

A hírközlési szolgáltatások igénybevétele során felmerülő adatvédelmi kötelezettségek különös tekintettel a hírközlési forgalmi adatok kezelésére vonatkozó közösségi irányelvvel kapcsolatos alkotmányossági problémákra

BEVEZETÉS

Jelen tanulmány célja, hogy áttekintést adjon a hírközlési szolgáltatók adatvédelmi kötelezettségeiről, különös tekintettel a forgalmi adatokkal kapcsolatos adatvédelmi problémákra. A témának különös aktualitást ad, hogy az EU jogszabálytervezetet (Ebben a témakörben a különböző európai uniós szervek különböző elnevezésű jogszabálytervezeteket (*Directive, Decision*) alkottak, melynek magyarázata, hogy a szervek között a jogalap és a kompetencia kérdésében vita volt, végül is azonban megegyezés alakult ki arról, hogy a jogszabály Irányelv formájában jelenjen meg.) dolgozott ki és fogadott el, amelyben a hírközlési szolgáltatók ilyen jellegű kötelezettségeit meg kívánja szigorítani. A szigorítás mögött azon terroresemények húzódnak meg, melyek az utóbbi években a fejlett országok nyilvánosságát több ízben is megrázták. Ezen sajnálatos eseményekkel összefüggésben terelődött a figyelem a hírközlési szolgáltatások egyre növekvő jelentőségére.

A hírközlési szolgáltatások jelentősége egyrészt lemérhető azon, hogy manapság bármiféle tevékenység - így a terrorista szervezkedés - összehangolt folytatása sem nélkülözheti az elektronikus kommunikációt, ugyanakkor ezen eszközök használata a bűnüldözést is segíti az elkövetők megfigyelése, leleplezése során. Az említett események során azonban minőségileg új szakaszába lépett a hírközlési hálózatoknak a bűncselekmények megvalósításához való felhasználása. A terrorcselekmények elkövetői már nemcsak kommunikációra használták a hírközlési eszközöket, hanem számos

A szerző a Köves Clifford Chance Ügyvédi Iroda Hírközlési és informatikai csoportjának szenior ügyvédje, 1998-ban a Bázeli Egyetemen Mesterfokozatot szerzett, jelenleg az ELTE 2. éves PhD hallgatója.

alkalommal a robbanószerkezetek kioldása is mobiltelefon segítségével történt.

Ez a jelentős változás ösztönözte egyes EU tagországok kormányait (Nagy-Britannia, Franciaország, Írország, Svédország), hogy olyan jogszabálytervezetet alkossanak, amely lényegesen megszigorítja a hírközlési szolgáltatók forgalmi adatok megőrzésére vonatkozó kötelezettségét. A jogszabálytervezetet több oldalról is kritika érte. Egyrészt, támadták a kibocsátás jogalapját, mivel egyesek szerint nem a szupranacionális együttműködést megvalósító Unió Szerződés, hanem a Belügy- és Igazságszolgáltatási Együttműködés keretében szabályozható ez a kérdéskör. Mások a liberális szabadságjogok nevében

A hírközlési szolgáltatások jelentősége egyrészt lemérhető azon, hogy manapság bármiféle tevékenység - így a terrorista szervezkedés - összehangolt folytatása sem nélkülözheti az elektronikus kommunikációt, ugyanakkor ezen eszközök használata a bűnüldözést is segíti az elkövetők megfigyelése, leleplezése során.

emelték fel hangjukat mivel az állami mindenhatóság törekvését vélték felfedezni a tervezetben. Noha az EU parlamentje a tervezetet 2005. szeptember 28-án leszavazta, a tervezet készítői rögvést bejelentették, hogy alapvető céljukat nem adják fel, és átdolgozták a tervezetet oly módon, hogy az a Parlament

kifogásait figyelembe vegye. Az átdolgozott szöveget decemberben a Parlament már elfogadta, ezt követően pusztán formalitást jelentett 2006. február 21-én az Európai Tanács jóváhagyása.

A dolgozat első részében áttekinti az adatvédelmi szabályozás fejlődését, a hírközlési szolgáltatók speciális adatvédelmi kötelezettségeit. Ezt követően az Irányelv, illetve annak alkotmányos szempontból történő értékelése következik.

1. Az Európai Unió adatvédelmi szabályozása

Az Európai Unió alapító szerződése 6. cikkének (2) bekezdése kimondja, hogy „az Európai Unió tiszteletben tartja az alapvető jogokat mint a közösségi jog általános alapelveit, ahogyan azokat az Európai Emberi

Jogi Egyezmény garantálja, és ahogyan azok a tagállamok közös alkotmányos hagyományából következnek.”

(a) Az Európai Emberi Jogi Egyezmény 8. cikke garantálja a magánélet védelméhez való jogot és a személyes adatok védelméhez való jogot.

(b) Az Európa Tanács Adatvédelmi Egyezménye a legfontosabb európai adatvédelmi dokumentum, amelyet az EU magára nézve kötelezőnek fogad el, és az Acquis Communautaire (közösségi jogi vívmányok) részeként ismer el.

(c) Az Európai Parlament és a Tanács 95/46 EK irányelve az egyének személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról.

(d) Az Európai Parlament és a Tanács 97/66 EK irányelve a személyes adatok feldolgozásáról és a magánélet védelméről a telekommunikációs szektorban.

(e) Az előbbi Irányelv átdolgozása az Európai Parlament és a Tanács 2002/58 EK irányelve a személyes adatok az elektronikus kommunikációs ágazatban történő feldolgozásáról és a magánélet védelméről.

