

A Nagytestvér – néhány gondolat

Néhány „hétfő reggeli gondolat” arról, hogy manapság milyen jogok illetik meg a munkáltatót, hogy alkalmazottai munkahelyi tevékenységébe bepillantást nyerjen.

Tárgyszavak: munkáltatói jog; Adatvédelmi Törvény (DPA); Emberi Jogi Törvény (HRA); Ellenőrző Szervek Szabályozásáról Szóló Törvény (RIPA).

RIPA 2K + HRA 98 + DPA 98 = Zavar 03

Hétfő reggel van, amikor ezt a cikket írom. Ez a hétfő reggel is olyan, mint a többi, ha figyelembe vesszük, hogy ugyanolyan kihívásoknak nézek elébe, mint a hét első napján bármikor, de ezt tetőzi még a péntek délutánról maradt befejezetlen munka is. Egy olyan nap reggele a mai, amikor legszívesebben egyedül dolgoznék csöndben és zavartalanul.

Ennek ellenére nem egyszer megzavartak. A recepciósök üzenetet hagytak egy telefonhívással kapcsolatban, amelyet még pénteken szasztottam el, a főnököm (aki jelenleg egy szinttel felettem dolgozik) szó szerint beszélni akart velem a tarifákról, valamint felhívott egy piacutató cég, hogy érdekelne-e egy ahhoz hasonló számítógép, amelyet kb. egy hónappal ezelőtt rendeltem interneten keresztül.

Ezek után megkérdezhetnék, hogy mi köze van mindennek az IT-hez vagy az ember magánélethez. Kis utánajárással kiderítettem, hogy mindhárom alkalommal technikai eszközök tették lehetővé, hogy az illető személyek megtudják, hol vagyok. A recepciósök onnan tudta, hogy az irodában vagyok, hogy aznap reggel már kezdeményeztem egy hívást. A főnököm egy általam elolvasott levél révén kapta a visszaigazolást, tehát ő is így tudta meg, hogy beszélhet velem, a komputercég pedig egy on-line formula segítségével jutott hozzá az adataimhoz.

Visszatekintve úgy tűnik, hogy elég könnyű volt megtalálni engem. Ha tovább nézzük a kérdést, gyakorlatilag bármilyen szervezet vagy cég a technológiai eszközök révén rendelkezik az adataimmal, tudja, hogy hol vagyok és mit csinálok.

A legtöbb emberhez hasonlóan én is fel vagyok háborodva egy pillanattal. „Nagytestvér!” kiáltok fel. Ennek ellenére nem kereshetek „kibúvót”, mivel ez nem azt jelenti, hogy mostantól nem fogok számítógépet rendelni a komputercégtől (de tény, hogy ők fogják a legjobban tudni, hogy mire van szükségem). Egy megjegyzés jut most eszembe: Nagyon is értékeljük a saját magánéletünket, magánszféránkat, de csak annyira, amennyibe egy babkonzerv kerül. Ami engem illet, egyetértek ezzel a kijelentéssel (azért annyiban módosítanám, hogy ez nem áll ám akármilyen fajta babkonzervre – csak a Heinz-re).

Mindenki ilyen nyugodt, amikor a magánéletéről van szó? Talán nem. A Reuters legutóbbi felmérése szerint több mint 9000 európai polgár úgy vélekedik, hogy nincs elegendő védelem a személyes adatok hozzáférhetőségét illetően, főleg az interneten való megjelenés aggasztja őket. Mindemellett Nagy-Britannia, Finnország, Ausztria és Svédország az Európai Bizottság felé továbbította álláspontját, amely szerint az Adatvédelmi Törvényt módosítani szeretnék, hogy könnyebb legyen Európán kívüli országokba személyes adatokat szolgáltatni, valamint az adatellenőrzés gátjait is némileg oldani szeretnék, amivel a személyiségi jogok nem sérülnek, viszont az adatfeldolgozás könnyebbé válik. Ha a munkahelyi körülményeket vesszük figyelembe, úgy tűnik, hogy a munkaadók 80%-a ellenőrzi alkalmazottait e-mail és internethasználat közben. Ezért aztán úgy tűnik, hogy a cégek és munkaadók ellenőrizni akarják tevékenységünket, valamint több okból is hozzá akarnak férni információkhoz, ezzel egyidejűleg pedig az alkalmazottak magánéletük biztonságát féltik.

