BALOGH Zsolt György

KÖZTERÜLETI TÉRFIGYELÉS ÉS ADATVÉDELEM

Az utóbbi években Magyarországon is gyorsan terjednek a közterületeken létesített elektronikus térfigyelő rendszerek, amelyek elsődleges célja a közbiztonság növelése, a bűnmegelőzés és a bűnüldözés technikai támogatása. A rendszerek alkalmazásának azonban nemkívánatos mellékhatása is van; új oldalról fenyegetik a személyiségi jogokat. A tisztességes és törvényes adatkezelés alkotmányos követelményeinek biztosítása érdekében olyan jogi szabályozásra és adatkezelési gyakorlat kialakítására van szükség, amely képes összebékíteni a biztonság iránti igényt és a személyi szabadságot, a magánszféra védelmét. A tanulmány e kérdéseket járja körül, és a megoldás egy lehetséges módjára is rámutat.

Kulcsszavak: **térfigyelés, adatkezelés, adatfeldolgozás, rendőrség, közterületfelügyelet, adatvédelmi legjobb gyakorlat, adatvédelmi audit**

Mind a napi sajtónak a jogvédő szervezetek tevékenységéről szóló tudósításaiban, mind a jogtudományi és biztonságpolitikai szakirodalomban egyre gyakrabban találkozhatunk a közterületi térfigyelő rendszerek, az úgynevezett biztonsági kamerák használatának technikai és szabályozási kérdéseit firtató gondolatokkal. Az érdeklődés nagyon is indokolt, hiszen az információs társadalomban élve – bármit is jelentsen ez a fogalom – mindennapi tapasztalattá vált, hogy kamerákon keresztül figyelő tekintetek szegeződnek ránk utcán és munkahelyen, közlekedési eszközökön és hivatali ügyintézés közben.[1] Jól tudjuk, hogy a technológiai lehetőségek nem merülnek ki a puszta megfigyelésben. Mód van a megfigyelt területen zajló események rögzítésére és bizonyos mértékig még az elkészült felvételek automatizált kiértékelésére is.[2]

Versengő érdekek

Kockázatokkal teli világunk egyik legfőbb kockázati tényezője maga az ember. A természeti katasztrófákon és műszaki hibára visszavezethető baleseteken kívül olyan személyek, szervezetek is veszélyeztetik biztonságunkat, akik/amelyek anyagi érdekekből, vagy szélsőséges ideológiák szolgálatában állva, esetleg egyszerűen öncélú romboló szándéktól vezérelve károsítanak anyagi javakat, okoznak személyi sérülést vagy idéznek elő tömegkatasztrófákat.

A megfigyelő rendszerek telepítésének célja a biztonság fokozása. Szögezzük le mindjárt az elején: ez a cél nem mindig teljesül. Jól ismertek azok a nemzetközi példák, mint például a néhány évvel ezelőtti robbantás a londoni metróban, amikor kamerákkal sűrűn ellátott területen, a megfigyelés folyamatossága ellenére, a hatóságok képtelenek voltak súlyos bűncselekményeket megelőzni, megakadályozni, s a megmaradt esetleg sok ezer órányi videofelvétel csak arra volt jó, hogy hosszú idővel a tragédia után a hatóságok bizonyos valószínűséggel azonosíthassák az elkövetőket és megállapíthassák a cselekmény lefolyását.

Közbiztonság, vagyonbiztonság, bűnüldözés, bűnmegelőzés

Az időnkénti látványos kudarcok ellenére a rendészeti szervek és az önkormányzatok, amelyek a közrend és a közbiztonság fokozásáért, de legalábbis megőrzéséért folyó mindennapi küzdelem első vonalában kell, hogy helytálljanak, komoly várakozásokkal tekintenek minden olyan technológiai, műszaki lehetőségre, amelynek segítségével lépést tarthatnak a fokozódó biztonsági kockázatokkal. A közterületi térfigyelő rendszerek telepítése és üzemeltetése azzal kecsegtet, hogy a meglévő – és persze mindig szűkös – erőforrások kímélésével, hatékonyabb felhasználásával tehetnek eleget közbiztonsági feladataiknak.[3]

A feladat ellátásáért felelős szervek: a rendőrség, az önkormányzatok és nem mellékesen a közterület-felügyeletek, valamint a személy- és vagyonőrök. Munkájuk megkönnyítésének ma már egyre kevésbé nélkülözhető eszközei a korszerű információtechnológiai berendezések, adatfeldolgozó rendszerek, hálózatok. A kamerákat a rendőrség és az említett további szervek abból a célból szerelik fel, hogy az állandó személyes jelenlétet a térfigyelőközpontban szolgálatot végző megfigyelők „virtuális jelenlétével" helyettesítsék.

A rendőrség és az önkormányzatok feladataival, tevékenységével e szervek hosszú idő alatt kialakult társadalmi beágyazottsága, széles körű ismertsége miatt e helyen nem foglalkozunk. A személy- és vagyonőrökkel bár naponta kerülünk kapcsolatba a legkülönbözőbb helyeken, tevékenységük jellege mégis talán kevésbé ismert. A vagyonőrök szolgálata igen sok területre terjed ki: vagyonőrök figyelnek az egyes boltok, bevásárlóközpontok biztonságára, rendkívüli felelősséggel járó őrzési feladatokat látnak el érték- és veszélyesanyag-raktárak, közüzemi telephelyek mellett. Vagyonőri feladat egyes rendezvények biztosítása, de szerepet vállalnak az értékszállításban vagy személyek védelmében is. A felsorolt tevékenységek nagyban különböznek egymástól, folytatásuk esetenként különböző szakmai szabályok szerint történik, és feladattípusonként természetesen más-más kockázati tényezők merülnek fel. Könnyen belátható, hogy míg egy veszélyes üzemet vagy bankfiókot akár fegyverrel is őrizni kell, addig egy közértben például nehezen indokolható a fegyveres biztonsági őr alkalmazása.
A legtöbb kamerás megfigyelés elsődleges funkciója

– a tulajdon védelme,
– a normakövetésre való rábírás, illetve
– a védekezés ellenére bekövetkező jogsértés esetén a számonkérés elősegítése, a szankcionálás lehetőségének megkönnyítése.