Az Európai Unió Alkotmányára vonatkozó nemzetközi egyezmény - mely kérdéses, hogy ebben a formában egyáltalán hatályba lép-e - alapvető szabadságjogokkal foglalkozó fejezetének II-68. cikke is rögzíti a személyes adatok védelméhez való alkotmányos jogot. A témánk szempontjából a 2002/58 EK irányelv tartalmazza a legérdekesebb szektor-specifikus szabályozást. Az irányelv hatálya a közcélú elektronikus kommunikáció teljes körére kiterjed - beleértve az Internetet és a mobil távközlési szolgáltatást is -, függetlenül az igénybe vett technikai megoldásoktól. Nem tartozik viszont a hatálya alá a közcélú hírközlési hálózaton keresztül nyújtott műsorszolgáltatás (kábeltevé). Az irányelv definiálja a forgalmi, illetve helymeghatározási adat, a kommunikáció, a telefonhívás, az értéknövelt szolgáltatás és az elektronikus levél fogalmát.

A 2002/58 EK Irányelv preambuluma kifejti, hogy az elektronikus távközlési

hálózatok felhasználóinak végberendezései és az azokon tárolt minden információ a felhasználók magánszférájának részét képezik, amely megköveteli az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény szerinti védelmet. Az ún. kémszoftverek, webpoloskák, rejtett azonosítók és más hasonló eszközök a felhasználó tudta nélkül hozzáférhetnek a felhasználó végberendezéséhez információszerzés, rejtett információk tárolása vagy a felhasználó tevékenységeinek követése céljából. Mivel ez súlyosan sértheti

a felhasználóknak a magántitokhoz fűződő jogát, ezeket az eszközöket kizárólag törvényes céllal, az érintett felhasználók tudtával lehet alkalmazni.

A preambulum kitér arra is, hogy ilyen eszközök - mint például az úgynevezett cookie-k (azonosításra szolgáló kódsorozatok) - törvényes és hasznos eszközök lehetnek, például a honlaptervezés és a hirdetés hatékonyságának elemzése, valamint az on-line ügyletekben részt vevő felhasználók azonosítása során. Törvényes célú használatuk azzal a feltétellel engedélyezhető, hogy a felhasználók - a 95/46/EK irányelvnek megfelelően - világos és pontos információt kapnak a cookie-k vagy a hasonló eszközök céljáról. A felhasználók figyelmét fel kell hívni az általuk használt végberendezésen elhelyezett információkra. A felhasználóknak lehetőséget kell adni arra, hogy megtagadják a cookie-k vagy hasonló eszközök tárolását végberendezésükön. Ez különösen fontos, ha az eredeti felhasználón kívül más felhasználók is hozzáférhetnek a végberendezéshez, és ez által minden, a berendezésen tárolt magánjellegű információhoz is.

Az Irányelv rendelkezései teljes mértékben átültetésre kerültek a magyar jogba, ezért azok részletes tárgyalására a magyar szabályozás ismertetése során térek ki.

2. Az adatvédelem hírközléssel és internettel való kapcsolata

2.1 Az elektronikus kereskedelem

Az *internetes kereskedelem* (e-commerce, m-commerce) a magyar jogi szabályozás szerint – általános jellemzőit tekintve – kereskedelmi tevékenységekkel azonos megítélés alá esik. E kereskedelmi formával foglalkoz-

hat a Magyarországon létrehozott, illetve a képviseletet, fióktelepet alapító külföldi székhelyű vállalkozás. Az elektronikus úton kötött szerződések távollevők között létrejött adásvételi szerződések, mint utáni vételként

határozhatók meg.

Az új információs technológiák az elektronikus kereskedelem rohamos elterjedését eredményezték. Az elektronikus kereskedelem kétségtelen előnye a gyorsaság, valamint, hogy lényegesen csökkenthető az áru árban értelemeszerűen megjelenő marketing, tranzakciós és egyéb (üzlet-helyiség fenntartása, eladók foglalkoztatása) költségek és így a fogyasztók kedvezőbb áron vásárolhatják meg az adott terméket vagy szolgáltatást.

2.2 Az új technológiákból fakadó veszélyek

Az új információs technológiák alkalmazása az előnyök mellett veszélyeket is magában rejt, ugyanis fokozott a fogyasztók megtévesztésének, félrevezetésének veszélye. A fogyasztók szempontjából nagy kockázatot jelent, hogy szerződéskötéskor a fogyasztó és az eladó földrajzilag egymástól távol van, így nincs lehetőség a termék vagy szolgáltatás megvizsgálására, és ebből következően olyan áru vagy szolgáltatás lesz a szerződés tárgya, amelynek lényeges tulajdonságai a vásárló előtt egészen a teljesítésig rejtve maradnak. A másik nem elhanyagolható veszély, hogy a távközlő eszközök alkalmasak arra, hogy a fogyasztó adatainak (lakcím, e-mail cím, telefonszám stb.) megszerzésével agresszív módon elárasszák az eladási és reklámcélú ajánlatokkal, prospektusokkal a fogyasztókat, betolakodva és sértve ezzel a személyek magánszféráját. Mindezen veszélyek miatt nagyon fontos szempont a megfelelő adatvédelmi és fogyasztóvédelmi garanciák kialakítása.

