TARTALOM

TANULMÁNYOK

DISPUTA

FIGYELŐ – ÜGYÉSZI HÍREK

FIGYELŐ – EGYESÜLETI HÍREK

FIGYELŐ – OKRI HÍREK

FIGYELŐ – EURÓPAI KITEKINTŐ

KÖNYVISMERTETŐ

KÖNYVAJÁNLÓ

MELLÉKLET

TÖRÖK ZSOLT[1]

Hivatali és korrupciós bűncselekmények bírói gyakorlatának aktuális kérdései

E tanulmányban igyekszem a bírói gyakorlat oldaláról bemutatni néhány olyan általam tipikusnak vélt esetet, amelyek akadályai lehetnek az ügyek gyors és szakszerű elintézésének. Ezek megoldása gyorsíthatja az ügyek jogerős befejezését, és így ténylegesen hozzájárulhat az ilyen cselekmények visszaszorításához. Érdemes ennek érdekében a büntetéskiszabási gyakorlatot is áttekinteni.

A hivatali bűncselekmények rendszere

A Btk. XV. fejezetében találhatók az államigazgatás, az igazságszolgáltatás és a közélet tisztasága elleni bűncselekmények. A törvény rendszere alapján – de lege lata – csak azokat a deliktumokat nevezhetjük hivatali bűncselekményeknek, amelyeket a Btk. XV. fejezet IV. címe határoz meg.[2] Nyilvánvaló azonban, hogy a hivatali bűncselekmények köre ettől bővebb, hiszen tágabb értelemben ide sorolhatjuk mindazokat a bűncselekményeket, amelyek alanya csak hivatalos személy lehet.

Egyik jellemző csoportosítási lehetősége e bűncselekményeknek az ún. sajátképi és nem sajátképi hivatali bűncselekményekre való osztása. A Btk. jelenlegi rendszerében a sajátképi hivatali bűncselekmények: a XV. fejezet IV. címében felsorolt deliktumok, a hivatali visszaélés bűntette (225. §), a bántalmazás hivatalos eljárásban bűntette (Btk. 226. §), a kényszervallatás bűntette (Btk. 227. §), a jogosulatlan titkos információgyűjtés bűntette (Btk. 227/A. §) és a jogellenes fogvatartás bűntette (Btk. 228. §). Álláspontom szerint ide kell sorolni a közélet tisztasága elleni bűncselekmények közül a Btk. 250. §-ába ütköző, hivatalos személy által elkövetett vesztegetés bűntettét, valamint a Btk. 275. §-ában megfogalmazott hivatalos személy által elkövetett közokirat hamisítás bűntettét is, mivel ez utóbbi bűncselekmények esetében a hivatalos személyként való elkövetés nem minősítő körülmény, hanem az az alaptényállás eleme. Csak a jogalkotói logika alapján került együtt kodifikálásra a többi korrupciós, illetve közbizalom elleni bűncselekménnyel, e bűncselekmények elhelyezésre kerülhettek volna a hivatali bűncselekmények sorában is.

---

[1] Török Zs., bíró, Fővárosi Ítélőtábla

[2] Angyal Pál több szempont alapján is osztályozza a hivatali bűncselekményeket. Így sajátképi és nem sajátképi, általános és különös, valamint abszolút és relatív hivatali bűncselekményeket különböztet meg. Angyal P.: Hivatali és ügyvédi bűntettek és vétségek. In: A magyar büntetőjog kézikönyve. Athenaeum–Attila-Nyomda, Budapest, 1943. 26. o.

A nem sajátképi hivatali bűncselekmények a következők: a Btk. 177/A. §-ában írt hivatalos személy által elkövetett személyes adattal visszaélés bűntette, a Btk. 244. § (3) bekezdés b) pontjába ütköző hivatalos személy által elkövetett bűnpártolás bűntette, a Btk. 261/A. § (2) bekezdés b) pontjában nevesített hivatalos személyként elkövetett gazdasági tilalom megszegésének bűntette, a Btk. 282/A. (2) bekezdés b) pontjában írt hivatalos személyként elkövetett kábítószerrel visszaélés bűntette, valamint a Btk. 323. § (2) bekezdés c) pontjába ütköző hivatalos személy által elkövetett zsarolás bűntette.

A hivatali bűncselekmények előbbiekben írt csoportosításának nem csupán elméleti jelentősége van. Angyal Pál ennek gyakorlati értelmét így határozza meg: „A hivatali bűncselekmények sajátképi és nem sajátképi osztályokra való kettéosztása a bűnrészesség szempontjából is jelentős. Míg ugyanis a sajátképi hivatali bűncselekményeknél a tettes közhivatalnoki jellege konstitutív személyes körülmény – az extraneus-nak erről való tudomása esetében osztható, azaz büntetőjogi hatásában a nem közhivatalnok részes irányában is érvényesül –, addig a nem sajátképi hivatali bűncselekményeknél a büntethetőség nem függvén a tettesnek közhivatalnoki minőségétől (…) a tettes közhivatalnoki jellegéből származó súlyosítás csak akkor hat ki az extraneus részesekre, amennyiben ezek a részesek – a tettes közhivatalnokságáról tudva – ezt a személyes körülményt eszközül használták fel.[3]

Szerintem további kézzelfogható, gyakorlati haszna is van e csoportosításnak. Általánosságban kimondható, hogy a sajátképi és nem sajátképi bűncselekmények alaki halmazata csupán látszólagos. A specialitás, illetve a konszumpció elve kizárja e különböző csoportokba tartozó hivatali bűncselekmények valóságos alaki halmazatát. Van olyan álláspont, amely szerint általában a hivatali bűncselekmények találkozása kizárja az egymással fennálló alaki halmazatot.

Néhány példa az előzőek alátámasztására:

A 3/2007. BJE elvi éllel fejti ki, hogy ha az elkövető egy cselekményével valósítja meg a hivatali visszaélést és a hivatalos személy által elkövetett személyes adattal visszaélés bűntettét, a bűnösség csak az utóbbi bűncselekményben állapítható meg, az alaki halmazat csupán látszólagos. Korábban az eltérő jogtárgy sértésére hivatkozva az eljáró bíróságok megállapították e két bűncselekmény halmazatát.[4]

Az elsőfokú bíróság – szemben a védői érveléssel, amely hivatalos személy által elkövetett vesztegetés miatt indítványozta a vádlottak felelősségének megállapítását – hivatalos személyként elkövetett zsarolásként minősítette a határőr vádlottak cselekményét, mivel a sértettet azzal fenyegették meg, ha nem fizet nekik, bejegyzik az útlevelébe, hogy 5 évig nem léphet be Magyarország területére. A fenyegetés hatására a sértett 200 DM-et adott át a vádlottaknak. A vádlottak

[3] Angyal, i.m. 29. o.
[4] lásd: BH 2005/338. számon közzétett eseti döntés

cselekménye tényállásszerű a hivatalos személy által kötelességszegéssel elkövetett vesztegetés bűntette vonatkozásában is, ezért joggal merül fel e két bűncselekmény elhatárolásának vagy halmazatának kérdése.

A másodfokú bíróság ezzel kapcsolatban kifejtette, hogy a hivatalos személyként elkövetett zsarolás bűntette speciálisabb, több ismérvvel körülírt bűncselekmény a hivatali vesztegetéshez képest, és más a védett jogtárgy is. Mindkét bűncselekmény alanyai hivatalos személyek, akik hivatalos eljárásban valósítják meg cselekményüket, azonban további ismérvei a hivatalos személyként elkövetett zsarolásnak a jogtalan haszonszerzési célzat, a kár okozása, de legjellemzőbb, ami elválasztja e két bűncselekményt egymástól, a sértettel szemben alkalmazott fenyegetés vagy az erőszak.[5]

Az FBK 1992/9. számon közzétett eseti döntés szerint a hivatalos személy egyetlen kötelességszegése esetén nem állapítható meg halmazatban a hivatalos személy által elkövetett bűnpártolás és a hivatalos személy által kötelességszegéssel elkövetett vesztegetés bűntette. A passzív alany egyetlen kötelességszegése alapján csupán egy hivatali bűncselekmény állapítható meg.

A bíróságok előtt legnagyobb számban két sajátképi hivatali bűncselekmény, a hivatali visszaélés és a hivatalos személy által elkövetett vesztegetés fordul elő. Amellett, hogy számarányuk jelentős a hivatali bűncselekmények között, leginkább ezek veszélyeztetik az állam zavartalan, pártatlan működéséhez fűződő közérdeket. Ezért a továbbiakban e két deliktum elbírálásakor felmerülő eljárási és anyagi jogi problémákat kívánom érinteni.

Eljárási nehézségek a korrupciós és hivatali bűncselekmények elbírálásakor

Van néhány olyan speciális eljárásjogi probléma, amely megnehezítheti, illetve késleltetheti a hivatali visszaélés és a vesztegetés bűntette miatt indult büntetőeljárások befejezését. Ezek túlnyomórészt a bíróságok hatásköri összeütközésével kapcsolatban jelentkeznek, de a bizonyítás során is felmerülnek olyan nehézségek, amelyek speciálisan e bűncselekmények elbírálásával összefüggésben jelentkezhetnek.

1. Hatásköri problémák

Ha áttekintjük a hatásköri összeütközésekkel kapcsolatos bírói gyakorlatot, a legtöbb BH-ban megjelenő jogesetet a megyei bíróságok és a megyei bíróságok katonai tanácsa között felmerülő hatásköri összeütközések adják. Ezeknek az eljárásoknak a tárgya szinte kivétel nélkül rendőrök által elkövetett hivatali visszaélések, illetve hivatalos személy által elkövetett vesztegetések.

[5] Főv.Itb.1.Kbf.3/2003.

A hatásköri konfliktusok azért merülnek fel, mert a rendőrök mint hivatalos személyek egyszerre alanyai lehetnek a sajátképi hivatali bűncselekményeknek, de a Btk. 122. §-a szerint katonának is tekintendők, katonai bűncselekmények alanyai is lehetnek, amely bűncselekmények elbírálása csak a katonai büntetőeljárás keretei között lehetséges. A Btk. 122. § (1) bekezdése szerint a törvény alkalmazásában katona a Magyar Honvédség tényleges állományú, valamint a Rendőrség, a büntetés-végrehajtási szervezet és a polgári nemzetbiztonsági szolgálatok hivatásos állományú tagja.

A Be. 16. § (1) bekezdésének e) pontja szerint a megyei bíróság hatáskörébe tartoznak a Btk. XV. Fejezet IV. Címében meghatározott hivatali bűncselekmények, és a Btk. XV. Fejezet VII. és VIII. Címében írt közélet tisztasága elleni bűncselekmények.

A Be. 470. §-a határozza meg a katonai büntetőeljárás hatályát. Eszerint katonai büntetőeljárásnak van helye

a) katona (Btk. 122. § (1) bek.) által a tényleges szolgálati viszonyának tartama alatt elkövetett katonai bűncselekmény (Btk. XX. Fejezet),
b) a Magyar Honvédség tényleges állományú tagja által elkövetett bármely bűncselekmény,
c) a polgári nemzetbiztonsági szolgálatok, valamint a büntetés-végrehajtási szervezet hivatásos állományú tagja által a szolgálati helyen, illetőleg a szolgálattal összefüggésben elkövetett más bűncselekmény,
d) szövetséges fegyveres erő tagja által belföldön, valamint e személyeknek a Magyar Köztársaság határán kívül tartózkodó magyar hajón vagy magyar légi járművön elkövetett, magyar büntető joghatóság alá tartozó bűncselekmények esetén.

A (2) bekezdés értelmében a katonai büntetőeljárás hatálya kiterjed a terhelt által elkövetett valamennyi bűncselekményre, ha ezek közül valamelyik miatt katonai büntetőeljárásnak van helye, és az elkülönítés nem lehetséges.

Azt gondolhatnánk, hogy a törvény szövege egyértelműen rendezi a hatásköri szabályokat. Eszerint rendőr esetében csak akkor van helye katonai büntetőeljárásnak, ha katonai bűncselekmény, illetve ezzel halmazatban más, pl. hivatali bűncselekmény miatt is folyik vele szemben a büntetőeljárás, és minden egyéb esetben az általános hatásköri szabályok érvényesülnek. A gyakorlat mégis rácáfol arra, hogy ezek a szabályok akadályoktól mentesen működjenek a gyakorlatban. A nehézségek részben a védelv értelmezéséből adódnak.

Tanulságos ebből a szempontból a következő büntetőügy sorsának a vázlatos áttekintése, amely BH 2008/328. számon közzétételre is került. Az elsőfokú tárgyalást a megyei bíróság folytatta le. Az ügy vádlottjai között voltak hivatalos személy által, kötelességszegéssel elkövetett vesztegetéssel vádolt rendőrök is, akiknek bűnösségét első fokon a bíróság e bűncselekményen kívül bűnsegédként elkövetett vagyon elleni bűncselekményekben is megállapította. A tényállás lé-

nyege szerint a vádlottak lopási cselekményüket mint bűnsegédek, rendőrként, szolgálatuk teljesítése közben követték el.

A másodfokon eljáró ítélőtábla hatályon kívül helyezte az elsőfokú bíróság ítéletét, és az eljárás lefolytatására a megyei bíróság katonai tanácsát jelölte ki. Álláspontja szerint a vádirati tényállás alapján a rendőr terheltek elkövették a szolgálatban kötelességszegés bűncselekményét is. Ez katonai bűncselekmény, ezért eljárási szabályt sértett a megyei bíróság, amikor a Be. 470. § (1) bekezdés a) pontja alapján katonai büntetőeljárás hatálya alá tartozó ügyet bírált el.

A katonai tanács, miután megkapta a hatályon kívül helyezést követően az ügyet, azt megküldte a vád átvételének megfontolása végett az illetékes katonai ügyészségnek. A katonai ügyész úgy nyilatkozott, hogy a vádat nem veszi át, mivel nem állapítható meg a vesztegetés mellett katonai bűncselekmény elkövetése is. A katonai tanács az ügyészi nyilatkozatra figyelemmel felterjesztette az iratokat eljáró bíróság kijelölése érdekében a Legfelsőbb Bíróságra.

A Legfelsőbb Bíróság úgy foglalt állást, hogy a hatályon kívül helyezést követően az ítélőtábla által kijelölt katonai tanácsnak el kell járnia. Ebben az esetben ugyanis nincs szó negatív hatásköri összeütközésről, amely miatt felmerülhetne a bíróság kijelölésének lehetősége. Ezért az iratokat visszaküldte a katonai tanácsnak a megismételt eljárás lefolytatása érdekében.

Időközben a rendőr vádlottak szolgálati idejének megszűnésétől számítva több mint egy év telt el, ezért a katonai tanács a részére visszaküldött ügyben a Btk. 124. §-ában írt büntethetőséget megszüntető okra figyelemmel, a szolgálatban kötelességszegés vétsége tekintetében megszüntette a büntetőeljárást, és az ügyet áttette a megyei bíróságra.

A megyei bíróság nem értett egyet e döntéssel. Kifejtette, hogy a rendőr vádlottak cselekménye szolgálatban kötelességszegés bűntettének minősülhet – nem érvényesül ezért a büntethetőséget megszüntető ok a rendőr vádlottaknál – és ismét felterjesztette az ügyet a Legfelsőbb Bíróságra eljáró bíróság kijelölése végett.

A Legfelsőbb Bíróság a megyei bíróságot jelölte ki az eljárás lefolytatására, mivel a szolgálatban kötelességszegés vonatkozásában a katonai tanács jogerős ügydöntő határozatot hozott, e döntés csak rendkívüli perorvoslattal lenne támadható, nincs már olyan bűncselekmény miatt eljárás folyamatban, ami megalapozná a katonai büntetőeljárás hatályát. Az előbb felvázoltak extrém módon növelték meg az eljárás időtartamát.

Amennyiben a bíróságok a Be.-t helyesen, az Alkotmánybíróság 14/2002. (III. 20.) AB határozatában kifejtett elveknek megfelelően értelmezik, az ügy már jogerősen lezárásra kerülhetett volna. A vádat emelő ügyésznek ugyanis esze ágában sem volt vádat emelni szolgálatban kötelességszegés vétsége miatt. Nyilván figyelemmel volt e döntése meghozatalakor az irányadó bírói gyakorlatra is. De ha más indok vezette is erre, a vád emelésére és vitelére jogosult döntésének

értékelése nem a bíróság feladata. Büntetőjogi igényét az ügyész az indítványában megjelölt körben kívánta gyakorolni.

Álláspontom szerint helytelen a katonai bűncselekmény miatti vádemelés mellőzését az ügyész jogi tévedéseként értelmezni, amelynek korrigálását az eljáró bíróságnak kell magára vállalnia. (Hiszen ha az ügyész tévesen dönt, és elejti a vádat, az sem korrigálható a bíróság által.) Amennyiben elfogadnánk ezt a nézőpontot, úgy nem lenne felróható az elsőfokú bíróságnak, ha az ügyészi indítványon nem terjeszkedik túl, és csak az ügyészi indítvány keretein belül állapítja meg a vádlottak büntetőjogi felelősségét.

A Legfelsőbb Bíróság által kifejtett 2007. E.II. El 3/19 sz. vélemény azonban az előzőekben vázoltakhoz képest eltérően értelmezi a vádelvet. Továbbra is fenntartja azt a Be. módosítást megelőző gyakorlatot, amely szerint a vádat a vádirati tényállás jelenti, a bíróság e tényállás alapján az ügyészi indítványtól függetlenül minősítheti a leírt bűncselekményeket.[6] Amíg ez a gyakorlat fennáll, előfordulhatnak az idézetthez hasonló esetek, hiszen az elsőfokú bíróság nem vállalhatja ítéletének hatályon kívül helyezésének veszélyét. Ezért ha a megyei bíróság a vádirati tényállásban katonai bűncselekményt vél felfedezni, erre vonatkozó ügyészi szándék nélkül is át fogja tenni az ügyet a katonai tanácshoz, miután jogerősen megállapította hatáskörének hiányát. Mindezt, nagy valószínűséggel az eljáró bíróság kijelölésére irányuló eljárás fogja követni.

Az idézett példánál maradva, további elvi kérdéseket vet fel az is, hogy mi történik akkor, ha a megküldött ügyben a katonai ügyész úgy nyilatkozik, hogy a vádat nem kívánja átvenni. Ezzel összefüggésben a Legfelsőbb Bíróság elvi éllel mondta ki több határozatában is, hogy amennyiben a fellebbviteli bíróság kijelöli a katonai tanácsot az eljárás lefolytatására, abban az esetben az illetékes katonai ügyész köteles a vádat képviselni a továbbiakban is. Nyilván a katonai ügyészt megilleti az a jog is, hogy a vádat elejtse a katonai bűncselekmény tekintetében, amennyiben jogi álláspontja szerint nem valósult meg katonai bűncselekmény. Nyilvánvaló azonban az is, hogy egy ítélő bírói állásfoglalást követően, különösen, ha ennek kifejezője a Legfelsőbb Bíróság volt, erre a legritkább esetekben fog sor kerülni. Az elvi kérdés tehát továbbra is fennmarad: amikor a bíróság kötelezi az ügyészt a vád vitelére, de facto nem veszi-e át az ügyészségtől a vádhatóság szerepét? Nem gyakorol-e a bíróság megengedhetetlenül nagy befolyást a vádra? (Az Alkotmánybíróság az AB 14/2002. számú határozatában kifejezetten helytelenítette a bíróság „vádhatósági" szerepét.)

Mindezeken túl elgondolkodtatónak tartom azt, hogy érdemes-e bíróságoknak a vád tárgyává tett súlyos büntetési tétellel fenyegetett vagyon elleni és korrupciós bűncselekmények mellett a büntetéskiszabás szempontjából súlytalan, vád tárgyává nem tett katonai bűncselekmény miatt pingpongozni az ügyekkel? Mindez

[6] A vádelv értelmezésével kapcsolatos álláspontomat lásd az alábbi tanulmányban: Török Zsolt: *A magyar büntető bíró és a vádelv*. Ügyészek Lapja 2008/4. szám

nem jelenti-e az officialitás elvének félreértelmezését, hiszen hatása a jogkövetkezmények alkalmazása szempontjából aligha van?

Hasonló ügytologatást eredményezett, amikor a Határőrség 2008. január 1-jével megszűnt, és a szervezet feladatait a Rendőrség vette át, ezzel egy időben a határőrök rendőri állományba kerültek. A Be. korábbi rendelkezése szerint a határőrök által szolgálati helyen és szolgálatukkal összefüggésben elkövetett bűncselekmények megalapozták a katonai tanácsok hatáskörét, rendőrök esetében azonban katonai büntetőeljárásnak csak a tényleges szolgálati viszony tartama alatt elkövetett katonai bűncselekmény miatt van helye. A megváltozott helyzetre figyelemmel néhány katonai tanács az előtte határőrök ellen, hivatali és korrupciós bűncselekmények miatt folyamatban lévő ügyeket áttette, és e döntésekkel az általános hatáskörű bíróságok nem minden esetben értettek egyet.

Az áttett ügyek egy része már tárgyalt ügy volt, ezért a Legfelsőbb Bíróság a katonai tanácsokat jelölte ki az eljárás lefolytatására. Felhívta a figyelmet a Be. 308. § (1) bekezdésére, mely szerint a tárgyalás megkezdése után az ügy áttételének csak akkor van helye, ha az ügy elbírálása a bíróság hatáskörét meghaladja, vagy az katonai büntetőeljárás hatálya alá tartozik, illetve az eljárásra valamely bíróságnak kizárólagos illetékessége van. Nyilván a katonai tanács, amely megyei elsőfokú hatáskörrel rendelkezik, nem tehette volna át az ügyet a tárgyalás megkezdése után.[7]

Érdekesebb azonban, amikor az előzőek szerint döntött, és a katonai tanácsot jelölte ki a Legfelsőbb Bíróság akkor is, amikor a katonai tanács a tárgyalás előkészítésének szakaszában hozta meg az áttételről szóló döntését. A Legfelsőbb Bíróság határozatainak hivatkozási alapját a Be. 605. § (3) bekezdése, (az új Be. hatályba lépésével összefüggő rendelkezés) képezte. Eszerint az eljárást a korábbi jogszabály szerint hatáskörrel és illetékességgel rendelkező bíróság folytatja le, ha az ügy iratai a törvény hatályba lépése előtt a bíróságra érkeztek. Ehhez az álláspontjához döntéseiben következetesen tarja magát a Legfelsőbb Bíróság. E gyakorlatot nehéz összeegyeztetni a Be. 11. § (1) bekezdésében foglaltakkal, mely szerint a büntetőeljárást a cselekmény elbírálásakor hatályban lévő törvény szerint kell elbírálni. E rendelkezést ugyanis azzal együtt kell értelmezni, hogy az eddigi általános gyakorlat szerint, amennyiben nem akarta a jogalkotó a folyamatban lévő ügyekre alkalmazni az új eljárási szabályokat, úgy kifejezett rendelkezést hozott erről az új törvényben. A jogalkotó az új Be.-nél ezt megtette, ami nem jelenti azt, hogy e rendelkezést – mint a Be. jelenleg is hatályos részét –, a jövőben megjelenő novellák esetében is alkalmazni kell.[8]

[7] A Legfelsőbb Bíróság Bkk.I.162/2009. számú végzése

[8] A Legfelsőbb Bíróság Bkk.I.291/2009 számú végzése. A Legfelsőbb Bíróság az új Be. hatályba léptető rendelkezését az eljárási törvény szerves részeként tekinti, és a jövőbeni eljárási novellák tekintetében is alkalmazni fogja a Be. 615. § (3) bekezdését. A korábban töretlen bírói gyakorlathoz való visszatérést segíthetné elő ennek a törvényhelynek a hatályon kívül helyezése.

Miként az előző példákból is látszott, a Legfelsőbb Bíróság jogosult dönteni a bíróság kijelöléséről általános és katonai hatáskör összeütközés esetén, ezért célszerű rögtön oda felterjeszteni az ügyeket. Figyelmetlenségből az ítélőtáblákra is felterjesztenek ügyeket a katonai és általános hatáskör összeütközése miatt, az eljáró bíróság kijelölése érdekében, amelyeket tovább kell küldeni a hatáskörrel bíró Legfelsőbb Bíróságra, és ez szintén hozzájárul az ügyek elhúzódásához.

Az előző példák alapján jól kirajzolódik az ügyek elhúzódásának egyik fő oka. Tanulságként leszűrhető mindebből az, hogy a bírónak nem kell feltétlenül hiperaktívnak mutatkoznia, és ott is bűncselekményt keresnie, ahol az ügyész nem indítványozta annak megállapítását, illetve a már tárgyalt ügyek esetében azok gyors, szakszerű befejezésére kell törekedni.

Folytatása következik.

VADÁSZ VIKTOR[1]

A számítógép demisztifikálása

A számítógép és a büntetőjog

A kezdetek

Minden jogterületre, de különösen a büntetőjogra igaz, hogy kullog az élet változásai után. A jogalkotó az élettapasztalatból, társadalmi elvárásokból, illetve a jogalkalmazói reakciókból szerez tudomást a szabályozás szükségességéről, de még ezt követően is hosszabb idő telik el, amíg egy jogszabály megalkotásra kerül, és a gyakorlatban is alkalmazni kezdik. Számos esetben nemzetközi trendek, a jogtudomány közreműködése, illetve az állam nemzetközi szerződéses kötelezettsége eredményezi a büntetőjogszabályok módosítását, a pönalizált területek kiterjesztését.
E megállapítások különösen igazak a számítógépre és a számítógépes bűnözésre. Mielőtt a Btk. 300/C. § 1994. május 15-én megalkotásra került, a jogalkalmazók az ilyen jellegű bűncselekményeket többnyire valamelyik vagyon elleni bűncselekmény törvényi tényállása alatt üldözték. Erre sok esetben a lopás vagy csalás törvényi tényállása a megtévesztés, illetve fizikai elvétel hiányában nem volt alkalmas. A technika fejlődésének eredményeként elszaporodó számítógéppel kapcsolatos bűncselekmények már nagyon indokolták a kodifikációt.
További probléma a számítógéppel kapcsolatos bűncselekmények esetében, hogy túlnyomórészt a harminc év feletti korosztályból reprezentált bírói karnak vajmi kevés affinitása van a számítógépekhez és a világhálóhoz, hiszen még felhasználóként is nagyon alapszintű ismeretekkel rendelkezik. A lehetőségeket és a bírói vezetés rálátását jól tükrözi az a tény, hogy van olyan megyei bíróság, ahol a bírák számítógépén munkaidőben nincs Internet hozzáférés, illetve más helyeken a bírák öt-tíz évvel korábbi verziójú, más programokkal inkompatibilis Open Office freeware programot kénytelenek használni, nyilvánvalóan költségvetési okokból.

A kodifikáció

Bár a jogalkalmazónak nem a jogszabályok kritizálása, hanem a lehető legjobb végrehajtása a feladata, az ítélkező bírák részéről mégis jogos a kritika, amikor azt mondják, hogy a számítógépes bűnözés jogalkalmazási problémái részben a jogalkotásban gyökereznek.

A 2001. november 23-án elfogadott Cyber Crime Egyezmény (2004. évi LXXIX. törvény) szükségessé tette a számítástechnikai bűnözésről szóló törvény módosí-

[1] Vadász V., gazdasági szakjogász, bíró, PKKB

tását, részletesebb szabályozását. Nemcsak a bűnözők, de láthatóan a jogalkotó is használja a modernkor vívmányait, mert az egyezményben használt fogalomértelmezések a 'copy-paste' szövegszerkesztési metódus használatával szó szerint kerültek átemelésre a Btk.-ba. Az ilyen jellegű jogalkotás meglehetősen sok problémát eredményez a gyakorlatban. Egy nemzetközi egyezmény, illetve egy büntetőjogi norma szövege alapvetően különbözik. A jogbiztonság azt indokolja, hogy a büntető jogszabályok pontosan, érthetően és egyértelműen legyenek megfogalmazva. Nem szerencsés, ha a törvényszöveg ugyanarra a dologra többféle fogalmat is használ. A 'számítástechnikai rendszer' kifejezés a Btk. 300/C. § mellett még a Btk. 178/A. §-ában is benne van, de törvényünkben több helyen szerepel a 'számítógép', illetve 'számítógépes program' kifejezés is (pl. Btk. 304/A. §, 313/D. §).

A 300/C. § tényállása egy nagyon széleskörű, rendkívül sokféle elkövetési magatartást felölelő, több alapesetben szabályozott bűncselekményt ír le. Az (1) bekezdés előrehozott védelme mellett, amely a jogtalan belépést rendeli büntetni, a jogalkotó a (2) bekezdésben az adatok bármilyen megváltoztatását és a rendszer megzavarását, a (3) bekezdésben pedig a vagyoni kárt okozó ún. számítógépes csalást rendelte büntetni. Sőt, emellett a 300/E. § a jogtalan belépés előkészületi alakzatát is üldözi, sui generis bűncselekményként. Olybá tűnik, a jogalkotó semmit nem bízott a véletlenre, és minden a számítógéppel kapcsolatos elképzelhető magatartást üldöz.

A számítástechnikai rendszer elleni tényállás alkalmazása napjainkban

Mint arra már utaltam, ma az élet legtöbb területén számítógépek teszik könnyebbé vagy éppen nehezebbé mindennapjainkat. A bűnözők is egyre többször használnak különféle számítógépeket, mivel ez megkönnyíti a bűncselekmény elkövetését, vagy enélkül nem is tudnák elérni bűnös céljukat.

Tíz-húsz évvel ezelőtt el lehetett lopni egy gépkocsit drótok összeérintésével, vagy a zárszerkezet eltörésével. Ma már komoly eszközökre van szükség, és komoly háttér kell egy autó indítókulcs nélküli elindításához. Az elkövetők viszik magukkal a fedélzeti számítógépet, amely az eltulajdonítani kívánt jármű számítógépével kicserélve, megkerüli a számítógépbe épített gyújtásmegszakítást, és indíthatóvá teszi a gépkocsit. Ismert a gyakorlatban olyan jogi álláspont is, amely ilyen esetben a számítástechnikai rendszer elleni bűncselekményt halmazatban állapítja meg a lopással, jármű önkényes elvételével. A két számítógép cseréje viszont – az abban feldolgozott adatok érintetlenül hagyása mellett – álláspontom szerint ezt a bűncselekményt nem valósítja meg. Más a helyzet, ha az elkövető által hozott fedélzeti számítógép fel van törve, és az adatmódosítás eredményeként azzal bármelyik gépkocsi indíthatóvá válik. Itt anyagi halmazattal állunk szemben. Külön bűncselekmény a korábban elvégzett jogtalan adatmódosítás, azaz feltörés, és külön bűncselekmény (lopás vagy jármű önkényes elvétele) a jármű ennek segítségével végrehajtott elvétele.

Megjelent a gyakorlatban egy ezen is túlmutató jogi érvelés, amikor az ügyészség már a Btk. 300/E. § szerinti előkészületi cselekmény miatt emel vádat. A vádhatóság jogi álláspontja szerint a személygépkocsi mint elektronikai rendszer, maga is számítástechnikai rendszernek minősül, és az ehhez jogtalan hozzáférést biztosító bármely eszköz, fedélzeti számítógép olyan adatokat tartalmaz, amely a jogtalan belépést teszi lehetővé. Ezáltal már önmagában az ilyen eszközi birtokolása is jogszabályba ütközik, függetlenül attól, végeztek-e rajta módosítást, vagy azt ki tette.

E jogi érvelés mögött két dolog is meghúzódik. Egyrészről az egyébként hivatásszerűen autók eltulajdonításával foglalkozó elkövetők a cselekmény „idő előtti" leleplezésekor lopás előkészülete miatt a törvény szerint nem büntethetők. Másrészről pedig elgondolkodtató, hogy a Btk. 300/F. § (3) bekezdés értelmező rendelkezése szerint[2] nem tekinthető-e mégiscsak a gépkocsi egésze számítástechnikai rendszernek, hiszen a jármű elektronikai berendezései között több olyan is található, amelyek automatikus adatfeldolgozást végeznek. Gondoljunk a programozható rádiósmagnóra, az esőérzékelős ablaktörlőre, az üzemanyag befecskendező rendszerre, vagy akár a fékerőelosztásra, a vészfékrásegítésre, illetve az ABS rendszerére. Ezek önálló számítástechnikai rendszerek. Előre programozott módon reagálnak a beérkező adatokra. Mindazonáltal ezzel a kiterjesztő jogértelmezéssel és az ahhoz kapcsolódó jogi okfejtéssel, véleményem szerint, átesünk a ló túlsó oldalára. Az elkövető ugyanis – hóna alatt a fedélzeti számítógépekkel – nem valamiféle számítástechnikai rendszerbe szándékozott jogosulatlanul belépni, hanem egyszerűen egy autót akart eltulajdonítani.

Hogy ne csak vagyon elleni bűncselekmények kapcsán vessem fel a problémát, példaként álljon itt egy nem is olyan ritkán megvalósuló tényállás: az elkövető belép a sértett internetes levelezésébe, és elolvassa a leveleit. A magántitok számítógépes kifürkészés útján elkövetett jogosulatlan megismerése – Btk. 178/A. § (1) bekezdés d) pont – nem valósul meg, ha az észlelteket technikai eszközzel nem rögzíti az elkövető (pl. kinyomtatás útján). Találkoztam olyan esettel, amikor a vádhatóság azért nem levéltitok megsértése miatt emelt vádat, mivel úgy látta, súlyosabb bűncselekmény is megvalósult: a Btk. 300/C. § (1) bekezdése szerinti jogosulatlan belépéssel megvalósuló számítástechnikai rendszer és adatok elleni bűncselekmény. Megjegyzem, a kizárólag pénzbüntetéssel fenyegetett levéltitok megsértésénél nem sok bűncselekmény nem súlyosabb. Mindazonáltal nem igazán látom, miben jelent nagyobb veszélyt a társadalomra, ha valakinek a postaládájából veszem ki és olvasom el a levelét, mint amikor mindezt az elektronikus levelezésével teszem meg. A jogalkotó egyébként a „távközlési berendezés útján továbbított közlemény kifürkészésének" beiktatásával épp amiatt egészítette ki a Btk. 178. §-át, mert nem a közlés módja, hanem annak személyes jellegére tekintettel kíván védelmet biztosítani.

[2] A 300/C. § és a 300/E. § alkalmazásában számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

Felsejlik bennem annak gyanúja is, hogy egyes bírák esetében a fenti érvelések erőltetése mögött bizonyos bürokratikus érdekek húzódnak. A gazdasági bűncselekmények esetén – mint amilyen a számítástechnikai rendszer és adatok elleni bűncselekmény is – a megyeszékhely szerinti, illetve Pesti Központi Kerületi Bíróság rendelkezik kizárólagos illetékességgel. Sokszor ez a legegyszerűbb módja az ügytől való megszabadulásnak.

A fenti esetekkel találkozva fogalmazódott meg bennem az a kérdés: nem misztifikálta-e túl a jogalkotó a számítógépeket, melyek a kommentárok szerint olyan fontos szerepet játszanak a 21. században, hogy megfelelő működésükhöz, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához és hitelességéhez fokozott társadalmi érdek fűződik.[3]

A 'számítógép' újraértelmezésének szükségessége

Álláspontom szerint a számítógépre eszközként kell tekinteni, mely mostanra életünk mindennapi részévé vált. Kétség sem férhet hozzá, vannak olyan számítástechnikai rendszerek, amelyeknek elvégzett feladatuk, társadalmi és gazdasági életben betöltött szerepük folytán kiemelt védelmet kell élvezniük. Ilyen például egy bank számítástechnikai rendszere, a bírósági ügyviteli rendszer vagy a Paksi Atomerőmű reaktorát irányító számítógép. Azt is elfogadom, hogy a büntetőjog eszközeivel is harcolni kell a gazdasági életben óriási károkat okozó hackerek ellen.

Kétségeim vannak viszont afelől, hogy egy autótolvaj szükségképpen megvalósítja a számítástechnikai rendszerbe történő jogtalan belépést, vagy az osztálytársa telefonjáról az sms-üzeneteket törlő suhancot mindenképp jogtalan adattörléssel megvalósuló számítástechnikai bűncselekmény miatt kell elítélni.

A megoldás alapvetően a jogalkotó kezében van.
Először is, véleményem szerint, a számítástechnikai rendszer, a számítógép, a számítástechnikai program és adat fogalmát pontosan és az egész Btk.-ra kiterjedően következetesen újra kellene szabályozni, leszűkítve egyben az indokolatlan kiterjesztő értelmezések lehetőségét.

Másodszor, fontosnak tartanám, hogy a felesleges kétszeres értékelés elkerülése érdekében a jogalkotó legalább az enyhébben minősülő alapesetekben csak alternatívan pönalizálja a számítástechnikai adatok és rendszer elleni bűncselekményeket. („ha más bűncselekmény nem valósul meg")

Harmadsorban, ha a jogalkotó a számítógépet mint elkövetési eszközt önmagában is veszélyesnek tekinti, szabályozza az egyes bűncselekmények esetén minősítő körülményként az elkövetés ilyen módját, de egyébként ne önálló számítástechnikai rendszer elleni bűncselekményként értékelje ezt.

[3] Belovics E. – Molnár G. – Sinku P.: Büntetőjog. Különös Rész. HVG-Orac Kiadó, Budapest, 2007. 560. o.

A számítástechnika útján elkövetett bűncselekmények eljárásjogi kérdései, bizonyítási nehézségei

Interneten keresztül elkövetett rágalmazások, becsületsértések

Egyre elterjedtebb, hogy az emberek személyes adataikat, képeiket, gondolataikat és véleményüket fórumokon, blogokban elérhetővé teszik a nagyközönség számára. Túl azon, hogy az Iwiw-hez, Facebook-hoz és Myvip-hez hasonló személyes fórumok – melyeket ma már nem kizárólag a fiatalok használnak – visszaélésekre adnak lehetőséget, az Internet arra is felbátorította az embereket, hogy véleményüket bátran, sokszor meggondolatlanul, esetenként artikulálatlan stílusban tegyék közzé bejegyzéseikben.

