2011
2.

BELÜGYI SZEMLE

A BELÜGYMINISZTÉRIUM SZAKMAI, TUDOMÁNYOS FOLYÓIRATA

59.
évfolyam

TARTALOM 2011/2.

SZERZŐINK 2011/2.

AMBRUS ISTVÁN tanársegéd, SZTE ÁJK
Büntetőjogi és Büntető Eljárásjogi Tanszék

DR. ASZTALOS ERIKA tanácsos,
Európai Együttműködési Főosztály

DEÁK ZOLTÁN ügyészségi fogalmazó,
Kecskeméti Városi Ügyészség

DR. IBOLYA TIBOR vezető ügyész,
Budapesti IV. és XV. Kerületi Ügyészség

DR. KARSAI KRISZTINA egyetemi docens, Szegedi Tudományegyetem
Állam- és Jogtudományi Kar
Büntetőjogi és Büntető Eljárásjogi Tanszék

MÁTRAI LÁSZLÓNÉ DR. ÓZSVÁRTH BABETT
rendőr százados,
Nemzeti Nyomozó Iroda Gazdaságvédelmi Főosztály
Pénzügyi Visszaélések Elleni Osztály
Vagyon-visszaszerzési Egység

DR. MEZEY NÁNDOR LAJOS fogalmazó,
Pécs Megyei Jogú Város Polgármesteri Hivatal

DR. RIGÓ ATTILA rendőr őrnagy, alosztályvezető,
Nemzeti Nyomozó Iroda Gazdaságvédelmi Főosztály
Pénzügyi Visszaélések Elleni Osztály
Vagyon-visszaszerzési Egység vezetője

DR. SZABÓ ADRIENN tanácsos, Európai Együttműködési Főosztály,
osztályvezető, BM EU Együttműködési Főosztály

DR. SZABÓ IMRE tudományos segédmunkatárs,
Országos Kriminológiai Intézet
Büntetőjog-tudományi Osztály

DR. SZIKINGER ISTVÁN ügyvéd,
Bólyai János és Társai Ügyvédi Iroda

Szabó, Imre
Dangers of IT terrorism in Hungary
[5–20]
The author provides a detailed description of the characteristics of IT terrorism, explaining how IT attacks for terrorist purposes constitute a crime under domestic law. The article also expands on anti-terrorist detection and prevention mechanisms and on how these may restrict freedom, especially in cyberspace.

Mezey, Nándor Lajos
Is cyberterrorism a real danger?
[21–48]
Cyberterrorism refers to the involvement of computer sciences and the internet in terrorist attacks and activities. Due to the widespread usage of computer technologies, this could be a source of danger in today's information dependent societies. The author investigates the validity of this claim.

Ibolya, Tibor
Torrent raids under Hungarian criminal law
[49–59]
The author investigates the legal background and utility of torrent raids in Hungary, and concludes that under, Hungarian criminal law, downloading is not a crime, and torrent site operators should not be criminally liable. Although uploading violates copyright law, since prosecution is almost impossible and excessively costly, thus, instead of a criminal law approach, a modernised copyright law should be the solution.

Karsai, Krisztina
Counterfeit products: a legal minefield
[60–84]
The article focuses on product counterfeiting, in particular on the complexities of identifying confusing products, and the legal nature of the lack of consent by the trademark's owner, as well as the discrepancies regarding mens rea (intent).

Ambrus, István – Deák, Zoltán
Major issues in bank card-related crimes
[84–103]
The authors examine three major questions relating to bank card-related crimes: the accumulation of bank card counterfeiting and bank card abuse committed through

marketing, the aiding of bank card counterfeiting as a sui generis crime, and the issue of impossible attempt.

Rigó, Attila – Mátrai, Lászlóné
Asset recovery in theory and practice: examples from the UK and Germany
[104–115]
In order to provide examples for Hungarian legislators and practitioners, the authors compare common law and continental traditions in asset recovery theory and practice.

■ **TOPIC-WATCH**
Asztalos, Erika – Szabó, Adrienn
Monthly overview of EU legislation and relevant events
[130–134]

DOI:10.38146/bsz-ajia.2011.v59.i2.pp5-20

SZABÓ IMRE

Az informatikai terrorizmus veszélyei

Az informatikai terrorizmus mint önálló kategória elterjedése a büntetőjog-irodalomban a 2001. szeptember 11. utáni időszakra tehető. Előrebocsátom, hogy ez a kategória több aspektusból is megközelíthető. Az interneten keresztül megvalósított terrorista tevékenység fő célja jelenleg még viszonylag puritán. A terroristák az internetet elsősorban mint új kommunikációs eszközt az emberek befolyásolására, manipulálására használják fel. Leegyszerűsítve azt lehetne mondani, hogy a politikai kommunikáció új módszereit ültetik át abba a sajátságos társadalmi környezetbe, amelyben céljaik megvalósítására törekszenek.

Ennek két következménye van. Az egyik, hogy a politikai kommunikáció módszerei a terroristák kommunikációs tevékenységében is tetten érhetők, másodsorban pedig az, hogy a terroristák által adaptált módszerek sajátosan új jellemzői a politikai kommunikációban is megjelennek. *Paul Wilkinson* a terroristák médiahasználatában négy fő célt különböztet meg: *„az első a propagandájuk közzététele és a félelemkeltés megvalósítása, a második a nagyobb (általában anyagi) támogatás megmozgatása a szervezetük számára, a harmadik lejáratni a kormányokat és mindazokat a szervezeteket, amelyeknek kötelességük lett volna megvédeni az állampolgárokat, a negyedik pedig további támadásokat inspirálni, akár más szervezetek részéről, akár a saját szervezetükbe való toborzással”*.[1]

Ezekből a célokból jelen tanulmány keretében a harmadikról esik a legtöbb szó, nevezetesen arról, hogyan kapcsolódik az informatikai terrorizmus a politikai hitelvesztéshez.

A terrorista módszerek elleni fellépés minden demokratikus értékrendet valló közösség elemi érdeke, tekintettel arra, hogy a pszichikai befolyásolás pont a bázisdemokráciák, demokratikus szerveződések, demokratikus államok struktúrái ellen irányulnak. *Irving Lachow* és *Courtney Richardson* az Amerikai Egyesült Államok és az iszlám terrorista csoportok közötti háborút elemző elmélete rámutat arra, hogy a terroristák az internetet az Egyesült Államok nemzeti védelmének megsértésére használják. Ezt a tevékenységet

1 Istvánffy András: A terrorizmus mint rituális kommunikáció. Paul Wilkinson: The Media and Terrorism: A Reassessment. Beszélő, 2005. augusztus

azonban nem azáltal valósítják meg, hogy kritikus infrastruktúrák, illetőleg katonai célpontok ellen intéznek számítástechnikai támadásokat, hanem azzal, hogy aláássák a kormány katonai és diplomáciai erőfeszítéseit, aminek célja az ideológiák harcának megnyerése *(to win the war of ideas)*[2]. A globálisan megjelenő ideológiai harc egyes elemei lokálisan is megjelenhetnek. Bár Magyarországon ténylegesen nem történt még a szó globális értelmében vett terrorcselekmény, de nem zárható ki, hogy a politikai kommunikációban a nemzetközi módszerek adaptációja tetten érhető. Természetesen ez nem jelenti azt, hogy minden – a terrorcselekmények jegyeit magán hordozó – politikai csatározás terrorcselekménynek minősül, nem szabad azonban figyelmen kívül hagyni az „ideológiák harca" módszereinek megjelenését a hazai kommunikációban, kiváltképpen azért, hogy ne essünk áldozatul önkéntelenül is valamely pszichológiai manipulációnak.

Az „ideológiák harcában" különböző értékrendek képviselői harcolnak egymással, ráadásul mindennek a vesztesei az állampolgárok. Ez egyik oldalról abban nyilvánul meg, hogy terrorcselekmény sértettjeivé válnak, másik oldalról pedig abban, hogy a terrorcselekmény felderítésére, megelőzésére hivatkozva az állam korlátozza az állampolgárok szabadságjogait. Ez a kettősség jól tetten érhető az informatikai terrorizmus vonatkozásában is.

Az informatikai terrorizmus jellemzői

A terrorcselekmény és a terrorcselekmény eszközcselekményeiként meghatározott bűncselekmények közötti alapvető különbség a cselekmény motívumában, illetőleg célzatában ragadható meg. A terrorcselekménynél ez a célzat politikai (társadalompolitikai, valláspolitikai stb.) motivációból fakad, míg egyéb esetben a motiváció többnyire az elkövető személyéhez, a személyiségéből fakadó igényeihez kötődik. Az informatikai terrorizmus legfontosabb célja, hogy a társadalom fenyegetettségérzetének szüntelen gerjesztésével lerombolja az állam cselekvőképességébe vetett bizalmat, és ily módon valóságosan is aláássa az állam abbéli képességét, hogy az események felett

2 Az Egyesült Államok politikai kommunikációjának jellemzője a következő példában jól tetten érhető: Az szovjet–afgán háború idején az amerikai sajtóban gyakran előforduló kifejezések voltak a „jihad" és a „mujahideen". Az előbbi jelentése szabad fordításban „igyekvés Istenhez", míg az utóbbi „szent harcost" jelent. Az amerikai–afgán konfliktus idején a médiában már megjelentek a „hirabah" és az „irhabists" kifejezések, jelentésük istentelen háború és terrorista.

kontrollt gyakoroljon (kormányzati politika befolyásolása, kormányzat kényszerítése, civil lakosság fenyegetése).

Az informatikai terrorizmus két határterülete az informatikai bűncselekmények köre, illetve az informatikai hadviselés körébe tartozó magatartások. 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 a lakosság ellen erőszakot alkalmazni, tilos a lakosság bármilyen sérelmét okozó cselekményt elkövetni, míg a terrorizmus egyik fő célja pont a lakosság ellen intézett támadások kivitelezése, illetve a lakosság demoralizálása.

A terrorizmus elleni nemzetközi fellépés érdeke számos nemzetközi szerződést hozott létre.[3] Ezzel szemben az informatikai terrorizmus mint újszerű jelenség elleni fellépés nem hívott életre önálló nemzetközi szerződést. Ennek fő oka, hogy a hagyományos értelemben vett terrorista cselekményekre vonatkozó szerződések értelmezésekor nem találunk joghézagot abból adódóan, hogy a terrorista cselekményeknél akár az elkövetés eszközeként, akár az elkövetés tárgyaként számítástechnikai rendszerek jelennek meg. Azok a cselekmények, amelyek vonatkozásában felvetődik az informatikai terrorizmus megállapításának lehetősége, főként csak abban különböznek a hagyományos módon elkövetett terrorcselekményektől, hogy a cselekmény kapcsolatba hozható valamilyen számítástechnikai rendszerrel. A terrorista támadással fenyegetés, terroristák kiképzése, toborzása, a terrorizmus finanszírozása, mind-mind megvalósítható informatikai környezetben is. Mitől számíthat mégis önálló kategóriának az informatikai terrorizmus?

Az informatikai terrorizmus körébe tartozó cselekmények

Az informatikai bűncselekményeket azok célzata különbözteti meg az informatikai terrorizmustól. 2000-ben Ausztráliában egy férfi behatolt egy hulladékgazdálkodó üzem számítástechnikai rendszerébe, és a rendszer által üzemeltetett szennyvíztisztítási mechanizmusok rendellenes alkalmazásával

3 A terrorizmus finanszírozásának visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 54. ülésszakán, 1999. december 9-én elfogadott nemzetközi egyezmény; A terrorizmus elleni küzdelemről szóló 2002/475/IB. kerethatározat. (2002. június 13.); A terrorizmus megelőzéséről szóló Európa tanácsi egyezmény; stb.

szennyvizet engedett a környező patakokba, folyókba. Bár a bűncselekményt számítástechnikai eszközökkel követték el, ez még nem jelenti azt, hogy informatikai terrorizmus valósult volna meg. A körülmények tisztázása után kiderült, hogy a férfit elbocsátották az üzemből, ezért ebbéli felháborodását akarta cselekményével kifejezésre juttatni. Cselekménye minősítésénél az játszott szerepet, hogy magatartását individuális célból követte el, és nem a terrorcselekményhez megkövetelt politikai célból, vagyis nem valósított meg terrorcselekményt.

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 eszköze *(weapon of mass disruption)*.[4]

A *tömeges pusztítás* kategóriájához azok a cselekmények tartoznak, amelyek olyan számítástechnikai rendszereket érintenek, amelyek közveszély előidézésére alkalmas berendezéseket kontrollálnak. Ilyen lehet például egy nukleáris erőműben zajló maghasadást szabályozó rendszer, amelynek megzavarásával a csernobilihoz hasonló baleset idézhető elő. Ez terrorista akciónak minősíthető ugyan, de nem minősíthető informatikai terrorizmusnak, hiszen a magatartás nukleáris katasztrófát idéz elő, és nem informatikai katasztrófát. Emiatt nem nevezzük például mechanikai terrorizmusnak az 1998-ban az amerikai nagykövetségek ellen autóban elhelyezett pokolgépekkel végrehajtott merényleteket.[5]

A *tömeges zavarkeltés* lényege a civil lakosság pszichológiai manipulációja. Idetartozik minden magatartás, amelynek célja a civil lakosság demoralizálása azáltal, hogy megingatja a lakosságnak a kormányzat hatékonyságába vetett hitét. Az e cselekménycsoport okán megvalósuló sérülések, illetőleg bekövetkező kár tipikusan csak közvetett következményei lehetnek a terrorcselekménynek. A tömeges zavarkeltés inkább valamely hagyományos módon megvalósított terrorcselekmény következményeinek a fokozására szolgál. Ebbe a körbe tartozott az *Al-Qaeda Alliance Online* terrorista formáció támadása, amikor is az Egyesült Államok kormányzati portáljaira

4 Susan W. Brenner: Cybercrime, Cyberterrorism and Cyberwarfare. Revue internationale de droit pénal, vol. 77, 3–4/2006.

5 A busheri atomerőművel kapcsolatos informatikai támadásról lásd: Szabó Imre: Informatikai bűncselekmény, informatikai terrorizmus vagy informatikai hadviselés? In: Vig Dávid (szerk.): Globalizáció kihívásai – kriminálpolitikai válaszok. Magyar Kriminológiai Társaság, Budapet, 2010, 98–110. o.

feltöltötte azt az üzenetet, miszerint Bin Laden egy szent harcos.[6] A szeptember 11-i események idején emberek milliói nézték a televíziós, illetve az interneten elérhető hírműsorokat, hírcsatornákat azért, hogy megtudják, mi történt pontosan. Ha ebben az esetben a nagyobb internetes hírportálok nyitóoldalait a terroristák olyan címoldalakra cserélték volna le, amelyekben kitalált hírek szerepelnek (például nukleáris holokauszt Európában és Ausztráliában, Oroszország atomcsapásra készül a nagyobb amerikai városok ellen stb.), bekövetkezhetett volna egy másik Orson Welles-i tömeghisztéria *(A világok harca* című mű rádiós közvetítése nyomán országszerte pánik tört ki az Egyesült Államokban). Ebből is adódik, hogy ezeknek a cselekményeknek nem céljuk a közvetlen károkozás, sokkal inkább a kormányzat elleni terror hatásának fokozása.

A hazai közigazgatási rendszer informatikai fejletlensége jelentős akadálya ilyen típusú cselekmények megvalósításának. Tegyük fel, hogy megvalósul a tűzoltóságok egységes riasztási rendszerének informatikai környezetbe ágyazása. Abban az esetben, ha ebbe a rendszerbe valaki terrorista célzattal belenyúlna, és riasztást adna le a Budapesten található összes tűzoltóságnak, hogy azonnal minden gépjárművet küldjenek a Parlament épületéhez, mert az lángokban áll, az egész város hamar értesülne a tűzoltóautók kivonulásáról. Ha kiderülne, hogy ez csupán egy baklövés volt, elképzelhető, milyen hírek jelennének meg erről a különböző médiákban.

A *társadalmi bizalom megdöntésének* eszköztára nagyon széles. Ebbe a körbe tartoznak azok a cselekmények, amelyeket a szakirodalom az „elektronikus dzsihád" kategóriájába[7] sorol. 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 leállásával járhat, ezáltal azt a látszatot keltve, hogy az állam nem képes megvédeni a társadalom működésének alapstruktúráit.

6 'Osama bin Laden is a holy fighter, and whatever he says makes sense'. Dorothy E. Denning: Terror's web: how the Internet is transforming terrorism. In: Yvonna Jewkes – Majid Yar (eds.): Handbook of Internet Crime. Willan Publishing, Portland, 2010, p. 199.

7 A tipikus hackertámadások körét foglalja magában. Az interneten számos – terroristák által publikált – forrás található az egyes támadások elkövetésének módszertanáról. Ezeken az oldalakon a módszertani útmutatók mellett számos szoftver is elérhető, amely az elkövetést hivatott elősegíteni. Ilyen gyakorlati útmutató például a „The Encyclopedia of Hacking the Zionist and Crusader Websites" és a „39 Ways to Serve and Participate in Jihad" címet viselő és online elérhető mű is.

A tömeges pusztítás következménye elsősorban fizikai (tangibilis), amely közvetlenül a megtámadott információs rendszer által működtetett eszközöknél jelenik meg, míg a társadalmi bizalom megdöntésénél digitális (intangibilis) következményről beszélhetünk. A digitális következmény során az adatokat törlik, megváltoztatják, hozzáférhetetlenné teszik stb., és ennek nyomán tipikus esetben a számítástechnikai rendszer működését akadályozzák.[8]

A társadalmi bizalom megdöntése és a tömeges zavarkeltés közös eleme a lakosság pszichikai befolyásolása. Míg utóbbi tisztán pszichikai következményeket gerjeszt, addig az előbbinél tényleges fizikai beavatkozás is megvalósul azáltal, hogy az érintett számítástechnikai rendszerek működésének akadályozása bekövetkezik.

Az informatikai terrorizmus veszélye Magyarországon

Az informatikai terrorizmus veszélye Magyarországon elsősorban nem a ténylegesen sértő, illetőleg károsító történések bekövetkezésének lehetőségéből adódik. A veszély abból következik, hogy míg a terrorcselekmény vonatkozásában maradéktalanul teljesítettük azt a nemzetközi kötelezettségünket, hogy kellő védelmet nyújtsunk a globális terrorizmus vonatkozásában a más államot vagy nemzetközi szervezetet fenyegető cselekményekkel szemben, addig nem fordítottunk kellő gondot saját védelmünkre. Elmulasztottuk az alapos számbavételét azoknak az eshetőségeknek, amelyeknél a terrorcselekmények Magyarországot érintik. Nem vizsgáltuk meg alaposan, hogy mi történik abban az esetben, ha a „nyugati világ részeként" Magyarország válik a globális terrorizmus célpontjává, vagy ne adj' isten a magyar társadalmi struktúra alakul úgy át, hogy lokális terrorizmus megjelenésével kell számolnunk.

A Tanács 2002/475/IB számú kerethatározata (2002. június 13.) a terrorizmus elleni küzdelemről (a továbbiakban: kerethatározat) részletesen rendelkezik bizonyos cselekmények terrorista bűncselekményekké nyilvánításáról.

8 A tudás egyik megjelenési formája a technológia, ami a javak és szolgáltatások előállításához szükséges módszerek és eszközök összességeként definiálható. A technológia lehet tangibilis vagy intangibilis. A tangibilis tudás és technológia gépek, eszközök, tőkejavak formájában ölt testet, míg a technológia intangibilis formája a tárgyi eszközökben meg nem testesült, a termelési folyamattal kapcsolatos azon tudáselemeket foglalja magában, amelyek speciális minőségű javak speciális folyamatok segítségével történő előállításához szükségesek. PeterArtenberg: Technology Transfer and New Institutional Economics. Dissertation zur Erlangung des akademischen Grades eines Doktors der Sozial- und Wirtschaftswissenschaften an der Wirtschaftsuniversitat Wien. Wien, Oktober 1999.

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. §-a szerinti terrorcselekmény (1) bekezdésének *c)* pontjában foglalt célzattól:

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

Felvetődhet 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 2003. évi II. számú törvény miniszteri indokolása adja, e 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 három bűncselekmény jöhet szóba a miniszteri indokolás alapján: az alkotmányos rend erőszakos megváltoztatása (Btk. 139. §), az alkotmányos rend elleni szervezkedés (Btk. 139/A §) és a rombolás (Btk. 142. §).

Mindháromnak 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 bűncselekmé-

nyek védik a Magyar Köztársaság alkotmányos politikai, gazdasági és társadalmi rendjét is. (Némileg ellentmond ennek az értelmezésnek a terrorcselekmény tényállása, amelyben az alkotmányos rend külön tényállási elemként jelenik meg, elkülönítve a társadalmi, gazdasági rendtől, ennek alapján joggal lehet azt gondolni, hogy ezek különböző védendő jogi érdekek.)

Lényeges, hogy az *alkotmányos rend erőszakos megváltoztatásánál* az elkövetés módja az erőszak, míg a bűncselekmény célzata az alkotmányos rend megváltoztatása. A terrorcselekménynél azonban nemcsak a megváltoztatási célzat, de a megzavarási célzat is szerepel.

Mitévő legyen a jogalkalmazó, ha a Magyar Köztársaság alkotmányos rendjének megzavarása vagy megváltoztatása céljából követnek el számítástechnikai rendszer és adatok elleni bűncselekmény(eke)t? A terrorcselekmény eszközcselekményei vonatkozásában erőszakos cselekménynek minősül ez a bűncselekmény is, ettől azonban még a cselekmény az egész Btk.-ra kiterjedően nem lesz erőszakos cselekmény. Nehéz elképzelni azt is, hogy valaki „puccsot" hajtson végre a személyi számítógépe mellől, mivel az alkotmányos rendet onnan szeretné megváltoztatni. Ha viszont a célzat csupán az alkotmányos rend megzavarására irányul (a tömeges zavarkeltés eszközeként), a cselekmény nem valósít meg se terrorcselekményt, se alkotmányos rend elleni cselekményt, annak ellenére, hogy a célzatban elgondolt fejlemény megvalósul.

A *rombolás* célzata az alkotmányos rend megzavarása ugyan, 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 (például www.mo.hu) nyitóoldalán elhelyezett zavarkeltő, lejáró szöveg elhelyezésével. A cselekmény nem tényállásszerű, mindazonáltal 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.

Az informatikai terrorizmus kategóriája láthatóan roppant széles spektrumot ölel fel, hiszen az informatikai bűncselekmények köre sincs még precízen körülhatárolva. Az informatikai módszerek gyors fejlődésére a jogalkotás, illetve a jogalkalmazás nehezen reagál. A fejlődés követését elősegítendő bekerült a számítástechnikai rendszer elleni cselekmények körében írt elkövetési magatartás, nevezetesen a rendszer működésének egyéb módon törté-

nő zavarása. Ez az elkövetési magatartás kellően határozatlan elem ahhoz, hogy kételyeket ébresszen az elkövető bűnössége iránt. Egy cselekmény terrorcselekménnyé nyilvánítását a magatartás célzata különbözteti meg az egyéb bűncselekményektől, ami nagy felelősséget ró a jogalkalmazókra. Ha valamely személy vonatkozásában terrorcselekmény gyanúja merül fel, a jelenlegi jogszabályi környezetben a szabadságjogok széles körben korlátozhatóvá válnak. Ehhez még az is társul, hogy mindezek a jogkorlátozások akkor is adottak, ha valaki a terrorcselekmény előkészületéhez kapcsolódó cselekményt valósít meg. Azt pedig kifejezetten nehéz megállapítani, hogy valaki akkor, amikor a terrorcselekmény eszközcselekményének elkövetéséhez szükséges vagy azt könnyítő feltételeket megteremti, szándéka a terrorcselekmény elkövetésére vagy az eszközcselekmény elkövetésére terjed ki. Fontos ezért, hogy a szabadságjogok korlátozásának szabályai egyértelműek, világosak, átláthatók legyenek, és a jogkorlátozás szükséges és arányos legyen az elérendő cél megvalósulása esetén bekövetkező előnnyel.

A magánélethez való jog a titkos információszerzés területén

A viselkedésalapú profilalkotás

Az állam célja a biztonság garantálása érdekében a leghatékonyabb módszerek igénybevétele. Ezzel szemben az alapvető emberi jogok jelentik a korlátot, e jogok folyamatosan konfliktusba kerülnek a hatóságok terrorizmus elleni küzdelemben betöltött bűnmegelőzési feladataival. Ennek következtében egyre több területen – a nemzetközi kötelezettségek teljesítése érdekében (eme együttműködés fontosságához sok kétség nem fér) – korlátozzuk szabadságjogainkat, annak ellenére, hogy Magyarországon idáig nem történt a nemzetközi terrorizmushoz kapcsolódó terrorcselekmény. Ennek a folyamatnak a következményét *Tálas Péter* szavaival tudnám legjobban összefoglalni: „*a szabadságjogok korlátozásával a terroristák céljait teljesítjük be magunkon*”.[9] Ebből adódik az államnak az a kötelessége, hogy csak olyan mértékben korlátozza a szabadságjogainkat, amennyire az a terrorcselekmények elkövetéséhez kapcsolódóan szükséges. Nem tekinthetünk minden magyar állampolgárra úgy, mintha potenciális terroristák lennének, vagy ha még nem

9 „A szabadságjogok korlátozásával a terroristák céljait teljesítjük be önmagunkon”. Interjú Tálas Péter biztonságpolitikai szakértővel. Fundamentum, 2005/3., 59. o.

azok, akkor azokká válhatnak. Az pedig eleve problémás, hogy e feltételezés alapján elrendelhetjük jogaik korlátozását.

Érdekes példája ennek az Amerikában szeptember 11. után elfogadott Patriot Act (hazafias törvény) azon rendelkezése, amely az egyetemi és közkönyvtárakat arra kötelezte, hogy az olvasók olvasási, kölcsönzési szokásairól megkeresésre, elektronikus úton információt szolgáltassanak a hatóságoknak. Ennek a korlátozásnak az volt a célja, hogy olvasási szokásaik alapján kiszűrje azokat a személyeket, akik lehetséges terroristák lehetnek. Erről az eshetőségről a kölcsönzött és kikért könyvek listájából vontak le következtetéseket.[10] A módszer legnagyobb veszélye abban rejlik, hogy pusztán az ilyen információk alapján alkotott vélemény, amely segíthet a terroristagyanús egyének feltérképezésében, széles körben magában foglalja a tévedés lehetőségét is.[11] Az informatika megjelenésével nagyban leegyszerűsödött a személyek adatainak kezelése, megismerése, szelektálása. Ezek az adatok szintén tartalmazhatnak olyan információkat, amelyek segítenek egy adott személyiség jellemzőinek összeállításában, lehetőséget adnak arra, hogy ezekből az adatokból valamely személyről különböző célokkal profilokat alkothassunk.

Az online marketing területén számtalan módszer született arra vonatkozóan, hogy az interneten keresztül történő termék-, illetve szolgáltatásértékesítéshez kapcsolódó reklámok csak a potenciális vásárlókhoz jussanak el, így növelve az értékesítés hatékonyságát, egyszersmind minimumon tartva a reklámozáshoz kapcsolódó költségeket. A módszert a szaknyelv *behaviour targeting*nek nevezi, e módszer segítségével az erre szakosodott információs társadalommal összefüggő szolgáltatást nyújtók a vásárlók internetes szokásai alapján vásárlói profilt alakítanak ki az egyénről. Erre a marketingtevékenységre felhatalmazást általában mindegyik online szolgáltatás igénybevételéhez szükséges regisztráció részeként felajánlott és javarészt olvasás nélkül elfogadott általános szerződési feltételek tartalmaznak. Ha két különböző személy egy időben ellátogat ugyanarra az általa gyakran látogatott hírportálra, akkor eltérő reklámokat olvashatnak. Ennek oka, hogy az adott szolgáltatók a reklámtevékenységük értékesítését összekötik a személyhez kapcsolódó

10 Miklósi Zoltán: A terrorizmus elleni „háború" és az emberi jogok. Fundamentum, 2004/3., 43. o.

11 Andrej Holm német társadalomtudós példáját lehet felhozni, akit a német hatóságok azért kezdtek el megfigyelni, mert olyan kifejezésekre keresett rá az interneten, amiből terrorista kötődéseire lehetett következtetni. Holm a berlini Humboldt Egyetem társadalomtudományi karán tanult, és tanulmányához kapcsolódóan gyűjtött információkat az interneten. Holm elfogása után egy hónapot töltött a hatóság őrizetében, szabadon bocsátását pedig annak köszönhette, hogy a Bundesgerichtshof hatályon kívül helyezte az elfogatóparancsot.

online direktmarketing-tevékenységükkel. A személyiségprofilunk pusztán annak alapján összeállítható, hogy milyen honlapokat látogatunk.

Ez úgy kapcsolódik az informatikai terrorizmus témájához, hogy azok az információk, amelyek alapján a vásárlói profilok készülnek, a bűnüldöző szervek, nyomozó hatóságok, nemzetbiztonsági szolgálatok, valamint az ügyészség rendelkezésére állnak egy évre visszamenőleg minden olyan állampolgárról, aki igénybe vette valamely hírközlő szolgáltató hírközlési szolgáltatását.

Az adatmegőrzési kötelesség és az adatszolgáltatási kötelezettség

Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve (a továbbiakban: adatmegőrzési irányelv) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről rendelkezik. Az adatmegőrzési irányelv (21) pontja értelmében az adatmerőzés célja, hogy az általa előírt adatok az egyes tagállamok nemzeti joga által meghatározott súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából a tagállamok rendelkezésére álljanak. Ennek alapján a hírközlő szolgáltatók megőrzik egyebek között a közlés forrásának és címzettjének megtalálásához és azonosításához szükséges adatokat, a közlés napjának, időpontjának és időtartamának megállapításához szükséges adatokat, illetve a közlés típusának megállapításához szükséges adatokat is (utóbbi az igénybe vett internetszolgáltatást takarja). Az adatmegőrzési irányelvben foglalt kötelezettségeket az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) tartalmazza.

Az Rtv. 68. §-a – bírói engedélyhez nem kötött titkos információgyűjtés keretében – lehetőséget ad az elektronikus hírközlő szolgáltatók által az Eht.-ban foglaltaknak megfelelően megőrzött adatok bekérésére. Ennek alapján minden kétévi vagy ennél súlyosabb szabadságvesztéssel büntetendő, szándékos bűncselekmény felderítése érdekében adott ez a lehetőség. Adatkérés keretében a hírközlő szolgáltató egyebek között a rendőrség rendelkezésére tudja bocsátani az internet-hozzáférési, internetes elektronikus levelezési, internetes telefonszolgáltatás, illetve ezek kombinációja esetén az elektronikus hírközlési szolgáltatás típusát és a szolgáltatás előfizető vagy felhasználó általi igénybevételének dátumát, kezdő és záró időpontját, az igénybevé-

telnél használt IP-címet, felhasználói azonosítót, illetve hívószámot. Az adatközléshez az ügyész előzetes jóváhagyása szükséges, de ha a késedelem veszéllyel jár, és az ügy kábítószer-kereskedelemmel, terrorizmussal, illegális fegyverkereskedelemmel, pénzmosással vagy szervezett bűnözéssel függ össze, az adatigényléshez az ügyész előzetes jóváhagyása sem kell, elegendő az adatkéréssel egyidejűleg intézkedni annak beszerzéséről.

Az adott rendelkezésekkel kapcsolatban két problémát látok körvonalazódni. Az első ellentmondás abból adódik, hogy a jogalkotó nem tett különbséget az adatszolgáltatási körbe vont adatok között, így az adat minőségétől függetlenül rendelte el az alapjogi korlátozást, ami néhány adat vonatkozásában ellentétes az Európa Tanács mint jogalkotó céljával. A második pedig abból adódik, hogy az adatmegőrzési irányelvben meghatározott, az adatkérésre alapot adó súlyos bűncselekmények körének meghatározása, illetve az Rtv.-ben meghatározott bűncselekményi kör a hazai jogszabályokban található értelmezésben ellentmondásra vezet. Jelenleg túl széles körben van lehetőségük a hatóságoknak az adatkérések előterjesztésére.

Az adatmegőrzési irányelv (20) és (22) pontjai értelmében az Európa Tanácsnak a számítástechnikai bűnözésről szóló 2001-es egyezménye (Cyber-Crime Convention; a továbbiakban: CCC), valamint az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló 1981-es egyezménye, az Európai Unió alapjogi chartájának 7. és 8. cikke vonatkozik az adatmegőrzési irányelv alapján megőrzött adatokra is.

A CCC három adattípus között tesz különbséget. Ezek az előfizetői adatok, a forgalomra vonatkozó adatok és a tartalomra vonatkozó adatok.[12] Az előfizetői, illetve a forgalomra vonatkozó adatok tekintetében alkalmazni lehet az adatmegőrzést, hiszen ezek az adatok nem tartalmaznak olyan érzékenységű személyes információkat, mint amilyeneket a tartalomra vonatkozó adatok. Ebből adódik, hogy az utóbbi adatokhoz csak bírói engedélyhez kötött titkos információgyűjtés/adatszerzés keretében lehet hozzáférni, az előző két csoportba tartozó adatokhoz az előbb tárgyalt adatkérés keretében is. A forgalomra vonatkozó adatok köre – azok személyhez kapcsolódó információtartalma vonatkozásában – eltérő jogkorlátozást indokolna. Míg az adott kommunikáció idejére, tartamára vonatkozó információk alapján arra lehet következtetni, hogy a kommunikációban részt vevő felek az adott idő-

12 Ahogy ez elnevezésükből is következik: az előfizető adatai tartalmazzák az előfizető személyének azonosításához szükséges adatokat, a forgalomra vonatkozó adatok a valamely informatikai kommunikáció azonosításához szükséges adatokat jelentik, míg a tartalomra vonatkozó adatokon a kommunikáció információtartalmát értjük.

pontban kapcsolatban voltak egymással, addig az igénybe vett szolgáltatás típusára vonatkozó információk alapján – az online-marketingmódszerekhez hasonló egyszerűséggel – bűnözői profil alakítható ki.

Ezekből az adatokból könnyen információ szerezhető egyebek között az adott személy társadalmi, politikai hovatartozására, hajlamaira és gyengeségeire is. Ha valaki gyakran látogat szexuális tartalmú oldalakat, akkor könnyen kapcsolatba hozható az illetővel a tiltott pornográf felvétellel visszaélés bűncselekmény. Ha valaki iszlám vallási oldalakat látogat, akkor személyében könnyen felfedezhető egy potenciális terrorista, hiszen előbb válhat terrorista abból, aki kapcsolatba kerül különböző terrorista oldalakkal, mint abból, aki elkerüli ezeket. Az iménti okfejtést támasztja alá a CCC indokolásának 227. pontja, amely a CCC 20. cikkére, a forgalomra vonatkozó adatok valós idejű összegyűjtésére vonatkozik. Az indokolás szerint: *„A forgalmi adatok az időről, az időtartamról, a kommunikáció hosszáról 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 (például a meglátogatott honlap vonatkozásában). Ezeknek az adatoknak a gyűjtése, néhány szituációban, lehetőséget kínál az adott ember profiljának összeállítására érdeklődési köréről, kapcsolatairól és társadalmi viszonyairól."*

Célszerű lenne ennek alapján különbséget tenni a különböző típusú forgalmi adatok között, és pontosan meghatározni, hogy melyek azok a bűncselekmények, amelyek esetén lehetősége lenne az államnak megismerni az egyes adatköröket.

A második probléma abból adódik, hogy jelenleg az Rtv. túl széles körben teszi lehetővé, hogy a felhatalmazott hatóságok megszerezzék az állampolgárokról az előfizetői, illetve a forgalomra vonatkozó adatokat. Az Rtv. 68. §-a minden kétévi vagy ennél súlyosabb szabadságvesztéssel büntetendő, szándékos bűncselekmény felderítése érdekében az üggyel összefüggő adatok szolgáltatását igényelheti a hírközlési szolgáltatóktól.[13] Az adatvédelmi adatmegőrzési irányelv 1. cikkének (1) bekezdése szerint az adatmegőrzés az egyes tagállamok nemzeti joga által meghatározott súlyos bűncselekmények kivizsgálása, felderítése és üldözése céljából áll rendelkezésre. Ez azt jelenti, hogy súlyos bűncselekménynek minősül – a bűntetti körnél szélesebben – minden legalább kétévi szabadságvesztéssel fenyegetett szándékos bűncse-

13 Az adatszolgáltatási kötelezettség az Eht. 156. §-ának (9) bekezdésében, 157. §-ának (10) bekezdésében, illetve 159/A §-ának (1)–(2) bekezdésében meghatározott adatokra terjed ki.

lekmény. Mivel a hatályos Btk.-ban viszonylag kevés az a bűncselekmény, amelynek büntetési tétele ne érné el a kétévi szabadságvesztést, ezért gyakorlatilag a hatályos szabályozás a legtöbb bűncselekményt súlyos bűncselekménynek minősíti. (A jelenlegi szabályozás alapján nem lehet megtudni egyebek között a zaklatás [Btk. 176/A §], a visszaélés személyes adattal [Btk. 177/A §], a rágalmazás [Btk. 179. §] és a számítástechnikai rendszerbe történő jogosulatlan belépés [Btk. 300/C §] bűncselekmények elkövetéséhez kapcsolódó forgalmi adatokat.) Sajátságos helyzetet okoz azonban, hogy az Rtv. 97. § (1) bekezdésének *i)* pontja a súlyos bűncselekmény fogalmán az ötévi vagy ezt meghaladó tartamú szabadságvesztéssel fenyegetett bűntetteket érti. Ez felveti annak a kérdését, hogy tényleg ilyen széles körben szükséges-e ezt az intézményt alkalmazni.