Legújabbán pedig az ún. 3G-s mobiltelefonos alkalmazások lehetővé teszik, hogy a szolgáltatók meg tudják határozni azt, hogy földrajzilag hol vannak felhasználóik, így képesek felhívni a figyelmüket bizonyos helyszínekre, mint például színházakra, éttermekre vagy vásárlási lehetőségekre. Adott személy tartózkodási helyére vonatkozó adatok megismerése azonban számos, az adatvédelemmel és adatbiztonsággal kapcsolatos kérdést vet fel. A mobiltelefonok igénybevételével megvalósuló termék- és szolgáltatásnyújtás tehát

különösen érinthet alkotmányos alapjogokat, és az e jogok tiszteletben tartására vonatkozó feltétlen kötelezettségeket.

3. A hírközlési szolgáltatók adatvédelmi kötelezettségei

A kötelezettségeket az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: „Eht.”) meglehetősen részletességgel tárgyalja. (Általános adatvédelmi szabályokat tartalmaz az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 13/A §-a is, azonban e törvényhez képest az Eht. *lex specialis*nek tekinthető, ezért az Eht. szabályai kerülnek részletes bemutatásra.) A hírközlési szolgáltatókat adatvédelmi kötelezettségek egyrészt az előfizetők személyes adatainak védelme, valamint a forgalmi és számlázási adatok védelme tekintetében terheli. Az Eht. 154. § (1) bekezdése szerint „a szolgáltató az elektronikus hírközlési szolgáltatásra irányuló szerződés létrehozatala, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése céljából kezelheti a felhasználó, illetve előfizető azonosításához szükséges és elégséges személyes adatot”.

Amint az idézett rendelkezésből látható, a hírközlési szolgáltatók adatkezelése célhoz kötött, és jól körülhatárolt, a hírközlési jogviszony „lebonyolításához” feltétlenül szükséges adatkezelésre szorítkozik.

A hírközlési szolgáltató jogosult a díjak számlázásához és a szolgáltatás igénybevételéhez kapcsolódó adatok kezelésére is. A hírközlési szolgáltatóknak biztosítaniuk kell, hogy az előfizetők a szolgáltatás igénybevétele során bármikor tájékozódhassanak, hogy a szolgáltató mely adatkezelési célokból, milyen személyes adatokat kezel.

3.1 A közlemény bizalmassága

A hírközlési szolgáltatók biztosítani kötelesek a közlés, közlemény bizalmasságát, melynek keretében a közlés és a közléshez kapcsolódó forgalmi adatok jogosulatlan lehallgatásának, tárolásának vagy megfigyelésének, valamint a véletlen hozzáférésnek a megakadályozása a feladatuk. A szolgáltatók a továbbított közlések tartalmát csak olyan mértékben ismerhetik meg, illetve azokat csak olyan mértékben tárolhatják, amely a szolgáltatás nyújtásához műszakilag elengedhetetlenül szükséges. Ennek a szolgáltató oly módon

tehet eleget, hogy műszaki és szervezési intézkedésekkel gondoskodik a nyújtott szolgáltatás biztonságának védelméről.

A szolgáltató tájékoztatni köteles az előfizetőt a szolgáltatás biztonságát veszélyeztető, a szolgáltató által megtett műszaki és szervezési intézkedések ellenére fennmaradó ismert kockázatokról, és a védelem érdekében az előfizető által tehető intézkedésekről. A szolgáltató e tájékoztatásának ki kell terjednie az előfizető által a továbbított közlések bizalmosságának védelme érdekében használható szoftver és titkosítási megoldások alkalmazásának lehetőségeire. A személyes adatokat a szolgáltatók az előfizetői szerződésből eredő igények elévüléséig kezelhetik, kivéve, ha más törvény az adatkezelésre eltérő határidőt ír elő.

3.2 Forgalmi és számlázási adatok

3.2.1 Az adatkezelés általános szabályai

Az Eht. szerint az elektronikus hírközlési szolgáltatóknak a szolgáltatás teljesítése után törölniük (ideértve az anonimizálást is) kell az előfizetőkre és a felhasználókra vonatkozó személyes adatokat, amelyeket a hívások létrehozása céljából feldolgoznak.

A szolgáltatók az előfizetők és a felhasználók részére történő számlázás és a kapcsolódó díjak beszedése, valamint az előfizetői szerződések figyelemmel kísérése céljából az előfizetők személyes adatait kezelhetik. Az elektronikus hírközlési szolgáltató saját üzletszerzési céljából - az előfizető kifejezett előzetes hozzájárulásával - kezelhet előfizetői személyes adatokat.

A szolgáltató a hívás vagy egyéb szolgáltatás típusa, iránya, kezdő időpontja és a lefolytatott beszélgetés időtartama, illetőleg a továbbított adat terjedelme, mobil rádiótelefon szolgáltatásnál a szolgáltatást nyújtó hálózat és cella, valamint a szolgáltatás igénybevételekor használt készülék egyedi azonosítója (IMEI), IP hálózatok esetén az alkalmazott azonosítókat tartalmazó, a rendszerében keletkezett fájlokat (CDR) az annak alapján kiállított számlára vonatkozó, az elévülést követő 1 év után, 30 napon belül köteles törölni.

3.2.2 Az adatok átadhatósága

Bennfentes kereskedelem, piacbefolyásolás, engedély nélküli szolgáltatás végzése ügyében indított eljárás esetén bizonyos adatok átadhatók a Pénzügyi Szervezetek Állami Felügyeletének.