Amíg a fórumozás gyakorlata nem öltött ilyen óriási méreteket, ezt az internetes etikett és a moderátorok kordában tudták tartani: a sértő bejegyzéseket törölték, a felhasználókat *bannelték*. Mára azonban egyre gyakrabban fordul elő, hogy az ilyen úton sérelmet szenvedők a bírósághoz fordulnak. Ilyenkor a bíróság első körben rendszerint a bejegyzést tevő felhasználó pontos személyazonosságának megállapítása végett nyomozást rendel el [Be. 499. §]. A nyomozóhatóság az IP cím alapján a szolgáltató megkeresésével kideríti az előfizető nevét és címét. Ezután a tanúként történő meghallgatása deríthet fényt arra, hogy ténylegesen ki használta a számítógépet. Ennek kapcsán a következő nehézségek adódnak:

- Nyilvánosan használt számítógépek (pl. munkahely, kollégium, Internetkávézó stb.) esetében nincs kötelező előírás arra, hogy a számítógép használóiról nyilvántartást vezessenek.
- Abban az esetben, ha a felhasználó kódolatlan WiFi rooteren keresztül kapcsolódik az Internethez, ahhoz más is hozzáférhetett.
- Egy számítógépet a családban általában többen is használnak, adott esetben az előfizető bizonyíthatja, hogy nem is tartózkodott otthon az elkövetés idejében, arra pedig nyilván nem kötelezhető, hogy hozzátartozóira terhelő vallomást tegyen.
- Ismertek olyan szoftverek (ún. IP Hide), amelyek segítségével az elkövető egy külföldi proxy szerveren keresztül csatlakozik a világhálóra ál IP címmel.

A bizonyítás említett nehézségein túl, ha az elkövető kiléte meg is állapítható, el kell dönteni azt az eljárási előkérdést, hogy melyik bíróság rendelkezik illetékességgel? Az elkövetés helyét a bíróságok ilyen jellegű bűncselekmények esetében nem következetesen ítélik meg. Nincs egységes gyakorlat, várhatóan a vitát a Legfelsőbb Bíróság jogegységi eljárása, vagy a jogalkotó fogja eldönteni véglegesen. Jelenleg három variáció is ismert a gyakorlatban:

- A bejegyzés beírásának helye, mivel az elkövető itt valósítja meg az elkövetési magatartást. Ez belföldi lakóhelyű elkövető esetén viszonylag problémamentesen megállapítható.
- A bűncselekmény észlelésének helye, azaz ahol a sértett azt elolvasta. Ez azonban teljesen ad hoc jelleggel alakul, és nincs sok köze magához a cselekmény-

hez, hiszen a világháló bárhonnan hozzáférhető. Kétségtelenül mellette szól, hogy az elkövető ilyenkor nem bújhat külföldi szerver mögé.

– Az írott média analógiájára (szerkesztő, kiadó székhelye) az elkövető IP címét kiosztó szolgáltató székhelye. Megjegyzendő, hogy ennek sincs túl sok köze magához a cselekményhez, hiszen a bejegyzés felküldése a világhálóra a szolgáltató szempontjából automatikus adattovábbítás, mindössze egy pillanat műve, így nagyban különbözik az újság felelős szerkesztőjétől, kiadójától.

Egyelőre tehetetlennek tűnnek a hatóságok a külföldi szerverekről futó, Magyarországon is elérhető, magyar nyelven megszólaló olyan fórumokkal, honlapokkal szemben, melyek tartalmukban nyíltan sértik mások jogait, bűncselekmények elkövetésére buzdítanak, nyíltan becsmérelnek egyes személyeket, illetve a lakosság egyes csoportjait. Ilyen kirívó esetben, álláspontom szerint, csak igazgatási úton léphet fel az állam, mivel a távol élő vagy elérhetetlen elkövetőkkel szemben a büntetőjog tehetetlen. Amennyiben a bíróság egy adott honlapon elhelyezett szövegek kapcsán sorozatos és súlyos jogsértést állapít meg, esetleg meg lehetne teremteni annak lehetőségét, hogy a honlap egyfajta internetes cenzúrával korlátozva legyen olyan módon, hogy a magyarországi szolgáltatók letiltják az adott IP címhez történő kapcsolódást. A pontos technikai megoldás előttem nem ismert, kizárólag a jogi lehetőség foglalkoztat, így csak ezt vizsgáltam. Amennyiben a szolgáltató azonos tartalommal új honlapon helyezné fel a tartalmat, az állam igazgatási úton, külön bírói eljárás nélkül is kiterjeszthetné a tilalmat az újabb IP címekre. Ez lényegesen megnehezítené a honlap üzemeltetőnek dolgát. A véleménynyilvánítás alapvető jogának garanciáját a megfelelően pontos jogi szabályozás és a bírói eljárás biztosíthatná. Úgy vélem, van olyan súlyú jogsértés, amellyel szemben a véleménynyilvánítás szabadsága mögé már nem lehet elbújni.

Ehhez hasonló probléma a külföldi levelezőprogramok (pl. g-mail) használata. A bizonyítás csak nemzetközi jogsegély keretében foganatosított megkeresés útján valósítható meg. Egy levelezőfiók tartalma, illetve az abban folytatott levelezés ezáltal csak hónapokkal, évekkel később lesz megismerhető a hatóság, bíróság által. Nem kívánok tippeket adni, de élelmes vállalkozók hamarosan létre fogják hozni a Kajmán-szigeteken és egyéb jogilag elérhetetlen helyeken bejegyzett szervereket, ahol jó pénzért IP címet és postafiókot adnak a szabad és ellenőrizhetetlen szörfözéshez, levelezéshez.

Számítógépes szoftverekre elkövetett szerzői jogsértések

A számítógépes szoftver a szerzői jogi törvény szerint szerzői jogi alkotásnak minősül. Ez már önmagában is több probléma forrása. A szoftverek esetében ugyanis – ellentétben egy könyv vagy zeneműszerzőjével – a személyhez fűződő jogok kérdése egyáltalán nem vetődik fel hangsúlyosan, sokkal inkább a vagyoni jogok. A szoftverek – melyek tulajdonképpen egy programozási megoldásként, meghatározott bináris adatsorként írhatóak le – jellegükben sokkal inkább hasonlítanak az ipari mintákhoz, semmint a szerzői jogi alkotásokhoz.

Mindezen túl a bizonyítás területén is számos problémába ütközünk.
Sok szoftvernek van ingyenes verziója (freeware, shareware), így amennyiben a lefoglalt szoftver verziószáma nem ellenőrizhető, nem zárható ki a felhasználás szabad, jogos volta.
A gyártó sokszor a teljes szoftvert letölthetővé teszi, azonban azonosító kulcs nélkül csak ingyenes próbaverzióként használható, esetleg időhöz kötött (trial version). További nehézség, hogy van olyan szoftver is, amely a próbaidő letelte után is tovább használható, és csak egy felugró ablak figyelmeztet a licencia hiányára (pl. Total Commander).

Jelenleg nincs olyan törvényi kötelezettség, amely előírná a felhasználónak, hogy köteles legyen nyilatkozni, a tőle lefoglalt adathordozó biztonsági másolat-e. Az sincs előírva, hogyan kell tárolni a biztonsági másolatokat, egyáltalán fel kell-e tűntetni azon ezt a jelleget. Természetesen a telepítő lemezen található feltörés (crack, keygen) kizárja azt a lehetőséget, hogy a másolat eredetiről készült, de ennek hiányában az eredeti lemez akár évekkel későbbi bemutatása is cáfolhatatlan védekezés. Az eredeti hardware környezet hiányában szakértőileg általában már nem lehet megállapítani, hogy a lefoglalt adathordozón található szoftver milyen lemezről lett feltelepítve.

A fájlcserélő rendszerek

Továbbra is a szerzői jogok területén maradva, nagyon aktuális téma a *peer-to-peer* (p2p) fájlcserélő rendszerek problémája. Egyre élesebben kérdőjelezik meg társadalmi csoportok ennek társadalomra jelentett veszélyét, gondoljunk csak az Európai Parlamenti képviselethez jutó svéd Kalóz Pártra, és az ingyenes fájlcserélést szorgalmazó más civil szervezetekre.
A jelenleg egységesnek mondható fővárosi ügyészi és bírói álláspont szerint, a zenefájlok és filmek fájlcserélő programmal történő letöltését – a szerzői jogvédő szervezetek legnagyobb bánatára – nem üldözik. Ennek jogi indoka részben a megosztás ingyenessége (nincs haszonszerzési célzat), részben pedig nem bizonyítható, hogy a fájlt letöltő valóban vagyoni hátrányt okoz, illetve ezzel tisztában van. Mindemellett viszont a zeneszámok és filmek feltöltése, azaz mások számára történő hozzáférhetővé tétele továbbra is büntetendő. A jogi érveléssel kapcsolatosan alapvető probléma, hogy a fájlok letöltését a fájlcserélő programok technikailag úgy valósítják meg, hogy a felhasználók (kliensek) a kiválasztott filmet, zenét szeletekben, darabokban töltik le egyszerre több elérhető felhasználótól, részben olyanoktól is, akik nem az összes darabbal rendelkeznek (seed), hanem csak részekkel. Ezáltal a fájlt letöltő kliens a már letöltött szegmensek tekintetében maga is megosztási csomópontként funkcionál (peer). A p2p letöltés ezáltal technikailag szükségképpen megosztást is jelent.

A fájlcserélést kétféleképp lehet tetten érni. Az egyik lehetőség, hogy a számítógépet lefoglalják, és a nyomozóhatóság megtalálja rajta a fájlcseréléshez használt kliensprogramot. A kliensprogram beállításainál ellenőrizhető, mely mappák kerültek megosztásra, és rögtön ellenőrizhető ezek tartalma is. A bizonyítást

nehezíti a terhelt későbbi védekezése, ha arra hivatkozik, hogy nem futtatta a programot, az csupán feltelepítésre került, így a 'share mappa' fájljai egyszer sem kerültek megosztásra.

A másik módja a bizonyításnak, amikor a hatóság próbaletöltéssel éri tetten az elkövetőt. Ilyenkor egy-egy fájl próbaletöltése mellett a közreműködő szaktanácsadó vagy szakértő pusztán kilistázza (*logolja*) a kiszemelt IP cím által megosztott fájlokat. A megosztás ilyen esetben nem kétséges, viszont a terheltek utóbb gyakran hivatkoznak arra, hogy valójában a zene és filmként megjelölt fájlok nem azt tartalmazták, ami az elnevezésük, azok pusztán a szükséges megosztási kvóta elérése érdekében lettek megosztva a fájlnév és a kiterjesztés megváltoztatásával (pl. családi fényképeket osztott meg mp3-ra átnevezve). A védekezés, noha elég életszerűtlen, csak körülményesen zárható ki, többnyire a fájlméretek egyeztetésével.

A számítástechnikai rendszerek lefoglalása

A számítástechnikai eszközzel elkövetett bűncselekmények üldözésének hőskorában a rendőrség a házkutatás során – biztos, ami biztos – lefoglalta nemcsak a számítógépházat, de a monitort, a billentyűzetet és az egeret is. Később finomodott az eljárás, és már csak számítógépházat foglalták le, utóbb már sokszor kizárólag a merevlemezt, sőt még azt sem: másolatot készítenek a merevlemezről (szakszóval: image). A Be. már kifejezetten rendelkezik adatok lefoglalásáról is, ilyenkor a nyomozóhatóság már csak a szükséges adatokat menti le a bizonyítás érdekében.

Ezzel, úgy vélem, ismét túllőttünk a célon. Egyrészt az elkövetés eszköze elkobzás alá esik. Ha a monitor és az egér nem is, de a CD és DVD író, illetve merevlemez adott esetben lehet az elkövetés eszköze is. Másrészt azzal, hogy a merevlemezt eltávolítják az eredeti hardware környezetből, a számítógépen futó programok egy része nem lesz többet indítható. Ennek hiányába igen nehezen állapítható meg a verziószám, az esetleges feltörések, illetve a próbaidőn túli jogosulatlan használat. Célszerű ezért a későbbi bizonyítás és az esetleg szükséges elkobzás végett az egész számítógépet lefoglalni, és a később szükségtelenné vált részeket a szakértői vizsgálatot követően visszaadni a lefoglalást elszenvedőnek.

A lefoglalás pillanata több okból is nagyon fontos. A nyomozóhatóság már ekkor kizárhat számos olyan kérdést, amely később már nem bizonyítható vagy cáfolható. Ilyen például a már említett WiFi használat. A házkutatás során indokolt ellenőrizni, van-e WiFi elérhetőség a lakásban, illetve védett-e biztonsági kóddal. Célszerű azonnal nyilatkoztatni a lefoglalást elszenvedőt – természetesen törvényes figyelmeztetést követően –, hogy ki használja a számítógépet, azon kiknek az adatai találhatók, illetve védett-e belépési kóddal. Ha mondjuk épp egy bekapcsolt gépet foglal le a hatóság, valamilyen módon célszerű lenne azt is rögzíteni, van-e internetes elérhetőség, illetve csatlakozik-e a kliensprogram, és milyen fájlokat oszt meg éppen.

Összefoglalás

Az általam felvetett kérdésekkel és problémákkal arra kívánom felhívni a figyelmet, hogy újra kellene értékelni a büntetőjog és a számítógép viszonyát. A jogalkotónak a számítógép fogalmát és a számítógépekkel kapcsolatos bűncselekmények szabályozását hozzá kellene igazítania az élethez. A számítógépre ne valami mitikus dologként vagy önmagában védendő jogi tárgyként tekintsünk, mert a számítógép egy egyszerű eszköz, a mindennapjaink eszköze. Olyan eszköz, amely kétségtelenül nagy kihívást jelent a jogalkalmazóknak, de a megfelelően felkészült és a számítástechnika terén az új ismeretekre nyitott jogászok eredményesen tudják venni ezt az újfajta akadályt is.

PESZLEG TIBOR[1]

A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük

Elvi alapvetés

Írásomban arra keresem a választ, hogy a büntetőeljárás során a bizonyítási eszközök beszerzésének elvei hogyan valósulhatnak meg. Úgy gondolom, hogy a bizonyítási eszközök beszerzésének elvei nem változnak akkor sem, ha azokat nem az eddig megszokott, kriminalisztikailag kimunkált közegből szerezzük be. Sőt, most, amikor a digitális bizonyítási eszközök beszerzésének módjait igyekszünk kimunkálni, pontos szabályokkal rögzíteni, igen nagy hangsúlyt kell fektetni arra, hogy az alapelvek ne változzanak, illetve az alapelveknek megfelelő legyen a digitális bizonyítékok beszerzése is.

A büntetőeljárási jog egyértelműen meghatározza, hogy melyek a bizonyítás eszközei, úgy mint a tanúvallomás, a terhelt vallomása, a szakvélemény, okirat és a tárgyi bizonyítási eszköz. A hatályos törvény más bizonyítási eszközt nem ismer. A bizonyítási eszközökről annyit mond a törvény, hogy azoknak törvényesnek kell lenniük, ami alatt azt érti, hogy a Be. rendelkezései szerint kell eljárni a bizonyítási eszközök felderítése, összegyűjtése, biztosítása és felhasználása során [Be. 77. § (1) bek.]. Továbbá külön jogszabály elrendelheti a *„bizonyítási cselekmények teljesítésének, a bizonyítási eszközök megvizsgálásának és rögzítésének, valamint a bizonyítási eljárások lefolytatásának meghatározott módját"*. Azonban a digitális bizonyítási eszközök megszerzésére nincsenek ilyen jogszabályi előírások. Útmutatók és egyéb előírások sem adnak számunkra segítséget.

A másik nagyon fontos szabály, hogy a bizonyítási eszközök beszerzése során az emberi méltóságot, a személyiségi és kegyeleti jogokat tiszteletben kell tartani. Kiemelném ezt azért is, mert a digitális bizonyítási eszközök értékelése során nagyon sok személyes adathoz juthatunk hozzá – egyéb érzékeny adatok mellett, mint az állam-, a szolgálati-, a bank- és az adótitkok, valamint a gazdasági titkok –, amelyek nem megfelelő kezelése sértheti az érintettek vagy más személyek személyiségi jogait.

Fontos garanciális szabályt állapít meg a Be. 78.§ (4) bekezdése, amely megtiltja azon bizonyítási eszközökből származó tény bizonyítékként való értékelését, melyet bűncselekmény útján, más tiltott módon vagy az érintettek eljárási jogainak lényeges korlátozásával szereztek meg. A törvény pontosabban nem határozza meg azon speciális módszereket, melyek alapján a digitális bizonyítási eszközöket be kell szerezni, így kénytelenek vagyunk az általános eljárási szabályok

[1] Peszleg T., jogász, független informatikai biztonsági szakértő

alapján, valamint a kriminalisztika szabályainak figyelembe vételével azt magunk meghatározni.

A kriminalisztika a következő elveket határozza meg számunkra követendőként: törvényesség, objektivitás, hitelesség, változatlanság és teljesség. A törvényesség fogalmával és meghatározásával már foglalkoztam, amikor a Be. elveit felsoroltam. A kriminalisztika is hangsúlyozza, hogy csak olyan bizonyítékokat lehet beszerezni, melyek megfelelnek a törvényben meghatározott feltételeknek. Ebből következik, hogy akkor törvényes az adott bizonyítási eszköz, ha azt a hatóság tagja a megfelelő eljárás keretében, annak az eljárásnak az alaki és tartalmi elemeit megtartva, megfelelő technikai eszközökkel szerzi be, valamint így is elemezi, értékeli azokat. A digitális bizonyítékok beszerzésénél különösen fontos, hogy a hatóság tagja arra kiképzett legyen.

Az objektivitás mint alapelv azt jelenti, hogy tárgyszerűen, előítéletek, előfeltételezések nélkül, csak a tényekre koncentrálva gyűjtsük össze a bizonyítási eszközöket, függetlenül attól, hogy azok alátámasztják-e az eseményekkel kapcsolatos valamely verziónkat, a terhelt vagy más személy bűnösségét vagy ártatlanságát. A bizonyítási eszközök beszerzésénél, értékelésénél hibás, sőt talán törvénytelen is, ha csak azokat a bizonyítási eszközöket gyűjtjük be, vagy azokat a következtetéseket vonjuk le, melyek egy-egy előfeltételezésünket, verziónkat alátámasztják. Az eljárás során ezt segíti elő, hogy egyes szakkérdésekben független – sem a váddal, sem a védelemmel kapcsolatban nem álló – személy vagy szervezet (igazságügyi szakértő) mond véleményt. Ez a függetlenség figyelhető meg akkor is, amikor a bűnügyi technikai szolgálat, vagy az elemző-értékelő egység nem a nyomozó hatóság szervezeti keretei közt végzi a munkáját, hanem attól elkülönül, ezzel is biztosítva a függetlenséget. Ez az elkülönülés a speciális szakismereteknek is köszönhető.

A bizonyítási eszközök beszerzése során a hitelesség kérdése is nagyon fontos. Ez biztosítja az eljárás során, hogy tényleg azt a bizonyítási eszközt vizsgálja a hatóság, majd a bíróság is, melyet rögzítettek. Ez a hitelesség nemcsak a rögzítés idején lényeges, hanem az egész eljárás során. A hitelességet a jegyzőkönyv felvételénél a jelenlévők aláírása biztosítja, míg a tárgyi bizonyítási eszközöknél a megfelelő csomagolás, a bűnjelcímke használata, valamint a jegyzőkönyv, melyet szintén aláírással hitelesítenek.

A Be. 153.§ (3) bekezdése még egy további szabályt is előír: *„A lefoglalt dolgot úgy kell őrizni, hogy az változatlanul maradjon, a bűncselekmény esetleges nyomai el ne tűnjenek, a lefoglalt dolgot ne lehessen kicserélni, és az azonossága könnyen megállapítható legyen."* Ez a szabály érinti a változatlanság kérdését. A bizonyítási eszközöket úgy kell tárolni, szállítani, vizsgálni, bármilyenek legyenek is, hogy azokon változtatást ne lehessen eszközölni az eredeti állapothoz képest. Ez általában nem jelent gondot, de a technikai adottságok miatt a digitális bizonyítási eszközöknél erre külön figyelmet kell fordítani. Ami ennél is fontosabb, hogy ezeket a bizonyítási eszközöket beszerezni is úgy kell, hogy azok a beszerzés során ne sérüljenek meg, a rajtuk tárolt adatok ne módosuljanak. Ez már speciális szakértelmet

és odafigyelést igényel. Ugyanez a helyzet pl. az ujjnyomok vizsgálatánál, illetve még számos krimináltechnikai nyomrögzítés esetében, de azok szabályai az elmúlt évtizedekben már kidolgozásra kerültek.

Végül, de nem utolsó sorban a teljesség elvével kapcsolatban megjegyzendő, hogy a bizonyítási eszközök beszerzésénél arra kell törekedni, hogy az üggyel kapcsolatba hozható minden adatot vizsgáljunk. Nem lehet megelégedni azzal, ha csak azokat vizsgáljuk, melyek számunkra kedvezőek, vagy könnyen elemezhetőek, hiszen akkor téves következtetéseket vonhatunk le.

A fenti okfejtés következtében azt a megállapítást tehetjük, hogy a bizonyítási eszközök beszerzésének a digitális térben is törvényesnek és szakszerűnek kell lennie. Megfelelően kell dokumentálni, és biztosítani kell a zárt bizonyítási lánc meglétét a megszerzéstől egészen az értékelésig. Ugyanazon adatokat kell látnia a bírónak is, mint a helyszínen intézkedő rendőrnek, szakértőnek, vagy az eljárás során az adatokat elemző szakembernek. Ezt minden esetben, az eljárás minden szakaszában biztosítani kell.

A digitális bizonyítási eszköz

A digitális bizonyítási eszközöket a számítástechnikai rendszerekből, azok adathordozóiról szerezzük be. A Btk. 300/F.§ (3) bekezdése a számítástechnikai rendszert nagyon széles körben határozza meg: *„[...] számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége."* Ilyenek az átlagos számítógépek, de a mobil telefonok, és sok más eszköz is. Ide tartoznak viszont olyan eszközök is, melyekről első ránézésre nem gondolnánk, hogy számítástechnikai rendszerek, mint pl. a gépkocsik vezérlő egységei vagy az intelligens háztartási eszközök.

Ha nem a jogi definíció oldaláról nézzük az eszköz meghatározását, már sokkal érdekesebb képet kapunk. Matus Márk rámutat, hogy a számítástechnikai környezet, illetve az informatikai rendszer fizikai eszközökből, az azokat irányító és azokon szolgáltatást nyújtó számítógépes adatokból (programok és beállítások), valamint egyéb adatokból (felhasználói adatok) áll.[2] Ebből a környezetből kell az informatikai bizonyítási eszközöket beszereznünk. Nézzük meg, hogy az összetevőkből melyek lehetnek a digitális bizonyítás eszközei, miből vonunk le következtetéseket egy-egy számítástechnikai rendszer vizsgálatakor.
Az első elem a fizikai eszköz. Az eszközön, dolgon lévő sérülések, ujjnyomatok, anyagmaradványok, átalakítások nem digitális bizonyítékok, így a témánk szempontjából irrelevánsak, bár sok esetben nagyon fontos bizonyítási eszközök

[2] Matus Márk: Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben. In: Kriminalisztika 1-2. (Szerk.: Bócz Endre) BM Duna Palota és Kiadó, Budapest, 2004. 10. fejezet 10.6

lehetnek. A dolgokkal, eszközökkel csak abból a szempontból foglalkozunk most, hogy ezek a hordozói az adatoknak, amelyek digitális bizonyítási eszközként a későbbiekben rögzítésre kerülnek.
A számítógépes környezet másik eleme az adat, amely a hardver elemeket irányítja, és emellett különböző szolgáltatásokat is nyújt. Ilyenek a számítógépes operációs rendszerek, programok és azok beállításait rögzítő adatok. Ezek az adatok már digitális formában léteznek, tehát digitális bizonyítási eszközök.

A számítógépes környezet következő elemei azok az adatok, melyeket felhasználói adatként definiálunk. A felhasználói adatokat felhasználók hozzák létre különböző programok vagy hardverelemek segítségével, így születnek a szöveges dokumentumok, képek, filmek, hangállományok stb. Ezek közös jellemzője, hogy a felhasználó közreműködésével, közvetlenül vagy közvetlen módon jönnek létre. Közvetett módon úgy, hogy a felhasználó akarata nem arra irányul, hogy egy ilyen adatot hozzon létre, de az általa használt felhasználói program működése során, mintegy a működés melléktermékeként létrehozza ezeket az adatokat. Például egy szövegszerkesztővel szerkesztett dokumentum készítése során az automatikus mentési funkció beállításával folyamatosan egy átmeneti, a felhasználó számára nem látható állomány keletkezik, melyben a dokumentum aktuális állapota található. Itt is csak adatokról beszélhetünk, melyek a hardveren, tehát az adathordozón tárolódnak.

Megállapíthatjuk, hogy a digitális bizonyítási eszköz adat, tehát nem megfogható dolog. Az adatok önmagukban nem léteznek, azokat csak valamilyen adathordozó rögzíti. Például a most olvasott adatokat papír rögzíti. Korábban a számítógépem adathordozóján voltak digitális formában, és a nyomdai munkálatok során még más adathordozókra is rákerültek. Ha ezen írásommal valamilyen bűncselekményt valósítanék meg, akkor nem az lenne a lényeges, hogy az írásom papíron vagy számítógépen található-e meg, hanem maga az adat, amelyet (közvetlenül) létrehoztam. Ebből is látható, hogy a bizonyítási eszköz nem az adathordozó, hanem az adat, ami az informatikai rendszerben csak digitális formában létezik. Az adatokat az informatikai rendszerek technikai sajátosságaik folytán csak egy értéksorozatként rögzítik (pl. az „adat" szót az informatikai rendszer a következő értéksorozatként tárolja: 01000001 01000100 01000001 01010100). Önmagában az adat csak egy értéksorozat, függetlenül attól, hogy az milyen adathordozón tárolódik. Ezt az értéksorozatot kell tehát vizsgálni, mert ennek van adattartalma. Az adat a rögzítés, az elemzés és a vizsgálat során egyik adathordozóról a másikra kerül. Az informatikai eszközök sajátossága, hogy ezek az értéksorozatok, adatok nagyon könnyen szinte nyom nélkül módosíthatók, törölhetők, így a biztosításuk során minden alkalommal fokozott óvatossággal és a szabályok pontos megtartásával kell eljárni.

Minden bizonyítási eszköz megszerzésének az egyik legalapvetőbb szabálya, hogy azt csak dokumentáltan lehet beszerezni. Minden esetben a megfelelő dokumentációt el kell készíteni, és figyelni kell arra, hogy azon minden lényeges momentum, jogszerűség, azonosító adatok, a biztosítás körülményei, ideje, helye stb.

fel legyen tüntetve. Ez az egyik alapvető kritérium a digitális bizonyítási eszközök beszerzésénél is.

A bizonyítási eszközöket a kriminál technika szabályai szerint leírással, rajzzal, fényképezéssel, az adathordozó lefoglalásával vagy egyéb módon való rögzítéssel, másolással lehet biztosítani. Bármilyen furcsának is tűnik, ezeket a módszereket adott esetben párhuzamosan is alkalmazni kell. A biztosítani kívánt számítástechnikai eszközök azonosító adatait jegyzőkönyvezni kell, szükség esetén a hálózati topológiát le kell rajzolni akár egy vázlatrajzon. A legáltalánosabb, hogy az adathordozókat lefoglalással biztosítjuk, de akár a helyszínen, akár később az adatokat át kell másolni egy másik adathordozóra, amelyeken az elemzéseket, vizsgálatokat el tudjuk végezni. Meglepő lehet, de egyes esetekben akár a hálózati forgalmat, vagy a gép operatív memóriájának tartalmát is rögzíteni kell. Mivel azok nem rögzülnek sehol, nekünk kell rögzítenünk egy adathordozón. A kriminál technika követelménye, hogy a rögzítés hiteles, változatlan és törvényes legyen.

Általában az adathordozókat lefoglalással biztosítja a nyomozó hatóság. Magának az eszköznek, a dolognak a lefoglalása kimunkált szabályok szerint történik. Nagy figyelmet kell fordítani a lefoglalandó eszközök körére. Régebben gyakorlat volt, hogy akár a monitort, vagy a klaviatúrát, egeret is elvitték a rendőrök. Későbbi ügyészi állásfoglalások e fölösleges lefoglalások visszaszorítása érdekében az adathordozókra korlátozták a lefoglalandó eszközök körét. Álláspontom szerint azonban nem elég, ha a nyomozó hatóság csak az adathordozókat foglalja le, szereli ki a számítógépből, attól félve, hogy olyan eszközöket ne foglaljon le, melyek feleslegesek az eljárás során. Több konkrét példa is igazolta, hogy a számítógépbe szerelt adathordozókat nem szabad kiszerelni, még akkor sem, ha ezt szakember teszi, mert az új technológiáknak köszönhetően ezek az eszközök már olyan egységet képezhetnek, hogy ha megbontják őket, már nem lehetséges az eredeti adattartalom visszaállítása (pl. RAID tömbök esetében). Ezért az egész gépet el kell hozni, és csak a perifériák hagyhatók a helyszínen. De vannak olyan helyzetek, amikor azokra is szükség lehet.

Az adathordozón lévő adatok biztosításánál arra kell ügyelnünk, hogy az adatok ne változzanak a biztosítás során. Hitelesíteni lehessen, hogy ugyanazokat az adatokat vizsgáljuk, tehát nem változtak meg az adatok. Az átlagos felhasználó számára talán meglepő az a tény, hogy ha bekapcsolja a számítógépét és mást nem csinál, egyetlen billentyűt sem üt le, az egérrel se kattint, már akkor is megváltozik a winchester adattartalma. Ahhoz, hogy az adathordozón lévő adatokat vizsgálni tudjuk és a vizsgálat során azok ne változzanak, át kell őket másolnunk egy másik adathordozóra. Felmerülhet, hogy ne minden adatot másoljunk, hanem csak azokat, melyek számunkra lényegesek lehetnek. A probléma ezzel az, hogy az eljárás elején sokszor még nem tudhatjuk, mi lehet a releváns adat, így sérülhet a teljesség elve. (Előfordulhatnak egyértelmű esetek, amikor csak naplóállományokat kell rögzíteni, de nem ez az általános.) Ezért amennyiben egy olyan egész adathordozót foglalunk le, amely újraírható, vagy az adatok módo-

síthatók rajta, akkor az egész adattartalmat kell átmásolni egy másik adathordozóra. Szükséges ez azért is, mert az adathordozón rejtett adattartalmak is találhatók, mint pl. a törölt, a *slack*[3] és az átmeneti állományok, melyek alapesetben nem láthatók. Az adathordozóról csak egy gondosabb vizsgálat tudja kimutatni, láthatóvá tenni az adattartalmat. Ezért az adathordozóról bit-szintű másolatot kell készíteni, tehát az adathordozón lévő adattartalmat bitről-bitre pontosan át kell másolni. Ez történhet ún. image másolatként, amikor az eredeti adathordozóról egy képfájlt készítünk, de készülhet ugyanilyen bit-szintű másolattal egy klón is, amely bitről-bitre megegyezik az eredeti adattartalommal. E másolatnak előnye, hogy rajta a törölt, rejtett vagy *slack* állományok ugyanúgy elemezhetők, mint az eredeti adathordozó.

A másolatot úgy kell elkészíteni, hogy közben véletlenül se írjunk az eredeti adathordozóra. Ennek az elvárásnak úgy tudunk megfelelni, ha írásvédővel, azaz egyirányú adatforgalommal készítjük el a másolatot. Az írásvédelem hardveres vagy szoftveres úton is megvalósítható. Ezzel az eljárással tudjuk biztosítani a teljesség elvét, illetve azt, hogy

1) a bizonyítási eszközt úgy vizsgáljuk, hogy az nem változik meg,
2) a teljes adatállományt vizsgáljuk minden egyes részletében úgy, hogy
3) az eredeti adathordozó megmarad, olyan állapotban, ahogyan azt lefoglaltuk.

A hitelességet azzal tudjuk biztosítani, hogy írásvédő eszközön keresztül készítünk egy ún. *hash* kulcsot, más néven digitális ujjnyomatot az eszközről. Azaz matematikai szabvány, kulcs szerint 256 vagy 512 bájt hosszúságú karaktersorozatot kapunk az adatállományról, amely egyedi, tehát csak az adott adatállományra jellemző. Amennyiben az eredeti adatállományon akár egyetlen bit változtatás is történik, annak a *hash* kulcsa már nem egyezik meg az eredeti értékével. Ilyen módon könnyen ellenőrizhető, hogy a másolat adattartalma megegyezik-e az eredeti adattartalommal.

Azokban az országokban, ahol ezt a módszert már mindennapi gyakorlatban használják, ez úgy történik, hogy három példányban készítik el a *hash* kulcsot tartalmazó riportot. Ebből egy példányt a lefoglalást elszenvedőnek adnak át, a másik példányt a nyomozati iratokhoz csatolják, míg a harmadikat a lefoglalt adathordozóval együtt, attól nem elválasztva kezelik. Ezzel a módszerrel az eljárás bármely szakaszában ellenőrizni lehet az eredeti és a másolat adathordozók hitelességét. Napjainkban az egyik legelterjedtebb és *hash* kulcs generáló, digitális ujjnyomat készítő eljárás az 512 bájt hosszú ellenőrző összeget adó MD5-ös eljárás.[4]

[3] A *slack* terület a fájl elejétől a fájl által használt utolsó *cluster* végéig terjedő lemezterület. Amennyiben ezt a területet nem írjuk felül valamilyen adattartalommal, úgy azon sok olyan adat is megtalálható lesz, mely egy korábbi fájl-állomány része volt.

[4] A matematikai módszerek fejlődésével ez a szabvány változhat, módosulhat, a mindenkori matematikai tudásunknak megfelelően. Akár a kulcsot generáló algoritmust válthatja

De még az előző két módszer együttes használata sem mentesíthet az alól a kötelezettség alól, hogy ezeket a műveleteket szigorúan szabályozott, törvényes, dokumentált rendben kell elvégezni, a megfelelő, törvényes eljárási keretek közt onnantól kezdve, hogy az adathordozót felkutatjuk, egészen a vizsgálatok elvégzésén át az adathordozó tárolásáig. E műveleteket csak olyan személy végezheti, aki ehhez megfelelő képesítéssel rendelkezik, és olyan eszközöket kell használnia, melyeket a rendészeti szervek a megfelelő szabályok követésével adoptáltak. Amennyiben ennek a másolatnak az elkészítését nem a rendészeti szerv alkalmazottja végzi el, hanem egy külső szakértő vagy szaktanácsadó, a másolatkészítést akkor is megfelelően dokumentálni kell. A másolatot készítő szakértőnek, szaktanácsadónak szintén képesítéssel kell rendelkeznie a tevékenység elvégzéséhez.

A digitális bizonyítási eszközök osztályozása

A fenti módszerrel megszerzett adatok, bizonyítási eszközök lehetnek digitális dokumentumok, digitális nyomok, valamint digitális okiratok.

A digitális dokumentumok jellemzően azok az állományok, melyeket a felhasználó akarattal hoz létre. Ilyenek a szöveges dokumentumok (.doc, .txt stb. kiterjesztésű állományok), a táblázatkezelővel, bemutatókészítővel készített táblázatok, de ide sorolandók a képek, videó- vagy hangállományok, különböző adatbázisok és minden olyan adatállomány, melyet a felhasználó készít. Közös jellemzőjük, hogy a létrehozásukhoz használt program birtokában minden különösebb szakértelem nélkül megtekinthetők, a bennük tárolt információk megismerhetők. Az élet nyelvére lefordítva: ezek ugyanolyan dokumentumok, mint a házkutatás során egyébként lefoglalt feljegyzések, kézzel vagy géppel írt naplók, rajzok, festmények, táblázatok. A digitális dokumentumok információtartalmának kiértékeléséhez egyetlen nyomozó hatóság sem kér fel szakértőt, hiszen az írni-olvasni tudás nem különleges szakértelem. A digitális írástudás ma már nem számít különleges szakértelemnek.

Természetesen ekkor csak a digitális dokumentumok mindenki számára megismerhető információtartalmát vizsgáltuk. Nem tartozik az alapvető digitális műveltség körébe, hogy ezen digitális dokumentumokban lévő rejtett vagy metaadatok milyen információkat hordoznak, azok mennyire valósak vagy módosítottak. Ezeknek a kérdéseknek a megválaszolásához már speciális tudás szükséges. A digitális dokumentumok vizsgálata tehát nem kíván különleges szakértelmet, így azt minden esetben a nyomozó hatóság tagjának kell elvégeznie, nem szakértőnek, főleg hogy azok tartalmi vizsgálata alapvetően jogkérdések eldöntésére irányul.

fel egy tökéletesebb, akár a kulcs hosszúsága növekedhet a nagyobb biztonság, és hitelesség elérése érdekében.

A digitális nyomok nem a traszológiai értelemben vett nyom fogalmával írhatók le, hanem az annál tágabb kriminalisztikai nyom fogalmába tartoznak. Ide sorolhatók azok az adatok, amelyek az adathordozón az őket létrehozó programmal nem tekinthetők meg, tehát vizsgálatuk többlet ismeretet követel. Ezek jellemzően az átmeneti-, a törölt állományok, vagy a *slack* területek. De ide tartoznak azok a regisztrációs, vagy napló adatok is, melyek a számítástechnikai rendszer működését befolyásolják vagy naplózzák, illetve a számítógépen futó programok bináris kódjai is. Ezek között akadnak olyan adatok, amelyek értelmezéséhez fölösleges külső szakértőt kirendelni. Ehelyett megfelelően kiképzett, vizsgázott bűnelemző is végezheti ezt a feladatot. Úgy gondolom, hogy a digitális nyomok felkutatására és elemzésére a nyugati mintákhoz[5] hasonlóan különlegesen kiképzett, informatikai bűnelemzői ismeretekkel rendelkező rendőri állomány lehet csak képes. Az informatikai bűnelemzésnek az operatív bűnelemzési területhez hasonló fejlődésére van szüksége: ma már teljesen elfogadott és bevett gyakorlat, hogy operatív bűnelemzők végzik az ügyek elemzését, de a híváslisták és a bankszámlaforgalom elemzését is, és ehhez nincs szükség külön szakértőre. Ugyanilyen státuszban végezhetnék el az informatikai bűnelemzők a digitális dokumentumok és nyomok elemzését. E megoldásnak két előnye lenne, amely úgy a védelemnek, mint a vád képviselőinek kedvezne, és egyben a törvényesség feltételeinek is megfelelne. Egyrészt sokkal gyorsabban kapna értékelhető eredményt a nyomozó hatóság, másrészt sokkal kisebb költségráfordítással folyhatna a nyomozás. Szakértőt csak abban az esetben kellene kirendelni, ha szakkérdésre várunk választ, pl. módosították-e a programot, vagy illetéktelen behatolás történt-e.