A adatmegőrzési irányelv Európa-szerte széles körben vitákat generált.[14] A megőrzés vitathatósága miatt az Eht. miniszteri indokolása a vitatható pontokkal kapcsolatban kitérő választ adott, az esetleges aránytalan alapjogi korlátozásból adódó felelősséget áthárította a büntető jogszabályokra: „*a hírközlési szolgáltatók természetesen nem végezhetnek bűnüldözési tevékenységet, azonban kötelesek az arra hatáskörrel rendelkező szervek ilyen irányú igényeinek kielégítését biztosítani. Erre tekintettel az Eht. szabályozásának sem lehet tárgya a konkrét esetkörök, feltételek meghatározása (például: súlyos bűncselekmények felderítése).*" Ebből következik, hogy az alapjogi aggályra okot adó szabályok az Rtv.-ben, illetve más ágazati szabályokban találhatók.

Az Emberi Jogok Európai Bírósága az ítéleteiben rámutatott, hogy a római egyezmény 8. cikk 1. bekezdésében garantált jog egy demokratikus társadalomban csak a 2. bekezdésben meghatározott törvényes keretek között, az ott rögzített célokból, a szükségesség igazolása mellett korlátozható.[15] Ehhez kapcsolódóan az Alkotmánybíróság 2/2007. (I. 24.) AB határozata 4.1. pontjában rögzítette, hogy a titkos adatgyűjtési eszközök és módszerek a demokratikus jogállamban egyes súlyos bűncselekmények kapcsán, ahol a hagyományos eszközök nem bizonyulnak elegendőnek, igénybe vehetők, ek-

14 Németországban az adatmegőrzési irányelvből fakadó kötelezettségekhez kapcsolódóan a német alkotmánybíróság hatályon kívül helyezte a kapcsolódó jogszabályokat. http://www.bundesverfassungsgericht.de/entscheidungen/rs20081028_1bvr025608.html; http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html

15 „1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges."

ként az ezzel járó alapjog-korlátozás önmagában nem szükségtelen, mindezekre azonban csupán kivételes, átmeneti, végső megoldásként kínálkozhat lehetőség. Az Emberi Jogok Európai Bírósága a Klass-ügyben[16] kifejtette, hogy az állampolgárok titkos megfigyelése a rendőrállamokra jellemző, így az csak annyiban fogadható el, amennyiben a nemzeti intézmények védelmében feltétlenül szükséges.

Ezek alapján elmondható, hogy önmagában az adatmegőrzési kötelezettség indokolt. A kérdés, hogy tényleg ilyen széles körben lehetőséget kell-e adni a hatóságoknak személyes adataink megismerésére. A szabályozás nemzetközi kötelezettségek teljesítési kényszerét követő jellege jól tetten érhető, hiszen pont azoknál a bűncselekményeknél nincs lehetőség a forgalomra vonatkozó adatok megismerésére, amelyek tipikusan vagy kizárólagosan informatikai környezetben követhetők el. Ezeknél a bűncselekményeknél az elkövető kilétének megállapításához szükséges az informatikai azonosítók, kommunikációs eszközök helyének meghatározása (például jogosulatlan belépés számítástechnikai rendszerbe). Ha az adatmegőrzési irányelv alapján kezelt adatok megismerhetőségét differenciálnánk, feloldanánk ezt az ellentmondást. Az IP-címek azonosítása a nyomozó hatóság elemi érdeke minden informatikai környezetben megvalósuló bűncselekmény esetében. Az ezzel kapcsolatos alapjogi korlátozás egyszerűen indokolható lenne úgy, hogy az adatkérésről a hatóságnak értesítenie kellene utólag az érintettet, mint ahogyan azt az Emberi Jogok Európai Bírósága a Mersch-ügyben[17] rögzítette. Az ítélet szerint egy demokratikus társadalomban az érdekelt személyeket az őket érintő titkos megfigyelésekről szükséges tájékoztatni, de csupán az után, hogy ez a tájékoztatás már nem veszélyezteti a művelet célját. Fontos lenne azonban, hogy ahhoz az adatkörhöz, amelyből az alapjogi jogosultak személyiségi, illetve tevékenységi profilja kialakítható lehet, bírói engedélyhez kötötten férhessen a hozzá a nyomozó hatóság vagy az ügyészség, annak érdekében, hogy a szükséges kontroll adott legyen. Ezt támasztják alá az említett AB-határozatban foglaltak is: az ellenőrzést a végrehajtó hatalomtól független „testületeknek" kell végezniük. Elsősorban az állandó, folyamatos és kötelező ellenőrzés a garancia arra, hogy a konkrét ügyekben nem sértik meg az arányosság követelményét[18].

16 Klass és társai kontra Németország (1978).

17 Julien Mersch és társai kontra Luxemburg (1985).

18 Például Case of Klass and Others v. Germany, judgment of 06/09/1978. Series A. 28; Case of Malone v. the United Kingdom, judgment of 02/08/1984. Series A 82.; Case of Leander v. Sweden, judgment of 26/03/1987. Series A. 116.

Az informatikai terrorizmus veszélye Magyarországon – az eddig megvalósuló cselekmények alapján – nem mondható nagynak. Nem szabad figyelmen kívül hagyni azonban azt a tényt, hogy más államokban egyre több energiát csoportosítanak különböző érdekcsoportok az informatikai támadások és az informatikai biztonság fejlesztése érdekében, tekintettel arra, hogy az „elektronikus dzsihád" terroristák általi használata, továbbá az egyre nagyobb számban megjelenő terrorista célzatú informatikai támadások ezt szükségessé teszik. Mindehhez azonban bölcs jogalkotásra és jogalkalmazásra van szükség, annak érdekében, hogy jogaink feleslegesen ne essenek áldozatául az ideológiák háborújának, különös tekintettel arra, hogy ez a harc tőlünk távoli hálózatokon keresztül folyik.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp21-48

MEZEY NÁNDOR LAJOS

Kiberterrorizmus: valós veszély?

Ha napjainkban meghalljuk a terrorizmus kifejezést, mindannyian öngyilkos merénylőkre, autókba rejtett pokolgépekre, emberrablásokra és hasonló, általában sok emberi életet követelő, jobbára politikai, vallási indíttatású cselekedetekre gondolunk, amelyekhez, mondhatni a terroristák legnagyobb örömére, kellő nyilvánosságot teremt mind a hagyományos, mind az elektronikus sajtó.

A terrorizmus hagyományos megjelenése mellett a számítástechnika előretörése a terroristáknak is rengeteg új elkövetési lehetőséget, célpontot kínálhat, ezáltal új feladatokat adhat a bűnüldöző szerveknek.

Az említett lehetőség ellenére, ha megállítanánk tíz embert az utcán, és megkérdeznénk, mit takar a kiberterrorizmus kifejezés, félő, hogy tíz egymástól jelentősen különböző választ kapnánk.

Ezen az arányon akkor sem tudnánk jelentősen javítani, ha a számítástechnika terén jártas embereknek tennénk fel a kérdést!

Márpedig ameddig a jelenségnek nincsen egységes fogalmi meghatározása, vagyis míg nincsen konszenzus a téren, pontosan mit is takar a jelenség, addig igen nehézzé válik a hatékony fellépés megszervezése.

A többféle értelmezés oka leginkább újdonságában keresendő. E jelenség, ellentétben a hagyományos terrorizmussal, nem a való világban zajlik, hanem virtuális számítógépes hálózatokon – jóllehet a hálózatok is valóságosak, mégis egy virtuális teret alkotnak.

Mondani sem kell, a politikusok, (biztonsági és informatikai) szakemberek és főként a média figyelmét gyorsan felkeltette e jelenség.

E tény nem is meglepő, hiszen ahogy a számítástechnika és a számítógépes hálózatok egyre inkább életünk és társadalmaink alapvető részévé válnak, továbbá egyre több információt tárolunk rajtuk, kiszolgáltatottabbá válunk hibátlan működésüknek.

Az előbbiekre tekintettel valóban ijesztőnek tűnhet a lehetőség, hogy egyes egyének, vagy csoportok a névtelenség és a nehezen azonosíthatóság védőernyője mögé bújva, meghatározott motívumok szerint, támadást indítanak az egyre komplexebbé – így egyre sebezhetőbbé – váló számítástechnikai rendszerek és alapvető, kritikus infrastruktúrák ellen, számítógépek és virtuális információk felhasználása révén.

Jóllehet a veszély mértéke semmiképpen sem elhanyagolandó, mindazonáltal ez eddig egyetlen nagyobb támadást sem jelentettek!

E tény felveti a kérdést: *egyáltalán, mennyire kell komolyan venni e jelenséget?*

Jelen cikkben a kiberterrorizmus jelenségét kívánom bemutatni, rávilágítva jellemzőire, elkövetőire, az elkövetés módszereire, a terroristák eszköztárára, a jelenség veszélyességére.

Fogalma

A kiberterrorizmus fogalmának meghatározása előtt szükségesnek tartom meghatározni a terrorizmus fogalmát is, hiszen a kiberterrorizmus a terrorizmus egyik megjelenési formája!

A *terrorizmus* az erőszak alkalmazásának vagy az azzal való fenyegetésnek olyan stratégiája, amelynek elsődleges célja félelem, zavar keltése és ennek révén meghatározott politikai eredmények elérése, vagy a hatalom megtartása.[1]

Az iménti definíciónak három lényegi eleme

– az erőszak alkalmazása, vagy azzal fenyegetés,
– politikai célok,
– félelem-, zavarkeltés.

A két jelenség közötti kapcsolat miatt nyilvánvalóan a kiberterrorizmusnak is bírnia kell e három jellemzővel.

Az egyes fogalomalkotási kísérletek bemutatása előtt ki kell emelni, hogy a jelenség pontos definiálását főként két tényező nehezíti.

– *Egyrészt* a média kiemelt figyelmet fordít e jelenségre, az újságírók azonban a pontos meghatározás helyett a jelenség felnagyításában, minél drámaibb színben feltüntetésében érdekeltek, megtévesztve az olvasókat.
– *Másrészt* gyakori, hogy a számítógépekhez kapcsolható jelenségek elnevezése során pusztán a „cyber", „computer", „information" stb. kifejezéseket illesztik egy már meglévő kifejezés elé, anélkül hogy pontosan meghatároznák azok lényegét.

1 http://hu.wikipedia.org/wiki/Terrorizmus

Jó példa erre a kiberterrorizmus is, hiszen e jelenséget rengeteg kifejezéssel illetik: *infowar, netwar, cyberterrorism, virtual warfare, digital terrorism, computer warfare* stb.[2]

Az iménti kitérő után, a teljesség igénye nélkül, íme, néhány meghatározás.

Az *FBI* a következő fogalmat alakította ki: *A kiberterrorizmus olyan bűncselekmény, amelyet számítógépes rendszerek, programok, adatok – polgári célpontok – ellen a nemzetnél kisebb csoportok vagy egyének intéznek politikai célok elérése érdekében.*[3]

Az amerikai nemzetiinfrastruktúra-védelmi központ (National Infrastructure Protection Center; NIPC) meghatározása a következőképpen hangzik: a kiberterrorizmus *olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs eszközökkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.*

Dorothy Denning a következőket érti kiberterrorizmuson: *Olyan jogellenes támadás, vagy azzal fenyegetés, amely számítógépek, hálózatok és az azokban tárolt adatok, információk ellen irányul, és célja a kormányzat vagy a lakosság megfélemlítése, vagy kényszerítése politikai, társadalmi célok elérése érdekében. Továbbá elengedhetetlen feltétel, hogy az erőszakos támadás személyek vagy tárgyak ellen irányuljon, de legalább kellő fenyegetést jelentsen ahhoz, hogy megfelelő mértékű félelmet keltsen.*[4]

Elhatárolása más hasonló jelenségektől

Hactivizmus – kiberterrorizmus

Az előbbi néhány meghatározás számbavétele után elengedhetetlen megkülönböztetni a kiberterrorizmust a *hacktivizmus* néven ismert jelenségtől. E megkülönböztetés két ok miatt is lényeges: egyrészt hasonló jelenségekről van szó; másrészt egyesek kifejezetten tagadják a kiberterrorizmus létezését, és csupán hackerkedésnek, hactivizmusnak tekintik.

2 Gabriel Weimann: Terror on the Internet. United State of Peace Press, Washington D.C., 2006, pp. 151–152.

3 Kathryn Kerr: Putting cyberterrorism into context. Computer Crime Research Center, October 9, 2004, http://www.crime-research.org/articles/putting_cyberterrorism/

4 Uo.

Az hactivizmus nem más, mint a hackerkedés és a politikai tevékenység, mozgalmak egyvelege. A hacktivisták (a hacker és az aktivista keveréke) és az „egyszerű" hackerek közötti legnagyobb különbség, hogy a hackerek tevékenységét nem politikai célok motiválják.

Ellentétben a kiberterrorizmussal, a hacktivizmus fegyvertára „mindöszsze" négy elemből áll:

– virtuális blokádok létrehozása,
– e-mail támadások, bombázás,
– hackelés és elektronikus betörés,
– vírusok és egyéb kártékony programok alkalmazása.

A *virtuális blokád* a valóságban is létesíthető blokádok, akadályok elektronikus megfelelője. Ennek keretében politikai aktivisták ellátogatnak a céloldalra, és megpróbálják – folyamatos forgalom létesítése révén – oly mértékben túlterhelni az oldalt, hogy az összeomoljon, mások számára elérhetetlenné váljon.

Az *e-mail bombázás* keretében a támadók több megoldás közül is választhatnak. Elsőként a célpont elektronikus levelezési címére egyszerre több száz vagy több ezer üzenetet, illetve annál kevesebb, de nagyméretű csatolmányokkal ellátott levelet küldenek, igen rövid időn belül *(Mass mailing).*

A második megoldás, amikor a célpont elektronikuslevél-címét bejegyzik több levelezési listára is, így a célpont hatalmas mennyiségben kap leveleket, ráadásul ebben az esetben nehezebb védekezni is, mivel sok helyről érkeznek üzenetek *(List linking).*

A levélbombázás e két esete egyrészt leterheli vagy megbénítja a levelezési fiókot, másrészt megtölti, így a fontos üzenetek nem feltétlenül érnek célba.

Az e-mail bombázás harmadik eseteként is felfogható, amikor a címzett számszakilag nem kap sok üzenetet, de azokhoz kártékony programokat kapcsolnak (sok esetben, a vírusirtók kijátszása céljából, tömörített állapotban) *(Zip bombing).*[5]

A sokak által jól ismert *spammelés* az e-mail bombázás egyik típusa, mégis jelentős különbséggel bír az ismertetett esetekhez képest.

A spam (kéretlen üzenet) küldése esetén egy vagy több e-mailt küldenek szét több (általában több száz) címzett részére, tehát a spammelésnél a cím-

5 http://en.wikipedia.org/wiki/E-mail_bomb

zettek száma a lényeges, ellentétben az említett esetkörrel, ahol a leveleket egy címzett kapja!

A *hackelés és elektronikus betörés* általánosságban engedély nélküli behatolást jelent számítástechnikai rendszerekbe, különböző célok elérése érdekében.

A hactivisták konkrétan az informatikai rendszereken tárolt olyan adatok (pénzügyi, üzleti, politika információk stb.) megszerzése érdekében törnek fel számítógépeket, számítógépes hálózatokat, amiket a későbbiekben felhasználhatnak politikai céljaik elérése érdekében.

A *vírusok és egyéb kártékony* programok működésük során – a valós vírusokhoz hasonlóan – folyamatosan többszörözik magukat, és megfertőzik a célszámítógépet, a tulajdonos tudta nélkül.

A vírusok különféle, akár jelentős károkat okozhatnak – például: adatvesztés, adatmódosítás, a rendszer lassítása vagy tönkretétele, politikai üzenetek továbbítása stb.

Az iménti ismertetésből is egyértelműen látszik, hogy a hactivizmus eszköztára széles körű, továbbá nagyobb szakismeret és nehézség nélkül alkalmazható.

Mint már korábban is kiemeltem, a hacktivizmus – akárcsak a vizsgált jelenség – politikailag motivált cselekedeteket takar, a két jelenség mégsem keverendő össze. A hacktivisták célja lehet figyelemfelhívás, az ellenfél ellehetetlenítése, megzavarása, de semmilyen körülmények között sem emberölés, megfélemlítés. Az előbbieken túl hangsúlyozni kell, hogy a két jelenség közötti határ elég keskeny, és könnyen elmosható, különösen akkor, ha a terrorista csoportok hackereket bérelnek fel, vagy saját maguk képeznek ki, illetve ha a hacktivisták kulcsfontosságú (kritikus) ellátórendszereket kezdenek támadni.[6]

A kiberterrorizmus lényege

Az átlagember – már csak a jelenséggel kapcsolatos véleménykülönbségek miatt is – a ténylegesnél több mindent sorolhat a kiberterrorizmus körébe, így célszerű tisztázni, mi *nem* kiberterrorizmus.

Nem tekintendő kiberterrorizmusnak:

– az ismert terrorista csoportok tagjai, támogatói közötti kommunikáció és adatátvitel biztonsága céljából *titkosítási technológiák alkalmazása,*

6 Gabriel Weimann: i. m. 157. o.

– az ismert terrorista szervezetek által különféle *kommunikációs megoldások alkalmazása* toborzási, támogatószerzési, szervezési, valamint propagandaterjesztési célból,
– egyes kibertámadási *technikák terroristák általi esetleges használata*, ami nem okoz jelentős károkat vagy félelmet a lakosság körében,
– olyan országból érkező *port-*[7] *szkennelés*[8], amely feltehetően támogat terrorista szervezeteket.[9]

Az előbbi negatív és leíró definíciókon, valamint csoportosításon túl a jelenség pontos megértéséhez fel kell tenni két lényeges kérdést:
– Léteznek-e olyan célpontok, amelyek támadása révén a terroristák elérhetik céljaikat?
– Ha léteznek alkalmas célpontok, vannak-e olyan személyek, akik képesek végrehajtani a támadásokat?[10]

Támadható rendszerek

Az első kérdést szinte fölösleges feltennünk, hiszen a válasz csakis igen lehet. A terroristák rengeteg célpont közül választhatnak, túlságosan is sok közül.

Mielőtt azonban átlépnénk a második és egyben lényegesebb kérdésre, célszerű alaposabban megvizsgálni a célpontokat, mivel azok vizsgálata révén, legalábbis részben, választ kapunk a második kérdésre is.

A célpontok számbavételekor mindenképp ki kell emelni, hogy napjaink társadalmai jelentős mértékben függenek az információs technológiai eszközök megbízható működésétől, ami jelentős veszélyeket rejt magában.

Gondoljunk csak arra, hogy az egyes társadalmak különböző területein (gazdaság, állami szektor, pénzügyi világ stb.) nélkülözhetetlenné váltak eme eszközök, mindamellett a számítástechnikai eszközök jelentős mértékű használata magával hozta az egyes rendszerek sebezhetőségét és támadhatóságát.

Általánosságban elmondhatjuk tehát, hogy minden olyan rendszer, amely valamilyen formában kapcsolódik a kibertérhez, potenciális célpontnak tekinthető a kiberterroristák számára (is).

7 *Port:* hálózatba kötött számítógépek, számítástechnikai eszközök egymás közötti kommunikációját lehetővé tevő csatlakozási pont. Lényegében az egyes eszközök közötti adatforgalom lehetőségét megteremtő kapu.

8 *Portszkennelés:* hálózati helyek portjainak vizsgálta, meghatározott cél érdekében.

9 Kathryn Kerr: i. m.

10 Gabriel Weimann: Cyberterrorism: How Real Is the Threat? United States Institute of Peace, May 2004, http://www.usip.org/pubs/specialreports/sr119.html

Értelemszerűen a terroristák kizárólag olyan célpontokat fognak támadni, amelyek egyrészt kellően sebezhetők, másrészt a támadás révén elérhetik céljaikat. E két feltételnek leginkább a *kritikus infrastruktúrák* felelnek meg.

Célkeresztben a kritikus infrastruktúrák

A kiberterrorizmus elsődleges célpontjai tehát az úgynevezett kritikus infrastruktúrák, számbavételük előtt szükségesnek tartom röviden kitérni az infrastruktúra fogalmának meghatározására.

Általánosságban infrastruktúrán azon eszközök és intézmények összességét értjük, amelyek bár nem részei a közvetlen termelési folyamatnak, viszont annak nélkülözhetetlen feltételei.

Az infrastruktúrákat sokféleképpen lehet csoportosítani, ezek bemutatása nélkül néhány példával szemléltetve, infrastruktúrának minősül: a közlekedés, hírközlés, kereskedelem, vízgazdálkodás, jogrend, adórendszer, szervezetek, állami apparátus, honvédelem, rend- és tűzvédelem, igazságszolgáltatás stb.[11]

Az egyes infrastruktúrák között meg kell különböztetnünk azokat, amelyek leállítása vagy működésük megzavarása súlyos következményekkel járhat, vagyis a kritikus infrastruktúrákat. E fogalmat is sokféleképpen lehet definiálni, de itt csak kettőt említek.

E speciális infrastruktúrák egyik lehetséges megfogalmazás szerint: „*a nemzeti, szövetségi és uniós infrastruktúra azon létfontosságú elemei, melyek jelentős károsodása, üzemzavara vagy megsemmisülése súlyos következményekkel járna a nemzet vagy a nemzetek biztonságára, a gazdaságra, a környezetre és közegészségre, illetve az egyes kormányok, az állam hatékony működésére*”.[12]

Egy általánosabb meghatározás szerint: *kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nem-*

11 Kovács Ferenc: A kritikus infrastruktúra elméleti alapjai. IVB Innovációs Klubnap, 2008. december 11. http://www.ivb.org.hu/documents/INNOVACIOSklub/200812ho/KIelmeletia.ppt

12 Uo.

zetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.[13]

A teljesség igénye nélkül a legfontosabb kritikus infrastruktúrák:

– energiatermelő és -elosztó infrastruktúrák (különböző típusú erőművek, energiahordozó-kitermelő, -feldolgozó egységek, energiahordozókat szállító vezetékek stb.);
– banki és pénzügyi infrastruktúrák (banki hálózatok, kereskedelmi központok, egyéb pénzügyi szervezetek stb.);
– vízellátó, közmű-infrastruktúrák (víztisztítók, víztározók, vízvezetékek és csatornák stb.);
– távközlési és kommunikációs infrastruktúrák (távközlési és kommunikációs eszközök, számítógép-alapú hálózatok stb.);
– szállító infrastruktúrák (nemzeti légitársaságok, repülőterek, személy- és teherszállítás, út- és autópálya-hálózatok, vasúti hálózatok, vízi szállítóeszközök stb.);
– katasztrófavédelmi infrastruktúrák (rendőrség, tűzoltóság, kórházak és egyéb egészségügyi intézetek, katasztrófaelhárító szolgálatok stb.);
– honvédelmi, katonai infrastruktúrák;
– élelmiszer-ellátási infrastruktúrák.

A felsorolásból is látszik, hogy egymástól különálló rendszerekről van szó, azok mégis legtöbbször feltételezik egymást, és alapjaiban befolyásolják egy egész társadalom működését.

Jelentőségük mellett tovább növeli e rendszerek sebezhetőségét, hogy szinte valamennyi teljesen vagy jórészt számítógépes hálózatokra, vagy ezek egyes elemeire, de mindenképp számítástechnikai eszközökre épül – e rendszerek irányítását és felügyeletét külön számítógépes rendszerek végzik.

Ki kell emelni, hogy a számítógépes hálózatok legtöbb esetben nem zártak, hanem – a minél nagyobb hatékonyság és a kooperáció kiaknázása céljából – kapcsolatban állnak egymással.

Nem nehéz belátni, hogy minél több kapcsolódási pontja van egy rendszernek, annál könnyebben támadható, illetve annál nehezebben védhető, hiszen a nagyszámú kapcsolódási pont felderítése és folyamatos levédése rengeteg erőforrást köthet le.

A nagyszámú kapcsolódási lehetőség mellett a számítógépes rendszerek, illetve a használt programok tökéletlensége is további problémákat vet fel.

13 Uo.

Hiába javítják folyamatosan a programokat, azok sosem lesznek tökéletesek, mindig lesznek kiskapuk, amelyeket felderítve be lehet törni a rendszerekbe!

Mindenképpen hangsúlyoznom kell, hogy e rendszerek nemcsak elektronikus úton, hanem fizikailag – mondhatni a „hagyományos" módszerekkel – is támadhatók, így a védelem megszervezésekor több irányú, különböző típusú (hagyományos, elektronikus) támadással is számolni kell.

A két támadási mód közötti jelentős különbségek igencsak megnehezíthetik a védelem megszervezését.

Az előbbi általános megállapítások mellett ki kell emelni, hogy a legtöbb állam nagy hangsúlyt helyez a kritikus infrastruktúrák, azon belül különösen a haditechnikai, honvédelmi rendszer védelmére, így a kritikus infrastruktúrákon belül meg lehet különböztetni jobban és kevésbé védett rendszereket. Példaként felhozható a fegyverraktárak és a kőolajvezetékek helyzete, mindkettő vitathatatlanul kritikus infrastruktúra, mégis egyértelműen az előbbit védik jobban, már csak lokalizálhatósága miatt is.

Az erősebben védett kritikus infrastruktúrák fizikailag gyakran nagyon nehezen támadhatók, így az elektronikus támadás lehetősége roppant kecsegtető lehet a terroristák számára.

Természetesen az egyes államok gyorsan felismerték e veszélyt, és megfelelő védelmi megoldásokat iktattak be.

E rendszerek többségénél egyedi – kifejezetten a rendszer adottságaihoz igazodó – programokat használnak (amelyek a telepítés előtt esetleg még külön állami hivatal általi ellenőrzésen esnek át), amelyek mellé erős, nehezen feltörhető védelmi megoldásokat párosítottak, nem beszélve arról, hogy a legtöbb ilyen rendszer nem is kapcsolódik közvetlenül az internetre (a kiberterroristák fő mozgási és vadászterülete), így azok kívülről elérhetetlenek a támadók számára.

Az említett megoldások alkalmazása miatt igen kicsi az esélye az erősen védett kritikus infrastruktúrákat érő támadásnak, így a kiberterroristák kénytelenek a kevésbé védett kritikus infrastruktúrák között válogatni, ezek jó része a magánszférában helyezkedik el.

Az alacsonyabb szintű védelem mellé az internet nagymértékű használta is társulhat, ami tovább növeli támadhatóságuk lehetőségét.

A kevésbé védett kritikus rendszerek támadása (például vízvezetékek, elektromos hálózatok stb.) nem feltétlenül fenyeget olyan hatalmas és azonnali pusztítással, mint például a katonai fegyvereket érő támadás, de mégis e

rendszerek megzavarása vagy tönkretétele jelentősen képes megzavarni a lakosság vagy az adott közösség életét.[14]

A kritikus infrastruktúrák mellett mindenképpen számolni kell az előbbi csoportba nem sorolható infrastruktúrák, rendszerek támadásának lehetőségével is.

Vegyünk például egy nagyszámú személyi adatot tartalmazó rendszert, amely ellen intézett támadással a kiberterroristák megszereznek több ezer személyi adatot.

Önmagában e cselekedet veszélyessége messze a kritikus infrastruktúrák ellen intézett támadás szintje alatt marad, mindamellett a megszerzett adatokat felhasználva a terroristák egy későbbi támadás vagy egyéb tevékenykedésük (például bizonyos termékek beszerzése interneten keresztül stb.) során elfedhetik valódi személyazonosságukat, nehéz helyzetbe hozva a hatóságokat, no meg persze azt, akinek ellopták az adatait.

A mai világban az iménti eset alapján számolni lehet a virtuális személyi adatok ellopásával is (közismert és adott személyhez köthető becenevek, belépési adatok, jelszavak stb.), amelyeket a kiberterroristák szintén fel tudnak használni támadásaik előkészítése, végrehajtása során.[15]

Alkalmas elkövetők

A lehetséges célpontok számbavétele után feltehetjük a fontosabb kérdést. Láthattuk, hogy a számítástechnika széles körű használata miatt rengeteg potenciális célponttal kell számolnunk, de vajon létezik olyan megfelelően képzett és főleg motivált elkövetői csoport, amely a számítástechnikai rendszerek tökéletlenségét kihasználva képes terrorcselekményeket végrehajtani a korábban bemutatott rendszerek ellen?

Mielőtt választ keresnénk a feltett kérdésre, szükségesnek tartom megvizsgálni, egyáltalán kik jöhetnek szóba lehetséges elkövetőként.

Akárcsak a számítógépes bűnözés egyéb megjelenési formáinál, a lehetséges elkövetőknek két konjunktív feltételnek kell megfelelniük:

– egyrészt olyan helyzetben kell lenniük, amely lehetővé teszi számukra a számítógép vagy egyéb számítástechnikai berendezés használatát,

14 Joshua Green: The Myth of Cyberterrorism, There are many ways terrorists can kill you—computers aren't one of them. Washington Monthly, November 2002 http://www.washingtonmonthly.com/features/2001/0211.green.html

15 Sarah Gordon: Cyberterrorism? Symantec Security Response. http://www.symantec.com/avcenter/reference/cyberterrorism.pdf, p. 7.

– másrészt megfelelő szinten kell érteniük a technikai eszközökhöz, azok kezeléséhez.

Ezek után vegyük számba, kiknek lehet megfelelő képzettségük ahhoz, hogy terrorcselekményt hajtsanak végre.

Talán nem meglepő módon a sort a *hackerek* nyitják! A hacker – általánosságban – olyan számítástechnikai szakember, aki az átlagosat messze meghaladó szinten ismeri az informatikai rendszerek működését (az ötvenes, de különösen a hatvanas években elsősorban azokat nevezték így, akik a szokásostól eltérő módon használták az új technológiát és kiemelkedő szintű szaktudásukat).

E szakemberek komoly szakismeretük segítségével képesek (lehetnek) egy adott rendszerbe „betörni" (azt engedély nélkül használni), és azon belül különféle módosításokat végrehajtani, avagy információt eltulajdonítani, megváltoztatni. Céljuk szerint a hackerek négy plusz egy csoportját különböztetjük meg:

Az *első* csoportot az úgynevezett „jó vagy etikus hackerek", más néven fehér kalapos hackerek *(white hat hacker)* alkotják. Ők károkozási cél nélkül törnek be rendszerekbe, és a sikeres műveletek után felhívják a rendszergazdák figyelmét a védelmi hiányosságokra, gyenge pontokra, vagyis segítő szándék vezérli őket. E csoporton belül külön kategória, akik eseti vagy állandó megbízás alapján végzik munkájukat, ők a szakértő rendszertesztelők.

A *második* csoportba, a mondhatni „kevésbé jóindulatú szakértők", a fekete kalapos hackerek *(black hat hacker)*, más néven *cracker*ek tartoznak. A köznyelvben általában a hacker kifejezésen kizárólag ezeket a szaktudásukkal visszaélő szakembereket értik, akik fehér kalapos társaikhoz hasonlóan szintén idegen számítógépes rendszerekbe az őket védő védelmi programok kijátszása, feltörése révén jutnak be, de gyökeresen más célokból. A fekete kalapos hackerek céljai igen sokfélék lehetnek: károkozás, haszonszerzés, képességeik tesztelése, erőfitogtatás, kíváncsiság, tapasztalatszerzés, de előfordul, hogy egyfajta sportként tekintenek saját tevékenységükre.

A *harmadik* csoportot az előbbi kettő keresztezését jelentő szürke kalapos hackerek *(grey hat hacker)* alkotják, akik hol legálisan, hol illegálisan tevékenykednek. Ki kell emelni, hogy általában nem önös érdekből vagy károkozási célból tevékenykednek, pusztán illegális cselekedeteket *is* elkövetnek legális munkájuk közben. E csoport egyfajta szürke zónát alkot.

A *negyedik* csoportot a hacktivisták alkotják, akik, mint korábban kiemeltem, olyan hackerek, akik technikai eszközöket használnak politikai, ideoló-

giai, vallási üzeneteik közvetítésére, általában weboldalak feltörése, átalakítása, túlterhelése (például DoS, flood) révén.[16]

A hacktivisták megmozdulására jó példa az 1999-ben amerikai szervereket érő kínai támadás, amely a belgrádi kínai nagykövetséget érő NATO-találat hatására történt.[17]

Végül az *ötödik* csoportba az úgynevezett *script kiddie*-k tartoznak, vagyis a képzetlen, mélyebb számítástechnikai ismeretekkel nem bíró crackerek. Ők a profi hackerek által készített és internetre feltöltött segédprogramok (scriptek) segítségével törnek fel szervereket, vagyis e csoport a szakértő hackerek nélkül nem is létezne. Tekintettel arra, hogy e személyek, magas szintű képzettség hiányában, kilógnak a valódi hackerek sorából, így nem tekinthetjük őket teljes értékű, ötödik csoportnak.

A lehetséges elkövetők sorában a következő csoport a *phreak*ek. A phreak olyan személy, aki telekommunikációs rendszereket – elsősorban telefonhálózatot és ahhoz kapcsolódó eszközöket – tanulmányoz, illetéktelenül igénybe vesz, felhasznál céljai elérése érdekében.

A phreakek tulajdonképpen telekommunikációs szakemberek, szaktudásuk segítségével akár telefonközpontok működését is manipulálhatják. Értelemszerűen a mobiltelefon-hálózatok sem menekülhettek el e csoport elől, különösen a hálózat illetéktelen lehallgatására kell gondolni. A telekommunikációs rendszerek komputerizálása után a phreakek és a hackerek közel kerültek egymáshoz, hiszen mindkét csoport tagjai a számítógépes hálózatok feltörésével, manipulálásával foglalkoznak.

Az említett változás következtében átalakuló *phreaking* jelenségre esetenként H/P (H = Hacking; P = Phreaking) kultúraként hivatkoznak.[18]

Az előbbi csoportok mellett az *ipari kémeket* is fel kell venni a lehetséges elkövetők listájára. Az egyes iparágakban folytatott illegális információszerzés régóta fennálló jelenség, az idők folyamán csupán az elkövetési módszerek változtak. A számítógépek és a számítástechnika elterjedése az iparban mind a tervezés, irányítás és rendszerfelügyelet terén magával hozta annak veszélyét, hogy a számítógépeken és hálózatokon tárolt hatalmas mennyiségű adatokat és információkat illetéktelenek (ipari kémek, konkurens cégek alkalmazottai) megszerezhetik és értékesíthetik.[19]

16 http://en.wikipedia.org/wiki/Hacker_(computer_security)

17 Kovács László: Az információs terrorizmus eszköztára. Robothadviselés 6. Konferencia. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006. november 22. Hadmérnök, Különszám, 2007. január http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html

18 http://en.wikipedia.org/wiki/Phreaking

19 Kovács László: i. m.

Hangsúlyozni kell, hogy e kémek nem kizárólag a magánszférában tevékenykedhetnek, a katonai adatok megszerzése és értékesítése révén szintén jelentős bevételre lehet szert tenni.

Tulajdonképpen az ipari kémek – amennyiben a számítógépes hálózatokat használják eszközként a kívánt adatok megszerzésére – is hackerek, de speciális céljaik miatt célszerű külön csoportba sorolni őket. Talán a legveszélyesebb potenciális elkövetők – szemben az előbbi külső támadókkal – éppen a *belső szakértők* és a rendszer működésébe bevont *külső személyek*.[20]

Egy komputerizált szervezet vagy rendszer működtetésében, amelyik rengeteg, esetleg rendkívül fontos adatot tárol, óriási szerep és felelősség hárul a szakértőkre. Szükségesnek tartom kiemelni, hogy nemcsak számítástechnikai szakértőkre kell gondolni, bár kétségtelen, hogy a vizsgált jelenség feltételezi a számítástechnika terén jártas elkövetők létét, de a belső szakértők, a bűnsegéd szerepét betöltve, más végzettségűek is lehetnek. A szakértők több szempontból is veszélyt jelentenek egy rendszerre.

Egyrészt magas szintű hálózati hozzáférésük van, illetve nem számítástechnikai szakember esetén, hozzáférnek a rendszer egyes elemeihez, még akkor is, ha megosztják a jogosultságokat az egyes szakértők között. *Másrészt* szakképzettségük folytán. *Harmadrészt* rendszerismeretük miatt, hiszen leginkább a belső szakértők ismerik a rendszer működését, annak gyengéit, hiányosságait.

A bemutatott veszélyességi tényezők miatt a belső szakértők szinte az ideális elkövetők, hiszen amellett, hogy hatékonyan képesek végrehajtani tettüket, jogosultságuk folytán az összes árulkodó nyomot is eltüntethetik.

Mindezeken túl a belső emberek akkor is veszélyt jelenthetnek, ha maguk nem követnek el semmilyen cselekményt, de kulcsfontosságú adatokat adnak ki harmadik személyeknek, akik aztán a megszerzett adatok birtokában támadhatják és esetleg működésképtelenné tehetik a rendszer kulcspontjait. A külső személyek szintén kaphatnak jelentős mértékű hozzáférési jogokat a teljes rendszerhez vagy egyes elemeihez. Ráadásul a külső személyek esetében még a munkavállalói hűségre sem lehet építeni, hiszen míg egy több éve a szervezetben dolgozó belső szakértő esetén számolni lehet e tényezővel, egy rövid ideig a szervezet keretében dolgozó külső személynél aligha.

A lehetséges elkövetők számbavétele után rátérhetünk a tényleges kérdésre: *A potenciális elkövetők, bár elméletileg képesek végrehajtani (kiber)ter-*

20 Uo.

rorcselekményeket, vajon ténylegesen is végrehajthatnak támadásokat a korábban bemutatott rendszerek ellen?

Mindenképp le kell szögezni, hogy – mivel nincsen feltörhetetlen rendszer – a potenciális elkövetők fel tudják törni a korábban nevesített rendszereket, de nem elegendő feltörni őket, mondhatni, ez a könnyebbik fele! A kívánt eredmény elérése érdekében a rendszer feltörése után megfelelő módosításokat kell végrehajtani.

A mai rendszerek többsége egyszerűen túl bonyolult ahhoz, hogy valódi rendszerismeret nélkül jelentős károkat, vagy akár csak jelentős üzemzavart lehessen előidézni bennük.

Az IBM Global Security Analysis Lab 2002-es jelentése szerint a hackerek csaknem kilencven százalékának nincsen kellő szakismerete, mondhatni amatőrök, így a kritikus rendszereket sem tudnák feltörni, kilenc százalékuk már elég képzett a rendszerek feltöréséhez, de a behatolás ellenére nem lennének képesek jelentős károkat okozni, végül mindössze egy százalékuk kellően képzett és motivált ahhoz, hogy feltört rendszerekben súlyos károkat okozzon, vagy akár megbénítsa őket.