Személyiségi jogok védelme

A kamerának mint a tulajdonvédelem technikai eszközének az alkalmazása a tulajdon tárgyainak óvására alkalmas ugyan, ám óhatatlanul személyekre, emberi magatartásokra, szokásokra, megnyilvánulásokra, illetőleg magára az emberi testre is irányulhat. Az elektronikus úton történő megfigyelés tehát alkalmas arra, hogy a magánszférába behatoljon, és akár intim, különösen szenzitív élethelyzeteket figyeljen meg, rögzítsen, tegyen a megfigyelő számára hozzáférhetővé.

Ez akár úgy is megtörténhet, hogy az érintett nem is tud a felvétel készítéséről, vagy nincs abban a helyzetben, hogy mérlegelhesse az ilyen felvételek megengedhetőségét és azok következményeit. Az így végzett megfigyelés a magánélethez való jog sérelmén túl – szélesebb és mélyebb értelemben – az emberi méltósághoz való jogot általában is érintheti. A magánszféra lényegi fogalmi eleme éppen az, hogy az érintett akarata ellenére mások oda ne hatolhassanak be, illetőleg be se tekinthessenek. Ha a nem kívánt betekintés mégis megtörténik, akkor nemcsak önmagában a magánélethez való jog, hanem az emberi méltóság körébe tartozó egyéb jogosultsági elemek, így a személyi szabadság, a testi-személyi integritáshoz való jog sérülhet.

E megfontolásokon alapulnak azok a törekvések, amelyek a kamerás közterületi térfigyelő rendszerek használatának korlátozását, működésük ellenőrizhetőségét kívánják alkotmányos eszközökkel megalapozni.

A személyiségi jogok védelme érdekében a közterületi térfigyelő rendszerek kontroll nélküli telepítése és használata ellen különösen az öntudatos, adatérzékeny adatalanyok, egyes jogvédő szervezetek – Magyarországon leghatározottabban talán a Társaság a Szabadságjogokért (TASZ) – és sajátos jogi eszközeivel az adatvédelmi biztos lép fel.

Adatvédelmi alapfogalmak

Személyes adat fogalma[4]

A személyes adat fogalma alapvető a közterületi megfigyelő rendszerekkel kapcsolatban. Tekintsük át most az általános szabályokat és fogalmakat.

Bár az adatvédelem közvetlen tárgya a *személyes adat*, közvetve ez a személyiség védelmét, az emberi méltóságot és szabadságot biztosítja. Ugyanis az adatkezelés törvényességének biztosításával kerülhető el a személyiség sérelme. Melyek tehát a személyes adatok?

Személyes adat minden olyan adat, információ és az ezekből levonható következtetés is, amely az érintett személyre vonatkozik, vagyis amely által az illető egyediesíthető, azonosítható, életviszonyai, kapcsolatai leírhatók. A rendkívül tág fogalomkörön belül alcsoportokat is megkülönböztethetünk. A két legalapvetőbb kategóriát az *azonosító* és a *leíró* adatok csoportja képezi.

Az azonosító adatok

Az azonosító adatok nyilvánvalóan az adatkezeléssel érintett személy egyediesítését, a többi érintettől való megkülönböztetését szolgálják. Erre a célra *természetes* és *mesterséges* azonosító adatok használhatók fel.

Személyek természetes azonosítói különösen a név (családi és utónév, illetve leánykori név), a születés helye és időpontja, az anya neve, valamint a lakcímadatok. A természetes azonosítók közül általában többet

kell alkalmazni egyszerre, hiszen a kívánt cél, a személy egyediesítése csak így biztosítható kielégítő pontossággal.

A mesterséges azonosítók általában valamilyen matematikai, illetve statisztikai eljárással generált kódok; többnyire számok vagy számok és betűk kombinációja. Mesterséges azonosító például a személyi igazolványszáma, az útlevélszám, a vezetői engedély száma, vagy az újabbak közül az adóazonosító szám, a társadalombiztosítási azonosító jel (TAJ) és a személyi azonosító kód.

A lényegi különbség a természetes és a mesterséges azonosítók között az, hogy az utóbbiak közül egy is elég a személy egyediesítéséhez. A mesterséges azonosítók ezért jól és igen hatékonyan használhatók adatkapcsolatok feltárására, követésére. Ugyanakkor sajnos ezekkel lehet a legkönnyebben visszaéléseket elkövetni. Éppen ez az a tényező, amely a kódszerű, rövid és egyértelmű azonosító adatokat meglehetősen veszélyes eszközzé teszi, s ami miatt az adatvédelem különös gyanakvással tekint ezek alkalmazására. Tagadhatatlan, hogy a hatósági munkában, a gazdasági életben és még számos más területen az azonosíthatóságra, az ügyfelek, partnerek megkülönböztetésére szükség van, de ezt a célt általában kielégítően szolgálják a természetes azonosítók is.

Leíró adatok

A leíró (deskriptív) adatok az adatkezelés célja szerint releváns személyes adatok. Az azonosítókon kívül minden az adatkezelésbe bevont személyes adat e kategóriába tartozik. A leíró adatok az érintett különböző személyi viszonyait fejezik ki; az adatkezelés valójában ezek megismerésére irányul.

Címzett és anonim adatok

Ha az érintettről felvett adatminta a leíró adatokon kívül azonosító adatokat is tartalmaz, akkor címzett, ha pedig nem tartalmaz, akkor *anonim* adatokról van szó. Az igazgatási célra szánt adatgyűjtések többnyire címzett, tehát visszakereshető, személyekre visszavezethető adatállomány létrehozására irányulnak. Az anonimitás biztosítása inkább a statisztikai adatfelvételekre és a közvélemény-kutatásokra jellemző.

Szenzitív adatok

A leíró adatok különleges csoportját képezik az úgynevezett érzékeny vagy szenzitív adatok. A szakmai közvéleményben már régóta elfogadott terminológiáról van szó, olyannyira, hogy már a nemzetközi ajánlásokban és egyezményekben is külön nevesítik ezt a kategóriát. Bár országonként vannak eltérések abban, hogy mely adatokat sorolnak e gyűjtőfogalom alá, az alábbiak tekintetében nemzetközi szinten is teljesnek mondható az egyetértés. Eszerint különösen

- az egészségi állapotra,
- a szexuális életre, illetőleg szokásokra,
- a kóros szenvedélyre,
- a faji eredetre,
- a nemzeti, etnikai hovatartozásra,
- a vallási vagy más ideológiai, illetőleg politikai meggyőződésre és
- a büntetett előéletre vonatkozó adatok alkotják az érzékeny adatok körét.