A csoportosítás utolsó eleme a digitális okirat. A digitális okirat olyan adat, amelyet hitelesként fogadunk el, mert a rendszer automatikusan generálja őket (pl. egy szerver napló-adatait a felhasználótól függetlenül, a felhasználó beavatkozását kizárva) vagy mert a felhasználó azokat nem tudja később módosítani, csak úgy, hogy a módosítás is rögzül a rendszerben. Ezek az adatok jellemzően nem a felhasználó saját számítógépén keletkeznek, hanem a szolgáltatónál. Ezért beszerzésük nem lefoglalással, hanem megkereséssel történik. Ilyenkor a nyomozó hatóság a Be. 71. §-a szerinti megkereséssel él a szolgáltató felé, aki kikeresi a saját rendszeréből a kért (napló- és regisztrációs) adatokat és egy adathordozón átadja. De ilyen napló-adatokat találhatunk a felhasználó számítógépén is (pl. egyes programok napló-adatai), amelyeket szintén digitális okiratként kezelünk.

A digitális okiratokat szintén a hatóság vizsgálja, értékeli. Ezek között vannak olyanok, amelyek értékeléséhez nem szükséges különleges szakértelem (pl. regisztrációs adatok), ugyanakkor másokhoz már magasabb szintű szakismeret

[5] A volt NSZK-ban a Berlini Tartományi Rendőrségnél, a jelenlegi Németországban a BKA szerveinél, az Egyesült Királyságban az NHTCU szerveinél, valamint Franciaországban is hasonló szervezeti megoldást alkalmaznak. Szakértőket csak a ténylegesen különleges szakértelmet kívánó feladatokhoz vesznek igénybe.

szükséges (pl. a napló-adatok elemzése). Az utóbbiakat az informatikai bűnelemzők értékelik – hasonlóan a papíralapú okirati bizonyítékokhoz.

A digitális okiratok speciális formája az elektronikus levél. Anélkül, hogy ezt az érzékenyebb témát mélyebben kifejteném, megjegyzem, hogy nem kellően rendezett ezen okiratok beszerzése a büntetőeljárás során. A Be. 151.§ (4) bekezdése értelmében *„A címzettnek még nem kézbesített postai és hírközlési küldeménynek […]lefoglalását a vádirat benyújtásáig az ügyész […] rendeli el"*. Ez olyan egyértelmű törvényi rendelkezés, amely a magán- és a levéltitkot védi. E törvényi rendelkezés alkalmazásával digitális környezetben az a probléma, hogy nem egyértelmű a jogalkalmazás számára, mikor kell az elektronikus leveleket kézbesítettnek tekinteni. Az egyik nézet szerint a kézbesítés akkor történik meg, amikor azt a felhasználó (a postafiók használója) a saját számítógépére letöltötte. Ez egyértelmű és pontos megfogalmazás, de a technikai lehetőségeket nem veszi figyelembe. Sok levelező rendszer ugyanis megengedi, hogy a leveleket a felhasználó ne töltse le a saját számítógépére, hanem azokat webes felületen nézze meg. Így a levelek soha nem töltődnek le a felhasználó saját számítógépére, tehát nem lehet tudni, hogy megtekintette-e azokat. Véleményem szerint ez a felfogás téves, és indok nélkül korlátozza a nyomozó hatóságot. A helyes megközelítés szerint akkor kell kézbesítettnek tekinteni az elektronikus levelet, amikor az bekerül a szolgáltatónál a felhasználó postafiókjába. Innentől kezdve a felhasználó már szabadon rendelkezhet a levéllel – megtekintheti vagy akár törölheti ugyanúgy, mintha a postafiókjába vagy levelesládájába kerülne a küldemény. Ezt a nézetet támasztja alá a postáról szóló 2003. évi CI. törvény 3.§ 28. pontja és a postai szolgáltatások ellátásáról és minőségi követelményeiről szóló 79/2004. (IV.19.) Korm. rendelet 14.§ (1) bekezdése is. Tiszta jogi megoldást az adna, ha erre a törvényalkotók olyan szabályt hoznának, mely tisztázná és egyértelművé tenné a helyzetet.[6]

Összegzés

A digitális bizonyítási eszközök beszerzésének szabályai sem tételes jogszabályok, sem belső normatívák, sem a szakirodalom területén nem kimunkáltak. A napi gyakorlatban egymástól nagyon eltérő jogértelmezésekkel és megoldásokkal találkozhatunk. Ezen a téren nagyon sokat fejlődtek a nyomozó hatóságok, ám még nem eleget. Úgy gondolom, hogy ha majd a fent vázolt elvek szélesebb körben elfogadottá válnak, és ezek alapján történik a munkavégzés, akkor az elektronikus bizonyítékok megszerzése sokkal szakszerűbb és törvényesebb lesz. Ennek következtében felgyorsulhatnak a büntetőeljárások és a törvényességi garanciák is sokkal egyértelműbbek lesznek.

[6] Természetesen a fenti probléma csak az elektronikus levelek tartalmának megismerésére vonatkozik, mert a már korábban említett Be. 71.§ szerinti megkereséssel a postafiók regisztrációs adatai, valamint napló adatai elérhetőek a nyomozó hatóságok számára, és azok digitális okiratokként értékelhetők.

Elkerülhetők lesznek az olyan esetek, amikor egy IP cím szolgáltatójának a megállapításához kötelezően szakértőt kell kirendelni, holott ez az információ az interneten megtalálható, hiszen közhiteles adatbázisból mindenki számára elérhető. Elkerülhető lesz az is, hogy a helyszíni intézkedést végző rendőrök bekapcsolják a számítógépet, és az abban lévő adathordozó tartalmát a helyszínen vizsgálják, kockáztatva ezzel a bizonyíték integritását.

Úgy gondolom, hogy a hatóság arra kiképzett szakembere rendszerbe állított technikai eszközeivel, a vonatkozó eljárási szabályok megtartásával maga készíthet másolatot az adathordozókról és ilyen módon maga is értékelheti az adathordozók tartalmát. Igazságügyi szakértőt csak akkor célszerű kirendelni, ha ténylegesen szakkérdés megállapítása szükséges, nem pedig a digitális írástudás pótlására. Így az eljárások gyorsabbak, olcsóbbak, mégis törvényesek, a Be. garanciái pedig biztosítottak lesznek. Természetesen ez azt is jelenti, hogy csak azok a szakértők lesznek képesek megmaradni a piacon, akik kellően felkészültek és elkötelezettek szakmájuk iránt. A másik oldalon viszont a bűnüldöző hatóságoknak kell egy olyan szakértelemmel rendelkező technikai és háttértárelemzéssel foglalkozó szakembergárdát kinevelni, és eszközökkel ellátni, akik ezeket a feladatokat el tudják végezni. Ez rövidtávon nem megoldható feladat, de a nemzetközi tapasztalatok alapján ez az egyetlen mód arra, hogy a felvegyük a harcot a 21. századi technikát alkalmazó bűnözőkkel szemben.

NAGY ZOLTÁN ANDRÁS[1]

A Pirate Bay-per tanulságai
De lege ferenda a fájlcseréről

A terresztriális, a műholdas, majd a kábelen történő műsorszórás szerzői jogi szabályozásának alapját általánosságban azok a tradicionális szerzői jogi rendelkezések képezik, amelyeket a könyvnyomtatás, a könyvterjesztés és a rádió- és televízió műsorok készítése területéről már ismerünk. A szerzői jognak az új és újabb technikai eszközöknek, technológiáknak a megjelenésére adott válasza és betartása (betartatása) – napjainkig – nem okozott különös nehézséget, mivel a szerzői művet készítők, továbbítók, forgalmazók stb. köre (pl. a rádió- és televíziós társaságok, könyv- és lemezkiadással foglalkozó cégek, kábeltársaságok, filmforgalmazók) behatárolható, és nem túl nagy létszámúak. A jogszabályok betartásának kontrollját éppen az teszi lehetővé, hogy a szerzői művek megjelennek a külvilágban, a valóságos térben, amely mindenki számára érzékelhető (kinyomtatták, kiadták könyvben, vetítették a filmszínházak, játszották színházban, rádióban, televízióban stb.).
De a másolatok készítése a másológépek fejlődésével egyre szabadabbá vált. Ehhez járult a kommunista diktatúrákban a másolás politikai, állambiztonsági ellenőrzésének (stencilgépek kötelező elzárása, használatuk, és használói naplózása, az intézményi és a vállalati írógépek ellenőrzése, azok betűmintáinak rögzítése stb.) megszűnése, amellyel a másolás, így a szerzői művek duplikálása is szabaddá, és tömegessé vált. Ez egyszersmind már évtizedekkel ezelőtt előrevetítette a szerzői jog rendelkezései betartatása nehézségét.
Az 1990-es évektől az Internet kommunikációs lehetőségeit kihasználva, továbbfejlesztve megalkották a fájlcserét lehetővé tevő programokat, amely segítségével ma már a felhasználók zárt hálózatot alkotnak.

Kriminológiai adalék

Egy az USA-ból származó forrás szerint 63 millió (!) felhasználó folytat állandóan, vagy alkalmakként fájlcserét, azaz a térben egymástól távollevő felhasználók egymás zeneszámait, filmjeit, képeit, szöveges dokumentumait (pl. regényeket) töltögetik le.[2] Ha az USA-ban 63 millió (de akár 53, vagy 73 millió felhasználó létezhet), akkor hányan vannak a világban? 800 millió, egy, esetleg másfél milliárd fájlcserélő felhasználó van? Ami azt jelenti, hogy ha minden felhasználó csupán egyetlen egy zeneszámot töltött le, akkor 800 millió, egymilliárd stb. zenei felvétel, film, könyv, szoftver és más szerzői alkotás után nem fizettek, fizetnek

[1] Nagy Z. A., docens, PTE ÁJK Büntetőjogi Tanszék
[2] http://www.szamitastechnika.hu/hirek_hir.php?id=32414

jogdíjat. Ez érinti az előadóművészen túl a mögé kiépült iparágat (a stúdióktól a forgalmazókig, a kereskedelmi és a mozilátogatottsági forgalmat egyaránt). Az adathordozókra kivetett üreskazetta-díj pótolhatja a veszteség egy részét, ám itt a szerzői jog intézményei, normái háttérbe kerülnek.

A fájlcsere dinamizmusa

A többféle technológiát[3] alkalmazó fájlcsere a program indításával, a szerverre kapcsolódó felhasználók zárt hálózatának kialakításával kezdődik, majd a felhasználók feltöltik a szerverre a felkínált fájlokat (pl. warez-oldalakon, hub-ok hálózatában), vagy az azokat elérő linkeket (pl. torrent hálózatokban).

A 1999. évi LXXVI. törvény a szerzői jogról (a továbbiakban Szjt.) terjesztésnek tekinti a mű eredeti, vagy többszörözött példányainak a nyilvánosság számára történő hozzáférhetővé tételét forgalomba hozatallal vagy forgalomba hozatalra való felkínálással (Szjt. 23. § (1) bekezdés). Az Szjt. 23. §-a tehát a hozzáférhető tétel fogalmába vonja a forgalomba hozatalt, és a forgalomba hozatalra való felkínálást. A büntetőjogban kivételes, hogy egy tényállásban a magatartás befejezett stádiuma és az előkészület is büntetni rendelt. Egy másik Szjt.-beli törvényhelyhez fűzött miniszteri indokolás a szerző terjesztéshez való jogával összefüggésben úgy érvel, hogy a terjesztés a mű eredetijének és másolatainak a közönség számára adásvétel vagy egyéb tulajdon-átruházás révén történő hozzáférhetővé tételét jelenti, alapvetően a dologi műpéldányok vonatkozásában (Szjt. 17. § b) ponthoz fűzött miniszteri indokolás.) Ez a jogirodalmi értelmezés a tulajdon-átruházásra koncentrál.

Ám a feltöltő tévedése (Btk. 27. §) a szerzői mű szabad felhasználása tekintetében nem zárható ki. A szabad felhasználású szerzői műveket (pl. freeware szoftvereket szabadon, a shareware szoftverek feltételekkel, a promóciós célú zenei felvételeket, a saját szerzői alkotásokat stb.) bárki terjesztheti az Interneten, és más hálózatokon. Az, hogy a szerzői mű szabadon felhasználható-e, olyan konstitutív erejű tény, amely a büntetőjogi felelősség megállapítása szempontjából releváns. Természetesen ne legyenek illúzióink abban, hogy ez csupán a feltöltött fájlok töredékére igaz. Igen magas arányban a szerző, vagy a szerzői mű kiadója hozzájárulásának hiányában is terjesztenek szerzői alkotásokat.
A feltöltés *felkínálásnak* értelmezhető, akár a szerzői mű a maga teljességében, akár csupán a hozzá vezető link jelenik meg a programban. Valamely szerzői alkotás fájlcsere-hálózatokra történő feltöltése tehát jogellenes cselekmény. Ha a feltöltés jogellenes, mert a feltöltő az adott szerzői művet a szerző engedélye nélkül terjeszti, akkor, úgy vélem, a *letöltést* is jogellenesnek kell értékelni a ius ex iniuria non procreatur (jogellenes cselekmény nem teremt jogszerűt) jogelvnek megfelelően.

[3] Nagy Z. A.: Bűncselekmények számítógépes környezetben. Ad-Librum Kiadó, Budapest, 2009.

Ahogy a feltöltő, úgy a letöltő tévedése sem zárható ki a szerzői mű szabad felhasználása vonatkozásában. Ehelyütt is, ismételve: az, hogy a szerzői mű szabadon felhasználható-e, vagy sem, olyan konstitutív erejű tény, amely a büntetőjogi felelősség megállapítása szempontjából releváns.

Tudhatja-e a letöltő, hogy az általa letöltött fájlok legális forrásból származnak-e vagy sem, hiszen több százezer-, millió fájl „kering" a fájlcserélő hálózatokban, és naponta változik a legális-illegális szerzői művek aránya az Interneten. Valószínűsíthetően a letöltött fájlok döntő többsége, különösen a filmek tekintetében illegális forrásból ered. Ami gyakorlati problémát jelent, hogy a letöltő a letöltéskor nem a szerzői mű egészét szerzi meg, hanem annak egy-egy részletét, a szerzői művet képező fájl egy-egy szeletét. Órák, esetleg napok múlva áll össze számítógépén a teljes fájl, azaz a teljes szerzői mű. A letöltéskor a tettenérésnél csak fájlszeletek letöltése bizonyítható.

A piaci érdekek előbbre valók

Ma a szerzői jog védelmében a szerzői jogi lobbyn kívül senki sem érdekelt. A felhasználók érdeke talán még érthető, de a számítástechnikai, a szórakoztató elektronikai ipar, az Internet-szolgáltatók, de még a telefontársaságok is saját piaci érdekeiket helyezik előtérbe a védendő jogok körének meghatározásánál.

1. A kereskedelmi forgalomban kapható DVD-lejátszók is mindinkább kettős (dual-) lézersugarasak, így a gyári DVD lemezek lejátszása mellett alkalmasak a CD-lemezre házilag, (S)VCD, DVD formátumban írott filmek lejátszására is. Már kaphatók olyan DVD-lejátszók (5-10 ezer forintért, tehát megfizethető áron), amelyek az .avi, az .mpg, az .mpeg és más videó-formátumba tömörített filmek lejátszására is alkalmasak. Az mp3 formátumba tömörített lemezek lejátszására olyan hagyományos zenei eszközök is alkalmasak, mint a DVD-lejátszó, a hi-fi torony, vagy a hordozható CD-lejátszó. A DivX-lejátszók azzal, hogy az .avi formátumú filmeket a televízión lejátszhatóvá teszik, megtakarítják a konvertáláshoz szükséges és a minőségében nem garantálható konvertálás relatíve hosszú idejét (a számítógép teljesítményétől függően 2-10 óra).

A probléma az, hogy *kereskedelmi forgalomban* avi, mpg, mpeg, valamint mp3 stb. fájlformátumokban *szerzői alkotás jelenleg nem kapható*. Bár lehetséges házivideó-felvételek konvertálása, saját zene konvertálása, de nem ezek a műveletek tűnnek meghatározónak. Egyébként a gyártók még nem is egyeztek meg ilyen fájlformátumok forgalmazásában. A mai zenei CD szabványa két óriáscég, a Philips és a Sony 1982-es megállapodásán (az ún. Vörös Könyvben lefektetetteken) nyugszik.

Az .avi és .mp3 stb. formátumokba tömörített szerzői jogi művek zömmel illegális forrásból szerezhetők meg az Internetről. Ezzel minden bizonnyal tisztában van az is, aki ezen eszközöket gyártja, forgalmazza. A vásárló tehát az eszközök megvásárlását követően keresni fogja az új fájlformátumokat az Interneten, vagy

másutt érdeklődik felőlük, és hamar rá fog találni a (jórészt nem legális) forrásokra.

A helyzet csak első látásra paradox. Hiszen ha a technikai eszközök iránt kereslet mutatkozik, a kereslet kielégítése pedig pénzt hoz. A technikai eszközök gyártói, forgalmazói természetesen saját profit-érdekeiket helyezik előtérbe. Persze, reális felvetés az, hogy egy eszköz sosem önmagában bűnös. Ám miért is gyártanak ilyen technikai eszközöket? Azért, mert funkciója miatt eladható.
El kell ismerni, hogy *nem ezek a technikai eszközök indukálják* alapvetően a szerzői jog megsértését, legfeljebb bővít(het)ik az elkövetői kört.

2. A tárhely-, illetve a hálózati hozzáférést biztosító szolgáltatóknak lenne lehetőségük a fájlcsere korlátozására, illetve visszaszorítására. Az elektronikus kereskedelemről szóló 2001. évi CVIII. törvény (a továbbiakban Eker. törvény) 7-12. §-ai gyakorlatilag „kilúgozzák" a szolgáltatók felelősségi rendszerét.

aa. A *tárhely-szolgáltatók* a tárhely-bérlő által szervereikre feltöltött adatállományokat, ha nem is rendszeresen, de véletlenszerűen ellenőrizhetik. A videófájlok méretük és kiterjesztéseik alapján könnyedén azonosíthatók és ellenőrizhetők lennének. A tárhely-szolgáltatók e tevékenysége azonban megmarad lehetőségként, hiszen sem az elektronikus kereskedelmi irányelv, sem pedig az Eker. törvény nem ad lehetőséget a tárhely-szolgáltatóknak a tartalom monitorozására. Ellenkező esetben azonban ez a tevékenység hozzájárulhatna a jogtisztulási folyamat elindulásához.

ab. A tárhely-szolgáltatóknak össze kellene fogniuk abban (pl. listát összeállítani), hogy azon személyekkel, akikkel szemben polgári-, vagy büntetőeljárás indult szerzői jogsértések miatt, nem kötnek bérleti szerződést.

ba. A *közvetítő szolgáltatók* hálózatán zajlik a forgalom, így ők gyakorlatilag „mindent látnak". Egy-egy felhasználó forgalma technikailag figyelemmel kísérhető, a szerződési feltételek eszközével korlátozható is lenne. Az ügyfélkör bővítése, a minél nagyobb sávszélesség elfogadtatása magasabb előfizetési díjért, komoly ellenérdek. A forgalomkorlátozás indokaként a hálózati torlódások elkerülése reális indok[4], de a fájlcsere visszaszorítását is szolgálhatja. A forgalmat növelő videófájl-letöltések kisebb arányban származhatnak legális forrásból is pl. ismeretterjesztő és vallási műsorok, házi videók, humoros videók stb. szabadon elérhetők, letölthetők.

3. A *keresőszolgáltatók és a cache-szolgáltatók* kapcsán egy más jellegű, in concreto jogi felelősség vethető fel. E szolgáltatók egy linkadatbázist tárolnak. Ám az általuk tárolt, és a keresésekre válaszként nyújtott linkadatbázis segítségével nemcsak a szerzői alkotásokat tartalmazó linkek érhetők el, hanem ezeken túl a pornográf, pedofil, rasszista, szélsőjobboldali, becsületsértést, rágalmazást

[4] http://index.hu/tech/jog/2009/08/05/elmarasztaltak_a_upc-t_mert_lassitja_a_fajlcseret/?rnd=666; [Letölve: 2010. február 5.]

tartalmazó, a kábítószert, hamis gyógyszert, vagy más hamis terméket árusító, vagy egyéb tiltott tartalmat megjelenítő weboldalak is.

Strict értelmezéssel a keresőszolgáltatás még akár bűnsegédi tevékenységként is felfogható. A keresőszolgáltatók által biztosított, a keresés eredményeként megjelenő linken érhető el a weboldal, ahová kattintva a felhasználó tiltott tartalmat tölthet le vagy fel. A le- vagy feltöltés elősegítése a Btk. 329/A. §-ában meghatározott alapcselekmény bűnsegédi magatartása megállapításához elégséges.

Ma a szolgáltatók felelőssége nem terjed túl a polgári jogi felelősségen, jóllehet az elektronikus kereskedelmi irányelv[5] jogági szűkítés nélkül rendelkezik azok felelősségéről.[6]

4. A telefontársaságok által a szerzői művek eléréséhez adott segítség (szolgáltatás) is aggályosnak tekinthető. Ugyanis a warez- és egyéb oldalakról történő letöltéshez a hazai telefontársaságok emelt díjas sms-szolgáltatással segédkeznek. 06-90 vagy 06-91-es kezdetű hívószámra küldött emeltdíjas sms-re a válasz-sms-ben kapja meg a felhasználó az illegális tartalmak eléréséhez szükséges jelszót vagy egyéb azonosítót. Azaz a hazai telefonszolgáltatók jogsértő tevékenységhez nyújtva keresnek – összbevételeik mellett nem jelentős – összeget, ám ezt az elérésben nyújtott segítséget is jogellenesnek tekinthetjük.

Magyarországi jogszabályi törekvések

Hazánkban a Kormány 2008 szeptemberében terjesztett be egy törvényjavaslatot a szerzői jogról szóló 1999. LXXVI. törvény módosításáról a fájlcserélők ellen. E törvényjavaslat elfogadva a ius ex iniuria non procreatur elvet a felhasználók büntetni fenyegetésével igyekezett volna visszaszorítani a fájlcserét.

„6. § (8) Az (1), a (4) és az (5) bekezdésben szabályozott esetekben nem minősül szabad felhasználásnak a többszörözés, ha a *szabad felhasználás kedvezményezettje tudja*, vagy az adott helyzetben általában elvárható gondosság mellett tudnia kellene, hogy a többszörözés *nem jogszerűen létrejött műpéldányról vagy a nyilvánossághoz nem jogszerűen közvetített műről történik*."[7]

Az Országgyűlés ezt a módosító javaslatot nem fogadta el. A javaslat szándéka és iránya egyértelmű, ám elfogadása végeláthatatlan vitát eredményezett volna, a fenti indokolással.

[5] Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól („Elektronikus kereskedelemről szóló irányelv"). HL L 178. szám

[6] Dósa I. – Polyák G.: Informatikai jogi kézikönyv. KJK-Kerszöv, 2004. 141. o.

[7] T/6374. Törvényjavaslat

A Pirate Bay-per lefolyása, kérdései

A per megértéséhez tekintsük át a fájlcserélés technológiáját. A Pirate Bay hálózat a torrent-technológián alapult. A torrent-technológiát Bram Cohen találta ki 2001-ben[8]. Az egy szerverhez kapcsolódó felhasználók egymással osztják meg a különböző fájlszeleteket. A technológia egyébiránt annyira jól használható, hogy nemcsak online játékok, hanem online televíziók elérése is lehetséges a technológia segítségével (SopCast, TvAnts, TvuPlayer-kliensek, sőt a Brüsszelből sugárzott EU TV is torrent-technológián alapszik).

A torrent szerverek (seed-servers) nem tárolnak fájlokat, hanem a tárolt fájok jegyzékét, és azok elérésének útját (linkjét). A felhasználók a fájl nevére kattintva érik el azt a felhasználót, akinél a fájl egésze van, továbbá azokat a felhasználókat, akiknél az egész fájl egy-egy szeletkéje, részlete található. Az egész fájlt a technológia fájlszeletekre bontja, majd ezeket a fájlszeleket szétosztja a felhasználók között. Majd a felhasználók a letöltött fájlszeleteket egymás között osztják meg, így a fájl összeáll egésznek. A torrent fájlok tartalma nem azonos a jogi védelmet élvező szerzői alkotással. Legfeljebb a fájlok elnevezése, információs címkéje vagy egy kisegítő .nfo fájl utalhat arra, hogy a fájlszeletke mely szerzői alkotás része, mely szerzői alkotássá fog összeállni. A feltöltőnek (seedernek) nem is szükséges a letöltés utolsó mozzanatáig jelen lenni a hálózatban. Ha a fájl egészét a felhasználók között a program szétosztotta, ezt követően a feltöltő kiszállhat, és a letöltők egymástól szerzik be a még hiányzó fájlokat. Így válik például a televíziós adások vételekor a videófolyam stabillá. A torrent szervereken tehát nem magukat a fájlokat, hanem csupán egy linkhalmazt – az elérhető weboldalak címét – találjuk.

A Pirate Bay szolgáltatás 2003 novemberében indult Svédországban, és az egyik legismertebbé nőtte ki magát. A per, amely a Pirate Bay (fájlmegosztó) hálózat üzemeltetői ellen indult, precedens értékű. Részben azért, hogy a fájlmegosztó hálózatok jogi felelőssége kimondásra kerüljön. Részben az egyik legnagyobb fájlmegosztó szolgáltatás szerepelt célkeresztben. A Pirate Bay napi forgalma 15-25 millió (!) felhasználó aktivitása.

Az Amerikai Filmgyártók Szövetsége (Motion Picture Association of America, MPAA) már többször próbálkozott a Pirate Bay-t (is) eljárás alá vonni. Maguk mögé állították az amerikai kormányzatot, így, kormányzati nyomásra a svéd hatóságok nyomozást indítottak a Pirate Bay ellen. 2006 márciusában a svéd hatóságok ellenőrzést tartottak a Rix Port80 internetszolgáltatónál, amelynek hálózatán volt elérhető a fájlcsere szolgáltatás. A 20 hónapig tartó nyomozást követően 2008. január legvégén a svéd ügyészség vádat emelt, majd a büntető- és polgári eljárás 2009. február közepén indult. 2009. április 17-én hirdették ki az elsőfokú ítéletet.

[8] Gardner, S. – Krug, K.: BitTorrent For Dummies. Wiley Publishing Inc., Indianapolis, 2006. 17. o.

A négy vádlottat a svéd Szerzői Jogi törvény (1960:729) 1., 2., 46., 53., 57 szakaszainak a svéd Büntető törvénykönyv (1999:36) 23. fejezet 4. szakasza szerinti közreműködőként (mi fogalmaink szerint talán bűnsegédként) vonták felelősségre.[9] Első fokon egy év szabadságvesztésre és összesen (árfolyamtól függően) mintegy 800 millió forintos kártérítés megfizetésére kötelezték őket. A megítélt pénzbüntetéseket filmforgalmazók kártalanítására kell felhasználni.[10]

Az ítélet ellen a vádlottak az ügyben eljáró ügyész és bíró elfogultsága miatt fellebbeztek, azok szerzői jogi társaságokban vállalt tagsága, illetve tisztsége miatt. A vádlottak emellett nemzetközi fórumokhoz is fordultak.

Az ítélethirdetés másnapján svéd városokban tüntetések voltak. Néhány nappal később a Pirate Bay szerverei más országból újraindultak, és azokat továbbra is 15-25 milliónyi felhasználó látogatja.

Mind a mai napig megosztott és néhol indulatos vélemények kísérik a pert és az ítéletet, a svéd alkotmány szabadságjogainak idézésétől az amerikai nyomásgyakorlás elítélésén át a fájlcsere kérdéséig.

A per tanulságai

A per a fájlcserélő szolgáltatást üzemeltetők ellen indult, és a nem a felhasználók ellen, szemben a korábbi Egyesült Államokbeli perekkel, ahol kifejezetten a felhasználók ellen indultak eljárások. A felhasználók jogi felelősségre vonása Svédországban is aggályos volt, mert tisztázatlan volt, hogy a szerzői alkotás egészből kiszakított részlete önmagában már szerzői alkotásnak minősül-e. Az ítélet szerint a fájlcserében közreműködő letöltők is a bűncselekmény tettesei és részesei a svéd jog szerint.

Ma Magyarországon nem találnánk azt a jogi formulát, amely alapján a letöltők büntetőjogi felelőssége fennállna. A magyar Btk. ma mereven elválasztja a tettességet és a részességet egymástól. A gyakorlatban, de az elméleti felfogásokban[11] is közös a tettesek esetében a tényállási elemek megvalósításának szükségessége.

[9] A svéd szerzői jogi törvény elérhető:
http://www.sweden.gov.se/content/1/c6/01/51/95/20edd6df.pdf; [2010. márc. 10.]

[10] Sony Music Entertainment (Sweden) 41 467 euro; Universal Music Aktiebolag 73 782 euro; Playground Music Scandinavia AB 28 159 euro; Bonnier Amigo Music Group AB 4 290 euro; EMI Music Sweden Aktiebolag 162 988 euro; Warner Music Sweden Aktiebolag 146 484 euro; Yellow Bird Films AB 3 150 000 svéd korona; Nordisk Film Valby A/S 225 000 svéd korona; Warner Bros Entertainment Inc. 2 484 225 svéd korona; Columbia Pictures Industries Inc. 5 579 325 svéd korona, Twentieth Century Fox Film Corporation 10 822 500 svéd korona; Warner Bros. Entertainment Inc. 414 000 svéd korona; Twentieth Century Fox Film Corporation és Mars Media Meteiligungs GmbH & Co. Film Productions 4 495 950 svéd korona.

[11] Mészáros Á.: A bűncselekmény elkövetői. Elméleti és gyakorlati kérdések. Ad-Librum, 2008. 83-87. o.

A részesek tevékenysége csak mint járulékos tevékenység minősíthető. Így, ha nem állapítható meg alapbűncselekmény, jelesül a fájlcsere keretében történő letöltés, amit a magyar Btk. 329/A.§-a pönalizál, akkor részesi tevékenység sem állapítható meg. Ezzel szemben a feltöltők büntetőjogi felelőssége vitán felül áll, hiszen ők a szerző hozzájárulása nélkül osztják meg a digitalizált szerzői alkotásokat.

Az ítélet adoptálható tanulságai

1. Jogharmonizációs törekvés az EU-s országok között a szerzői jogi törvényekben, és azok értelmezésében a ius ex iniuria non procreatur elv alapján.

2. Nemzetközi és nemzeti együttműködés[12] a szerzői jogi jogsértések üldözésében. Ha az adott országban jogsértő tevékenységet folytató szerver egy másik ország szerverén megjelenhet, akkor a jogi üldözés szinte értelmét veszti. Még mindig szükséges a jogalkalmazók felkészítése, továbbképzése.[13]

3. Cél az illegális feltöltések megakadályozása. Ha a feltöltéshez a szerző nem járult hozzá, akkor a szerzői alkotásnak a szerző engedélye nélküli terjesztése Szjt.-ben írt tilalmára tekintettel, a Btk. 329/A. §-a alkalmazható.

4. A letöltés bár jogellenes (jogtalanságból jog nem származhat), de a fájlszeletek nem képezik a szerzői mű egészét. Bizonyítani az adathordozón (winchester, külső merevlemez, pendrive-okon stb.) levő szerzői mű esetében a letöltés beismerése által lehet.

5. De lege ferenda javaslat. A feltöltések visszaszorításának másik lehetősége a fájlcserét üzemeltetők felelősségének – vitán felül álló – megteremtése. Ám a magyar büntető törvénykönyvben több delictum sui generis tényállás található. Így de lege ferenda a Btk. 329/A. §-ának olyan sui generis bűnsegédi alakja nyerhetne szabályozást, amely esetében a szerzői jogsértések bűnsegédeinek (esetleg más részeseinek) büntetőjogi felelőssége megteremthető.

[12] Parti K.: Gyermekpornográfia az interneten. Bíbor Kiadó, 2009. 205. o.
[13] Parti K.: i.m. 2009. 207-208. o.; Nagy Z.: Az informatika és a büntetőjog. Magyar Jog 38. 1991/1. szám, 21-26. o.

Kerekasztal-beszélgetés az online terrorizmusról[1]

Az online terrorizmus kerekasztal-beszélgetésre az OKRI 50. évfordulója keretében megrendezett, Online biztonság című tematikus hónap keretében került sor, 2010. február 10-én. A kerekasztal résztvevői: *Szádeczky Tamás*, CISA, adatvédelmi szakértő, Adatvédelmi Biztos Irodája, tanársegéd, Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, valamint *dr. Balogh Zsolt*, tanszékvezető, egyetemi docens, Pécsi Tudományegyetem ÁJK Infokommunikációs és Jogi Tanszék voltak. A beszélgetés moderátora *dr. Szabó Imre*, az OKRI tudományos segédmunkatársa volt.

Az Interneten megvalósuló terrorista tevékenység és határterületei

Szabó Imre: Az informatikai terrorizmus mint önálló kategória elterjedése a büntető jogirodalomban a 9/11 utáni időszakra tehető. A terrorcselekmény és annak eszközcselekményeiként meghatározott bűncselekmények közötti alapvető különbség a cselekmény motívumában, illetőleg célzatában ragadható meg. A terrorcselekménynél ez a célzat politikai motivációból fakad, míg egyéb esetben a motiváció többnyire az elkövető személyéhez, személyiségéből fakadó igényeihez kötődik. Az informatikai terrorizmus célja az, hogy a társadalom fenyegetettségérzetének szüntelen gerjesztésével az állam cselekvőképességébe vetett bizalmat lerombolja, és ilyen módon valóságosan is aláássa az állam képességét arra, hogy az események felett kontrollt gyakoroljon (kormányzati politika befolyásolása, kormányzat kényszerítése, civil lakosság fenyegetése).

Az informatikai terrorizmus két határterületét az informatikai bűncselekmények köre, illetőleg az informatikai hadviselés körébe tartozó magatartások képezik. Ha az informatikai bűncselekményekhez a terrorizmushoz kapcsolódó célzat is társul, informatikai terrorizmusról beszélhetünk. Az informatikai hadviselést pedig az különbözteti meg az informatikai terrorizmustól, hogy a háborúban tilos lakosság ellen erőszakot alkalmazni, fosztogatni, tilos a lakosság sérelmét okozó cselekményt elkövetni, míg a terrorizmus célpontja elsődlegesen pont a civil lakosság.

Az informatikai terrorizmus három fő fejlődési iránya különböztethető meg: informatikai terrorizmus mint a rombolás, pusztítás eszköze (*weapon of mass destruction*); mint a tömeges zavarkeltés eszköze (*weapon of mass distraction*); és mint a társadalmi bizalom megdöntésének eszközei (*weapon of mass disruption*).[2]

---

[1] A beszámolót készítette Parti Katalin

[2] Brenner, S. W.: Cybercrime, Cyberterrorism and Cyberwarfare. In: International Review of Penal Law, Cybercrime. 2006. 77 année nouvelle série ¾ trimesters, 453–473. o.

A *tömeges pusztítás* kategóriájához azok a cselekmények tartoznak, melyek olyan számítástechnikai rendszereket érintenek, melyek közveszély előidézésére alkalmas berendezéseket kontrollálnak. Ilyen lehet például egy nukleáris erőműben zajló maghasadást szabályozó rendszer, melynek megzavarásával hasonló baleset idézhető elő, mint amilyen Csernobilban történt. Ez ugyan terrorista akciónak minősíthető, azonban nem tekinthető informatikai terrorizmusnak, hiszen a magatartás nukleáris katasztrófát idéz elő, és nem informatikai katasztrófát. Emiatt nem nevezzük például mechanikai terrorizmusnak az autóban elhelyezett pokolgépekkel végrehajtott merényleteket sem. (Vö: Vadász Viktor lopás/számítástechnikai rendszer elleni bűncselekmény-elhatárolásával.)
A *tömeges zavarkeltés* lényege a civil lakosság pszichológiai manipulációja. Ide tartozik minden magatartás, melynek célja a civil lakosság demoralizálása azáltal, hogy a lakosság a kormányzat hatékonyságába vetett hitét megingatja. Ennek a cselekménycsoportnak a sérülést, illetőleg kárt okozó magatartás inkább csak közvetett következménye lehet. A tömeges zavarkeltés valamely hagyományos módon megvalósított terrorcselekmény következményeinek a fokozására szolgál. A 9/11 esetében az emberek milliói nézték a televíziós, illetve az interneten elérhető hírműsorokat, hírcsatornákat azért, hogy megtudják, mi is történt pontosan. Ha ebben az esetben a nagyobb hírportálok honlapjait olyan címoldalakra cserélték volna fel a terroristák, melyben kitalált hírek szerepeltek volna (pl. nukleáris holokauszt Európában és Ausztráliában, Oroszország atomcsapásra készül az USA nagyobb városai ellen stb.) bekövetkezhetett volna egy másik Orson Welles-i tömeghisztéria (a *Világok harca* rádiós közvetítése miatt országszerte pánik tört ki az USÁ-ban). Ebből is adódik, hogy ezeknek a cselekményeknek nem célja a közvetlen károkozás, sokkal inkább a kormányzat elleni terror hatásának fokozása.
A *társadalmi bizalom megdöntésének* eszköztára nagyon széles. Az ilyen típusú, informatikai terrorcselekmény körébe vonható magatartások elsődleges célpontjai a kritikus infrastruktúrához kapcsolódó eszközök, szoftverek, adatbázisok (energiaellátás, közlekedés, egészségügyi informatika, e-közigazgatás, infokommunikációs szolgáltatások). A támadások célja, hogy az infrastruktúra működésébe vetett bizalom megdöntésével demoralizálja a lakosságot. A támadás az adott rendszer leállását eredményezi, és azt a látszatot kelti, hogy az állam nem képes megvédeni a társadalom működésének alapstruktúráit.

Milyen cselekmények alkotják az informatikai terrorizmust? Szükséges-e ezen cselekmények önálló kategóriaként történő kezelése?