A jelentést alátámasztja *Douglas Thomas*nak, a Dél-kaliforniai Egyetem professzorának vizsgálata is. Thomas több száz hackert hallgatott meg tevékenységük jobb megértése érdekében. Kutatása eredményét a következőképpen összegezte: *„A hackerek túlnyomó többsége, legalább 99 százalékuk részéről elhanyagolható a kiber-terrortámadás veszélye, azon egyszerű ok miatt, mivel az említetteknek egyszerűen nincsen kellő szakismeretük vagy lehetőségük egy olyan támadás végrehajtásához, mely egy kisebb zavarnál többet tudna okozni."*[21]

A külső támadók próbálkozásai mellett, mint már hangsúlyoztam, nagyobb veszélyt jelentenek a belső alkalmazottak, akiknek ráadásul kellő rendszerismeretük is van, így sokkal nagyobb eséllyel okoznak súlyos károkat.

A következő, gyakran hivatkozott eset 2000 márciusában történt az ausztrál Queenslandben, a Maroochy Water Services szennyvízkezelő üzemben. *Vitek Boden*, miután elbocsátották munkahelyéről, egy laptop és egy rádió adóvevő segítségével behatolt az üzem számítógépes rendszerébe, és több pumpa átállításával egymillió liter szennyvizet engedett a Queensland menti vizekbe. Az elkövető előállítása után derült fény arra, hogy Boden a szennyvízkezelő üzem biztonsági rendszerét tervező vállalat dolgozója volt.[22]

21 Gabriel Weimann (2006): i. m. 165. o.

22 http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

A kritikus infrastruktúrákat irányító számítógépes rendszerek nem megfelelő védettsége esetén kialakuló veszélyhelyzetek lehetőségének igazolására többször is felhozták a szennyvízkezelő üzemben történteket.

Jóllehet a hasonló esetek súlyos veszélyeket hordoznak magukban, az eset mégis speciális, hiszen a támadást olyasvalaki hajtotta végre, aki jól ismerte a rendszer működését, ráadásul a bosszú vezérelte, és nem politikai, vallási célok, így a hasonló eseteket semmiképpen sem lehet kibertámadásnak minősíteni.

Tekintettel arra, hogy a kritikus infrastruktúrák a külső és a rendszert nem ismerő személyek számára nehezen támadhatók, így elméletben lehetséges, hogy a terroristák – saját dolguk megkönnyítése érdekében – belső embereket szerveznek be. A károkozás mértéke ebben az esetben is csupán korlátozott lehet, egyrészt a rendszerek – jobb esetben a személyzet által kiiktathatatlan – védelmi megoldásai miatt, másrészt a személyzet többi tagja miatt, akik megpróbálnák elhárítani társuk károkozását.[23]

Összegezve az eddigieket, a lehetséges elkövetők többségének lehet megfelelő szintű szaktudása és eszköze ahhoz, hogy számítógépes rendszereket támadjanak, mindazonáltal hiányzik a kellő motivációjuk a súlyos következményekkel járó támadások végrehajtásához.

Az igazi veszélyt tehát nem az említett lehetséges elkövetők jelentik. Jóllehet fejtörést okozhatnak a biztonsági szakembereknek, és mindenképp szükséges velük számolni, mint lehetséges veszélyforrással, a legnagyobb veszélyt pontosan azok a csoportok jelentik, amelyek a való világban is terrorcselekményeket hajtanak végre.

A kiberterrorizmus struktúrája

1999 augusztusában a kaliforniai Montereyben található Terrorizmus- és irregulárishadviselés-vizsgáló központ (Naval Postgraduate School Center for the Study of Terrorism and Irregular Warfare) jelentése *(Cyberterror: Prospects and Implications)* a következőképpen rendszerezi a kiberterrorizmus struktúráját:

a) Egyszerű, szervezetlen: e szervezetek képesek a mások által készített programokkal egyszerűbb támadásokat végrehajtani egyéni rendszerek ellen. Az ilyen szervezeteknek általában semmilyen célpontelemzési, irányítási és vezetési, valamint önfejlesztési képességük nincs.

23 Joshua Green: i. m.

b) Fejlett, szervezett: elméletileg már több és nagyobb rendszerek, illetve hálózatok ellen is végrehajthatnak sikeres támadásokat, valamint egyszerűbb programokat is készíthetnek. Az ilyen szervezetnek alapvető célpontelemzési, irányítási, vezetési és fejlődési képessége van.

c) Összetett, koordinált: e szervezet már összehangolt, súlyos zavart és esetleges károkat okozó támadások végrehajtására is képes. A szervezet tagjai már valódi hackeléshez használt programokat is készíthetnek. Magas szintű célpontelemzés, irányítás, vezetés és önfejlesztő képesség jellemzi e csoportokat.

A vizsgálat összegzése szerint egy az alapoktól induló csoportnak legalább kettő-négy év kell a szervezett, és hat-tíz év az összetett szint eléréséhez. Természetesen külső források bevonásával erősen csökkenthető ez az időintervallum.[24]

Miért használnák a kiberterroristák az internetet, mik a céljaik?

Az internet előnyei a kiberterroristáknak

Feltehetjük a kérdést: a számítástechnika felhasználásával elkövetett terrorcselekmények vajon miért lehetnek vonzóbbak a terroristák számára a hagyományosnak nevezhető módszereknél akkor, amikor több évet kell tölteniük a kellő szakismeret megszerzésével, programokat és számítástechnikai eszközöket kell beszerezniük, és a siker, az egyre fejlettebb védelmi megoldások következtében, messze nem garantált?

Ráadásul a hagyományos elkövetési módszerek esetében jóval rövidebb idő alatt hozzá lehet jutni a szükséges eszközökhöz.

Több előnye is van az elektronikus útnak:

– *Egyrészt* messze olcsóbb, mint a hagyományos módszerek, hiszen a támadás megvalósításához csupán számítógépre és internetkapcsolatra van szükség, ezek, ellentétben például a robbanóanyagokkal, fegyverekkel, könnyedén, bármely számítástechnikai üzletben, jogszerűen beszerezhetők, ezzel is csökkentve a lelepleződés veszélyét.

24 Dorothy E. Denning: Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University May 23, 2000 http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

– *Másrészt* a kiberterrorizmus személytelenebb, mint a hagyományos módszerek. Ez esetben ugyanis a terroristáknak nem szükséges fizikailag is jelen lenniük az elkövetés helyszínén (vagy annak közelében), ez pedig szintén a lelepleződés veszélyét csökkenti. Nem is beszélve a célpontig és vissza vezető utazás közben fennálló lelepleződés veszélyéről (ellenőrző pontok, rendőrségi útzárak, határok stb.). Hagyományos társával ellentétben a kiberterrorista fantomnév, vagy korábban megszerzett létező személy valós vagy interneten használt adataival beléphet weboldalakra, rendszerekbe, ezáltal jelentősen megnehezítve valódi személyazonosságának kiderítését, ráadásul más személyre terelhetik a gyanút.
– *Harmadrészt* a célpontok nagy száma is pozitív tényezőként esik latba. A korábban bemutatott célpontok igen széles körén is látszik, hogy a kiberterroristák szabadon válogathatnak kormányzati, illetve magánszférában lévő célpontok (számítógépes rendszerek, kritikus infrastruktúrák) között. A célpontok nagy száma szinte garantálja, hogy előbb-utóbb még a kevésbé képzett elkövetők is találnak olyan célpontot, amely nem kellően védett, vagy olyan gyenge pontot, amelyen keresztül kellő mértékű zavart kelthetnek egyes rendszerekben. További előnyt jelentenek a kiberterroristák számára a számítógépes hálózatok és elsősorban az internet felépítéséből és jellemzőiből következő támadási és adatszerzési lehetőségek. Példának okáért egy jelentős károkkal fenyegető kártékony program szétküldése, amely gyorsan terjed az interneten, tökéletes „elterelő hadművelet" is lehet a támadások előtt.
– *Negyedrészt* a kibertámadásokat számítógépekkel hajtják végre, így, ellentétben a hagyományos terroristákkal, nem szükséges felkészíteni őket, sem testileg, sem lelkileg. Az emberveszteség lehetősége szinte kizárt, a lelepleződésé pedig jóval alacsonyabb, mint a hagyományos támadások esetén. A kiképzés kiiktatása idő és leginkább jelentős költségek megtakarítását jelenti. Jóllehet egyfajta kiképzésre a kiberterroristáknak is szükségük van, mégpedig kellő számítástechnikai jártasságot kell szerezniük, de ez könyvekből is elsajátítható. Esetükben nincs szükség külön táborra és kiképzőhelyre, a testi kiképzéshez szükséges felszerelések beszerzésére stb.
– *Ötödrészt* a kibertámadásokkal jóval több ember életét befolyásolhatják, gondoljunk például a víztisztító rendszerekre. A nagyobb veszély – még ha csak lehetőség is – nagyobb visszhangot és nagyobb médiaérdeklődést vált ki, így az adott terrorszervezet nagyobb nyilvánossághoz juthat.[25]

25 Gabriel Weimann (2004): i. m.

Az előbbi felsorolásból is kitűnik, hogy jó néhány igen jelentős előnnyel kecsegtet a számítástechnika alkalmazása mind a hagyományos, mind a kiberterroristák számára, de e csúcstechnika nyújtotta lehetőségeket nemcsak a konkrét támadások végrehajtásakor használhatják ki, hanem egyéb területeken is.

Kommunikáció, koordináció, tervezés, információszerzés – könnyen belátható, hogy a terroristák – akár a hagyományos, akár a modern módszereket választók – kezében az internet nagy segítséget nyújthat mind a kommunikáció, mind a szervezés területén. Az interneten több kapcsolattartási mód közül is válogathatnak az elkövetők (például chatszobák, weboldal-üzenőfal, azonnali üzenet küldésére alkalmas programok), ezek segítségével személyes kapcsolat nélkül szervezhetik akcióikat. A személyes kapcsolat hiánya tovább nehezíti a nyomozó hatóságok munkáját is, hiszen egy sikeres rajtaütéskor egyszerre csak egy terroristát foghatnak el, aki ráadásul nem is ismeri társai valódi személyét, így információkat sem adhat róluk.

Az internet viszonylagos névtelensége, illetve esetlegesen lopott adatok segítségével valós személyazonosságuk tekintetében a terrorista szervezet tagjai egymást is megtéveszthetik.

Akárcsak a való világban, az interneten és egyéb számítógépes hálózatokon alkalmazhatók különféle titkosítások. A könnyedén beszerezhető titkosító programok akár erős titkosítással is kódolhatják a kívánt dokumentumot, és segítségükkel a terroristák ilyen formában is eljuttathatják társaiknak különösen fontos adataikat.

Az erős titkosítások a világ titkosszolgálatainak rémálmai, így nem csoda, hogy igyekeznek kiskapukat beépíttetni a kereskedelmi forgalomba kerülő titkosító eszközökbe, az ezek által generált kódot, egyéb támpont hiányában, kizárólag „nyers erővel" *(brute force)* – vagyis az összes létező kombináció végigpróbálása révén – lehet feltörni. Mindazonáltal a terrorista szervezetek könnyen toborozhatnak programozókat is, ők pedig olyan algoritmust készítenek, amelyben nincsenek kiskapuk…

A titkos üzenetváltás kevésbé egyértelmű, de a történelemben és a terroristák által is széles körben alkalmazott változata a *szteganográfia*, vagyis az üzenet elrejtésének tudománya. E megoldás során látszólag érdektelen hordozókba építenek be a külső személyek számára láthatatlan vagy értelmezhetetlen titkosítani kívánt információkat. Néhány példa: üzenetek „zajos" kép- vagy hangfájl legkisebb bitjeibe rejtése; futtatható programokban való elrej-

tés; kódolatlan üzenetek, amelyekből adott rendszer alapján olvasható ki az információ.[26]

Az interneten keresztüli kommunikáció nemcsak az adott szervezet tagjai között, hanem terrorszervezetek egymás közötti viszonyában is elképzelhető, ez szintén jelentős információforrás lehet.

A tervezés terén is támaszkodhatnak az internetre, hiszen információkat, programokat, adatokat szerezhetnek, sok esetben teljesen legálisan, segítségükkel megszervezhetik támadásaikat.

Az információk megszerzése kapcsán hangsúlyozni kell, hogy az interneten található elképesztő adatmennyiség miatt megfelelő keresőszavak segítségével, vagy megfelelő weboldalak látogatásával könnyedén hozzá lehet jutni szinte bármilyen, az internet előtt csak jelentősebb nehézségek árán megszerezhető információhoz. Ráadásul nem pusztán leírásokat találhatunk, hanem akár szemléltető videókat, interaktív térképeket, műholdfelvételeket is.

Toborzás, propaganda terjesztése, források szerzése – a kommunikáció és szervezés mellett az új tagok toborzása, nézetek terjesztése terén szintén hatalmas lehetőségeket nyújt az internet mind a hagyományos, mind a kiberterrorista szervezeteknek. Tekintettel arra, hogy a terroristák nem férnek hozzá a televíziók és rádiók műsorszórásához – hacsak támadásaik révén közvetetten nem –, így nézeteik terjesztésének egyetlen útja az internet. A különböző terrorista szervezetek weboldalaikon, illetve a követőik által létesített további oldalakon (például *Hizbullah: The Party of God*[27]) nyíltan toborozhatnak tagokat, hirdethetik nézeteiket. A weboldalakon a lehetséges új tagok toborzásának számos módszerét is bevethetik. A céljaikat bemutató írások mellett eddigi akcióikról, vezetőikről, ellenségükről készített képeket, videofelvételeket helyezhetnek el, adományokat gyűjthetnek.[28]

Az internet hivatkozási lehetőségeit kihasználva más oldalakon elhelyezhetnek olyan hivatkozásokat, figyelemfelkeltő animációkat, amelyek megragadják az emberek figyelmét, és elvezetik őket a kívánt oldalakra.

A kiberterroristák fegyvertára

E fejezetet akár egyetlen szóban is össze lehetne foglalni, hiszen a kiberterroristák alapvető fegyvere – és célpontja is – maga a számítógép. Persze

26 http://hu.wikipedia.org/wiki/Szteganográfia
27 http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah
28 Kovács László: i. m.

utóbbi rengeteg elkövetési módszert és további támadási eszközöket foglal magában.

Mielőtt rátérnénk az egyes eszközökre, általánosságban elmondható, hogy egy új technológiai eszköz kifejlesztése után számolni kell az új eszköz bűnözők általi felhasználásával is – ez a kiberterrorizmus terén sincs másként. Másképp fogalmazva, a kiberterrorizmus – akárcsak a számítógépes bűnözés – fejlődése szorosan összefügg a számítástechnika fejlődésével. A számítástechnika terén kevésbé jártas egyének feltehetik a kérdést: *egy olyan robusztus hálózat, mint az internet, illetve egyéb hálózatok, hogyan támadható hatékonyan?*

Az elkövetők elég széles eszköztárból válogathatnak!

Az eszközök alapvetően két csoportba sorolhatók: az elsőt a rosszindulatú szoftverek mint eszközök, a másodikat a részben ezeket felhasználó támadási módszerek alkotják.[29]

Hangsúlyozni kell, hogy a kiberterroristák által felhasználható eszközök legnagyobb veszélyei, hogy az elkövetéskor nem kell a támadás helyszínén tartózkodniuk; akár több ezer kilométer távolságból is csapást mérhetnek, mégpedig nehezen felderíthető módon. Így könnyen előfordulhat, hogy az esetleges üzemzavart a támadás után nem is kapcsolják külső támadáshoz, hanem belső meghibásodásnak tulajdonítják.[30]

Eszközök: a rosszindulatú szoftverek (malware)

A *malware*-ek az olyan rosszindulatú számítógépes programok összefoglaló elnevezése, amelyek a felhasználók engedélye nélkül hatolnak be számítógépekbe, és azokban nem kívánt változásokat idéznek elő, egyebek között: erőforrásokat kötnek le; adatokat módosítanak, törölnek; egyéb jellegű kárt okoznak, vagy ennek veszélyét hordozzák magukban. A malware-ek nem összekeverendők a hibás programokkal, amelyek céljukat tekintve hasznos programok, de valamilyen programozási hiba maradt a szoftverkódban.[31]

A malware-ek két csoportját különböztethetjük meg, előbbibe a programalapú (különösen: vírusok, programférgek, trójai programok, keyloggerek stb.), utóbbiba a szöveges malware-ek (spam, hoax, phishing, pharming stb.) tartoznak. Ezek közül csak a legjelentősebbeket veszem számba.

29 Uo.
30 http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/terrorism.html
31 http://en.wikipedia.org/wiki/Malware

Programalapú malware-ek

A számítógépes *vírusok* olyan kisméretű, rosszindulatú programok, amelyeket arra terveztek, hogy saját másolataikat más végrehajtható programokban vagy dokumentumokban elhelyezve megfertőzzenek számítógépeket.[32] A számítógépes vírusok működése megfelel a biológiai értelemben vett vírusok viselkedésének, így általában használhatatlanná teszik vagy törlik a megfertőzött állományokat, de előfordul, hogy „csak" túlterhelik a rendszert, és egyéb kárt nem okoznak. Veszélyességük különösen abban áll, hogy a számítógép bármely részét megfertőzhetik (alkalmazások, dokumentumok, rendszervírus stb.), mégpedig minden előjel nélkül, és a felhasználó már csak a vírus tevékenykedésének következményével szembesül.

A programférgek (worm) olyan rosszindulatú programok, amelyek programkódjaikat nem más programok belsejébe építik be (vagyis nincs szükségük gazdaprogramra), hanem azt önálló fájlban tartalmazzák, és ezt másolva sokszorozódnak. A sokszorosítás közben módosítják azokat a fájlokat is, amelyekkel a programindítás lehetséges. A programférgek észlelése és működésük megakadályozása nehezebb feladat, mint a vírusoké. A vírusok esetén a vírusirtó programok az egyes programanomáliák alapján könnyen felderítik a vírusokat, a programférgek azonban nem módosítják a programfájlok kódjait, így az észlelésük is nehézkesebb.[33] A wormok saját másolataikat a megtámadott számítógép merevlemezén készítik el, és hálózati kapcsolódási pont esetén a hálózaton keresztül továbbítják is más gépeknek.

A trójai falovak olyan programok, amelyek működése a felhasználó megtévesztésén alapul. E programok látszólag hasznosnak tűnnek, de a valóságban nem kívánt műveleteket hajtanak végre, általában terhelik a rendszert, adatvesztést okoznak. Lényeges tulajdonságuk a vírusokhoz képest, hogy általában nem többszörözik önmagukat, terjedésük egyéni támadások következménye. Előfordulhat, hogy nem tartalmaznak rosszindulatú programkódot, de ettől függetlenül többségük úgynevezett hátsó ajtó telepítését is elvégzi, amely a fertőzés után hozzáférést enged a célszámítógéphez.[34]

A hátsóajtó- (backdoor) programok szoftverekbe épített, a felhasználók számára láthatatlan kiegészítések, amelyek bizonyos kiválasztott személyek részére (illetéktelen) hozzáférést engednek a programokhoz, számítógéphez, vagy az azokon tárolt adatokhoz. A backdoor terjesztője vagy használója a

32 http://hu.wikipedia.org/wiki/Számítógépes_vírus
33 http://www.antivirus.hu/virved/displayer.php?site=antivirus&page=40.10
34 http://hu.wikipedia.org/wiki/Trójai_faló_(számítástechnika)

hátsó ajtó segítségével az interneten keresztül a megtámadott gépen tárolt adatokat megtekintheti, módosíthatja, törölheti, vagy megfigyelheti a felhasználót.[35]

A pottyantók (dropper) olyan programok, amelyek önállóan szaporodó vírusokat, trójai programokat, programférgeket vagy egyéb rosszindulatú programokat juttatnak be a megtámadott rendszerekbe oly módon, hogy miután beférkőztek a számítógépekbe, legyártanak meghatározott számú, az operációs rendszer által futtatható vírust vagy egyéb ártó programot, majd futtatják őket.[36]

Szöveges malware-ek

Az előbbi programokkal ellentétben léteznek szöveges, nem programalapú malware-ek is, amelyek szintén veszélyt jelenthetnek. A leggyakoribbak: kéretlen üzenetek (spam, hoax), adathalászás (phishing, pharming).

Kéretlen üzenetek (spam) – a spamek a fogadó által nem kért, elektronikusan (jobbára: e-mailben) tömegesen küldött hirdetések, felhívások, igen változatos témákban. A nagy számban szétküldött kéretlen levelek hátrányos következményei egyrészt a lefoglalt tárhelyben, másrészt a lekötött sávszélességben nyilvánulnak meg.

Hoax – a kéretlen levelek egyik típusa, általában szintén e-mailben terjesztett álhír-lánclevelek különféle változata. A megtévesztés gyakran kiegészül honlapokkal, illetve esetenként a hagyományos média is hajlamos átvenni. Fontos hangsúlyozni, hogy a hoax célja a célközönség megtréfálása, nagyon ritkán irányul illegális célokra.[37]

Célja ellenére hatásai a spaméivel azonosak, mivel a hoax annál hatásosabb, minél több ember tudomást szerez róla, így sok szétküldés esetén szintén sávszélességet és tárhelyet köt le. Nem is beszélve arról, hogy mellékletként egyéb rosszindulatú programot lehet csatolni hozzá.

Adathalászat (phishing) – az emberek hiszékenységére építő csalási módszer, amelynek során egy csaló egy ismert cég (általában pénzintézet) nevében e-mailt vagy azonnali üzenetet küld a címzettnek, és például üzemzavarra vagy adategyeztetésre hivatkozva megpróbálja – válaszlevél keretében vagy a cég weboldalához nagyon hasonlító weboldal segítségével – kicsalni

35 http://www.virushirado.hu/lexikon.php?l=b
36 http://www.antivirus.hu/virved/index.php?CN=40.4&CIE=0
37 http://hu.wikipedia.org/wiki/Hoax

a felhasználó személyi adatait (azonosítók, jelszavak, bankkártyaszámok stb.). A másik jellemző levéltípus esetén hatalmas összegű internetes lottónyeremény átutalásához kérik a fogadó adatait. Fontos kiemelni, hogy a levelek minden esetben hivatalos megkeresés látszatát keltik.

Pharming – a phishing fejlettebb változataként, ugyancsak csalárd eljárásról van szó. A kétfajta csalási módszer között két jelentős különbség van. Egyrészt az utóbbi esetben kizárólag az áloldalon lehet megadni a kért adatokat, másrészt egy rosszindulatú szoftver segítségével a csaló az eredeti lapról a saját hamisított weboldalára téríti a felhasználót; vagyis a felhasználó hiába írja be helyesen a cég weboldalcímét, a böngésző az áloldalra vezeti.[38] A megszerzett adatokkal pedig már könnyedén visszaélhetnek a csalók.

Eszközök: greyware-ek

A *greyware* kifejezés olyan programokat takar, amelyek nem okoznak olyan károkat, mint a malware-ek, de jelenlétük bosszantó, zavaró. E programok főként a hálózatba kapcsolt számítógépek teljesítményét befolyásolják, illetve lehetőséget adnak károkozó cselekmények végrehajtására. Ahogy nevük is jelzi, egyfajta szürke zónát jelentenek a normális programok és a malware-ek között. A greyware-ek közé sorolható programok különösen a kémprogramok *(spyware)*, reklámprogramok *(adware)*, a *trackware*.

Kém- és reklámprogramok

A *kémprogramok* olyan főként az interneten terjedő rosszindulatú programok, amelyek célja, hogy megszerezzék a megfertőzött számítógép felhasználójának személyes adatait (egyebek között felhasználói nevek, belépési jelszavak, bankkártyaszám stb.), és elküldjék a kémprogram felhasználójának, és később akár jogszerűtlen cselekményekhez is felhasználhatják. A kémprogramok feltelepülése észrevétlenül történik, a felhasználó figyelmetlenségének és a számítógép böngészőprogramja biztonsági hiányosságainak kiaknázásával. Kizárólag többféle védelmi program kombinációjával lehet ellenük hatékonyan védekezni (víruskereső programok, intelligens tűzfalprogramok, illetve spyware-ek felismerésére készített programok használata).[39] A *reklámprogramok* olyan szintén az interneten terjedő programok, amelyek célja, hogy egy termé-

38 http://www.cert.hu/index.php?option=com_content&task=view&id=378&Itemid=155
39 http://hu.wikipedia.org/wiki/Spyware

ket és annak készítőjét vagy egy céget reklámozzanak. Jóllehet több reklámprogram egyben kémprogram is, mégis jelentős különbség van a kettő között. Amíg a kémprogramok mindig rejtetten működnek és szerzik meg a felhasználó adatait, addig a reklámprogramok, érthető módon, jól láthatóan, általában a böngészőprogramban jelenítenek meg hirdetéseket, amelyek sávszélességet vonnak el a felhasználótól, adott esetben közvetetten okozva kárt.[40]

Kiberterrorista módszertan

Számos olyan eljárási módszer létezik, amelyekkel – a rosszindulatú programok felhasználásával, illetve kiegészítésükkel – károkat lehet okozni egy hálózatban. Tekintettel arra, hogy a hálózatok általában kapcsolatban állnak más hálózatokkal, a károk tovább növelhetők, hiszen egy hálózat kiesése más hálózatokban is károkat okozhat, de legalábbis hatással lehet annak működésére.
A legjelentősebb támadási módszerek:

– Denial of service.
– Distributed denial of service.
– Flooding.
– SMTP backdoor command attack.
– IP address Spoofing attack.
– IP fragmentation attack.
– TCP Session High jacking.
– Information leakage attack.
– JavaScript, applet attack.
– Cross site scripting (XSS).

A felsorolásban szereplő módszerek közül csupán az első kettőre térek ki, egyrészt gyakoriságuk miatt, másrészt terjedelmi okokból.

A *szolgáltatásmegtagadással járó támadás (Denial of Service; DoS)* lényege, hogy a támadás következében egy adott szolgáltatás – az azt biztosító hardver vagy szoftver megbénítása vagy működésének zavarása révén – részben vagy egészben elérhetetlenné válik. A támadók az elérni kívánt céljukat a korlátolt erőforrások kimerítésével vagy a kommunikációban és a kiszolgálásban részt vevő egységek működésének zavarásával érik el.

Az említett állapot két fő módszerrel érhető el. Az elsőnél egy szervert olyan mennyiségű kéréssel bombáznak, hogy a rendszer egyszerűen nem ké-

40 http://hu.wikipedia.org/wiki/Adware

pes ellátni feladatait, és legrosszabb esetben összeomlik. A másodikban a programok és az operációs rendszerek gyenge pontjainak *(bug)* vagy a protokollok szabálytalan alkalmazását használják fel a DoS-támadáskor. A DoS-támadások tehát mindig közvetlen, frontális támadások. A DoS-támadások – a felhasznált programok fejlettsége miatt – felderítése elég nehézkes, mivel a támadás során az érkező adatok útja bizonytalanná válik.[41]

A DoS-támadásoknak, az alkalmazott támadási módszer szerint, több alfajtájuk is létezik, de ezek közül csupán az egyik legjelentősebbre térek ki, az *elosztott szolgáltatásmegtagadással járó támadásra (Distributed Denial of Service; DDoS).*

A szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése történhet megosztva is, több forrásból (DDoS). Ellentétben az egyszerű DoS-támadással, a DDoS esetén a támadó már több irányból is támadja a célpontot. A DDoS-támadások összetettek, a támadón és támadotton kívüli számítógépek kapacitásait, illetve a külső számítógépek nagy mennyiségét használják a támadáshoz.

Külső gép két módon kapcsolható be a támadásba:

– egy automatizált szoftver felkutatja a hálózatra kapcsolódó, sebezhető számítógépeket, amelyekre feltelepít egy rejtett támadóprogramot, ettől a megtámadott gép úgynevezett zombigéppé alakul;
– a másik lehetőség keretében az említett rejtett programot nem egy külön szoftver, hanem vírusok vagy trójai programok segítségével juttatják be a leendő zombigépbe.

A DDoS-támadás folyamata a következőképpen zajlik: a támadáskor a zombigépek távolról vezérelhetők egy mestergépről. Ha elégséges számú gépet sikerült megfertőzni a támadóprogrammal, a mestergép jelet ad a zombigépnek vagy gépeknek a támadás megkezdésére.

A támadás idején mindegyik zombigép kis mennyiségű adatot kér vagy küld a célpontnak, de mivel egyszerre teszik ezt, több száz vagy akár ezer támadó esetén a sok kisméretű adatcsomag hatalmas adatáramlást gerjeszt, ami megbénítja a célpontot.[42]

41 http://www.biztonsagosinternet.hu/node/42
42 http://hu.wikipedia.org/wiki/DDoS

A kiberterrorizmus jelene és jövője

Jelen pillanatban – még – elmondhatjuk, hogy a kiberterrorizmus jelensége túlbecsült. Mint már a cikk elején is jeleztem, eddig egyetlen nagyobb támadást sem észleltek. Az egyetlen kiberterrorista támadásnak nevezhető akciót a Tamil Eelam Felszabadító Tigrisei (Liberation Tigers of Tamil Eelam; LTTE) követte el még 1997-ben.

Akciójuk során kéretlen levelekkel bombázták a világ különböző országaiban működő Srí Lanka-i követségek elektronikus postaládáit. A támadások nem okoztak nagyobb károkat, inkább csak rámutattak az információs rendszerek sebezhetőségére. A helyi vagy nemzetközi konfliktusok közben amúgy is gyakran tapasztalható, hogy az adott felek szimpatizánsai az interneten is hadat üzennek egymásnak, és különféle önmagában jelentős károkat nem okozó támadásokat intéznek egymás ellen.

Ha mindezeket tényként fogadjuk el, adódik a kérdés: *miért került ennyire reflektorfénybe a jelenség?*

A lehetséges okok közül az első helyre a *tömegmédia* helyezhető. A médiában sokféle csúsztatással, a fogalmak egybemosásával találkozhatunk, így nem is meglepő, hogy a kiberterrorizmust gyakran keverik a hackeléssel, ily módon jelentősként feltüntetve a vizsgált bűnözési formát.

A képzeletbeli dobogó második fokára a jelenség *újdonsága* kerül. Mint láthattuk, a kiberterrorizmus lényegében technológiai terrorizmusként is felfogható, technológiai volta miatt azonban sokak számára nehezebben érthető. A kellő fokú ismeretek hiánya közismerten félelemkeltő…

Harmadik okként a *politikusok egyéni érdekei* is felhozható, hiszen érdekükben állhat egy ellenség – jelen esetben: a kiberterrorista – létrehozása, így az ellenük való fellepés hangoztatásával könnyen népszerűvé válhatnak.

Negyedik tényező a jelenség kapcsán észlelhető *bizonytalanság.*[43]

Jó néhány kérdés vár még eldöntésre, illetve több bizonytalan pontot kell tisztázni. Néhány fontosabb kérdést kiragadva:

– Hogyan értelmezhető a virtuális erőszak, mit tekinthetünk az erőszak virtuális megfelelőjének?
– A határok nélküli interneten hogyan értelmezhető a nemzeti jelleg (például nemzeti jelleget hangoztató terrorszervezetek esetén)?
– Vajon teljes bizonyossággal eldönthető-e, mely állam hatósága járjon el adott ügyben, és ha igen, melyik jogrendszer szabályai alapján?

43 Gabriel Weimann (2004): i. m.

– A való világban észlelhető jelenségek, veszélyek és dolgok (például tulajdon) könnyen felfoghatók, de vajon létezik virtuális megfelelőjük is? Ha igen, hogyan illeszthetők be a kiberterrorizmus jelenségvilágába?[44]

Leszögezhetjük, hogy a jövő terroristái feltehetően jóval több lehetőséget fognak látni a számítástechnikában, mint elődeik. A számítástechnika fejlődésével és még gyorsabb elterjedésével nagyobb veszélyt hordoz e jelenség.

Nem zárhatjuk ki annak a lehetőségét sem, hogy a jövőben a kiberterrorizmus – a világ számítástechnikai kiszolgáltatottsága miatt – veszélyesebb lesz, mint a jelenlegi „hagyományos" terrorizmus.

Mindazonáltal az egyik legnagyobb veszélyt a hagyományos és a kiberterrorizmus eszköztárának egyidejű bevetése okozhatja, hiszen ebben az esetben maximalizálható a hagyományos támadások hatása.[45]

Konklúzió

Az eddig leírtakat végigolvasva egyértelmű, hogy a kiberterrorizmus, tűnjön bármilyen veszélyesnek is, jelenleg egyfelől lehetőség a terroristák kezében, másfelől potenciális veszélyforrás a társadalmak számára. Súlyos veszélyforrás, hiszen a társadalmakban létező infrastruktúrák – amelyek pontos működése létfontosságú is lehet – jelentős része nagymértékben támadható. Láthattuk, hogy a kritikus infrastruktúrákban okozott kisebb zavar is súlyos károkat okozhat. A veszélyt csak tovább növeli az információs társadalom egyes elemeinek kiépítése, ami még tovább fokozza a társadalmak számítástechnikai függőségét, így sebezhetőségét. Továbbá nem sok magyarázatot igényel, hogy a társadalmakat leginkább a hagyományos és kiberterrorizmus közös, egymást kiegészítő és erősítő támadásai fenyegetik.

Mindamellett, paradox módon, minél összetettebbé válnak az egyes rendszerek, annál nehezebb jelentős károkat előidézni, mivel az eredményes támadás nagyobb szaktudást igényel.

Bár a társadalmak számára súlyos veszélyt jelent e jelenség, a technika és így a fegyverként használható eszközök fejlődése mellett számolni kell a biztonsági megoldások fejlődésével és terjedésével is.

Láthattuk, hogy a kritikus infrastruktúrák sem sebezhetetlenek, de többségében erősebb védelmet élveznek, mint az egyéb, jobbára magántulajdonban

44 Sarah Gordon: i. m. 10–11. o.
45 Gabriel Weimann (2004): i. m.

lévő infrastruktúrák, így azok támadása is nagyobb próbatétel a kiberterroristák számára. Vagyis olyan személyek számára, akiket néha nem egyszerű megkülönböztetni a hackerektől, különösen azért, mivel a kiberterroristák is alkalmazhatnak olyan eszközöket és módszereket, mint a hackerek, vagy egyszerűen toborozhatnak hackereket.

Mindamellett az is látható volt, hogy motivációik (ideológiai, vallási, vagy politikai) és céljaik (nem a haszonszerzés) szerint mégis kellő biztonsággal elkülöníthetjük a kiberterroristákat az egyéb számítógépes bűnözőktől. E jelenséget, mint kitértem rá, többen túlbecsülik, a kelleténél jóval súlyosabb jelenségként feltüntetve.

Való igaz, hogy a dolog akár már a közeljövőben is sokkal jelentősebbé válhat, mint napjainkban, de úgy tűnik, hogy napjaink terroristái egyelőre megmaradnak a jól bevált módszerek mellett.

Érdekes jelenségként könyvelhetjük el, hogy az Amerikai Egyesült Államok által meghirdetett terrorizmus elleni küzdelem *(war on terror)* hatására beszűkültek a terroristák valós világbeli lehetőségei, így figyelmük várhatóan inkább a virtuális világ felé fordul, ahol kellő szakismerettel jelentős károkat okozhatnak a nem kellően felkészült társadalmaknak.[46]

46 Dorothy E. Denning: i. m.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp49-59

IBOLYA TIBOR

A torrentrazziák büntetőjogi megítélése

2010. június 16-án a magyar rendőrség átlépte a büntetőjogi Rubicont a szerzői jogok védelme érdekében indított harcában: nem az smsweb-alapú, audiovizuális tartalmakat fizetés ellenében letölthetővé tevő kalózoldalak vagy a másolt DVD-ket a piacokon árusítók ellen lépett fel, hanem hazai torrentsiteok szervereit foglalta le és vitte el egy jól szervezett akció keretében. Az eljárást a ProArt – Szövetség a Szerzői Jogokért hazai jogvédő szervezet kezdeményezte, a feljelentés után pedig *„a XIII. kerületi kapitányság emberei hónapokig dolgoztak a szerverek felderítésén”*. Sikerrel jártak, mert az akció következtében a legnagyobb magyar torrentsite-ok mintegy *kétheti időtartamra* elérhetetlenné is váltak, majd ott folytatták, ahol abbahagyták…[1]

Az akció nagy visszhangot váltott ki a hazai médiában és a netes társadalomban egyaránt, hiszen hasonló esetre még nemigen volt példa, a Nemzeti Nyomozó Iroda ilyen jellegű akciói többnyire fizetős kalózoldalak ellen irányultak. A site-okat feljelentő ProArt sietett is leszögezni, hogy *„fontos mérföldkőnek tartja a sikert, egyúttal mindenkit meg is nyugtat: bár elítélik a fájlcserélők használatát, de továbbra sem üldözik az otthoni internetezőket”*[2].

Az esetről a neten elérhető cikkek és az azokhoz fűzött kommentárok, amellett, hogy a ProArt előbbi kijelentését eleve megkérdőjelezték, a site-ok gyors újraindulásának ismeretében sokszor gúnyosan tették fel a kérdést: mi értelme volt ennek az egésznek?

Annak a ténynek az ismeretében, hogy állításuk ellenére a szerzőijog-védő szervezetek valóban jelentenek fel néha egyéni torrentezőket is, illetve hogy a hasonló eljárások mennyire elhúzódnak, milyen sokba kerülnek és végül milyen arányban kerülnek bírósági ügyszakba, a kérdést laikus részről jogosnak kell tekintenünk. Egy büntetőeljárás lefolytatása megkérdőjelezésének azonban gazdasági alapon nem lehet értelme, mert annak sikere esetén társadalmilag hasznos hatásai nem feltétlenül fejezhetők ki gazdasági mód-

1 Az akcióra 2010. június 16-án került sor, a legnagyobb magyar torrentsite, a több mint százezres (!) tagságú NCore pedig július negyedikén már ismét üzemelt.