Mindez különösen időszerű, mivel a Munkavállalói Adatvédelmi Törvény 3. részének módosított változata hozzáférhető az informatikai megbízott honlapján. A törvénykönyv az az 1998-as Adatvédelmi Törvény (Data Protection Act = DPA) gyakorlati alkalmazását segíti. A 3. részben pedig segítséget kíván nyújtani abban, hogy a munkaadók törvényesen mennyiben ellenőrizhetik (akár CCTV – Closed Circuit Television – kamerával, akár interneten vagy e-mailen keresztül) alkalmazottaik munkahelyi tevékenységét.

Miért fontos az ellenőrzés?

Manapság, sokkal inkább mint valaha, a munkaadónak meg kell győződnie arról, hogy alkalmazottai megfelelően viselkednek a munkahelyen. Már-már közhelynek számít, hogy egy munkaadó felelős alkalmazottai munkahelyen folytatott tevékenységéért, de ezzel a ténnyel

mindinkább számot kell vetni az információs technológia széleskörű fejlődésével, és munkahelyi alkalmazásával.

Ha az alkalmazottak obszcén képeket nézegetnek a munkahelyen (pornográfia), vagy munkatársaikat e-mailen keresztül zaklatják, vagy rágalmazzák, a felelősség a munkaadót terheli, ezért résen kell lennie. Ez nem csak azt jelenti, hogy az alkalmazottak munkahelyi tevékenységét ellenőrzi, hanem arra is kiterjed, hogy „meg kell ismernie” alkalmazottját.

Másfelől viszont az alkalmazottat is megilleti az a jog, hogy magán-szféráját bizonyos fokig tiszteletben tartsák valamint, hogy a munkahelyén autonómiát élvezzen. Az igaz, hogy az alkalmazottak és munkaadók közötti viszony meglehetősen kényes: kölcsönös megbecsülés és bizalom nélkül nem lehet együtt dolgozni, ezért a túlzott ellenőrzés a munkaadó részéről lehetetlenné teheti a munkafolyamatokat.

Ha figyelembe vesszük az Adatvédelmi Törvény (DPA) által a munkavállalóknak biztosított jogokat, és az 1998-as Emberi Jogi Törvény (HRA) az előbb említett törvény illetve a „bizalmasság” homályos kifejezésének értelmezésére kifejtett hatását, egyértelműen arra a következtetésre juthatunk, hogy a munkaadót a legkevésbé sem kívánatos jogok illetik meg az alkalmazottak ellenőrzésére.

Az ellenőrzés területe meglehetősen összetett, de az egymással versengő célok világosak. Ugyan a célok sokszor ellentmondásosak, és egyúttal a jogi keret is meglehetősen összetett. Az előbbi tényező tehát tovább bonyolítja a másodikat.

A jogi összefüggés

A jogi keret ebben a kérdéskörben az ellenőrzők és az ellenőrzöttek egymással versengő érdekeit és céljait tükrözi. Mindazonáltal vezet út ezen a mocsáron keresztül is, ha óvatosan lépkedünk.

Az Ellenőrző Szervek Szabályozásáról Szóló Törvény (Regulation of Investigatory Powers Act = RIPA), 2000

Az első lépés nem alkalmazható minden helyzetre, de azokban az esetekben, ahol a kommunikáció ellenőrzése bizonyos információk továbbjutásának megakadályozását jelenti, mindezt úgy kell megtenni, hogy a fent említett 2000. évi törvény (RIPA) értelmében ne minősüljön bűnténynek illetve törvénysértésnek.

A RIPA, amelyet 2000. július 27-én fogadtak el, tiltja a kommunikáció megszakítását, kivéve, ha

- a küldő és a fogadó fél is hozzájárult az információ továbbításának megszakításához, vagy
- az információ továbbítását engedélyezte a 2000. évi Telekommunikációs Szabályzat (Törvényes Üzleti Eljárások) (Kommunikáció Megszakítása).