Hans-Jörg Albrecht szerint az internetes terrorizmus nem önálló kategória, az internet csak egy újabb eszköz a terrorcselekmények megvalósítására, valamint a terrorista sejtek felépítéséhez, kapcsolattartásához. Ezzel szemben *Ulrich Sieber* szerint az internet pótolhatatlan eszközt adott a terroristák kezébe, amely megváltoztatta a terrorizmus jelentését, hiszen az online terrorcselekmények nagyobb tömegeket veszélyeztetnek, sokkal kevésbé ismert az elkövető személye és célja, nagyobb az elkövetés szervezettsége, tehát nagyobb a cselekmények társadalmi

kockázati értéke is. Ezért az informatikai terrorizmus olyan, korábban nem tapasztalt nemzetközi összefogást igényel, amely felette áll a szuverén jogrendszerek egyéni megoldásainak. Ha úgy tetszik, ez a fajta cselekmény hozzájárult az önálló európai büntetőjog fogalmának kialakulásához. Ennélfogva az informatikai terrorizmus önálló kategóriának tekinthető.[3]

Balogh Zsolt értelmezésében a világon eddig négy információs forradalom volt, az első a beszéd, a második az írás, a harmadik a könyvnyomtatás, és a negyedik, egyben legutolsó az internet-korszak, amelynek ma mi is tanúi vagyunk. Mindegyik információs forradalom magával hozott valamiféle pánikreakciót, amely egyfelől a tudásmonopólium elvesztésével, másfelől az adott médium karakterisztikájához kapcsolódó káros tartalmak terjedésével volt kapcsolatos. Ezek a félelmek az internet terjedésével is megfogalmazódnak. Az internet-korszaknak az egyik ilyen „káros" hozadéka az, hogy újabb alkalmakat teremt a bűnelkövetésre, amely természetszerűleg a terrorista akciók szervezésében is megmutatkozik. Balogh Sieber tanát osztja. Úgy gondolja, az internet nem csupán új platformot teremt a bűnelkövetéshez, hanem számos nóvum is kapcsolódik hozzá, amely a korábbi információs forradalmakra nem volt jellemző. Ilyen nóvum például az internet hálózatának decentralizáltsága, amely nem tesz lehetővé semmiféle központi szabályozást. Az internetet csak az online közösségek képesek szabályozni és a szabályokat megtartatni a közösségek tagjaival: az önszabályozás iskolájának számos példáját ismerhetjük meg az online közösségépítő fórumok, a tartalomszabályozás vagy a minősítési eljárások területén. Az elektronikus adatbázisokat éppen azért nem célszerű egyetlen központi szerverre telepíteni, mert ez a megoldás szinte online terrortámadásért kiáltana. Az internet decentralizált technológiájának kifejlesztésére eredetileg éppen azért került sor az 1950-es években, hogy ne legyen képes az ellenség egyetlen csapásával ártalmatlanná tenni a megtámadott infrastruktúrát. Balogh azonban hozzáteszi, hogy az informatikai terrorizmust nem feltétlenül büntetőjogi kategóriaként képzeli el, hiszen a büntetőjog centralizált eszközével képtelenség szabályokat alkotni rá, ahogyan képtelenség ezeket a szabályokat megtartatni is. Az informatikai terrorizmus az informatikai bűnözés egyes elemeinek terrorizmus köré való csoportosításaként is felfogható, amely egészben ugyan nem büntetendő, de elemei mind megtalálhatók a Btk. különböző tényállásaiban.

Szádeczky Tamás csak akkor értelmezi önálló kategóriaként az online terrorizmust, hogyha az online infrastruktúra ellen irányul, kizárólag online módszerekkel. Ugyanakkor nem tartja minden esetben járható útnak a büntetőjogi reagálást az online terrorizmus kezelésére. Véleménye szerint az informatikai terrorizmus az informatikai bűncselekmények tömeges, koncentrált elkövetése, tehát büntetőeljárás során a felelősség a „hagyományos" informatikai bűncselekmények alapján is megállapítható. A terrorcselekmények kapcsán nehéz meghúzni azt a határt,

[3] Lásd: Sieber, U.: International Cooperation against Terrorist Use. In: International Review of Penal Law, Cybercrime. 2006. 77 année nouvelle série 3/4 trimesters, 395–453. o.

amelynek az előkészületi cselekmények büntetendősége miatt rendkívüli jelentősége van. Szádeczky a témafelvető kérdésben a példálózó felsorolásból csak a *destruktív támadások az Interneten keresztül* kategóriát sorolja a cyberterrorizmushoz. Az informatika mint csupán az elkövetés eszköze (pl. illegális tartalmak tömeges terjesztése az interneten, az internet mint individuális kommunikációs eszköz) nem tartozik ide.

Szabó Imre *Herbert George Wells: Világok harca* c. science fiction regénye (1898) nyomán az internetet olyan új világként fogja fel, amely ha nem is pusztítja el a régit, a hagyományosat, de gyökeresen megváltoztatja azt. A régi világ csak úgy képes fennmaradni és fejlődni, ha adaptálódik az internet jellegzetességeihez. Az első tisztán online terrortámadás 2007 tavaszán történt a világon, amikor az észt kormány- és bankrendszer online infrastruktúráját támadták meg (feltehetően, ám ezidáig nem bizonyítottan orosz) hackerek, és a támadás nyomán a teljes kormányzat és bankrendszer megbénult.[4] Ennek tanulsága, hogy bár a kritikus infrastruktúrák fokozatos elektronizálása a jövőben nem kerülhető el, ezzel párhuzamosan megfelelő technikai védekezésről is gondoskodni kell.

Balogh Zsolt *Victor Hugo A párizsi Notre Dame* c. regényének *„ez elpusztítja amazt"* sorát idézve csatlakozott az előbbi gondolatmenethez. Kifejtette, hogy a technikai fejlődés determinálja az ember alkalmazkodóképességét is. Az embernek folyamatosan és egyre gyorsabban kell alkalmazkodnia a technika kihívásaihoz.

Létező veszély-e Magyarországon az informatikai terrorizmus?

Szabó Imre: A Tanács 2002/475/IB számú kerethatározata (2002. június 13.) terrorizmus elleni küzdelemről részletesen rendelkezik egyes cselekmények terrorista bűncselekménnyé nyilvánításáról. Ezt a kötelezettséget a Btk. 261.§-ában foglalt terrorcselekmény hivatott teljesíteni, ezért a kerethatározatban meghatározott – az elkövetéshez kapcsolódó – célok jórészt egyeznek a törvényi tényállás célzatával. A kerethatározat értelmében:
„Minden tagállam megteszi a szükséges intézkedéseket a nemzeti jogban bűncselekményként meghatározott azon szándékos cselekmények terrorista bűncselekményekké nyilvánítására, amelyek az elkövetés módja vagy összefüggéseik folytán egy államot vagy nemzetközi szervezetet komolyan károsíthatnak, ha azokat azzal a céllal követik el, hogy:

- *a lakosságot komolyan megfélemlítsék, vagy*
- *állami szervet vagy nemzetközi szervezetet jogellenesen arra kényszerítsenek, hogy valamely intézkedést megtegyen vagy ne tegyen meg, vagy*
- *egy állam vagy nemzetközi szervezet alapvető politikai, alkotmányos, gazdasági vagy társadalmi rendjét súlyosan megzavarják vagy lerombolják."*

A harmadik, a kerethatározatban megjelenített célzat különbözik a Btk. 261. § szerinti terrorcselekmény (1) bekezdésének c) pontjában foglalt célzattól:

[4] Lásd pl. http://www.govtech.com/dc/articles/129661

„c) más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetőleg nemzetközi szervezet működését megzavarja."

Felmerülhet a kérdés, hogy ez utóbbi célzattal megvalósított bűncselekmények esetén milyen szabályok védik a Magyar Köztársaságot, tekintettel arra, hogy a tényállás *más állam védelmét* szolgálja. A magyarázatot a Btk.-t módosító törvény miniszteri indokolása adja, mely szerint:

„Tekintettel arra, hogy a magyar állam alkotmányos rendjének megváltoztatására irányuló cselekmények a Btk. X. Fejezete szerinti állam elleni bűncselekményt valósíthatnak meg, a törvény csak a más állam alkotmányos, társadalmi vagy gazdasági rendjének megváltoztatása, illetőleg nemzetközi szervezet működésének megzavarása céljából elkövetett személy elleni erőszakos, közveszélyt okozó, illetve fegyveres bűncselekmények elkövetését minősíti terrorcselekménynek."

Ha megvizsgáljuk az állam elleni bűncselekmények körét, akkor a miniszteri indokolás alapján három bűncselekmény jöhet szóba: az alkotmányos rend erőszakos megváltoztatása (Btk. 139. §), az alkotmányos rend elleni szervezkedés (Btk. 139/A. §) és a rombolás (Btk. 142. §). Mindhárom cselekmény közös eleme, hogy a cselekmények a Magyar Köztársaság alkotmányos rendje ellen irányulnak. A miniszteri indokolás szerint az alkotmányos renden az alkotmányt és az abban foglalt elveken alapuló társadalmi viszonyokat kell érteni. Ebből levezethető, hogy az állam elleni bűncselekmények védik a Magyar Köztársaság alkotmányos, politikai, gazdasági és társadalmi rendjét is. (Némileg ellentmond ennek az értelmezésnek a terrorcselekmény tényállása, melyben az alkotmányos rend külön tényállási elemként jelenik meg, elkülönítve a társadalmi, gazdasági rendtől, mely alapján joggal lehet azt gondolni, hogy ezek különböző védendő jogi érdekek.)

Témánk szempontjából lényeges, hogy az alkotmányos rend erőszakos megváltoztatásánál az elkövetés módja az erőszak, míg a bűncselekmény célzata az alkotmányos rend megváltoztatása. A terrorcselekménynél azonban nemcsak az adott rend megváltoztatásának célzat, de annak megzavarására irányuló célzat is szerepel. Mitévő legyen a jogalkalmazó, ha a Magyar Köztársaság alkotmányos rendjének megzavarása vagy megváltoztatása céljából követnek el számítástechnikai rendszer és adatok elleni bűncselekményeket? A terrorcselekmény eszközcselekményei vonatkozásában erőszakos cselekménynek minősül ez a bűncselekmény is, azonban ettől még a cselekmény az egész Btk.-ra kiterjedően nem lesz erőszakos cselekmény. (Ugyanakkor nehéz elképzelni, hogy valaki „puccsot" hajt végre a személyi számítógépe mellől.) Ha a célzat pedig csupán a megzavarásra irányul (a tömeges zavarkeltés eszközeként (*weapon of mass distraction*) a cselekmény nem valósít meg se terrorcselekményt, se alkotmányos rend elleni cselekményt.

A rombolás célzata ugyan az alkotmányos rend megzavarása, az elkövetési magatartások (megsemmisítés, használhatatlanná tétel, rongálás) azonban szűkítik a védelmet. Mitévő legyen a jogalkalmazó, ha a kritikus informatikai infrastruktúra elleni informatikai támadás nem az előbb említett három elkövetési magatartás elkövetésével valósul meg, hanem csupán például valamely honlap (pl.

www.mo.hu) nyitóoldalán elhelyezett zavarkeltő, lejáró szöveg elhelyezésével. A cselekmény nem minősíthető rombolásnak, ugyanakkor az elkövető célzata, miszerint az állam cselekvőképességébe vetett bizalmat lerombolja, megvalósul. Ebben az esetben nem állapítható meg sem a rombolás, sem a terrorcselekmény, csupán a számítástechnikai rendszer és adatok elleni bűncselekmény.

Szádeczky Tamás szerint a terrorizmus Magyarországon ugyanúgy létező veszély, mint a váratlan légitámadás. A védelem szükséges szintjét úgy állapítjuk meg, hogy kockázatbecslést végzünk. A kockázatbecslés figyelembe veszi az előfordulás valószínűségét és a bekövetkező káresemény veszteségeit (emberi, anyagi, erkölcsi, stb.) és ez alapján ad egy mérőszámot. Például a váratlan légitámadás bekövetkezési valószínűsége nagyon alacsony, a kárérték viszont rendkívül magas (több tízezer emberélet, hatalmas anyagi kár), ezért megéri radarrendszert, légvédelmi fegyverzetet, óvóhelyeket, szirénarendszert és az ezekhez kapcsolódó adminisztratív hátteret üzemeltetni Magyarországon. A védelem szükségessége pedig nem merül fel minden konferencián. Ugyanezt a számítást kell elvégezni az informatikai terrorizmus kapcsán és felelős döntést kell hozni a védelem szükségességéről. Az informatikai terrorizmus veszélye egyébként a kritikus infrastruktúrák (pl. kormányzati rendszerek, közművek) informatikai függőségének növekedésével, valamint ezek interdependenciájának (kölcsönös függőségének) növekedésével arányosan fokozódik. A kritikus infrastruktúra-elemek interdependenciája miatt sokkal nagyobb a támadási felület és a kockázati érték, mint az internet kora előtt volt.

Milyen veszélyeket rejt magában a lehallgatás, az állampolgárok megfigyelése, egyáltalán a terrorizmus és a hozzá kapcsolódó jogszabályi változások az emberi jogok területén?

Szabó Imre: Az állam célja a biztonság garantálása érdekében a leghatékonyabb módszerek igénybe vétele. Ezzel szemben az alapvető emberi jogok jelentik a korlátot, mely jogok folyamatosan konfliktusba kerülnek a hatóságok terrorizmus elleni küzdelemben betöltött bűnmegelőzési feladataival. Ennek jó példája a 9/11 után elfogadott Patriot Act (Hazafias törvény) azon rendelkezése, mely az egyetemi és közkönyvtárakat kötelezte arra, hogy az olvasók olvasási, kölcsönzési szokásairól információt szolgáltassanak a hatóságok számára. Az informatikai adatforgalomra vonatkozó adatok szolgáltatási kötelezettségei hasonló megfontoláson alapulnak. Az Rtv. 68.§-a – bírói engedélyhez nem kötött titkos információgyűjtés keretében – lehetőséget biztosít az elektronikus hírközlő szolgáltatók által az elektronikus hírközlésről szóló 2003. évi C. törvényben foglaltaknak megfelelően megőrzött adatok bekérésére. Minden kétévi vagy ennél súlyosabb szabadságvesztéssel büntetendő, szándékos bűncselekmény felderítése érdekében adott ez a lehetőség. Ennek keretében a hírközlő szolgáltató a rendőrség rendelkezésére tudja bocsátani többek között az internet hozzáférési, internetes elektronikus levelezési, internetes telefonszolgáltatás, illetve ezek kombinációja esetén az elektronikus hírközlési szolgáltatás típusát és a szolgáltatás előfizető vagy fel-

használó általi igénybevételének dátumát, kezdő és záró időpontját, az igénybevételnél használt IP címet, felhasználói azonosítót, illetve hívószámot.
Az online marketing egyik bevált módszere, az un. *behaviour targeting*. Ennek lényege, hogy a kínált terméket eljuttassa az interneten keresztül a potenciális kereslethez, minimalizálva a reklámozás költségét. A módszer célja személyre szabott viselkedési profilok kialakítása, melyből megállapíthatóak többek között a fogyasztó szokásai, igényei, érdeklődési területei. Nagyon kifinomult informatikai módszerek vannak már arra vonatkozóan, hogy minél pontosabb profilképet kapjon a hirdető a fogyasztóról. Ennek a profilnak a lényegét a fogyasztó által igénybe vett szolgáltatások adják, pont az az információ, mely a nyomozó hatóság rendelkezésére áll szinte minden bűncselekmény felderítéséhez kapcsolódóan.
Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK Irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről rendelkezik. Az Irányelv (20) pontja kimondja, hogy az Európa Tanácsnak a számítástechnikai bűnözésről szóló 2001-es egyezményének szabályrendszere az Irányelv értelmében megőrzött adatokra is alkalmazandó. Az Irányelv 1. cikkének (1) bekezdése pedig meghatározza az Irányelv hatályát, mely szerint az adatmegőrzés az egyes tagállamok nemzeti joga által meghatározott súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából állnak rendelkezésre.
Ezek alapján a hazai szabályozásban két probléma látszik kibontakozni. Az első, hogy a súlyos bűncselekmény fogalmán az Rtv.-ben az ötévi vagy ezt meghaladó tartamú szabadságvesztéssel fenyegetett bűncselekményeket kell érteni. Ehhez képest az Rtv. az adatkérés körét túl szélesre szabja meg. Ez adott esetben felveti annak a kérdését, hogy tényleg ilyen széles körben alkalmazható ez az intézmény a hazai jogban?
A második, hogy az előfizetői, illetve a forgalomra vonatkozó adatok vonatkozásában szélesebb körben lehet alkalmazni az adatmegőrzést, tekintettel arra, hogy ezek az adatok nem tartalmaznak olyan érzékenységű személyes információkat, mint például a tartalomra vonatkozó adatok. Ez utóbbi adatkörben az alapjogi korlátozás lényegesen nagyobb. Az ET számítástechnikai bűnözésről szóló 2001-es egyezményének indokolása szerint *„A kommunikáció időpontjára, időtartamára, a kommunikáció hosszára vonatkozó forgalmi adatok kevés személyes információt tartalmaznak arról, hogy az illető mit gondol stb.. Ennél fontosabb azonban, hogy a kommunikáció célja és forrása vonatkozásában szigorúbb védelmi szabályok érvényesüljenek (pl. a meglátogatott honlap vonatkozásában). Ezeknek az adatoknak a gyűjtése, néhány szituációban, lehetőséget kínál az adott ember profiljának összeállítására érdeklődési köréről, kapcsolatairól, és társadalmi viszonyairól."*
A hazai szabályozásban a jogszabály nem tesz különbséget ezen adatok között, pedig a fenti két szempont alapján ez indokolt lenne.

Szádeczky Tamás szerint napjainkban a terrorelhárítás célja gyakran felülírja az alkotmányos alapjogokat. Ezeknek persze, a szükségesség, az arányosság és célhoz kötöttség vizsgálata mellett lehet racionális indoka is. Másrészről nem

biztos, hogy ezek a módszerek Szent Grálként használhatók a terrorizmus elleni „harcban". Gyakran aránytalanságok tapasztalhatóak. Ilyen például az, hogy a közterületi térfigyelő kamerák felvételeit csak három napig lehet megőrizni, míg a telefonos hívásadatokat egy évig, pedig mindkettő alkotmányos alapjogi korlátozást takar.

Milyen módon lehetne megvalósítani az online házkutatást? A Be. hatályos szabályai értelmezhetőek úgy, hogy az alapján lehetőség van az online házkutatás alkalmazására, vagy szükség van a szabályok módosítására?

Szabó Imre: Az információtechnológia megjelenése több jogterületet is jelentősen érintett. Ilyen például a szerzői jog területe, mely jelenleg sem tudja kezelni a szerzői művek információtechnológián alapuló hatékony többszörözését, hozzáférhetővé tételét biztosító, a korábbi piaci struktúrát felborító magatartásokat és az ezzel járó érdekveszteségeket. Az információtechnológia azonban másik oldalról veszélyt jelenthet az egyes állampolgárokra is. Tegyük fel, hogy valamely kormányzat létrehoz egy olyan kémprogramot, melynek az a funkciója, hogy ellenőrizzen meg nem határozott számítógépéken található tartalmakat, és abban az esetben, ha a paramétereinek megfelelő tartalmat talál, arról tájékoztassa a program készítőjét, ellenkező esetben semmisítse meg magát. A házkutatás intézkedés alkalmazása költséges és nem jár minden esetben eredménnyel. Egy kémprogram megírása egyszeri kiadást feltételez, további alkalmazása azonban már ingyenes. Ha a kémprogram alkalmazása eredményre vezet, a házkutatás is minden esetben eredményes lesz. Lawrence Lessig szerint ezért is fontos, hogy az Internet átláthatóságának biztosítása okán mielőbb fellépjünk az állampolgárok jogai védelme érdekében, mert különben hasonló utópisztikus helyzetekbe kerülhetünk. Az on-line házkutatás már több európai országban alkalmazott módszer.

Parti Katalin: Az USA mintájára ma már Európa számos országában lehetőség nyílik arra, hogy olyan súlyos, főként állam elleni bűncselekmények esetén, amilyen a merénylet vagy a hazaárulás, a nyomozó hatóság online házkutatással gyűjtsön adatokat a bűncselekménnyel kapcsolatban.[5] A titkos nyomozás e módszere azonban szembe megy az információs önrendelkezési jog, a privát szféra és a magánlakás sérthetetlenségéhez fűződő joggal.[6] A nyomozó hatóság számítástechnikai rendszerbe való behatolásával ugyanakkor az ügyhöz szorosan nem kapcsolódó adatokhoz is hozzájut, amely adatok sorsa tisztázatlan. A nyo-

[5] Az online házkutatás vitás kérdéseiről lásd pl. dr. Mohácsi B.: Bűnüldözési érdek kontra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. Magyar Jog 2008/12. szám 827-832 o.

[6] Hofman, M.: Die Online-Durchsuchung – staaliches „Hacken" oder zulässige Ermittlungsmaßnahme? In: Neue Zeitschrift für Strafrecht 2005, Heft 3, 121; Huber, B.: Trojaner mit Schlapphut – Heimliche Online-Durchsuchung nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz. In: Neue Zeitschrift für Verwaltungsrecht 2007, Heft 8, 880-882 o.

mozó hatóság célhoz nem kötött adatgyűjtése az internetes keresőmotorok „személyiség-felderítő" funkciójára (*behaviour targeting*) emlékeztet, amelynek nyomán a keresőmotorok profilt alkotnak a felhasználóról annak érdekében, hogy a keresést leginkább a felhasználó érdeklődési körére formázhassák. Ez a profilalkotás azonban nemcsak a keresőmotor használatát könnyíti meg a felhasználó számára, de a kéretlen reklámok célba juttatását is elősegíti. Az online házkutatást végző nyomozó hatóságok és a keresőmotorok profilalkotási funkciójának összekapcsolása talán egy kissé távoli analógia, a védett jog azonban végső soron ugyanaz: a privát szféra sérthetetlensége. Az számítástechnikai rendszer védelmére azért keletkezik alkotmányos igény, mert a felhasználó online tevékenységéből komplett személyiség-profil alkotható, és ilyen átfogó kép alkotására az internet előtt eddig egyetlen médium sem volt alkalmas önmagában.

A Magyarországon jelenleg még gyakorlatot nem képező titkos házkutatás ***Szádeczky Tamás*** szerint a Be. meglévő szabályaiból ugyan levezethető lehetne, de mivel valamely szabály analógiaként való alkalmazása alkotmányos jogok sérelme esetén tilos, ezért ez nem lehetséges. Alkotmányos jogok korlátozásánál várjuk el a jogalkotótól, hogy explicit módon meghatározza a korlátozás, tehát az online házkutatás lehetőségét és módját. Technikai szempontból szintén nem túl egyszerű a helyzet, hiszen az online házkutatás során használt eszközök fennakadnak a víruskeresőn, hacsak a gyártó le nem paktált a hatóságokkal, amire az USA és Németország hírszerzési szervei esetében erős a gyanú.

Az ügyészi szervezet és az ügyész polgári jogi felelőssége Európában

(Konferencia-beszámoló)

Az ügyészi szervezet és az ügyész polgári jogi felelőssége Európában címmel a hazai és a moldovai Legfőbb Ügyészség kétnapos konferenciát szervezett a Danubius Helia Hotelben 2010. március elején, amelyet az Európa Bizottság Bővítési Főigazgatósága Technikai Segítségnyújtási és Információs Szolgálata, a TAIEX is támogatott.

A közhatalom gyakorlásával összefüggő polgári jogi felelősség érvényesítése Európa egyes országaiban az ügyészeket érintő lényeges kérdés, ezért Magyarország magára vállalta, hogy ebben a témában konferenciát szervez.

Kovács Tamás legfőbb ügyész megnyitó előadásában felhívta a figyelmet arra, hogy *„a közhatalom gyakorlásával összefüggésben egyre több kártérítési és személyiségi jogi pert indítottak a közhatalmat gyakorló intézményekkel […] szemben. A perek számának emelkedésével természetszerűleg nőtt a kereseti követelések összege, miközben – különösen az ítélőtáblák felállításával – polarizálódott a bírói gyakorlat. […] A pereket és a kialakuló joggyakorlatot elemezve többször felmerült a nemzetközi gyakorlat megismerésének szükségessége."*

A felkért előadók és a nemzeti hozzászólások a különböző országokra jellemző modelleket mutatták be. A téma több szempontú megközelítése így lehetővé tette az egyes államok különböző megoldásainak megismerését, és felvillantotta a jövő várható közös irányait.

A legfőbb ügyész megnyitó beszéde után Tímár Anikó, a Jogi Képviseleti Osztály osztályvezető ügyésze a bevezető előadásában kitért az ügyészi szervezet, illetve az ügyész polgári jogi felelősségének elméleti és gyakorlati kérdésére Magyarországon, majd Cucz Ottó, az Európai Közösségek Elsőfokú Bíróságának bírája az Európai Unió joggyakorlatáról beszélt. A hazai előadók közül a délelőtt folyamán még Lábady Tamás, a Pécsi Ítélőtábla elnöke, illetve Lévai Ilona a Legfőbb Ügyészség Nemzetközi Képviseleti Önálló Osztály osztályvezető ügyésze kaptak szót. Előbbi dogmatikai kérdésekről beszélt, Lévai Ilona pedig a tagállamok közötti kárfelelősségről és a 2009/426/IB számú új Eurojust Határozatról.

A délelőtt folyamán, a külföldi országokon belül a portugál ügyészi kárfelelősség helyzetéről folyt a disputa.

A délutáni szekcióban Varga Zs. András, a Jogi Képviseleti Önálló Osztály ügyésze a magánjogi felelősség elméleti hátteréről tartott előadást. A külföldi példák közül pedig megismerhettük a francia, a német és török ügyészségek helyzetét.

A rendezvény másnapján a common law jogcsalád és az Orosz Föderáció megoldásairól hallhattunk, valamint a szerb, illetve az ukrán szakemberek szóltak hozzá a témához.

A tanácskozás Tímár Anikó összefoglaló megjegyzéseivel zárult.

A konferencia előadásait az Ügyészek Lapja 3. számában közöljük.

MISKOLCZI BARNA[1]

Aktuális kérdések az Európai Ügyészségről

Ez év februárjában a Francia Köztársaság Semmítőszéke konferenciát szervezett az Európai Ügyészség jelenlegi helyzetéről és fejlődésének perspektíváiról. A konferencián dr. Farkas Ákos professzor jóvoltából, a legfőbb ügyész úr hozzájárulásával, mint a Magyar Jogászok az Európai Büntetőjogért Egyesület tagja vehettem részt. Az alábbiakban a konferencia tanulságait igyekszem felvázolni. Túlnyomórészt terjedelmi okokból elsősorban a gyakorlat szempontjából fontos aspektusokra helyezem a hangsúlyt. Európai Ügyészség természetesen még nincs, de reményeim szerint sikerül bemutatnom, hogy az európai büntetőjog fejlődése (melynek a már mai szemmel is belátható, gyökeres változást hozó jövőbeli eredményei közül a legközelebbinek éppen az Európai Ügyészség felállítása tűnik) olyan szintre ért, ami már a ma jogalkalmazóira is feladatokat ró.

A konferencia előadói a fejlődésnek kizárólag a jelenkori szakaszáról szándékoztak egyfajta állapotjelentést adni. A történeti előzmények, az Európai Ügyészség létjogosultságát igazoló tényezők, illetve az, hogy miért is van szükség Európai Ügyészségre, most nem kerültek részletes tárgyalásra, hisz a résztvevőket már annak tudatában választották ki és hívták meg, hogy ezekkel tisztában vannak. Ezért szükségét érzem annak, hogy pár szóban ismertessem az ezzel kapcsolatos legfontosabb összefüggéseket.

Az európai ügyészség ideája abból a felismerésből eredeztethető, hogy az Európai Közösség saját pénzügyi érdekeinek büntetőjogi védelme az ezzel foglalkozó konferenciák és az első szakirodalmi fejtegetések idején (ez nagyjából az 1995-öt közvetlenül megelőző időszak volt) lényegében nem volt biztosítható. Sőt, nemcsak hogy nem volt biztosítható, de a büntetőjog fejlődése sem az első, sem a harmadik pillérben nem mutatott fel olyan perspektívákat, amelyekből a helyzet gyökeres változására lehetett volna következtetni. Az európai igazságügyi térség fragmentált volt, a harmadik pilléres igazságügyi együttműködés – leszámítva néhány kétoldalú szerződést – lényegében egy régi (1959-ben aláírt, ráadásul nem is uniós) egyezmény, a Strasbourgi Európai Bűnügyi Jogsegélyegyezmény alapján működött. A jogsegélyi ügyintézés elképzelhetetlenül lassú, színvonala pedig a legnagyobb jóindulattal is csupán változó volt. Ami azonban még nagyobb baj, hogy nem látszott olyan kibontakozási lehetőség, ami a nemzetközi együttműködést eléggé hatékonnyá tette volna. Bár már ekkor felmerült, hogy a nemzetközi bűnügyi jogsegélyi ügyintézés alapvetően a nemzetközi közjog talaján álló rendszere túlságosan nehézkes, a kölcsönös elismerés elvén alapuló együttműködés első európai terméke, az európai elfogatóparancs ötlete csak 2002-ben vezetett konkrét jogi normához. Még ha elfogadható alternatívát jelentett is a

[1] Miskolczi B., ügyész, Legfőbb Ügyészség

kölcsönös elismerés elvén alapuló együttműködés a bűnügyi jogsegélyhez képest, akkor sem lett volna azonban elegendő. Az igazi hatékonysághoz több kellett volna: olyan igazságügyi rendszer, amely a tagállamihoz hasonló módon, és legalább ugyanazon a színvonalon képes fellépni a közösségi jogtárgy védelme érdekében, leküzdve az eltérő büntetőjogi rendszerekből eredő különbségeket, a szuverenitásból fakadó problémákat, a nyelvi akadályokat stb.

A hagyományos bűnügyi jogsegély intézménye tehát elavult és egyúttal fejlődésképtelen volt, a kölcsönös elismerés nyújtotta lehetőségek kiaknázása pedig konkrét jogszabályban még nem öltött testet, és önmagában amúgy is elégtelen lett volna a problémák kezelésére.

A bűnügyi együttműködés területén (ami ekkor kizárólagosan az "európai büntetőjog" képlékeny fogalmának eljárási részét képezte) a kilátások nem voltak túl fényesek. Ami az anyagi jogot illeti, az európai büntetőjogi jogfejlődés legfontosabb eredménye a harmadik pillérből jött. 1995-ben fogadták el az Európai Közösségek pénzügyi érdekeinek védelméről szóló egyezményt (a továbbiakban: PIF-egyezmény). A PIF-egyezmény (és kiegészítő jegyzőkönyvei) legfontosabb vívmánya az volt, hogy megalkotta az EK pénzügyi érdekeit sértő csalások fogalmát, és előírta, hogy ezeket a tagállamoknak ugyanúgy kell üldözniük, mint a saját pénzügyi érdekeiket sértő csalásokat. Az egyezmény egyértelműen büntetőjogi jellegű volt, s mint ilyen, ugródeszkául szolgált egy sor első pilléres vívmányhoz is. Ezek sorában nagy jelentősége van az EK pénzügyi érdekeinek védelméről szóló 2988/1995 EK, Euratom rendeletnek, amely kifejezetten adminisztratív jellegű ugyan, de preambulumában megfogalmazott egyik célja egy egységes jogi keret biztosítása az EK pénzügyi érdekeit sértő *csalások* ellen. 1996-ban, az Európai Közösségekről szóló Szerződés 280. Cikke alapján, a Tanács 2185/1996/EK, Euratom rendeletével a csalások elleni közösségi küzdelem adminisztratív nyomozati feladatait az Európai Bizottságra ruházta, amely az 1999/352/EK, ESZAK, Euratom határozattal ennek végrehajtására létrehozta a nyomozásai végrehajtása során független szervezetét, az Európai Csalás elleni Hivatalt (OLAF).

Számtalan vélemény és álláspont ütközött már, számtalan vita alakult ki arról, hogy az említett első pilléres eszközök és szervezetek milyen kapcsolatban állnak a büntetőjoggal, illetve –különösen az OLAF – milyen jogokkal rendelkezhetnek a tagállami büntetőeljárásokban. A jogalkalmazók kevés támpontra leltek az uniós jogban. Bár első pillantásra az EKSZ 280. Cikke 4. bekezdése, továbbá a 2185/1996/EK, Euratom rendelet 1. cikke egyértelmű abban a tekintetben, hogy a közösségi intézkedések nem érinthetik a nemzeti büntetőjogot. Az 1999/352/EK, ESZAK, Euratom határozat ("OLAF-határozat") 2. cikke szerint is az OLAF "adminisztratív nyomozó hatóság", mégis, az említett uniós jogszabályok szóhasználata szerint a küzdelem az ún. "szabálytalanságok" ("irregularities"), és az azokon belüli részhalmazként a "csalások" ("fraud") ellen folyik; aminthogy az OLAF is "csalás elleni" hatóság. A csalás pedig minden tagállamban bűncselekmény. Megindult tehát a büntetőjogi gondolkodás beszivárgása

a közösségi jog szférájába, ennek folyományaként pedig a közösségi jog kezdetben halkan, majd egyre erőteljesebben zörgette a nemzeti büntetőjog ajtaját. Hosszan tartó erjedési folyamat vette kezdetét, amelyből a luxemburgi Európai Bíróság jogfejlesztő tevékenysége is jócskán kivette a részét. Már a Lisszaboni Szerződés hatályba lépése előtt sem tudott a nemzeti büntetőjog teljes egészében elzárkózni a közösségi hatások elől, az OLAF például csalásellenes küzdelmében ma már a tagállamok túlnyomó részének igazságügyi hatóságaival akár folyamatban lévő büntetőeljárásokban is együttműködhet.

A folyamat egyenlőre megállíthatatlannak és visszafordíthatatlannak tűnik, ha pedig ez így van, akkor a közösségi büntetőjogi jogfejlődés egyik végpontja valószínűleg az Európai Ügyészség lesz. A Francia Semmítőszék által most megrendezett konferencia e következtetést mind a tudomány, mind pedig a gyakorlat szempontjából elemezni kívánta. Ehhez olyan jeles előadók részvételét sikerült biztosítani, mint az Európai Ügyészség gondolatának első megfogalmazója, Mireille Delmas-Marty és John Vervaelle professzor, az Utrechti Egyetem tanára, sok kiváló elméleti munka szerzője. A gyakorlat képviselői közül jelen volt a Francia Semmítőszék melletti Legfőbb Ügyészség vezetője, a luxemburgi Európai Bíróság Főügyésze, a spanyol legfőbb ügyész, a lengyel Legfelsőbb Bíróság elnöke, a teljesség igénye nélkül. Előadást tartott Jacques Barrot, az Európai Bizottság (előző nap még hivatalban lévő) volt alelnöke, az Eurojust alelnöke, és az OLAF több magasrangú vezetője. A teljesnek aligha nevezhető enumeráció végén ki kell emelnem Michèle Alliot-Marie jelenlegi és Robert Badinter volt igazságügyi minisztert és szenátort, akik mindketten érdemi előadást tartottak.

Az Európai Ügyészségről általában

Ma már aligha van olyan, az európai büntetőjoggal kapcsolatos szakirodalmi vagy tudományos mű vagy előadás, ami a fejlődés lehetséges további irányai között ne említené meg az Európai Ügyész intézményét. Az Európai Ügyészség gondolata tehát kellőképpen beleivódott a szakmai és tudományos köztudatba. Azt azonban jóval kevesebben látják tisztán, hogy mi is lenne valójában az EU ügyész. Ez a felelős a kollégák részéről leggyakrabban elhangzó kérdésért: milyen pluszt hozna egy ilyen intézmény létrejötte a már meglévő együttműködési formákhoz képest?

Ez a kérdés magában foglalja a leggyakoribb félreértést is: az EU ügyész ugyanis elsősorban nem egy új együttműködési fórum lenne. Létét legalább három tényező együttesen igazolja: a nem tagállami jogtárgy védelme, a specializáció és persze ide tartozik az együttműködés is, ám nem a megszokott formában, hisz az EU Ügyészség ennek a fogalomnak is új jelentést ad.

Az Európai Közösségek (Európai Unió) létrejöttével új vadászterület nyílt a bűncselekmények elkövetői (elsősorban a gazdasági bűnözők) számára. Ők felismerték, hogy bűncselekmények elkövetésére az EU különösen jó terep, mivel legalább

két jelentős támadási felületet hordoz: rendelkezik saját költségvetéssel és rendelkezik egy sajátos működési struktúrával. Mindkettő alkalmat nyújt a jogtalan nyerészkedésre. Emellett – számukra külön bónuszként – azt is felismerték, hogy a cselekményeik gyakorta következmények nélkül maradnak. Ennek oka pedig egyfelől éppen az, hogy ezek a cselekmények sajátos, nem tagállami jogi tárgyat sértenek (költségvetés, vagy az Unió működése), amelyek elbírálásánál a tagállami hatóságok hirtelen elbizonytalanodnak; másfelől pedig az, hogy sok esetben e cselekmények határon átnyúló jellegűek, és a hatóságok közötti nemzetközi együttműködés rendkívül nehézkes.

Az EU költségvetését sértő cselekmények a költségvetés kiadási oldalát sértő csalások (az egyszerűség kedvéért: szubvenciós csalások), és a bevételi oldali csalások (a vámra, az áfára, a mezőgazdasági illetékre és a cukorlefölözésre elkövetett csalások). A csalásokat elősegítő, megkönnyítő tényezők közé tartozik a korrupció, gyakori kísérőjelensége pedig a pénzmosás.

A közösségi jogtárgyak védelme a tagállamokban eltérő terjedelmű és színvonalú mind a mai napig, annak ellenére, hogy a tagállamoknak asszimilációs kötelezettségük van, köszönhetően a PIF-egyezménynek és Jegyzőkönyveinek. Ez ahhoz a nem kívánt következményhez vezet, hogy bizonyos országokban szigorúbban, máshol enyhébben büntetik az ilyen cselekményeket, megint máshol egyáltalán nem (ld. Ausztria, ahol a saját pénz mosása nem bűncselekmény). Ez pedig – és itt elérkeztünk az EU-csalások elleni küzdelem igazi okához – magát az európai integrációt veszélyezteti, amelynek alapvető feltétele a belső piac egysége. Az igazi veszély nem az, hogy kevesebb pénz áll rendelkezésre, hanem az, hogy a bevételek és kiadások kijátszása elleni védelem nem mindenütt ugyanolyan erős. A tőke ugyanis nyilvánvalóan oda fog vándorolni, ahol a kisebb szigor miatt barátságosabb gazdasági klímát talál, ez pedig aláássa a piaci egyensúlyt.

Adott tehát egy szupranacionális jogtárgy, amely nem minden jogrend szerint, és nem minden büntetőkódexben volt büntethető. Az ezt sértő bűncselekmények elbírálásának egységessége tehát nem biztosított, ugyanakkor – éppen a szupranacionális jelleg miatt – a tagállamok idegenkednek is a nemzeti igazságszolgáltatást bevetni ellenük. Az EU Ügyészség létrehozásának egyik fő oka éppen az, hogy az Ügyészség kiküszöbölné a nem nemzeti jogi tárgy miatti bizonytalanságot és bizalmatlanságot, illetve egységes eljárást és elbírálást biztosítana a tagállamonként eltérő igazságszolgáltatási rendszerekben.

Ez egyben megnyugtathatja a tagállami szuverenitás csorbulása miatt aggodalmaskodókat: az EU ügyész szupranacionális jogi tárgyat védelmez, működése a tagállami *ius puniendit* nem érinti.