2 Vámosi Gergő: Sebészi pontosságú akció volt a torrentrazzia. [origo] techbázis, 2010. június 23. http://www.origo.hu/techbazis/internet/20100623-sebeszeti-pontossagu-akcio-volt-a-torrentszerverek-lefoglalasa.html

szerekkel. Ha azonban egy magát jogvédőnek beállító, valójában nyereségorientált cégek érdekvédelmi szervezeteként működő egyesület a magyar bűnüldöző hatóságok igénybevételével, őket felhasználva, rendkívül költséges, időben elhúzódó, rendszeresen eredménytelennek vagy igen csekély társadalmi eredménnyel kecsegtetőnek bizonyuló, ráadásul büntetőjogi szempontból ingatag alapon álló büntető eljárásokat indít, akkor ezeket a kérdéseket már fel kell tennünk, és a kérdéseket meg kell fogalmaznunk.

Mielőtt azonban ezt megtennénk, tisztázzunk néhány alapfogalmat az internetes fájlcsere köréből, mert ezek ismerete nélkül azokat a jogi, tényállásbeli és bizonyítási problémákat sem tudjuk megérteni, amelyeket a hasonló ügyek miatt induló büntetőeljárások generálnak.

Technikai háttér és alapfogalmak

A *torrent (torrentezés)* jelen pillanatban a többfajta fájlcserélő közül a legelterjedtebb és legnépszerűbb módszer a világon, amelyet a széles sávú internethozzáférés elterjedése következtében Magyarországon is rendkívül sokan használnak. Az úgynevezett BitTorrent technológia lényege, hogy a fájlokat a felhasználók szeletekben (torrent), darabokban töltik le egymástól oly módon, hogy a szeletek egymást „keresik meg" az interneten; minden csomópont megkeresi a hiányzó részhez a lehető leggyorsabb kapcsolatot, miközben ő is letöltésre kínálja fel a már letöltött fájldarabokat. A BitTorrent esetében minél keresettebb egy fájl, annál többen vesznek részt az elosztásában, ezáltal az elosztása gyorsabban megtörténik, mintha mindenki egy központi helyről (szerverről) töltötte volna le [ellentétben a népszerű előző generációs fájlcserélő módszerrel a Direct Connect (DC)-Hubbal, ahol minél keresettebb volt egy fájl, annál lassúbb volt a letöltés, hiszen a letöltők ott egy felhasználóhoz kapcsolódtak, lefoglalva ezzel a sávszélességet]. A módszer ideális bármilyen (tehát nem csak jogvédett) nagyméretű fájl megosztására.

Ahhoz, hogy a felhasználó torrentezni tudjon, szüksége van egy úgynevezett *kliensprogramra*, amely nem más, mint egy szoftver, amely a kezelői felületet is megteremti. Ezek némelyikét, mint például az egyik legnépszerűbb *µTorrent* nevű programot, még telepíteni sem szükséges a felhasználó számítógépére. A kliensprogramba kell aztán betölteni azt a .torrent kiterjesztésű fájlt, amellyel az egész művelet megkezdhető. A .torrent kiterjesztésű fájlokat legkönnyebben egy úgynevezett *tracker*ről (felhasználói közösség) lehet letölteni, ezek között vannak nyíltak, ahová bárki beléphet (például Pirate-

Bay), és zártak, ahová csak meghívóval, regisztrációval stb. lehet bekerülni, a regisztráció és maga a tracker használata azonban ingyenes. *A trackeren (a webszerveren) egyébként nincs meg maga a fájl (a keresett film, zenemű, program stb.), tehát nem vesz részt a tényleges adatcserében*, csak közvetít a felhasználók *(peerek)* között. Azokat a felhasználókat, akiknek a teljes fájl a rendelkezésére áll, és a többiek tölthetnek tőlük, *seeder*nek, azokat, akik ezektől és egymástól is töltenek, *leecher*nek nevezzük, az egymáshoz kapcsolódó peerek összességét pedig *swarm*nak (boly). A kliensprogramokban akár korlátozni is lehet a leech-/seed-sebességet, amely egyébként teljes mértékben a felhasználók által használt sávszélességtől függ.

Ez tehát a technológiai háttere annak a világjelenségnek, amely ellen egyesek szerint a büntetőjog mint ultima ratio eszközeivel kell fellépni, és a magyar nyomozó hatóság jelentős erőket mozgósítva ezt meg is teszi.

A bűncselekmény

A torrent technológia használatakor (ha az szerzői jogi védelem alatt álló műveket érint) a büntetőeljárás megindításának alapjául szolgáló gyanú nem lehet más, csak a Btk. 329/A (1) bekezdésébe ütköző szerzői jogok megsértésének vétsége.

Btk. 329/A § (1) Aki másnak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát haszonszerzés végett, vagy vagyoni hátrányt okozva megsérti, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.

A törvényi tényállás úgynevezett keretdiszpozíció, az annak keretét kitöltő *kizárólagos* jogszabály a szerzői jogról szóló 1999. évi LXXVI. törvény (Szjt). A szerzői jogról szóló törvény kizárólagosságát azért kell kihangsúlyoznunk, mert például a ProArt honlapján a működésük jogi hátteréneként feltüntettek több, a Szerzői Jogi Szakértői Testület által a ProArt kérésére elkészített, nem vitatottan magas színvonalú szakértői vélemény is, az ezekben foglaltak azonban a bűncselekmény megállapíthatósága szempontjából természetesen nem bírnak jogi relevanciával.[3]

3 A jogellenes forrásból történő másolásról, illetve a fájlcseréről szóló SzJSzT 17/2006. és SzJSzT 7/2008. számú szakértői vélemények elemzéséről lásd Ott István: A szerzői jog büntetőjogi védelmének egyes kérdései. Rendészeti Szemle, 2009/12.

A torrent technológia használatakor a letöltés az Szjt. 18–19. §-a szerinti *többszörözésnek*, a feltöltés pedig az Szjt. 26–27. §-a szerinti *nyilvánossághoz történő közvetítésnek* számít.[4]

Az audiovizuális tartalmak letöltése azonban nem lehet bűncselekmény, mert a jogosult engedélye, illetve a díjfizetés nélkül megengedett magáncélú többszörözésre vonatkozó Szjt. 35. §-a értelmében természetes személy magáncélra a műről másolatot készíthet, ha az jövedelemszerzés vagy jövedelemfokozás célját közvetve sem szolgálja. Ebben a körben *„az úgynevezett magáncélú másoláshoz kapcsolódó vagyoni jogok érvényesülését az biztosítja, hogy a törvény értelmében az üres kép- és hanghordozók forgalomba hozóinak a szerzői jogok közös kezelését végző szervezet által megállapított díjat kell fizetni, amelyet a szervezet a törvényben meghatározott szabályok szerint osztja fel a jogosultaknak.* Mindebből következően a szerzői jogvédelem alatt álló elkövetési tárgyak – a szoftverek kivételével – letöltése, másolása legális, a szabad felhasználás körébe illeszthető."[5]

A Szerzői Jogi Szakértői Testület véleményével ellentétben ebben az esetben a hatályos Szjt. alapján annak sincs jelentősége, hogy a letöltés (többszörözés) nem jogszerűen létrejövő műpéldányról történt. Nem véletlen, hogy a kormány 2008 szeptemberében, engedve a jogvédő lobbi befolyásának, a T/6374. törvényjavaslatában kísérletet tett a szerzői jogról szóló törvény ilyen értelmű módosítására. Ez expressis verbis kimondta volna, hogy *„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"*. Mivel azonban a módosító javaslatot az Országgyűlés nem fogadta el, a hatályos törvényben ez továbbra sem szerepel, a letöltés tehát továbbra sem illegális.

Más a helyzet a feltöltéssel. A torrent technológia használatakor a szerzői-jog-védők által hangoztatott állítás („a letöltés egyben feltöltéssel is jár") elméletileg igaz, sőt a technológia erre épül. A gyakorlatban azonban részben azért, mert a felhasználó magában a kliensben vagy a tűzfalon le is tilthatja a seedelést, részben pedig azért, mert egy sokak által seedelt fájl letöltésénél hiába kínálja fel a már letöltött fájldarabot a program, mivel ha nem tartozik a leggyorsabbak közé, nem jön létre a kapcsolat és így a feltöltés sem, már korántsem biztos, hogy a letöltés feltöltéssel is jár. Egyáltalán nincs feltöltés

4 A közérthetőség kedvéért én a letöltés és feltöltés köznapi kifejezéseit használom.

5 Belovics Ervin – Molnár Gábor – Sinku Pál: Büntetőjog. Különös Rész. Nyolcadik, átdolgozott kiadás. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2009, 768. o.

például abban az esetben sem, ha a letöltő olyan bolyhoz csatlakozik, ahol rajta kívül nincs más letöltő, vagyis mindenki seedel.

A hazai szolgáltatók által nyújtott széles sávú internetkapcsolat ama tulajdonsága, hogy a letöltési sávszélesség sokszorosan meghaladja a feltöltési sávszélességet, az oka annak, hogy a zárt trackerek általában meghatároznak egy arányt (például 0,2), amely alatt a felhasználót IP-címének blokkolásával kitiltják a közösségből. Ilyen arányt azonban a nyílt, bárki által használható trackerek nem követelnek meg, ezeknél könnyen megtehető, hogy a fájl letöltése után a felhasználó azonnal kilép anélkül, hogy akár egy kilobájtot is feltöltött volna. Zárt trackerek esetén a feltöltés (seedelés) egyértelműen elvárt ugyan a felhasználótól, az 1/1-es arány (vagyis a letöltött fájl teljes egészében történő „visszatöltése") azonban nem követelmény, fájlszeletek feltöltése pedig nem alkotja a szerzői mű egészét. A szerzői jogi védelem az Szjt. 16. § (1) bekezdésében foglaltak alapján a szerzői mű valamely *azonosítható* részét is megilleti ugyan, kérdés azonban, hogy mit ért a törvényalkotó azonosíthatóságon. Ha az „azonosíthatóság" a felhasználó általi „érzékelhetőséget" jelenti (ahogy azt például a SzJSzT 7/2008. számú szakértői véleménye is tartalmazza), akkor a fájlszeletek egyes felhasználók általi feltöltése ennek nem felel meg, hiszen azok nem érzékelhetők, mert önmagukban nem játszhatók le, nem nézhetők és hallgathatók meg. Az azonosíthatóság (érzékelhetőség) a folyamat végén, az akár több 100-1000 forrásból (egyéni felhasználótól) származó adatmennyiség összeillesztése után következik csak be, *a letöltő* számítógépén. A büntetőjogi felelősség azonban individuális, az egyéni felhasználót a Btk. 329/A § (1) bekezdésében foglalt bűncselekmény elkövetésének megalapozott gyanúja esetén is *csak a saját tevékenysége miatt lehet felelősségre vonni.*

Esetünkben ez azt jelenti, hogy a torrent trackert (illetve azt a szervert, amelyen a tracker fut) üzemeltető büntetőjogi felelősségét bűnsegédi bűnrészesként csak akkor lehet megállapítani, ha a nyomozó hatóság bizonyítani tudja, hogy *szándékosan nyújtott segítséget egy konkrét szerzőijog-védelem alatt álló mű feltöltéséhez.* Figyelemmel arra a technikai ismertetésben már leírt tényre, hogy a trackeren (webszerveren) nincs meg maga a fájl, tehát nem vesz részt a tényleges adatcserében, csak közvetít a felhasználók között, a büntetőjogi felelősség megállapítása, álláspontom szerint, kizárt.

Egyébként a torrent tracker jogi besorolása sem egyértelmű, meghatározásának alapja – jogi analógiával – *az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény* lehet, amelynek 2. § ld) pontja szerint olyan

közvetítői szolgáltatónak minősülhet, amely információk megtalálását elősegítő segédeszközöket nyújt az azt igénybe vevők számára (keresőszolgáltatás).

Ugyane törvény 7. § (3) bekezdése alapján *„a közvetítő szolgáltató nem köteles ellenőrizni az általa csak továbbított, tárolt, hozzáférhetővé tett információt, továbbá nem köteles olyan körülményeket vagy tényeket keresni, amelyek jogellenes tevékenység folytatására utalnak”*.

Mindazonáltal a törvény 13. § (1) bekezdése alapján *„az a jogosult, akinek a szerzői jogi törvény által védett szerzői művén, előadásán, hangfelvételén, műsorán, audiovizuális művén, adatbázisán fennálló jogát, továbbá a védjegyek és a földrajzi árujelzők oltalmáról szóló törvényben meghatározott, a védjegyoltalomból eredő kizárólagos jogát a szolgáltató által hozzáférhetővé tett információ* – ide nem értve a hozzáférhetővé tett információ szabványosított címét – *sérti, teljes bizonyító erejű magánokiratba vagy közokiratba foglalt értesítésével felhívhatja a szolgáltatót az információ eltávolítására”*.

Az értesítés átvételétől számított 12 órán belül a szolgáltató – a jogosult jogát sértő információt nyújtó igénybe vevő három munkanapon belül történő írásbeli tájékoztatása mellett – köteles intézkedni az értesítésben megjelölt információhoz való hozzáférés nem nyújtása vagy az információ eltávolítása iránt. A torrent tracker üzemeltetője azonban, ahogy már kifejtettük, nem helyez el semmilyen fájlt, nem tárol jogsértő adatokat, ezért hiába szólítják fel a jogvédett tartalom eltávolítására, azt nem tudja megtenni, mivel épp úgy nincs hozzáférése a tartalomhoz, ahogy a többi keresőnek sem. Ami a torrent trackeren látható, az a mű címe, az pedig nem jogsértő, ebből következően az előbbi szabályok összevetése alapján a torrent trackert működtetőket még ezen az alapon sem lehet felelősségre vonni.

Visszatérve a torrentező egyéni felhasználó büntetőjogi felelősségére: abban az esetben, ha a feltöltő az általa letöltött szerzői jogi védelem alatt álló művet nem tölti vissza százszázalékosan, a büntetőjogi felelősség tettesként történő megállapítása, álláspontom szerint, (az azonosíthatóság problémája miatt) szintén kétséges, illetve a feltöltés bizonyítása eleve nagy problémákat okoz, és ez már az eljárás megindításánál is jelentkezik.

Az eljárás megindítása, a gyanú és a megalapozott gyanú

Az 1998. évi XIX. törvény (Be.) 6. § (2) bekezdése szerint büntetőeljárás csak bűncselekmény gyanúja alapján és csak az ellen indítható, akit bűncselekmény megalapozott gyanúja terhel. A vizsgálódásunk tárgyául szolgáló

büntetőeljárások tipikusan a szerzőijog-védő szervezetek által tett feljelentések nyomán indulnak, de nem ritka a hatóság saját észlelése sem, amikor legtöbbször *más* bűncselekmény gyanúja miatt induló eljárásban elvégzett házkutatás folyamán észlelnek az eljárás alá vont személy számítógépén másolt audiovizuális tartalmakat.

A második esetben a nyomozás elrendelésére egyáltalán nincs törvényes lehetőség, mert a bűncselekmény gyanúja hiányzik. A letöltés nem bűncselekmény, annak *vélelmezése* pedig – még abban az esetben is, ha az otthoni felhasználó számítógépén volt torrent kliens –, hogy azt feltöltés mellett töltötték le, a már részletezett technikai lehetőségek miatt büntetőeljárás alapjául nem szolgálhat.

A torrent kliens használata önmagában nem bűncselekmény, azt egyébként sem csak a szerzőijog-védelem alá eső művek megosztására lehet használni, másrészt audiovizuális műveket nem kizárólag torrentezéssel vagy más, feltöltéssel is járó módon lehet az internetről letölteni [például fizetős http (smsweb) vagy úgynevezett newsgroupok használata, privát ftp-k, irc, rapidshare használata, streamelt (sugárzott) tartalom lementése, amelyek esetén a letöltő részéről egyáltalán nincs feltöltés].

Aligha szorul bővebb magyarázatra, hogy „a legvalószínűbb verzió *az, hogy a filmet torrent hálózatból töltötték le"*[6] és a Be. 4. § (2) bekezdésében foglalt ama szabály, miszerint a kétséget kizáróan nem bizonyított tény *nem értékelhető a terhelt terhére* – nem ugyanazt jelenti.

A szerzőijog-védő vagy közös jogkezelő szervezetek által tett feljelentések konkrét személy (általában felhasználói névvel és IP-címmel azonosítva) vagy konkrét tracker – korábban DC Hub – ellen irányulnak, és minden esetben a nyomozás elrendelését vonják maguk után. A feljelentés megtételének jogát a szerzőijog-védő szervezetektől, ahogy bárki mástól sem lehet elvitatni, hiszen közvádra üldözendő bűncselekmény gyanúja miatt bárki tehet feljelentést.

Fontos azonban leszögezni, hogy a sértetti jogok nem illetik meg automatikusan ezeket a szervezeteket. A Be. 51. § (1) bekezdése alapján sértett az, akinek a jogát vagy jogos érdekét a bűncselekmény sértette vagy veszélyeztette.

A Be. 56. § (1) bekezdése alapján a sértett, a magánvádló és az egyéb érdekelt a jogait a képviselője útján is gyakorolhatja. Képviselőként *meghatalmazás alapján* ügyvéd vagy nagykorú hozzátartozó járhat el, illetve a Be. 58. § (3) bekezdése alapján egyebek között, *ha a bűncselekménynek több sértettje van, a sértettek képviselőjeként a közhasznú szervezetekről szóló törvény – 1997. évi*

6 Idézet egy konkrét ügyben készült szakértői véleményből.

CLVI. tv. – hatálya alá tartozó olyan közhasznú szervezet is eljárhat, amelyet a sértettek vagy a sértettek egyes csoportjainak érdekképviseletére hoztak létre.

Ennek azért van jelentősége, mert a Be. 51. § (2) bekezdése elég széles körű jogokat ad a sértetteknek a büntetőeljárásban, de ezekkel csak azok a szerzőijog-védő vagy közös jogkezelő szervezetek élhetnek, amelyek egyben közhasznú szervezetként sértetti érdekképviseletre is be vannak jegyezve, ezért ennek vizsgálata elengedhetetlen például egy a nyomozást megszüntető határozat ellen bejelentett panasz elbírálásakor.

Visszatérve a feljelentés alapján megfogalmazható gyanú minőségére, leszögezhetjük, hogy egy feljelentésben leírt tényállítás, illetve az azt alátámasztó, a feljelentő által becsatolt bizonyíték *sohasem lehet önmagában elegendő a megalapozott gyanú konkrét személlyel szembeni közléséhez*. Különösen vonatkozik ez a feljelentő által felkért „számítástechnikai szakértő szakvéleményére". A feljelentő által felkért fedett nyomozó informatikus ebben az esetben *a felhasználókat megtévesztve* gyakorlatilag *beépül* a feljelentő által bűnözők gyülekezetének tartott torrent tracker tagjai közé, ott *a jogosultak engedélye nélkül személyes adatokat* (felhasználói név, IP-cím, e-mail cím stb., ami alapján a felhasználó konkrétan beazonosítható) *gyűjt, próbaletöltéseket végez*, majd ezeket dokumentálja a megbízó részére. Ezek nélkül az adatok nélkül a feljelentő gyakorlatilag semmit nem tudna meg a tracker működéséről, ez azonban, álláspontom szerint, akkor is súlyosan aggályos, ha a feljelentő nem mellékeli az adatokat a feljelentéséhez. A feljelentő, még ha a sértettet képviseli is egyben, egyébként sem kérhet fel a büntetőeljárás nyomozati szakaszában szakértőt (mert azt csak a nyomozó hatóság, az ügyész vagy a bíróság rendelheti ki), illetve az általa így megbízott szakértő szakértői véleménye a továbbiakban a Be. 108. §-ban meghatározott szakértői véleményként nem, maximum okirati bizonyítékként használható fel.

Egy ilyen feljelentés esetén tehát a nyomozó hatóság a bűncselekmény gyanúját megállapíthatja ugyan (nagyvonalúan túllépve az illegális személyes adatgyűjtés problematikáján), de a személyre szóló megalapozott gyanú meglétét hivatalból, a saját eszközeivel, a törvényes bizonyításnak megfelelően kell kivizsgálnia. Ha tehát a megalapozott gyanú megállapításához számítástechnikai szakértő szakvéleményének beszerzése válik szükségessé, azt a nyomozó hatóságnak kell kirendelnie.

Az ilyen ügyek jellegéből adódóan a számítástechnikai szakértő kirendelése gyakorlatilag elkerülhetetlen, a szakértő kirendelése sem fogja azonban megoldani a feltöltés bizonyításának, illetve a büntetőjogi (individuális) felelősség megállapításának problémáit.

A bizonyítás egyéb problémái

Az Szjt. 26–27. §-a szerinti nyilvánossághoz történő közvetítés – feltöltés – a büntetőjogban megkívánt kétséget kizáró módon történő bizonyítása még a szerzőijog-védő szervezetek szerint is *csak próbaletöltéssel lehetséges*, méghpedig a konkrét szerzői műpéldány egészére, megfelelő dokumentálás mellett, reprodukálható, tehát valamilyen adathordozóra történő lementés biztosításával. Természetesen annak bizonyításához, hogy a gyanúsított *„több terrabájtnyi*[7] *audiovizuális tartalmat tett az interneten torrenthálózaton keresztül elérhetővé”*, a több terabyte tartalmat kellene próbaletöltéssel letölteni.

Ennek oka, hogy ellenkező esetben (a szerzői műpéldány nélkül) nem lehet cáfolni a gyanúsított ama védekezését, hogy az általa feltöltött műpéldánynak csak a neve azonos a szerzőijog-védelem alatt álló fájllal, valójában az tartalma szerint jogvédelem alatt nem álló tartalmat takar, például a gyanúsított átnevezett házi videóját. Épp ezért a bizonyításhoz nem lehet elegendő a feltöltés alatt álló mű nevét és a fájl kiterjesztését tartalmazó, a torrent klienst működés közben ábrázoló úgynevezett „print screen” kép.

A nyomozó hatóság által kirendelt számítástechnikai szakértő a szerzőijog-védelem alatt álló művet a próbaletöltés során akár feltöltés mellett is letöltheti, mert az Szjt. 41. § (2) bekezdése alapján *a bírósági, továbbá államigazgatási vagy más hatósági eljárásban* a mű bizonyítás céljára, a célnak megfelelő módon és mértékben felhasználható. Ebből következik, hogy ugyanezt a szerzőijog-védő vagy közös jogkezelő szervezet által felkért szakértő hatósági eljárás hiányában viszont nem teheti meg, illetve csak a jogtulajdonos egyedi, a konkrét szerzői műre vonatkozó engedélyével, de a véleményét akkor sem lehet – a feljelentések kezelésénél már leírt okok miatt – szakértői véleményként figyelembe venni.

A nyomozó hatóság (illetve annak szakértője) által végzett és megfelelő módon dokumentált próbaletöltések, bár kétséget kizáró módon tudják bizonyítani a gyanúsított által végzett feltöltést, mégsem szolgálhatnak a büntetőjogi felelősség megállapításának alapjául, mert ebben az esetben a büntetőjogi tényállás lényeges eleme, a vagyoni hátrány okozása mint eredmény, hiányzik. A vagylagos tényállási elem, a haszonszerzési célzat, fel sem merül, hiszen ahogy a technikai háttérnél már olvashattuk, a torrent trackerek használata ingyenes, a felhasználók pedig nem kérnek egymástól pénzt a torrentezésért – nem is tudnának.

7 Általánosan alkalmazott a sajtóban helytelenül elterjedt helyesírás. Helyesen terabyte.

A vagyoni hátrány a büntetőjogban nem egy elvont, hanem a Btk. 137. § 5. pontjában konkrétan meghatározott fogalom, amely a vagyonban okozott kárt és az elmaradt vagyoni előnyt egyaránt magában foglalja, és minden esetben forintra pontosan ki kell számolni. Szerzői művek esetén kárról nem beszélhetünk, hiszen az tényleges értékcsökkenést jelent, marad tehát az elmaradt vagyoni előny, amelyet a szerzőijog-védők hajlamosak úgy meghatározni, hogy az azonos minden egyes letöltés és a szerzői műpéldány kiskereskedelmi árának szorzatával.[8] Az elmaradt vagyoni előny konkrét kimunkálásának módszeréről lehet ugyan vitatkozni, az viszont nem lehet vita tárgya, hogy annak meghatározásához szükség lenne arra az adatra, hogy a szerzői művet attól, aki seedelte vagy leechelte, hányan töltötték le. Ez azonban gyakorlatilag meghatározhatatlan, hiszen maga a seedelés is, ahogy már írtam, csak próbaletöltéssel bizonyítható. Annak belátásához pedig nem szükséges különösebb indokolás, hogy *a vagyoni hátrány mint eredmény nem következhet be a jogtulajdonosnál abban az esetben, ha az elkövető által feltöltött műpéldányt a nyomozó hatóság tölti le…*

Álláspontom szerint *ez a tény önmagában lehetetlenné teszi a cselekmény bizonyítását*, és akkor még meg sem említettem a többek által közösen használt számítógép problémáját (ahol a családtagok természetesen megtagadhatják a vallomástételt, illetve nem kötelesek egymásra terhelő vallomást tenni), vagy a gyanúsított védekezésének a Btk. 27. §-ában foglalt *tévedésre* alapítását, mely védekezéseket a büntetőügyekben eljáró hatóságoknak kell(ene) tételesen megcáfolniuk.

A bizonyítási nehézségekhez tartozik az is, hogy a digitális bizonyítási eszközök biztosításának szabályai szerint a lefoglalt adathordozók közvetlen szakértői vizsgálata nem lehetséges, mert ebben az esetben nem garantálható az eredeti adathordozó változatlanságának fenntartása. A kriminalisztikai szabályok szerint[9] az egész adattartalmat át kell másolni egy másik adathordozóra, mégpedig azért, mert az eredeti adathordozón rejtett adattartalmak és átmeneti állományok is találhatók, amelyek vizsgálata a bizonyításkor szükséges lehet. Mondanom sem kell, hogy a magyar nyomozó hatóságok erre nincsenek felkészülve, az ezzel ellentétes gyakorlat azonban azzal járhat, hogy a bíróság előtti eljárásban a védelem megkérdőjelezheti az egész szakértői bizonyítást, amely a bizonyítékok törvényes és szakszerű beszerzésének voltára (helyesen) egyre nagyobb súlyt fektető bíróság előtt könnyen sikerrel járhat.

8 Ez azért is nonszensz, mert nagyon sok esetben *Magyarországon egyáltalán nem kapható* szerzői művekről van szó. Az ezzel kapcsolatosan kirendelt árszakértői (!) véleményeket nem kívánom kommentálni.

9 Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek Lapja, 2010/2.

Összegzés

Írásommal arra szerettem volna rávilágítani, hogy a fájlcserélő programokat használók nem tekinthetők automatikusan bűncselekményt elkövető potenciális gyanúsítottaknak, ezért az ellenük történő általános büntetőjogi fellépés nem indokolt, de nem is lehetséges. Az audiovizuális művek letöltése Magyarországon legális, a feltöltés (a nyilvánosságnak közvetítés) pedig egyrészt bizonyíthatatlan, illetve rendkívül költséges bizonyítással jár, másrészt a vagyoni hátrány okozását mint következményt ekkor sem lehet megállapítani, az elmaradt vagyoni előny konkrét összegének hiányában.

Az egyes felhasználók elleni büntetőeljárások megindítására az említett bizonyítási nehézségek miatt nem látok lehetőséget, épp ezért indokolatlan és érthetetlen a torrent trackerek elleni nyomozó hatósági fellépés.[10] Ezzel szemben azonban, mivel a társadalomra veszélyessége jóval nagyobb, a bizonyítása viszont jóval könnyebb, a továbbiakban az FTP-szervereket működtető, több száz terabyte jogvédett anyagot smsweben keresztül letölthetővé tevő és ebből havonta milliós hasznot húzó kalózok elleni nyomozó hatósági fellépés lenne indokolt.

A számítástechnika ilyen irányú gyors fejlődése kétségkívül nehéz, olykor méltánytalan helyzetbe hozta a szerzői művek jogtulajdonosait.[11] Az állampolgárok tömegeinek kriminalizálása helyett[12] azonban a szerzői jogok érvényesítésének új lehetőségeit kellene inkább megnyugtató módon rendezni, mert a razziák és egyéb hatósági fellépések szemmel láthatóan kudarcot vallottak, az egyre modernebb fájlcserélő módszerek elterjedését pedig ilyen eszközökkel máskülönben sem lehet eredményesen megakadályozni.

10 Annál is inkább, mert már létezik és hamarosan robbanásszerűen el fog terjedni a torrent tracker nélküli torrentezés technikai lehetősége. Az úgynevezett *magnet link* használatával nincs szükség a tracker közvetítésére, a technika lehetővé teszi, hogy a felhasználók közvetlenül egymáshoz kapcsolódjanak, ezzel lehetetlenné téve a jogvédők beépülését, ez pedig egyenlő a jogvédők ilyen irányú tevékenységének ellehetetlenülésével.

11 Tegyük hozzá, hogy jelenleg *nincs* korrekt számítási módszer arra vonatkozóan, hogy a fájlcsere mekkora bevételkiesést jelent, az viszont tagadhatatlan, hogy vannak *bevételnövelő* hatásai is.

12 Óvatos becslések szerint Magyarországon már több mint egymillió ember használ rendszeresen fájlcserélő programokat.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp60-84

KARSAI KRISZTINA

Jogi taposóaknák a hamis áruk piacán[1]

Egy ártalmatlannak tűnő bűncselekmény analízisekor feltárt jogalkalmazási és jogértelmezési anomáliák

Jelen tanulmány a fogyasztóvédelem és büntetőjog témakörében írt nagyobb lélegzetű munka előtanulmánya: a *Belügyi Szemle* hasábjain az áru hamis megjelölése bűncselekményének analízise során feltárt jelenségeket és – nem várt – jogi (jogalkalmazási) problémákat összegzem.

A bűncselekmény analízise a bűncselekményi tényállás részletes elemzését, a hazai jogirodalom ellentmondásainak feloldását (legalábbis erre irányuló kísérletet), a bűncselekmény miatt indult büntetőeljárások jellemzőinek az ítélkezési gyakorlaton[2] keresztül történő bemutatását jelenti.

E helyütt a teljes feldolgozásból – terjedelmi okok miatt – néhány válogatott problémakör bemutatására kerül sor, így az áru hamis megjelölése tényállásából az áru *összetéveszthetőségének* kérdése és ennek következményei az igazságügyi *szakértői* tevékenységre; a *versenytárs beleegyezése hiányának* dogmatikai kategorizálása; a *szándékosságot* érintően észlelt aggályos gyakorlat; valamint az elkövetési *érték* viszonylatában tetten érhető jogalkalmazói elhajlások és ennek következményei. Ezen kívül röviden összefoglalom a bűncselekmény *jogtárgyával* kapcsolatos eredményeket is.[3]

1 A tanulmány az OTKA K 72692 nyilvántartási számú kutatás („Fogyasztóvédelmi büntetőjog" 2008–2011) résztanulmánya. A kutatásban szereplő akták feldolgozása dr. Katona Tibor bíró (Szegedi Ítélőtábla) közreműködésével történt.

2 Az említett OTKA-kutatásban nyolc megye büntetőügyeinek aktáit dolgoztuk fel, amelyek a vizsgált „fogyasztóvédelmi" bűncselekmények miatt történt vádemeléssel kerültek bírói szakba. Az áru hamis megjelölése büntette tárgyában 150 megindult büntetőeljárást dolgoztunk fel: 12 végződött felmentéssel, kettő a büntetőeljárás megszüntetésével, a többiben büntetést szabott ki vagy intézkedést alkalmazott a bíróság.

3 A bűncselekményi analízis az itt nem említett további törvényi tényállási elemek mindegyikére nézve alapos vizsgálatot és az ezekkel kapcsolatos gyakorlat elemzését tartalmazza, kiterjed a szankciókiszabások értékelésére, valamint kimutatja a szimbolikus fogyasztás társadalmi jelenségének befolyását a büntetőjogi jogtárgyakra. A kézirat megjelenés alatt áll az Acta Juridica et Politica Szeged Tomus Fasc. LXXIV. kötetében.

Az áru összetéveszthetősége

A hatályos magyar Btk. a 296. §-ban szabályozza az áru hamis megjelölésének bűntettét, e szerint három évig terjedő szabadságvesztéssel büntetendő, aki árut – a versenytárs hozzájárulása nélkül – olyan jellegzetes külsővel, csomagolással, megjelöléssel vagy elnevezéssel állít elő, amelyről a versenytárs, illetőleg annak jellegzetes tulajdonsággal bíró áruja ismerhető fel, vagy ilyen árut forgalomba hozatal céljából megszerez, tart, illetőleg forgalomba hoz.

A bűncselekmény elkövetési tárgya olyan áru, amely összetéveszthető a versenytárs árujával. Az *összetéveszthetőség* – álláspontom szerint – lehet abszolút (objektív) és relatív (szubjektív) is. Az abszolút tartalmú összetéveszthetőség azt jelentené, hogy a két entitás (eredeti és hamisítvány) fizikai és esztétikai jellemzőinek összevetése eredményeképpen megállapítanánk a jellegzetességek objektív hasonlóságát vagy egyezését, s amennyiben nagyfokú[4] vagy teljes az átfedés van (három-három csík, ugyanaz a betűtípus, ugyanaz a szín stb.), az összetéveszthetőség adott lenne. Ez egy objektív kategória – értsd: az elkövető tudattartamától független –, amit például a védjegybitorlás megállapításakor kiválóan lehet alkalmazni. A büntetőjogi relevanciája azonban meglehetősen kérdéses (lásd később).

A büntetőjogi tényállásban szereplő *„amelyről a versenytárs, illetőleg annak jellegzetes tulajdonsággal rendelkező áruja ismerhető fel”* kitétel azonban az összetéveszthetőséget szükségképpen relativizálja, mivel a *felismerhetőség* mindig attól függ, hogy éppen ki látja az adott árut fizikai valójában. A büntetőjogban lehetőség szerint korlátozni kell az ilyen esetlegességet, és kísérletet kell tenni az alkalmazandó zsinórmérték megtalálására. Ebben az esetben erre alkalmas lehet az átlagfogyasztó mércéje, aki tudatos és kellően informált[5]: az eredetivel ugyanis nyilvánvalóan – az átlagfogyasztó ismeretei miatt – össze nem téveszthető utánzott áru nem eshet a tényállás hatálya alá.

Ebből az is következik, hogy a tényállás szerkezete nem önmagában az utánzást vagy a hamisítványokat teszi elkövetés tárgyává, hanem az olyan hamisítványt, amely az összetévesztésre is alkalmas. A hamisítvány – ontológiai és logikai szempontból – az, ami a tárgy, az eredeti igazságát sérti, a valóságnak nem megfelelő: utánzás, hamisítás, meghamisítás útján is létrejöhet. Az érdekes azonban az, hogy a hamisítás ténye nem tartalmazza egyben az összetéveszthetőséget („más áruja ismerhető fel róla”) is mint fogalmi ele-

4 Persze vitás lehet, hogy mit jelenthetne a nagyfokú hasonlóság.

5 Az átlagfogyasztó fogalmának más jogágakban és Európában kialakult ismérveinek büntetőjogbeli alkalmazásáról e kutatási program keretében másutt fejtem ki részletesen a nézeteimet.

met, még akkor sem, ha tudjuk, a hamisítók tipikusan az összetéveszthetőségből fakadó előnyök miatt hamisítanak, bármilyen hamisítható dologról legyen is szó.

Ezt egyébként alátámasztja az is, hogy a jogalkotó nem elégedett meg a hamis megjelölés (csomagolás, külső, elnevezés) tényével, hanem ahhoz az összetéveszthetőség kritériumát is hozzárendelte. Véleményem szerint tehát az összetéveszthetőség nem adott, ha a *hamisítvány nagyon gyatra*, vagy a meghatározott jellegzetes tulajdonságok kivitelezése olyan silány, hogy fel sem merülhet az eredetiség látszata. Nyilvánvalóan nincs összetéveszthetőség például akkor, ha az autókereskedő az eladandó Lada gépjárművekre Porsche jelet ragaszt: a Porscheként eladott Lada ügyében legfeljebb csalás miatt kellene büntetőeljárást indítani, nem pedig áru hamis megjelölése miatt. Mindebből az következik, hogy az összetéveszthetőség ténye éppen olyan fontos eleme a tényállásnak, mint a „hamisítás" (hamis jellegzetes tulajdonságok alkalmazása), ezért ezt a büntetőeljárásban is bizonyítani kell, nem elég önmagában a hamisítás tényére koncentrálni.

Érdemes e helyütt azt is megemlíteni *a contrario* argumentumként, hogy – az előbbiekkel szemben – a pénz vagy az okiratok hamisításánál a megtévesztésre (összetévesztésre) alkalmasság nem tényállási elem, ezért a gyakorlat a silány minőségű, azonnal felismerhető hamisítványoknál is megállapítja a bűncselekményt.

Nagyvonalú jogalkalmazás – „a versenytárs hozzájárulása nélkül"

Mindenekelőtt kiemelendő, hogy ez a tényállási elem csak az előállítási fordulathoz járul, a megszerző, tartó és forgalomba hozó változatokhoz nem. Ez azt jelenti tehát, hogy a gyakorlatban is tipikusan megvalósuló forgalmazói cselekményeknél a versenytárs hozzájárulása irreleváns, ezeknél az elkövetési tárgy „hamissága" és összetéveszthetősége (lásd a korábban kifejtetteket) az irányadó, s az, hogy a tettes tudja, az általa forgalmazott áru meghatározott külső sajátosságai a versenytárs hozzájárulása nélkül kerültek az árura.

A Btk.-rendelkezés lényeges eleme, hogy a cselekményre a versenytárs hozzájárulása nélkül kerül sor. A témakört – a tankönyv- és kommentárirodalomban – feldolgozó különböző szerzők összességében már abban sem értenek már egyet, hogy *tényállástanilag* minek minősül ez az elem, illetve igazából abban sem, hogy mit is jelenthet.