A RIPA-t sokszor olyan törvényként tartják számon, amely a cégek ellenőrzési jogait hivatott korlátozni és szabályozni. Valójában pontosan ennek az ellenkezője igaz. A Malone, Kruslin és a legújabb Khan ügy bebizonyította, hogy pl. a rendőri szervek nyomozó ellenőrzése jogos és törvényes a hazai törvények alapján. Ha ez az igen fontos alap nem lenne meg, bármely ellenőrzés jogtalan volna, még akkor is, ha nem volna egy kifejezetten rá vonatkozó törvény.

Ennek értelmében a RIPA ezt a jogi alapot kell, hogy biztosítsa, amelynek révén a közszervek ellenőrzést eszközölhetnek.

A Törvényes Üzleti Eljárások Szabályzat 2000. október 24-én lépett életbe és lehetővé teszi, hogy a munkaadók a küldő és fogadó felek hozzájárulása nélkül törvényesen rögzítsék a kommunikációt, amely személyes telekommunikációs rendszereken belül folyik, az alábbi szituációkban, hogy:

- a munkaadó igazolja az üzletmenethez kapcsolódó információk és tények meglétét,
- meggyőződjön arról, hogy az alkalmazottak betartják az üzleti szabályokat,
- meggyőződjön arról, hogy a telekommunikációs rendszert használó ellenőrzött személyek betartják-e a szabályokat,
- megakadályozhasson illetve felderíthessen egy törvénysértést,
- biztosíthassa a telekommunikációs rendszer hatékony működését vagy
- felfedezhesse ill. felderíthesse, hogy kik használják jogosulatlanul a telekommunikációs rendszert.

A Törvényes Üzleti Eljárások Szabályzat azt is lehetővé teszi, hogy egy adott cégnek joga van a kommunikációt törvényesen ellenőrizni (de nem rögzíteni), illetve azt vizsgálni, hogy a kommunikáció mennyiben üzletszerű.

Ez gyakorlatilag azt jelenti, hogy a hangüzeneteket és az e-mail-rendszer postafiókjait ellenőrizni lehet az alkalmazott távolléte esetén.

Annak érdekében, hogy a Törvényes Üzleti Eljárások Szabályzat jogi alapot biztosíthasson a telekommunikációs folyamatok megszakításá-

hoz ellenőrzés céljából, az adott cégnek minden esetben mindent meg kell tennie azért, hogy a telekommunikációs rendszert használó alkalmazottak tudomására hozza, hogy ellenőrzésre számíthatnak. Ez annyit tesz, hogy a munkavállalóknak tudniuk kell, hogy a hívásaikat ill. levelezésüket ellenőrizhetik, valamint amennyiben lehetséges, a cég lehetséges vagy gyakori partnereit is tájékoztatni kell erről.

Ennek értelmében, csak akkor legális a telekommunikációs eszközök ellenőrzése, ha megfelel a RIPA ill. a Törvényes Üzleti Eljárások Szabályzat előírásainak.

Az Adatvédelmi Törvény 1998

Telefonbeszélgetéseket véve alapul, nyilvánvaló, hogy az ellenőrzés, nyomkövetés során információt rögzíthetünk létező, beazonosítható személyekről. Ennek értelmében az ellenőrzésnek itt is meg kell felelnie a RIPA, a Törvényes Üzleti Eljárások Szabályzat, valamint a DPA (Adatvédelmi Törvény) előírásainak.

A DPA szempontjai szerint a telefonbeszélgetés során rögzített információ ugyanolyan információnak minősül, mint más „adat”, olyan berendezés rögzíti, mint bármely más elektronikus adatot. Ennek megfelelően, ha bizonyos információt lehallgatnak egy másik telefonon keresztül, az nem minősül adatnak – a DPA szerint. Ha viszont rögzítve van, akkor annak minősül.

A telefonbeszélgetés során elhangzott információ akkor minősül személyes jellegűnek (és ezáltal a DPA által szabályozottnak), ha az az adat egy élő, beazonosítható személyhez kapcsolódik. Nagyon fontos figyelembe venni, hogy a DPA értelmében már a beazonosítható hangok mindkét telefonáló részéről is személyes adatnak minősülnek, tekintet nélkül arra, hogy mi hangzott el a beszélgetés során és mi került rögzítésre. Például lehet, hogy maga a beszélgetés nem elég bizonyíték egy alkalmazott kilétére, de ha egy felügyeleti személy, vagy a telefonvonalat figyelő illetékes felismeri az alkalmazottat és be tudja azonosítani, akkor a felvett beszélgetés máris személyes adatnak minősül.