Ezenkívül egyes adatok, amelyek az adatkezelés céljához szükségesek, átadhatók:

(a) azoknak, akik az elektronikus hírközlési cég megbízása alapján a számlázást, a

vetelések kezelését, a forgalmazás kezelését, illetőleg az ügyfél-tájékoztatást végzik;

(b) a számlázási és forgalmazási jogviták rendezésére jogszabály alapján jogosult szervek részére;

(c) a nemzetbiztonság, a honvédelem és a közbiztonság védelme, a közvédelem és a közbiztonság védelme, a közvédelem bűncselekmények, valamint az elektronikus hírközlési rendszer jogosulatlan vagy jogsértő felhasználásának üldözése céljából az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságoknak, az ügyészségnek, valamint a bíróságnak;

(d) a bírósági végrehajtásról szóló törvény előírásai szerint a végrehajtónak.

Az átadott adatokkal kapcsolatban az adatokat átvevőket a szolgáltatóval azonos titoktartási kötelezettség terheli.

Az elektronikus hírközlési szolgáltató a fent megjelölt adatokat adatszolgáltatás biztosítása céljából köteles 3 évig megőrizni.

Az elektronikus hírközlési szolgáltató a fent megjelölt adatokat adatszolgáltatás biztosítása céljából köteles 3 évig megőrizni.

Ha valamely értéknövelt - vagyis az alapszolgáltatást meghaladó funkcionalitással bíró - szolgáltatás nyújtásához a forgalmi adatokon kívüli helymeghatározási adatok szükségesek, ebben az esetben a hírközlési szolgáltató ezen adatokat az előfizető hozzájárulása estén kezelheti és csak olyan mértékben és időtartamig, amely szükséges az értéknövelt szolgáltatás nyújtásához.

3.3 Az előfizetői névjegyzék

Az elektronikus hírközlési szolgáltatások előfizetőinek névjegyzékeit széles körben hozzáférhetővé és nyilvánosá kell tenni. A természetes személyek magánéletének védelme és a jogi személyeknek a jogos érdeke megkívánja, hogy az előfizetők maguk dönthessék el, hogy személyes adataik megjelenjenek-e valamely előfizetői névjegyzékben, és ha igen, pontosan mely adatok. A nyilvános előfizetői névjegyzékek szolgáltatóinak az ilyen névjegyzékekben feltüntetendő előfizetőket tájékoztatniuk kell a névjegyzék céljáról, továbbá minden olyan felhasználási célról, amely a nyilvános előfizetői névjegyzék elektronikus változatában - különösen a szoftverbe beépített kereső funkciók révén - lehetséges. Így például a fordított keresési funkciók tekintetében, amelyek a névjegyzék felhasználója számára lehetővé teszik, hogy

mindössze egy telefonszám alapján megtalálja az előfizető nevét és címét.

A természetes személyek magánéletének védelme és a jogi személyeknek a jogos érdeke megkívánja, hogy az előfizetők maguk dönthessék el, hogy személyes adataik megjelenjenek-e valamely előfizetői névjegyzékben, és ha igen, pontosan mely adatok.

Védeni kell az előfizetőket attól, hogy a közvetlen üzletszerzés céljából, különösen automatizált hívóberendezéseken, telefaxon és e-mailben - az SMS-üzeneteket is beleértve - küldött, nem kívánt tájékoztatás az előfizetők magánéletét zavarja. A nem kívánt reklámküldemények ilyen formái egyrészt viszonylag könnyen és olcsón elküldhetők, másrészt a címzettre terhet és/vagy költséget róhatnak. A közvetlen üzletszerzési célú, nem kívánt tájékoztatás ilyen formái tekintetében indokolt megkövetelni azt, hogy ilyen tájékoztatást csak a címzettek előzetes és kifejezett hozzájárulásának megszerzését követően lehessen küldeni.

4. A hírközlési forgalmi adatok megőrzéséről szóló irányelv

A tanulmány bevezetőjében említett események kapcsán az EU a forgalmi adatokkal kapcsolatos megőrzési kötelezettséget jelentősen ki kívánja szélesíteni. Egyes kritikusok ezzel

kapcsolatban az állami kontroll túlbúrjánzásától, a privát szféra sérelmétől tartanak.

4.1 Az Irányelv alapvető rendelkezései

Az Irányelv előírja a kommunikációs szolgáltatók számára valamennyi, a kommunikációs partnerek kilétének, elhelyezkedésének, csakúgy, mint a kommunikáció módjának, az időtartamának és útvonalának meghatározá-

sához szükséges kommunikációs adatok megőrzését. Az ilyen adatok megőrzésére a hírközlési szolgáltatók - a tagállami implementációtól függően - legalább 6, de legfeljebb 24 hónapig kötelesek. A tárolandó adatmennyiség így jelentősen meghaladná a számlázáshoz vagy a kommunikációs szolgáltatók számára egyéb, legitim célok érdekében tárolni szükséges adatok mennyiségét. Ezen felül az Irányelv alapján a jogalkalmazó szervek „súlyos” bűncselekmények kapcsán folytatott nyomozás, illetve vádeljárás során

Az új információs technológiák alkalmazása az előnyök mellett veszélyeket is magában rejt, ugyanis fokozott a fogyasztók megtévesztésének, félrevezetésének veszélye. A másik nem elhanyagolható veszély, hogy a távközlő eszközök alkalmasak arra, hogy a fogyasztó adatainak (lakcím, e-mail cím, telefonszám stb.) megszerzésével agresszív módon elárasszák az eladási és reklámcélú ajánlatokkal, prospektusokkal a fogyasztókat, betolakodva és sértve ezzel a személyek magánéletét.

jogosultak az ilyen adatokhoz való hozzáférésre. A nyomozati szervek e joga a tagállami szabályozásban rögzített bűncselekmények esetén, a vonatkozó büntető eljárási normák szerint gyakorolható.