A szupranacionális jogtárgy védelme speciális ismereteket is igényel. Nem is lehet ez másként, hiszen az Unió létrejötte (az alapító tagállamok számára) és a csatlakozások ablakot nyitottak a közösségi jogra, (egyes Btk.-beli keretténállások háttérjoga ma már nem a nemzeti, hanem az uniós jog), ami irdatlan mennyiségű jogszabály és – ami legalább ennyire fontos – az Európai Bíróság határozatainak

ismeretét kívánja meg a kollégáinktól. Ugyan Magyarországon ma még nem jellemző a közösségi jogon alapuló védekezés, de hamarosan eljönnek a szakosodott védőügyvédek napjai is. Jogos igény ezért, hogy a szupranacionális jogtárgyak védelmét (többek között a közösségi verseny-, a kereskedelmi-, vagy éppen az agrárpolitika joganyagát) az azokat mélységében ismerő ügyész egységes elvek mentén, hatékonyan biztosítsa.

Mára az is nyilvánvalóvá vált, hogy a közösségi jogtárgy hatékony védelmének a specializáció nehézségei mellett a másik jelentős gátja a nemzetközi együttműködés nehézkessége. Valamennyi ügyész tapasztalhatta már a napi munkája során, hogy az eredményes nyomozásokat miként akasztja meg a jogsegélyi ügyintézés támasztotta "szűk keresztmetszet". Az eddigi próbálkozások, amelyek a gyorsaság növelésére irányultak, csak csekély eredményt hoztak. Az Európai Ügyészség a hagyományos jogsegélyi együttműködés kiiktatását is elérheti. Az *európai területi elv* biztosítaná neki, hogy az egyes tagállami nyomozó hatóságokkal ne jogsegély útján, hanem ahhoz hasonlatosan kommunikálhasson, ahogy saját állama nyomozóival teszi. Ez természetesen a bizonyítékok megszerzésére is vonatkozik.

A konferencia legfontosabb tanulságai

A konferencián két nap alatt nagyon sok jeles előadás hangzott el, amelyek ismertetése messze meghaladná a jelen írás kereteit. Ezért csak arra teszek kísérletet, hogy a legégetőbb kérdések számbavételét elvégezzem. Ennek keretében az EU Ügyészség hatáskörét, létrehozásának bizonyos elméleti kérdéseit és személyi feltételeit, valamint a tagállamok, és azok igazságügyi hatóságai által elvégzendő legfontosabb feladatokat emelem ki.

Bár a nemzetközi szakirodalmat olvasva nem hat a meglepetés erejével, de most újabb megerősítést nyert, hogy az EU ügyész *szükségességét* illetően az elmélet és a gyakorlat képviselői között konszenzus mutatkozik. Ami az EU Ügyészség felállításának politikai feltételeit illeti, ezek akadályt jelenthetnek, amint arra a szkeptikusabb vélemények rámutatnak. Látható azonban, hogy a fejlődést bizonyos önmozgások jellemzik: az EU interszektorális kooperációs mechanizmusként indult, ma pedig már a transznacionális és szupranacionális jogi együttműködés kérdései vannak napirenden. A folyamatot felgyorsítja a Lisszaboni Szerződés és a Stockholmi Program. Mindkettő kifejezetten szól az EU ügyészről. A lisszaboni reform szerint egységes szerkezetbe foglalt Európai Unió működéséről szóló Szerződés a 86. cikkében megnyitja az utat az EU ügyész megerősített együttműködés keretében történő létrehozása előtt, az Unió pénzügyi érdekeinek védelmében. A bel- és igazságügyi együttműködés (vagyis a volt 3. pillér) irányát 2010. és 2014. közt kijelölni hivatott Stockholmi Program 3.1.1 pontja említi az Ügyészség felállítását, mint lehetséges megoldást. Kétségtelen, hogy az elkövetkező időszak elnökségi programjai (s ez alól a magyar sem lehet kivétel) a korrupció és a csalás elleni harcot prioritássá, de legalábbis frekventált témává fogják tenni.

Ami a szkeptikus véleményeket illeti, az EU ügyész szükségességének hangsúlyozása mellett ezek a megvalósítás lehetséges nehézségeire mutatnak rá. Az új intézménynek ugyanis jogi tradíciókra kell épülnie, amelyek azonban tagállamonként eltérőek. A jogi tradíciók, a jogi kultúra alapjai azonban nem összeegyeztethetetlenek az EU Ügyészséggel. Jelentős akadály, hogy a létrehozás körül alapjogok ütközése várható, melyek közül talán a legérzékenyebb az integrált büntetőjogi térség biztosította biztonsághoz való jog és a szuverenitás kollíziója. Felmerülhetnek kompatibilitási problémák is: egyelőre megoldatlan az EU Ügyészség és az Eurojust, illetve az OLAF jövőbeli viszonyrendszere.

Az EU Ügyészséget nem egy állam, hanem államok közössége hozhatja létre a közös jogi kultúra alapelvei mentén. Ezen alapelvek közössé tétele jelentős erőfeszítéseket kíván a tagállamoktól, amelyek csak a tapasztalatok kicserélése, az egymástól való tanulás útján lesznek képesek haladást elérni. Hubert Haenel, a Szenátus EU-ügyi Bizottságának elnöke szerint a megvalósítás útján az első lépés a már meglévő büntetőjogi vívmányok mind teljesebb implementációja és alkalmazása.

Ez a kijelentés némi magyarázatot igényel. Az implementáció sohasem egy jogszabály kihirdetésével, hanem az implementált norma eredeti jelentésének megfelelő jogalkalmazással fejeződik be. (Bizonyos esetekben még a belső jogi változtatás sem szükséges az implementációhoz, más esetekben a törvényben való kihirdetés sem elegendő.) Viszont az uniós vívmányok helyes implementálása sem csak az egységes jogalkalmazás biztosítása miatt fontos: álláspontom szerint ezek a jövőbeli együttműködés legfontosabb jogelveinek *proving ground*-jai ("tesztpályái"). Példaként említhető a Schengen-II egyezmény és a 2000-es Egyezmény az Európai Unió tagállamai közötti bűnügyi jogsegélyről (pl. a közvetlen ügyintézés és a közös nyomozócsoportok tekintetében), az európai elfogatóparancsról szóló kerethatározat (a határozatok kölcsönös elismerése tekintetében) stb.

Az EU Ügyészség hatásköre

A legvalószínűbb forgatókönyv szerint az EU Ügyészség kizárólag az EU-t érintő (közösségi) jogi tárgyakat fenyegető bűncselekmények esetében járna el. Az azonban még nem világos, hogy melyek tartoznának e körbe. Kézenfekvő, hogy a Corpus Iuris "eurobűncselekményei" tartozzanak a hatáskörébe, de sokan – köztük magam is – óvatosabban húznák meg a határt.

Ez utóbbi elgondolás szerint – legalábbis az első időszakban – kizárólag az Unió pénzügyi érdekeit sértő bűncselekmények képeznék az Ügyészség hatáskörét, abban az értelemben, ahogyan azt az 1995-ös, az Európai Közösségek pénzügyi érdekeinek védelméről szóló egyezmény csalás-definíciója tartalmazza. Mivel az ott tárgyalt bűncselekmények az EK pénzügyi érdekei mellett tagállami jogi tárgyat aligha sértenek (bár ez a megállapítás az áfa-csalásokra nem igaz), ez a

forgatókönyv alkalmas lenne arra, hogy a szuverenitás féltésére alapozott tagállami ellenkezés vitorlájából kifogja a szelet. Igaz, hogy ez a megközelítés viszont kitenné magát egy másik irányú politikai jellegű nyomásnak, amely az összes súlyos, transznacionális jellegű bűncselekményt az EU Ügyészség hatáskörébe utalna (pl. terrorizmus, EU-n belüli korrupció, euróhamisítás stb.) Mindazonáltal a szűk hatáskörrel elkezdett munka tapasztalatai alapján a hatáskört a későbbiekben ki is lehet majd terjeszteni.

EU Ügyészség nélkül – állítják az előadók, köztük Jacques Barrot, az Európai Bizottság volt alelnöke – folytatódna az a trend, hogy a tagállami ügyészek – megfelelő uniós jogi képzettség nélkül – vagy eleve figyelmen kívül hagyják a transznacionális elemeket és csak a bűncselekmények nemzeti vonatkozásaira koncentrálnak, vagy pedig hiányos ismereteikkel, a tagállami uniós büntetőpolitika iránymutatásait is nélkülözve kényszerülnek eljárni az egyre bonyolultabb uniós bűnügyekben. Hatékonyságra számítani ilyen feltételekkel természetesen nem lehet. Minderre tekintettel az EU igazságügyi széttagoltsága a továbbiakban már nem indokolható.

Az EU Ügyészség létrejöttének főbb kérdései

Az EU Ügyészség létrehozását sem a Stockholmi Program, sem az Európai Unió működéséről szóló Egyezmény nem írja elő. Az említett dokumentumok csupán lehetővé teszik a létrehozását, azzal, hogy az Európai Ügyészség az Eurojustból jöhet létre uniós aktussal. Erről a kitételről részletesebb eligazítást egyik dokumentum sem tartalmaz, ami bizonytalanságot okoz. A két szervezet ugyanis jelentős különbségeket mutat. Az Eurojust elsősorban a tagállamok hatóságai közötti *kooperációt* elősegítő szervezet. Az EU Ügyészség feladata ugyanakkor a magyar ügyészségéhez hasonló lenne, és magába foglalná a *nyomozás* irányítását és felügyeletét, a *vádemelést* és a *vád képviseletét* is. A nemzetközi kooperációt kevésbé, illetve csak újabb formájában, mert egyrészt bizonyos EU-csalásos ügyeknek nincs is nemzetközi vonatkozása (ilyen pl. a területalapú támogatásos ügyek egy része), másrészt ha van, az EU ügyész amúgy sem kérelemmel fordulna a nemzeti hatóságokhoz valamely cselekmény teljesítése céljából, hanem utasítaná őket, határidő tűzésével.

Az eltérő feladatkörökből fakadó problémák dióhéjban az alábbiak:

Az EU Ügyészség az Eurojustból jön létre, de nem derül ki, hogy szervezetileg, vagy a személyi vonatkozások tekintetében.

Amennyiben szervezetileg, úgy ez a következőképp lehetséges: az Eurojust-tagállamok közül legalább kilenc (a megerősített együttműködés keretében) úgy dönt, hogy létrehozza az Európai Ügyészséget. Ekkor ki kell válniuk az Eurojust szervezetéből, és EU Ügyészséggé kell válniuk, űrt hagyva maguk mögött (vagyis a megerősített együttműködésben résztvevő tagállamok helye az Eurojustban betöltetlenül maradna). Amennyiben ugyanis az Eurojust szervezete

érintetlenül maradna az EU Ügyészség létrehozását követően is, akkor az Ügyészség nem "az Eurojustból" jönne létre, hanem azzal párhuzamosan, külön szervezetként.

Még kevésbé szerencsés, ha a személyi vonatkozásokat tekintve jönne létre "az Eurojustból" az Ügyészség. Ez esetben a folyamat úgy alakulna, hogy a kilenc tagállam *nemzeti tagja* hagyja ott az Eurojustot, és alakít Ügyészséget (helyük ez esetben betölthető). Kérdéses azonban, hogy a nemzetközi kooperációban bizonyára jártas nemzeti tagok az EU pénzügyi érdekeit sértő, elsősorban gazdasági bűncselekmények nyomozásának irányítására, felügyeletére, a vádemelésre is kellő kvalifikációval és naprakész tapasztalattal rendelkeznek-e. E feladataikat ők ugyanis már nem delegálhatják tovább: EU ügyészként, vagy helyettes EU ügyészként ők az "ügy urai". Itt az "Eurojustból" történő létrehozatal nem jelent mást, mint hogy a tagállam keze meg van kötve: ahelyett, hogy erre specializált ügyészét küldhetné az EU Ügyészségre, a nemzeti tagot kell delegálnia.

Az OLAF helyzete további fejtörést okoz. Adva van ugyanis egy kb. 500 fős szervezet, amelynél nagyobb tapasztalattal aligha rendelkezik bárki is az EU érdekeit sértő csalások és szabálytalanságok vizsgálata tekintetében. Ugyanakkor az új büntető igazságügyi térségben elfoglalt helye még mindig nem tisztázott, vizsgálatainak a büntető igazságügyi rendszerben történő nyomon követése sem megoldott minden tagállamban, pedig ez a feladat a 1073/1999. sz. tanácsi rendeletből következik. Mivel a pillér-rendszer eltűnt és a büntető igazságszolgáltatás területe is közösségi területté vált, nem "szentségtörés" felvetni azt a gondolatot, hogy az OLAF az EU Ügyészség nyomozó hatósága lehetne, természetesen kizárólag a közösségi jogtárgyakat sértő bűncselekmények vonatkozásában.

Mindazonáltal ma még az OLAF helyzete a büntetőeljárásokban nem teljesen tisztázott, bár a jelenlegi trendek szerint büntetőjogi szerepe várhatóan erősödni (és talán intézményesülni is) fog. Erre "ráerősít" az OLAF-nak az a – Magyarországon különösen hangsúlyos – törekvése, hogy a csalás és a korrupció elleni munkájában nem a tagállami AFCOS-okat (Anti-Fraud Coordination Service),[2] hanem a tagállami ügyészségeket tekinti első számú partnerének.

Ami az alkotmányos kérdéseket illeti, a Pau-i Egyetem professzora, Henry Labayle megfigyelése szerint az EU-ban kétféle logika működött: egy integrációs és egy kooperációs logika, ez utóbbin belül megkülönböztethető volt a horizontális és a vertikális kooperáció. A Lisszaboni Szerződés éppen a korábban a 3. pillérhez tartozó területeken hoz forradalminak is bátran tekinthető változást. Hatálybalépését követően nincs már "vasfüggöny" az EU integráció és a büntetőjog között. Ez nyilvánvalóan a szervezetek jelenlegi rendszerében is változást hoz majd. Eltekintve attól a lehetőségtől, hogy feláll az EU Ügyészség, az Eurojust sem maradhat a régi, az OLAF szerepe pedig várhatóan felértékelődik.

[2] a magyar AFCOS a VPOP keretein belül működő OLAF Koordinációs Iroda. Létrehozta a 2004. évi XXIX tv. 123-138. §§

Az EU Ügyészség személyi feltételei

Az elhangzott előadásokat követő viták egyikén a résztvevők egyöntetűen arra az álláspontra helyezkedtek, hogy a leendő EU ügyészeknek speciális ismeretekkel kell rendelkezniük, amit külön képzés során tudnak elsajátítani. Ugyanakkor EU ügyészt képezni a szó szoros értelmében nem lehet, hiszen e magisztrátusoknak már jelentős ügyészi tapasztalatokkal kell bírniuk, elsősorban a gazdasági bűnügyek nyomozásának irányítása/felügyelete területén. Megjegyzendő, hogy az egyes tagállamok, illetve jogrendek (Pl. Nagy-Britannián belül Anglia és Skócia) ügyészségei egymásétól jelentősen eltérő feladatokat is elláthatnak, de a fejlődés mai iránya szerint az EU Ügyészség a magyar ügyészséghez hasonló feladatkörrel működne.

A saját tapasztalatok és a speciális képzés elősegíthetné egy uniós igazságügyi kultúra, és egy európai büntető magisztrátusi intézmény kialakulását. Ez alapjaiban térne el a ma működő Eurojust-tól, hiszen utóbbi nemzeti tagjai nemzeti magisztrátusi jogállásúak. A képzés területén különösen aktív a Francia Magisztrátusképző Intézet, mely idejekorán felismerte, hogy a büntetőjog európai dimenzióinak az oktatásban is nagyobb figyelmet kell szentelni, ezért 2008-tól minden magisztrátusnak kötelezően meg kell felelnie egy EU-teszten is, és – az Intézet vezetője, J. F. Thony előadása szerint – az EU-büntetőjogra specializálódni szándékozó ügyészek, bírák külön tanszéken képezhetik magukat. A magisztrátusok nem feltétlenül franciák, jelenleg is számos külföldi hallgató vesz részt a képzésben, és arra is lehetőség van, hogy a képzést a saját anyanyelvükön kapják. Mód van a magisztrátusok tagállami csereképzésére, és kiépült az egyes oktató intézmények európai hálózata is. Thony úr előadásából kitűnt az az ambíció, hogy ez az intézet legyen a jövő EU ügyészeinek akadémiája: az egyéves képzés alatt anyagi és eljárásjogot, kriminológiát, EU-jogot és EU-büntetőjogot tanulnának. A képzés hangsúlyozottan gyakorlat-orientált lenne.

A jelenlegi teendők

Az Európai Ügyészség létrehozásának egyik feltételeként megjelölt európai büntetőjogi kultúrát nem kizárólag képzéssel lehet létrehozni, ám nem kell pusztán a meglehetősen lassú jogi evolúcióra sem hagyatkozni. Számos eszköz áll rendelkezésre már most is, amelyeket a csalások és a korrupció elleni európai büntetőjogi küzdelemben csatasorba lehet állítani. Elegendő csupán az európai elfogatóparancsra, vagy a közös nyomozócsoportokra utalni, de ezeken kívül több tucat uniós vívmány segíthetné az ügyészek munkáját. Sajnos a tagállamok egy része még ma is ezek *létrehozását* tekinti a legfontosabb vívmánynak, célként (félre)értelmezve az eszközt, s az *alkalmazásra* kevesebb, vagy semmilyen figyelmet nem fordít. Különösen a közös nyomozócsoportok frekventáltabb alkalmazásának a hiánya fájó, hiszen igen hatékony fegyverek lennének a transznacionális bűnözés elleni harcban. Megszervezésüket, finanszírozásukat ráadásul az Unió a

nemzetközi szervein (Eurojust), vagy szupranacionális szervein (OLAF) keresztül magára is vállalhatja.

A legfontosabb vívmányok egyike a már említett PIF-egyezmény, amely az európai büntetőjogi integráció alapdokumentuma, s egyben – Mireille Delmas-Marty professzor előadásából kitűnően – az EU Ügyészség gondolati kiindulópontja is volt. Effektív alkalmazására néhány tagállamban igen gyorsan sor került, máshol (köztük Magyarországon) még ma sem történt meg a de facto implementáció (a de iure már igen).

A PIF-egyezmény nyomán beindult büntetőjogi evolúció egyébként meglehetősen lassú volt. Az egyezmény elfogadásának évében, 1995-ben kezdte meg a munkát az a szakértői csoport, melynek feladata az EK pénzügyi érdekei védelmi rendszerének kidolgozása volt. 1997-ben került sor az azóta is Corpus Juris-ként (CJ) ismert dokumentum első publikálására. A CJ hat irányító elv és harmincöt normát tartalmazó technikai szabályzat segítségével vázolta fel a jövőbeni eljárás alapjait. Az első publikációt nyilvános vita követte, amely messze túlmutatott az egyetemek zárt világán. 1999-ben a brit Lordok Háza élénk vitát követően igen részletes és kimerítő jelentést tett közzé a CJ-ról, és meg kell említeni a Max-Planck Intézet által szervezett vitát is. Ezt követően került sor a viták nyomán módosított CJ második kiadására (ez az ún. "Firenzei verzió"). A CJ nem lett kötelező norma, de már akkor termékenyítőleg hatott az uniós büntetőjogi integráció alakulására. Számos fontos lépés következett: az UCLAF-ból létrejött az OLAF, a Nizzai Szerződés utat nyitott az Eurojust-nak, létrejött a Zöld Könyv, különböző egyezmények láttak napvilágot, de a gyakorlat mindig az elmélet és a politika után kullogott. A PIF-egyezmény tekintetében ez különösen a tagállami anyagi büntetőjog alakulásánál szembeötlő. Noha minden tagállam köteles a büntetőjog eszközeivel üldözni az EK pénzügyi érdekeinek megsértését, bizonyos országok a büntetőjogukat önként a PIF-egyezményhez alakították és az abban definiált bűncselekményeket üldözik ilyenként; mások számára az egyezmény szövegének és értelmének átvétele csatlakozási feltétel volt (Románia, Bulgária); megint mások gondos vizsgálat után megállapították, hogy nemzeti joguk nem igényel változtatást, mert az egyezményben definiált magatartás pönalizálása anélkül is biztosított (pl. Svédország). Végül van olyan is, amely az egyezmény szövegét elfogadta, de nem az abban foglalt magatartásokat üldözi az EK pénzügyi érdekeinek megsértéseként (Magyarország). Első lépésként tehát a PIF-egyezmény egységes értelmezését kellene biztosítani, és mindenhol azonos elkövetési magatartást tekinteni az EK költségvetését sértő bűncselekménynek. Ezek nyomozását és elbírálását a tagállami hatóságok és bíróságok a saját nemzeti joguk alapján végeznék, hatékony nemzetközi segítséget nyújtva egymásnak a meglévő uniós vívmányok felhasználásával. Az európai büntető anyagi és eljárási jog ilyetén előkészítése után az EU Ügyészség felállítása és működésének beindítása már zökkenőmentesen menne, s az Ügyészség szinte azonnal a tőle elvárt hatékonysággal kezdhetne neki a munkának.

FEJES PÉTER[1]

A fiatalkorú elkövetők büntető igazságszolgáltatásáról

Bevezetés

Magyarországon a büntetőjogi kodifikáció lassan húsz éve folyik. 1991-ben az új büntetőeljárási törvény kidolgozásával vette kezdetét, s a munkálatok hét év után fordultak termőre. A(z egyesek szerint keserű) gyümölcs az 1998. március 23. napján kihirdetett – majd hosszú hányattatás után – 2003. július 1-jén hatályba lépett 1998. évi XIX. törvény a büntetőeljárásról, amelynek jogtörténeti érdekessége, hogy már mint érvényes, de még nem hatályos törvényt is több jelentős módosítás érte. A tizenegy éve kihirdetett, hat éve hatályba lépett büntetőeljárási törvényt pedig a mai napig immár negyvennégyszer (!) módosították, s egy-egy rendelkezését tizenegy alkotmánybírósági határozat semmisítette meg.

2001-ben indultak az új Btk. előkészületei, amelyek eleddig nem eredményeztek új kódexet [és jelen állás szerint belátható időn belül nem is kecsegtetnek azzal, habár egyes nóvumokat a 2009. évi LXXX törvény (a továbbiakban: Btk. Novella) már becsempészett a hatályos Büntető Törvénykönyvbe]. A megfáradt, 1978. december 31. napján kihirdetett és 1979. július 1. napján hatályba lépett 1978. évi IV. törvény a Büntető Törvénykönyvről (a továbbiakban: Btk.) is az elmúlt harminc évben számtalan változást élt meg, a jogalkotó közel kilencven alkalommal módosította és az Alkotmánybíróság határozatai is tucatnyi esetben érintették, ezáltal több mint ezer helyen módosult. Nem csoda, hogy felmerült egy új, korszerű anyagi büntetőjogi törvény megalkotásának igénye.

A Btk. egységes szemléletű felülvizsgálatára és az új kódex tervezetének kidolgozására 2001. március 14. napján alakult meg az Első Kodifikációs Bizottság (soraiban egyetemi tanárokkal, bírákkal, ügyészekkel, ügyvédekkel, minisztériumi alkalmazottakkal), amely 17 ülést tartott, azokon elsősorban az Általános Rész főbb kérdéseit tárgyalva, de normaszöveget nem alkotva. A Különös Rész vonatkozásában 2005 nyarán hoztak létre egy új Bizottságot, amelynek erejéből 3 ülésre futotta, majd feloszlott. 2006-ban állt fel a Második Kodifikációs Bizottság, amely 10 alkalommal ülésezett. 2007. elején az Igazságügyi és Rendészeti Minisztérium előrukkolt az új Általános Rész első tervezetével, majd 2007. június 22. napján már a Harmadik Kodifikációs Bizottság alakult meg, amelynek 14 ülésnapja után készült el az új Általános Rész második tervezete, s azzal egyidejűleg az új Különös Rész megalkotásáról átmenetileg letett az igazságügyi kormányzat.

---

[1] Fejes P., főügyész, Veszprém Megyei Főügyészség

A fiatalkorúakra vonatkozó szabályok reformja

A kodifikálási kísérletek természetesen kiterjedtek a fiatalkorúakra vonatkozó szabályokra is. A hatályos Btk. egységes kódex, amely magában foglalja – az európai jogtechnikai megoldásoktól eltérően – a katonákra és a fiatalkorúakra vonatkozó rendelkezéseket is. A kodifikáció során élénk vita dúlt az egységes kódex megtartását, illetőleg a külön – a katonákra, illetve a fiatalkorúakra vonatkozó – büntető törvények megalkotását illetően.

Alternatívaként készült is az új büntető kódexen kívüli külön koncepció és tervezet a fiatalkorúak büntető igazságszolgáltatási törvényéről és tervezet általános indokolással a katonai Büntető Törvénykönyvről, de értelemszerűen ezek is megfeneklettek.

A fiatalkor büntetőjogi fogalom, de nemcsak a büntető anyagi jogban, hanem a büntető eljárásjogban és a büntetés-végrehajtási jogban is speciális jogszabályi rendelkezéseket von maga után. („A „más elbánást" biztosító rendszer először az Amerikai Egyesült Államokban jött létre azzal, hogy 1899-ben Illinois Államban elfogadták a fiatalkorúak bíróságát létrehozó törvényt."[2]

„A „más elbánás" lényege: a nevelési eszme középpontba állítása, a speciális prevenció előtérbe helyezése, intézményi szinten a felnőtt bűnelkövetőktől elkülönülő büntető igazságszolgáltatási rendszer."[3]) Ennek indoka a tizennegyedik életévüket már betöltött, de a tizennyolcadik évüket még be nem töltött [Btk. 107. § (1) bekezdés] elkövetők életkori sajátossága. Ezen életkoron belül is differenciál még a törvény [Btk. 110. § (2)-(3) bekezdés; 120. § (1) bekezdés] a tizenhat év alatti és feletti, illetve ezen túl még az ítélet meghozatalakor a tizennyolcadik (2010. május 1-jétől tizenhatodik) életévét [Btk. 113. §], a javítóintézeti nevelés alatt a tizenkilencedik életévét [118. § (6) bekezdés], illetve a szabadságvesztés megkezdésekor már, vagy a végrehajtás alatt a huszonegyedik életévét [111. § (4) bekezdés] betöltött fiatalkorúak vonatkozásában.

A fiatalkorúakra vonatkozó szabályok reformja tehát mindezekre figyelemmel magában foglal(hat)ja az anyagi büntetőjogi, a büntető eljárásjogi és a büntetés-végrehajtási jogi normák módosítását, de értelemszerűen ezen túl és ezeken belül számos (avagy számtalan) további tagolás is lehetséges. A büntetőjogágak közül bármelyiknek a fiatalkorúakra vonatkozó rendelkezéseinek, illetve azok reformjának teljes elemzése messze meghaladná e korreferátum terjedelmi kereteit, ezért csak a fiatalkorúak életkora alsó határának és a fiatalkorúak büntetőjogi szankciórendszerének egyes kérdéseit tárgyalom, de lege lata és de lege ferenda.

---

[2] Lévai M.: A gyermek érdekétől a megérdemelt büntetésig: a fiatalkorúakra vonatkozó büntető igazságszolgáltatás alakulása az Amerikai Egyesült Államokban. In: OKRI Szemle (Szerk: Virág Gy.), OKRI, Budapest, 2009. 149. o.

[3] A fiatalkorúak büntető igazságszolgáltatási törvényének koncepciója. IRM, Budapest, 2007. 2. o.

A hatályos szabályozás

A fiatalkorúak életkorának alsó határa

A Btk. 107. §-ának (1) bekezdése értelmében fiatalkorú az, aki a bűncselekmény elkövetésekor tizennegyedik életévét betöltötte, de a tizennyolcadikat még nem. A bírói gyakorlat értelmében az elkövető a tizennegyedik születésnapja másnapján válik gyermekkorúból fiatalkorúvá, míg a tizennyolcadik születésnapján szűnik meg fiatalkorú lenni, s annak másnapján lesz felnőtt korú, azaz a tizennegyedik születésnapján elkövetett bűncselekmény miatt még nem büntethető, míg a tizennyolcadik születésnapján elkövetett bűncselekmény miatt még fiatalkorúként büntethető, és alkalmazandóak rá a fiatalkorúakra vonatkozó eltérő szabályok [Büntetőjogi Döntvénytár 3838.].

A fiatalkor tehát büntetőjogi fogalom (amelyet egyébiránt az 1878. évi IV. törvényt, a Csemegi Kódexet módosító első büntető novella, az 1908. évi XXVI. törvénycikk vezetett be), míg a polgári jog a kiskorú fogalmát használja, amely szerint kiskorú az, aki tizennyolcadik életévét még nem töltötte be, kivéve, ha házasságot kötött [Polgári Törvénykönyv 12. § (2) bekezdés]. A polgári jog szempontjából a házasságkötéssel szerzett nagykorúságot a házasság felbontása már nem érinti, azaz a házasság felbontása nem eredményezi azt, hogy a tizennyolcadik életévét még addig sem betöltött személy „visszaminősülne" kiskorúnak. A büntetőjog számára azonban eleve fiatalkorú marad a házasságkötés folytán polgári jogilag nagykorúvá vált személy is.

A reform [az új Büntető Törvénykönyv Általános Részének koncepciója (a továbbiakban: *Koncepció*), amelynek „szakmai megalapozásához hozzájárult 11 külföldi törvénykönyv magyarra fordítása és összehasonlító elemzése[4]; a Törvénytervezet a Büntető Törvénykönyvről (a továbbiakban: *Első Tervezet*); a fiatalkorúak büntető igazságszolgáltatási törvénye; illetőleg a Törvénytervezet a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról (a továbbiakban: *Második Tervezet*); illetve az Előterjesztés a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról (a továbbiakban *Előterjesztés*)] során a vita az alsó és felső életkorhatár körül és a joghátrányok körének szélesítése vonatkozásában is erőteljes volt. Az első kérdés tárgyában jobbára az alsó életkorhatárt illetően; leszállítandó-e a tizennégy év, s ha igen, mennyire, s kevésbé a felső életkorhatárt illetően, hogy az esetlegesen felemelendő-e, s ha igen mennyire (hanem helyette az *Előterjesztés* intézményesíti az ítélkezési és az európai gyakorlat által már ismert fiatal felnőttek kategóriáját); míg a második kérdés tárgyában a büntető joghátrányokon kívül az eljárási törvényben szabályozott elterelési lehetőségek bővítése is szóba jön.

[4] Az új Büntető Törvénykönyv Általános Részének koncepciója. 1.1. pont utolsó előtti bekezdés

A fiatalkorúak büntetőjogi szankciórendszere

A fiatalkorúakkal szemben kiszabható főbüntetések a szabadságvesztés, a közérdekű munka, amelyet fiatalkorúval szemben akkor lehet kiszabni, ha az ítélet meghozatalakor tizennyolcadik (2010. május 1-jétől tizenhatodik) életévét betöltötte [Btk. 113. §] és a pénzbüntetés, amelyre a fiatalkorút kizárólag akkor lehet ítélni, ha önálló keresete (jövedelme) vagy megfelelő vagyona van, és csak behajthatatlansága esetén kell szabadságvesztésre átváltoztatni [Btk. 114. § (1)-(2) bekezdés]; a mellékbüntetések pedig a közügyektől eltiltás, amelyre fiatalkorút egy évet meghaladó szabadságvesztés esetén lehet ítélni [Btk. 115. §], a foglalkozástól eltiltás, a járművezetéstől eltiltás, a kitiltás, amelyet a megfelelő családi környezetben élő fiatalkorúval szemben nem lehet kiszabni [Btk. 116. §], a kiutasítás és a pénzmellékbüntetés (2010. május 1-jéig), amelyet csak behajthatatlansága esetén kell szabadságvesztésre átváltoztatni [Btk. 114. § (2) bekezdés]. Intézkedésként a fiatalkorúval szemben javítóintézeti nevelés is alkalmazható [Btk. 109. § (2) bekezdés]; vele szemben próbára bocsátásnak bármely bűncselekmény esetén helye van, és tartama egy évtől két évig terjedhet, a tartamot pedig években és hónapokban kell meghatározni [Btk. 117. (1) és (2) bekezdés], s megszüntetése esetén javítóintézeti nevelés is elrendelhető [Btk. 117. § (3) bekezdés]. A pártfogó felügyelet a felfüggesztett szabadságvesztésre ítéléssel, a próbára bocsátással, a feltételes szabadságra bocsátással, a javítóintézetből ideiglenes elbocsátással és a vádemelés elhalasztásával együtt jár [Btk. 119. §].

A fiatalkorúakkal szemben alkalmazott büntetés és intézkedés célja a felnőtt korúaktól eltérő, elsősorban az, hogy a fiatalkorú helyes irányba fejlődjék, és a társadalom hasznos tagjává váljék [Btk. 108. § (1) bekezdés]. Büntetést akkor kell kiszabni, ha az intézkedés alkalmazása nem célravezető [Btk. 108. § (2) bekezdés]. Szabadságelvonással járó intézkedést alkalmazni vagy büntetést kiszabni csak akkor lehet, ha az intézkedés vagy a büntetés célja más módon nem érhető el [Btk. 108. § (3) bekezdés].

A gyermekkorú bűnelkövetőkkel szemben egyébként különböző családjogi, gyermekvédelmi és gyámügyi igazgatási eszközök, mint a védelembe vétel, az ideiglenes hatályú elhelyezés, az átmeneti nevelésbe vétel, a tartós nevelésbe vétel és a nevelési felügyelet alkalmazhatók.

A tervezett szabályozás

Mindenekelőtt azt kell hangsúlyozni, hogy a *Koncepció*, a *Második tervezet* és az *Előterjesztés* is következetes abban, hogy a fiatalkorúakra vonatkozó rendelkezések a Btk. keretein belül maradnak (ahova azokat még az 1961. évi V. törvény hozta be) és nem kerülnek külön kódexbe – amit pedig többen is javasolnak,[5] s

[5] Csemáné V. E. – Lévay M.: A fiatalkorúak büntetőjogának kodifikációs kérdéseiről – történeti és jogösszehasonlító szempontból. Büntetőjogi Kodifikáció, 2002/1. 25. o.

amely megoldás általában jellemző a nyugat-európai szabályozásokra –, amelyet alternatív megoldásként az *Első Tervezet* vetett fel, s a fiatalkorúak büntető igazságszolgáltatási törvényének tervezete testesített meg, egyaránt szabályozási körébe vonva a fiatalkorúakra és a fiatal felnőttekre vonatkozó anyagi büntetőjogi és eljárási rendelkezéseket.

Az európai jogrendszerek a fiatalkorúak büntetőjogának külön szabályozását illetően eltérő modelleket követnek:

A.) A fiatalkorúak büntető igazságszolgáltatásának önálló szabályozása, ahol egy kódex foglalja magában a fiatalkorúakra vonatkozó anyagi büntetőjogi, eljárási és végrehajtási szabályokat (Ausztria, Lengyelország, Portugália, Svájc), vagy még családjogi és gyermekvédelmi rendelkezéseket is (Németország, Spanyolország).

B.) A fiatalkorúak vonatkozó anyagi büntetőjogi, eljárási és végrehajtási szabályokat több külön törvény szabályozza (Finnország, Franciaország, Egyesült Királyság, Olaszország).

C.) A fiatalkorúak büntetőjogának relatíve önálló szabályozása, ahol az anyagi büntetőjogi szabályokat a Btk. tartalmazza, míg elkülönült intézményrendszer feladatát képezi a fiatalkorúak büntetőeljárása és a büntetés-végrehajtás (Dánia, Görögország, Hollandia, Svédország).

D.) A fiatalkorúak büntetőjogának az általános büntető törvényekben szabályozása (Csehország, Magyarország, Szlovénia).[6]

„Az *Előterjesztés* követi a magyar büntetőjogban közel fél évszázada kialakult azon hagyományt, hogy a fiatalkorú elkövetőkre vonatkozó büntetőjogi szabályokat nem külön kódex, hanem az egységes büntető törvénykönyv egy külön fejezete tartalmazza."[7]

Az *Előterjesztés* (maradva immár csak a reformfolyamat ez idáig utolsó állomásánál, figyelemmel arra is, hogy a *Második Tervezetben* és az *Előterjesztésben* azonos módon érlelődött ki a normaszöveg-tervezet) fiatalkorúakra vonatkozó eltérő rendelkezései a büntetőjogi felelősség, a szankciórendszer és a mentesítés területén találhatóak meg.

Az *Előterjesztés* a fiatalkorúak mellett immár törvényi szinten (a jogalkalmazói gyakorlatot követve és nemzetközi ajánlásoknak, így a *Pekingi Szabályoknak* és az *Európa Tanács R (2003) 20. számú ajánlásának* eleget téve)[8] megkülönbözteti a fiatal felnőtteket, azokat az elkövetőket, akik a tizennyolcadik életévüket már betöltötték, de a huszonnegyedik életévüket még nem [*Előterjesztés* 101. § (1) bekezdés]. Az új speciális elkövetői csoport megkülönböztetésének indoka, hogy a

[6] A fiatalkorúak büntető igazságszolgáltatási törvényének koncepciója, i.m. 2. o.
[7] Részletes előterjesztés 167. o.
[8] Részletes előterjesztés 166. o.

felnőtté válás, a személyiség-fejlődés egy folyamat, amelyben pontos határvonalat meghúzni nem lehet és nem ildomos.[9]

A fiatal felnőttekre vonatkozó speciális rendelkezések kizárják az életfogytig tartó szabadságvesztésre ítélésüket [*Előterjesztés* 40. § (1) bekezdés], viszont lehetővé teszik velük szemben a javítóintézeti nevelés [*Előterjesztés* 104. §], valamint az ötévi szabadságvesztésnél nem súlyosabban büntetendő bűncselekmény esetén is a próbára bocsátás alkalmazását [*Előterjesztés* 112. § (2) bekezdés], továbbá kiterjesztik rájuk is – a büntetőeljárási törvény egyidejű módosításával – a vádemelés elhalasztásának a fiatalkorúakra vonatkozó szabályait.[10]

A fiatalkorúak életkorának alsó határa

Az *Előterjesztés* nem szállítja le a fiatalkor alsó határát (amely az 1961. évi V. törvény hatályba lépéséig egyébként tizenkettő év volt), hanem meghagyja a hatályos Btk. meghatározását mind az alsó, mind a felső határt illetően. Az alsó határ le nem szállításával a miniszteri indokolás ténylegesen nem foglalkozik, annál inkább a fiatal felnőttek eltérő büntetőjogi megítélésének alapjával.[11] A büntetőjogi fiatalkorú fogalmat illetően továbbra is irreleváns a házasságkötéssel szerzett polgári jogi nagykorúság.