Magyarázatként annyit tehetünk hozzá, hogy ha ezek az adatok nyilvánosságra kerülnek vagy illetéktelen személyek tudomására jutnak, az az érintettre nézve különösen hátrányos következményekkel járhat. Ezek az adatok csupa olyan életviszonyról tudósítanak, amelyek az egyén legintimebb magánügyeit alkotják, illetőleg amelyekkel kapcsolatban a XX. század történelme során a legvisszataszítóbb bűnöket követték el; indokolt tehát a fokozott óvatosság.

Az érzékeny adatok a törvény fokozott védelme alatt állnak, vagyis ezen adatok kezelésére szigorúbb szabályok vonatkoznak, mint egyébként a többi adatra.

Az adatvédelmi törvény módosításai során a személyes adat fogalmát is pontosította a jogalkotó. Az eredeti változat szerint – amely a törvény kihirdetésétől 2003. december 31-ig volt hatályban – a *„személyes adat a meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható.”*

2004. január 1. után a definíció kicsit módosult. Ennek legfontosabb elemeként kiegészült egy az értelmezést segítő mondattal.

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

A 2004. évi módosítás új értelmezést adott az adatkezelésnek is, amely *az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, vagy a*

műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is.

A fentiek szerint tehát a technikai eszközzel rögzített kép- és hangfelvétel is személyes adat. Ez a megállapítás az eredeti definíció alapján is nyilvánvaló, de legalábbis igazolható, levezethető volt. Az ítélkezési gyakorlatban mégis zavarokat, egyes jogalkalmazóknak logikai nehézségeket okozott ennek belátása. Az új szabályozás egyértelműen utal az adat azonosíthatósági elemére, és kevesebb kibúvást tesz lehetővé.

Az adatvédelmi törvény által bevezetett és szabályozott információs önrendelkezési jog a személyes adat fenti fogalmán alapul.

Információs önrendelkezési jog

Az információs önrendelkezési jog leglényegesebb tartalma az a felhatalmazás, amely szerint az adatalany maga határozhat arról, hogy adatait más személyekkel vagy szervezetekkel megismerteti-e vagy sem.[5] A fő szabály szerint tehát személyes adat csak az érintett hozzájárulásával kezelhető. Mint állampolgári alapjog az információs önrendelkezési jog is csak kifejezett törvényi rendelkezés által korlátozható, vagyis az érintettet adatközlésre csak törvényben lehet kötelezni.

Az adatkezelőre azt a kötelezettséget rója az adatalany információs önrendelkezési joga, hogy a teljes adatfeldolgozási eljárás során biztosítsa az adat sorsának követhetőségét, az erről való érthető tájékoztatást és a megfelelő technikai *adatbiztonságot*. Az önrendelkezés jogát abban az értelemben is tiszteletben kell tartania a hivatásos adatkezelőnek, hogy mindenképpen biztosítsa a bizalmas kezelés körülményeit, és ha az érintett kívánja, kifejezetten tekintse titkosnak a birtokában lévő személyes adatokat. A bizalmas kezelés azt is jelenti, hogy megfelelő rendszabályok megalkotásával és betartásával gondoskodjon arról, hogy az adatokhoz jogosulatlan személy ne férhessen hozzá.

Az adatvédelem legfontosabb – nemzetközi dokumentumokban és nemzeti törvényekben egyaránt kinyilvánított – alapelvei az adatfelvétel és adatkezelés *tisztességessége és törvényessége, arányossága*, valamint *célhozkötöttsége*.

Természetes igény, hogy az érintett tudjon a rá vonatkozó adatkezelésről. Ezt a tudomást kiterjesztetten kell értelmezni, tehát sok részmozzanatot értünk alatta. Ennek körében különösen tudnia kell az adatkezelés létezéséről és helyéről, valamint arról, hogy miképpen tekinthet bele a róla felvett és tárolt adatokba. Biztosítani kell részére, hogy a betekintéshez kapcsolódóan az adatokról másolatot, kivonatot készíthessen, illetve helyesbíthesse a téves adatokat. Minden alkalommal, ha ilyen történik, tájékoztatni kell adatainak más személy vagy szervezet részére való megadásáról. Mindezen jogairól az adatkezelés megkezdésekor, ami sok esetben magát az adatfelvételt jelenti, tájékoztatni kell az érintettet. E jogainak gyakorlását szükségtelen költségek, valamint az adatkezelő által okozott indokolatlan késlekedés nem akadályozhatja.

Ezen túlmenően az adatkezelés szabályainak megszegése esetére biztosítani kell, hogy az érintett jogorvoslásban részesülhessen, ami egyrészt a sérelmes magatartás vagy helyzet megszüntetését jelenti, másrészt az okozott kár megtérítését a polgári jogi felelősség szabályai szerint. A különösen súlyos esetekre tekintettel meg kell teremteni a büntetőjogi felelősségre vonás alkalmazásának lehetőségét.

Sajátos tartalma az információs önrendelkezési jognak az az érintett számára szóló felhatalmazás, hogy adataiba, személyes ügyeibe csak akkor és annak engedjen betekintést, amikor és akinek jónak látja. Az egyén önrendelkezési joga megáll mind az állam szerveivel, mind a magánszemélyekkel, és ezek különböző társulásaival szemben is. A tulajdonjog mintájára szabottan abszolút szerkezetű jog, vagyis mindenkit kizár a magánszférából, s a személyes adatok urává az érintett személyt teszi, aki tetszése és belátása szerint engedheti közel magához a külvilágot.

Az arányosság elve

Mint a védelmi jogok általában, a személyes adatok védelméhez való jog, és így az információs önrendelkezési jog is csak túlnyomó közösségi érdekből korlátozható. Többek között a közigazgatás működőképességének fenntartása, az arányos és egységes közteherviselés megvalósítása (adóigazgatás, társadalombiztosítás) lehet az a kivételes érdek, amely indokolhatja az információs önrendelkezési jog gyakorlásának korlátozását. A korlátozás többnyire kötelező adatszolgáltatás előírását jelenti, s ez akár szankcionálható is, például pénzbüntetéssel.

Mivel állampolgári alapjogról van szó, a korlátozás csak törvényben állapítható meg, így az sem kívánatos, hogy a parlament a jog érdemét érintő kérdésekben a kormány számára rendelet alkotására szóló felhatalma-

zást adjon. Egyes területeken tehát előírható ugyan kötelező adatszolgáltatás, ehhez azonban a törvény kell, s ugyancsak törvényben kell megállapítani a felhasználás részletszabályait is.