Az ilyen adatok megőrzésére a hírközlési szolgáltatók - a tagállami implementációtól függően - legalább 6, de legfeljebb 24 hónapig kötelesek.

Ezek a bűnüldözés számára releváns adatok a kommunikációs hálózatok használata esetén bármely módon előállhatnak, így telefon, SMS, MMS, Voice over IP (VoIP) és Internet használata esetén egyaránt. Fontos megjegyezni, hogy az Irányelv tárgyi hatálya nem terjed ki az elektronikus hálózaton folytatott kommunikáció tartalmára, ezen „lehallgatás” típusú tevékenységek EU szintű jogharmonizációjáról nincs szó.

4.2 A privátszféra sérülése

A folyamatos változásnak, a technológiai fejlődésnek és a gyorsan terjedő Internet- és mobilhasználatnak köszönhetően a kommunikációs adatok jelentős információforrássá léptek elő. Átfogó információk szerezhetők a felhasználók és az egyéni kommunikációs útvonalak nyilvántartásba vételével. Közben a felhasználó weblapokat keres fel, egy sor adatot hoz létre, amely alapvetően különbözik a korábbi idők telefonforgalmának adataitól. Az ilyen technológiák interaktív használata lehetővé teszi - pl. az IP címek rögzítése révén, amelyek könnyen alakíthatók át domain nevekké - egy, az egyén személyes érdeklődését, preferenciáit, tevékenységét tartalmazó átfogó nyilvántartás kiépítését. Ezen felül a mobil telefonokról rögzített adatok alapján akár az egyén tartózkodási helye is feltárható. Ezen adatok felhasználásával lehetővé válik azon időszakok meghatározása, amikor két egyén azonos cella-azonosítón belül együtt tartózkodik, illetve ha együtt érkeznek oda, vagy távoznak onnan. Következésképpen elegendő információ szerezhető be egy, akár az emberi kapcsolatokat ábrázoló térkép elkészítéséhez. Az Irányelv tulajdonképpen azt sem zárja ki, hogy egy valamennyi egyéni profilt tartalmazó, átfogó nyilvántartás kerüljön kialakításra.

4.3 Az Irányelv értékelése alkotmányos szempontból

Az alapvető alkotmányos jogok áthatják a jogrendszer egészét, ugyanakkor e jogokat többrétegű védelmi rendszer oltalmazza. Egyrészt a különböző jogágakban elhelyezett szabályok mögöttes tartalmaként jelennek meg, másrészt e jogszabályok védelmi rend-

szere érvényesülésüket biztosítja. A sokrétű védelmet mindenekelőtt az alapvető jogok sokszínűsége, összetettsége indokolja.

Az alapvető jogok nem alkotnak zárt, koherens rendszert, hanem olykor összeütközésbe kerülnek egymással. A témánk szempontjából azt érdemes megvizsgálni, hogy az alapvető jogokat lehet-e korlátozni, illetve, hogy hol helyezkedik el az egyes alapjogok határa. Ezen megközelítés alapján megkülönböztethetünk abszolút és korlátozható alapjogokat.

Az Alkotmánybíróság autentikus elemzése alapján az *abszolút jogok* csoportjába - vagyis abba a csoportba, amelyeket nem lehet korlátozni - két egymással összeforrott jog szerepel. Az emberi élethez és méltósághoz való jog. Minden más alapjog hierarchiában ezek alatt helyezkedik el. A többi alapjog, a fentebb említettekkel való ütközés esetén mindig alulmarad. Mérlegelésre tehát csak abban az esetben kerülhet sor, ha az összeütközésben lévő jogok egyike sem tartozik ezek közé. A mérlegelés eredményeképpen az ún.

gyengébb jog (korlátozható alapjog) kerül korlátozásra, feloldva ezzel az összeütközést.

Az Irányelv esetében egy alapjog-közérdek típusú összeütközésről van szó. Az egyén integritása, magánszférához való joga, a magántitok védelme, a személyes adatok védelme - melyek az általános személyiségi jog származékai - találhatók az egyik oldalon, míg a másik oldalon a közbiztonság, köznyugalom fenntartásában megnyilvánuló közérdek található. Az Alkotmánybíróság, mind a két oldalon található érdekek pontos tartalmának értelmezésével foglalkozott már határozataiban.

a) A magánszférához való jog, magánélethez való jog, magántitok, a személyes adatok védelme

Az Alkotmánybíróság rámutatott arra, hogy az Alkotmány 54. § (1) bekezdésében található emberi méltósághoz való jog, az általános személyiségi jog egyik megfogalmazása, a személyiségi jogok anyajoga. Mint anyajog ebből származtatathatók olyan konkrét alapjogok, mint például a *magánszférához való jog* is, amelyet az Alkotmány nem nevesít. Viszont az 56/1990 (XI. 10.) AB határozat egyértelműen rögzíti: „A *magánszférához való jog, az önmegvalósítás joga, a személyiség szabad kibontakozása és az autonómia védelme megköveteli az Alkotmány 8. § (1) bekezdésében írt szempontok érvényesülését, azaz azt, hogy az állam az ember sérthetetlen és elidegeníthetetlen alapvető jogait tartsa tiszteletben és védelmezzé.*”

További támpontot ad az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv. Az Egyezmény 8. Cikke, amely „Magán- és családi élet tiszteletben tartásához való jog” címen foglalkozik a témával a következőket tartalmazza: „1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme,

avagy mások jogainak és szabadságainak védelme érdekében szükséges.”

b) A közérdek mint korlátozást indokló jogelv

A közérdek kifejezés magába foglalja a közbiztonságot és a köznyugalmat, amelyek egy demokratikus jogállami értékeit jelentik.