A továbbiakban részletesebben elemzem az előállítási alakzathoz járuló elkövetési módot.

Szakirodalmi álláspontok

A „*kapcsos" kommentár*[6] például „negatív tényállási elemnek", „a tényállásszerűség negatív feltételének" tekinti[7], ami teljesen félrevezető, különösen, hogy később ugyane műben ezzel összefüggésben a jogellenesség hiánya merül fel. Ez az értelmezés feltehetően a negatív tényállási elemek tanának félreértéséből adódik, amelynek lényege *Nagy* szerint, hogy a pozitív és negatív tényállási elemek közötti megkülönböztetésben az utóbbiak bizonyos büntethetőséget kizáró okok hiányát jelenthetik. Így a negatív tényállási elemek tana alapján például a jogos védelemből elkövetett cselekmény nemcsak nem bűncselekmény, de nem is tényállásszerű, mivel a társadalomra veszélyességet (jogellenességet) kizáró okok egyike nem hiányzott, hanem fennforgott. Nagy kifejti azonban, hogy egy olyan dogmatikai rendszerben, amely nem tekinti a törvényi tényállás alkotóelemének sem a társadalomra veszélyességet, sem a jogellenességet, az ezeket kizáró okok hiánya sem fogadható el tényállási elemnek.[8] Egyetértek továbbá álláspontjával, miszerint a büntethetőséget kizáró okok tényállási elemmé transzformálása ellentmond mind a Btk. szerkezeti felépítésének, mind pedig a bírói gyakorlatnak, amely a büntethetőséget kizáró okokat csak a büntethetőségi akadályok, nem pedig a tényállásszerűség síkján vizsgálja. Mindezek alapján megállapítható, hogy a kapcsos kommentár e tekintetben – mind a dogmatikai struktúrák nem megfelelő hivatkozásával, mind pedig a zavaró önellentmondással – nem nyújt irányadó megközelítést.

A *pécsi tankönyv*[9] szerint vitatható, hogy erre a tényállási elemre szükség van-e, hiszen a sértett beleegyezését az elméleti jogászok többsége törvényben külön nem szabályozott, de elismert büntethetőséget kizáró oknak tekinti. Igaz, ettől függetlenül egyfelől az elkövetés módjaként, másfelől jogellenességet kizáró okként kezeli, ami aligha tekinthető kiérlelt és dogmatikailag megalapozott álláspontnak. Méghozzá azért, mert az elkövetés objektív té-

6 Berkes György (szerk.): Magyar Büntetőjog. Kommentár a gyakorlat számára. 2. kiadás. HVG-ORAC Kiadó, Budapest, 2006, I. kötet, Btk. XVII. fejezet

7 Molnár Gábor: Gazdasági bűncselekmények. HVG-ORAC Kiadó, Budapest, 2009, 870. o.

8 Lásd Nagy Ferenc: A magyar büntetőjog általános része. HVG-ORAC Kiadó, Budapest, 2008, 144. o.

9 Erdősi Emil – Földvári József – Tóth Mihály: Magyar büntetőjog. Különös Rész. Osiris Kiadó, Budapest, 2005

nyeihez tartozó elkövetési mód nem lehet egyben jogellenességet kizáró ok. Az igaz, hogy *lehetne* épp jogellenességet kizáró ok is, de amennyiben a jogalkotó a tényállás részeként szabályozza, az a tényálláshoz tartozik, nem pedig azon kívüli büntethetőséget megszüntető ok, így hiánya esetén (az adott bűncselekménynél tehát a beleegyezés fennállása esetén) már eleve nem is tényállásszerű a cselekmény.

Hasonlóan vélekedik *Tóth* is, mivel kimondja, hogy az elkövetés módja a hozzájárulás hiányában történő elkövetés, ennek ellenére a hozzájárulás a jogellenességet zárja ki nála is.[10] Ez a nézet sem következetes.

Beleegyezés hiányának vélelmezése

A megvizsgált büntetőügyekben a versenytárs beleegyezésének hiányát szinte kivétel nélkül minden esetben vélelmezték a bíróságok, és ehhez azt a szakértői megállapítást vették alapul, miszerint a kérdéses árucikkek hamisítványok. Mindehhez még a korábban is említett, meglehetősen *nagyvonalú jogértelmezés* is járul, amelynek következtében a forgalmazói jellegű magatartások esetén is vizsgálták a hozzájárulás meglétét, holott az – a korábban kifejtetteknek megfelelően – nem tényállási elem.

A szakértői véleményekben több esetben nincs nyoma annak, hogy például az adott védjegyjogosult nyilatkozott volna a beleegyezése hiányáról, az meg végképp elő sem fordult, hogy a szakértő esetleg külföldi versenytársakra is kiterjesztette volna a vizsgálatot (például semmi nem zárja ki annak elvi lehetőségét, hogy a más országból behozott gyenge minőségű áru vonatkozásában meglegyen a másik országbeli lehetőség az ilyen előállításra; még akkor sem, ha ez nyilván nem tipikus). Kétségtelen tény persze ez utóbbival kapcsolatban, hogy már egy versenytárs hozzájárulásának hiányában is tényállásszerű lehet a cselekmény.

Amennyiben nem volt adat a versenytárs beleegyezéséről, a hamisítvány rendkívül alacsony minőségéből vonta le a szakértő a következtetést, hogy az csak hamisítvány lehet, aminek következtében látta kimondhatónak, hogy hiányzik a versenytárs beleegyezése. A tényállási elemként szabályozott versenytárs beleegyezésének hiánya *azonban nem vélelem, azt kétséget kizáróan bizonyítani kell.* De a jelenlegi tényállási konstrukció és a lefolytatott bizonyítások nem felelnek meg egymásnak. Megállapítható ugyanis, hogy ha nincsen adat, akkor nincs kétséget kizáróan bizonyított tény sem, azaz nincs két-

10 Tóth Mihály: Gazdasági bűnözés és bűncselekmények. KJK-Kerszöv, Budapest, 2000, 167. o.

séget kizáróan bizonyítva a beleegyezés hiánya. Ennek következtében nem lehetne megállapítani a tényállásszerű elkövetést: a nyomozó hatóságoknak legalább egy versenytárs vonatkozásában bizonyítaniuk kell a beleegyezés hiányát.

Kritika

Véleményem szerint e tényállási elem meglehetősen problematikus mind dogmatikai, mind gyakorlati szempontokból. Ha e tényállás jövőbeni fenntartása szükségesnek mutatkozik, a versenytárs hozzájárulása nélküli tényállási elemet tanácsos lenne elhagyni. Ebben az esetben a versenytárs beleegyezése a jogellenesség szintjén jelenne meg, s mind gyakorlati (bizonyítási), mind dogmatikai szempontból megfelelőbb helyzet állna elő. A jogellenességet kizáró okként való figyelembevétel esetén a versenytárs hozzájárulása a büntetőjogi felelősség alól mentesítő tényező lenne, ami meghaladja a tényállásszerűség szintjét. A cselekményt lényegében jogellenesnek vélelmezzük – mint ahogy minden tényállásszerű cselekmény esetében tesszük –, és ha van adat és bizonyíték a versenytárs(ak) hozzájárulására, a jogellenességet kizáró ok érvényesülhetne, s az elkövető mentesülhetne a felelősség alól. Ez a jogellenességet kizáró ok a sértett beleegyezésének felel meg, s az ehhez kidolgozott dogmatikai és elvi tételek[11] maradéktalanul alkalmazhatók lennének.

Más kérdés, hogy a gazdasági szférában az ilyenfajta sértetti beleegyezés értelemszerűen szerződésen alapul, ami a védjegy, használati minta stb. értékek használására vonatkozik. Amennyiben van tehát adat a versenytárs(ak) beleegyezésével kapcsolatosan, tudniillik arra nézve, hogy az áruk meghatározott megjelölésével tisztában voltak és azzal egyetértettek, akkor jogellenesség hiánya okán fel kell menteni az elkövetőt.

A bizonyítás elméleti sémája más lenne tehát ebben az esetben, a bizonyítási teher is lényegében megfordulna: míg a tényállási elemek meglétét maradéktalanul bizonyítani kell, a jogellenességet kizáró okokat nem kell külön egyesével megvizsgálni, ellenkező adat hiányában azokra (pontosabban azok hiányára) külön bizonyítást nem kell lefolytatni. Hiszen a hatóságnak nem kellene bizonyítania a beleegyezés hiányát minden egyes esetben, ha azonban van a versenytárs beleegyezésére utaló adat, azt alaposan meg kell vizsgálni, mivel a beleegyezés fennállása elbuktatja a vádat.

11 Nagy Ferenc: i. m. 129–141. o.

Kiválóan példázza az előbbieket a következő tényállás, amely egy bírósági ügy ítéleti tényállása: *„A vádlott 2003. május hónapban – közelebbről meg nem határozható időpontban – a […] Kft. ügyvezetőjeként a miskolci […] boltban »The North Face Inc.« szóvédjeggyel ellátott ruházati termékeket – 4 db kabátot, 2 db polár felsőt, valamint 1 db hátizsákot hozott forgalomba összesen 140.000 forint értékben, melyeket ezt megelőzően egy ismeretlen személytől szerzett meg."*

Az ügyben a kirendelt szakértő megállapításait – amelyeket a vádirat is tartalmazott – a bíróság szó szerint átvette: *„a termékek gyártója, illetve forgalmazója ismeretlen, erre tekintettel a kft. nem rendelkezett a védjegyjogosult engedélyével a fent említett, védjegyoltalom alatt álló megjelölésekkel ellátott termékek forgalmazására, ezért ilyen engedély hiányában a kérdéses termékek hamisítványoknak minősülnek"*.[12]

A bíróság a kérdéses termékek gyártójának (forgalmazójának) ismeretlenségéből következtet arra, hogy a vádlottnak – mivel ismeretlen a gyártó – nem lehet engedélye a forgalmazásra. Megismételhető azonban e helyütt is, hogy a tényállás a forgalomba hozatali elkövetési magatartás vonatkozásában azt követeli meg, hogy a „hamis" árut hozza forgalomba, itt a versenytárs hozzájárulása irreleváns. Emiatt alapvető hiba a forgalmazón számon kérni a forgalmazáshoz szükséges engedélyt, legalábbis a büntetőjogi felelősség megállapítása szempontjából. Amit az ilyen cselekmény elkövetőjén számon kell kérni, az az, hogy tudta-e (belenyugodott-e), hogy az árut a versenytárs hozzájárulása nélkül látták el az adott jellegzetes tulajdonsággal. Ha azonban releváns lenne az engedély, akkor az *ismeretlenség ténye* a konkrét ügyben sem jelenthetné azt, hogy nincs engedély, hanem azt, hogy nem lehet tudni, van-e. Ez pedig lényeges különbség. Pont ez lenne az a mezsgye, ahol a kétség az úr, s amennyiben fennáll, azt a terhelt javára kell értékelni *(in dubio pro reo*[13]*).* A bíróság akkor járt volna el következetesen (igaz, rossz premisszával), ha a felmerülő kétség miatt nem állapítja meg a bűncselekmény elkövetését. Amennyiben pedig helyes premisszával az áru hamisságának ismeretét vizsgálná, ott a termék gyártójának (forgalmazójának) ismeretlensége csupán egy körülmény a sok közül, ami alapján az elkövető tudattartalmát vizsgálni kellene. A konkrét eljárásban a vádlott – az áruk hamisságára

12 B.0128.2005 Miskolci Városi Bíróság.

13 Lásd részletesen Karsai Krisztina – Katona Tibor: Az ártatlanság vélelme és a vádlott meg nem cáfolt védekezése. Jogtudományi Közlöny, 2010/4., 171–179. o.

vonatkozó – meg nem cáfolt védekezését a bíróság az előbbi érveléssel söpörte le, s az engedély hiányára alapozta a büntetőjogi felelősséget. Ezzel – sértve az anyagi jogi legalitás elvét – a Btk.-tól eltérő tényállási elemek megvalósítását kérte számon a bíróság terheltől, másfelől pedig az *in dubio pro reo* elvet sem alkalmazta.[14]

Tolódás az objektív felelősség irányába?

A bűncselekmény szándékosan követhető el, gondatlan alakzatát a törvény nem rendeli büntetni. A büntetőjogi – bűnösségen alapuló – felelősség akkor állapítható meg, ha a tettes ismerte a ténybeli körülményeket, s a tényállás objektív elemeivel kapcsolatban nem volt tévedésben. A Btk. 296. § szerinti bűncselekmény esetén így a szándékosság tudati oldalának ki kell terjednie arra, hogy az adott áru adott jellegzetes tulajdonsága összetéveszthető, arra, hogy a versenytárs nem egyezett bele az adott jelzés (stb.) használatába, valamint a szándékosságnak értelemszerűen ki kell terjednie a megfelelő elkövetési magatartások tanúsítására.

Az egyik ügyben ezt olvashatjuk: „*A törvényi tényállás az elkövető tudattartamától függetlenül követeli meg törvényi tényállási elemként, hogy az elkövetési magatartásra a versenytárs hozzájárulása nélkül, annak hiányában kerüljön sor, továbbá szintén objektív feltételként rögzíti azt, hogy a megszerzett áru mely körülmények folytán lesz, illetőleg válik alkalmassá arra, hogy összetéveszthető legyen a versenytárssal, illetőleg annak jellegzetes árujával.*”[15] Hasonló tartalmú indokolások olykor előfordulnak más ügyekben is, azonban ez – véleményem szerint – rendkívül aggályos és nem tartható jogi álláspont, aminek ráadásul kifejezetten káros következményei vannak.

Először is e nézet az objektív tényállási elemek szerepét meglehetősen nagyvonalúan kezeli, s lényegében minden lényeges tárgyi körülményt függetlenít az elkövető tudattartamától. Azaz azokra vonatkozóan a büntetőjogi felelősség megállapításához semmiféle szubjektív „kapcsolatot” nem követel meg. Ez azt jelenti, hogy eleve kizárt és nem releváns a tévedésre való hivatkozás, azaz még ha például a versenytárs – rosszhiszemű – megtévesztő ma-

14 Az ügy további sajnálatos jellemzője, hogy az aktában nem szerepel a polgári jogi igény előterjesztése, erről azonban a bíróság döntött ítéletében – így csak azt lehet feltételezni, hogy valamikor megvolt, majd elveszett. Igaz, annak iktatására sem került sor, vagy az irat létezésének más nyilvántartási nyoma sincs, így a polgári jogi igényt kereseti kérelem nélkül bírálta el a bíróság.

15 30.B.340.2006 Miskolci Városi Bíróság.

gatartása következtében alakul is ki az engedély fennállásával kapcsolatos tévedés, az az előbbi érvelés alapján nem zárja ki a bűnösséget. Itt nem az a kérdés, hogy ez mennyire életszerű vagy sem, hanem annak gyanúja, hogy a bíróság a bűnösségen alapuló felelősséget eltolja e bűncselekmény körében az *objektív felelősség* irányába. Ez pedig megengedhetetlen.

Az összetéveszthetőség mint „objektív feltétel" vonatkozásában pedig – fenntartva a korábbiakat – azért értékelem hibás jogi álláspontnak az előbbit, mivel a tényállási elem éppen hogy egyfajta „relatív (szubjektív) összetéveszthetőséget" követel meg csupán, ami a fogyasztók érzékelésében megjelenő téves képzet lehetőségét jelenti. Attól relatív az összetéveszthetőség, hogy „amiről a versenytárs áruját szokták felismerni" megfogalmazás a címzetti kör tévedési lehetőségét tartalmazza, azaz szükségképpen feltételezi az adott versenytárs és árujának ismertségét és ismeretét. Ez azonban nem „abszolút összetéveszthetőség", aminek tárgyában a szakértők nagy előszeretettel szoktak állást foglalni: azaz amikor a különböző jellegzetes tulajdonságokat védjegylajstromi leírás alapján hasonlítják össze. Emiatt, véleményem szerint, a védjegybitorlás ténye – mint ahogy az az előbbi ügyben előzményként fennforgott – nem ad még választ arra a kérdésre, hogy az adott védjegy-e az, amelynek alapján a fogyasztók fel szokták ismerni az árut. Így tehát például a négycsíkos, nem Adidas nevű cipők esetében a Fővárosi Ítélőtábla (8.Pf.21.139/2004/4) megállapította ugyan a védjegybitorlást, a tipikus fogyasztót a „csíktöbblet" nem téveszti meg, hiszen az átlagos fogyasztó tudja, hogy az Adidas cipőnek három csíkja van. Elképzelhető azonban, hogy más, kevésbé ismert márkáknál a védjegybitorlás ténye az összetéveszthetőség körében is releváns.

Bűncselekményi értékhatár

A bűncselekmény elkövetési értékének meghatározása

A bűncselekményi tényállásnak nem eleme a hamisan megjelölt áru értéke, a szabálysértési alakzat miatt azonban a bűncselekményi változat csak akkor valósul meg, ha az áru értéke, amire elkövették a bűncselekményt, a százezer forintot meghaladja.

Az, hogy a joggyakorlat mit tekint az áru értékének, rendkívül színes képet mutat, azonban korántsem megnyugtató módon.

Az ügyek átvizsgálása meglepő eredményt hozott a tekintetben, hogy az áru értéke miként jelenik meg a büntetőeljárásokban, mivel hatféle, ismétlődő, de mégis *különböző* megjelenési módot lehetett elkülöníteni:

a) nem merül fel az áru értékének a kérdése az adott ügyben, e tényre nézve nincs adat az ítéletben (az e csoportba tartozó ügyeknél volt olyan, amelyben a nyomozás során szakvéleményt még kértek, de a későbbi szakaszokban azt nem vették figyelembe),
b) az áru értéke helyett más, pénzben kifejezett összegszerűség szerepel (például vagyoni hátrány),
c) az áru értékének megemlítése, de követhető bizonyítás vagy következtetés nélkül,
d) az áru értékének megállapítása megtörténik a lefolytatott szakértői vélemény alapján (annak figyelembevételével vagy annak kizárásával),
e) az áru értékének megállapítása megtörténik a vádlott bemondása alapján,
f) az áru értékének megállapítása megtörténik a sértett bemondása alapján.

Kis számban ugyan, de előfordul, hogy az aktában (vád, jogerős határozat) az áru értékének a kérdése egyáltalán fel sem merül, az általunk megvizsgált aktákból öt esetben.[16] Ezen esetekben is elképzelhető, hogy a szakértő megállapított valamilyen értéket, azzal azonban a jogalkalmazó hatóságok nem foglalkoztak, azt nem tartották relevánsnak a felelősség megállapítása szempontjából. Így csak jóhiszeműen vélelmezhetjük, hogy a hamisított áruk értéke meghaladta a százezer forintot.

Az esetek jelentős részében (ötven ügy) előfordult, hogy az aktákban (vád, jogerős határozat) az áru értékét megemlítik ugyan, de sem a szakértői vélemény, sem az akta egyéb adatai (például áru darabszáma) alapján nem értelmezhető, hogyan jutott el a hatóság az adott érték meghatározásáig. Ezekben az esetekben a szabálysértési értékhatár meghaladását már vizsgálja a hatóság, de a bizonytalansági tényező még mindig jelentős: csak remélhetjük, hogy a bűncselekményi értékhatár átlépését az áru értékének *megfelelő* számítása idézte elő.

Az esetek többségében (85 ügy) az akták pontosan tartalmazták az áru értékét, és annak nyomát is, hogy az értéket a szabálysértéstől való elhatárolás céljából vizsgálta az eljáró bíróság (ügyészség). Ellentétben az előző esetek hiányos ténymegállapításaival, ezen ügyekben tehát számszakilag is pontosan levezethető értékek szerepelnek, azonban itt az a probléma merül fel, hogy vajon a bíróság pontosan mit is tekint az áru értékének.

16 Itt értelemszerűen az 1998. évi LXXXVII. törvény hatálybalépése (1999. március 1.) előtti elkövetéseket nem vettem figyelembe, mivel az értékhatár kérdése csak ezen időponttól bír relevanciával.

Már önmagában aggályosnak tartom, hogy ebben a vonatkozásban háromféle értékmeghatározás érvényesül egymás mellett, olyanok, amelyek soha nem vezethetnek azonos értékre mint eredményre; így az elkövető szabálysértésért vagy bűncselekményért való felelőssége csupán attól is függhet, hogy épp melyik számítási módszert választja a bíróság. Ez azonban ellentétes az anyagi joggal: a joggyakorlatnak meg kell változnia.

A felkért szakértők általában kétféle számítási módot adnak meg az áru értékével kapcsolatosan, egyfelől az eredeti márkás termék kiskereskedelmi forgalmi értékét, másrészről viszont a hamisítvány márkajelzés nélküli piaci (feketepiaci) átlagárát, ami a konkrét minőségi jellemzőkkel bíró áru tényleges piaci ára. A megvizsgált ügyekben e kétféle számítási mód valamelyikét, vagy egy a két érték között elhelyezkedő köztes értéket vették figyelembe.

A 85 ügy iratából 23 esetben az eredeti márkás áru (azaz az utánzott áru) értéke volt az irányadó, ami teljességgel elfogadhatatlan, mert olyan ténytől teszi függővé az elítélést, amire nézve az elkövetőnek semmiféle befolyása, tudattartalma nem terjedt ki.

Ilyen elbírálás minden általunk megvizsgált megyében történt, de az is megállapítható, hogy ezekre kivétel nélkül a BH 2007/398. eseti döntés közzététele előtt kerül sor, azaz a döntéssel a Legfelsőbb Bíróság a jelentős mértékben eltérő ítélkezési gyakorlatot egy irányba terelte. A helyesen figyelembe veendő érték az előállított, megszerzett, tartott vagy forgalmazott nem márkás termék kiskereskedelmi, piaci árához igazodik, ezt követte a hatóság az elbírálás során 57 ügyben. Öt további esetben a bíróság – lényegében indokolás nélkül – valamilyen köztes értéket alkalmazott: e csoportban azonban van olyan ügy is, amit bár az említett BH után bíráltak el, nem követték annak orientáló jellegét.

Az *eredeti márkás áruk* értékének számításával sokkal magasabb érték jön ki, mint a hamisítvány piaci átlagárával való számításkor, ennek éppen a bűncselekményi alakzat megvalósulása és az egyén büntetőjogi felelőssége szempontjából döntő jelentősége van. Megállapítható továbbá, hogy ezen esetek felénél a nem márkás áru piaci értékének figyelembevétele mellett egyáltalán nem valósult volna meg bűncselekmény. Ezen esetekben tehát a helyes jogértelmezés felmentést hozott volna, ezzel szemben a vádlottakat elítélték.

Kirívó, de szerencsére nem gyakori bírói (ügyészi) megállapítás, hogy a cselekmény valamely összegű vagyoni hátrányt (13 ügy), elmaradt vagyoni hasznot (2), illetve kárt (6) okozott; ezen ügyekben polgári jogi igényt nem bírált el a bíróság. Nem világos az akták alapján, hogy pontosan milyen jog-

értelmezés vezetett ezekhez a megállapításokhoz, feltehetően a szakértői véleményben foglaltak mérlegelés nélküli átvétele, mivel az említett ügyek többségében (ahol vagyoni hátrány, illetve vagyoni haszon jelent meg a vádban, illetve az ítéletben) a szakvélemény tartalmazza ezen – inadekvát – kitételeket. Azt hiszem, felesleges is e helyütt részleteiben kitérni e megállapítások teljességgel tarthatatlan mivoltára.

Több ügyben és több megyében – a nyomozati iratok alapján – azt észleltük, hogy az eljárásban, így az ítélet meghozatalában is a vádlott által, a lefoglaláskor megadott érték játszik szerepet. A vádlott tehát arról nyilatkozik, hogy mennyiért kívánta értékesíteni a hamisított árut, s az ő bemondása lesz az alapja – ha, mint néhány esetben, nincs szakértői vélemény – a bűncselekménnyé minősítésnek. Ezzel lényegében a vádlottnak engedjük át a kérdés eldöntését, hogy szabálysértési vagy büntetőjogi felelősségre vonást „kíván-e". A vádlott bemondása alapján történő bűncselekményi értékhatár átlépésének megállapítása csak akkor megalapozott, ha az ügy egyéb körülményei nem cáfolják ezt az állítást.[17]

Az ügyek jelentős részében maga a sértett (márka-, védjegyjogosult) az, aki meghatározta az áru értékét, vagy ha nem ő, akkor az általa megbízott szabadalmi képviselő, illetve – tipikusan világcégeknél – a cég hazai képviselete. Ilyenkor szükségképpen az eredeti áru értéke jelent meg az aktákban, amely alapján a bűncselekményi értékhatár átlépését is megállapították. Véleményem szerint a sértett általi meghatározástól az a megoldás sem különbözik, hogy a hatóságok a Márkavédők Egyesületét vagy a Védjegy- és Szerzői Jogvédő Alapítványt rendelik ki szakértőként. E szervezetek abból a téves feltevésből indulnak ki, hogy a fogyasztók mindegyike megvette volna az eredeti terméket is, ezért képviselik azt, hogy a már eladott hamisított áruk után közvetlenül kár is keletkezett. E feltételezés azonban meglehetősen egyoldalú, és nem számol a ténnyel, hogy a márkás áruk vásárlása akkor sem szükségszerű, ha épp azok hamisítványa nincs a piacon. Az egész problémakör legkifogásolhatóbb megoldása pedig az, amikor az említett szakértő a szakvéleménnyel együtt terjeszti elő a polgári jogi igényt.[18]

Elkövetési értékek

A rendelkezésre álló büntetőügyek aktáiból 103-ban az egy védjegyjogosult vonatkozásában megvalósult áru hamis megjelölése nem haladta meg az egy-

17 Vö. Karsai Krisztina – Katona Tibor: i. m.
18 B. 3803.2001 Miskolci Városi Bíróság.

millió forintot.[19] Tíz ügyben egy- és ötmillió forint között volt a hamisított áruk értéke, egy ügyben hatmilliós elkövetési értéket állapított meg a bíróság, egyben pedig harmincmillión felülit. Tizenöt esetben nem állapított meg a bíróság semmifajta elkövetési értéket, öt esetben pedig csak a százezer forint meghaladásának tényét tartalmazta az ítélet. A kimaradó további tizenöt esetben a megindított büntetőeljárásban a szabálysértés elbírálása történt meg, mivel az adott áru értéke nem haladta meg a százezer forintot.

Bűncselekményi értékhatár átlépése

Öt olyan ügy volt, amelyben – helytelenül – a különböző védjegyjogosultak sérelmére elkövetett cselekményekben szereplő áruk értékét összesítették, és így állapították meg a bűncselekményi értékhatár átlépését.

Volt olyan ügy is, amelyben a bíróság csakis a szabálysértési értékhatár meghaladását vizsgálta meg, a továbbiakban nem terjeszkedett ki az áru értékének meghatározására. E „jelenség" egy kevéssé tárgyalt kérdés közelebbi megvizsgálását indokolta, méghozzá azt, hogy vajon helyesen járt-e el a bíróság, amikor nem állapította meg a pontos „elkövetési értéket", illetve hogy egyáltalán milyen jelentőségű lehet az érték e bűncselekmény megítélésénél.

A bűncselekményi értékhatár kérdése a Btk.-ban

A Btk. különös része számos olyan bűncselekményt tartalmaz, amelyek minősítése az elkövetés szempontjából releváns, pénzben is kifejezhető összeghez kötődik, így az elkövetési tárgy értékéhez, az okozott kárhoz, illetve vagyoni hátrányhoz, adóbevétel (vámbevétel) csökkenéséhez (Btk. 138/A §). Ilyen esetben az anyagi jogi jogszabály szerinti összeghatárok döntőek a felelősség megállapításakor, amelyeknek a büntetőeljárásban bizonyított tényként kell megjelenniük. A bűncselekményi értékhatár átlépése (akár van szabálysértési alakzat, akár nincs) felelősséget megalapozó tény, ezért ezt is kétséget kizáróan bizonyítani kell. A Legfelsőbb Bíróság 56. BKv (BK 154.) értelmében, ha a minősítés függ az értékhatártól, enyhítő körülmény, ha a kár, az érték vagy a vagyoni hátrány az alsó határ, súlyosító, ha a felső határ közelében van.

19 A vagyoni hátrány, kár stb. megállapítását tartalmazó ügyeket e helyütt úgy tekintettem, mintha az eljáró hatóságok helyesen az adott áru értékét állapították volna meg.

A bűncselekményi értékhatárral bíró bűncselekmények közül három esetében nem találunk további minősítést az érték alapján, így a jogosulatlan gazdasági előny megszerzésénél (Btk. 288. §); a rossz minőségű termék forgalomba hozatalánál (Btk. 292-294. §); és az áru hamis megjelölésénél (Btk. 296. §). Ezen esetekben, mivel a bűncselekményi értékhatárt meghaladóan nincs olyan további érték, amely a felelősséget fokozná, s amihez hasonlítani lehetne a konkrét elkövetési értéket (hamis vagy rossz minőségű áru értéke, illetve a támogatás vagy gazdasági előny mértéke), az LB említett véleménye nem ad iránymutatást.

Felvetődik a kérdés, hogy e bűncselekmények esetében, s különösen a most vizsgált áru hamis megjelölése esetében a bűncselekményi értékhatárt meghaladó összegű elkövetés esetén „általános" súlyosító körülményként megjelenhet-e valamely magasabb értékhatár átlépése, s ezzel összefüggésben, hogy a büntetőeljárásban meg kell-e határozni a pontos értéket. Az itt képviselt álláspont szerint mindenképpen foglalkoznia kell a bíróságnak az érték meghatározásával, nem elegendő a bűncselekményi értékhatár, azaz a hatályos törvény szerinti százezer forintos határ átlépésének megállapítása. A bűncselekménnyel védeni kívánt jogtárgyra figyelemmel mindenképpen van annak jelentősége, hogy mekkora összegben hamisították a jogosult áruját, hiszen ettől függ a bűncselekmény elkövetőjének potenciális haszna.

Megállapítható továbbá, hogy a bűncselekményi értékhatár átlépésének vizsgálata is az összegszerűség megállapításával történik, ezért nem tekinthető megalapozott releváns ténymegállapításnak – a konkrét ügyekben –, ha a bíró csupán azt a tényt rögzíti, miszerint a bűncselekményi értékhatárt meghaladta a hamis áru értéke.

Az ilyen bűncselekmények vonatkozásában lényegében a bűncselekményi értékhatár átlépése után nincs felső határ, az adott büntetési tételkereten belül kell értékelni azt is, ha épp 150 ezer forintnyi hamis árura, de azt is, ha harmincmilliónyira követik el az áru hamis megjelölését. Emiatt indokolt az értéket súlyosító körülményként figyelembe venni, amennyiben az áru értéke jóval meghaladja az bűncselekményi értékhatárt. Tekintettel arra, hogy sem irányadó gyakorlat, sem összehasonlítható Btk.-beli megoldás nem található, az *argumentum a simile* alapján a Btk. fogalomrendszerével tanácsos dolgozni, így a nagyobb vagy a jelentős érték közül választani. Az általunk megvizsgált ügyek alapján megállapítható, hogy azok nagy részében (77%) egy-egy védjegyjogosultat érintően általában nem haladta meg az egy-egy millió forintot a hamisított áruk értéke. A Btk. szerinti értékhatárokra vetítve

ez azt jelenti, hogy kisebb és nagyobb értékre történt áru hamis megjelölése volt a leggyakoribb a vizsgált ügyekben (88%).

Mindezek alapján úgy vélem, megfelelően megalapozottnak tűnik a nagyobb értéket meghaladó elkövetési érték figyelembevétele: a hatályos joghelyzetben súlyosító körülményként, illetve de lege ferenda minősítő körülményként.

Az itt vizsgált bűncselekmény körében – ahogy említettem – az értékhatár nem tényállási elem, hanem büntethetőségi feltétel. Így tehát az adott áru értéke nem jelenik meg a tényállásban, ellentétben például a lopással vagy más vagyon elleni bűncselekménnyel, aminek az is következménye, hogy az elkövető tudatának nem kell átfognia e tényt.[20] Ha azonban a minősített tényállás része lesz valamekkora érték, akkor ez azt jelenti, hogy az elkövetőnek legalább eshetőleges szándékkal kell majd eljárnia a hamisított áruk értékére vonatkozóan, különben a minősítő körülményt képező érték (az elkövetési tárgy értéke) nem lesz a terhére írható. A jogalkotó megteheti azt is, hogy az alapeseti tényállásban is rögzíti a százezer forintos (vagy bármekkora) elkövetési értéket, ebben az esetben a felelősség enyhébb fokú szűkítéséről van szó, hiszen az elkövetőnek ismernie kell a hamisítványok értékét. Ezt is járható útnak tekintem, mivel a jelen tényállás minden elkövetési magatartása feltételez valamifajta tényismeretet az áru értékével kapcsolatosan: az előállító tisztában van vele, hogy mekkora költséggel járt az előállítás, a forgalmazó pedig azt bizonyosan tudja, hogy mennyiért fogja árulni, ez pedig jó indícium lehet az áru értékére nézve. Ha azonban megelégedne a minősítő körülmény beiktatásával, akkor a vagyoni bűncselekményekhez hasonló rendszert alkalmazna.

Szakértői tevékenység a vizsgált ügyekben

Kérdések a szakértőnek

Az áru hamis megjelölése bűncselekménye miatti büntetőeljárásokban a hatóság már a nyomozati szakban kirendeli a szakértőt vagy a szaktanácsadót[21], akinek tipikusan a következő kérdésekre kell választ adnia:

20 Annyit azért érdemes e helyütt megjegyezni, hogy a jelenlegi bírói gyakorlatban az értékben való tévedésre nem lehet hivatkozni például a lopásnál, lényegében az idegen dolog elkövetési értéke függetlennek tűnik a tényállástól, annak ellenére, hogy tényállási elem. Amennyiben azonban bizonyítható, hogy a tettes szándéka a ténylegesen elvett (elvenni kísérelt) dolog értékét meghaladó értékű dolog elvételére irányult, megállapítják a lopás valamely súlyosabb esetének kísérletét. Ez nem felel meg maradéktalanul a tényállási szerkezetnek.

21 Itt csak megemlítem, hogy csupán szaktanácsadó véleményére alapozni az értékmeghatározást nem lehet. A Legfelsőbb Bíróságnak a BH 2008/326. számú eseti döntésében ki is kellett mondania, hogy

– van-e hamis külső, csomagolás, megjelölés, elnevezés;
– hiányzik-e a versenytárs beleegyezése;
– mekkora az áru értéke.

Ezek azok a rendszerinti kérdések, amelyeket a legtöbb hatóság feltesz a szakértőnek (szaktanácsadónak). A szakértői véleményeknek tartalma azonban jelentősen eltér ettől a tartalmi követelménytől, legtöbb esetben – a Be.-nek megfelelően – konkrét kérdésre válaszolva ugyan, de olyan válaszokat adnak, amelyek sem szakmai, sem jogi szempontból nem elfogadhatók. Több esetben (lásd például áru értéke) a büntetőjogi felelősségre közvetlenül kiható megállapításokat tesznek, illetve jogkérdésben nyilatkoznak.[22] A jogi lehetőség, miszerint a bíró mérlegelheti a szakvélemény elfogadását, elméletileg alkalmas a szakvélemény deficitjének kiküszöbölésére, sok vizsgált ügyben azonban – amikor pedig szükség lett volna rá – a bíróság nem élt a szakvélemény kizárási lehetőségével. Ennek pedig az ügyek egy részében, megítélésem szerint közvetlen negatív hatása volt a felelősség megállapítására.

Az áru *minőségével* kapcsolatos kérdések és szakértői válaszok akkor helytállók, ha az eljáró bíróság a rossz minőségű termék forgalomba hozatalával kapcsolatos elhatárolás (esetleges halmazat) megállapítása szempontjából kíváncsi erre. Meglepő tény azonban, hogy bár az akták 99 százalékában volt szakértői bizonyítás, amelyek jelentős részében a gyenge minőségű hamisítványokra történő elkövetést mutatták ki, a bíróság ez után nem foglalkozott a gyenge (rossz) minőséggel kapcsolatos esetleges további tényállásszerűséggel.

Az áru *értékére* vonatkozó rendkívül helytelen szakértői gyakorlatra már korábban kitértem, e helyütt azt a további – véleményem szerint – jogsértő gyakorlatot tartom érdemesnek felvetni, miszerint a legtöbb esetben a *sértett* (vagy érdekeiket képviselő szervezet) kirendelésére kerül sor szakvélemény vagy szaktanácsadói vélemény megadása céljából. A büntetőeljárás szempontjából lényeges szakmai objektivitás megkérdőjelezhető mind az adott védjegyjogosult hazai képviseletének véleményével (például Nike, Adidas, Puma stb.), mind azon társadalmi szervezetek véleményével kapcsolatosan,

„a szaktanácsadó véleménye nem bizonyítási eszköz; az a Be. 76. §-a (1) bekezdése szerinti felsorolásban nem szerepel. Szaktanácsadó csak a Be. 182. § (1) és (2) bekezdésében meghatározott okból – vagyis bizonyítási eszközök felkutatásához, összegyűjtéséhez, rögzítéséhez stb. – vehető igénybe. Szaktanácsadói vélemény alapján tehát tény bizonyítottnak nem tekinthető."