A kényes kompromisszumok területe ez, ahol két követelményrendszer ütközése, illetőleg egyensúlya a tét. Az egyik a személyiség szabadságának, önállóságának, méltóságának elve. Eszerint a személyiség olyan érték, amelynek szabad kibontakozását, korlátozásoktól mentes fejlődését védeni kell, többek között olyan módon is, hogy személyes adatainak, magánügyeinek feltárásába rajta kívül senkinek sem lehet beleszólása.

A másik érvrendszer kiindulópontja szerint az egyén a társadalom tagja. Szinte valamennyi életfeltétele tekintetében rá van utalva arra a támogatásra, amit a társadalom biztosít számára. Ebből következik, hogy a szükséges mértékben el kell viselnie még szabadságjogainak társadalmi érdekből való korlátozását is, azaz személyiségének részleges feladása árán is hozzá kell járulnia a közösségileg fontos funkciók ellátásához. Így bizonyos ponton túl nem gördíthet akadályt személyes adatainak megismerése elé sem.

Láthatólag egymásnak szögesen ellentmondó megfontolások ezek. Összhangjuk megteremtéséhez fogalmazzunk meg egy közvetítő elvet; ez pedig az arányosság elve.

Az *arányosság elve* megköveteli, hogy a két ellentétes érdeket együttesen, kölcsönhatásában vizsgáljuk meg, s korlátozásuk fokát e mérlegelés szerint határozzuk meg. Olyan kompromisszumra kell törekedni, amely a társadalmi cél eléréséhez is garantálja a minimálisan szükséges feltételeket, és még alkalmas a reális állampolgári jogvédelemre. Felül kell vizsgálni alkalomról alkalomra a szóban forgó érdekek viszonyát az egyéniséget ért veszteséghez, és az ilyen áron megvalósítani kívánt társadalmi célhoz, s ennek alapján megállapítani, hogy mi az a szükséges mérték és idő, amelynek erejéig korlátozható az egyén információs önrendelkezési joga.

Már az információs önrendelkezési jog deklarálása és tartalmának definiálása is igen nagy jelentőségű lépés a személyiség állammal, illetve a többi adatkezelővel szembeni emancipálódásának folyamatában. Ez azonban még nem elegendő. Az adatvédelmi szabályoknak garanciákkal kell védeniük az adatkezelések törvényességét.

A célhoz kötöttség

Mint az Alkotmánybíróság 15/1991. (IV. 13.) sz. döntése is rámutat, az információs önrendelkezési jog gyakorlásának legfontosabb garanciája a *célhoz kötöttség*. Lényegében azt jelenti, hogy az adatkezelés csak pontosan meghatározott, törvényes célra irányulhat. A meghatározott *törvényes cél nélküli,* „készletre", előre nem meghatározott jövőbeli felhasználásra irányuló adatkezelés alkotmányellenes.

A célhoz kötöttséget meg kell erősíteni a közérthetőség követelményével is, azaz a célt közölni is kell az érintettel, mégpedig olyan formában, hogy az megítélhesse az adatfeldolgozás hatását jogaira, és megalapozottan dönthessen az adat kiadásáról.

Mint az alapfogalmak között láttuk, az adatkezelés többlépéses művelet, amelynek két végpontja, az adatgyűjtés, illetve adatfelvétel és az adatok törlése, közöttük pedig számos további részművelete különíthető el. A célhoz kötöttség elve csak akkor tölti be rendeltetését, ha a feldolgozási folyamat minden pillanatában érvényesül, azaz ha az adatkezelés során mindvégig biztosított a „törvényes adatminőség". A célhoz kötöttség elvének érvényesítése zárja ki az adatok tetszőleges jövőbeni felhasználásra való gyűjtését, előkészítését, *készletezését*, amely az állandóan meglévő feltöltött adattárak révén folyamatos fenyegetést jelent az információs önrendelkezési jogra; vagyis a személyiség szabadságára, s ezen keresztül az egész – információs – társadalom szabad és demokratikus jellegére.

Kötelező adatszolgáltatás is csak a célhoz kötöttség szem előtt tartásával rendelhető el. Törvényes célra irányuló adatkezeléshez írható elő törvény által a kötelező adatszolgáltatás, amelynek célját természetesen megfelelő formában közölni is kell az érintettekkel.

Az adattovábbítás és a nyilvánosságra hozatal korlátozása

A célhoz kötöttségnek az egész adatkezelésre vonatkozó követelménye mellett igen fontos külön garantálni az adattovábbítás és a nyilvánosságra hozatal korlátozását.

Az adattovábbítás során az adatot a feldolgozó *meghatározott harmadik személy* számára hozzáférhetővé teszi. A nyilvánosságra hozatal pedig azt jelenti, hogy az adatot *bármely harmadik személy* megismerheti.

Az adattovábbítás fogalmába a különböző jellegű, feladatú, *célú* adatbázisokból történő adatátvétel is beleértendő. Ezek a technikai műveletek teljesen kívül maradhatnak az adatalany figyelmén és beavatkozási lehetőségének körén, és illuzórikussá tehetik az információs önrendelkezési jog gyakorlását.

Ezek a műveletek különösen sérthetik az információs önrendelkezési jogon túl a magántitok és az emberi méltóság védelméhez való jogot is. Legbelsőbb magánügyeinek nyilvánossá tétele társadalmi kapcsolataiban lehetetlenítheti el az egyént, arról a helyzetről

nem is beszélve, ha tényszerű adatokon kívül az ezekből levont, esetleg kétes valóságértékű következtetések kapnak nyilvánosságot.

Az adattovábbításra nem rendelhető el egyértelmű tilalom, az ugyanis sok kényelmetlenséget okozhat magának az érintettnek is, ha hivatalos ügyeinek intézése során minden egyes hivatal, minden egyes rutinszerű adatfelvétel miatt külön felkeresi. Fő szempontként itt is az az irányadó, hogy a célhozkötöttség elvéhez tartsák magukat az adattovábbításban érintett hivatalok. Legyenek olyan törvényes felhatalmazások, amelyek garanciák megteremtésével egyidejűleg teszik lehetővé személyes adatok továbbítását, s gondoskodnak arról is, hogy az átadott adatokat az eredetitől idegen célra ne használhassák fel.