Ezen értékek biztosításán keresztül próbálja meg elősegíteni az állam az emberi jogok érvényesülését, amelyre az Alkotmány 8. § szerint kötelezettsége is van (ld. 18/2000 (VI. 6.) AB határozat, 13/2001 (V. 14.) AB határozat, 13/2003 (IV. 9.) AB határozat, 41/2003 (VII.2.) AB határozat). Azonban pusztán a közérdek védelmében teendő intézkedések mindegyike nem esik pozitív elbírálás alá. Szükség van valamilyenfajta plusz tartalomra, amely az adott korlátozást konkrét, ténylegesen indokokkal támasztja alá.

Ezért az Alkotmánybíróság működése során kialakította a „nyomós közérdek” fogalmát. Határozataiban kifejtette, hogy csak a „nyomós közérdek” fennállása szolgálhat alapul az alapjogok korlátozásához.

A „nyomós közérdek” fennforgásáról akkor beszélhetünk, ha a védendő érdekek (jelen esetben a közbiztonság, az állam, a társadalmi jólét biztosítása) megóvása érdekében teendő intézkedések *feltétlenül szükségesek*, valamint, az ennek a nevében tett korlátozások *arányosak* is. Ebben az esetben is csak a cél eléréséhez még elegendő, legszükségesebb mértékben lehet korlátozni az emberi jogokat, úgy, hogy a korlátozás ne érintse azok lényeges tartalmát

Amennyiben a szükségesség-arányosság feltételei fennállnak és fennforog a „nyomós közérdek”, valamint a kívánt intézkedések célszerűsége is megállapítható, akkor meghatározott módon és mértékben korlátozni

lehet az érintett alapjogokat, jelen esetben a magánszférához, a magánélethez való jogot, a magántitok, valamint a személyes adatok védelmét.

c) Az arányosság problémája

A korlátozás akkor minősül arányosnak, ha a beavatkozás nem haladja meg a demokratikus társadalomban szükséges mértéket. A távközlési adatmegőrzésre vonatkozó Irányelv a bűnmegelőzés, nyomozás és vádemelés törvényes érdekét szolgálja, és e célok elérésére alkalmas is. Ahhoz azonban, hogy az egyének jogait csorbító rendelkezés arányos legyen, a jogalkotónak általánosságban biztosítania kell, hogy az ilyen beavatkozások nem túlzott mértékűek, azaz a kitűzött cél eléréséhez szükségesek és egyben elégségesek is.

Ebből a szempontból vizsgálható, hogy a rendelkezések sértik-e az európai állampolgárok millióinak magánélethez fűződő jogait annak érdekében, hogy a lakosság egy szűk, bűnöző tevékenységet folytató részéről információk gyűjtése lehetővé váljon. Az összes kommunikációs csatorna szisztematikusan átvizsgálása és a hosszú, akár 24 hónapos megőrzési időszak a magánszféra jelentős korlátozásaként tekinthető. Bár a cél nem az egyéni beszélgetések tartalmának rögzítése, a résztvevők személyazonosságának, tartózkodási helyének, csak úgy, mint az időpont, az időtartam és a kommunikációs útvonal megfigyelése szintén káros lehet.

Említésre érdemes, hogy az Emberi Jogok Európai Bírósága alkalmazhatónak találta a Konvenció 8. par. (1) bekezdését, amikor a román hírszerzőszolgálat elfogott és visszatartott

egy kérelmező állítólagos szélsőséges szervezethez fűződő kapcsolatára vonatkozó információt. Problematikusnak tűnik továbbá, hogy a távközlési szolgáltatók a jövőben a megőrzendő adat helyi tárolására kötelesek, amelynek következtében megnőhet a jogtalan hozzáférés és visszaélés lehetősége.

Mint korábban említésre került, az összegyűjtött adatok képessé tehetnek illetéktelen személyeket bármely európai állampolgárról részletes személyes profil kialakítására. A bűnmegelőzés céljaival összhangban kialakított, a privátszférát jobban tiszteletben tartó adatbázis - a kritikusok szerint - legalább olyan hatásos lett volna, mint egy széleskörű, feleslegesen sok adatot rögzítő rendszer.

4.4 Kritikai észrevételek

Bár a jogérvényesítés kétségtelenül fontos cél bármely társadalomban, az azonban megkérdőjelezhető, hogy ehhez mennyiben járulhatnak hozzá az adatkezelés kötelező követelményei. A kritikusok szerint a szándékolt rendelkezések a kezelendő adatmennyiség jelentős felhalmozódásához vezethetnek, ennek következtében hosszú időbe telhet egy bizonyos információ kikeresése. A bűnfelderítésben való közreműködés így nem valósulhatna meg.

Továbbá a kötelező előírások csak akkor járulhatnak hozzá a büntető eljárás eredményességéhez, ha a távközlési hálózatot használó bűnöző személyek megbízható módon visszakereshetők. A kritikusok szerint valószínűtlen, hogy a kommunikációs jegyzőkönyvek révén e feltétel megvalósítható lenne (pl. a forgalmi zavarok illetve hamisításokán) mivel a hívások, lekérdezések nem feltétlenül a tényleges felhasználóknak tudhatók be. Ezen kívül a szervezett bűnözésben és terrorizmusban érintett személyek könnyen kivonhatják magukat a szabályozás hatása alól az Európai Unión kívüli telekommunikációs eszközök és szolgáltatók igénybe vétele, vagy az előre fizetett telefonos SIM kártyák gyakori cseréje révén.