Mindennek annyiban van jelentősége számunkra, hogy ahol személyes információk kerülnek ellenőrzésre és rögzítésre, ott az adott cég is meg kell, hogy feleljen a DPA előírásainak.

A DPA szempontjából a munkaadó minősül adatellenőrzőnek, és ennek megfelelően a DPA előírásait be kell tartania. A munkaadó legfőbb kötelessége megfelelni az 1. jegyzék 1. alapelvében leírtaknak, azaz, a személyes adatokat törvényesen és igazságosan kezelni.

Az igazságos és törvényes adatkezelés két külön fogalom a DPA értelmezése szerint. A törvényességnek megfelelően (azon túl, amit a szó-kásos értelemben jelent) a személyes adatfeldolgozásnak meg kell felelnie a DPA 2. jegyzékében szabott feltételeknek. Ahol kényes személyes adatok kerülnek rögzítésre, a cégnek mind a 2., mind a 3. jegyzékben leírtaknak meg kell felelnie, leszámítva a kivételeket.

Az igazságosságnak megfelelően, csak akkor igazságos az adatfeldolgozás – leszámítva a kivételes eseteket – ha ennek megtörténte előtt a munkaadó informálja az alkalmazottat ennek lehetőségéről, ezt az 1. jegyzék 2. részének második bekezdése tartalmazza. Ennek tartalmaznia kell a cég profilját, hogy mire szeretnék felhasználni az adatokat és bármi mást, amely szükséges ahhoz, hogy az adatok feldolgozása igazságos legyen.

Ha figyelembe vesszük, hogy a személyes adatok rögzítése egy telefonbeszélgetés során, illetve egy e-mail megszakítása és tartalmának átnézése a DPA fogalmai szerint „adatfeldolgozásnak” minősül, láthatjuk, hogy a telekommunikációs hálózatot használó személyeket minden esetben tájékoztatni kell arról, hogy ellenőrzés folyik, valamint arról is, hogy milyen célból. Azon túl, hogy a munkáltató biztosítja az ellenőrzés törvényes menetét a Törvényes Üzleti Eljárások Szabályzatnak megfelelően, az ellenőrzésnek meg kell felelnie a DPA 2. jegyzékének, illetve ahol szükséges, ott a 3. jegyzéknek is. Ezért tehát ez még tovább bonyolítja a Törvényes Üzleti Eljárások Szabályzat előírásainak betartását.

A Munkavégzést Érintő Adatvédelmi Törvény (the Employment Practices Data Protection Code = the Code)

Mindazonáltal nem elegendő, ha a munkáltatók a törvényt szó szerint értelmezik. Az Informatikai Megbízott éppen most dolgozik a Munkavégzést Érintő Adatvédelmi Törvény 4. részén, amelyet hamarosan törvénybe iktatnak és amely segítségül szolgálhat a munkáltatók számára, akik alkalmazni szeretnék a DPA-t. Jelenleg a törvény 3. része – amely az alkalmazottak ellenőrzésére vonatkozik – még vázlat formájában készült csak el, végleges verziója az év végére (2003) várható.

A munkáltatóknak, ill. a munkáltatók tanácsadóinak azonban óvatosságnak kell lenniük a törvény értelmezésekor, ugyanis nem tesz különbséget aközött, hogy mit követel meg maga a törvény és mi az, amit az Informatikai Megbízott jónak tart. Eszerint ugyanis a munkáltatók súlyosabb követelményeket támaszthatnak (jelentős költségek árán), mint amit a törvény előír. Ezenfelül azt is hozzá kell tennünk, hogy az Infor-

matikai Megbízott szigorúbban értelmezi a DPA-t, mint a bíróság. A Biztos Törvénye legálisan nem kötelező érvényű, tehát a munkáltatók belátásán múlik, hogy mennyiben követik azt.