Szabad-e akkor egyáltalán adatfeldolgozási rendszereket adattovábbítás céljából egymással összekapcsolni? Igen, de törvényesen ez csak akkor tehető meg, ha minden egyes adat vonatkozásában teljesül az adattovábbítást megengedő összes feltétel. Ez pedig ténylegesen azt jelenti, hogy az adattovábbítás címzettjének – az adatkérőnek – vagy konkrét törvényi felhatalmazással kell rendelkeznie ahhoz, hogy a továbbított adatokat feldolgozhassa, vagy az érintett beleegyezését kell megszereznie. Végső soron ezen a téren *a tiltás* a fő szabály, a szorosan értelmezett *kivételeket* pedig törvényben kell meghatározni.

Az adatintegráció tilalma

A harmadik garancia, az adatbázisok integrációjának tilalma, jól összeillik az előzővel. Tulajdonképpen az integráció során is adattovábbítás történik, csakhogy ez az adattovábbítás az adatbázisok teljes állományát érinti, és számos következményt von maga után. Világosan látnunk kell a különbséget az adatbázisok integrációja és adattovábbítás céljából való – esetleg alkalmi jellegű – összekapcsolása között. Az utóbbi esetben az összekapcsolt adatbázisok mindegyike megőrzi különállását, nem történik összeolvadás, mert az adattovábbítás az egyes adatbázisok teljes tartalmának csupán valamely jól körülhatárolt részhalmazát érinti.

Ezzel szemben az integráció révén két vagy több különálló adatbázisból – a véglegesség igényével – egy új adatbázis, s az adatkapcsolatok révén egy *új minőség* jön létre. Ebben az integrált adatbázisban pedig az adatok már biztosan elszakadnak attól a törvényes céltól, amire az érintett eredetileg megadta őket. Fokozott veszélyt jelent továbbá, hogy az adatbázisok integrálása egyszerűen egy technikai művelet, ami nyilvánvalóan elvégezhető anélkül, hogy az érintett bármit is sejtene róla, hiszen még adatfelvétel céljából sem kell őt megkeresni, mert az eredeti adatbázisok már tartalmazzák a kiinduló adatokat.

Az integrált feldolgozás veszélyei között fontos utalni a számítógép adatfeldolgozási teljesítményére, és arra, hogy segítségével rövid idő alatt teljes *személyiségprofil*[6] állítható elő anélkül, hogy az érintett kielégítően ellenőrizhetné annak helyességét, felhasználását, az adatkezelés törvényességét. Törvénytelen adatkezelési műveletekre s nehezen ellenőrizhető következtetések levonására ugyanis éppen az integrált adatfeldolgozó rendszerek kínálják a legtöbb lehetőséget.

Mindezek a tényezők az adatbázisok integrációját a legkockázatosabb és az adatvédelem szempontjából a leginkább kifogásolható adatkezelési cselekménnyé teszik. Minden indok amellett szól, hogy az adatbázisok integrációjára generális tiltást kell alkalmazni.

Sajnos a magyar adatvédelmi törvény nem foglal világosan állást ebben a fontos és kényes kérdésben, csupán az adattovábbításra és az adatkezelések pontosabban nem definiált *„összekapcsolására”* nézve állapít meg szabályokat.

Alapvető jogszabályok

Mivel a magánszféra nem szűkül le a magánlakásra és az ahhoz tartozó területre, a jogi szabályozás során figyelembe kell venni azt a tényt, hogy a betekintésre alkalmas biztonságtechnikai rendszerek működési körén belül a magánszféra védelme szempontjából érzékeny területek is előfordulhatnak.

A hatályos magyar jogban a képfelvevő, -rögzítő berendezések – közterületen vagy nyilvános helyen történő – működtetéséről, illetve kép-, filmfelvétel, fénykép vagy képmás készítéséről, felhasználásáról kevés szabály rendelkezik; néhány törvény általában, míg mások egy-egy szervezet tevékenységéhez kapcsolódva határoznak meg előírásokat.

A megfigyelést végző kamerák működése ma Magyarországon törvényben szabályozott. Az ilyen jellegű eszközök használatakor fokozott gondot kell fordítani arra, hogy az alkotmány keretei között tartsuk ezeket. A közterületeken működő megfigyelőrendszerek esetében különösen fontos, hogy az adatok megismerését alkotmányos alapokra helyezzük, csökkentve ezzel a magánszférát ért jogkorlátozást.

Az Alkotmány 59. §-a garantálja a személyes adatok védelmén túl a magánszféra (magántitok) tiszteletben tartását. A kamerás megfigyelőrendszerek az állampolgárok alkotmányos jogát korlátozzák. Az adatkezelés jellege preventív. Nem arról van szó, hogy a büntetőeljárás sikere érdekében meghatározott alanyi kör jogait korlátozni kell (erre számos példa van, a körözéstől a hatósági erkölcsi bizonyítványig), hanem arról, hogy

bármelyik jogkövető állampolgár az ellenőrzés alanya lehet. A kamerás megfigyelés korlátlan számú embert érinthet, akik nemhogy bűncselekményt nem követtek el, de semmilyen módon nem érintettek egyetlen büntetőeljárásban sem.

A térfigyelés speciális kérdései

A térfigyelés mint adatkezelési tevékenység speciális mozzanatokból tevődik össze. Ilyenek a közvetített

- képek megfigyelése,
- azok rögzítése,
- a felvétel feldolgozása, kiértékelése és
- megőrzése.

Az alkalmazott lépéseknek komoly jelentősége van az egész megfigyelési folyamat adatkezelési, adatvédelmi megítélése szempontjából. Ha ugyanis csak olyan közterületi megfigyelés történik, ahol a megfigyelt személyek nem felismerhetők, azt nem tekinti adatkezelésnek sem a jogi szabályozás, sem a joggyakorlat, sem a mérvadó jogi szakirodalom. Ellenvethető, hogy ebben az esetben is történik adattovábbítás, hiszen a technológia természeténél fogva a megfigyelt területet ábrázoló képek valamilyen távközlési megoldás alkalmazásával eljutnak a térfigyelő központba. Ha azonban ezeket a képeket harmadik személy számára nem teszik hozzáférhetővé, akkor nem beszélhetünk az adatvédelmi törvény fogalmi körébe eső adattovábbításról.

Egészen más a helyzet akkor, ha a képeket nemcsak megfigyeli a térfigyelő központ személyzete, hanem azzal további műveleteket is végez, azokat rögzíti, tárolja, megőrzi. Ezek a műveletek már mindenképpen az állampolgári alapjogok korlátozását jelentik, és a felvételek feldolgozása során már mód van a képeken szereplő természetes személyek azonosítására, velük kapcsolatban személyes adatok kezelésére. Ezekben az esetekben feltétlenül alkalmaznunk kell a személyes adatok védelméről szóló speciális szabályokat.