Az Irányelv sok tekintetben a szándékolt jogharmonizációt nem valósítja meg, hiszen az egyes tagállami jogrendszerek a „súlyos bűncselekmény” fogalmát igencsak eltérően definiálhatják. Jelentős különbséget okozhat, ha valamely tagállam mindössze 6, míg egy másik 24 hónapos

megőrzési kötelezettséget ír elő. Mivel a hírközlési szolgáltatások gyakorlatilag határookra tekintet nélkül nyújthatóak, illetve vehetők igénybe, a rövidebb idejű kötelezettséget előíró tagállam vonzó lesz a hírközlési szolgáltatók számára, míg egyéb tagállamokban a szolgáltatások drágulhatnak. Ez természetesen nem kívánatos versenytörzítő hatásokat is generálhat.

4.5 Összevetés a hatályos magyar szabályozással

Az Irányelvet a hatályos szabályokkal összevetve azt az érdekes következtetést vonhatjuk le, hogy nálunk ezen szabályok átültetése nem jár különösebb megrázkódtatással, hi-

szen jelenlegi szabályaink is legalább ennyire szigorúak. Ezen felismerés meglehetősen érdekesnek tűnik annak fejében, hogy más EU országokban mekkora felzúdulást váltott ki már az Irányelv tervezete is.

Persze, ha jobban belegondolunk, nem meglepő, hogy nálunk a civilszférát mélyebben érintő szabályok hallatán sem szisszenünk fel, azokat természetesnek vesszük. E szabályok így is sokkal demokratikusabbak, polgárbarátabbak, mint a jogtudatunkat még ma is sok tekintetben átható korábbi rendszer szabályai voltak. Az összehasonlítás azonban mégis arra mutat rá, hogy mind a jogszabályok, mind a civil tudatosságunk terén bőven van tér a fejlődésre.

Látható ugyanakkor, hogy konkrét esetre vonatkoztatva – vagyis a terrorizmus elleni küzdelem érdekében a hírközlési információk bűnüldözési szervek általi megismerhetőségére – a nálunk korlátozottabban érvényesülő civil szabadság előnyös lehet, ezért akarnak a nálunk régebbi demokratikus hagyományokkal rendelkező országok is a szabályaikon szigorítani. Semmiképp sem tekinthető vállalkozásbarátnak és követendőnek viszont, hogy az Eht. 92. § (3) bekezdésében előírja, hogy a hírközlési szolgáltatók az ezzel kapcsolatos költségeket maguk kötelesek állni. Ilyen egyértelműen állami feladatot magánvállalkozások eszközeivel megvalósítani nem tűnik alkotmányos szempontból elfogadhatónak, ezért a jogalkotó részéről tanácsos volna a megfelelő kompenzációra való jogosultság törvénybe iktatásán elgondolkodni. Megjegyzendő, hogy hasonló tárgyú vitában már alulmaradt Európai Unió tagállam, amelynek során az érintett állam alkotmánybírósága a magánvállalkozás kompenzáció nélküli kényszerítését államcél megvalósítására alkotmányellenesnek mondta ki. (lásd VfGH, G 37/02-16, 2003. február 27., Osztrák Alkotmánybíróság)

Zárszó

Az adatforgalom felgyorsulásával, és a kommunikációs eszközök rohamos elterjedésével a jogtudományok is komoly kihívásokkal kell szembenéznie a tekintetében, hogy hogyan lehet bizonyos mértékű kontrollt gyakorolni ezen „szabad médiák” felett. Napjainkban ez a kérdéskör az egész világon különös aktualitással bír. Sajnálatos módon mára már bebizonyosodott, hogy a bűncselekmények elkövetői ugyanúgy használják a technika vívmányait, mint az átlagemberek (interne-

Az Irányelvet a hatályos szabályokkal összevetve azt az érdekes következtetést vonhatjuk le, hogy nálunk ezen szabályok átültetése nem jár különösebb megrázkódtatással, hiszen jelenlegi szabályaink is legalább ennyire szigorúak.

tes tartalmak, mobiltelefon segítségével működésbe hozott bombák, fenyegetések stb.). Mivel a technika fejlődésének eme negatív hatásait a világ szinte minden táján megtapasztalta már az emberiség, a többség nem kételkedik abban, hogy ezeket az eszközöket, csatornákat valamilyenfajta kontroll alatt kell tartani.

A közösség, a társadalom létét, biztonságát veszélyeztető cselekmények minél eredményesebb üldözése megkívánja a beavatkozást. A közérdek fogalma, amely magába foglalja a közbiztonság, köznyugalom fogalomköréit is, olyan érdekeket jelenít meg, amelyek

érdekében korlátozások, ellenőrzések alkalmazhatóak. Kérdés az, hogy a beavatkozás milyen mélységű, mértékű lehet. Azáltal, hogy az információáramlás, illetve az azt kezdeményező és az abban résztvevő kontroll alá kerül, a privátszférának egy eddig viszonylag kevésbé szabályozott területe kerül az állami adminisztráció látókörébe. Nem vitás, hogy a több száz vagy akár több ezer ember életét követelő terrorcselekmények kellő alapot jelentenek a kontrollálás, minél teljesebb megfigyelés irányába történő gondolkodásra. A jogász feladata egy jogállamban azonban többek között az is, hogy

biztosítsa, hogy az állami beavatkozás csak a feltétlen szükséges mértékre és eszközökre korlátozódjék.