Mindazonáltal, ha azt vesszük alapul, hogy a Törvény végső verziója nem tér majd el ettől, a következő segítséget meríthetjük belőle:

- A legjobb gyakorlat szerint csakis speciális, erre felhatalmazott személyek végezhetnek ellenőrzést.
- Mielőtt egy cég bármilyen ellenőrzést is végezne, meg kell vizsgálnia az ellenőrzés hatásait és figyelembe kell vennie, hogy alkalmazottai milyen mértékben jogosultak a munkahelyen folytatott magánéleti tevékenységre. A hatások megállapításánál azt is figyelembe kell venni, hogy az ellenőrzés mennyiben segíti az üzletmenetet, nem ártalmas-e. A gyakorlatban mindig azt a módszert kell kiválasztani, amely a cég üzleti érdekeinek szem előtt tartásával a legkevésbé bántó.
- Az ellenőrzés hatásainak vizsgálatát, valamint az ellenőrzésről hozott döntés részleteit dokumentálni kell (ha másért nem is, legalább azért, hogy az Informatikai Megbízott ellenőrzése esetén fel lehessen mutatni).
- Az ellenőrzés hatásainak vizsgálatakor konzultálni kell az illetékes szakszervezetekkel, vagy más alkalmazottakat képviselő testülettel. Fontos megjegyezni ugyan, hogy ez nem kötelező.
- Kerüljük a teljes átvilágítást. A munkáltatóknak azokon a területeken kell elsősorban ellenőrzést eszközölniük, amelyekben erre szükség van annak érdekében, hogy az üzleti célokat el lehessen érni. Az arányosság nagyon fontos szempont, amikor azt vizsgáljuk, hogy mi az, amit feltétlenül szükséges ellenőrizni és mit nem.
- Nagyon fontos, hogy a munkáltató dokumentálja azokat a lépéseket, amelyeket az ellenőrzés végett tesz, valamint fontos, hogy az ellenőrzött alkalmazottak tudjanak arról, hogy milyen céllal vizsgálják munkahelyi tevékenységüket. Általában ennek az a legjobb módja, ha a cég írásos irányelvek, illetve e-mail üzenetek révén tájékoztatja erről alkalmazottait.
- A munkáltatók kerüljék a kizárólagosan üzleti célokat szolgáló ellenőrzés során összegyűjtött magánjellegű információk más célokra történő felhasználását kivéve, ha az információ olyan jellegű, amelyet egy munkáltató sem hagyhat figyelmen kívül. Ez olyan esetekben áll fenn, amikor a rejtett ellenőrzés során rendkívül szabályellenes viselkedést derítenek fel.

- Ezenfelül a munkáltatóknak tiszteletben kell tartaniuk azt az esz- közt, amelyen keresztül megkapják az információt. A CCTV terje- delem, az internet használatáról kapott listák sokszor félrevezetők lehetnek, rosszul értelmezhetőek, pontatlanok vagy szándékosan manipuláltak. Mielőtt az így szerzett információk alapján döntést hozna a munkáltató, mindenképpen esélyt kell adnia a munkavál- lalónak, hogy megcáfolja a bizonyítékokat, illetve magyarázatot adjon az eredményekre.

Az 1998-as Emberi Jogi Törvény (Human Rights Act = HRA)

A fenti kérdéskörben leírtak alapján a jogi helyzet már így is eléggé bonyolultnak tűnik, ezt még tovább bonyolítja, hogy mindezt az Emberi Jogi Törvénynek megfelelően kell vizsgálnunk. A legidegesítőbb kérdés az Emberi Jogi Törvény (HRA) esetében az, hogy vajon lesznek-e hori- zontális hatásai, és ha igen, milyen mértékben.

A HRA 6. bekezdése értelmében törvényellenes cselekedetnek mi- nősül, ha a közhatóságok nem tartják be az egyezmény bármely törvé- nyét. A HRA általánosan közhatóságként definiál minden olyan „jogi személyt...aki olyan funkciót tölt be, amely közösségi jellegű”. Ennek ér- telmében egy személy tevékenysége határozza meg, hogy a HRA érvé- nyes-e az adott szituációban. Mindemellett a HRA arra is kitér, hogy ha az adott szervezet magánjellegű területen nem tartja be a törvényt, vagy elmulasztja annak maradéktalan teljesítését, akkor ebben az esetben nem minősül közhatóságnak.