Különösen kényes kérdéseket vet fel a felvételek megőrzése. Az információs önrendelkezési jog alapelvei közé tartozik a célhoz kötöttség, ami fogalmilag kizárja a személyes adatok meghatározott cél nélküli, készletezésre való gyűjtését. Mármost milyen hosszúságú megőrzési időt tekintünk megengedhetőnek anélkül, hogy a készletezés tilalmát megsértenénk? A kérdés nehézségét az jelenti, hogy valamennyi időre feltétlenül szükség van ahhoz, hogy a képek kiértékelésével megállapítható legyen, történt-e a megfigyelt területen olyan jogsértés, aminek felderítéséhez, üldözéséhez, a szükséges eljárások lefolytatásához a felvételek további kezelése, megőrzése segítséget jelent. Az érdekelt szereplők – különösen a rendőrség és az adatvédelmi biztos – eddigi egyeztetései alapján sikerült kialakítani egy olyan gyakorlatot, amit kölcsönösen elfogadhatónak tartanak. A gyakorlatban kimunkált kompromisszumos megoldást emelte be később – 2008. január 1-jei hatállyal – a jogalkotó a rendőrségi törvénybe.

A térfigyelő központba történő belépés/benntartózkodás ugyancsak lényeges kérdéseket vet fel. Alapvető követelmény, hogy illetéktelen személynek ne juthasson tudomására olyan adat, amit a térfigyelő rendszer segítségével szereznek meg az erre feljogosított szervek. Tehát a térfigyelő rendszer központi kezelési helyiségébe csak az ott szolgálatot ellátó állomány, az ellenőrzésre jogosult vezetői állomány, a rendszergazda, az érintett rendőri szervnél a térfigyelő rendszer működtetésének szabályait tartalmazó belső normában meghatározott személyek, valamint az adatvédelmi biztos és munkatársai léphetnek be és tartózkodhatnak. Ezeken a személyeken kívül más a térfigyelő rendszer központi kezelési helyiségébe csak rendszert működtető rendőri szerv vezetőjének előzetes engedélyével léphet be, illetve tartózkodhat. A térfigyelő rendszer központi kezelési helyiségébe belépő, ott szolgálatot teljesítő személyekről szolgálati naplót kell vezetni.

Ágazati szabályozás

A térfigyelésről szóló ágazati szabályozást alapvetően három fontos törvény hordozza. Ezek a rendőrségről szóló 1994. évi XXXIV. törvény, a közterület-felügyeletről szóló 1999. évi LXIII. törvény és a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény. E jogszabályok legfontosabb térfigyeléssel kapcsolatos szabályait vesszük sorra az alábbiakban.

Rendőrségi törvény

Rendkívül érdekes a rendőrségi törvény képfelvételekkel kapcsolatos rendelkezéseinek evolúciója.

A törvény hatályba lépésétől kezdve módot ad a rendőrségnek arra, hogy a rendőri intézkedéssel összefüggésben az intézkedéssel érintett személyről, a környezetről, illetőleg a rendőri intézkedés szempontjából lényeges körülményről, tárgyról kép- és hangfelvételt készíthessen. Ez a rendelkezés azonban igen szikár és a lényeges alapjogi kérdésekről, garanciákról – a más jogszabályra utaló szokásos „elhárító" szabályon kívül, amely szerint „az intézkedés alapjául szolgáló esemény helyszínén a rendőr, valamint a más által készített kép- és hangfelvétel jogszabály előírásai szerint használható fel" – semmit sem mond.

Az 1996. szeptember 1-jén hatályba lépett módosításnak köszönhetően nagyot lépett előre a rendőrségi törvény a tisztességes és arányos adatkezelés útján. Vélhetően az egy évvel korábban megválasztott adatvédelmi biztos időközben kifejtett munkájának is része volt abban, hogy a felvételek korlátlan idejű készletezését kizáró rendelkezés megszületett. Eszerint a felvételeket, amennyiben a rajtuk rögzített cselekmények miatt sem büntető- vagy szabálysértési eljárás nem indult, sem egyébként, a felvételek nem képeznek maradandó értéket – bármit is jelentsen ez – 6 hónap elteltével meg kell semmisíteni.

A következő módosítás során – 1999. szeptember 1-jétől kezdődő hatállyal – a készletezés korlátozása mellé belépett az adatalanyok, a megfigyelt területen tartózkodó személyek tájékoztatására vonatkozó kötelezettség. A rendőrség nemcsak arra köteles, hogy a térfigyelő rendszer kameráit jól látható, nyilvánvalóan felismerhető módon szerelje fel, hanem kifejezetten tájékoztatnia is kell a lakosságot a berendezés elhelyezéséről és működtetéséről.

A jelenlegi szabályozás 2008. január 1. óta hatályos. Ennek differenciáltsága és kifinomultsága már valósággal összehasonlíthatatlan a törvény eredeti rendelkezéseivel. Jól kifejeződik ebben a rendőrségi feladatok összetettebbé válásán és a technikai eszközök alkalmazásának növekvő jelentőségén kívül az is, hogy az adatvédelmi joggyakorlat és tudatosság hatalmas fejlődésen ment keresztül az elmúlt másfél évtized során. A jelenlegi szabályok részletesen rendezik a rendszer üzemeltetőjének tájékoztatási kötelezettségét, a felvételek felhasználásának feltételeit, módját és a – korábbinál lényegesen rövidebb, 3-tól 30 napig terjedő időtartamban megszabva – a megőrzés, illetve megsemmisítés határidejét.

A közterület-felügyeleti törvény

A közterület-felügyeleti törvény esetében nem beszélhetünk olyan töretlen ívű fejlődési pályáról, mint a fenti történetben. A kép- és hangfelvétel készítéséről szóló rendelkezések 2000, a törvény hatályba lépése óta változatlanok. Közterület-felügyelő a törvény szerint szintén jogosult az intézkedéssel érintett személyről, az intézkedés vagy az eljárás szempontjából lényeges környezetről és körülményről, tárgyról kép- és hangfelvételt készíteni. Az ilyen felvétel kizárólag az adott eljárásban, jogszabály előírásai szerint használható fel.