22 Csak néhány, kirívó példa: „a vádlott védjegybitorlást követett el", „a vádlott tisztességtelen magatartást tanúsított", „a vádlott megvalósította a tényállási elemeket", „a vádlott nyolcrendbeli bűncselekményt követett el".

amelyek tagjai maguk a védjegyjogosultak vagy a márkás árukat forgalmazó cégek (Márkavédők Egyesülete). E kérdéskörhöz tartozik az a meglehetősen aggályos gyakorlat is, hogy a szakértőként benyújtott véleményekben terjesztik elő a polgári jogi igényt.[23] E szervezetek egyébként fontos szerepet töltenek be a hamisítás elleni küzdelemben, de nem engedhető a szakértőkénti részvételük, amennyiben érintettek az adott „hamisítási ügyben" (például a Puma hazai képviseletének véleménye a „Pumo" cipők miatt folyt büntetőeljárásban).[24]

Néhány esetben a szakértő nem foglal egyértelműen állást abban a kérdésben, hogy akkor mennyi is az áru értéke. Abban az ügyben például, amelyben 47 db hamis „Nike" jellel ellátott melegítőt és 12 széldzsekit foglalt le a hatóság, a szakértő megállapította, hogy a lefoglalt áruk értéke (darabonként) ötezer és tízezer forint közé tehető, ennél közelebbit azonban nem fogalmazott meg. E bizonytalanságon a hatóságok túlléptek, s míg a vád „295-590.000 forint értékben", az ítélet „295.000.- valamint 590.000.- forint értékben" kitételt tartalmazta.[25] Véleményem szerint az ilyenfajta értékmeghatározás teljességgel nélkülözi a törvényes alapot, és súlyos szakmai hanyagságot is implikál – még akkor is, ha a konkrét ügyben a vádlott büntetőjogi felelősségét a kérdés nem befolyásolta.

Hamisítvány-e?

A lefoglalt áruval kapcsolatosan mindig megjelenik a kérdés, hogy vajon hamisítvány-e, azaz a hatóságok kifejezetten erre kérdeznek rá. Ami persze teljesen inadekvát kérdésfeltevés. Ahogy azt korábban már kifejtettem, a hamisítás ténye nem közvetlenül mérvadó a tényállás szempontjából.

Emiatt az ilyen kérdésfeltevés meglehetősen elnagyolt, hiszen lényegében a kérdéses áru külseje, csomagolása, megjelölése vagy elnevezése vonatkozásában az összetéveszthetőség lehetősége a lényegi kérdés, az, hogy hamisítvány-e, önmagában nem lenne elég. Fenntartva a korábban, az összetéveszthetőség tárgyában tett megállapításokat, itt szükséges tehát hozzátenni, hogy a szakértő valóban meg tudja állapítani, hogy hamis-e az adott jellegzetes tulajdonságjelölés. Ezzel azonban az összetéveszthetőség kérdése még nyitott maradt. Véleményem szerint azonban ez nem szakkérdés, ezt az átlagos fogyasztó szemszögéből kell megállapítania a bíróságnak, méghozzá

23 B.3803.2001 Miskolci Városi Bíróság.
24 16.B.206.1999 Pesti Központi Kerületi Bíróság.
25 B.0141.2001 Miskolci Városi Bíróság.

azon fogyasztók szemszögéből, akik tipikusan az adott piaci környezetben „fogyasztanak", átlagos iskolázottsággal és élettapasztalattal bírnak. Az átlagos fogyasztó kategóriája ugyanis jogi-büntetőjogi kategória, emiatt szakkérdés hiányában az összetéveszthetőség tényére (lásd korábban: relatív és abszolút összetéveszthetőség) a szakértői vizsgálat nem terjedhet ki.

Meglepő – és elfogadhatatlan – argumentációt alkalmaz a szakértő, amikor kizárja a hamisítás tényét azért, mert *„az ismert mesefigurát pusztán dekorációs céllal helyez el egy terméken a gyártó […], nincs eredeti Kitty cicás vagy Donald kacsás pénztárca, amit hamisítani lehetne"*.

Szakvélemények kritikája

A bíróságnak a szakvéleményt kritikusan kell szemlélnie, a szabad mérlegelése körében eldöntheti, hogy elfogadja-e azt bizonyítéknak. A megvizsgált ügyekben tipikusnak mondható, hogy akár a nyomozás során, akár a bírósági eljárásban kirendelt szakértő véleményét minden további nélkül elfogadta a bíróság, még akkor is, ha annak tartalma meglehetősen kétséges vagy éppen jogi szempontból elfogadhatatlan következtetést is tartalmazott. Fontos azonban e képet annyiban relativizálni, hogy az ügyek másik részében viszont az alkalmatlan szakvélemény elutasítása is előfordult. Tekintettel arra, hogy ezekben az ügyekben eléggé behatárolt a szakértői kör, a szakvélemény el nem fogadása jogi-szakmai szempontok alapján közvetíthet olyan minőségi kontrollt az érintett szakértői szervezetek számára, ami a munkájuk színvonalának emelését, illetve az el nem fogadott szakvélemények számának csökkenését idézheti elő.

Említésre különösen érdemesnek tartjuk a Baranya Megyei Bíróság másodfokú határozatának indokolását[26], amellyel a Márkavédők Egyesületének szakvéleményét zárta ki a bizonyítékok köréből: *„[m]ellőzi a másodfokú bíróság a tényállás azon megállapítását, miszerint a vádlott a hamisítványok forgalomba hozatalával az engedéllyel rendelkező versenytársaknak 132.000.- forint kárt okozott. Nem merült fel adat arra az eljárás során, hogy a vásárlók az eredeti termékeket megvásárolták volna. Ráadásul az eladási ára semmiképpen sem azonos mértékű a hamis márkajelzésű termékeknek az eredeti termékekével. A kár sem lehet azonos az eredeti NIKE termékek eladási árával."*

26 B.300.2005 Baranya Megyei Bíróság.

Volt olyan ügy[27], amelyben a tárgyaláson is sor került szakértő kirendelésére, de a nyomozáskor kirendelt szakértő véleményével szemben fennálló ellentmondásokat nem tisztázták, és a nyomozati eljárásban kirendelt szakértőt nem is idézték a tárgyalásra, hogy megállapítsák az ellentmondás okát.

A jogi tárgy keresése

A hazai vélemények megoszlanak a tényállás jogi tárgyát illetően. *Varga* véleménye szerint[28] mind a versenytársak védelmét, mind pedig a fogyasztók védelmét is ellátja a tényállás. A szerző eme állásfoglalása feltehetően mechanikus jogértelmezésre vezethető vissza, ami a rendszerváltozás előtti időszak tényállása esetében még igaz is lehetett, de a modern piaci viszonyok között aligha. Másfelől pedig erősíthette ezt a hamis képet az is, hogy a BH-kban közzétett, egyébként kevés számú ilyen ügyben a Legfelsőbb Bíróság kritikai hozzáállás nélkül elismételte e tételt (BH, 1998/522). Ezen kívül az a vélemény is megjelenik, hogy a törvényi tényállásból közvetlenül nem érvényesül a fogyasztói érdekvédelem, hanem csak a versenytársak védelmén keresztül.[29] Tóth Mihály szerint viszont a közérdek védelme is megvalósul a fogyasztói érdekek védelmén keresztül.[30] Megemlíthető még az a nézet is, miszerint a fogyasztók érdekeinek védelme nem önálló jogi tárgy[31], amihez jómagam is csatlakozom a következők miatt.

A rendszerváltozás előtti jog- és társadalmi rendben nem lehetett a versenytársak érdekeit büntetőjogi védelem alá vonni (mivel verseny sem volt), szükség volt egy objektív, az állampolgárok érdekeihez jobban közelítő s „védelemre szoruló" érdekre: a termék „versenytárs" általi forgalomba hozatala, ha nem megfelelő jelzéssel látták el azt, egyfajta minőségbeli hibát jelentett. Ez arra utal, hogy a megfelelő jelzés használata adott minőségi standardok betartását is jelentette, így a jelzés egyben a termék minőségi megfelelőségét is hordozta. Amennyiben viszont a megfelelő jelzés hiányzott, a minőségi követelménynek való megfelelőség sem volt feltételezhető,

27 17.B.176/2006 Pécsi Városi Bíróság.

28 Varga Zoltán: A gazdasági bűncselekmények. In: Jakucs Tamás (szerk.): A büntető törvénykönyv magyarázata. KJK-Kerszöv, Budapest, 2004, 1074. o.

29 Uo.; Belovics Ervin – Molnár Gábor – Sinku Pál: Büntetőjog. Különös Rész. HVG-ORAC Kiadó, Budapest, 2005, 468. o.

30 Tóth Mihály: i. m. 167. o.

31 Hollán Miklós – Kis Norbert: A magyar büntetőjog tankönyve II. Különös Rész. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2008, 1116. o.

amiből pedig az következik, hogy a termék forgalmazása alkalmas volt a fogyasztók érdekeinek a sértésére is. A versenytörvény (és a piacgazdaságra való áttérés) által teremtett helyzetben a Btk.-módosítás ezt a vonalat nem engedte el, de tágabb kontextusban jelenik meg az elkövetési tárgy: az összetéveszthető külső jegyekkel bíró árut teszi elkövetési tárggyá, amiből az következik, hogy a fogyasztókkal kapcsolatos védendő jogi tárgy nem lehet más, mint a fogyasztói döntések befolyásmentessége. Az összetéveszthető külső jegyek ugyanis alkalmassá teszik az árut arra, hogy a fogyasztóban téves feltevést (miszerint az áru bír az eredetire jellemző és a fogyasztó által ismert tulajdonságaival) alakítson ki, s így lényegében szándéka ellenére vásárol nem eredeti árut. Ez a jogtárgyfelfogás központi elemének tehát a téves feltevés kialakítását (vagy e lehetőséget) és abból fakadóan a fogyasztó és a vele szemben egyfajta „hatalmi" pozícióban lévő kereskedő (termelő stb.) közötti bizalmi viszony megtörését teszi.

A fogyasztói érdekeket a tényállás sem célkitűzésében, sem pedig gyakorlatában nem védelmezi. De az is megállapítható, hogy *végső soron* a védett jogosultságok (szerzői jogi, iparjogvédelmi) kedvezményezettjeit sem védelmezi (vertikális védelem hiánya), mivel a fogyasztó mások jogsértő cselekményét támogató magatartása ellen nem nyújt védelmet, azaz a fogyasztók általi keresletet (a hamisítványok iránt) nem szorítja vissza. A fogyasztók védelme mint jogi tárgy ebben a kontextusban tehát éppen azért nem jelenik meg, mivel itt a kereskedő és a fogyasztó közötti bizalmi viszony megtörése, a bizalmi viszony híján, fel sem merül. Mind a vásárló, mind az eladó pontosan tudja, hogy amit elad, az nem az adott – másik – cégnek a terméke, az áru csupán annak *szimbolikus javait*[32] birtokolja. Nem védelmezhető az a fogyasztó e tényállással, aki a szimbolikus javak megszerzése érdekében lényegében *„konspirál"* a bűncselekmény elkövetőjével. E tényállást azonban – véleményem szerint – nem lehet leszűkíteni, hogy csak azok részesüljenek védelemben, akiknél a téves felismerés kialakítása történik meg, azaz azok a fogyasztók, akik eredetiként (nem hamisítottként stb.) vették meg az árut. Erre azonban nincs is szükség, ugyanis, álláspontom szerint, ha végre elszakadunk attól az örökségtől, hogy e tényállás a fogyasztókat is védelmezi, ilyen esetben – a tényállás körülményeitől függően – csalás vagy fogyasztó meg-

32 A szimbolikus javak fogyasztása, vagy másképpen a szimbolikus fogyasztás tömören azt jelenti, hogy „az vagy, amit birtokolsz". Vö. Russel Belk: Studies in the New Consumer Behaviour. In: Daniel Miller (ed.): Acknowledging consumption. Routledge, New York, 1996, pp. 58–95. Erről bővebben Karsai Krisztina – Prónay Szabolcs: Javak szimbolikus fogyasztása társadalomtudományi megközelítésben. Kézirat, 2010. Megjelenés alatt.

tévesztése bűncselekményének halmazatban történő megállapításának lehetne helye, mivel e tényállásban a fogyasztói érdekek valóban védelmezett jogi tárgyként jelentkeznek.

Mindezek alapján a tényállás csak horizontálisan, a versenytársak vonatkozásában adja meg a szükséges védelmet. A kérdés csupán az, hogy ez volt-e a jogalkotó szándéka, azaz az, hogy a hamisítás piacát keresleti oldalon nem kívánta korlátozni.

Az e helyütt (is) alkalmazott jogtárgyharmonikus értelmezés[33] módszerével kettős eredményre juthatunk: egyfelől azt kell megállapítani, hogy a tényállás – elemei, jelen értelmezése és alkalmazása alapján – nem védi a fogyasztók érdekeit, a deklarált jogi tárgy nincs összhangban a törvényi tényállással (értelmezési eredmények harmadik változat, lásd korábban). A szimbolikus fogyasztás mint társadalmi jelenség figyelembevétele pedig azt az eredményt hozza, hogy a tényállás nem irányulhat a fogyasztók ellen.

Kétségtelen, hogy a fogyasztókat nem feltétlenül a büntetőjog eszközeivel kell megtanítani arra, hogy hamisítványt vásárolni több szempontból sem érdemes, de a szimbolikus fogyasztás jelenségét és jelentőségét sem szabad lebecsülni. Utóbbi azért lényeges, mert elképzelhető, hogy a jogalkotó éppen az elismert társadalmi jelenség mivolta okán nem teszi jogtárggyá. Ettől még azonban a márkajogosultak érdekeinek sértése és a tényállást megvalósító személyek cselekményének támogatása továbbra is virulni fog. Legalábbis a világ e tájékán.

A bűncselekmény tárgyi súlya

A bűncselekmény tárgyi súlya jelentős, hiszen bűntettként kategorizálta a jogalkotó, és háromévi szabadságvesztéssel rendeli büntetni. De vajon mit jelent ez? Mekkora a bűncselekmény tárgyi súlya? Egyfelől a jogtárgyak sértése szempontjából megadható egyfajta „abszolút" tárgyi súly, azaz amennyiben meg tudjuk ragadni, hogy az adott bűncselekmény a védendő társadalmi érdek érvényesülését hogyan befolyásolja, meghatározhatjuk például, hogy a bűncselekmény az érdekek és értékek (konkrét vagy általános) érvényesülésének kizárásával tipikusan jelentős tárgyi súlyt fog képviselni (emberölés). Ez természetesen az adott jogtárgy társadalmi fontosságától is függ, a rang-

33 Nagy Ferenc: i. m. 71–74., 103–104. o.; Pokol Béla: A jogellenesség és a jogi tárgy mint a büntetőjogi dogmatika kategóriái. Jogelméleti Szemle, 2008/4.; Szomora Zsolt: A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés. Bűnügyi Szemle, 2009/2., 11. o.

sor elején álló jogi tárgyak esetében – tipikusan – már a veszélyeztetés is jelentős tárgyi súllyal bír. Másfelől megjelenhet a bűncselekmények „relatív" tárgyi súlya is mint orientációs alap, ami nem független a jogalkotó által meghatározott büntetési tételektől (így a szankciók arányosságának kérdésétől), ugyanis – véleményem szerint – egy bűncselekmény „relatív" tárgyi súlyát azzal a módszerrel tudjuk „megmérni", ha ugyanilyen büntetési tételű bűncselekményekkel (bűntettek) egy csoportba helyezzük, s végignézzük, hogy a jogalkotó mely jogtárgyak sértését ítélte hasonló súlyúnak.

Az áru hamis megjelölése bűncselekmény e módszerrel egy társaságba kerül[34] – egyebek között – a magzatelhajtás alapesetével [Btk. 169. § (1) bek.]; a súlyos testi sértés alapesetével [Btk. 170. § (2) bek.]; a kényszerítéssel (Btk. 174. §); a személyi szabadság megsértése alapesetével [Btk. 175. § (1) bek.]; az emberkereskedelem alapesetével [Btk. 175/B. § (1) bek.]; a minősített magánlaksértéssel [Btk. 176. § (2) bek.]; a közúti veszélyeztetéssel (Btk. 186. §); a tiltott pornográf felvétellel visszaélés alapesetével [Btk. 204. § (1) bek.]; a kitartottsággal (Btk. 206. §); a hivatali visszaéléssel (Btk. 225. §); a hivatalos személy elleni erőszak alapesetével [Btk. 229. § (1) bek.]; a hamis vád alapesetével [Btk. 233. § (1) bek.]; a minősített bűnpártolással [Btk. 244. § (2) bek.]; az aktív hivatali vesztegetés alapesetével [Btk. 253. § (1) bek.]; a minősített garázdasággal [Btk. 271. § (2) bek.]; a közokirat-hamisítás alapesetével [Btk. 274. § (1) bek.]; a természetkárosítás alapesetével [Btk. 281. § (1) bek.]; a rossz minőségű termék forgalomba hozatalával (Btk. 292. §); a piramisjáték szervezésével (Btk. 299/C §); a minősített adócsalással [Btk. 310. § (2) bek.]; és a lopás, csalás, sikkasztás megfelelő minősített esetével.

Az itt vizsgált bűncselekménynek jelentősebb a tárgyi súlya, mint a fogyasztó megtévesztésének, a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének, illetve az iparjogvédelmi jogok megsértésének, mivel ezek a bűncselekmények vétségek, és alapesetben két évig terjedő szabadságvesztéssel büntetendők. Hasonló tárgyi súllyal a jogalkotó értékelésében a minősített esetek (jelentős vagyoni hátrány okozása, illetve üzletszerűség esetén) bírnak.

Véleményem szerint annak a jogalkotói döntésnek, amelynek következtében ez a bűncselekmény az említett bűncselekményekkel azonos tárgyi súlyú, a büntetőeljárásokban is meg kellene jelennie. Nyilvánvalóan nem vezethet helyes következményre a mechanikus összehasonlítás, s minden egyes

34 A Btk. 2010. április 1-jei állapota szerint.

ügy értelemszerűen más-más körülményeket tartalmaz, de önmagában a tény, hogy e jelentős tárgyi súlyú bűncselekmény miatt kiszabott szankciók *korántsem tekinthetők súlyosnak*[35], a jogalkotói és a jogalkalmazói értékelés közötti diszkrepanciát bizonyítja. A felsorolt bűncselekmények esetén csak valóban „különleges" esetekben alkalmazzák az enyhítő szakaszt és szabnak ki pénzbüntetést. Mindezek alapján, álláspontom szerint, a jogalkotó számára két lehetőség adódik: vagy elfogadja a szimbolikus fogyasztás tolerálását jelentő jelenlegi tényállást, akkor azonban a büntetési tételt csökkenteni kell, hogy a bűncselekmény tárgyi súlya is közvetítse a jogalkotói értékítéletet. Vagy pedig ezt el nem fogadva olyan lépést tesz, amely megváltoztathatja az enyhe ítélkezési gyakorlatot: felemeli a bűncselekmény büntetési tételét. A jogalkalmazás az enyhe ítélkezési gyakorlatot – talán – könnyebben szigoríthatná, ha a bírák elkezdenének súlyosabb büntetéseket kiszabni.

Szimbolikus fogyasztás a büntetőeljárásban

A bűncselekmény elkövetésére – úgy tűnik – jelentős társadalmi igény van, és ennek a jelenségnek a lenyomata a büntetőeljárásokban is megjelenik, méghozzá a terhelti védekezések körében. Az elkövetők egy részének az erkölcsi elvetendőség hiánya eleve adott: szinte minden ügyben a „láttam a piacon, hogy van erre kereslet, én is megpróbáltam" típusú védekezésekkel találkoztunk.

A hamisítványok olcsóságára és arra a tényre, hogy az áruk hamisított voltát ismerik a vásárlók, a legtöbb vádlott hivatkozott a jegyzőkönyvek szerint.

A hamisítás, illetve a hamisított áruk kereskedelmének tilalmával kapcsolatos tévedésre hivatkozás tipikusan úgy jelentkezik, hogy a cselekmény büntetlenségére (jogszerűségére) a számlával történt „nagykereskedelmi" beszerzés tényéből következtettek: „legálisan vásároltam különböző outletekben", „számlával vettem, azt hittem, jó termékek", „katalógusból rendeltem Törökországból".

A konkrét márka védettségével kapcsolatban is jelentős számban jelenik meg a tévedésre hivatkozás, az elkövetők tehát nem állítják, hogy nem tudtak a cselekmény büntetendőségéről, azt próbálják meg azonban érvényesíte-

35 Az áru hamis megjelölése analízisében a szankciókra vonatkozó eredmények közlésére másutt kerül sor, jelen kutatási keresztmetszethez azonban mindenképpen szükség van a következők megemlítésére: a megvizsgált ügyek 65 százalékában pénzbüntetést szabott ki a bíróság (átlagosan kétrendbeli elkövetések), 17 százalékában próbára bocsátást alkalmazott, míg nyolc százalékában felfüggesztett szabadságvesztést szabott ki (más bűncselekményekkel való valódi anyagi halmazat körében). Az esetek tíz százaléka felmentéssel vagy eljárás-megszüntetéssel végződött.

ni, hogy nem ismerték az adott márkát („nem vagyok járatos a márkák világában", „nem tudtam, hogy a KEYO híres márka, az ADIDAS, a PUMA, a NIKE márkákat ismerem", „kereskedő vagyok, nem márkaszakértő", „az eljárás előtt nem ismertem a PUMA márkát").

A ténybeli védekezésként tipikus a nagy tételben vásárlásra és annak megszokott rendjére (miszerint nem nézik meg az összes árut egyenként) hivatkozás, valamint megjelent a „nem tudtam, mit jelentenek a jelzések a ruhán" állítás is.

Az általunk megvizsgált ügyek közül négy felmentés vezethető vissza a vádlotti védekezés sikerére: az egyik esetben a vádlott azt állította, hogy tranzitutasként hozta be Magyarországra a hamisítványokat, azokat át akarta vinni az országon; illetve az átlátszatlan csomagolással ellátott termékeket (nagy tételben) nem látta sem megvásárláskor, sem piacra szállításkor. A harmadik sikeres védekezés az adott márka nem ismeretére vonatkozott, a negyedik pedig az adott márka védettségével kapcsolatos tévedésre *(„a vádlott alaposan következtethetett arra, hogy védjegyoltalom alatt nem álló terméket vásárolt, amelyeket a versenytárs hozzájárulása nélkül szabadon forgalmazhat, figyelemmel a számlára történő vásárlás tényére, a vásárolt farmernadrágok árára, illetve a vásárolt áruk hazai piaci részesedésére [nincs jelen lényegében a Versace farmer] és a Versace termékek hazai bevezetettségére."*[36]*).* Véleményem szerint a tranzitutas felmentése nem volt megalapozott, mivel – még ha a magyar kereskedelmi forgalomba nem kívánta is az árut bevinni – a magyar tényállás megvalósulása szempontjából a külföldön történő forgalomba hozatal célzata is releváns. A másik három felmentés vonatkozásában pedig csupán annyit kívánok megjegyezni, hogy – ahogy láttuk – ezek a védekezések mindennaposak, viszont az összes többi esetben mégsem jártak felmentéssel. Sok büntetőügy aktája nem tartalmaz adatokat a védekezésekben foglaltak vizsgálatára, így azok cáfolata hiányzik. Mivel a vádlott meg nem cáfolt védekezése *(in dubio pro reo)* a felmentés alapjául szolgálhat[37], felvetődik a kérdés, hogy vajon a vizsgált esetekben miért az elítélés mellett döntött a bíróság.

Konklúziók

Az előzőekben bemutatott problémakörök egy teljes vizsgálat eredményeinek önkényes válogatás szerinti bemutatása, úgy vélem, a felvetett témák

36 B.1877.2003 Szegedi Városi Bíróság.

37 Lásd részletesen: Karsai Krisztina – Katona Tibor: i. m.

mindegyike – a konkrét eljárások tapasztalataival megerősítve – a nem megfelelő jogi megoldás veszélyét hordozza magában. Fontos lenne elkerülnünk e veszélyeket, és megóvnunk az „alkalmazott" büntetőjogot a taposóaknák pusztításától, azaz attól, hogy helytelen vagy nem kellően figyelmes jogértelmezés (és jogalkalmazás) a vádlott büntetőjogi felelősségének alapítását vagy fokozását idézze elő. Ennek érdekében e helyütt talán nem haszontalan összefoglalni az áru hamis megjelölése bűncselekményének analízisekor megállapított eredményeket és javaslatokat.

a) A Btk. 296. § szerinti bűncselekménynek a fogyasztók védelme *nem* jogi tárgya, ezt a jogtárgyharmonikus értelmezéssel mutattam ki.

b) Ha az áru hamis megjelölés tényállásába illeszkedő elkövetési tárgy (a hamis áru) ténylegesen rossz minőségű termék, akkor indokolt lehet a valódi halmazat megállapítása a rossz minőségű termék forgalomba hozatalával. Amikor viszont a hamisítvány nagyon gyatra vagy a meghatározott jellegzetes tulajdonságok kivitelezése olyan silány, hogy fel sem merülhet az eredetiség látszata, azaz az összetéveszthetőség nem adott, akkor nincs helye a Btk. 296. § megállapításának. Ilyenkor – az eset körülményeitől függően – felmerülhet a csalás, a rossz minőségű termék forgalomba hozatala, valamint a fogyasztó megtévesztése is.

c) A versenytárs beleegyezésének hiánya mint tényállási elem nem adekvát, azt de lege ferenda javasolt kiejteni a tényállásból.

d) A bűncselekmény tárgyi súlya nem adekvát az ítélkezési gyakorlattal, emiatt változtatás indokolt. A dogmatikai szempontok alapján végső soron mindegy, hogy jogalkotás vagy a jogalkalmazás megváltozása idézi-e ezt elő.

e) De lege lata megalapozottnak tűnik a nagyobb értéket meghaladó elkövetési érték súlyosító körülményként történő figyelembevétele, de lege ferenda azonban minősítő körülményként lenne érdemes szabályozni.

f) Az áru összetéveszthetőségének kérdése nem szakkérdés, arról a bíróságnak kell véleményt alkotnia az átlagos fogyasztó mércéje alapján.

g) A hamisított áru értékét minden esetben meg kell állapítani.

h) A sértett vagy képviselője ne lehessen szakértő/szaktanácsadó, a helytelen gyakorlatot meg kell szüntetni.

i) A hamis áruk keresletével kapcsolatos büntetőjogi fellépés hiánya, azaz a hamis áru fogyasztása iránti közömbösség („tudom, hogy hamisítványt veszek", vagy „eleve hamisítványt akartam venni") generálhatja is a hamis áruk iránti keresletet. Ha pedig ez így van, a büntetőjogi tényállás a jelen értelmezésben (jogtárgyaival együtt) nem alkalmas a védelem ellátására.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp85-103

AMBRUS ISTVÁN – DEÁK ZOLTÁN

Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből

Hazánkban az 1980-as években meginduló, majd az 1990-es években kiteljesedő politikai, társadalmi, gazdasági változások, s ezzel párhuzamosan a technikai fejlődés szinte törvényszerűen magával hozta a hagyományos készpénzes fizetés és a már korábbról ismert készpénz-helyettesítő eszközök (így például csekk, váltó) mellett olyan modern *technikai eszközök* megjelenését a mindennapi pénzforgalmi életben, amelyek alkalmasak a társadalom részéről a pénzforgalomtól mindinkább elvárt *nagyfokú mobilitás* megteremtésére. E szükséglet kielégítését szolgálta a *bankkártyák* megjelenése a magyar pénzpiacon, erre a rendszerváltozás időszakában került sor. Ez után, a bankélet felvirágzásának tulajdoníthatóan is, rohamos fejlődésnek indult, és mind természetesebbé vált a plasztiklapokkal történő fizetés, illetve annak elfogadása: napjainkban – különösen az internet segítségével – gyakorlatilag a világ bármely pontjáról bármilyen termék megrendelhető, feltéve, hogy az ellenérték megfizetéséhez van megfelelő technikai eszközünk, vagyis bankkártyánk.

Csak helyeselhető az a kriminológiai álláspont, amely szerint abban az esetben, ha egy új technikai eszköz bevezetésére kerül sor, ez után – rövidebb-hosszabb idővel – szükségképpen számolni kell azon bűnelkövetők megjelenésével, akik *vissza kívánnak élni* ezzel az eszközzel, és e visszaélésként értékelhető cselekményük – a társadalom védelme érdekében – *büntetőjogi reagálást* igényel a jogalkotó részéről.

Bankkártyával kapcsolatos, társadalomra veszélyes cselekményeket a hazai jogalkotó első ízben az 1994. évi IX. törvény 26–27. §-ai alapján pönalizálta. A vonatkozó tényállások elnevezése ekkoriban bankkártya-hamisítás, illetve a bankkártyával visszaélés volt. Ez után – különös tekintettel az Európai Unió Tanácsának 2001. május 28-án elfogadott, a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló 2001/413/IB számú kerethatározatára – hazánk európai uniós tagságából fakadó kötelezettségének tett eleget a törvényhozó akkor, amikor a nem készpénzes fizetőeszközökkel kapcsolatos Btk.-beli tényállásokat módosította és egységesítette. A 2003. évi II. törvény 25–28. §-ai általánosabb megnevezést vezettek be az említett bűncselekményi tényállásoknál: *készpénz-helyettesítő*

fizetésieszköz-hamisítás és *készpénz-helyettesítő fizetési eszközzel visszaélés* lett a korábban említett két bűncselekmény elnevezése, s részben ezek keretében, részben ezek mellett más, készpénz-helyettesítő fizetési eszközzel kapcsolatos bűncselekményi alakzatok bevezetésére is sor került.[1] Mindezekről a hatályos Btk. 313/B–313/E §-ai rendelkeznek.

E tanulmánynak *nem célja* a bankkártya mellett más, nem készpénzes fizetési eszközökkel (például váltóval) kapcsolatos kérdések vizsgálata. Szintén nem kerül sor a dolgozat keretei között a vonatkozó bűncselekményi tényállások részletes elemzésére. Célunk mindössze a bankkártyával kapcsolatos bűncselekmények körében *néhány alapvető fontosságú, súlyponti dogmatikai kérdés* felvetése, illetve lehetőség szerinti megválaszolása. Mindezt a vonatkozó jogirodalmi és az ítélkezési gyakorlatból származó álláspontok ismertetése, ütköztetése, helyeslése vagy cáfolása útján végeztük el.

A készpénz-helyettesítő fizetésieszköz-hamisítás és a készpénz-helyettesítő fizetési eszközzel visszaélés egység-többségtani problémái

Vitatott kérdés a jogirodalomban, hogy abban az esetben, ha *ugyanazon elkövető, azonos elkövetési tárgy vonatkozásában, több cselekményt megvalósítva* kimeríti mind a Btk. 313/B § (1) bekezdésében foglalt készpénz-helyettesítő fizetésieszköz-hamisítás, mind a Btk. 313/C § (1) bekezdés *a)* pontja szerinti készpénz-helyettesítő fizetési eszközzel visszaélés törvényi tényállását, e két deliktum között *valóságos vagy látszólagos anyagi halmazat megállapításának van-e helye*.[2]

E kérdésben a kommentárirodalom egy része, több jogirodalmi szerző és – mint látni fogjuk – a bírói gyakorlat is a valóságos anyagi halmazat mellett

1 Így a készpénz-helyettesítő fizetési eszközzel visszaélés megszerzéses alakzata [Btk. 313/C § (7) bekezdés] és a készpénz-helyettesítő fizetési eszköz hamisításának elősegítése (Btk. 313/D §). Utóbbihoz lásd A Btk. 313/D § szerinti készpénz-helyettesítő fizetési eszköz hamisításának elősegítése – a büntethetőség túlzott előrehozatalának intő példája című részt.

2 Szintén vizsgálandó, ám jóval kevesebb polémiára okot adó kérdés a jogirodalomban, hogy a készpénz-helyettesítő fizetési eszközzel visszaélés úgynevezett *megszerzéssel megvalósuló alakzata* [Btk. 313/C § (7) bekezdés] milyen viszonyban áll a 313/C § (1) bekezdés szerinti visszaéléssel, illetőleg a 313/B §-ban szabályozott hamisítással. Az általánosan elfogadott álláspont itt az, hogy a megszerzéses alakzat – a látszólagos anyagi halmazati viszonyra tekintettel – háttérbe lép mind a hamisítással, mind a súlyosabb visszaélési alakzattal szemben. Kiemelést igényel, hogy a Legfelsőbb Bíróság egy friss jogegységi határozata (1/2009. BJE) alapján a készpénz-helyettesítő fizetési eszközzel visszaélés ezen alakzatának ítéletbeli megállapítása nagymértékben visszaszorult, e kérdés elemzése azonban nem tárgya e tanulmánynak.

foglal állást. A „kapcsos kommentár" szerzői ennek indokát abban látják, hogy *„a készpénz-helyettesítő fizetési eszköz hamisítás nem szükségszerű eszköz-, illetve előcselekménye a készpénz-helyettesítő fizetési eszközzel visszaélésnek, ezért anyagi halmazatuk mindig valóságos"*.[3] Ugyanezt az álláspontot képviseli *Molnár Gábor,* szerinte *„ha a hamisítást követően külön elkövetői magatartással a készpénz-helyettesítő fizetési eszközzel visszaélésre is sor kerül, valódi anyagi halmazat megállapításának van helye"*.[4]

Más szerzők szerint azonban a két bűncselekmény halmazata látszólagosnak tekinthető, s ilyen esetekben csak a készpénz-helyettesítő fizetési eszközzel visszaélés állapítható meg. Így foglal állást *Varga Zoltán,* indokait azonban nem részletezi.[5]

A *Hollán – Kis* szerzőpáros közelebbről is megjelöli a halmazat mellőzésének okát. Mint írják, *„a készpénz-helyettesítő fizetési eszköz hamisítása, a készpénz-helyettesítő fizetési eszközzel visszaéléshez (Btk. 313/C §) képest látszólagos anyagi halmazatban* – büntetlen eszközcselekményként – *háttérbe szorul, ha a hamis készpénz-helyettesítő fizetési eszköz felhasználásra is kerül" (kiemelés tőlünk. – A szerzők).*[6]

Kereszty Béla a kérdés kapcsán úgy fogalmaz, hogy *„a készpénz-helyettesítő fizetési eszköz hamisítása (Btk. 313/B. §) a tárgyalt bűncselekménynek nem szükségszerű eszköz-, illetve előcselekménye, ám felfogható külön tényállásban rögzített sui generis előkészületi cselekményként is, ezért* kizárt a halmazat, *mivel a készpénz-helyettesítő fizetési eszköz felhasználása* szükségszerűen konszumálja *a hamisítást vagy a hamis fizetési eszköz készítését"*[7] *(kiemelések tőlünk. – A szerzők).*

3 Berkes György (szerk.): Kommentár a gyakorlat számára. 2. kiadás. 29. pótlás. HVG-ORAC Kiadó, Budapest, 2009, 1006/26. o.

4 Molnár Gábor: A gazdasági bűncselekmények. In: Belovics Ervin – Molnár Gábor – Sinku Pál: Büntetőjog. Különös rész. HVG-ORAC Kiadó, Budapest, 2008, 669. o.

5 Varga Zoltán: A gazdasági bűncselekmények. In: Varga Zoltán (szerk.): A büntető törvénykönyv magyarázata 2. Complex Kiadó, Budapest, 2009, 1337. o.

6 Hollán Miklós – Kis Norbert: A magyar büntetőjog tankönyve II. Különös rész. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2008, 690. o.

7 Kereszty Béla: A gazdasági bűncselekmények. In: Nagy Ferenc (szerk.): A magyar büntetőjog különös része. Korona Kiadó, Budapest, 2005, 732. o. Röviden rá kell még mutatnunk a Kereszty-féle álláspont *terminológiai pontatlanságára:* a konszumpció, lévén hogy az nem a látszólagos anyagi, hanem a látszólagos *alaki* halmazat egyik kategóriája (tehát az az eset, amikor az elkövető egyetlen cselekménye valósít meg látszólagos több bűncselekményt) ez esetben nem foroghat fenn, mivel itt *két, elkülönülő cselekmény* (tudniillik a hamisítás és az attól térben és időben többnyire elkülönülő felhasználás) az, amelyek kapcsán az egység és a halmazat kérdésében dönteni kell. Ebből következik, hogy akár valóságos, akár látszólagos halmazatot állapítunk meg végül, az nem alaki, hanem anyagi halmazat lesz, ahol viszont nem konszumpcióról, hanem például összeolvadásról szólhatunk.

Az első álláspontot elfogadó szerzők tehát, azon oknál fogva, hogy a hamisítás nem szükségképpeni eszközcselekménye a visszaélésnek, valóságos halmazat megállapítását tartják indokoltnak a két említett bűncselekmény találkozása esetén, míg a második felfogást vallók – különféle indokolásokkal – csak látszólagos halmazati viszony fennállását látják.

Az a felfogás, amely *általános jelleggel* valóságos halmazatot lát megállapíthatónak azon esetekben, amikor *két bűncselekmény in abstracto nem szükségképpen, hanem csupán rendszerint jár együtt*, napjaink bírói gyakorlatában gyakran hivatkozott elv, éspedig mind az úgynevezett *eszköz- és célcselekmények*, mind pedig az úgynevezett *elő- és utócselekmények* vonatkozásában. Így a judikatúra valóságos halmazatot állapít meg például az eszközcselekményként jelentkező *magánlaksértés* (Btk. 176. §) és a lakásban elkövetett különböző célbűncselekmények között[8] ugyanúgy, mint például abban az esetben, amikor a bolti eladó részéről a *vásárlók megkárosítását* (Btk. 328. §) *sikkasztás* (Btk. 317. §) követi.[9]

Ismeretesek azonban olyan esetek is, amikor két, együttesen előforduló bűncselekmény között nem forog fenn absztrakt szükségképpeni összefüggés, a bíróság az egyik bűncselekmény önálló megállapítását valamilyen alapon mégis mellőzi. Így például a Legfelsőbb Bíróság 5/2000. büntető jogegységi határozatában arra az álláspontra helyezkedett, hogy a Btk. 276. § szerinti *magánokirat-hamisítás* megállapításának nincs helye, amennyiben az az *intellektuális közokirat-hamisítás* [Btk. 274. § (1) bekezdés *c)* pont] megvalósításához szolgált eszközként.[10]

Témánkhoz szorosabban kapcsolódik az az ítélkezési gyakorlatban régtől érvényesülő felfogás[11], amely alapján nincs helye halmazat megállapításának a *pénzhamisítás* [Btk. 304. § (1) bekezdés *a)* pont] és a forgalomba hozatallal

8 Például BH, 1981/302., BH, 1996/291., BH, 1998/4.

9 BJD, 902., BJD, 2888.

10 Bár a Legfelsőbb Bíróság a hivatkozott BJE indokolásában a halmazat mellőzését azzal indokolta, hogy a magánokirat-hamisítás *szükségszerűen* megvalósul az intellektuális közokirat-hamisítás elkövetésekor, e két bűncselekmény között valójában csak *in concreto*, az elbírált jogesetben meglévő, és *nem in abstracto*, a törvényi tényállások szintjén fennforgó szükségképpeni összefüggés állt fenn, tekintettel arra, hogy az intellektuális közokirat-hamisítás *általánosságban* elkövethető a magánokirat-hamisítás nélkül is. Az in concreto szükségképpeni összefüggés azonban önmagában nem lehet elégséges a halmazat mellőzéséhez, ezért véleményünk szerint a két okirat-hamisítás halmazatának látszólagossága együttes előfordulásuk *in abstracto rendszerinti* (nem szükségszerű, de igen gyakori, jóformán mindennapi) voltával magyarázható. Ehhez lásd Ambrus István: A büntetlen eszköz-, utó- és mellékcselekményekről. Jogelméleti Szemle, 2009/4. http://jesz.ajk.elte.hu/ambrus40.mht

11 Mint Tóth Mihály írja, „a pénzhamisításban testet öltő *csalás* megállapítását a gyakorlat töretlenül kizárja”. Tóth Mihály: Gazdasági bűnözés és bűncselekmények. KJK, Budapest, 2000, 329. o.

