E. (2013). Az életkor szerepe a munkajogi szabályozásban. *HR és Munkajog*, 3, 47-52.

Bennett, C. J. & Grant, R. (1998). *Visions of Privacy: Policy Choices for the Digital Age* (Studies in Comparative Political Economy and Public Policy). Toronto: University of Toronto Press.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). *Review of the European Data Protection Directive*. Santa Monica, CA: RAND Corporation.

Európai Bizottság (2012). *Sajtóközlemény. IP/12/46*. Brüsszel.

Európai Unió Alapjogi Ügynöksége és az Európa Tanács (2019). *Európai adatvédelmi jogi kézikönyv 2018. évi kiadás*. Luxemburg: Az Európai Unió Kiadóhivatala.

Európa Tanács 108. számú Egyezménye (1989). *Az egyének védelméről a személyes adatok gépi feldolgozása során és a CETS 223-as számú jegyzőkönyv által módosított Korszerűsített 108. Egyezmény (2015)*. Brüsszel.

Európa Tanács (2015). *Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.* Retrieved from https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

Farkas, F., Jarjabka Á., Lóránd, B., & Bálint, B. (2013). Munkahelyi motivációk Magyarországon 2013-ban. *Vezetéstudomány. 44*(10), 12-23.

Hrportal.hu (2017). *Ítélet született a munkahelyi levelezésről.* Retrieved from https://www.hrportal.hu/hr/itelet-szuletett-a-munkahelyi-levelezesrol-20170905.html

Hegedűs B. (2013). Az adatvédelmi jog általános tanai. In Tóth András (ed.) (2013), *Infokommunikációs jog II.* (pp. 137-145). Budapest: Patrocínium.

Hegyeshalmi R. (2017). *A munkáltató csak akkor figyelheti meg a levelezést, ha az alkalmazottak tudnak róla.* Retrieved from https://index.hu/tech/2017/09/05/a_munkaltato_csak_akkor_figyelheti_meg_a_levelezest_ha_az_alkalmazottak_tudnak_rola/

Jarjabka, Á. & Lóránd, B. (2010). *Az innováció alapjai és megjelenési területei*. Pécs: Pécs-Baranyai Kereskedelmi és Iparkamara.

Jay, R. & Hamilton, A. (1999). *Data Protection. Law and Practice*. London: Sweet & Maxwell.

Jóri A. (2005). *Adatvédelmi kézikönyv.* Budapest: Osiris Kiadó.

Jóri A. (2009). *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése.* Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola.

Kállai P. (2017). Magán- és családi élet tiszteletben tartásához való jog Bărbulescu Románia elleni ügye. *Fundamentum, 2017*(3-4), 99-114. Retrieved from http://epa.oszk.hu/02300/02334/00073/pdf/EPA02334_fundamentum_2017_03-04_099-114.pdf

Karoliny M-né, Ásványi Zs., & Bálint B. (2017). Erőforrás-biztosítási rendszerek: toborzás, kiválasztás, beillesztés és leépítés. In Karoliny M-né, & Poór J. (eds.), *Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások* (pp. 165-202. Budapest: Wolters Kluwer.

Kiss Gy (2001). *Az Európai Unió munkajoga*. Budapest: Osiris Kiadó.

Kiss, Gy (2020). *Munkajog (kézirat).* Budapest: Dialóg Campus Kiadó.

Korff, D. (2002). *EC study on implementation of data protection directive comparative summary of national laws*. Colchester, UK: Human Rights Centre University of Essex.

Majtényi, L. (2003). Az információs jogok. In Halmai, G. & Tóth G. A. (eds.), *Emberi jogok* (pp. 580-636). Budapest: Osiris Kiadó.

Majtényi L. (2006). *Az információs szabadságok.* Budapest: Complex Kiadó.

Majtényi L. (2010). *Információs és médiajog I*. Budapest: Bíbor Kiadó.

Mayer-Schönberger, V. (1997). *Generational Development of Data Protecton in Europe. Technology and Privacy: the new landscape, 1997*(1), 219-241. Retrieved from https://dl.acm.org/doi/10.5555/275283.275292

Mészáros, J (2017). *Adatvédelem a XXI. században és az internet világában* (PhD-*értekezés*). Szeged: Szegedi Tudaományegyetem. Retrieved from http://doktori.bibl.u-szeged.hu/3998/1/Meszaros_Janos_ertekezes.pdf

NAIH Tájékoztató (2016). *A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről.* Retrieved from https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

Nepszava.hu (2017). *Tudta? - A munkahelyi levelezését nem „kukkolhatja" a főnök.* Retrieved from https://nepszava.hu/1139620_tudta-a-munkahelyi-levelezeset-nem-kukkolhatja-a-fonok

OECD Iránymutatás (2013). *Az adatvédelemre és az országhatárokat átlépő személyesadat-áramlásra vonatkozó iránymutatások*. Párizs: OECD.

Poór J., Balogh G., Bálint B., Dobay P., & Kollár Cs. (2017). Integrált és integráló EEM-rendszerek és eszközök. In Karoliny M-né, & Poór J. (eds.), *Emberi erőforrás menedzsment kézikönyv - Rendszerek és alkalmazások* (pp. 359-392). Budapest: Akadémiai Kiadó (Wolters Kluwer).

Rózsavölgyi B. (2018). Mikor lehet jogszerű a munkáltató ellenőrzése? – az Emberi Jogok Európai Bírósága Nagykamarája Bărbulescu kontra Románia ügyben hozott ítéletének iránymutatásai. *Munkajog, 2*(1), 43-48.

Sipka P. & Zaccaria M. L. (2018). A munkáltató ellenőrzési joga a munkavállaló munkahelyi számítógépén tárolt magánadatai fölött. *Munkajog, 2*(2), 45-49. Retrieved from http://real.mtak.hu/100072/1/Munkajog%2020182.pdf

Sólyom L. (1983). *A személyiségi jogok elmélete.* Budapest: Közgazdasági és Jogi Könyvkiadó.

Szőke G. L. (2013). Az adatvédelem szabályozásának történeti áttekintése. In *Infokommunikációs és Jog, 10*(3), 107-112. Retrieved from https://infojog.hu/szoke-gergely-laszlo-az-onszabalyozas-audit-es-tanusitas-lehetosegei-es-korlatai-az-adatvedelem-teruleten-20141-57-14-20-o/

Szőke G. L. (2014). *Adatvédelem és önszabályozás. Adatvédelmi irányítási rendszer az adatkezelőnél* (Doktori értekezés). Pécs: PTE ÁJK.

Warren, S. D. & Brandeis, L. D (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. Retrieved from http://links.jstor.org/sici?sici=0017-811X%28189001215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Vizsgált európai ügyek:

Bărbulescu kontra Románia (2017). 61496/08. sz. ügy

Copland kontra Egyesült Királyság, (2007). 62617/00. sz. ügy

Halford kontra United Kingdom ügy (1997). 20605/92 sz. ügy

Köpke kontra Németország (2010). 420/07. sz. ügy

Libert kontra Franciaország (2018). 588/13. sz. ügy

López Ribalda és társai kontra Spanyolország (2019). 1874/13 & 8567/13 sz. ügyek

Worten ügy (2013). C-342/12. sz. ügy

Lindqvist ügy (2003). C-101/01. sz. ügy