A megőrzés idejét a rendőrségi törvény akkor hatályban volt rendelkezéseivel összhangban szintén 6 hónapban állapította meg a jogalkotó, amennyiben a felvételen rögzített cselekmény miatt nem indult eljárás. Ez a megőrzési idő ma már lényegesen meghaladja azt az időtartamot, amit a törvény a rendőrség hasonló tevékenysége számára engedélyez. Ezzel kapcsolatban nyilvánvaló jogalkotói mulasztás áll fenn, amit mihamarabb orvosolni kell.

A vagyonvédelmi törvény

Az eddigiek alapján joggal merülhet fel az a gondolat, hogy a fenti testületek tevékenységével rokonságot mutató személy- és vagyonőrök is jogosultak volnának elektronikus megfigyelőrendszert telepíteni és alkalmazni. A vagyonvédelmi törvény azonban határozottan kizárja azt a lehetőséget, hogy közterületen ilyen berendezéseket szereljenek fel.[7]

Ugyanakkor nincs törvényi akadálya annak, hogy magánterületen, az őrzött létesítményben ilyen technikai berendezéseket alkalmazzon a vagyonőr a szerződésben vállalt kötelezettségének teljesítése érdekében.

Legjobb gyakorlatok és az adatkezelések auditálása

A legjobb gyakorlat követése

A bevezetőben láttuk, hogy a közterületi térfigyelő rendszerek alkalmazása kapcsán két fontos érdek csap össze. Nyilvánvaló igény van a biztonságot fokozó technológiai eszközök telepítésére, ugyanakkor ezek használata nem járhat azzal a következménnyel, hogy a jogállami alkotmányok által garantált személyiségi jogok súlyos sérelmet szenvedjenek. Az ellentét, ha nem is teljesen kibékíthetetlen, de a konfliktusok csak lassan és gondos fejlesztéssel oldhatók fel. Márpedig a technikai védelmi eszközök iránti közbizalmat meg kell teremteni, mert e-nélkül nem beszélhetünk ezek társadalmi elfogadottságáról, és így alkalmazásuk is csak felemás eredménnyel járhat.

Az adatkezelések és technikai eszközök vizsgálata, elemzése arra enged következtetni, hogy a törvényi szabályozás nem képes minden részletkérdésre kitérni. Az egyes konkrét rendszerek telepítése és üzemeltetése során kell gondoskodni arról, hogy a törvényi rendelkezések, az alkotmányos alapelvek tiszteletben tartásával sikerüljön elérni a biztonság növelésével kapcsolatos célokat. A részletek kimunkálása tehát helyi feladat, és ehhez zsinórmértékül a szakterületen alkalmazott legjobb gyakorlatok tanulmányozását és megvalósítását ajánlhatjuk.

Természetesen nem szükséges mindenhol elölről kezdeni a helyes magatartási módok kidolgozását. Ma már léteznek és elérhetők azok a szabványok, ajánlások, módszertanok, amelyek számos ország és nemzetközi szervezet ismereteinek, gyakorlatának

felhasználásával követendő mintát tudnak mutatni az információs technológia privacy-konform felhasználására.

EU-tagállamként Magyarország számára az Európai Szabványügyi Bizottság (European Committee for Standardization, CEN) 1997 közepén elindított kezdeményezésének, az Információs Társadalom Szabványosítási Rendszer (Information Society Standardization System) nevű projekt[8] (CEN/ISSS) követése volna kézenfekvő, amelynek célja az információs társadalom közegében megjelenő, a szabványosítás hagyományos és újszerű módjai segítségével megoldható kérdések azonosítása és e kérdések rendezése.

A CEN/ISSS keretében indult meg az a projekt, amelynek célja annak vizsgálata, hogy szükséges és lehetséges-e az EU adatvédelmi irányelvéhez kapcsolódóan olyan szabványok megalkotása, amelyek a piaci szereplők számára segítséget nyújthatnak az irányelv és az egyéb adatvédelmi rendelkezések követéséhez; amennyiben a projekt keretében – legalább meghatározott kérdések esetében – a válasz pozitív, akkor pedig annak meghatározása, hogy a szabványosításnak egy adott kérdésben milyen előnyei és hátrányai vannak. A projekt keretében jelenleg a digitális azonosítás, illetve személyazonosság kérdéseit kutatják.

Az auditálás hasznossága

Az adatvédelmi auditálás[9] általánosságban az az eljárás, amelynek során külső szakértő értékeli az adatkezelő adatvédelmi intézkedéseit és elképzeléseit, valamint az elképzelések megvalósításának képességét, és az adatkezelőt az értékelés pozitív eredményének nyilvánosságra hozatalára jogosítja fel. E meghatározás szerint az auditálás feltételezi egyrészt az adatkezelő tudatos, célirányos adatvédelmi tevékenységét, az adatvédelmi elképzelések ellenőrizhető és számon kérhető rögzítését és az eredmények folyamatos belső ellenőrzését.

Szükség van másrészt olyan ellenőrző szervezetre, amely az ellenőrzést nem hatósági jogkörök alapján, hanem szakmai megbízhatóság és társadalmi elfogadottság alapján végzi; az auditálási eljárásban az ellenőrző szerv nem szankciót helyez kilátásba kedvezőtlen értékelés esetén, hanem ösztönző jogkövetkezményt kedvező értékelés esetén. A külső szerv általi értékelés lényegében az adatkezelő belső ellenőrzésének hitelesítését – auditálását – jelenti. Az auditálás összességében nem elsősorban a fennálló követelmények megtartását kéri számon, hanem jövőbeli erőfeszítések megtételére ösztönöz – az intézmény ezzel hatékony kiegészítője lehet a korábbi adatvédelmi ellenőrzési formáknak. Az auditálás az eredmény közzétételével végső soron a nyilvánosságot teszi a legfontosabb ellenőrző tényezővé.

Az adatvédelmi auditálás koncepciója megfelel az adatvédelem dinamikus rendszerként történő értelmezésének. Az audit – mint az önellenőrzés és a külső ellenőrzés együttese – alkalmas arra, hogy meghatározza a vizsgált adatkezeléssel kapcsolatban felmerülő adatvédelmi kockázatokat csökkentő eszközök körét, valamint arra, hogy az adatkezelőt a védelmi eszközöknek a módosuló adatkezelési feltételek szerinti továbbfejlesztésére ösztönözze. Az értékelés tárgyát elsősorban az adatkezelő adatvédelmi elképzelései és az elképzelések megvalósítására való alkalmasság jelenti (dinamikus tényezők), amihez elengedhetetlen a tényleges adatvédelmi eszközrendszer értékelése is (statikus tényező).