[Btk. 304. § (1) bekezdés *c)* pont] megvalósulni látszó *csalás* (Btk. 318. §) esetén.[12]

Az említett bűncselekmények relációjában azonban a halmazat kiküszöbölése nem oly módon történik, hogy a pénz utánzását, illetve meghamisítását a forgalomba hozatallal megvalósuló alakzat, illetve a csalás büntetlen eszközcselekményének tekintjük, hanem épp *fordítva:* önállóan csak a 304. § (1) bekezdés *a)* pontja szerinti bűncselekmény, tehát a pénz utánzásával vagy meghamisításával megvalósuló pénzhamisítás megállapítására kerülhet sor, a csalást *büntetlen utócselekményként* kell értékelni, így az önállóságát veszti.[13] Ennek indoka egyrészt abban a körülményben keresendő, hogy a hamis vagy meghamisított pénz forgalomba hozatalával az elkövető az általában már az utánzáskor, illetve meghamisításkor fennforgó *célzatát realizálja,* amivel a jogalkotó is számolt a pénzhamisítás törvényi tényállásának megalkotásakor. Másrészt a csalás büntetlen utócselekményi jellegét támasztja alá az is, hogy a pénz utánzásával vagy meghamisításával elkövetett pénzhamisítást *in abstracto rendszerint követi* a forgalomba hozatal, s a harmadik személy tévedésbe ejtésével előidézett károkozás. Vélelmezhető tehát, hogy a jogalkotó a pénzhamisítás büntetési tételkeretének meghatározásakor e körülményekre figyelemmel volt, s ennek megfelelően állapította meg a bűncselekmény alapesetére irányadó kettőtől nyolc évig terjedő szabadságvesztést, amelyben a tényleges hamisítás mellett a forgalomba hozatal és a károkozás is kellőképpen értékelhető, ezért a halmazati értékelés ez esetben szükségtelen, és a kétszeres értékelés tilalmába is ütközne.

Laikus szemlélő számára sem tűnik megalapozottnak a *kirajzolódó különbség:* amennyiben az elkövető *a készpénzt magát* hamisítja meg, amelyet ez után forgalomba is hoz, s így mást tévedésbe ejtve kárt okoz: egy bűncselekmény, a 304. § (1) bekezdés *a)* pontjába foglalt pénzhamisítás megállapításának van helye. Ha azonban ugyanezt nem készpénzzel, hanem *készpénz-helyettesítő fizetési eszközzel, például bankkártyával* teszi, az elsőként említett felfogás szerint a készpénz-helyettesítő fizetésieszköz-hamisítás [Btk. 313/B § (1) bekezdés] mellett a felhasználással megvalósuló készpénz-helyettesítő fizetési eszközzel visszaélés [Btk. 313/C § (1) bekezdés *a)* pont] valóságos halmazatban áll. A két eset közötti, törvényi szinten fennálló különbség – amelyet egyébként a halmazati minősítéshez érvként is használnak

12 Vö. BH, 1988/390. és BH, 1999/198.

13 Így Nagy Ferenc: A magyar büntetőjog általános része. HVG-ORAC Kiadó, Budapest, 2008, 239. o. Ellentétesen Földvári József: Az egység és a halmazat határesetei a büntetőjogban. KJK, Budapest, 1962, 229. o.

egyes szerzők – abban áll, hogy a pénz utánzását vagy meghamisítását, illetve a hamis vagy meghamisított pénz forgalomba hozatalát *nem két elkülönülő törvényi tényállásban*, hanem a pénzhamisítás tényállásában, annak két bűncselekményi változataként feltüntetve szabályozza a törvény. Ezzel szemben a készpénz-helyettesítő fizetésieszköz-hamisítás, illetve a készpénz-helyettesítő fizetési eszközzel visszaélés – amely a felhasználást szabályozza – külön tényállásban kapott helyet.[14] Nézetünk szerint jócskán gyengíti ezt az érvet az a körülmény, hogy a pénzhamisítás és a csalás – akárcsak a készpénz-helyettesítő fizetésieszköz-hamisítás és az azzal való visszaélés – külön tényállásban szerepel ugyan, halmazatuk az említett esetben mégis csupán látszólagos.

Részünkről elfogadhatóbbnak tartjuk a második idézett álláspontot: tekintettel arra, hogy

– a készpénz-helyettesítő fizetésieszköz-hamisítás gyakorlatilag a készpénz-helyettesítő fizetési eszközzel visszaélés *sui generis előkészületeként* értékelhető;
– az elkövető a hamis vagy hamisított készpénz-helyettesítő fizetési eszköz felhasználásakor a készpénz-helyettesítő fizetési eszköz hamisításakor fennforgó *célzatát realizálja;*
– a készpénz-helyettesítő fizetésieszköz-hamisítást *rendszerint követi* a felhasználással megvalósuló visszaélés,

a *halmazatot mellőzve* egy bűncselekmény, a készpénz-helyettesítő fizetési eszközzel visszaélés megállapításának van helye. A készpénz-helyettesítő fizetésieszköz-hamisítás tehát – tekintettel a közte és a visszaélés között fennálló *eszköz–cél viszonyra – büntetlen eszközcselekményként* értékelhető, s önálló megállapítása nézetünk szerint mellőzendő.

Szintén a halmazat látszólagos voltát támasztja alá az, hogy

– mind a készpénz-helyettesítő fizetésieszköz-hamisítás, mind az azzal való visszaélés *azonos jogi tárgy elleni támadást* jelent. Ez a körülmény pedig – bár általános érvényű rendezőelvként nem fogadható el az egység és a többség elhatárolásához[15] – jelentős *indíciumnak* tekinthető ahhoz, hogy a halma-

14 Így például Molnár Gábor szerint „a vizsgált bűncselekmények tényállása oly mértékben elkülönül egymástól", hogy az a valóságos halmazat megállapítását teszi szükségessé. Molnár Gábor: Gazdasági bűncselekmények. HVG-ORAC Kiadó, Budapest, 2009, 497. o.

15 Békés Imre „rendezőelvei" kapcsán így Nagy Ferenc: A magyar büntetőjog általános része. Korona Kiadó, Budapest, 2004, 319–320. o.

zat mellőzésével csak az egyik, éspedig a jogi tárgy elleni jelentékenyebb támadásként értékelhető bűncselekmény megállapítására kerüljön sor.

A bírói gyakorlatban – mint arról már volt szó – az elsőként említett álláspont érvényesül, tehát többnyire valóságos anyagi halmazatot állapít meg a bíróság, amennyiben az elkövető például a hamis bankkártya elkészítése után azt utóbb jogtalan haszonszerzés céljából fel is használja. E gyakorlat véleményünk szerint – a kétszeres értékelés tilalmára figyelemmel – kifejezetten *aggályos*. Ennek ellenére a judikatúrában érvényesülő felfogás nem tekinthető megalapozatlannak, s meglátásunk szerint annak kialakítására nem az önkényes jogértelmezés vezetett. Az a körülmény, amely az említett, bankkártyával kapcsolatos bűncselekmények esetén a valóságos halmazatkénti értékelés mellett szólhat, e bűncselekmények *büntetési tételeiben* és a készpénz-helyettesítő fizetési eszközzel visszaélés *minősítési rendszerében*, illetve annak a pénzhamisítás minősítési rendszerétől való *eltérésében* keresendő.

Ha vizsgálatnak vetjük alá a pénzhamisítás (Btk. 304. §) törvényi tényállásának (1)–(3) bekezdését, azt láthatjuk, hogy a kettőtől nyolc évig terjedő szabadságvesztéssel büntethető alapeset megállapításának csak a nagyobb, illetve a jelentős értékre történő elkövetés esetén van helye. Kisebb vagy azt el nem értő értékű pénzre történő elkövetéskor az öt évig terjedő szabadságvesztéssel fenyegetett (3) bekezdés szerinti privilegizált eset állapítható meg, míg a különösen nagy vagy azt meghaladó értékre elkövetett pénzhamisítás a (2) bekezdés szerint minősül, és öttől tíz évig terjedő szabadságvesztéssel büntetendő – ez a pénzhamisítás egyik minősített esete.[16]

A készpénz-helyettesítő fizetési eszközzel visszaélés minősítési rendszere – tekintettel arra, hogy e deliktum a pénzhamisítással ellentétben *materiális bűncselekmény* – a visszaéléssel okozott kár mértékéhez igazodik. Ha minősítő körülmény (üzletszerűség vagy bűnszövetség) nem áll fenn, a nagyobb kárt okozó készpénz-helyettesítő fizetési eszközzel visszaélés [Btk. 313/C § (3) bekezdés *a)* pont] három évig, a jelentős kárt okozó változat [Btk. 313/C § (4) bekezdés *a)* pont] öt évig terjedő szabadságvesztéssel büntetendő, s a pénzhamisítás alapesetére irányadó büntetési tételt – kettőtől nyolc évet – csak a különösen nagy kárt okozó készpénz-helyettesítő fizetési eszközzel visszaélésre [Btk. 313/C § (5) bekezdés *a)* pont] ír elő a törvény.

E rendelkezésekből az következik, hogy amennyiben a pénzhamisítást például 210 ezer forint értékű pénzre követik el, ez a cselekmény a Btk.

16 Az értékhatárokhoz lásd Btk. 138/A §.

304. § (1) bekezdése szerint minősül, és kettőtől nyolc évig terjedő szabadságvesztéssel büntetendő. Ha a készpénz-helyettesítő fizetési eszközzel visszaélés tettese ugyanekkora kárt okoz, büntetése a Btk. 313/C § (3) bekezdés *a)* pontja alapján legfeljebb három évig terjedő szabadságvesztés. Azt láthatjuk tehát, hogy ahhoz, hogy az alapeseti pénzhamisítás elkövetőjével azonos büntetési tételkeretben lehessen kiszabni a bankkártya-hamisító büntetését, utóbbinak ötvenmillió forintot meghaladó kárt kell okoznia cselekményével![17] A hatályos rendelkezések alapján tehát úgy tűnhet, hogy „jobban megéri" bankkártyát hamisítani, mint készpénzt, mert ugyanakkora összeg mellett lényegesen súlyosabb tételkereten belül kell kiszabni a büntetést a pénzhamisítóra, mint a bankkártya-hamisítóra. Álláspontunk szerint a bírói gyakorlat szerinti valóságos halmazatot tehát ennek a *jogalkotási aránytalanságnak a részbeni kiküszöbölése* indokolhatja, mivel ilyenkor lehetőség nyílik *halmazati büntetés* kiszabására, amely adott esetben jobban tükrözheti az elkövetett cselekmények társadalomra veszélyességét, mint az egységkénti értékelés.[18] A pénzhamisítás esetében azonban – tekintettel arra, hogy már az alapeset büntetése is kellőképpen súlyosnak tekinthető – a megfelelő súlyú büntetés kiszabhatósága érdekében a halmazati büntetésre vonatkozó szabályok segítségül hívására nincs szükség, így a tényleges hamisítás utáni forgalomba hozatalt és a tévedésbe ejtéssel elkövetett károkozást büntetlen utócselekménynek lehet tekinteni, és a büntetést az egy bűncselekményre irányadó büntetési tételkereten belül kell kiszabni. Azt a körülményt pedig, hogy az elkövető a pénz utánzásán vagy meghamisításán felül a hamis vagy meghamisított pénzt forgalomba is hozza, adott esetben a büntetéskiszabás körében kell megfelelően – súlyosító körülményként – értékelni.

Nézetünk szerint a judikatúra álláspontja gyakorlati szempontból érthető, elméletileg azonban nem igazolható. A vélt vagy valós *jogalkotási visszásságok* ugyanis – az elkövető terhére – nem oldhatók fel a jogalkalmazás síkján, különösképp büntetőjogi alapelvek, így a *kétszeres értékelés tilalmának megsértése* árán.[19] Mindezekre tekintettel a valóságos halmazat megállapítását a készpénz-helyettesítő fizetési eszközzel kapcsolatos bűncselekmények vonatkozásában mellőzni indokolt.

17 Vö. Btk. 313/C § (5) bekezdés a) pont, figyelemmel a Btk. 138/A § d) pontjára is.

18 Például a nagyobb kárt okozó készpénz-helyettesítő fizetési eszközzel visszaélés [Btk. 313/C § (3) bekezdés a) pont] és a készpénz-helyettesítő fizetésieszköz-hamisítás miatt halmazati büntetésként négy és fél év szabadságvesztés is kiszabható [Vö. Btk. 85. § (3) bekezdés].

19 Nagy Ferenc (2008): i. m. 57–59. o.

A Btk. 313/D § szerinti készpénz-helyettesítő fizetési eszköz hamisításának elősegítése – a büntethetőség túlzott előrehozatalának intő példája

A törvényhozó egyrészt hazánknak az uniós tagságával járó nemzetközi kötelezettségeinek, másrészt a szigorúbb büntetőjogi fellépésre vonatkozó igényeknek tett eleget akkor, amikor a Btk. 313/D §-ában a *készpénz-helyettesítő fizetési eszköz hamisításának elősegítése* elnevezésű – egyébként a 304/A §-ba foglalt pénzhamisítás elősegítése elnevezésű bűncselekményre „rímelő" – sui generis előkészületi jellegű bűncselekmény törvényi tényállását megalkotta. A 313/D § szerint, aki készpénz-helyettesítő fizetési eszköz hamisításához szükséges anyagot, eszközt, berendezést vagy számítógépes programot készít, megszerez, tart, átad, forgalomba hoz vagy azzal kereskedik, vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.

A tényállási elemek vizsgálata révén arra a következtetésre juthatunk, hogy itt a jogalkotó egy önálló, külön tényállásban oly módon határozott meg materiális előkészületi jellegű bűncselekményi alakzatokat, hogy emellett az előkészülethez egyébként feltétlenül szükséges *célzatot* nem követelte meg a büntethetőséghez. Nagy Ferenc az ehhez hasonló tényállásokat ezért sorolja az úgynevezett *rendszeridegen* sui generis előkészületi tényállások körébe.[20]

Ha vizsgálat tárgyává tesszük a 313/D §-beli bűncselekmény és a többi, készpénz-helyettesítő fizetési eszközzel kapcsolatos deliktum viszonyát, azt láthatjuk, hogy a hamisítás elősegítése és a 313/B § (1) és (3) bekezdéseiben szabályozott készpénz-helyettesítő fizetésieszköz-hamisítás, illetve annak előkészülete több esetben is *konkurálhat* egymással.

Az első vizsgálandó esetkör az, amikor az elkövető a *saját maga által megvalósítandó* készpénz-helyettesítő fizetésieszköz-hamisítás érdekében fejti ki a 313/D § szerinti, a bűncselekmény elkövetéséhez szükséges elkövetési magatartások valamelyikét. Tipikusan ilyen lehet az elkövetési magatartások közül a *készít, a megszerez,* illetve a *tart* fordulat. Mint Kereszty helyesen megállapítja, ilyenkor – attól az időponttól, hogy az elkövető legalább a *kísérlet* szakába juttatja a készpénz-helyettesítő fizetésieszköz-hamisítást – a 313/D § szerinti bűncselekmény megállapításának már nem lehet helye. Emellett akkor sem minősíthető az elkövető cselekménye a 313/D § szerint, ha a készpénz-helyettesítő fizetésieszköz-hamisítás még nem jutott ugyan a kísérlet stádiumába, ám az elkövető hamisításra irányuló *célzattal* jár el:

20 Uo. 194. o.

ilyenkor a 313/B § (3) bekezdés szerinti előkészületként kell a cselekményt minősíteni.[21] A valóságos halmazat mellőzésének indoka az, hogy abban az esetben, amikor az elkövető ugyanazon bűncselekmény elkövetéséhez több cselekményével is hozzájárul, csak az in abstracto legjelentősebb jogi tárgy elleni támadása vehető figyelembe, a többi – mint *önállótlan részcselekmény* – külön megállapítására nem kerülhet sor.[22]

Nézetünk szerint ez a megállapítás áll arra az esetre is, ha a jogalkotó nem(csak) *expressis verbis* az előkészületet rendeli büntetni adott deliktum kapcsán, hanem emellett (vagy ehelyett) külön törvényi tényállásban határoz meg egy *kvázi előkészületi jellegű* bűncselekményt. A készpénz-helyettesítő fizetési eszköz hamisításának elősegítése tehát a készpénz-helyettesítő fizetésieszköz-hamisítás mellett nem állapítható meg halmazatban, s előbbit a készpénz-helyettesítő fizetésieszköz-hamisításra irányuló valódi előkészület is háttérbe lépteti. Ennek indokát abban látjuk, hogy a készpénz-helyettesítő fizetésieszköz-hamisítás előkészülete *teljes egészében lefedi* a készpénz-helyettesítő fizetési eszköz hamisításának elősegítését, s emellett *többletként* tartalmazza a befejezett bűncselekmény létrehozására irányuló *célzatot* is, így a valódi előkészületre jellemző célzattal eljáró elkövető cselekményének minősítésekor valamennyi körülményt akkor értékelhetünk, ha nem a 313/D § szerinti sui generis befejezett bűncselekményt, hanem a 313/B § (3) bekezdése szerinti előkészületet állapítjuk meg terhére.

Ezzel ellentétesen foglal állást a Hollán – Kis szerzőpáros. Álláspontjuk szerint *„a Btk. 313/D §-ában írt sui generis előkészület – látszólagos alaki halmazatban – előtérbe lép a Btk. 313/B § (3) bekezdésében szabályozott valódi előkészülethez képest. A fenti megoldást a két bűncselekmény a Btk. 313/D § javára eltérő büntetési tétele is alátámasztja. Hasonlóképpen kell elbírálni a két tényállás közötti anyagi halmazatot.”*[23] Ezt a felfogást helytelenítjük, ugyanis a valódi előkészület és a 313/D §-beli bűncselekmény – tekintettel arra, hogy a valódi előkészület a materiális előkészületi magatartásokon felül célzatot is tartalmaz – a *több és a kevesebb viszonyában van.* Éspedig annak ellenére tekinthető az előkészület többnek, a sui generis befejezett bűncselekmény pedig kevesebbnek, hogy a büntetési tételek összevetéséből az tűnik ki, hogy az utóbbi bűncselekmény a súlyosabb. Az a körülmény ugyanis, hogy melyik cselekményt fenyegeti súlyosabb büntetéssel a törvény, önmagában semmiképp nem lehet döntő minősítési kérdésben. Részünkről

21 Kereszty Béla: i. m. 733–734. o.
22 Nagy Ferenc (2008): i. m. 238. o.
23 Hollán Miklós – Kis Norbert: i. m. 698. o.

tehát *Földvári József* elvi álláspontjához csatlakozunk, szerinte „*soha nem a büntetés mértéke befolyásolja a minősítést, hanem a minősítés a büntetés mértékét*”.[24] Ezért a valódi előkészület, tekintettel arra, hogy célzat fennforgása esetén valamennyi körülmény csak ennek kereteiben értékelhető, háttérbe lépteti a hamisítás elősegítését mint sui generis befejezett bűncselekményt, amely így csak abban az egészen kivételes esetben állapítható meg, amikor az elkövető az előkészülethez szükséges célzat nélkül jár el, vagy – mint látni fogjuk – önkéntes visszalépés esetén.

Varga Zoltán szerint a készpénz-helyettesítő fizetésieszköz-hamisítás előkészülete csak akkor valósul meg, „ha az elkövető *saját maga szerzi be saját maga számára”* a bűncselekmény elkövetéséhez szükséges eszközöket, berendezéseket. Szerinte „e tényállás alá […] nem vonhatók azon elkövetők, akiknek a *tevékenysége nem a saját, hanem a más személy által a jövőben elkövetendő* készpénz-helyettesítő fizetési eszköz hamisításának elősegítésére irányul. Ezt a hiányt pótolja a […] Btk. 313/D § szerinti bűncselekmény” *(kiemelések tőlünk. – A szerzők)*.[25]

E felfogással nem tudunk egyetérteni. A Btk. 18. § (1) bekezdése alapján ugyanis az előkészületi magatartást kifejtő személy célzata nemcsak a saját, hanem a *tettesként más által elkövetendő* bűncselekmény elkövetésére is irányulhat.[26] Így a készpénz-helyettesítő fizetésieszköz-hamisítás kapcsán ilyen magatartást tanúsítók (például az elkövetéshez szükséges eszközöket célzatosan beszerzők) – mindaddig, amíg a majdani tettes a bűncselekményt nem juttatja legalább a kísérlet szakába – e bűncselekmény előkészületéért vonhatók felelősségre. Ha pedig a tettes cselekménye a kísérlet stádiumába lép, a bűncselekmény elkövetésének feltételeit megteremtő, előkészületi jellegű magatartás kifejtője bűnsegédként felel. Álláspontunk szerint tehát a Varga által említett *jogalkotási űr* (amelyet a készpénz-helyettesítő fizetési eszköz hamisításának elősegítése lenne hivatott betölteni) valójában *nem létezik*, mert a készpénz-helyettesítő fizetésieszköz-hamisítás előkészülete akkor is megállapítható, ha annak elkövetője cselekményével a *más által elkövetendő* hamisításhoz járul hozzá (és mint az előző pontban kifejtettük, a valódi előkészület mellett a hamisítás elősegítése háttérbe lép, így felhívására jelen esetben sem kerülhet sor).

Az előbbiek alapján felmerülhet a kérdés, hogy egyáltalán mikor kerülhet sor a készpénz-helyettesítő fizetési eszköz hamisításának elősegítése megállapítására, mivel nagyon ritkának és életszerűtlennek tűnik az olyan eset,

24 Földvári József: A büntetés tana. KJK, Budapest, 1970, 388. o.
25 Varga Zoltán: i. m. 1342–1343. o.
26 Nagy Ferenc (2008): i. m. 194. o.

amikor az elkövető – akár saját, akár más személy által elkövetendő – hamisításra vonatkozó *célzat nélkül* mozdítja elő a készpénz-helyettesítő fizetésieszköz-hamisítást. Abban az esetben ugyanis, ha akár a saját, akár más személy hamisítása és az elkövető között a szubjektív oldalon kapcsolat mutatható ki, már nem kerülhet sor a Btk. 313/D § szerinti bűncselekmény megállapítására, s ennek előfordulása a gyakorlatban elhanyagolható.

Nézetünk szerint e rendszeridegen előkészületi jellegű deliktumnak *önálló hatóköre* akkor lehet, ha az elkövető a készpénz-helyettesítő fizetésieszköz-hamisítás kísérlete, illetőleg előkészülete vonatkozásában teljesíti a Btk. 17. § (3), illetve 18. § (2) bekezdésébe foglalt feltételeket, vagyis a kísérlettől, illetve az előkészülettől *visszalép.* Ebben az esetben a Btk. 17. § (4), illetve a 18. § (3) bekezdése alapján az úgynevezett *maradék-bűncselekményért* felelősséggel tartozik, s ez ilyenkor tipikusan a készpénz-helyettesítő fizetési eszköz hamisításának elősegítése lehet. A hamisítás *kísérletétől* történő visszalépés esetén a büntetési tételek arányosságával kapcsolatban dogmatikai aggályunk nemigen merülhet fel (tudniillik az alapesetben legfeljebb két évig terjedő szabadságvesztéssel büntethető bűncselekmény maradékcselekményénél a legfeljebb egy évig terjedő szabadságvesztés nem tekinthető aránytalannak). Ezzel szemben meglehetősen visszás helyzet áll elő akkor, ha az elkövető a 313/B § (3) bekezdés szerinti *előkészülettől* lép vissza. A készpénz-helyettesítő fizetési eszköz hamisításának előkészülete ugyanis mindössze pénzbüntetéssel büntetendő, míg az ettől történő elállást, és így a maradékcselekményként értékelt 313/D § hatályosulását egy évig terjedő szabadságvesztés kilátásba helyezésével „honorálja" a jogalkotó. Ennek alapján azt a következtetést vonhatjuk le, hogy az elkövető lényegében „jobban jár", ha előkészületétől nem lép vissza, mint ha igen, mivel utóbbi esetben a súlyosabb büntetéssel fenyegetett maradék-bűncselekményért vonható felelősségre. Ez a szabályozási aránytalanság – amely egyébként nem példa nélküli a hatályos Btk.-ban[27] – arra vezethet, hogy a büntetőeljárásban a ter-

27 Más, a büntethetőség előrehozatalát célzó sui generis előkészületi jellegű tényállás vizsgálatakor is hasonló anomáliára bukkanhatunk. Például szolgálhat a Btk. 300/E §-ába foglalt *számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása* mint sui generis előkészületi jellegű bűncselekmény és a 300/C §-ban szabályozott *számítástechnikai rendszer és adatok elleni bűncselekmény* viszonya. Itt az elkövető, ha a 300/C § (1) bekezdés szerinti befejezett bűncselekményt megvalósítja, legfeljebb egy évig terjedő szabadságvesztéssel büntethető, ellenben ha e bűncselekményre irányuló különböző előkészületi jellegű magatartást tanúsít, ez a magatartás szükségképpen kimeríti a 300/E §-át, amely alapján a kiszabható büntetés legfeljebb két évig terjedő szabadságvesztés. Ebben az esetben a terhelt védekezése csak az lehet, hogy ő befejezetti stádiumba juttatta a számítástechnikai rendszer és adatok elleni bűncselekményt, mert ekkor az enyhébb büntetéssel sújtható 300/C § (1) bekezdése alapján, s nem a 300/E § alapján felel.

helt úgy fog védekezni, hogy ő *nem lépett vissza* a készpénz-helyettesítő fizetésieszköz-hamisítás előkészületétől, mivel ellenkező esetben a hamisítás elősegítését, s ezzel a súlyosabb büntetést lenne kénytelen magára vállalni.

A kifejtettekre tekintettel megállapítható, hogy a készpénz-helyettesítő fizetési eszköz hamisítás elősegítésének előfordulása önmagában gyakorlatilag elhanyagolható, és csak az önkéntes visszalépés körében juthat némi önálló jelentőséghez. Éppen ebben a körben azonban megengedhetetlen aránytalanságokra vezethet a tényállás léte azáltal, hogy a jogszerűség talajára visszatérő elkövetőt súlyosabb büntetéssel fenyegeti, mint azt, aki előkészületétől nem lépett vissza. Ezért álláspontunk szerint *de lege ferenda* e bűncselekményi tényállás hatályon kívül helyezése lenne kívánatos[28], mivel az mind dogmatikai, mind gyakorlati szempontból visszásságokra vezethet, továbbá a büntetőjog ultima ratio jellegével sincs megfelelő összhangban. Szintén a tényállás hatályon kívül helyezése mellett szól az a körülmény, hogy az ilyen és ehhez hasonló rendszeridegen tényállások kreálásával a jogalkotó *a büntetőjogi dogmatika évszázados múltra visszatekintő elveit rúgja fel* (tudniillik az előkészület régtől fogva fogalmilag feltételezi a szubjektív oldalon a célzat fennforgását).

Ellenérvként felmerülhet, hogy az említett *dekriminalizációnak* útját állja az a körülmény, hogy a készpénz-helyettesítő fizetési eszköz hamisításának elősegítése tényállásának megalkotására az ET 2001/413/IB számú kerethatározatának 4. cikke kötelezte hazánkat. A Btk. 313/D §-ban rögzített magatartások büntetendővé nyilvánítása nemzetközi kötelezettségünk ugyan, a 313/D § hatályon kívül helyezése e kötelezettséget azonban csak *látszólag sértené:* a kerethatározat által tételesen felsorolt előkészületi jellegű magatartások[29] ugyanis kivétel nélkül a Btk. 313/B § (3) bekezdése alá szubszumálhatók, így uniós kötelezettségeink sem szenvednének csorbát a 313/D § „veszni hagyásával". Kiemelést igényel még, hogy az a körülmény sem ad létjogosultságot a 313/D § fenntartásához, hogy a 313/B § (3) bekezdése kizárólag pénzbüntetéssel büntethető; az idézett kerethatározat ugyanis csak annyit ír elő az előkészületi jellegű magatartások vonatkozásában, hogy azokat a tagállamoknak *bűncselekménnyé kell nyilvánítaniuk*, emellett szank-

28 Felfogásunk tehát – további érvek felsorakoztatása mellett – lényegében egybeesik a Kereszty által megfogalmazottakkal: szerinte „a Btk. 313/D §-ban meghatározott bűncselekményt mint feleslegest ki kell iktatni a Btk.-ból". Kereszty Béla: i. m. 734. o.

29 „A készpénz-helyettesítő fizetési eszközök hamisítása vagy hamisítását elősegítő berendezés, tárgy, számítógépes program vagy más eszköz jogosulatlan előállítását, elfogadását, megszerzését, más személy részére történő értékesítését, átruházását vagy birtoklását" kell – egyebek között – a kerethatározat értelmében a tagállamoknak bűncselekménynek minősíteniük.

cióminimumról nem rendelkezik. Így ha a hazai jogalkotás csupán pénzbüntetéssel rendelné büntetni e magatartásokat, uniós kötelezettségeinknek már ezzel eleget tenne.

Az alkalmatlan kísérlet problematikája

A szándékos bűncselekménynek a magyar büntetőtörvény alapján három értékelhető szakasza van: az előkészület, a kísérlet és a befejezett bűncselekmény. A stádiumtannak a magyar jogirodalomban periferikusnak tekintett problémája az alkalmatlan kísérlet kérdése[30], amelynek azonban, álláspontunk szerint, a készpénz-helyettesítő fizetési eszközzel visszaélésnek a Btk. 313/C § (1)–(6) bekezdésében meghatározott, *károkozást* feltételező eseteinél erős gyakorlati relevanciája van.

A mindennapok jogalkalmazása során gyakran felmerülő jogeset szerint az elkövető a sértett táskájából elveszi annak pénztárcáját, amelyben a sértett bankkártyája is benne van, majd a bankkártya felhasználásával megkísérel pénzt felvenni egy pénzautomatából anélkül, hogy ismerné az ehhez egyébként az esetek döntő többségében szükséges úgynevezett PIN kódot. Az elkövető e cselekményét vajon az alkalmatlan kísérlet fogalmi körébe lehet-e vonni, vagy az rendes kísérletet valósít meg?

A hatályos Btk. szerint *a büntetést korlátlanul enyhíteni vagy mellőzni is lehet, ha a kísérletet alkalmatlan tárgyon, alkalmatlan eszközzel vagy alkalmatlan módon követik el.*[31] A Btk. eredeti miniszteri indokolása szerint az alkalmatlan kísérlet esetén az elkövető tévesen feltételezi azt, hogy az eszköz vagy tárgy alkalmas a bűncselekmény megvalósítására, holott az valójában alkalmatlan, illetve lehet, hogy az elkövető a bűncselekmény megvalósítására alkalmas tárgyat vagy eszközt választ, de ezeket alkalmatlan módon használja fel. A Btk. és miniszteri indokolása rövid, és a legkevésbé sem igazít el az alkalmasság és az alkalmatlanság elhatárolásának kérdésében, csupán annyit rögzít, hogy az alkalmatlanság alapja a bűncselekmény elkövetésének eszköze, tárgya vagy módja.

Az alkalmatlan kísérlet problémájának megoldására a jogirodalomban két meghatározó teória alakult ki: az objektivista és a szubjektivista.

30 Nagy Ferenc: Az alkalmatlan kísérletről európai kitekintéssel. Magyar Jog, 2007/1., 26. o.

31 A Btk. 17. § (2) bekezdésébe foglalt rendelkezés új szövegét a 2009. évi LXXX. törvény 1. §-a állapította meg, lehetőséget adva arra, hogy ne csupán a *tárgy*, illetve az *eszköz*, hanem a *mód* alkalmatlansága is megállapítható legyen a kísérlet vonatkozásában.

Az *objektivista irányzat* azon az alapon vizsgálja az alkalmatlan kísérletet, hogy objektíve veszélyes-e a cselekmény, amelyet az elkövető kifejtett. Az irányzat különbséget tesz a nem büntethető abszolút és a büntetést érdemlő relatív alkalmatlanság között. *Abszolút* alkalmatlan az az eszköz, tárgy vagy mód, amely már eleve, természeténél fogva, tehát in abstracto alkalmatlan a befejezett bűncselekmény megvalósítására (például próbababán végrehajtott ölési cselekmény). Ezzel szemben *a relatíve* alkalmatlan tárgy, eszköz vagy mód a cél elérésére in abstracto alkalmas, azonban az adott eset körülményei folytán, in concreto bizonyult alkalmatlannak (például csekély menynyiségű méreg keverése a kiszemelt áldozat poharába).

A *szubjektivista irányzat* szerint a kísérlet–alkalmatlan kísérlet közötti különbségtétel felesleges, a hangsúly az elkövető szándékára helyezendő, és minden olyan kísérlet büntetendő, amelyben a tettesnek a bűncselekmény elkövetésére irányuló szándéka fejeződik ki.[32]

A magyar bírói gyakorlat az alkalmatlan kísérletet döntően az objektivista irányzatnak megfelelően kezeli, és különbséget tesz abszolút és relatív alkalmatlanság között, bár általában mindkettőt büntetést érdemlőnek tekinti. A bíróság (relatíve) alkalmatlan eszközzel elkövetett emberölés bűntettének kísérletét állapította meg, amikor az elkövető egy lemezkádba próbált áramot vezetni, hogy az abban fürdő élettársát megölje, de nem megfelelően rögzítette a vezetékeket, így az adott esetben nem vezethetett a szándékolt eredmény eléréséhez.[33] Az intellektuális közokirat-hamisítás bűntettének abszolúte alkalmatlan kísérletét állapította meg a bíróság abban az esetben, amikor a terhelt ügyvédi ellenjegyzés nélküli magánokiratra – mint objektíve alkalmatlan eszközre – alapozottan kívánt tulajdonjogra vonatkozó valótlan tényt bejegyeztetni az ingatlan-nyilvántartásba.[34]

A hazai judikatúrában találkozhatunk azonban olyan eseti döntéssel is, amely szubjektivista alapon, a tettes szándékához kapcsolódva állapított meg büntetőjogi felelősséget. Így a BH 1978/266. számon közétett eseti döntésében alkalmatlan tárgyon elkövetett emberölés kísérletének minősítette a Legfelsőbb Bíróság annak az anyának a cselekményét, aki az általa nem tudottan *halott* gyermekével szemben hajtott végre egyébként tényállásszerű ölési cselekményt.

Részünkről elvetjük az alkalmatlan kísérlet büntetendőségének tisztán szubjektív, szándékközpontú megközelítését, azt ugyanis összeegyeztethetet-

32 Nagy Ferenc (2008): i. m. 198–201. o.
33 BH, 2007/325.
34 BH, 2004/497.

lennek tartjuk a tettbüntetőjogi alapon felépülő bűncselekménytannal. A modern jogállamban a büntetőjogi felelősség megállapításának alapja az *elkövetett cselekmény* kell hogy legyen.

Az alkalmatlan kísérlet problémájának vizsgálatakor, nézetünk szerint, kiindulópontként kell rögzíteni, hogy az alkalmatlan kísérlet nem önálló, elkülönülő stádiuma a bűncselekménynek, vagyis az alkalmatlan kísérletet csakis a kísérlet fogalmán belül lehet és kell értelmezni, és a kísérlet valamennyi fogalmi eleme egyben az alkalmatlan kísérletet is jellemzi. Dogmatikailag vitathatónak tartjuk azt a jogirodalomban megjelent álláspontot, amely szerint az alkalmatlan kísérlet esetén a cselekmény nem jut a tényállás keretei közé, lévén hogy eleve alkalmatlan, így a befejezettség nem következhet be.[35] Az alkalmatlan kísérlet, ahogyan a kísérlet is, a törvényi tényállás tárgyi (objektív) oldalának részleges megvalósulását jelenti, míg a szándékosság szempontjából semmiben sem különbözik a befejezett bűncselekménytől. Az alkalmatlan kísérlet tárgyi oldalának ismérve az elkövetés, vagyis a törvényi tényállásban meghatározott *elkövetési magatartás megkezdése*.[36]

Alkalmatlan kísérlet esetén tehát a bűncselekmény megvalósul, és az elkövető büntetőjogi felelősségét *a szándékolt bűncselekmény kísérletében* kell megállapítani, a Btk. 17. § (2) bekezdése csupán a büntetés korlátlan enyhítését vagy mellőzését teszi lehetővé.[37]

Az előbbiek alapján súlyos logikai ellentmondásnak véljük alkalmatlan kísérlet megállapításakor a *maradék-bűncselekményért* való felelősségre vonást. E szerint ugyanis, ha az alkalmatlan kísérlet már önmagában is megvalósít más bűncselekményt, az elkövető e bűncselekmény miatt büntetendő. Így például a Legfelsőbb Bíróság megállapította, hogy annak az elkövetőnek a cselekménye, aki a tulajdonjog bejegyzésére egyébként alkalmatlan valótlan tartalmú magánokiratot használ fel arra, hogy az ingatlan tulajdonjogát megszerezze, közokirat-hamisítás bűntette kísérletének minősül, amelyet alkalmatlan eszközzel követett el. A terhelt azonban azzal, hogy a valótlan tartalmú magánokiratot a földhivatalhoz benyújtotta, azt felhasználta, s ezzel már megvalósította a Btk. 276. §-a szerinti magánokirat-hamisítást, ezért a Btk. 17. § (4) bekezdése alapján a terhelt terhére a magánokirat-hamisítás vétségét mint maradék-bűncselekményt kell megállapítani.[38]

35 A magyar jogirodalomban megjelent, eltérő nézeteket ismerteti Lőrinczy Judit: Az alkalmatlan kísérlet a magyar büntetőjogban. In: Szomora Zsolt (szerk.): Tudományos Diákköri Szemle 2006. SZTE ÁJK, Szeged, 2006, 450. o.