A kérdés csak az, hogy a magánszektorban alkalmazottak mennyire támaszkodhatnak az Alapvető Emberi és Szabadságjogokról szóló euró- pai konvenció 8. cikkelyében megfogalmazottakra, miszerint vannak bi- zonyos határok arra, hogy egy munkáltató milyen mértékben ellenőrizhe- ti alkalmazottait.

Mindez tisztázatlan marad, bár egyes megfigyelések szerint a bíró- ságok ugyanúgy kezelik a magánszektorban dolgozók, mint a közható- ságok alkalmazottainak eseteit.

A Törvény egyik alappillére az „arányosság”, amely szintén azt mu- tatja, hogy az Informatikai Megbízott a törvény vázlatos megírásakor jo- gosan vette figyelembe a HRA-t.

Kétségtelen, hogy a bíróságoknak és esküdtszékeknek „el kellene olvasniuk és alkalmazniuk kellene a törvényt, méghozzá oly módon, hogy az az egyezmény törvényeivel összhangban legyen, már amennyi-

re ez lehetséges. Egy esküdtszék, illetve bíróság a DPA-t, a RIPA-t egyszerű ésszerűség alapján értelmezné (egy elbocsátási szituációban például), de ezeket az alapelveket is szem előtt tartaná.

Mielőtt az Emberi Jogi Törvény befolyásolná egy munkáltató ellenőrzési jogait, egy munkáltatónak más alapokon kell megindokolnia a jogsértést: mint pld. igazságtalan vagy törvénytelen elbocsátás. Azáltal viszont, hogy az Informatikai Megbízott a HRA-val összhangban próbálta megalkotni a törvényt, a követelményeket „rákényszerítette” olyan privát szektorbeli munkáltatókra is, akik amúgy nem estek volna a törvény hatálya alá.

Ennek értelmében, a munkáltatóknak tekintettel kell lenniük arra a tényre, hogy a kommunikáció ellenőrzésében a szituáció négyszeresen bonyolult és az egyik maga után vonja a másikat. Míg a HRA-t nem lehet egyértelműen alkalmazni a magánszektorban tevékenykedő munkáltatókra, a törvény nagyszerű referencia, amelyre minden munkáltató hivatkozhat. Természetesen az már, hogy betartják-e a törvényt, a gyakorlatban azért a költségek ezt a döntést nagyban befolyásolják.

Rejtett ellenőrzés

A törvény vázlatos 3. része is szót ejt azokról az ellenőrzésekről, amelyek nem a kommunikációra irányulnak. Az Informatikai Megbízott különösen érdekes módon közelíti meg a rejtett ellenőrzés kérdését. A Biztos a következőket állítja:

Rejtett ellenőrzéshez csak akkor folyamodjunk, ha alapos okunk van törvénytisértésre gyanakodni, ebben az esetben nem ajánlatos előre értesíteni az alkalmazottakat, mert ez befolyásolná a nyomozás végkimenetelét.

Ajánlatos ebben az esetben is megtalálni a megfelelő jogi alapot. A rejtett ellenőrzés titkos ellenőrzést jelent. Az 1. alapelv értelmében viszont nagyon fontos, hogy az információt megfelelően és igazságosan kezeljük. Az információkat csak akkor lehet korrekt módon begyűjteni, ha az 1. jegyzék 2. részének 2. bekezdésében leírtak alapján járunk el és ezt közzé is tesszük. Nyilvánvalóan, ha ezen a részek közzététele meg hiúsítaná a rejtett ellenőrzés célját.

A törvény IV. része számos kivételt említ bizonyos adatok gyűjtésével és feldolgozásával kapcsolatban. A 29. bekezdés értelmében a törvénytisértés felderítésére, megelőzésére összegyűjtött személyes adatok mentesülnek az adatvédelmi alapelv hatályai alól (kötelezettség arra nézve, hogy korrekt és törvényes módon kerüljenek összegyűjtésre az

adatok), leszámítva, hogy a 2. jegyzékben, valamint bizonyos esetekben a 3. jegyzékben foglalt feltételnek viszont meg kell felelnie. Ez azt jelenti, hogy bűnmegelőzési célból történő adatgyűjtés mentesül a kötelezettség alól, miszerint csak korrekt módon lehet összegyűjteni. Tehát a ily módon történő rejtett ellenőrzés nem szegi meg a DPA-ban leírtakat.