Az audit, mint az ellenőrzés és az ösztönzés módszere, hatékonyan hozzájárul ahhoz, hogy az adatkezelő a legmegfelelőbb eszközökkel és intézkedésekkel az elvárható legmagasabb adatvédelmi színvonalat garantálja, azaz megvalósítsa az adatvédelmi „legjobb gyakorlatot". Mivel az auditálás fontos eleme a pozitív eredmény megjelenítése a nyilvánosság felé, az intézmény arra is alkalmas, hogy „felmutassa" a „legjobb gyakorlatot", követhető mintát állítson más adatkezelők elé.

A szabványoknak való megfelelés eredményeként az adatkezelő szervezeten belüli folyamatok ellenőrizhetőbbé válhatnak. Az ellenőrizhetőség pedig olyan tényező, amely a rendszerek alkalmazásához fűződő bizalom növelése irányába hat.

Ennek következtében növekedhet az ilyen hatékony informatikai rendszereket alkalmazó tisztességes adatkezelők száma.

Az adatvédelmi auditálás további lehetséges következménye az egyes adatkezelők azonos szempontokat követő, hiteles összehasonlíthatósága.

Az auditáláshoz fűzött jogkövetkezmények

A hazai adatvédelmi szabályozás egyelőre nem ismeri az auditálás intézményét, így természetesen jogkövetkezményekről sem beszélhetünk, tehát a következő gondolatok csak a szerző hipotéziseként értékelhetők. Hipotézis, amely mögött azonban az az erős meggyőződés áll, hogy az adatvédelmi audit az adatvédelem olyan új eszköze, amely tartalmazza az önszabályozás és a verseny elemeit, és kiegészíti az adatvédelem rendszerszabályozó eszközeit. Annak a lehetőségnek a biztosítása, hogy az adatkezelő adatvédelmi erőfeszítéseivel bizalmat teremthet maga iránt, az adatkezelőt olyan önkéntes adatvédelmi rezsim létrehozására ösztönzi, amely hozzájárul az adatvédelem színvonalának folyamatos javulásához.

Az adatvédelmi audit célja egyrészt a pillanatnyi állapot összevetése az elvárt állapottal. Ez feltétele-

zi az adott adatvédelmi színvonal feltérképezését, az adatkezelés technikai, szervezeti, eljárási körülményeinek felmérését. Az összehasonlíthatóság feltételezi továbbá valamiféle „optimális" adatvédelmi színvonal megfogalmazását, olyan értékelési szempontok rögzítését, amelyek mentén meghatározható a fejlődés iránya.

A fennálló és az elvárt állapot közötti eltérés megállapítása önmagában nem teszi érdekeltté a szolgáltatókat az auditálásban. Az audit célja tehát másrészt az, hogy olyan környezetet teremtsen, amelyben megtérülnek a magas adatvédelmi színvonal elérésére irányuló befektetések. E cél elérését sok és sokféle ösztönző segítheti.

Ilyen jogkövetkezmény lehet egyes olyan adatvédelmi terhek megszűnése vagy egyszerűsödése, mint az előzetes ellenőrzési kötelezettség vagy a bejelentési kötelezettség. A jogalkotó részéről biztosított ösztönző lehet például az auditált adatkezelők adminisztrációs kötelezettségeinek egyszerűsítése (pl. az adatvédelmi nyilvántartással kapcsolatban), vagy akár a nekik nyújtott adókedvezmény, a piaci szereplők részéről pedig az adatvédelmi kockázatok csökkentéséért megállapított alacsonyabb biztosítási díj.[10]

Az auditból származó legnagyobb előny azonban az lehet, ha az a felhasználók döntéseinek befolyásolójává válik. Az audit intézménye ezért feltételezi az érintettek adatvédelmi tudatosságát, és egyúttal hozzá is járul annak erősödéséhez. Kiemelkedő szerepe lehet az érintettek és az adatkezelők közötti bizalom megalapozásában, ami az elektronikus szolgáltatások működéséhez elengedhetetlen. Az audit tehát egyfajta adatvédelmi minőség-ellenőrzés és minőségjelzés.

Lábjegyzet

[1] Az adatvédelmi biztos beszámolója 2008. Adatvédelmi Biztos Irodája. Budapest, 2009. 126. o.

[2] Elhangzott „Az elektronikus közigazgatás alkalmazásának lehetőségei és elkerülendő kockázatai" című konferencián a Miskolci Egyetem Állam- és Jogtudományi Karán 2009. március 31-én.

[3] Galántai Zoltán (2003): E-privacy olvasókönyv. Arisztotelész Kiadó, Budapest, 6. o.

[4] V. ö. Balogh Zsolt György (1998): Jogi informatika. Dialóg Campus Kiadó. Pécs, 170–171. o.

[5] Jóri András (2005): Adatvédelmi kézikönyv. Osiris Kiadó. Bp., 17. o.

[6] Balogh: id. mű. 169. o.

[7] V. ö. Az adatvédelmi biztos beszámolója 2008. 127. o.

[8] http://www.cen.eu/cenorm/sectors/sectors/isss/about_isss/index.asp 2009. május 10.

[9] Balogh Zsolt György – Jóri András – Polyák Gábor (2002): Adatvédelmi „legjobb gyakorlat" kialakítása az elektronikus közigazgatásban. Szakmai anyag az Informatikai és Hírközlési Minisztérium számára, december, 20.1. fejezet. 324. o.

[10] Königshofen, T. (2000): Chancen und Risiken eines gesetzlich geregelten Datenschutzaudits, DuD, 6. 358. o.

Felhasznált irodalom

Az adatvédelmi biztos beszámolója 2008. Adatvédelmi Biztos Irodája. Budapest

Balogh Zs. Gy. (1998): Jogi informatika. Dialóg Campus K, Pécs

Balogh Zs. Gy. – Jóri A. – Polyák G. (2002): Adatvédelmi „legjobb gyakorlat" kialakítása az elektronikus közigazgatásban. Szakmai anyag az Informatikai és Hírközlési Minisztérium számára

Galántai Z. (2003): E-privacy olvasókönyv. Arisztotelész Kiadó, Budapest

Jóri A. (2005): Adatvédelmi kézikönyv. Osiris Kiadó, Bp.

Königshofen, T. (2000): Chancen und Risiken eines gesetzlich geregelten Datenschutzaudits, DuD, 6/2000. 358. o.