A fiatalkorúak büntetőjogi szankciórendszere

Az *Előterjesztés* új büntetési nemet a fiatalkorúakra vonatkozóan sem vezet be. Újítása mindössze annyi, hogy a főbüntetetések megnevezés helyett a büntetések elnevezést favorizálja, s a büntetések – kettő kivétellel [*Előterjesztés* 38. § (6) bekezdés] – egymás mellett is kiszabhatók [*Előterjesztés* 38. § (5) bekezdés], míg mellékbüntetésnek [*Előterjesztés* 38. (2) bekezdés] csak a közügyektől eltiltást tekinti, mivel arra a terheltet önállóan nem, hanem csak járulékosan, büntetés mellett lehet ítélni. A büntetés célja a fiatalkorúakkal szemben továbbra is elsősorban a nevelés.[12]

A hatályos szabályozástól eltérően fiatalkorút csak legalább kétévi végrehajtandó szabadságvesztés kiszabása esetén lehetne a közügyektől eltiltani [*Előterjesztés* 111. §], a javítóintézeti nevelés a fiatalkorú elítéltnek nem a tizenkilencedik, hanem a huszonegyedik életévéig tarthatna [*Előterjesztés* 113. § (6) bekezdés], a közérdekű munka pedig az ítélet meghozatalakor nem a tizennyolcadik, hanem már a tizenhatodik életévét betöltött fiatalkorú terhelttel szemben is kiszabható lenne [*Előterjesztés* 109. §], összhangban a Munka Törvénykönyvével.[13] Utóbbi rendelkezést időközben a Btk. Novella – 2010. május 1-jei hatállyal – a Btk.-ba már beiktatta.

[9] Általános előterjesztés 87. o.; Részletes előterjesztés 166-167. o.
[10] Részletes előterjesztés 168. o.
[11] Részletes előterjesztés 166–167. o.
[12] Részletes előterjesztés 167. o.
[13] Részletes előterjesztés 170. o.

Észrevételek, javaslatok

A fiatalkorúak életkorának alsó határa

Köztudomású, hogy a fiatalok biológiailag egyre korábban érnek. Kétségtelen, hogy ez nem feltétlenül jár együtt azzal, hogy erkölcsi-szellemi érettségük is hamarabb következne be. Ennek ellenére magam is – a közvélemény nagyobb részével egyetértve – hajlanék a fiatalkor alsó határának tizenkettő életévre csökkentésére.

Európában a fiatalkor büntetőjogi fogalma változatos képet mutat.[14] A büntethetőségi korhatár többségében tizennégy év (vagy akörüli), a legalacsonyabb Írországban és Svájcban (vagylagosan hét év), a legmagasabb (több országban vagylagosan, míg máshol kizárólagosan, így) Portugáliában és Spanyolországban (tizenhat év). A felnőtt kor büntetőjogi fogalma pedig általában a tizennyolcadik életév betöltésével kezdődik, de van példa a tizenötödik életévvel kezdődő szabályozásra is (lásd Törökország). A vagylagosság lényege, miszerint „az adott életkor betöltése nem egyetlen kritériuma a büntetőjogi felelősségnek: többnyire – részint a cselekmény jellegének függvényében – sor kerül valamilyen értelmi, erkölcsi, avagy akarati feltétel, ítélőképesség vagy belátási képesség meglétének vizsgálatára […] Ekkor azt vizsgálják, hogy az elkövető gyermek vagy fiatal rendelkezett-e a szükséges érettséggel, illetve a jó és rossz közötti különbségtétel képességével […] Más országokban e feltételek mellett, illetve túl jelentőséghez jut a fiatal által elkövetett cselekmény jellege is."[15]

Magyarországon elképzelhetőnek tartanék olyan szabályozást, amely a büntetőjogi vétőképességet – csak a külön nevesített személy elleni erőszakos, súlyos bűncselekmények esetében – a tizenkettedik életév betöltéséhez kötné, azzal, hogy a tizenkettő és tizennégy év közötti életkorban igazságügyi orvos-szakértő (pszichológus) vizsgálja az erkölcsi-értelmi érettséget. Indoka ennek az, hogy a korábban érés folytán bizonyos súlyos bűncselekmények esetén már tizennégy év alatt is rendelkezhet a szükséges ítélőképességgel, belátási képességgel az elkövető. Ilyen személy elleni erőszakos, súlyos bűncselekménynek tekinteném, nemcsak az emberölést, a súlyos testi sértést, hanem például a csoportos garázdaságot, rablást is. Ezeknek (és más) cselekményeknek a tilalmazott voltát, figyelemmel az ezen életkorban is már ismert erkölcsi-vallási normák tartalmára is, megítélésem szerint egy tizenkettő éves kiskorú is képes (lehet) felismerni.

Ezt támasztja alá az *acceleráció*, azaz a biológiai érés – amely persze nem azonos a szellemi éréssel, amelynek alapján a személy képes különbséget tenni a jogos és jogtalan között, és az erkölcsi éréssel, amely a bűn, a bűnösség megélésének élményét jelenti – felgyorsulása, amelynek következtében a gyermekeknél ma már a biológiai érés tizenkettedik életévükben bekövetkezik, azaz két évvel korábban,

[14] Csemáné – Lévay, i.m. 16. o., 2. számú táblázat
[15] Csemáné – Lévay, i.m. 17. o.

mint például száz évvel ezelőtt. (A fiatal felnőtt kategória bevezetését pedig a *posztadoleszcencia*, azaz a társadalmi érés kitolódása igazolja, amely szerint a megváltozott társadalmi viszonyok folytán a felnőtté válás, azaz a szülőktől való anyagi és döntési függetlenedés következik be később, a huszonegyedik és a huszonötödik életév között.)

Egyébiránt a gyermekkorúak által elkövetett büntetendő cselekmények mintegy 60%-áért a tizenkettő-tizennégy közötti kiskorúak a felelősek.
A szellemi és erkölcsi érés kapcsán kell még kitérni a belátási képességre, mint felelősségi feltételre, amely együtt jelenti az elkövető értelmi, erkölcsi és szellemi érettségét. Sem a hatályos szabályozás, sem a tervezett szabályozás nem ismeri a belátási képességet, mint felelősségi kategóriát.

Németországban bevett a belátási képesség vizsgálata, a német bírói gyakorlat szerint a következő tíz szempont alapján: 1. Reális életterv; 2. Az önálló, indokolt döntésre való képesség; 3. A jövőt is magában foglaló gondolkodásra való képesség; 4. Az érzelmeknek az értelem alá rendelésére való képesség; 5. A személyiség bizonyos fokú önállósága a szülőkkel szemben; 6. Az egyívású csoport tagjaival szembeni önállóságra való képesség; 7. A napi feladatok önálló intézésére képesség; 8. A tartós kötődésre való képesség; 9. A felnőttekre jellemző szexualitás; 10. Az iskolát, illetve a munkát illetően reális beállítottság.

A belátási képesség bevezetése a fiatalkorúak büntetőjogi felelősségét feltételes felelősséggé változtatja, azaz büntetőjogi felelősség megállapítására csak akkor kerülhet sor, ha az adott bűncselekmény vonatkozásában a fiatalkorú elkövetőnek megvan a belátási képessége, az értelmi, erkölcsi és szellemi érettsége, ami egyébként – ahol ismert ez a kategória – nem szakértői kompetencia, hanem az ügyész, a bíró hatáskörébe tartozó kérdés.

A fiatalkorúak büntetőjogi szankciórendszere

A hatályos Btk. szankciórendszere mind a felnőtt korúak, mind a fiatalkorúak esetében szegényes. Sajnálatos, hogy ezen az Előterjesztés sem képes változtatni.

A fiatalkorúak esetében a bíróságok által a gyakorlatban ténylegesen alkalmazható és alkalmazott joghátrányok általában a próbára bocsátás és a (felfüggesztett) szabadságvesztés.[16] A pénzbüntetésre ítélés gátja, hogy a (bűnöző) fiataloknak csak nagyon kevés hányada rendelkezik önálló keresettel (jövedelemmel) vagy megfelelő vagyonnal, míg a közérdekű munka csak az ítélet meghozatalakor a tizennyolcadik (2010. május 1-jétől viszont már tizenhatodik) életévét betöltött fiatalkorúval szemben szabható ki,[17] s a gyakorlatban a felnőtt korúakra nézve is csekély a végrehajtásra lehetőséget adó munkahely, foglalkoztató. A javítóintézeti nevelés alkalmazását pedig (a bíróságok idegenkedése mellett) a büntetőeljárások

[16] Fülöp Á. – Nagy E.: Új törekvések a fiatalkorúak büntetőjogában. In: Kriminológiai Tanulmányok 42. (Szerk: Irk F.) OKRI, Budapest, 2005. 311. o.
[17] Fülöp – Nagy, i.m. 310. o.

általános elhúzódása zárja ki. Az Előterjesztés kétségtelenül növeli az alkalmazhatóságát azzal, hogy végrehajtását a huszonegyedik életév betöltéséig tolja ki.

Nem vitatott, hogy „egy gazdagabb palettájú intézkedési rendszer”[18] (és büntetési rendszer) lenne kívánatos.[19]

Megfontolandónak látnám ezért például a pártfogó felügyelet önálló alkalmazhatóságát (a vádemelés elhalasztása és próbaidővel járó intézkedés és büntetés alkalmazása nélkül); a terápiás csoportban, foglalkozásokon részvételt, avagy kötelező orvosi (pszichológiai) kezelésnek való alávetést mint intézkedéseket (amelyek lényegében a pártfogó felügyelet magatartási szabályai közül lennének kiemelve); az elbíráláskor tizenhatodik életévét betöltött elkövető esetén a közösségi munkavégzésre kötelezést (például graffitik eltüntetésében, iskolák kitakarításában, kifestésében részvétel, amelynek végrehajtásáról a települési önkormányzatoknak vagy a gyámhivataloknak kellene gondoskodnia); a felfüggesztett vagy halasztott pénzbüntetést, amelyet a tizennyolcadik életév betöltését követően kellene az elkövetőnek megfizetnie, ha a próbaidő alatt elkövetett újabb bűncselekmény elkövetése miatt elítélnék; s pénzbüntetés kiszabhatóságát az ítélet meghozatalakor a tizennyolcadik életévét betöltött fiatalkorúval szemben.

Ezen túlmenően is szükséges lenne még újabb büntetési és intézkedési nemek bevezetése, hogy a (ténylegesen alkalmazható) szankciók ne legyenek egysíkúak, s a differenciált, a cselekmény súlyához és a fiatalkorú elkövető személyiségéhez mért joghátrányok kerülhessenek alkalmazásra.

[18] Fülöp – Nagy, i.m. 304. o.
[19] Lásd pl. Csemáné – Lévay, i.m. 26. o.

INFOLABOR – Az elektronikus bizonyítékszerzés helye és szerepe a jogérvényesítésben[1]

Az *„INFOLABOR" – Az elektronikus bizonyítékszerzés helye és szerepe a jogérvényesítésben* c. konferenciát 2010. február 12-én rendezték Budapesten, a Gábor Dénes Műszaki Főiskola (SZÁMALK Zrt.) épületében. A konferenciát a Magyar Tartalomipari Szövetség (MATISZ) támogatta. A MATISZ az Európai Bizottság Biztonságosabb Internet Programja[2] keretében biztosította a helyszín bérletét és a megjelent mintegy 110 résztvevő étkeztetését. A program keretében a Bizottság támogatja az ún. biztonságosabb internet centrumok működését. A MATISZ ilyen biztonságosabb internet centrum, amelynek egyik tevékenysége az illegális és káros internetes tartalmak bejelentésére szolgáló hotline[3] üzemeltetése. A MATISZ 2005 óta tagja az INHOPE (International Association for Internet Hotlines)[4] nemzetközi szervezetének, ennek keretében részt vesz a magyar tartalomszolgáltatók önszabályozási rendszerének kiépítésében. Jelen konferencia is ilyen önszabályozási kezdeményezés volt, hiszen az elektronikus bizonyítási eszközök hiteles rögzítésének, megőrzésének és bíróság előtti felhasználásának eszközeit ismertette meg a jórészt jogalkalmazókból – a rendőrség, ügyészség, bíróság képviselőiből – álló közönséggel.

A nyitóelőadást **dr. Peszleg Tibor** független szakértő tartotta. Hangsúlyozta, hogy mennyire megnőtt az igazságügyi informatikai szakértő szerepe azokban az ügyekben, ahol elektronikus adathordozót kell lefoglalni és vizsgálni. De mielőtt az informatikai szakértő elkészítené az adathordozó hiteles másolatát (image),[5] a házkutatás és az adathordozó lefoglalása is informatikai szaktanácsadó jelenlétében zajlik, hiszen biztosítani kell, hogy a számítástechnikai eszközökön található adatok ne törlődjenek, módosuljanak. A nyomozó hatóság nem rendelkezik az image-másolat elkészítésének eszközeivel, éppen ezért ezt az egyébként különleges szakértelmet nem igénylő műveletet is a szakértőre bízza. Emellett, a nyomozó hatóság rendszeresen olyan jogkérdéseket is feltesz a szakértőnek, mint amilyen tipikusan a tiltott pornográf felvétellel visszaéléssel kapcsolatos ügyekben az adathordozón található gyermekpornográf felvételek leválogatása. Pedig

[1] A beszámolót Parti Katalin, az OKRI munkatársa készítette.

[2] Az Európai Bizottság a Biztonságosabb Internet Programot még 1999-ben hirdette meg, az utóbbi 10 évben azonban többször meghosszabbította. (A programról lásd: http://ec.europa.eu/information_society/activities/sip/index_en.htm)

[3] A magyar forródrót elérhető: http://www.matisz.hu/Hotline.141.0.html

[4] Az INHOPE szintén az Európai Bizottság Biztonságosabb Internet Programja keretében jött létre, 1999-ben. (Lásd: http://www.inhope.org)

[5] Az image-másolat készítése ún. checksum eljárással, azaz bitről bitre másolással történik garantálva, hogy a másolat pontosan megegyezzen az eredeti adathordozóval.

ilyen esetben a szakértő legfeljebb az adathordozón található képi anyagok leválogatását végezhetné el, hiszen a pornográf minőség és az ábrázolt személyek életkorának megbecslése jogkérdések.

Vita tárgyát képezi, hogy az e-mail mikor számít kézbesítettnek: ha megérkezik a webes levelezőszerverre, ha már a címzett postafiókjában van vagy ha a címzett meg is nyitja – tehát meg is ismerte – az elektronikus levél tartalmát. A kézbesítésre vonatkozó általános szabályok alkalmazása helyett mindig a nyomozást felügyelő ügyésszel kell konzultálni az irányadó gyakorlat szerint. Kérdés, hogy az elektronikus levél eltérő megjelenési formája indokolja-e a különbségtételt vagy csak a jogalkalmazó idegenkedése okozza az eltérő kezelést.

Az azonban bizonyos, hogy az e-mail önmagában semmit sem bizonyít. Amellett, hogy kinyomtatott formában nem alkalmas a benne foglaltak bizonyítására, az elektronikus változat is csak a fejlécben szereplő adatokkal együtt bizonyíthatja, hogy milyen e-mail címről, mikor és milyen tartalommal küldték. A papír ugyanis könnyen hamisítható, azonban az elektronikus levélről készített elektronikus másolat bitről bitre megegyezik az eredetivel.

Dr. Peszleg Tibor javasolta, hogy legyenek informatikai szakértői szakterületek, ugyanis az informatika olyan ütemben fejlődik, hogy minden területéhez már nem érthet minden (általános informatikai) szakértő. A specializálódásnak praktikus, időkímélő és kontroll-funkciói is lennének: nem minden, egyébként igen sokba kerülő technikai eszközt kellene beszereznie a szakértőnek, hanem a szakértők csak saját szakterületüknek megfelelő eszközökkel rendelkeznének. Ez megkönnyítené a feladat-leosztást, a szakértők az időtakarékosság jegyében gyorsabban járnának el, nem utolsó sorban az eljárások sztenderdizálásához vezetne, amely ellenőrizhetőbbé és hitelesebbé tenné a szakértők munkáját.

Ehhez kapcsolódóan **Illési Zsolt** igazságügyi informatikai szakértő felvetette a metaadatok[6] vizsgálatának kérdését. A metaadatok vizsgálatához nem lenne szükség különleges szakértelemre, azonban technikai felszerelés hiányában jelenleg mégis a szakértő feladata csakúgy, mint a hiteles másolat készítése.[7]

Ezután az INFOLABOR Infokommunikációs Szakértői Iroda két munkatársa – **Szabó Attila és Komáromi László** – bemutatta az informatikai szakértő másoláshoz és hitelesítéshez használt eszközeit. Habár a lefoglalást elszenvedő fél kíméletének követelménye ezt indokolná, a teljes körű adathordozó-lefoglalás nem mindig kerülhető el. Ennek egyik oka, hogy nem minden számítástechnikai eszköz vizsgálható a helyszínen, pl. a nagy adattároló kapacitással bíró adathordozók másolásához sokszor nincs megfelelő nagyságú adathordozó a szakértőnél.

[6] Egy másik adatot leíró, meghatározó adat, amely összefoglalja az adat használatára vonatkozó összes fontos tényt. (http://www.mimi.hu)

[7] A metaadatok elemzése bűnelemző szoftverek segítségével lehetséges. Ilyen szoftverekkel azonban csak a megyei rendőr-főkapitányságok rendelkeznek, korlátozott számban. (Lásd még: http://www.sg.hu/cikkek/46759/bunelemzo_szoftvereket_kaptak_a_rendor_fokapitanysagok)

A lefoglalt adathordozó hiteles megőrzésének eszközei és módszerei nem egységesek, pl. hogyan kell ütés- és sérülésmentes csomagolással ellátni az adathordozót, hogyan kell lezárni a csomagot, hogyan biztosítják, hogy a szakértő a vizsgált eszközöket, és ne másokat adjon vissza a nyomozó hatóságnak, milyen adatoknak kell szerepelnie a címkén, plombán stb. A szakértő sokszor szembesül azzal, hogy az adathordozót már sérült állapotban kapja meg, vagy az az elégtelen csomagolás miatt nem vizsgálható, használhatatlan. Az ilyen adathordozó nemcsak a bizonyítási eljárásban való felhasználásra alkalmatlan, de kiadás után a lefoglalás elszenvedője sem használhatja már tovább. A szakértők felhívták a figyelmet a részletes kérdésfeltevés jelentőségére: minél részletesebben kérdez az ügy előadója, annál könnyebb dolga van a szakértőnek meghatározott adatok keresésekor, elemzésekor. A pontos kérdés-feltevés nemcsak a véleményadás idejét rövidíti le, de a költségeket is csökkentheti. Ennek érdekében a szakértők összeállítottak egy bianco szakértői kérdés-blokkot, amelyet a konferencia résztvevői az előadások absztraktjaival és a szponzor ismertetőivel együtt megkaptak.

Szongoth Richárd r. százados, a BRFK Gazdaságvédelmi Főosztály Számítógépes Bűnözés Elleni Osztály vezetője elmondta, hogy a számítógépek és az internet térnyerésével számos olyan kérdés merül fel, amelyről nem lehet eldönteni, hogy szakkérdés-e (tehát informatikai szakértő *szakértelmét* igényli), vagy csupán olyan jogkérdés, amelyet a nyomozó hatóság tagja kellő *szaktudás* birtokában megválaszolhat. Nem egységes a nyomozó hatóságok gyakorlata pl. az IP-cím vagy az IP-cím szolgáltatója megállapításában, a weboldal IP-címének megállapításában. Ezekre a kérdésekre az alapvető informatikai, internet-felhasználói ismeretek birtokában ma már az ügy előadója is válaszolhatna, ennek ellenére a szokás hatalmának engedelmeskedve azt a mai napig a szakértő feladatává teszik. Hasonló a helyzet azokban a kérdésekben, amelyek ugyan jogkérdések, de alapvető számítástechnikai eszközök hiányában mégis a szakértő válaszolja meg azokat. Szongoth Richárd ezért szorgalmazza a nyomozó hatóság számítástechnikai elemző alapfelszereléssel való ellátását és tagjainak technikai képzését.

Dr. Zaránd Viktor, a Budapest VIII. Kerületi Ügyészség ügyésze előadásában felhívta a figyelmet az adatvisszatartási irányelv[8] követelményeinek megfelelően módosított elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) ellentmondásaira.[9]

Dr. Vadász Viktor, a Pesti Központi Kerületi Bíróság bírája szerint alapvetően át kell értékelni a számítógép és a jogalkotó/jogalkalmazó viszonyát. Ezzel nemcsak arra utalt, hogy a bíróságok vonakodva fogadnak el elektronikus úton benyújtott

[8] Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (adatvisszatartási irányelv {(HL L 105., 2006.4.13., 54–63. o.})

[9] Zaránd Viktor előadásának részleteit lásd: Ügyészek Lapja, 2010/1. szám, 89–74. o.

tárgyi bizonyítási eszközöket, hanem emellett aggályosnak tartja azt is, hogy a magyar jogalkotó különböző definíciókat állapított meg a számítástechnikai rendszerre, a számítógépes programra és a számítógépre. Igaz, az Európa Tanács Számítástechnikai bűnözésről szóló egyezménye sem fogalmaz elég világosan, mindenesetre a változtatás nélküli implementálás elhatárolási gondokat okozhat a joggyakorlatban, tekintve, hogy ma már majdnem minden gép beépített számítástechnikai eszköz segítségével működik. Így ha pl. egy személygépkocsit a beépített számítástechnikai rendszerébe („fedélzeti számítógép") való illetéktelen behatolással indítanak be, hogy azt eltulajdoníthassák, a lopás mellett nem lesz megállapítható a számítástechnikai rendszer és adatok elleni bűncselekmény[10] is, az uralkodó gyakorlattal ellentétben. Ugyanígy tisztázatlan a gyakorlatban, hogy a levéltitok/magántitok megsértése vagy a számítástechnikai rendszer elleni bűncselekmény állapítható meg abban az esetben, ha az elkövető a sértett elektronikus levelezését tekinti meg engedély nélkül. Az azonban nem véletlen – és a minősítésnél is segít –, hogy a jogalkotó a magántitok jogosulatlan megismerése minősített esetévé tette a számítástechnikai rendszer útján történő elkövetést.[11] A dilemmák feloldása érdekében a jogalkotónak vagy részletesebben kellene meghatároznia, mit kell érteni számítástechnikai rendszeren vagy az egyes tényállások minősített eseteiként kellene szabályoznia a számítástechnikai rendszerben való elkövetést.

Dr. Vadász Viktor felvetette, hogy a számítástechnikai környezetben elkövetett bűncselekmények nyomozása olyan nehézségekbe ütközhet, mint a rejtett IP címekhez[12] tartozó számítógépek felkutatása, valamint a szerzői jog megsértése miatt indult ügyekben annak bizonyítása, hogy a gyanúsított tényleg jogtalanul használta a kérdéses szoftvert. Ilyen pl. a próbaszoftverek (trial version) próbaidőn túli használata, vagy az, hogy az ingyenesen is letölthető szoftverek forrását – legális használatát – a gyanúsított nem mindig tudja igazolni. Ezekben az esetekben természetesen nem állapítható meg a szerzői jog megsértése.

A magyar joggyakorlat az interneten ingyenesen elérhető szerzői művek letöltéséért nem, csak terjesztéséért vonja felelősségre az elkövetőket. Némileg ellentmond ennek, hogy a fájlcserélő rendszerek használói a letöltéskor egyben technikailag meg is osztják a letöltött részleteket mások előtt, ez viszont már nyilvánossághoz

[10] Btk. 300/C. §
[11] Btk. 178/A. §
[12] Az IP hider, azaz IP cím elrejtő szolgáltatások nagyon népszerűek a felhasználók körében. Nem csupán az illegális tevékenységek maradnak rejtve az IP hider szoftverek használatával, hanem – mivel így nem marad nyoma a böngészési útvonalnak, tehát a felhasználói preferenciáknak sem – a felhasználó a kéretlen levelek áradatától is megóvhatja gépét. A módszer azon az elven alapul, hogy minden proxy szerver egyben anonimizálja is az IP hider program segítségével böngésző felhasználó IP címét. Más kérdés, hogy az anonimizált IP-ket a szolgáltatók meg is őrizhetik, így elviekben minden anonimizált IP visszakövethető – természetesen csak akkor, ha a böngészésben résztvevő minden proxy-szolgáltató meg is őrizte az eredeti, anonimizálás előtti IP-t. (Bővebben lásd pl.: http://www.hide-ip-soft.com/)

közvetítésnek minősül. Ehhez képest rendre csak a torrent (fájlcserélő)-oldalak üzemeltetőit marasztalja el a bíróság.

Dr. Németh Zoltán ügyvéd egy sor jogesettel szemléltette, mire lehet alkalmas az elektronikusan rögzített adat a bizonyítás során és milyen új elkövetési formák jelentek meg az elektronikus úton történő kommunikáció elterjedésével. Amellett, hogy az online közösségi portálok lehetőséget adnak az ügyről rendelkezésre álló ismeretek bővítésére, a hagyományos kérdezési technikának is nagy a szerepe az ügyek feltárásában. A személyes adattal visszaélés új, internetes kommunikációt kihasználó formái az „elektronikus identitás kompromittálása", amikor az elkövető visszaél a valós felhasználó által megadott személyes adatokkal – azokat megváltoztatja vagy sajátjaként használja; a kommunikációban való közbeékelődés (a kommunikáció „lehallgatása"); valamint a billentyűzet áramköréhez kapcsolódó szoftver (keylogger) használata a sértett felhasználó adatainak kifürkészése érdekében.

Dr. Németh Zoltán felvetette, mennyire praktikus lenne az elektronikus irattanulmányozás bevezetése. Az ügyvéd a rendelkezésére bocsátott belépési kódok birtokában csak azokat az iratokat tanulmányozhatná, amelyekhez egyébként is joga van. Így pl. a vesztegetéses esetekben annyiszor lehetne végignézni a vesztegetési pénz átadásáról készült – általában nem mozifilm minőségű – felvételt, ami csak alkalmas a vesztegetés megtörténtének/meg nem történtének megerősítéséhez. Ezzel természetesen nem a közvetlen bizonyítás elvének átlépésére biztat: a kérdéses felvételt a bírósági tárgyaláson ugyan levetítenék, de fölösleges ismétlések nélkül. Az ötlet annál is aktuálisabb, mert 2011-től a polgári, 2012-től pedig a büntetőügyekben eljáró bíróságoknak egészében át kell térniük az elektronikus nyilvántartásra.[13]

Mamuzsics Gábor informatikai szakértő, az APEH informatikai biztonsági auditora előadásában részletesen elemezte, mi teszi az iratot elektronikus bizonyítékká (büntetőjogi, közigazgatási és polgári jogi szabályok), tehát az elektronikus bizonyítás jogszabályi környezete adott. Mint ahogyan az elektronikus adóbevallás feltételei is (2004 óta), azonban ha valaki él ezzel a lehetőséggel, az adóhatóság az elektronikus üzletvezetés minden dokumentumát bekérheti, tehát az adóellenőrzés is teljes mértékben elektronikus úton történik. Ezzel rendkívüli mértékben megnőtt az elektronikus adatok biztonságának jelentősége. Ennek ellenére Magyarországon nehéz meghonosítani a tudatos informatikai biztonságot, az emberek általában nem aggódnak adataik biztonságáért, tehát az adatvédelmi szempontú ráfordítás sem kielégítő.

Az adóhatóság az ellenőrzés elvégzésekor olyan körültekintéssel köteles eljárni, mint az igazságügyi informatikai szakértő a lefoglaláskor, annyi különbséggel, hogy nincs lehetősége az adathordozók elvitelére. Így az adóhatóságnak minden

[13] 2009. évi LII. törvény a hivatalos iratok elektronikus kézbesítéséről és az elektronikus tértivevényről

eshetőségre felkészülten kell kiszállnia az ellenőrzés helyszínére, ahol adott esetben minden iratmásolatot a helyszínen kell elkészítenie és eredeti állapotában hitelesítenie.

Antalóczy György, a Gazdasági Versenyhivatal (GVH) Kartell Csoportjának munkatársa megerősítette, hogy a versenyhivatal is image-másolattal (un. klónnal vagy tükörmásolattal) dolgozik a kartell-megállapodások és tevékenység vizsgálata során, az eredeti adatokat vizsgálni nem szabad. A GVH-nak annyiban több a jogosultsága az adóhatósághoz képest, hogy a helyszínen talált összes adathordozót lefoglalhatja (tehát elviheti a helyszínről), azonban nem minden elektronikus iratot ismerhet meg teljeskörűen. Így például az ügyvédi titoktartás körébe eső (Legal Professional Privilege – LPP)[14] ügyfél-levelezés tartalmát a GVH sem ismerheti meg, és nem használhatja fel az eljárása során. Az „LPP-bélyeg" azonban – mivel tartalma titkos – minden olyan szenzitív iratra „ráüthető", amelyről az ügyfél nem akarja, hogy a GVH kezébe kerüljön. Ezen iratok vizsgálatára még nem sikerült olyan eljárást kifejleszteni, amely kizárhatná az adatok titokban maradását.

A lefoglalt adatok az ügy, az akta részévé válnak, és zárt bizonyítási lánc segítségével bármikor visszaellenőrizhető az eljárás jogszerű menete.

A konferencián élénk vita alakult ki arról, hogy mi választja el a *különleges szakértelmet* és az *informatikai szakismereteket*. Az elektronikus nyomrögzítés- és elemzés korában már a nyomozó hatóságnak is egyre szélesebb körű informatikai szakismerettel kell rendelkeznie annak érdekében, hogy az alapvető információk beszerzéséhez és elemzéséhez nem kelljen szakértőt kirendelni. A tanácskozáson mind a nyomozó hatóság, mind az informatikai szakértők oldaláról felmerült, hogy meg kellene szüntetni a „megszokás"-alapú szakértői kirendelést azokban a kérdésekben, amelyekhez egy évtizede még ugyan szükség volt szakértőre, ma már azonban az alapvető felhasználói ismeretek körébe tartoznak (pl. az IP-cím megállapítása szabad internetes adatbázisok használatával). Ennek veszélye, hogy elvitatja a szakértő kompetenciáját, másfelől pedig a bíróságok a nyomozó hatóság tagjának szakismerete tárgyában tett megállapításait nem fogadják el bizonyítékként, legfeljebb csak szakértő véleményével megtámogatva. Az ügyek egyre bonyolultabbá válása és a gyors reakcióidő, nem utolsó sorban pedig a költségtakarékosság követelménye mégis a jogalkalmazói elemzés kiterjesztését és a szakértő szerepének korlátozását tenné szükségessé. A korlátozás ugyanakkor nem csökkentené a szakértők felé érkező megbízások számát, hiszen ezzel egy időben az informatikai szakértők részterületekre való szakosodása, az elemzési tevékenység szofisztikáltabbá válása is elkezdődhetne. A jogalkalmazó a megfelelő technikai felszerelés birtokában elvégezhetné a háttértár-elemzést, amelynek során válaszolhatna az – eddig jórészt szakértőnek feltett – jogkérdésekre, másfelől pedig biztosabb számítástechnikai ismeretek birtokában nagyobb

[14] 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról, 65/B. §

rálátása lenne az ügyre. Arra a kérdésre, hogy hogyan ellenőrizhető, hogy a nyomozó hatóság tagja az elektronikus bizonyíték-rögzítést szabályszerűen hajtotta-e végre egyszerű a válasz: a rendelkezésre álló technikai felszerelés (IT forensic toolkit) olyan hitelesítési folyamatot biztosít, amelynek szabályszerűségéről – azaz hitelességéről – bárki, így az eljáró bíróság is meggyőződhet. A baj alapvetően az, hogy a rendőrségnek nincsenek ilyen eszközei, ugyanakkor, ha lennének is, szemléletváltásra lenne szükség: a bíróságnak el kellene fogadnia, hogy nemcsak a szakértőtől várhat igazoltan hiteles eljárásban igazoltan hiteles adatokat.

Lente Csaba, a Magyar Igazságügyi Szakértői Kamara Informatikai Szakbizottságának elnöke összefoglaló hozzászólásában kifejtette: a kamara azon fáradozik, hogy a szakértők számára egységes protokollokat biztosítsanak a lefoglalt adathordozó vizsgálata, a szakértőnek feltehető kérdések és a szakértő jogai/kötelezettségei – pl. válaszadás megtagadásának körülményei – terén. Abbéli reményét fejezte ki, hogy e célok érdekében hamarosan megrendezhetjük a következő, hasonló témájú fórumot, ahol immár nem(csak) a jogalkalmazók, hanem a szakértők (is) megjelenhetnek, hiszen az állandó párbeszéd a konstruktív együttgondolkodás és a konszenzus alapja.

SZABÓ IMRE[1]

"The Pirate Bay" case in a mirror of Hungarian criminal law

The Pirate Bay site[2] (TPB) is one of the biggest[3] BitTorrent technology using sites in the world. The page could be reached from servers located in Sweden till 31st may 2006, when the Swedish police confiscated these servers. With this measure, the Swedish police made the service offline (unavailable) for three days. However, TPB re-launched after resettlement, operating from other countries' servers, and it is still available.
On the 17th April 2009 four persons (P. S., F. N., G. S. and C. L.), who where involved in the operation of TPB, were found guilty by the Swedish first instance court of aiding and abetting the infringement of rights related to copyright[4], and therefore each of them was sentenced to one year served in prison, and fined 30 million SEK (approximately 2,684,000 Euros). The verdict is not final.[5]

The reason for the examination of the first instance verdict was to find out what was the justification of the claim, which was established on the basis of the website operators' liability. I focused on the acts which can establish the liability of the intermediary service providers. Therefore, inter alia, I don't deal with the problems of the calculation of the damages according to harmful results, or with the documentation of the punishable offence (the principal offence).
Although the Swedish court found jurisdiction in this case, given the fact that in the IT environment the current meaning of the rules of jurisdiction shows different views across Europe, it is conceivable that the appeal procedure will require further clarification, particularly with regard to the act of complicity, where Sweden did not have jurisdiction applicable to the committing of the principal offence.[6]

---

[1] Szabó I., junior researcher, OKRI
[2] http://www.piratebay.org
[3] The data from 2008 November shows, that TPB have 3,800,000 registered users, which of course does not mean that they are all involved in the infringement of intellectual property. http://en.wikipedia.org/wiki/The_Pirate_Bay 27th October 2009
[4] Copyright infringement (or copyright violation) – Complicity in breach of the Copyright Act
[5] Following the appeal the trial is expected to continue in September 2010. Ricknäs, M.: IDG News Service. PC World, 11 March 2010, http://www.pcworld.com
[6] Ulrich, S.: Internationales Strafrecht im Internet. Das Territorialitätsprinzip der §§ 3,9 StGB im globalen Cyberspace. In: NJW 1999, p. 2065–2073; Vassilaki, I. E.: Anmerkung zum Urteil des BGH vom 12.12.2000 – 1 StR 184/00; Online: »Auschwitzlüge« und deutsches Strafrecht. In: CR 2001, p. 262–265.; Hilgendorf, E.: Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips. In: NJW 1997, p. 1873–1878.

Regardless of this, in order to investigate the criminal liability of participants in the operation on TPB, joint examination of the following areas is required: the operation of file sharing services which use the BitTorrent protocol, the grounds for freedom from liability for intermediary service providers, the regime of criminal responsibility for complicity, carried out by omission, and the copyright infringement of the principal offence.

The operation of BitTorrent technology

The BitTorrent technology is a data transmission protocol[7] based on P2P (peer to peer) principles. Files can be transferred between communicating computers which are on an equal footing with each other using particular client software[8]. In this case, because of the decentralized nature of the exchange, the parties download information from each other.[9]

The starting point is a file (principal file) containing certain named recordings of sound or moving pictures, or computer software such as computer games, any of which might be copyright-protected. When somebody wants to make such a file available for the general public through a BitTorrent file-sharing system, s/he needs to first download a client program, which is then installed on the computer. After installation, one needs to use the client software to make a torrent file[10] about the principal file. This prepared torrent file contains information about the file you want to share, the distributed data packets and their control amount. The torrent file also contains one or more tracker[11] addresses, servers on which information about the transfer may be registered. The client software divides the file into various sections (data packets from 64kbyte–4 Mbytes), and give them a mathematical number (known as a hash total[12]).

[7] The protocol – in the information technology – is a convention or standard that describes how the participants in the network can communicate with each other. The protocol includes the rules of the contact, communication and data transmission arrangements.
[8] Bitcomet, µTorrent, Bittornado ect. The program which allows the BitTorrent-based P2P file sharing between two or more computers.
[9] There are centralized file-sharing technology's too. The FTP server using the method in which a central computer is linked to more than one client machine. All information will be recorded in the central server, where clients can download them.
[10] Files with .Torrent extension, which contains standard meta information's about the principal file. The standards helps for the readability for the different client software's.
[11] The tracker is a computer application, with the task of providing information to users that who are another users who are downloading (duplication) and sharing (making available) the file too, allowing by this the parallel download of the principal file's data packets.
[12] The checksum is the result of mathematical operation carried out on the data package elements. Operation itself is called the hash. A complex mathematical procedure which is

When a user downloads a data packet, the client can use the hash total to check the accuracy and the completeness of transfer.

The user uploads the torrent file to a website, from where other users can download it. If a user other than the original uploader wants to get to the principal file, then s/he needs to run the downloaded torrent file using a torrent client, which initiates the data exchange between the torrent file uploader and the user. During the process data packets of the principal file will be downloaded one after the other.

When the first data packet is downloaded to the second user (first downloader), the tracker will record this fact in the torrent file, and so subsequent downloaders will have the address of both the first uploader, and any other downloaders. From this point the second downloader can download the first data packet from the first downloader and the second data packet from the first uploader simultaneously. From that moment the first downloader will be the second uploader, as s/he is making part of the principal file available too.

The justification of the judgement[13]

Within the meaning of the charge – determined by the Swedish prosecutor[14] – the defendants were aiding and abetting copyright infringements, as they provided others with the opportunity to upload torrent files to the service, provided others with a database linked to a catalogue of torrent files and they provided the opportunity for others to search for and download torrent files and also provided the functionality with the assistance of which individuals wishing to share files with each other could contact through the file sharing service's tracker function. The prosecutor also pointed out that TPB website operators suggested in many sub-sites that they were aware that illegal file sharing takes place through TPB: on the website they published information about letters of formal notices, which were sent to them by the victims of copyright infringement, asking them to remove the torrent files referring to offending content.[15] For establishing the basis of the intermediary service provider's liability the prosecution defined it as hosting, because of the hosting of the database that included the torrent files.

intended to indicate the integrity of data during transmission or storage. The operations before and after trained checksum can help to verify the transmissed data. (Source: http://www.wikipedia.hu – 'checksum' 15 October 2009)

[13] The first instance judgement by the Stockholm District Court in TPB case, translated and published in English by the IFPI (International Federation of the Phonographic Industry). Judgement, p. 15

[14] The International Public Prosecution Office in Stockholm

[15] http://thepiratebay.org/legal

The defendants submitted a defence against the charge: the torrent files on TPB only provided information and are not themselves illegal. The server contains only torrent files and doesn't store any copyright-protected and/or illegal material. As such, TPB servers don't make illegal data transmissions. Their actions weren't at fault, because tracking the torrent files was not unlawful: only the actions of individual users was.