Viszont feltehetjük azt a kérdést, hogy a CCTV ellenőrzést – ellenőrzés, amely nyilvánosságra hozatal nélkül, az alkalmazottak előzetes értesítése nélkül történik – csak ilyen esetekben lehet-e alkalmazni, illetőleg más esetekben is (bizonyítékszerzés céljából, ha ismétlődő törvénysértés gyanúja forog fenn)? Ezzel kapcsolatban érdemes elolvasni az Informatikai Megbízott magyarázatát, ahol a videós ellenőrzés esetén például pontosan meg kell határozni a kamerák térbeli elhelyezkedését, viszont egy átlagos, kommunikációt ellenőrző tevékenység esetén általánosabb információk is elegendőek ahhoz, hogy a korrekt ellenőrzés kritériumának megfeleljünk.

Ebben az esetben semmilyen alapos indokunk nincs arra, hogy a videó általi ellenőrzést máshogy kezeljük, mint az egyszerű kommunikációs csatornák ellenőrzését. Az Informatikai Megbízott szerint a CCTV esetében csak kétfajta legális ellenőrzésről beszélhetünk: a rejtett ellenőrzésről (amely mentes attól a követelménytől, miszerint az ellenőrzés tényéről tájékoztatni kell a vizsgálat alanyait), valamint az egyszerű ellenőrzésről, amelyről mindig tájékoztatni kell a vizsgált személyeket és amely teljesen nyilvános. Mindazonáltal, e két ellenőrzési mód között is van egy harmadik megoldás, amelyet a legtöbb cég szeretne alkalmazni: ebben az esetben a munkáltatók a cég adatvédelemről vagy magánjellegről szóló előírásában informálnák az alkalmazottakat azokról az esetekről, amikor „rejtett” ellenőrzést folytathat a cég. Természetesen felvetődik az a kérdés, hogy ily módon a cég megfelel annak az előírásnak, miszerint az ellenőrzés tényét közölni kell, de így a nem csak törvénysértést megelőző-felderítő videós ellenőrzés is lehetővé válik.

Így tehát a törvény, talán nem meglepően, választ ad egy sor kérdésre, de néhányat azért válasz nélkül hagy. Bizonyos szempontból talán még bonyolítja is a dolgokat. Összegezve viszont elmondhatjuk, hogy jól írták meg és hasznos lesz a HR vezetők számára, amennyiben van idejük végigolvasni.

Ugyanakkor ügyelni kell arra is, hogy a munkáltatók és tanácsadók figyelmesen járjanak el a törvény alkalmazásánál, és fontos megérteni a jogi alapot egyes részek esetében. Ha valaki nem ismeri elég alaposan a törvényt, lehetetlen különbséget tenni aközött, hogy mit kell tenni, és

hogy mit gondol az Informatikai Megbízott és szerinte mi a legjobb megoldás.

Ha a törvényt, és különösen a vázlatos 3. részt a RIPA, a Törvényes Üzleti Gyakorlat szabályzata, valamint a HRA értelmében nézzük, láthatjuk, hogy a kommunikáció ellenőrzésének módja jogosan kihívás marad számunkra. Mindazonáltal egy vázlatokba szedett, jól megírt előírás a munkahelyen végzett ellenőrzésekről minden munkáltató esetében nagyon hasznos követelmény, de a munkavállalót természetesen nem kell tájékoztatni arról, hogy miként végezzük az ellenőrzést. Adjunk részleteket az ellenőrzésről és legyünk nyíltak. De bizonyos dolgokat tartsunk szem előtt!

Összeállította: Zemlincki Marianna

Flint, D.; Mallon, D.; MacRoberts: Big Brother – some reflections. = Computer Law & Security Report, 19. k. 1. sz. 2003. p. 30–35.

Sharpe, A.; Russel, C.: Employee monitoring. = Computer Law and Security Report, 19. k. 5. sz. p. 411–415.

Employee representation in the public service sector. = European Industrial Relations Review, 2003. 353. sz. jún. p. 30–32.

The EU Generalised System of Preferences and workers' rights. = European Industrial Relations Review, 2002. 346. sz. nov. p. 26–29.