A mérleg két oldala tehát: a köz érdeke, a közbiztonság köznyugalom a másik oldalra pedig az ember magánszférához való joga, a magánélet szabadságának a joga, magánítok, személyes adatok védelme kerül. Ez a rövid áttekintés a két ellentétes érdek rövid elemzésén keresztül próbált választ adni arra, hogy ezen érdekek összeütközése esetén melyik oldal és milyen mértékben kaphat elsőbbséget a másikkal szemben.

Irodalom

Adatvédelmi Ombudsman Országgyűlési beszámoló 2000-2004

Ádám Antal: *Alkotmányi értékek és alkotmánybíráskodás*. Osiris Kiadó, Budapest, 1998

Garzaniti, Laurent: *Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation*. Sweet & Maxwell, London, 2003

Gellért, György (szerk.): *A Polgári Törvénykönyv magyarázata 1-2*. KJK-Kerszöv, Budapest, 2004

Halmi Gábor - Tóth Gábor Attila: *Emberi jogok*. Osiris Kiadó, Budapest, 2003

Jóri András: *Adatvédelmi kézikönyv*. Osiris Kiadó, Budapest, 2005

Jóri András: *Az adatvédelemről rendszergazdáknak*. In: www.jogiforum.hu

Jóri András: *Az új adatvédelmi törvény elé*. In: PhD tanulmányok. 1. köt. 2004. 201-234.

Péterfalvi Attila: *Az adatvédelem és az információszabadság aktuális kérdései*. In: Polgári Jogi Tudományos Diákkör évkönyve. 2004. 149-156.

Sajó, András: *A szólásszabadság kézikönyve*. KJK-Kerszöv, Budapest, 2005

Zscherpe, Kerstin A. - Stüher, Frank: *Data Retention in Europe*. In: World Internet Law Report, July 2005

VEREBICS JÁNOS

Az elektronikus közbeszerzés szabályozásának új keretrendszere az Európai Unióban és Magyarországon (2. rész)*

Napjaink európai információs társadalmi politikái a közbeszerzési eljárások „elektronizálhatóságának” kérdését két szempontból is kulcsfontosságú elemnek tekintik. A közbeszerzések révén az állam, mint a modern gazdaságok egyik legjelentősebb piaci szereplője vásárlóként jelenik meg, javak és szolgáltatások iránt támaszt közvetlen keresletet: a vállalkozások részéről alapvető igényként merül fel, hogy az újonnan kiírt pályázatokra vonatkozó információkhoz a lehető legszélesebb körben, gyorsan, rendszerezett formában, költség hatékonyan juthassanak hozzá, s hasonló módon tehessek meg esetleges ajánlatukat is. Ezt felismerve minden elektronikus kereskedelmi politika lényeges részét képezi az elektronikus közbeszerzéseket lehetővé tevő feltételrendszer mielőbbi megvalósítása.

A szerző egyetemi adjunktus a Budapesti Műszaki és Gazdaságtudományi Egyetem üzleti jog tanszékén. Szakterületei az információs társadalom – ezen belül különösen az elektronikus kereskedelem és az e-kormányzat – jogi kérdései és az európai üzleti jog.

Ugyanakkor az állami szervek közbeszerzéseik során a költségvetésből származó forrásokat, közpénzeket költenek el: e források hatékony, nyomon követhető felhasználása, a közbeszerzési eljárások költségeinek csökkentése, a pályázatással kapcsolatos cselekmények egyszerűsítése, felgyorsítása és költségkímélőbbé tétele már az elektronikus kormányzati koncepciókon belül jelentkezik követelményként. Mindeme célok az infokommunikációs eszközök, az informatika lehetőségeinek a közbeszerzési eljárásokba való bevezetésével, tudatos, tervezett és jogilag is lehetővé tett felhasználásával érhetőek el.

4.

Az Országgyűlés 2003 decemberében elfogadta a közbeszerzésekről szóló 2003. évi CXXIX. törvényt (Kbt.), amely főszabályként 2004. május 1-jén lépett hatályba. Az új törvény alapvető célja egyrészt a magyar köz-

beszerzési jog szabályainak a közösségi jog irányadó normáihoz való teljes körű igazítása, másrészt a hatályos közbeszerzési törvény 1995. évi megalkotása, és hatályba lépése óta eltelt időszak jogalkalmazási tapasztalatainak hasznosítása, és ennek alapján a közbeszerzési szabályok kiigazítása volt.

A magyar jogszabály-előkészítési folyamat ugyanakkor figyelembe kívánta venni a szabályozott területre vonatkozó közösségi jogalkotás újabb fejleményeiként született irányelv-tervezeteket is. Ezek egyes rendelkezéseit (így az e-közbeszerzésre vonatkozó bizonyos szabályokat is) már a normaszövegbe be is építette, illetőleg felhatalmazást adott arra, hogy az e-közbeszerzés tárgykörében az elektronikusan gyakorolható eljárási cselekmények szabályait, az elektronikus úton történő beszerzés szabályait és a központosított eljárások részletes – a közbeszerzési törvénytől az ilyen eljárások sajátossága miatt szükséges módon eltérő – szabályait kormányrendelet határozza meg (204. § (1) bek.). Ez a felhatalmazás lehetőséget biztosított arra, hogy