The users' identities or their place of residence were not recorded by the defendant. They were not aware of how the users got the shared files, so it was not possible to know whether it came from illegal sources or not. The defendants said that the services offered by TPB are "mere conduit".

Liability of service providers

TPB website provides a file sharing service which uses the BitTorrent protocol. This website allows users to upload and store torrent files to the website's database. The database, which consists of these torrent files, is always available, and provides technical terms that a user can free search and download related torrent files. The service of operating a tracker helps the users involved in file sharing to make contact with each other.

TPB website provides under the Hungarian e-commerce act[16] (HeC) different intermediary service activities: a hosting service which allows users to upload torrent files through the torrent server; a search engine service which made searches possible to the users of stored torrent files through user-defined criteria; and merely conducting features of the tracker file-sharing service functions helps file-sharing participants to contact each other. [17]

The purpose of the Directive on electronic commerce (DeC)[18] was to join into a common European base infocommunication participants' liability, consolidating the same technological information society service providers liability rules. DeC rules are horizontally scoped, and they are all valid and applicable in the field of law. The rules for freedom from liability for service providers are found in the Articles 12-14 of DeC. In the constituting freedom for intermediary service providers, they can not be held responsible for the transmitted, stored or made-available information.

[16] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (herein after referred to as HeC)
[17] HeC Section 2 Subsection l), la), lc), and ld).
[18] DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce; herein after referred to as DeC)

The Swedish court found that the activities within TPB are electronic services, even if provided free of charge, because through the large number of recipients, the advertising-generated revenue can be assessed as contribution, which is sufficient to establish that the activities are subjects of the Swedish Electronic Commerce Act (SeC).[19] In Section 2 of SeC, information society services are specified as services which are normally provided against payment, and which are supplied at a distance, electronically and at the individual request of a service receiver (the user of the services).[20] The court accepted the prosecution's position, and rejected the application of freedom from liability for hosting. The reason for this was that the operators – although they were aware that torrent files from illegal principal files are located on TPB server – have not shown positive action to remove these files.[21]

The defendants have not differentiated the various features of the site, and have asserted that the tracker service is simple data transfer process (mere conduit). The freedom from liability provisions for mere conduit activity of DeC are similar in Swedish and in Hungarian law. The mere conduit provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission, and does not select or modify the information contained in the transmission. [22]However, the prosecution might have said that the tracker service establishes the connection between individual users when it sends, via the initial torrent file, information about the location of the principal files data packets. That means the rules governing freedom from liability are not applicable.

The accomplices carried out by omission

The case for complicity in TPB case is based on breach of copyright law: the punishable offence (the principal offence) was making available of copyright works to the public without the permission of the copyright owner.[23] Under Section 53 of Swedish Copyright Act, *anyone who takes actions which involve infringement of the copyright associated with the work can be sentenced to a fine or imprisonment for a maximum of two years, provided that the infringement was intentional or the result of gross negligence*. Section 53 Subsection (5) of the

[19] The Electronic Commerce and Other Information Society Services Act
[20] HeC Section 2. point f.) 'Information society service' shall mean services provided electronically – normally for financial consideration – at a distance and at the individual request of the recipient of the services; The justification of the Minister of Law about HeC says that it's include any service provided free of charge, which does not belong to the field of the freedom of expression.
[21] SeC Section 18.
[22] DeC Art. 12., HeC Section 8 Subsection (1)
[23] Judgement, p. 35

Copyright Act states that *an attempted breach or preparation of breach of the Copyright Act is punishable pursuant to Chapter 23 of Swedish Criminal Code*.

Provisions for sentencing a person for complicity in breach of copyright are included in Chapter 23 Section 4 of Swedish Criminal Code which states *not only the person who committed the act can be found liable, but so too a person who aided and abetted the act in word or deed.* The Code also prescribes that this shall apply to any action for which a prison sentence can be imposed under other laws or statutes. Punishment as provided for an act in this Code shall be imposed not only on the person who committed the act but also on anyone who furthered it by advice or deed.

The District Court made some important findings: the abettor's liability can be established against a person who contributes slightly to the perpetration of the principal offence. The District Court has concluded that the District Prosecutor has succeeded in proving that the alleged principal offence has taken place in the way claimed. There is no requirement for the perpetrators to be known for liability for complicity to be considered. The District Court has already stated that it is sufficient for the District Prosecutor to prove that the objective requisites for the principal offences have been fulfilled. If a certain action is regarded as having aided and abetted the principal offence, liability for complicity comes into play. However, that the perpetrator is not punishable because of lack of intent does not mean that this crime's abettor would not be punishable. So the Court held the perpetrators guilty in the crimes described in the indictment.

The Hungarian legal framework related to these issues does not show significant difference. An accomplice is a person according to Section 21 of Hungarian Criminal Code who knowingly and voluntarily helps another person commit a crime. There are three circumstances that I need to prove here: that there is a principal offence, that it relates to the intentional accomplice conduct, and that the act assists the principal offence.

The principal offence according to Hungarian regulation

The principal offence for file-sharing is the infringement of certain rights related to copyright.[24] There are two questions which I need to answer: what is the criminal conduct, and what is the result of the crime? For the use of copyright

[24] Hungarian Criminal Code Section 329/A.
(1) A person who infringes the copyright or certain rights related to copyright of another person afforded under the Copyright Act for the purpose of financial gain or advantage and/or thereby causing pecuniary injury, is guilty of a misdemeanour punishable by imprisonment of up to two years, community service work, or a fine.
(2) Any person who fails to pay the blank media fee or reproduction fee that is due to the author or the holder of a right related to copyright afforded under the Copyright Act in respect of copying for private purposes shall be punishable in accordance with Subsection (1)

and related rights of protected works, the copyright owner's authorization is required. There are, in the HCA, named forms of the use which are relevant in this case: reproduction and making available. [25]

If someone downloads a torrent file relating to a copyright-protected work, that doesn't in itself constitute unlawful conduct. If the user executes this torrent file assisted by the torrent client, then – ideally from the user's perspective – it will start downloading the file. That is a reproduction. If the work is from illegal sources the fair use does not come into the scope in the opinion of the Council of Copyright Experts.[26] When the downloaded files – either the entire file or some data packet – become available for others, we can speak about making available. [27]

For the result of the crime it is important that the HCA Section 16 Subsection (4) says *'Unless otherwise provided by this Act, remuneration shall be due to the author against the licence s/he has given for the use of his/her work, which remuneration – unless otherwise agreed – shall be proportional to the revenue earned by the use of the work'*. Both for the legal reproduction and making available such a licence is necessary. If somebody operates without these conducts it is illegal as it causes loss of financial gain because to be legal they would need to pay for it. Pecuniary injury means damage (the loss of value of one's property) and the loss of financial gain. However, it is difficult to prove the loss of financial gain, because if the offender just downloaded the copyright protected work, which in his view was free, if it was not available for free download, then he might not have bought it.

This means that the victim had been incurred in respect of loss of financial gain because this is exactly the amount it would have been charged by the legitimate purchase of the work would have paid. Because the perpetrator without the

[25] Hungarian Copyright Act (herein after referred to as HCA) {1999. évi LXXVI. törvény a szerzői jogról}: Section 18: *The author shall have the exclusive right to reproduce his work and to grant authorization therefore. Reproduction shall be taken to mean: a) the direct or indirect fixation of the work in any manner on a tangible carrier, whether definitively or temporarily, and b) the making of one or several copies of the fixation.* Section 26 Subsection (8): *The author shall also have the exclusive right to communicate his work to the public in a manner other than broadcasting or the means referred to in paragraph (7) and to authorise anyone therefore. This right shall cover, in particular, the case when the work is made available to the public by cable or any other means or in any other manner so that the members of the public may access these works from a place and time individually chosen by them.*

[26] Council of Copyright Experts No. SZJSZT 07/08/1. expertise and No. SZJSZT 17/2006. expertise

[27] HCA Section 16 Subsection (1): *By virtue of the copyright protection, the author shall have the exclusive right to use his entire work or an identifiable part thereof in any tangible or intangible form and to authorise any such use. (*"Identifiable part" criterion is meaningful sharing of movies, but for software is no longer so clear.)

potential absence of the free download would not have concluded a contract for pecuniary interest, there is no pecuniary injury. [28]

Assistance as the conduct of the accomplice

In TPB case the fundamental issue was in the aspect the liability of the accused: did they perform any kind of conduct which can be interpreted as assistance? The Court decided that the perpetrators have aided and abetted the principal offence by enabling users to upload and store torrent files for the file sharing service of TPB by providing a database linked to a catalogue of torrent files, by enabling users to search for and download torrent files, and by providing the functionality with which users who wished to share files could contact each other through the file sharing service's tracker function.
The complicity was based on the fact that TPB functioned as meeting points for file-sharing users. The accused developed TPB to ensure that the technical capacity of the site contribute effectively to the needs of users of file-sharing.[29]
The torrent technology's fundamental objective is that the files what you want to share with others on the internet through the communication / data transfer functions are forwarded to those who want the file copied. Therefore, the technology function is that the transmission of files is achieved efficiently. This technology is determined by the process, regardless of whether the currently transmitted data is illegal or not. It can be concluded that the technology promotes the reproduction or the making available of the principal file.

The intent of the accomplice

The defendants said that they were not aware of any copyright infringing file-sharing, so their intention is not to extend the offences' underlying facts, against which they could do nothing.
The subjective prerequisite must be fulfilled, not only with respect to the aiding and abetting itself, i.e. co-perpetration, but also with respect to the act which constitutes the principal offence. Complete agreement between an accomplice's view of the course of events and the actual course of events is not, however, a requirement. In assessing the level of intent which must be present, each individual principal offence should be considered.[30] The defendants intent does not, however, have to cover the specific works which it is alleged have been made available. It is, rather, sufficient for them to have had the intent to bring about the existence of copyright-protected material on the website.

[28] Presentation of Dr. LLM. Nagy Csongor I. (PhD)
[29] Judgement, p. 48
[30] Judgement, p. 51

The examination of the defendants, the letters from right holders published on the website, TPB, and the e-mail correspondence indicating that the operation involved pirate copying, make it clear that the defendants have been aware that copyright protected works were available via the website, and were shared via the tracker embedded within the framework of TPB's operation. Despite the knowledge they don't do anything to protect the copyright holders.

The basis obligation which establish the omission in the Hungarian legal environment with reference to different legal solutions

1. The omission in the criminal law

The criminal conduct of complicity is assistance, which can be either active or by omission. Omission is not just a simple inaction: in this context, it means that there is an obligation to do something, but against the obligation, the accomplice does nothing. The statutory obligation is based, inter alia, on an act, or a relationship in civil law, or an administrative decision, or on the perpetrator's prior act which established the risk of injury or harm (those are, to a certain extent, non-legal norms). If the principal offence is realized through the help of the website's tracker, the operators are assisting: if the website operator was obligated to terminate infringing activity, and s/he – in spite of the knowledge about this fact – does not prevent further violations, can be liable for the omission.

The operators of a torrent technology based website actually have the opportunity to modify the tracker function. They can influence the sharing of information through the tracker, they can prevent the sharing of information about the "owners" of a principal file. Here, however, a fundamental question arises: what are the appropriate obligations for a service provider? When s/he gets the knowledge about those facts, does this give him/her an obligation to do something?

2. The obligation's for the service provider's in HeC

HeC Section 7 says that the intermediary service providers shall not be required to monitor the contents of the information which they transmit or store or provide access to, nor shall they be required to actively seek facts or circumstances indicating illegal activity. This concerns cases where the provider hasn't got knowledge of any involving illegal content.

Is there any general obligation for the service providers to do something when he gets knowledge that somebody uses his/her services for an illegal operation? Is there any obligation from the perpetrator's prior act which established the risk of injury or harm in the case of a website based on file sharing technology? We can say definitively that there isn't such an obligation. While the owner of the house can be held liable if s/he fails to do the necessary repair work, and therefore a

fallen part of the roof causes injury to someone, s/he can not be held liable because the tenant of a house throws a plant pots out of the window which injures someone. Similarly, the intermediary service provider can't be held directly liable, because the recipient of the hosting service conducts illegal activities. Furthermore, it can be expected that the service provider in some cases assists in the elimination of illegal activities. Those contributions may be required from them.

There are three different situations, in which the service providers must do something to earn freedom from liability.

HeC Section 7 Subsection (5) says *'The exoneration of the intermediary service provider from liability according to Subsection (2) shall not affect the possibility for the person who has sustained any injury by way of the information with unlawful content to enforce his claims stemming from the infringement in front of a court, including the requiring of the intermediary service provider – in addition to the infringer – to terminate or prevent an infringement'*. In this case the obligation for the conduct comes from an act, directly from an administrative decision. This obligation is for all kind of intermediary service providers for any crimes.[31]

In other cases there are obligations on conduct for hosting and search engines service providers in any kind of crimes. HeC Section 10 and 11 say:

The intermediary service providers (hosting, search engine) shall not be held liable for the information stored at the request of a recipient of the service, on condition that:

a) the provider does not have actual knowledge of illegal activity in connection with the information and is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b) the provider, upon obtaining knowledge or awareness of what is contained in Paragraph a) acts expeditiously to remove or to disable access to the information.

The third case comes from the notice and take-down process, regulated in Section 13 of HeC. It's only applicable for the host and search engine service providers, and only in relationship with HCA and the Act on the Protection of Trademarks and Geographical Indications. In this case, conducting the notice-and-takedown process is a part of the obligations which the service provider must perform for freedom from liability. The aim of the notice-and-takedown process, according to the justification of the Minister of Law about HeC, is to ensure to the copyright holder the removal of the suspected infringing content before civil proceedings.

However, that rule does not help to resolve issues related to criminal liability.

3. The positive obligation from the knowledge of an infringing act

The Swedish court in its decision was not obligated to take into account the notice-and-takedown process. In its decision the court claimed that the

[31] The mere conduit service provider's criminal liability can only be based in this situation.

perpetrators knew of the violations, but nevertheless did not prevent them, even though they are, as hosting service providers, required for action if they have the knowledge. Given that any aid is sufficient to establish complicity, the prosecution case was well founded. So it did not need to take into account the assistance of the search engine, or the mere conduit process in connection with the conduct of the nature of complicity.

According to the German legal literature (and it appeared in the TPB's decision too), the knowledge (*Kenntnis haben*) of foreign content should be construed as a positive knowledge. This means that general notices that the service provider provides various illegal contents are not a sufficient statement of the knowledge of illegal content.[32] The intention (*dolus eventualis*) is already establishable when the provider, despite detailed, credible and sufficient information, doesn't try to check the illegal act of making available, even though it would be possible for him.[33]

An additional requirement of knowledge is that the positive obligation must be for only unique and specific information. For that, the service provider needs to know the exact location of the illegal content. The information that somewhere illegal content found on this server is insufficient.[34]

4. Problems of interpretation in the notice-and-takedown process

A related observation about the knowledge is that in the notice-and-takedown process it is not necessary to say that the service provider has sufficient knowledge to establish his/her liability. This means that before the notice-and-takedown process, we can handle the service provider's criminal liability, so that there is no need for the notice-and-takedown process. Except in the situation that we recognize that without the notice-and-takedown process – which is the normal way of the removal of infringing content – we may not impose on the provider criminal liability, and omission can not be established if s/he takes part in the take-down procedure.

The takedown process starts with a notification, whose form and content requirement is regulated in HeC.[35] In this case, when the notice's substantive

[32] Spindler, G.: Dogmatische Strukturen der Verantwortlichkeit der Diensteanbieter nach TDG und MDStV. MMR 1998, p. 641

[33] LK-Schroeder (Fn. 70) § 16 Rn. 93

[34] Hilgendorf, F. V.: Computer- und Internetstrafrecht. Rn. 306.; Spindler, ibid p. 641; Compuserve case: MMR Multimedia und Recht 1998, Heft 8. p. 429; Urteil des AG München gegen den ehemaligen Geschaeftsführer der Compuserve Deutschland GmbH, Herrn Felix Somm, http://www.jura.uni-muenchen.de/sieber [Downloaded from 3 October 2004]; Moritz, H.-W.: Entscheidungsanmerkung zum Urteil des AG München vom 28.05.1998 (Somm-Urteil), CR 1998, p. 505

[35] The notification shall contain: the subject-matter of the infringement and the facts supporting the infringement; the particulars necessary for the identification of the illegal

and procedural requirements are perfect, and the intermediary service provider receives the notification, s/he has 12 hours to take action. S/he need to not guarantee access to information or to remove the information. On this basis, if the service provider within 12 hours fails his obligation, with that omission s/he helps to commit a principal offense. A notification which was received via e-mail, that does not have a certified e-signature, is not capable of starting a takedown process, because this is a requirement of HeC.

Problems could arise due to procedural error, if something is not appropriate with the notification, because such a notification is not suited to place obligation on the intermediary service provider. The question is, in such situation, should we apply criminal law to the service provider for the reason that s/he did nothing, despite having knowledge about the exact location of the illegal content, because the notification included such information. HeC Sections 10 and 11 create obligation for such an act, when a host and search engine service provider gets knowledge about illegal content. If we accept that knowledge is different from the requirements set out in takedown proceedings, and that creating an obligation to act is the basis of the freedom from liability rules, then we don't need the takedown process for a criminal procedure. In principle, the takedown procedure constitutes one more obligation for the freedom of liability exemption. If a service provider fulfils these obligations, s/he will released from the challenge. What happens when the service provider disputes with the copyright holder about the legality of the notification?

Suppose that the parties question the lawsuit of the court. During the trial, has the service provider any obligation to remove the illegal content? From the service provider's side the argument is well founded, if s/he thinks that the notification is wrong: s/he protects the service recipients. In this case, how may one develop a case for criminal liability?

It is certain that, until this issue is resolved, the criminal court can't pass sentence, because it may lead to the conclusion that after a winning position with a release from civil liability, the criminal liability is established. At the same time it also means that if the civil court found that the notification of the takedown proceedings were legal, then the service provider immediately will be responsible with the rules of criminal responsibility. This situation is contrary to the purpose of the legislation.

Conclusion

The biggest contradiction in Hungarian law is that in copyright infringement cases, the removal procedure makes a uniform interpretation difficult. As with

information; the proprietor's name, residence address or registered office, phone number and electronic mail address.

other illegal content (e.g. illegal pornographic images) there is an obligation for action by the service providers after becoming aware of the infringing content, and in the area of copyright, where the awareness is in connection with takedown process-related rules, this obligation satisfies a number of conditions.

The criminal liability of intermediary service providers would set a difficult task for the application of the law. Difficulties arise from the interpretation of the current regulatory environment about service providers who are using torrent technology based file-sharing.

Therefore, it would be appropriate to extend the rules of notice-and-takedown procedures against the spread of illegal content, while strengthening the relationship between the obligations which comes from the notice-and-takedown procedure, and which comes from the freedom of(?) liability basic rules.

DAVID ANTHONY KARLA[1]

Music File Sharing

The War Between Industry and Consumer

In the wake of two recent high profile cases against BitTorrent trackers, the (successful) Swedish case involving The Pirate Bay, and the (unsuccessful) UK case against a similar site, OiNK, it is clear that there are basic confusions about the fundamentals of file sharing in the legal community, both technically and sociologically, and that there is a sense of desperate and aggressive directionlessness coming from the music industry bodies that is leading them to alienate the people they should be trying to reach.

Basic Definitions and technologies

There are important distinctions here that many legal authorities and public commentators on this issue have not made and do not seem to understand. In very loose terms,

- A 'protocol' is a collection of agreements about the how data is transmitted between computers. Typically, in a single communication, there are several different protocols in use at the same time, each handling different levels and aspects of the communication.
- A 'format' or 'encoding' is a simply a way of storing and/or transmitting digital information, and it typically refers to the layout of a static file. For digital media files, these terms are largely interchangeable.
- A 'language' is a type of format that allows a high degree of expression and flexible structure.

Thus, what we call 'The Internet' is simply the collection of computers and assorted machines that communicate over public channels (wire, satellite, radio, optical cable, etc) using the TC/IP and DP protocols. The 'Worldwide Web' is the collection of machines connected to the Internet that serve documents in the HTML language using the HTTP protocol. Your web browser understands HTML to represent a layout of words, images and references to other HTML documents on the web. Simple, complex, and a can of worms ready to spring open. Your 'true name' in this can of worms is a sequence of four dot separated numbers, called an IP address: generally, this is assigned to you by your ISP, and may vary with time.

[1] David, A. K., multimedia programmer

Sound Media Formats

Digital music is generally stored as a sequence of snapshots of an acoustic signal called samples. The characteristics of this process which affect the overall perceived quality of the reproduced sound is governed by the choice of sound media format, and includes: sample rate (the number of samples per second that constitute the sample), sample size (the level of accuracy of an individual sample), and bit rate (this is the amount of storage space devoted to storing a second of music, so it is related to the sample rate, size and any compression that a particular format might use).

Formats for sound media can be classified in two main ways. A 'lossless' format is a format that can be converted directly and precisely back into the stream of samples that constitute the original digital recording. A CD consists of raw data at a sample size of 16 bit and a bit rate of 1411.2 Kbit/s. Formats such as wav and aif preserve this information exactly, but provide meta data that allows for higher sample sizes and sample rates: they are typically used in quality audio recording. Formats such as flac and ape are similar to these, but they also offer a small amount of file compression. Typically these formats are offer a file size about half that of the raw CD data.

A 'lossy' format is one in which some audio information from the original recording is omitted to enable higher compression. They cannot be converted back into the full original stream of samples. The classic version of this is MPEG1 audio layer 3, commonly called MP3. In this patented approach, frequencies that are considered 'not perceptible' are removed from the signal, allowing for lower file sizes. For music, this generally gives typical bitrates between 128 and 256 Kbit/s, and files are typically one tenth the size of the original CD data. There are many variations of this algorithm which have different perceived levels of quality. Different programs have different approaches to this 'perceptual encoding', so even at the same level of compression, not all mp3 files will be identical in sound. For many circumstances, a program called LAME[2] is a very popular choice for balancing quality with compression.
Several modern formats such as AAC and WMA provide options to store music in either a lossless or lossy form.
Generally low bit rate formats are ok for a mobile telephone or portable media player. A home sound system with definitely bring out the deficiencies and will need a higher bit rate medium (say 256 Kbit/s). Audiophile or professional audio systems, such as used by a DJ or for broadcast media, will bring out the weaknesses in all but the highest quality media: here, typically only full CD quality will suffice.

[2] 'Lame in not An Mp3 Encoder' so called because it is free and open source, and is not published as an encoder, but as a teaching tool for learning about encoding. This is a nicety to get around certain software patents.

Client-server file transfer protocols

In protocols in this style, a single machine, the server, communicates with and provides services, such as storing and retrieving files, for other machines (the clients). Most legal music services fit into this category, as well as several of the illegal or quasi-legal services. Typically these services use the File Transfer Protocol (FTP) or a variant thereof to distribute media files.

Peer-peer file transfer protocols

A peer to peer (P2P) network is just a collection of machines in which connections are established between machines without a hierarchy. It's an important distinction, but in practice, all it means is that any participant in the network can take the 'client' role or 'server' role, or perhaps both simultaneously.

There are two significant P2P protocols used to exchange audio files. Both of these protocols are 'paradigm-breaking', as they drastically change aspects of how digital music is shared, and both are associated with strong online communities. Both protocols have fully legal and legitimate purposes that are highly beneficial, and they can also be used to enable the exchange of copyrighted material.

Slsk is the protocol used by the Soulseek[3] network. It allows users to privately publish an index to selections from the digital music stored on their personal hard-drive, and to allow other users on the network to download this music directly from their hard drive. The network operates using a specific computer program, 'Soulseek'. Downloading is via the FTP protocol, and so is usually quite slow, limited by the speed of the internet connection of the machine which is storing the music. However, it is interesting on several levels. First it lets you browse the personal music collections of strangers located anywhere on the network: for music lovers, this is always fascinating, and leads to many discoveries. It also strongly supports the growth of a community around the sharing of music: certain people may be blocked (particularly if they do not participate in the sharing of music); mutuality is encouraged, as it is possible to browse the collection of people who are downloading music from you own hard drive ('if someone likes what I like, maybe they will have something that I would enjoy in their collection'); independent artists may use this to publish their own work, and Soulseek has an independent music label which has grown from this.

BitTorrent is the file sharing protocol used by most other P2P music networks and services. There are a few variants to it that use other names, and that are tied to particular networks or programs e.g. LimeWire, EMule, EDonkey, but these are in essence just a rebranding of the original. It was devised by programmer

[3] http://www.slsknet.org/

Bram Cohen in April 2001. Cohen himself developed the program as an intellectual exercise, as a means to download large files in an efficient distributed manner, and claims that he has never infringed copyright[4].

The protocol has many legitimate purposes, in particular the downloading of large open source software packages, such as full distributions of the Linux operating system. While it not perhaps as culturally innovative as the Soulseek approach, it is an ingenious breakthrough that allows for very fast dissemination of media files to a large number of users, and for this reason, it is the web sites and communities that use bittorrent that have put the major record companies on the back foot, and it is involved in most of the legal cases brought against file-sharing users and web sites. To see why it has generated this attention, and why many of these cases have foundered, it is unfortunately necessary to get a general understanding of how bittorrent operates.

Bittorrent

A shared file is conceptually (not literally) divided into pieces, and a numerical hashcode, typically SHA1, is taken of each particular piece to ensure the accuracy of the data once it has reached a user. The information describing the pieces of the media file, the hash codes, and the IP address of people who are connecting to the torrent, both people who are downloading and people who are uploading, is placed in a file called a torrent file. The torrent file can be read by a special program which understands the bittorrent protocol, and which initiates the connection to the actual data, and handles the download. There are several different programs available which use bittorrent: BitTorrent (Bram Cohen's original program), µTorrent, and Azureus, to name a few. Generally the torrent files can be created by the BitTorrent program.

The users who are connected to a torrent at any particular time are collectively called the 'swarm'. Users who have all the pieces to a media file are called 'seeds', and users who have only some of the pieces are called 'leeches'. BitTorrent sites, generally called 'trackers', such as Pirate Bay, do not store any of the copyrighted media. They merely index the torrent file. The data is stored and uploaded initially on the machine of the person who first shares the file.

Once the initial seed has published a torrent, and someone has connected to it to download the data, the seed will begin uploading the elements of the file, piece by piece. Once a user connected to the torrent has received and verified (with the hashcode) a piece, he will be also offering that piece for download. At any point in time, most leeches in the swarm will be simultaneously uploading and downloading. This leads to a file transmission protocol that is both resilient

[4] Clive, Th.: "The BitTorrent Effect".
http://www.wired.com/wired/archive/13.01/bittorrent.html. (Wired. January 2005)

(because in the right circumstances it is proof against any connectivity failure of any individual seed), quick (because eventually pieces may be simultaneously downloaded from a large number of sources), and relatively painless bandwidth wise for the original uploader (because he is sharing the strain with other seeds and leeches). Thus, it is an ideal medium for distributing large files such as operating system distributions, for distributing music files in lossless formats, and for small music labels and independent artists for whom this saves precious bandwidth.

It is even conceivable that the original uploader of the file could leave the swarm. The file being shared may at times not even exist in its entirety in one person's hands. For instance, one user may have half the pieces, and be exchanging pieces with another user who has the other half, and both could simultaneously be sharing their halves with another user who has just joined. The point is that it is not necessarily a simple task to decide who is 'sharing' and who is 'copying'.

An important aspect of modern versions of the protocol is the distributed hash table (DHT). This has been possible in some form since 2005 and means that the 'tracker' is not actually necessary for the running of the torrent, as the tracker database is shared and distributed across the whole swarm. Some tracker sites have specifically not taken advantage of this, as they try to keep their swarms associated only with associated member-users.

However, since November 2009, The Pirate Bay has enabled this feature. In such swarms, all that is necessary is a torrent file to make the initial connection, and if the tracker site is closed down, the active swarms can continue. In such a situation, the torrent files can be distributed without 'tracker' websites, over email, or through online chat, and torrent-based sharing becomes largely unstoppable. Other technical 'solutions' to torrent based file sharing are likewise bound to fail. Deep Packet Inspection (DPI) is easily defeated through the use of virtual private networks (VPN) and encrypted proxies.

Other sharing technologies

The last 10 years have seen the growth of portable USB flash drives to reasonable sizes. It is now possible to share with friends a substantial amount of music within minutes. I know of no survey which says how prevalent this is, but I suspect that many who would not use a torrent based service are more than happy to swap files with friends on such small devices, and I think perhaps that as much music as is swapped over the internet is swapped by these much simpler technologies.

Similarly, 'push' technologies on most mobile devices enable the sharing of individual songs with great ease and frequency, and it is unlikely that anything can or will be put into place to prevent this.

Recording companies, contracts, labels, and artists

Generally the people prosecuting sharers or sites that facilitate sharing are representatives of people who own the copyright of the recordings. In most cases, these people are not the artists, not the authors. They are typically large corporations. In the end, four large corporations (Warner Music Group, EMI, Sony Music Entertainment, and Universal Music Group) control 70% of the worlds recorded music by volume.[5]

What is the situation for the musicians at the coalface then? Traditional record deals are generally a bad situation for most artists. Record company estimates are that less than one in seven albums is successful, in terms of recouping production costs[6] (and the artist will not get paid until those costs are recouped). Even in the best case, it is very unlikely that the artist will be making more than 5% of the retail price of a CD[7]. From this they will need to pay costs (recording, advertising, video production) […] to the record company, plus interest: yes, that advance you took was actually a loan with a ridiculous interest rate. On the other hand, the company is already making a sizeable cut from the retail price (closer to 30%). Very few records do better than break even for the artists, though the corporations will do quite well. Independents are a little bit better for the artist, though in general distribution and sales networks are tied to deals by the recording cartels. It is also not an uncommon practice for the cartels to 'sign up' bands that they perceive as competitors to either established or highly promoted new acts, and then to keep them in limbo to avoid confusing the consumer. This is not the activity of someone who is interested in fostering young artists, a cry that seems to be heard frequently when the media cartel spin doctors talk to the press about file sharers. Advances in the last decade, such as affordable quality home recording, independent CD production and stronger independent labels have seen these kinds of practices diminish, but not disappear: and for a band, the price of independence is losing access to those distribution networks.

These large cartels are now struggling, and, searching for someone to blame for their financial woes have principally targeted file sharers. They have spent a lot of time, effort and money in lobbying governments to put draconian legislation in place. In the EU, this is typified by the mire surrounding the current ACTA agreement. In a moment of almost pure Kafka-esque absurdity we have the European Parliament threatening to sue the European Commission over the secrecy of these negotiations[8].

[5] http://www.oligopolywatch.com/2003/06/28.html
[6] http://www.docstoc.com/docs/29031798/ANATOMY-OF-A-RECORD-DEAL
[7] http://www.kzfr2.org/blog/record-industry-profits-distribution-breakdown
[8] http://www.out-law.com/default.aspx?page=10825

Yet there is no clear link between the cartels' estimates of 'losses due to file sharing' and reality. In fact, several studies have suggested the opposite. In an economic model by Harvard University and the University of North Carolina it was estimated that it took 5,000 downloads to displace the sale of just one physical CD[9]. Typically people will download music that they would not pay for. And a recent survey in the UK suggests that it the biggest downloaders of free music, are also amongst the biggest spenders on music[10]. Another study[11] suggests that even in an era of increased file sharing, artistic output is on the rise, relatively. This same study, from Harvard Business School, found that on a typical portable player with 3500 songs, on average, 65% of those songs were never played, further suggesting that much of the music we possess is not music that we would pay to own.

The amount of money the cartels are losing, and the dents into the retirement funds of dinosaur rock acts, have perhaps been overestimated. Although it is clear that the profits of the record industry have contracted over the last 10 years, there are many possible causes for these losses other than a growth in filesharing.

- The general economic climate: people have less disposable income to spend on music.
- A general flabbiness, inefficiency and all around corruption in the industry. This has certainly been the case of the situation with EMI, the biggest struggler at the moment, taken over in 2007 by someone outside the industry, who found that there were interesting budget items that had very little to do with music or art[12].
- The rise of gaming and DVDs in the same target market.
- Changes in musical tastes, such as the rise of the dance music industry: people in this community are perhaps likely to collect less, and spend more money going to events where professional collectors (ie DJs) present their collections.
- Unbundling of the album. This is definitely an important factor, especially with the growth of online services such as iTunes: the costing of production and recording is generally in units of 'album'. For most consumers though an album means the hit single they like, 3 songs that aren't too bad, 4 pieces of filler, and the rest which could for all intents and purposes be consigned to a digital void. Digital downloads reflect this: whereas in the past, a fan would buy an album, with all it's great artwork and imagery, now (unless she wants to own the cd) she can just download that one fantastic single.

[9] http://news.cnet.com/2100-1027_3-5181562.html
[10] http://www.demos.co.uk/files/DemosMusicsurvey.ppt
[11] http://www.hbs.edu/research/pdf/09-132.pdf
[12] http://www.businessinsider.com/2008/1/emis-400000-coke-and-hookers-budget

- The rise of successful online marketplaces such as iTunes, and the cartels' failure to provide a digital service that customers would want at a fair price.
- A general missing of the plot, and failure to have a desirable product. An anecdote from an EMI focus group tells of a group of teenagers being invited "to help themselves to a big pile of CDs sitting on a table. But none of the teens took any of the CDs, even though they were free. 'That was the moment we realised the game was completely up,' says a person who was there"[13]. Personal taste perhaps, but one school of thought believes that if it hadn't been for the invention and marketing of the CD getting people to replace their existing vinyl collection, for a couple of these cartels, something brown and slimy would have hit an electrically driven breeze generator 20 years ago.

And how have the cartels responded to this situation. As well as taking the bittorrent-facilitating websites to court, with mixed success. They have taken to attacking their own customers. These instances of heavy-handed court cases for copyright offences are well known and well documented. Mostly, they have been unsuccessful, and in the two or three major successes, the judgments have been well out of proportion with the offenses. Likewise, they have not had any noticeable deterrent. A different response was taken by Sony Music Entertainment in 2005. They included a very serious copy protection mechanism which put what is known as a rootkit on a user's computer to limit copying if the music CD was placed in an unprotected computer. Generally this is the kind of thing done by the writers of viruses and Trojans. This is a serious computer offense in most jurisdictions, generally regarded as a criminal act (as distinct from copyright infringement which is in most jurisdictions a civil offense). Interestingly, the computer program so installed infringed the copyright of several other computer programs as it had included pieces of these programs without appropriate licensing.

The Consumers

Here is a typical comment by a typical user on the closure of torrent tracker OiNK after pressure was applied by the British Phonographic Industry (BPI): "I'll admit I had an account there and frequented it quite often. At the end of the day, what made OiNK a great place was that it was like the world's greatest record store. Pretty much anything you could ever imagine, it was there, and it was there in the format you wanted. If OiNK cost anything, I would certainly have paid, but there isn't the equivalent of that in the retail space right now."[14] The user in this case is Trent Reznor, founder of Nine Inch Nails, a very successful band, and someone who, one would think, would be supporting the position of

[13] http://arstechnica.com/old/content/2008/01/state-of-digital-music-2007.ars
[14] http://nymag.com/daily/entertainment/2007/10/trent_reznor_and_saul_williams.html

the major labels. Instead, he underlines much of the case for the need for a new solution to digital recording distribution and a better deal for musicians and consumers.

Currently, there is one online seller that is truly succeeding. This is iTunes. It provides access to 11,000,000 songs at prices up to $1.29US for popular songs, at bit rates ranging between 128 Kbit/s and 256 Kbit/s. 20% of the music is encumbered with digital rights management, which restricts the uses to which that the music tracks could be put to. A few years ago, this figure was 100%. This may sound like a lot of music, but it is in fact a very small and specific amount of music relative to the amount that could be there.
One nascent service provider, Spotify, is gaining some interest and some success, though it is yet to turn a profit. It is basically providing streamed music on demand.

Against these two, we have a complex ecology of illicit services, and the battered corpses of the failed attempts to create a viable online market for music.

If we accept the previously mentioned survey results, it seems a distinct possibility that the illegal services are working because they are providing a service that the established music industry can't fit into. As Trent Reznor points out, they simply are providing a better shop. How and Why?

- Price. You can't beat free. If we believe the previously mentioned surveys, this might not be the important reason, but it is the one to get out of the way: it is the one that the cartels are looking at. If I buy a CD's worth of songs from iTunes, I am paying nearly as much as an album: given the sound quality, this does not really seem like fair pricing.
- Audio quality. File sharing is often of lossless formats such as flac or ape, or high quality mp3 (variable bit rate or greater than 256 Kbit/s). The best that legal download sites provide music at a quality too low to be considered high quality, at 256 Kbit/s or less. Certainly this is useless for audiophile use, for professional playing (ie DJ'd), or for broadcast media. But even if for the consumer this lack of quality is telling. If a purchaser has a small low quality phone, she might want to make audio files at 128 Kbit/s, to allow more songs, for her car she might want a higher quality. At home, she'll play everything from level zero variable bit rate files into decent speakers, and she'll back up the lossless originals as flacs on a Blue Ray Disc. Unfortunately, she can only buy these 256 Kbit/s files legally. And of course, if music files start being sold in lossless formats, P2P protocols such as bittorrent will start to come into their own.
- Choice. Much music is not released to legal file sharing sites. In fact, much music is still not available on CD, and several uploaders to illegal torrent sites specialize in these 'vinyl rips'. And even of music that does have a legal digital release, much of it still lies buried, as it is not considered popular or marketable. Some is also tied up with contractual difficulties: think, obscure bands such as The Beatles.

- Community. Sites such as Soulseek, and some private trackers, such as OiNK, provide different music-loving community, ones that share music, and share ideas about music, can suggest interesting music to investigate.
- Musical exploration. Most music downloaded probably would not be bought on the marketplace. It is downloaded for exploration. Some people download on a 'try before you buy' basis.
- The increasingly poor reputation of the major labels. The Sony rootkit fiasco made few friends, and neither does the continuing prosecution of tracker sites and filesharing individuals. Rather than discouraging sharers, it is likely to incite rebellious attitudes, particularly in that major music consuming market under the age of 20.
- Freedom from DRM (Digital Rights Management). Attempts to lock down the options for usage using methods such as Apples Fair Play technology, or Sony's rootkit system, have proven to be a bad way to reach an audience. There is a certain ambiguity with which the record production system have viewed their product, and this problem is a symptom of that: at times, the music is 'licensed', unless you want to make a backup copy of the music, or request a fresh physical medium holding the music for which you have 'purchased a license', or transfer the music you have licensed to a different form. The law in this case is vague, and has been slanted to the advantage of the cartels.

Looking forward

What is needed is a solution that provides a fair return to all artists, a fair return to the recording companies (both major and independent), choice and flexibility for the consumer, and recompense for the digital providers.
There are several alternatives, though nothing yet leaps out as being a clear win-win solution for all parties. But now is the time to consider the all the options with a clear mind free from pre-conceptions with the aim of creating such a solution.

PARTI KATALIN[1]

Könyvismertető

Nagy Zoltán András: Bűncselekmények számítógépes környezetben

Nagy Zoltán András, a Pécsi Tudományegyetem ÁJK Büntetőjogi Tanszék egyetemi docense személyében magyar büntetőjogász először vizsgálja teljes terjedelmében a számítástechnikai bűnözést. A kiadvány már csak emiatt is hiánypótló. Emellett a szerző jelentősen megkönnyíti az olvasó dolgát azzal, hogy bőséges példákkal világítja meg az egyes bűncselekményeket. Ilyen módon nemcsak büntetőjogászok, de laikus érdeklődők is könnyedén megérthetik a számítógépes bűnözés jelenségét. A könyvet, amely teljes körű kitekintést ad és részletes tartalomjegyzékkel rendelkezik, joghallgatóknak is nyugodt szívvel ajánlom. A munka ugyanakkor jóval túlmutat a számítástechnikai bűnözés jelenségén, amelynek egyes elemei mára beszivárogtak más, például a gazdasági bűncselekmények elkövetési eszközei közé. A gazdag példatár így nem tisztán a számítástechnika iránt érdeklődők, hanem a bűnözés új jelenségei, a nyomozóhatóságot új kihívások elé állító elkövetési magatartások kutatói számára is gondolatébresztő kiindulópontként szolgálhat.

A címválasztás igen szerencsés. Jó érzékkel kikerüli a népszerű, ám pontatlan „számítógépes bűnözés", vagy az „internetes bűnözés" megjelölést. Ezek a bűncselekmények ugyanis jóval összetettebbek annál, mintsem a jelzős szerkezet kifejezhetné természetüket. A szerző – amellett, hogy nem mulasztja a jelenség gazdag szakirodalmának taglalását – ezt helyesen érzékeli és tudatosan építi fel saját csoportosítását: a számítógépes környezetben elkövetett bűncselekmény középpontjában az adat áll, amely lehet a bűncselekmény eszköze vagy célja. (51-52. o.) A szerző részletes csoportosításában az ET 9 (89). sz. Ajánlásában megfogalmazott ún. minimális listához igazodik.

A könyv tárgyának minden aspektusát taglalja, így a részletes történeti bevezetőt követően felvillantja a számítógép-használattal kapcsolatos pszichológiai problémák mibenlétét. Felsorolja a kriminológiai jellemzőket, úgy is mint a magas látenciát, az okozott (becsült) kárérték összetételét, a cselekmények motívumát és célzatát, valamint a megelőzés eszközeit.

A szerző alapos dogmatikai fejtegetés keretében foglalkozik a bűncselekmények jogi tárgyával. A számítástechnikai bűncselekményeket lényegében azért tekinti speciálisnak, mert szabályozásukra *„a fizikai léttel bíró, testi dolgok védelmére hivatott büntetőjogi eszköz- és intézményrendszer nem alkalmazható"*. (56. o.) E bűncselekmények jogi tárgya nem illeszkedik a Btk. által hagyományosan védett jogtárgyak körébe, hiszen az elektronikus adathoz való jog egyben az információhoz

[1] Parti K. PhD, munkatárs, OKRI

való jog, *„amely ilyen módon nem azonos a vagyontárgyak tulajdonosának vagy jogszerű birtokosának mindenki mást kizáró jogosultságával. Ha így lenne, az információ szabad áramlásának elve csorbulna. Ezen elvnek az érvényesülése a társadalom technológiai, tudományos fejlődésének, az anyagi jólét jobbításának elengedhetetlen feltétele"*. (55. o.) A szerző tehát paradigmaváltást sürget.

Mielőtt új tényállás(ok) keretében szabályoznánk a számítástechnikai környezet bűncselekményeit, alaposan meg kell vizsgálni, hogy a pönalizálandó magatartások újfajta társadalomra veszélyes tevékenységet takarnak-e, amely szankcionálását nem biztosítják már eleve a meglévő tényállások (a tényállások megkettőzésének veszélye: 59., 65. o.). Ezzel persze nem azt mondja a szerző, hogy az önálló tényállások alkotásának nincs létjogosultsága. Ellenkezőleg, egyenesen azt hangsúlyozza, hogy napjaink megoldása – azaz a számítástechnikai bűncselekmények szétszórt különös részi jelenléte – után, a tárgyi oldalon mutatkozó hasonlóságok, szoros összefüggések miatt e bűncselekmények a büntető törvénykönyvek önálló fejezetét fogják majdan képezni. (61. o.)

A számítástechnikai rendszerekbe való jogellenes behatolásról szóló fejezet a *hacker* és a *cracker* tevékenységén túl az érdeklődővel megismerteti a kevésbé ismert *script kid* és *phreaker* kifejezéseket is. A jogtalan adatkikémlelés körében olyan fontos történeti előzményekre tér ki, amilyenek a szocialista-kapitalista társadalmi struktúrák eltérő működési elvein alapultak és a mai napig éreztetik hatásukat a posztszocialista jogrendszerek felépítésében. Míg hazánkban a szocialista államigazgatás a magánszemélyek adatait korlátlanul gyűjtötte, a közérdekű információk az állampolgárok elől rejtve maradtak. Ennek megfelelően ma a posztszocialista országok gyakorlatát a nyugat-európaitól eltérő, ellentétes tendencia jellemzi, amely a személyes adatok védelmére kisebb, a közérdekű adatok megismerhetővé tételére nagyobb hangsúlyt helyez. Kivétel talán a szocializmus titkosügynök-aktáinak megismerhetővé tétele, amelynek szabályai még mindig kimunkálatlanok. (88. o.) A számítógépes csalás kriminológiai jellemzői között a szerző a jelenség jobb megértése érdekében felvonultatja és részletesen magyarázza a modus operandi tipikus formáit, úgy is, mint az adatok *„lóvá tételét"*, a *trójai programot*, a *szalámi technikát*, *malacháton lovagolást* és a csak „veszély esetén" használatos *superzapp* programot. (130. o.)

A számítástechnikai bűncselekmények evolúcióját plasztikusan mutatja be a számítógépes csalásról szóló fejezet, amely a kezdeti kaotikus szabályozást kritizálja. A számítógépes vírus készítését és terjesztését csak valamiféle nyakatekert jogalkalmazói gondolkodással lehetett az akkor (1999) hatályos számítástechnikai csalás büntetőjogi tényállása szerint minősíteni, és ha a vírus nem valamely kiterjedt számítástechnikai hálózat (közérdekű üzem) működésének megzavarására irányult, egyáltalán nem minősült bűncselekménynek. A számítástechnikai csalás tényállását végül az Európa Tanács számítástechnikai bűnözésről szóló (budapesti) egyezményének ratifikálása után módosították, illetve egészítették ki a megfelelő elkövetési magatartásokkal. (139. o.)

A szerző a számítástechnikai eszközökön tárolt szerzői művek jogszabályi védelméről érdekes és tanulságos polémiát mutat be. A jogszabályi szintű konfliktus hátterében az áll, hogy a szerzői művek védelmére létrejött hatályos hazai jogszabályok elavultak, nem felelnek meg az Európai Parlament és a Tanács 2001. május 22-i 2001/29/EK Irányelvének. A szerzői jogi törvény például még mindig nem tesz különbséget az analóg és a digitális másolás között, nem ismeri el a magáncélú digitális többszörözést és nem építette be a szerző kieső díjazásának pótlólagos megteremtésére hivatott rendelkezéseket. (247. o.) A szerző – ehelyütt is a büntetőjog ultima ratio elvét alkalmazva – védelmébe veszi a magáncélú másolást. Rámutat arra, hogy a szoftvermásolás nem tiltható meg büntetőjogi eszközökkel. A büntetőjogi szigornak az üzletszerű másolókkal és a kereskedőkkel szemben kellene csak érvényesülnie. Az internet mint hatékony reklámeszköz bemutatása mellett kételkedik abban, hogy a szerzői alkotások letöltése valódi anyagi veszteséget okozna a művészeknek. Az európai bírói gyakorlatot is latba veszi, amikor kijelenti, a Btk. 329/A. § alkalmazása aggályos a magáncélú másolás és a fájlcserélés ellen. (252. o.) A fejezet nagy érdeme, hogy végül konkrét javaslatokkal felvázol egy lágyabb és egy keményebb utas szabályozási megoldást is, amellyel a tömeges fájlcsere és ingyenes letöltés visszaszorítható lenne. (254. o.)

A könyv az „internet egyéb veszélyei" c. fejezetben olyan, napjainkban közkeletű, tipikus visszaélés-formákat tárgyal, mint a *phishing*, a *kémprogramok* használata, a *flash mob*, a *wardriving* és a *wifi-lopás*. E bűncselekmények megvalósításánál különösen nagy közrehatása van magának a sértettnek. A felhasználók hiszékenységét használja ki az elkövető, amikor pl. a sértettet telefonon felhívja, hogy közölje, letiltották a bankkártyáját, és arra kéri, hogy egy adott telefonszámon adja meg nevét, azonosítóit, bankkártyaszámát, hogy ezzel reaktiválja a kártyáját (*vishing*). (262. o.) A cselekménysorozat első fázisa olyan hagyományos bűncselekményt valósít meg, mint a személyes adattal visszaélés. Az adathalászatnál tehát a hagyományos és a speciális számítástechnikai bűncselekmények elkövetése összefonódik. Emiatt különösen nagy jelentősége van a fejezetek végére beszúrt, prevenciós célú megjegyzéseknek. A hibrid bűncselekmények körébe tartozik a „villámgyülekezés", azaz a *flash mob* is, amely az internet-adta gyors kapcsolatteremtési lehetőséget aknázza ki. Olyan civil kezdeményezés, spontán megmozdulás, amelynek keretében embereket hívnak rövid időn belül meghatározott helyre, valamely békés demonstráció érdekében. A *flash mob* tehát nyilvános rendezvény, amely azonban nem illeszkedik, nem illeszthető a gyülekezési jogról szóló törvény szerinti megmozdulások közé, hiszen lényege a spontaneitás. Bár az Alkotmánybíróság a villámgyülekezést megengedhetőnek minősítette,[2] itt is olyan *„új jelenségről van szó, amellyel kapcsolatban a jogszabályok életszerűvé alakítása kívánatos"* lenne – jegyzi meg alappal a szerző. (271. o.)

[2] 75/2008. (V. 29.) AB hat. (Magyar Közlöny 2008. évi 80. szám, AB Közlöny XVII. évf. 5. szám)

A fejezet végén tanulságos eszmefuttatást olvashatunk a *wifi-lopás* minősítési nehézségeiről. A vezeték nélküli hálózat jogellenes használata – ha azt jelszóval védik – a 300/C. § (1) bekezdésébe ütközik, ám ha a tulajdonosa a hálózatát semmiféle módon nem védi, ez nem minősül bűncselekménynek (sem csalásnak, sem lopásnak) még akkor sem, hogyha a jogtalan használó olyan adatforgalmat generál, amely már akadályozza a jogos felhasználó adatforgalmát.[3]

A szerző gondot fordított arra, hogy az egyes cselekmények szabályozásának ne csak hazai, hanem külföldi – angolszász és kontinentális – elméleti és gyakorlati megoldásait is bemutassa. A kötet talán egyedüli hiányossága, hogy a számos külföldi példa mellett nem tartalmaz elegendő hivatkozást a *magyar* bírósági jogalkalmazásra, kivéve a szerzői joggal kapcsolatos anomáliák bemutatását. (248., 251-255. o.) A joggyakorlati példák kétségtelenül közelebb vinnék az olvasót a hazai jogalkalmazási viták és elhatárolási nehézségek megértéséhez.

[3] Lásd még: Blutmann L. – Karsai K. – Katona T.: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? In: Bűnügyi Szemle, 2008/1. 42–49. o.

KISS ANNA[1]

Iustitia kirándul

(Tanulmányok a "Jog és Irodalom" köréből. Könyvismertető)

Iustitia kirándul – Tanulmányok a "Jog és Irodalom" köréből címmel több mint érdekes tanulmánykötet jelent meg a Szent István Társulat gondozásában. A könyvet Fekete Balázs, H. Szilágyi István és Könczöl Miklós szerkesztették.

A tanulmánykötet a II. Jog és irodalom szimpóziumon elhangzott előadásokat, illetve a később ennek kapcsán felkért szerzők tanulmányait tartalmazza.

A könyv előszavából, H. Szilágyi Istvántól megtudjuk, hogy miért kapta a kötet a *Iustitia kirándul* címet. Sőt, nemcsak kirándul – mint megtudjuk –, hanem előtte még kardját és mérlegét is leteszi. Miért? Hogy meglátogassa barátnőit, a Hellász hegyén. Bár szeméről is levette a kendőt, mégis eltéved útközben, de éppen ezért tud eljutni Európa, valamint Ázsia egyes tájaira, de még az Újvilág déli részét is bebarangolja. A könyvben megjelenő számos tanulmány e kiruccanás különböző állomásait jeleníti meg: a kortárs magyar irodalomból kiindulva, térben és időben is követi Iustitia kalandos utazását.

Bár mindegyik tanulmány önmagában is teljes és értékes (én például arra a bizonyos lakatlan szigetre magammal vinném), a jogalkalmazók figyelmét talán most „csak" két rész kiemelésével ragadom meg:

Mivel a jogalkalmazói munka egyik legnehezebb része éppen a múltban megtörtént bűnös emberi magatartás rekonstruálása, ezért igaza van H. Szilágyi Istvánnak,[2] amikor kritizálja a jelenlegi jogi oktatást, mivel az „alapvetően a szabályok elsajátítására és dogmatikai elemzésére koncentrál, szinte elvétve találkoznak a hallgatók a ténymegállapítás – fact finding – feladatával. Még azokon a tételes jogi kurzusokon is, ahol bírósági döntéseket elemeznek, már előre 'megrágott', a jogilag releváns elemeket kiemelő történeti tényállásokkal van dolguk, ezért magának a tényfeltárásnak a nehézségeiről és buktatóiról vajmi kevés fogalmuk van a hallgatóknak. Holott a történeti tényállás felállítása a jogászi munka egyik alappillére, nem csupán az ítélkezésben, hanem szinte mindenféle gyakorlati jogi munkában."[3]

---

[1] Kiss A. PhD, főmunkatárs, OKRI

[2] H. Szilágyi István a Pázmány Péter Tudományegyetem Jog- és Államtudományi Karán, a „Jog és Irodalom" szemináriumon keretében, a hallgatókkal *Marquez: Egy előre bejelentett gyilkosság krónikája* segítségével igyekszik megértetni a büntetőeljárási megismerés nehéz folyamatát.

[3] H. Szilágyi I.: Egy előre bejelentett gyilkosság krónikája: Visszatekintés. In: Iustitia kirándul. Budapest, 2009. 113. o.

A gyakorló jogászok jól tudják, hogy nagyon nehéz helyzetben van a jogalkalmazó, amikor megindul a büntetőeljárás. Bár a jog döntési programot kínál a jogalkalmazónak akkor, amikor az anyagi jogszabályok pontosan körülírják az egyes törvényi tényállásokat, mégsem elég a jogszabályok pontos ismerete ahhoz, hogy a hétköznapok gyakorlatában a jogalkalmazó felderíthesse a múltban megtörtént bűnös emberi cselekedetet, rekonstruálhassa a tényállást. A felderítéshez ugyanis a törvényben nem szabályozott, másfajta ismeretekre is szükség van. Ezek megszerzéséhez pedig segítséget nyújt(hat) a szépirodalom, mivel számos olyan mű létezik, amelynek olvasása által jobb jogászok születhetnek. Ilyen pl. Marquez híres regénye, az Egy előre bejelentett gyilkosság krónikája is, ahol az író éppen a nyomozás elején fontossággal bíró verziók szerepére hívja fel a (jogász-)olvasó figyelmét. Amikor Marquez vizsgálóbírája 12 nappal a gyilkosság elkövetése után a faluba érkezik, döbbenten tapasztalja, hogy ahány szemtanúja volt a bűncselekménynek, annyi verziója lesz a múltbéli történésnek is.

Más irodalmi művekben is találunk a jogalkalmazás számára hasznos kriminalisztikai ismeretanyagot: ilyen pl. Szolzsenyicin Gulág szigetcsoport című alkotása, amely szintén „számos jogi vagy a joghoz szorosan kapcsolódó réteggel rendelkezik."[4]

A kötet szerzői között szerepel még H. Szilágyi Istvánon és Fekete Balázson kívül Nagy Tamás, Hörcher Ferenc, Horváth Attila, Tallár Ferenc, Somlai Dorottya, Könczöl Miklós, Jany János, P. Szabó Béla, Falusi Márton, Cserne Péter, Frivaldszky János.

A Jog és irodalom szimpóziumokat kétévenként rendezik. A harmadik ilyen összejövetelre idén áprilisban, Piliscsabán került sor. Itt is érdekes előadásokat hallottak a résztvevők. Várjuk az elhangzottak kötet formájában való megjelenését.

[4] Fekete B.: A nyugati jog vágyálma. Jogi rétegek Szolzsenyicin Gulág szigetcsoport című művében. In: Iustitia … i.m. 63. o.

Bűntények a könyvtárszobából

Interaktív iratmintatár büntetőjogi komplex gyakorlathoz és szakvizsgához

Rendhagyó iratmintatár megalkotását határozták el a könyv szerzői, akik hazánk különböző jogi karain oktatnak, illetve legtöbbjük a jogalkalmazás mindennapjaiban is aktívan tevékenykedik. A közölt határozatok alapját nem a hétköznapi élet jogesetei, hanem a különböző korok irodalmi alkotásai adják, hiszen arra jöttek rá a szerzők, hogy ezek is hűen tükrözik a társadalomban élő erkölcsi és jogi normákat, ugyanakkor sokkal ismertebb, érdekesebb és érthetőbb élethelyzeteket dolgoznak fel.

A joghallgatók számára az egyetemi tanulmányaik folyamán a jog világa gyakran zavaros szabályok összességeként jelenik meg, és az oktatók legtöbbször a vizsgán szembesülnek azzal, hogy a diákok nem tudják alkalmazni a bemagolt jogszabályokat. Ezért úgy gondolták, hogy nem érdektelen, ha az alapvető jogi és technikai kérdéseket irodalmi műveken keresztül értetik meg a leendő jogászokkal úgy, hogy a Btk. Különös Részének egyes fejezeteit is alapul véve, az ide tartozó, de nem a hétköznapokban, hanem a klasszikus szépirodalomban megjelenő konkrét bűncselekmények miatt „indított" büntetőeljárásokat képzelik el: hol az egész eljárás folyamán megszületett valamennyi határozat, hol pedig csak a leglényegesebb döntések segítségével. Azoknál az irodalmi jogeseteknél, ahol az összes irat szerepel, ott a büntetőeljárás teljes folyamata végig követhető, kezdve a nyomozás megindításától, az előzetes letartóztatáson és a vádemelésen keresztül, a bírói határozatok megszületéséig. Ahol nem az egész büntetőeljárást dolgoztuk fel, ott viszont „bemerészkedtek" a büntetés-végrehajtás területére is, és a szabadságvesztés letöltése alatt keletkező döntések bemutatásával segítik a joghallgatók, illetve a szakvizsgára készülő bírósági, ügyészségi fogalmazók, valamint ügyvédjelöltek munkáját.

Szerkezetileg az iratmintatár leginkább a Btk. Különös Részének fejezeteiből merít, de kakukktojásként beiktatja, a törvényben így nem nevesített családon belüli erőszakot is.

1. Az élet elleni bűncselekmények közül Kosztolányi Dezső Édes Annáját, valamint Stendhal Vörös és fekete c. regényét használták az iratok megszerkesztésénél, a testi épség elleni bűncselekmények körében pedig Kosztolányi Aranysárkányát, illetve Zola Nanáját. A személy elleni bűncselekményekhez Shakespeare Velencei Kalmárját választották. Ennél a jogesetnél eredetileg közösség elleni izgatás miatt indul meg a büntetőeljárás, de „átvált" becsületsértésre, így alapozza meg helyét ebben a fejezetben.

2. A családon belüli erőszakra vonatkozó részben Shakespeare Othellója reprezentálja a „négy fal között" történt borzalmakat.
3. A házasság, a család, az ifjúság és a nemi bűncselekmények közé Apollinaire Don Juanja (Egy ifjú don Juan emlékiratai) került, aki több bűncselekményt is elkövetett.
4. A közrend elleni bűncselekményeknél, ezen belül is a közbiztonságot érintőknél, az állatkínzással kapcsolatos határozatokat Csáth Géza Kis Emmája ihlette, a közbizalom elleni bűncselekményekre pedig példának Ibsen Nóráját találták. Nóra, bár elkövette az okirat-hamisítást, a bűncselekmény elévülése miatt őt felelősségre vonni nem lehet.
5. A gazdasági bűncselekményekre talán a legjobb példa Jókai Mór Aranyembere, akinek cselekményei több büntetőjogi tényállást is megvalósítottak, és nem csak a gazdasági bűncselekmények köréből.
6. A vagyon elleni bűncselekményeken belül a rablást emelték ki, Fazekas Mihály Ludas Matyija kapcsán.
7. A katonai bűncselekményeknél Gárdonyi Géza Egri csillagok c. regényét vették alapul a határozatok elkészítésénél.
8. Az emberiség elleni bűncselekmények: Ezek a bűncselekmények, bár a Btk. Különös részének első fejezetéhez tartoznak, a szerzők mégis a könyv végére tették, mert úgy gondolták, hogy ez a rész elkülönül az ezt megelőző fejezetektől, mivel itt nem írtak iratokat, hanem „csak" a radbruchi formulára hívták fel az olvasó figyelmét.

A határozatokat aláíró bíráknál, ügyészeknél, nyomozóknál híres külföldi írók neveit fordították magyarra. Az ötlet Eörsi Gyulától származik, aki szinte rajongott Thomas Mannért. Egyik kedvenc novellája a Tonio Kröger volt. A név magyarul Korsós Antalt jelent. Nagyon bosszantotta Eörsi Gyulát, hogy amikor megjelent az egyik könyve, semmilyen recenzió nem érkezett a szakma részéről, ezért Korsós Antal álnéven kritizálta saját művét, majd Eörsi Gyulaként válaszolt is a felvetett kérdésekre. Később tanítványa, Sárközi Tamás pedig ifj. Korsós Antal néven készítette interjúit híres jogászokkal és politikusokkal.

SÜMEGINÉ TÓTH PIROSKA[1]

Válogatás a szakirodalomból

BÜNTETŐJOG

LAJTÁR ISTVÁN:
A büntetés-végrehajtás garancia- és kontrollrendszere Magyarországon
Lezárva: 2010. február 1., HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2010.

Bűntények a könyvtárszobából
Interaktív iratmintatár büntetőjogi komplex gyakorlathoz és szakvizsgához. (szerk.: Kiss Anna) Complex Kiadó, Budapest, 2010.

GAZDASÁGI JOG

BOGNÁR PIROSKA:
A nonprofit gazdasági társaságok
Második, hatályosított, bővített kiadás. Lezárva: 2010. január 1. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2010.

KÖZIGAZGATÁSI JOG

FOGARASI JÓZSEF (SZERK.):
A helyi önkormányzatok
Lezárva: 2009. november 30. HVG-Orac Lap- és Könyvkiadó Kft., Budapest, 2010.

BERTA ZSOLT (ÖSSZEÁLL., SZERK.):
Választójogi kézikönyv. Jogszabályok és joggyakorlat
Textpert Kft., Budapest, 2010.

POLGÁRI JOG

BOÓC ÁDÁM – FÁBIÁN FERENC – SÁNDOR ISTVÁN – TÖRÖK GÁBOR:
A civilisztika dogmatikája
(szerk.: Török Gábor) HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2010.

---

[1] Sümeginé Tóth P.: könyvtárvezető, a Legfelsőbb Bíróság Könyvtára

FÉZER TAMÁS:
Kártérítési jog
Lezárva: 2010. január 15. CompLex Jogi és Üzleti Kiadó, Budapest, 2010.

SÁRKÖZY TAMÁS:
Sportjog (A 2004-es Sporttörvény magyarázata)
Második, hatályosított kiadás. HVG-ORAC Lap- és Könyvkiadó, Budapest, 2010.

ÁLTALÁNOS TÉMA

Iustitia kirándul
Tanulmányok a „Jog és Irodalom" köréből
(szerk.: Fekete Balázs – H. Szilágyi István – Könczöl Miklós) Szent István Társulat Könyvkiadó, Budapest, 2009.

BENISNÉ GYŐRFFY ILONA:
28. Jogász Vándorgyűlés, Sopron, 2009. május 21-23.
Magyar Jogász Egylet, Budapest, 2009.

BLUTMAN LÁSZLÓ:
Az Európai Unió joga a gyakorlatban
Lezárva: 2010. febr. 15. HVG-ORAC Lap- és Könyvkiadó, Budapest, 2010.

BOTOS KATALIN (SZERK.):
Idősödés és globalizáció. Nemzetközi pénzügyi egyensúlytalanság
Tarsoly Kiadó, Budapest, 2009.

Jogi Tájékoztató Füzetek 205-209.
MKIK Jogi Szekció, Budapest, 2009.

POKOL BÉLA:
Autentikus jogelmélet
Institutiones Juris. Dialóg Campus Kiadó, Budapest-Pécs, 2010.

TABLER, CHRISTA – BEGLINGER, JACQUES:
Essential EU Law in Charts
HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2010.

TABLER, CHRISTA – BEGLINGER, JACQUES:
Essential EU Law in Text
HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2010.

Új Európai börtönszabályok és magyarázatuk – VIII. rész

(összeállította: Vókó György[1])

Etnikai vagy nyelvi kisebbségek

38. Szabály

38.1. Speciális megoldásokat kell kialakítani az etnikai vagy nyelvi kisebbséghez tartozó fogvatartottak szükségletei tekintetében.

38.2. Amennyiben lehetséges a különböző csoportoknak lehetőséget kell kapniuk arra, hogy a büntetés-végrehajtási intézetben is tiszteletben tartsák kulturális szokásaikat.

38.3. A nyelvi igényeket szakavatott tolmácsok igénybevételével és az egyes büntetés-végrehajtási intézetekben beszélt különböző nyelveken fogalmazott tájékoztató füzetek átadásával kell kielégíteni.

A börtönnépesség növekvő diverzifikálódása okán Európában új szabályt kell bevezetni az etnikai és nyelvi kisebbségek igényei kiemelt figyelembe vételének biztosítása végett. A 38. Szabály ezt a gondolatot általános fogalmazásban mondja ki. A büntetés-végrehajtás személyi állományát fogékonnyá kell tenni a különböző csoportok kulturális gyakorlatai iránt a félreértések veszélyének elkerülése érdekében.

III. Rész: Egészség

Egészségügyi ellátás

39. Szabály

39. A büntetés-végrehajtási hatóságoknak védeniük kell az őrizetükben lévő fogvatartottak egészségét.

Ez a szabály új és a Gazdasági, Szociális és Kulturális Jogok Nemzetközi Egyezségokmányának 12. cikkén alapul, amely deklarálja „mindenkinek azt a jogát, hogy a legjobb testi és lelki egészségi állapotot élvezze, amelyet elérni tud". Ezzel az alapjoggal párhuzamosan – amelyet mindenkire alkalmazni kell – a fogvatartottak többletvédelemmel rendelkeznek státuszuk okán. Ha egy ország személyeket szabadságuktól foszt meg, vállalja annak felelősségét, hogy egészségükkel törődjék, figyelemmel a fogvatartási feltételekre és az egyéni kezelésre,

[1] Vókó Gy. PhD, habilitált doktor, CSC, Legfőbb Ügyészség

amely ezen feltételek tényénél fogva szükségesnek bizonyulhat. A büntetés-végrehajtás adminisztrációjának nem csupán az a felelőssége, hogy biztosítsa a fogvatartottak egészségügyi ellátáshoz jutásának tényleges voltát, hanem az is, hogy olyan feltételeket teremtsen, amelyek kedvezőbb egészségügyi helyzetbe hozzák a fogvatartottakat és a büntetés-végrehajtás személyi állományát. Kívánatos, hogy a fogvatartottak a befogadásuk időpontjához képest nem rosszabb egészségi állapotban hagyják el a börtönt. Ez a börtönélet minden aspektusára vonatkozik, különösen az egészségügyi ellátásra.
Ezt az elvet a Miniszteri Bizottságnak a gondozás etikai és szervezeti aspektusairól a tagállamokhoz intézett (98)7 ajánlása erősítette meg, valamint a CPT, különösen a 3. Általános Jelentésében [CPT/Inf (93)12.]. Ehhez adódik még az Európai Emberi Jogi Bíróság által generált mind jelentősebb joganyag, amely megerősíti, hogy az államok feladata az őrzésük alatt lévő fogvatartottak egészségének védelme.

Az egészségügyi ellátás szervezete a büntetés-végrehajtási intézetben

40. Szabály

40.1. A büntetés-végrehajtási intézetben nyújtott egészségügyi ellátást a helyi önkormányzat vagy az állam általános egészségügyi ellátási szolgálatával szoros kapcsolatban kell megszervezni.

40.2. A büntetés-végrehajtási intézetekben az egészségpolitikát a nemzeti közegészségügyi politikába kell integrálni, amellyel összhangban kell lennie.

40.3. A fogvatartottak számára a jogi helyzetükre alapozott hátrányos megkülönböztetés nélkül kell elérhetővé tenni az egészségügyi szolgálatokat.

40.4. A büntetés-végrehajtási intézet egészségügyi szolgálatainak törekedniük kell minden testi vagy mentális betegség, valamint azon hiányosságok vagy fejlődési rendellenességek kiszűrésére és kezelésére, amelyekben a fogvatartottak esetleg szenvednek.

40.5. Ennek érdekében, minden fogvatartottnak részesülnie kell a szükséges orvosi, sebészeti, pszichológiai ellátásban, azokat is ideértve, amelyek szabad környezetben állnak rendelkezésre.

A 40. szabály leghatékonyabb végrehajtási módja az lenne, hogy a nemzeti egészségügyi hatóságok is felelősek legyenek a börtönökben nyújtott egészségügyi ellátásokért, a számos európai országban folytatott gyakorlathoz hasonlóan. Ha nem ez a helyzet, akkor a lehető legszorosabb kapcsolatot kellene kialakítani a börtönökön belül egészségügyi ellátást nyújtók és a börtönökön kívüli egészségügyi szolgálat között. Ez nem kizárólagosan a kezelések nyomon követésének biztosítását jelenti, hanem a fogvatartottak és a büntetés-végrehajtási személyi állomány olyan helyzetbe hozását is, hogy a legszélesebb körben részesülhessenek a kezelések, a szakmai normák és a képzés fejlődéséből.

A Miniszteri Bizottság (98)7. ajánlása úgy ítéli meg, hogy „a büntetés-végrehajtás egészségügyi politikáját integrálni kellene a nemzeti egészségügyi politikába és azzal összhangba kellene hozni". Azon kívül, hogy ez a fogvatartottak érdekét szolgálja, ugyanez vonatkozik az egész népesség egészségére is, különös tekintettel a fertőző betegségekkel kapcsolatos politikára, amelyek a börtönökből a nagyobb közösség irányában is elterjedhetnek.
A fogvatartottak azon jogát, hogy korlátozás nélkül hozzájussanak az ország egészében rendelkezésre álló egészségügyi szolgáltatásaihoz, megerősíti az Egyesült Nemzetek Szervezetének a fogvatartottak kezeléséről szóló Alapelveinek 9. alapelve is. A CPT 3. Általános Jelentése hasonlóképpen nagy jelentőséget tulajdonít a fogvatartottak egyenértékű egészségügyi ellátáshoz való jogának. Az is alapvető fontosságú, hogy a fogvatartottak térítésmentesen jussanak hozzá az egészségügyi ellátáshoz (az Egyesült Nemzetek Szervezetének a fogvatartás bármely formája vagy szabadságvesztés büntetés hatálya alatt álló minden személy védelmét szolgáló Alapelvgyűjteményének 24. alapelve). Számos ország komoly nehézségekkel küzd a népesség egésze számára nagy volumenű egészségügyi szolgáltatás nyújtása terén. A körülményektől függetlenül azonban a fogvatartottak jogosultak az egészségügyi ellátás legjobb felszereléseihez jutni, mégpedig térítés nélkül. A CPT kifejtette, hogy még jelentős gazdasági nehézségek időszakában sem mentesíti semmi sem az államot attól a felelősségétől, hogy ellássa a legszükségesebb/alapvető fontosságú cikkekkel a szabadságuktól megfosztott személyeket, hangsúlyozva, hogy az alapvető fontosságú cikkek magukba foglalják az elégséges mennyiségű és megfelelő egészségügyi cikket is {v.ö. például a Moldvai Köztársaságról készült jelentéssel [CPT/Inf (2002) 11]}.
A szabályok között nincs olyan, amely gátolná a fogvatartottakat abban, hogy saját költségükre saját orvosuk vizsgálja meg őket.

Orvos- és ápolószemélyzet

41. Szabály

41.1. Minden büntetés-végrehajtási intézetnek legalább egy általános orvos szolgáltatásaival kell rendelkeznie.

41.2. Intézkedni kell arról, hogy sürgős esetben mindenkor okleveles orvos azonnal beavatkozást végezzen el.

41.3. A teljes munkaidőben foglalkoztatott orvossal nem rendelkező büntetés-végrehajtási intézeteket részmunkaidős orvosnak kell rendszeresen látogatnia.

41.4. Minden büntetés-végrehajtási intézetnek megfelelő egészségügyi képesítéssel rendelkező személyzettel kell rendelkeznie.

41.5. Minden fogvatartott számára lehetővé kell tenni az okleveles fogorvosi és szemészeti ellátást.

Ez a szabály a fogvatartottak számára az egészségügyi ellátáshoz való tényleges hozzájutás iránti alapvető igényt érinti mindenkor, amikor az szükséges; ez azt

jelenti, hogy minden büntetés-végrehajtási intézetben kívánatos orvost kinevezni. Ennek a gyakorló szakembernek minden szükséges kompetenciával kívánatos rendelkeznie. A nagy büntetés-végrehajtási intézetekben az orvosnak teljes munkaidős állást kívánatos betöltenie. Minden esetben biztosítani kell az orvos közreműködésének lehetőségét a sürgős esetekben való intézkedés végett. Ezt a követelményt a Miniszteri Bizottság (98)7 ajánlása megerősíti.
Az orvosokon kívül megfelelő képesítéssel rendelkező ápolószemélyzetnek is lennie kell. Egyes Kelet-Európai országokban az egészségügyi szakképesítéssel rendelkező, az orvos alárendeltségében működő gyakorlati szakemberek (akiket helyenként „felcser"-nek neveznek) is nyújthatnak egészségügyi ellátást. A másik legfontosabb csoport a kellően képzett ápolónők csoportja. 1998-ban az Ápolónők Nemzetközi Tanácsa nyilatkozatot tett közzé, amely többek között deklarálta, hogy az ápolónők nemzeti egyesületeinek bizalmas jellegű állásfoglalásokat, tanácsokat és segítséget kellene nyújtaniuk a büntetés-végrehajtási intézetek ápolónői számára. [Az ápolónők szerepe a foglyok és a fogvatartottak gondozásában, az Ápolónők Nemzetközi Tanácsa, 1998.]
A fogvatartottakkal való kapcsolataikban az orvosoknak ugyanazon szakmai alapelveket és normákat kívánatos alkalmazniuk, mint amelyeket a börtönön kívüli funkcióik gyakorlásában alkalmaznának. Ezt az alapelvet a Büntetés-végrehajtási Egészségügyi Szolgálatok Nemzetközi Tanácsa erősítette meg, amikor az Athéni Esküt elfogadta:
„Mi, egészségügyi hivatást gyakorlók, akik büntetés-végrehajtási intézetekben dolgozunk, és Athénben, 1979. szeptember 10-én találkoztunk, kötelezettséget vállalunk itt, a Hippokratészi eskü szellemének megfelelően, hogy a legjobb egészségügyi ellátást biztosítjuk azoknak, akik bármilyen okból börtönbe vannak zárva, előítéletek nélkül, és megfelelő szakmai etikánk keretei között".
Ezt követelik meg az Egyesült Nemzeteknek az első, az egészségügyi személyi állomány, különösen pedig az orvosok szerepére alkalmazandó Egészségügyi Etikai Alapelvei is, a foglyok és a fogvatartottak kínzás és más kegyetlen, embertelen vagy lealacsonyító büntetések vagy bánásmódok elleni védelmében.

Folytatása következik.

Impresszum

Alapítva, 1993-ban
(© Ügyészek Országos Egyesülete)
Szakmai Érdekképviseleti folyóirat

Kiadja az Ügyészek Országos Egyesülete (ISSN 1217-7059)
A kiadásért felel: Máriánné Molnár Mária, az ÜOE elnöke
A szerkesztőség címe: 1122 Budapest, Maros u. 6/a.
Főszerkesztő: Kiss Anna PhD
Társszerkesztő: Parti Katalin PhD és Szabó Imre
Főszerkesztő-helyettes: Fazekas Géza, Központi Nyomozó Főügyészség
(Egyesületi Hírek rovat)
Felelős szerkesztő: Fürcht Pál, Budapesti Nyomozó Ügyészség
Olvasószerkesztő: Sümeginé Tóth Piroska, Legfelsőbb Bíróság
(Anyanyelvi Ügyelet és Könyvajánló rovat)
A szerkesztőség elnöke: Hadler Andrea, Budakörnyéki Ügyészség
Szerkesztőségi titkár: Szabó Imre, OKRI

Közlési feltételek

A Szerkesztőség olyan tanulmányok közlését vállalja, amelynek témája a különböző jogterületek elméleti és gyakorlati kérdéseivel kapcsolatos. Az írás nem állhat ellentétben az Ügyészek Országos Egyesületének Alapszabálya preambulumában megfogalmazott célokkal.
A kéziratot e-mailen kell a Szerkesztőséghez eljuttatni. A cikkek terjedelme maximum 20.000 leütés lehet. Nem tudunk színes táblázatokat, grafikonokat, diagramokat közölni. A Szerkesztőség a kéziratot stilizálhatja. A Szerző hozzájárul, hogy írásműve az internet-hálózaton is nyilvánosságra kerüljön.