36 Nagy Ferenc (2008): i. m. 195. o.

37 Vö. BH, 2004/351. és BH, 2003/270.

38 BH, 2004/351.

Ezzel szemben a BH 2004/497. számon közzétett jogesetben a Legfelsőbb Bíróság intellektuális közokirat-hamisítás alkalmatlan eszközzel elkövetett kísérletének és nem magánokirat-hamisítás vétségének minősítette annak az elkövetőnek a cselekményét, aki ügyvédi ellenjegyzés nélkül készült, hamis adásvételi szerződést nyújtott be a földhivatalhoz a tulajdonjog bejegyzése céljából. A bíróság ítéletének indokolásában kifejti, hogy a maradék-bűncselekmény büntetendősége az alkalmatlan kísérlet eseteire vonatkoztatva gyakorlatilag csak azt idézheti elő, hogy a bíróság (éppen a maradék-bűncselekményre figyelemmel) az alkalmatlan tárgyon vagy eszközzel megvalósított bűncselekmény kísérlete kapcsán a büntetés mellőzésének lehetőségével nem élhet.

Álláspontunk szerint ez utóbbi jogértelmezés tekinthető helyesnek, de a bíróságétól eltérő indokok alapján. Az előbbiekben már kifejtett álláspontunk szerint az alkalmatlan kísérlet esetén az elkövető bűnösségét a megkísérelt bűncselekményben kell megállapítani, és az e bűncselekményre előírt büntetést lehet korlátlanul enyhíteni vagy mellőzni. A magunk részéről nem is igen tudjuk értelmezni a maradék-bűncselekmény fogalmát az alkalmatlan kísérlet vonatkozásában. Abban az esetben ugyanis, ha az elkövető (alkalmatlan) kísérleti szakban rekedt cselekménye önmagában is megvalósít más bűncselekményt, nem maradék-bűncselekményről, hanem két önálló bűncselekményről, még közelebbről, e két bűncselekmény *alaki halmazatáról* kell beszélnünk, ha pedig a kísérleti szakban maradt bűncselekmény megvalósulása kizárja azon bűncselekményi alakzatok megállapítását, amelyek keretei közé az elkövető cselekménye egyébként illeszkedik, a halmazat csupán *látszólagos*, s ezen mit sem változtat a kísérlet alkalmas vagy alkalmatlan mivolta.

Így például ha az elkövető a tulajdonjog bejegyzése céljából hamis magánokiratot nyújt be a földhivatalhoz, cselekménye intellektuális közokirat-hamisításnak minősül, amellyel a magánokirat-hamisítás csupán látszólagos alaki halmazatban áll, és a *konszumpció* folytán nem állapítható meg[39], s ez természetesen irányadó az alkalmatlan kísérlet esetére is. Látszólagos halmazat esetén sincs tehát lehetőség az elkövető maradék-bűncselekmény miatti felelősségre vonására, hiszen csak az elkövető által megkísérelt bűncselekményt lehet megállapítani, és csak emiatt lehet büntetéssel sújtani. Ha az alkalmatlan kísérlet látszólag más bűncselekményt is megvalósít (így például az intellektuális közokirat-hamisítás a magánokirat-hamisítást is), ennek legfeljebb az alkalmatlan kísérletre előírt büntetés kiszabása során lehet jelentő-

39 Például BH, 1996/290.

sége, de a törvény kifejezett rendelkezése folytán – az LB jogértelmezésével szemben – ekkor is helye lehet a büntetés teljes mellőzésének.

Álláspontunk szerint az alkalmatlan kísérlet nem azért érdemel büntetést, mert a bűnelkövetési akarat fennáll. Az alkalmatlan kísérlet büntetendőségének alapja – ugyanúgy, mint az „alkalmas" kísérlet esetében – csakis a *jogtárgysértés*, illetve *-veszélyeztetés* lehet. Az olyan cselekmény, amely jogi tárgyat egyáltalán nem sért vagy veszélyeztet, a társadalomra nem veszélyes, s így – a Btk. 10. § (2) bekezdése alapján – nem tekinthető bűncselekménynek.[40] Abban az esetben tehát, amikor az anya az általa élőnek vélt, ám valójában *halott* gyermekével szemben hajtott végre tényállásszerű ölési cselekményt, könnyű belátni, hogy ez az emberölés jogi tárgyát, az emberi életet se nem sértette, se nem veszélyeztette, vagyis cselekménye nem az emberölés alkalmatlan tárgyon elkövetett kísérletét valósította meg, hanem egész egyszerűen *nem volt bűncselekmény.*

Visszatérve immár kiinduló jogesetünkre – vagyis arra az esetre, amely szerint az elkövető jogtalanul szerzett bankkártya segítségével, a PIN kód ismerete nélkül próbál a pénzautomatából pénzt leemelni –, e cselekmény büntetendősége, az alkalmasság és az alkalmatlanság elhatárolása kérdésében nézetünk szerint a készpénz-helyettesítő fizetési eszközzel visszaélés *jogi tárgya* orientálhatja a jogértelmezést, mivel kizárólag a jogi tárgy figyelembevételével tudjuk racionálisan megindokolni a büntetőjogi fenyegetést.[41] E bűncselekmény károkozást feltételező változatának *jellegzetes* jogi tárgyát a bankszámla-tulajdonos – aki egyben a bankkártya birtokosa – érdekei adják (feltéve természetesen, hogy *bankkártya* az elkövetés tárgya). Emellett azonban a *számlavezető hitelintézetek vagyoni érdekei* és a pénzhelyettesítő fizetési eszközök *forgalmának biztonsága* is jogi tárgyként szerepel.[42]

A bíróság több ítéletében is megállapította, hogy a bankkártya önmagában, a rendelkezési jogot megtestesítő kódszám ismerete nélkül a pénzkifizető automatából való pénzfelvételre vagy vásárlásra nem használható fel.[43] Nézetünk szerint azonban a bankkártya a PIN kód ismeretének hiányában is *alkalmas eszköz* lehet a pénzfelvételre, hiszen az elkövetőnek in abstracto van esélye arra, hogy a helyes kódot adja meg (bár ennek esélye nyilvánva-

40 Lásd Nagy Ferenc (2008): i. m. 133. o.; Vö.: Lőrinczy Judit: i. m. 450–453. o.

41 Szomora Zsolt: A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés. Bűnügyi Szemle, 2009/2., 12. o.

42 Karsai Krisztina – Kereszty Béla: A gazdasági bűncselekmények (Btk. XVII. fejezet). In: Nagy Ferenc (szerk.): A magyar büntetőjog különös része. HVG-ORAC Kiadó, Budapest, 2009, 561. o.

43 Például BH, 1999/57. és BH, 2002/474.

lóan csekély). Erre tekintettel az automatánál újabb és újabb PIN kódokkal „próbálkozó" elkövető magatartása a készpénz-helyettesítő fizetési eszközzel visszaélés jogi tárgyát veszélyezteti, és így megalapozza a büntetőjogi felelősséget. A jogi tárgyat fenyegető veszély foka azonban olyannyira minimális, hogy az a büntetés korlátlan enyhítését alapozza meg a felhasználás *alkalmatlan módjára* tekintettel (hiszen az elkövető csak a PIN kód birtokában tudja helyesen használni a bankkártyát).[44]

Nézetünk szerint alkalmatlan kísérlet állapítható meg abban az esetben is, ha az elkövető a PIN kód ismeretében olyan bankkártyával kísérel meg pénzt felvenni, amelyhez tartozó bankszámlán *pénz nem található.* Ebben az esetben a bankkártya mint eszköz és felhasználásának módja a szándékolt eredmény elérésére in abstracto alkalmas ugyan, az adott körülmények között azonban in concreto alkalmatlan volt a kívánt eredmény, a pénzszerzéssel okozati összefüggésben lévő károkozás előidézésére.

Más megítélés alá esik azonban annak az elkövetőnek a cselekménye, aki *lejárt érvényességű* bankkártya felhasználásával kíván pénzhez jutni. A lejárt érvényességű bankkártya fizetési eszközként egyáltalán nem használható, az készpénz-helyettesítő fizetési eszközként az érvényességi időn túl nem funkcionál, így büntetőjogi védelemre sem szorul.[45] Tekintettel arra, hogy a lejárt bankkártya nem lehet a készpénz-helyettesítő fizetési eszközzel visszaélés elkövetési tárgya, az ilyen bankkártya felhasználása esetén a bűncselekményi jelleget tehát már a *tényállásszerűség hiánya* kiküszöböli.

Kiemelést igényel még, hogy a Btk. 313/C § (1)–(6) bekezdés szerinti készpénz-helyettesítő fizetési eszközzel visszaélés alkalmatlan kísérlete esetén – maradék-bűncselekmény címén – nem állapítható meg a Btk. 313/C § (7) bekezdésében meghatározott, megszerzéssel megvalósuló készpénz-helyettesítő fizetési eszközzel visszaélés, az ugyanis *beolvad* a Btk. 313/C § (1) bekezdés szerinti bűncselekmény alkalmatlan kísérletébe ugyanúgy, mint annak alkalmas kísérletébe. A látszólagos anyagi halmazati viszony szempontjából tehát a kísérlet alkalmas vagy alkalmatlan volta közömbös.

44 Itt jegyeznénk meg, hogy egyes üzletekben és internetes oldalakon továbbra is lehetőség van arra, hogy az elkövető *a PIN kód ismerete nélkül*, kizárólag a bankkártya birtokában fizetni tudjon – erre tekintettel az alkalmatlan kísérlet kapcsán tett megállapításainkat a tanulmány Az alkalmatlan kísérlet problematikája című részének legelején ismertetett jogesetre vonatkoztatjuk.

45 Vö. BH, 2009/349.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp104-115

RIGÓ ATTILA – MÁTRAI LÁSZLÓNÉ DR. ÓZSVÁRTH BABETT

A vagyonvisszaszerzés jogi és gyakorlati lehetőségei az Egyesült Királyságban és Németországban

A *Rendészeti Szemle* májusi számában már bemutattuk a magyarországi vagyonvisszaszerzés általános helyzetét. Ehhez kapcsolódva a *Nyomozási módszerek és technikák a vagyon felderítése során* címmel az Európai Unió Bizottsága bűnmegelőzési programja keretében megvalósuló középtávú (kétéves) projekten belül a magyar Vagyon-visszaszerzési Hivatalnak lehetősége nyílt, hogy részletekbe menően megismerje egyebek között az Egyesült Királyság és Németország jogi megoldásait és gyakorlati lehetőségeit ebben a témakörben.

Egyesült Királyság

Az *Egyesült Királyságban* a *West Midlands-i Regionális Rendőrség Vagyonfelderítő Egységénél* (Regional Asset Recovery Team; *RART*) tettünk szakmai látogatást. A következőkben összefoglaljuk az itt szerzett tapasztalatokat.

Az ország kilenc nagy régióra tagozódik, ötben létezik *RART*, ezek számát a későbbiekben bővíteni szeretnék. A nemzetközi kapcsolatokért a *Súlyos Szervezett Bűnözés Elleni Ügynökség* (Serious Organised Crime Agency; *SOCA*) mint a hivatalosan kijelölt nemzeti vagyon-visszaszerzési hivatal felelős.

A RART szerkezete

A West Midlands-i RART személyi állományába 11 *rendőr tartozik*, továbbá három, nyugdíj mellett foglalkoztatott köztisztviselő. A rendőrök nem viselnek rendfokozatot, hanem a beosztásuk alapján differenciálódnak *(sergeant, inspector, chief inspector, superintendent)*. Nagyon fontos, hogy a RART egységet a pénzügyi nyomozásban három *könyvelő* is segíti, a jogi kérdések tekintetében pedig három *jogász* ad tanácsot.

Az *adóhivataltól (Tax Authority)* és a *vám- és pénzügyőrségtől (Her Majesty's Revenue and Customs)* is egy-egy személyt delegáltak a RART-hoz, nekik hozzáférésük van az adó-, illetve vámadatokhoz, így a személyesen továbbított megkeresés alapján percek alatt hozzájuthatnak a szükséges információhoz.

A büntetőeljárás, illetve az utána következő elkobzási eljárás jogi mederben tartására, valamint szintén jogi tanácsok adására az ügyészségtől *(Criminal Prosecutor Service)* is delegáltak egy *ügyészt* a hivatalhoz, az ügyészség és a rendőrség közötti megállapodás alapján. Az előbbiek mellett azért is van kiemelt jelentősége a jelenlétének, mert a büntetőeljárás elrendelésénél, a biztosítási intézkedés, az elkobzási parancs esetében a bíróság részére elkészíti az előterjesztést, megadja az ügyészi engedélyeket, ezzel idő takarítható meg.

Mind a RART, mind a gazdaságvédelmi területen dolgozó személyi állomány, mind az ügyészek rendszeres továbbképzéseken vesznek részt.

Mindenekelőtt hangsúlyozni kell, hogy az Egyesült Királyságban a bűncselekményt vizsgáló büntetőeljárás és az annak jogerős befejezése utáni *elkobzási eljárás (confiscation procedure)* – ez *polgári* – teljesen elkülönül egymástól. Természetesen az alapeljárásban minden fellelhető vagyont próbálnak biztosítani, de a bűnösséget megállapító jogerős ítélet után a bíróság által kiadott úgynevezett elkobzási parancs *(confiscation order)* alapján indulhat meg a vagyon felderítésére összpontosító civil eljárás, amely az elkövető által a bűnöző életvitelhez kötődő vagyon elvonására szolgál úgy, hogy a bizonyítási teher a nyomozó hatóságról az elkövetőre hárul.

Hatáskörmegosztás az Egyesült Királyságban

Az Egyesült Királyság területén a hatáskör az elkövetett bűncselekmények súlyosságához, illetve az elkövetési értékhez, valamint a nemzetközi vonatkozáshoz igazodik, a következők szerint:

Az *első szinthez (level 1)* a kisebb súlyú bűncselekmények tartoznak (kisebb értékre elkövetett vagyon elleni bűncselekmények, egyszerű megítélésű ügyek), amelyeket a helyi rendőri szervek vizsgálnak. Ezek a szervek a magyar helyi, illetve Budapest esetében a kerületi kapitányságoknak felelnek meg. Ehhez a szinthez tartozik az úgynevezett *magisztrátusi bíróság (Magistrates' Court).*

A *második szinthez (level 2)* a súlyosabb bűncselekmények tartoznak, magasabb elkövetési értékkel, esetleg több kerület vagy város illetékességi területét érinti. Ehhez a szinthez tartoznak a RART egységei is. Ezen a szinten lehetséges, hogy az első szinttől átvegyenek ügyeket, illetőleg az első szint is küldhet vezetői döntés alapján, ha túlterheltek, vagy az ügy bonyolultsága indokolja. Az ügyek elbírálása ebben az esetben a *Koronabíróság (Crown Court)* hatáskörébe tartozik.

A *harmadik szint (level 3)* esetében a kiemelt rendőri szervek nyomoznak, amikor a súlyos bűncselekményeket szervezett formában követik el, esetleg

az egész Egyesült Királyság területét érinti, és nemzetközi vonatkozása is van. Tipikusan ilyen szerv a SOCA, amely ezen kívül a nemzetközi kapcsolattartásért is felelős. Ennél a szintnél a *Főbíróság (High Court)* jár el.

A büntetőeljárás (alapeljárás)

A bűncselekményeket felderítő büntetőeljárás mint alapeljárás – amelyet a *Rendőri bűnügyi bizonyítékokkal kapcsolatos törvény (Police Criminal Evidence Act)* alapján indítanak el – kifejezetten a bűncselekmény bizonyítására szolgál. A megindításhoz szükséges a bíróság engedélye, amelyet az ügyészség terjeszt elő. A büntetőeljárásban történik a bizonyítékok beszerzése, amivel magát a bűncselekményt támasztják alá. Meg kell jegyezni, hogy ebben az eljárásban is minden eszközzel igyekeznek biztosítani a bűncselekményből származó, valamint a fellelhető vagyont, amelynek majd az elkobzási eljárásban lesz jelentősége.

A pénzügyi, gazdasági és vagyon elleni bűncselekményeken kívül más típusú bűncselekmények (például kábítószerrel visszaélés, emberölés) esetében is ügyelnek arra, hogy házkutatáskor ne kizárólag a bűncselekmény elkövetését bizonyító dolgokat foglalják le, hanem minden fellelhető okiratot (például bankszámlakivonatot, számlát, ingó és ingatlan adásvételéről szóló szerződést, váltót, értékpapírokat), amelyek később bármilyen összefüggésbe hozhatók az elkövetővel. E bizonyítékok vonatkozásában a magyar büntetőeljárási rendelkezések szerinti *biztosítási intézkedéssel (restraint order)* biztosítják a vagyont, amelyet egyébként az elkobzási eljárásban is kiadhat a bíró. A biztosítási intézkedés időben mindig megelőzi az elkövető őrizetbe vételét, illetve letartóztatását.

Általánosságban az alapeljárás két éven belül (többnyire fél év alatt) jogerős ítélettel zárul, amelynek keretében, a tárgyaláson a 12 tagú esküdtszék megállapítja az elkövető bűnösségét, illetőleg, ha nem találja megalapozottnak a felhozott bizonyítékokat, felmenti őt. A bűnösség megállapítása esetén ennek tényét az ítéletbe foglaló bíró kiszabja a büntetést, majd különböző feltételek fennállása esetén az elkobzási paranccsal elrendeli magát az elkobzási eljárást.

Az elkobzási eljárás

Az elkobzási eljárás célja, hogy az elkövető bűnözői magatartásából *(criminal conduct)* származó vagyoni előnyt felfedje. Magára az eljárásra vonatkozó rendelkezéseket a vagyonfelderítés területén mérföldkőnek számító *bűn-*

cselekményből származó javakról szóló törvény *(Proceeds of Crime Act 2002)* tartalmazza, amely 2003-ban lépett hatályba. Kormányzati szinten fogalmazódott meg az az igény, hogy generális prevenciót alkalmazzanak a bűnismétlés megelőzése érdekében, és hogy a vagyont véglegesen elvonják az elkövetőktől, ezért a törvény alapjaiban változtatta meg a büntetőeljárások során alkalmazott bizonyítási szabályokat, mivel bizonyos tekintetben megfordította a bizonyítási terhet. A törvény nem kizárólag a bűnözőkre vonatkozik, ugyanis ügyvédek, könyvelők, bankárok éppúgy kerülhetnek olyan helyzetbe, hogy nekik kell bizonyítaniuk a jövedelmük legális eredetét.

A törvény értelmében a bűnöző magatartás szempontjából figyelembe kell venni az Egyesült Királyságon kívül elkövetett bűncselekményeket is, amelyek a hazai jog szerint is büntetendők (megegyezve a magyar Btk. területi és személyi hatályával).

A jogszabály szerint az elkövető bűnöző magatartásából eredő vagyoni előnynek minősül, amely a bűncselekmény elkövetéséből, illetve annak további értékesítéséből származik. Példával élve, ha valaki eltulajdonít egy ezer font értékű gépkocsit, majd eladja ötezer fontért, a vagyoni előnye összesen tizenötezer font.

Az elkobzási eljárás határideje két év, amely indokolt esetben meghosszabbítható, de általában fél év alatt szintén befejezik, tekintettel arra, hogy sokszor már a büntetőeljárásban meghozzák a bűnös vagyont biztosító intézkedéseket.

Az eljárás egy speciális formanyomtatvány *(application to refer)* kitöltésével indul, amely iránymutatásul szolgál az ügy előadójának. Az első része röviden tartalmazza a tényállást, az előadót, illetve az ügyért felelős személyek nevét, az eljárás alá vont személyazonosító adatait, a nyomozásban ismertté vált lakcímet, a munkavállalással kapcsolatos dokumentumokat, az alapügyben ismertté vált pénzügyi információkat, például a zár alá vett vagyont, a lefoglalt készpénzt. A második részt már az ügy előadója tölti ki, és ez tartalmazza a konkrét pénzügyi analízist, ezen belül az esetleges legális jövedelemből származó pénzt, a közös háztartásban élők jövedelmi viszonyait, a banki információkat, a személyhez köthető gépjárművekkel kapcsolatos adatokat, valamint azt, hogy melyik hatóságot mikor keresték meg, valamint a kapott válasz eredményét.

Az eljárásban elsőként azokat az információkat szerzik be, amelyek kifejezetten a bűncselekmények bizonyítási tárgyául szolgálhatnak. Ezen túlmenően azonban egy általános kötelezettséget jelent, hogy a nyomozók a házkutatás során a pénzügyi információk felkutatásának dokumentálását is elvégezzék, úgy-

mint feljegyzések, bankszámlakivonatok, csekkfüzetek stb. összegyűjtése a későbbi sikeres elkobzási eljárás érdekében. Ezen túl fényképet készítenek a házról, a szobákról, a műszaki berendezésekről, márkás ruhákról. Lehetőség van a házkutatás foganatosításában részt vevő nyomozó megkeresésére, további információk beszerzése érdekében kérdések tehetők fel neki.

Lehetőség van az elítélt és egyéb érintett személyek kihallgatására, hogy nyilatkozzon a vagyonáról; a vallomást megtagadhatják, mindazonáltal a már felderített vagyonra vonatkozóan is megpróbálják őket nyilatkozatra bírni.

Bűnöző életmód

Az elkobzási eljárás fontos jogintézménye az úgynevezett *bűnöző életmód (criminal lifestyle)* vélelme, amely azon az alapelven alapul, hogy bizonyos bűncselekmények elkövetése esetén azzal a feltételezéssel kell élni, hogy az elkövető minden vagyona bűncselekményből származik. A bűnözői életmód megállapításának három módja van:

Az *első* esetben a következő bűncselekmények *bármelyikének elkövetésével* az elkövető megvalósítja a bűnöző életmódot: kábítószerrel visszaélés, pénzmosás, terrorcselekmény, embercsempészet, fegyvercsempészet, pénzhamisítás, szerzői vagy szomszédos jogok megsértése, kerítés, üzletszerű kéjelgés elősegítése, kiskorú megrontása, zsarolás, valamint ezek kísérletei, illetve állam elleni összeesküvés kísérlete, felbujtása, elősegítése vagy biztosítása.

A *második* esetben az elkövető az *elmúlt hat évben* egy vagy több, bármilyen jellegű bűncselekményt követett el, és ebből *legalább ötezer font* vagyoni előnye származott.

A *harmadik* eset az első kettő kombinációja, amely szerint az elkövető négy vagy annál több bűncselekményt követett el, amelyből legalább ötezer font vagyoni előnynek kellett származnia. További fontos feltétel, hogy a minimum négy bűncselekményt egy eljárásban bírálják el.

A bírói vélelem (feltételezés, assumption)

Szintén az elkobzási eljárás fontos tartalmi eleme a bírói vélelem, amikor a bíróság úgy dönt, hogy az elkövető bűnöző életmódot folytat. A bíró négyfajta feltételezéssel élhet – ügyészi előterjesztés alapján – annak érdekében, hogy eldöntse, az elkövető bűnöző magatartást tanúsított-e, ha pedig erről határoz, megállapítja az ebből származó vagyoni előny nagyságát. Hozzá kell

tenni, hogy a vélelemfajtákat nem alkalmazzák, ha azt a bíróság helytelennek ítélné, vagy súlyos mérvű igazságtalanságot jelentene. A vélelmek esetei a következők:

1. Az első esetben a büntetőeljárás alatt az elfogatóparancs kibocsátásának, illetve a vádemelés első napjától visszamenőleg számított hat év alatt szerzett minden vagyontárgyat úgy tekint a bíróság, hogy bűncselekményből kellett származnia.
2. A második esetben a jogerős elítélés napjától számítva az elkövető által megszerzett, illetve rendelkezésre álló minden vagyontárgyáról azt kell feltételezni, hogy bűnös életvitelből származik.
3. A harmadik feltételezésnél a 2. pontban meghatározott nap után felmerülő mindenfajta kiadásról (például nyaralás, megélhetési túlköltekezések) azt feltételezi a bíróság, hogy bűncselekményből származik.
4. A negyedik esetben a bíróság azzal a feltevéssel él, hogy az elkövető vagyontárgyával kapcsolatos járulékos költségek (például fűtés, fenntartás), illetve például az ingatlan bérbeadásából származó bevétel bűnös vagyonnak tekintendő. A bíróság egyébiránt a visszaszerezhető és a rendelkezésre álló összegekkel számol.

Amikor a bíróság megállapította a vagyoni előny nagyságát, elrendeli annak az elkövető részéről történő befizetését. A törvény erre a jogerős elítélés után hat hónapos határidőt állapít meg. Gyakran előfordul, hogy az elkövető a hat hónapon belül nem tudja a meghatározott összegű pénzt befizetni, mert az adott vagyontárgy már nincs meg, az ellenértéket pedig felélte, vagy azt – ingatlan esetében – közeli hozzátartozója nevére íratta. Érdekes, hogy a vagyon felélése, illetve átíratása nem mentesíti az elkövetőt a pénzbefizetés kötelezettsége alól, ekkor a bíróság a jogerős ítélettel kiszabott büntetéshez halmazatban megállapítja az adott, elmaradt pénzösszeghez meghatározott szabadságvesztést, amely akár tíz év is lehet.

Az ellenkező bizonyítás természetesen lehetséges, de az elkövetőnek kell bizonyítania, hogy az adott vagyon vagy vagyontárgyak legális forrásból származnak. Felmerül kérdésként, hogy ha az elkövetőt előzetes letartóztatásba helyezték, hogyan szerzi meg a szükséges igazolásokat. Ilyenkor a védőjén keresztül tartja a kapcsolatot a hozzátartozóival, és magát a védőt is megbízza, hogy járjon el helyette, és a dokumentumokat gyűjtse össze.

Nagyon fontosnak tartjuk hangsúlyozni, hogy a vagyonfelderítésben érdekeltté tették a résztvevő igazságügyi és rendészeti szerveket, tekintettel arra, hogy a véglegesen *elkobzott vagyon részben visszaáramlik* hozzájuk. Fő sza-

bály szerint a vagyon értékének felével a kormányzat rendelkezik, a másik fele egyharmad-egyharmad-egyharmad arányban megoszlik az ügyben eljáró bíróság, ügyészség és rendőrség között. Hozzá kell tenni, hogy készpénz esetén a rendőrséget megillető hányad ötven százalék.

Németország

Ettől eltérő jogi lehetőségeket ismerhettünk meg a projekt keretén belül Németországban. Elmondható, hogy évek óta tartó hosszú fejlődési folyamat nyomán szintén hatékony jogi és gyakorlati rendszert sikerült kialakítani.

Németország 16 szövetségi tartományból áll, minden tartományban ugyanazok a szövetségi büntetőjogi és büntetőeljárás-jogi jogszabályok érvényesülnek, a vagyoni kényszerintézkedésekhez bírói engedély kell, de a vagyonfelderítés vonatkozásában az igazságszolgáltatási (ügyészségi, bírói) alkalmazás eltérő.

A 2007/845/IB számú tanácsi határozat értelmében létrehozandó nemzeti vagyon-visszaszerzési hivatalt minden tartományban kijelölték, és ezek egymással, illetve a külföldi partnerszervekkel is kölcsönösen cserélhetnek információt.

A nyomozások folyamán *két bűncselekményt* emeltek ki, amelynek a vagyonfelderítés miatt külön jelentősége van. Az egyik a kábítószer-kereskedelem, a másik a csalás.

A csalás esetén mindig van sértett, a bíróság pedig az eljárásban nem az állam, hanem az áldozat javára foglalja le a bűnös vagyont. Hangsúlyozták, hogy egy bank ellen elkövetett milliós nagyságrendű csalás és egy állampolgár ellen elkövetett kis értékű utcai rablás azonos tekintet alá esik, illetve vagyonvisszaszerzést – a szűkös kapacitása miatt – utóbbi esetben indítanak. Ennek oka, hogy számukra a legfontosabb az állampolgároknak a rendőrségbe vetett bizalmának megszerzése és fenntartása, a szubjektív biztonságérzet növelése.

Lefoglalás

A *lefoglaláskor* a bíróság akkor dönt a vagyon elvonásáról, ha jogellenes cselekedetről van szó, ismert az elkövető, és az elkövetésből illegális vagyon származik. A vagyon elvonásánál érdekes módon a polgári jog szabályait alkalmazzák, és tulajdonképpen egy közigazgatási eljárásban egy közigazgatási bíró dönt a vagyon sorsáról.

A vagyon vonatkozásában megkülönböztetik a bruttó és nettó jövedelmet. Régebben az elkövető leírhatta, visszaigényelhette azokat az igazolható költségeit, amelyeket a bűnösen szerzett vagyonból költött *(nettó jövedelem).* A jelenlegi joggyakorlat alapján azonban semmilyen költség nem számolható el, tehát az elkövetőtől elvonható valamennyi vagyont lefoglalják *(bruttó jövedelem).*

Hozzá kell tenni azonban, hogy például egy gazdasági társaságot érintő lefoglaláskor mindig mérlegelni kell, hogy az nem lehetetleníti-e el annak működését, gondolva az ott dolgozó, a bűncselekmény elkövetésében nem érintett személyekre. Ilyen esetben – ha ez lehetséges – valamilyen más vagyont kell találniuk.

A lefoglalás szabályait tovább árnyalja, hogy a szerencse-, illetve nyereményjáték során szerzett pénzt nem lehet elvonni.

Ezen kívül, amennyiben az elkövető legális jogügylet (például szerződés) alapján a jóhiszemű harmadik személynek mint jogosultnak szolgáltat pénzt, a harmadik személytől nem lehet lefoglalni. Természetesen nem lehet alkalmazni ezt a szabályt, ha a harmadik személy tudott arról, hogy a pénz bűncselekményből származott.

Előfordul az is, hogy a bűncselekményből származó dolgot nem találják, vagy készpénz esetén nem tudják megkülönböztetni a legális és illegális eredetű vagyont. Ilyenkor a pénz helyébe lépő tárgyat, illetve a tárgy értékének megfelelő értéket vonják el. Ebben az esetben csak azt kell bizonyítania a rendőrségnek, hogy a tárgy az elkövetőé, és hogy ő követte el a bűncselekményt.

Nyomozástaktikai szempontból mindig igyekeznek olyan dolgokat is lefoglalni – még akkor is, ha az lényeges értékkel nem bír –, amelyekhez lelkileg kötődik az elkövető, hogy ezzel is törekedjenek a pszichikai megtörésére.

A német rendőrségi törvény 43. §-a felsorolja azokat az eseteket, amikor le lehet foglalni (biztosítani) az intézkedés során megtalált értéket. A lefoglalásra akkor van lehetőség, ha

– veszély elhárítása a cél,
– ezzel a tulajdonost kártól vagy veszteségtől lehet megóvni, vagy
– veszélyes anyagok, eszközök vannak az érintett birtokában.

A jogintézmény lényege, hogy a rendőri intézkedés során, az előbbi indokok alapján lefoglalt értékeket három napig tudja magánál tartani a rendőrség, de amennyiben ennyi idő nem lenne elegendő annak megállapítására, hogy a lefoglalt dolog jogszerű forrásból származik-e, abban az esetben a közigazgatási bíróság harminc napra elrendelheti a dolog lefoglalását.

A 43. § (1) bekezdésében meghatározott veszélyen minden olyan esetet értenek, amely a közrendet, közbiztonságot veszélyeztetheti, vagy amely vagyonban bekövetkező kárhoz vezet, illetve arra utal. Például, ha az intézkedő rendőr azt tapasztalja, hogy a gépjármű vezetője ittas, akkor lefoglalhatja a kulcsokat, hogy kizárja a további károkozás lehetőségét, vagy ha a rendőr azt tapasztalja, hogy egy autót nem zártak be, akkor azt a lopás vagy egyéb bűncselekmény megakadályozása céljából lefoglalhatja.

A német gyakorlatban a bűncselekmények nyomozása és a lefoglalás során a károsultak kárpótlását tekintik elsődleges szempontnak.

Ha a sértett ismert, az ügyészség elrendelheti a *vagyontárgyak előzetes biztosítását*, hogy abból megfelelő módon kárpótolhassa az áldozatokat, de ezzel a lehetőséggel saját bevallásuk szerint nem élnek elég gyakran. Amennyiben nincs közvetlen sértett, a lefoglalt vagyonból a nyomozást végző rendőrség közvetlenül nem kap pénzt, hanem az a tartományi költségvetésbe kerül. Szövetségi hivatalok esetében a lefoglalt vagyon a szövetségi köztársaság büdzséjébe áramlik.

Ami a lefoglalt készpénzt illeti, azokat egy a bíróság által vezetett számlára kell befizetni. Amennyiben az elkövetőt elítélik, a pénzt egy másik számlára könyvelik el. Az elkövető felmentésekor a pénzt visszakapja, a zárolás alatti kamatokért pedig perelhet, mivel az automatikusan nem jár neki. A lefoglalt vagyonból a rendőrség nem részesül, egyes lefoglalt dolgokat (például gépjármű) azonban használhat.

Becslés

A becslés *(die Schätzung)* jogintézményét abban az esetben lehet alkalmazni, ha ismerik az elkövetőt és meghatározták azt a bűncselekményt, amelyből a vagyon származott. Ekkor egy úgynevezett veszélyeztetési prognózist kell adni, amely alapján meg kell becsülni azt a vagyont, amely a bűnös tevékenységből minimálisan származhatott, tekintet nélkül arra, hogy ténylegesen felleltek-e. Ennek megértéséhez egy jogesetet hoztak fel: egy éjszakai bárt üzemeltető elkövető prostitúcióval is foglalkozott, és kb. egy hónapon keresztül megbecsülték, hogy átlagosan mennyi vendég járt a bárba, mennyi időt tartózkodtak ott, hányan vették igénybe a prostituáltak szolgáltatásait. Ezen adatok birtokában pedig megbecsülték, hogy az elmúlt öt évben mennyi volt az a legkevesebb bevétel, amennyit a bűncselekmények elkövetésekor megszerzett, ezt az összeget pedig meg kellett fizetnie.

Bizonyos becslések megkönnyítéséhez táblázatokat adnak ki, a becslésnek pedig valósnak, követhetőnek kell lennie.

További terhet jelent az elkövetőnek, hogy a bűncselekményből származó jövedelem után adófizetési kötelezettséget is megállapítanak.

Az adónyomozás mellett elrendelhető az úgynevezett *kiegészítő vizsgálat*, amely egy adminisztratív eljárás, de ez idő alatt hatékonyabban tudják biztosítani a vagyont (ingó, ingatlan). Igaz, hogy nekik is vannak tárolási nehézségeik (például gépjármű).

Kiterjesztett vagyonelkobzás

Abban az esetben, ha az elkövetőnek nincs jövedelme, bejelentett munkahelye, nem tudja igazolni, hogy örökölt, a házkutatás idején felkutatott mindennemű vagyontárgyat le lehet foglalni.

Ekkor a rendőrség javaslatot tesz a közigazgatási – nem büntető-! – bíróságnak, hogy az említett körülmények miatt feltételezik a fellelt vagyon bűncselekményből származását. Tehát a nyomozó hatóság egyfajta vélelemmel él az elkövetőt illetően, e szerint bűnözésből tartja fenn magát (hasonlóan az angol bűnöző életmódhoz), és ellenkező bizonyításig a vagyont lefoglalják, majd végleg elvonják.

E jogintézményhez azt is hozzáfűzték, hogy minden tartományban létezik ugyan ez az intézmény, de alkalmazása tartományonként különböző. Berlinben például a nyomozó hatóságnak még nem sikerült így vagyont elvonnia, de más tartományok sikeresen élnek ezzel az eszközzel.

Integrált pénzügyi nyomozások

Egyes tartományok vagyon-visszaszerzési hivatalai úgynevezett *integrált pénzügyi nyomozásokat* folytatnak, amelyek alapján a bűncselekmény beazonosításától kezdve a bizonyítékok beszerzésén keresztül a vagyon lefoglalásáig terjed az eljárás. A vagyon-visszaszerzési hivatalok tevékenységi köre a következőkből épül fel:

a) szervezett bűnözői hálózatok beazonosítása;
b) a bűncselekmény bizonyításához szükséges bizonyítékok felkutatása;
c) a bűncselekményből származó vagyon felkutatása, beazonosítása és lefoglalása;
d) a regionális rendőri szervek szakmai támogatása, tanácsadás;

e) taktikai, nyomozati módszerek összegyűjtése, elemzése és a többi rendőri szervvel való megosztása;
f) továbbképző tanfolyamok szervezése, lebonyolítása;
g) a kifejezetten a vagyonfelkutatáshoz kifejlesztett számítógépes program *(Abschöpfer Archiv:* lefoglalási archívum) továbbfejlesztése és karbantartása; ebben minták, formanyomtatványok is szerepelnek.

Internetes értékesítés

Németországban két *internetes platform* – az előbbit a vám- és pénzügyőrség, az utóbbit az igazságügyi minisztérium üzemelteti – is működik, ahol a lefoglalt vagyontárgyakat árverezik. Beletartoznak a preventív vagyonelkobzás során elvont vagyontárgyak is. Ezzel a megoldással felgyorsíthatják az értékesítés folyamatát, megkönnyítve ezzel a vagyonkezelés okozta nehézségeket, amelyek abból adódnak, hogy a lefoglalt vagyon romlandó, vagy tárolása aránytalan költséggel jár, illetve a tárolás értékcsökkenéshez vezet.

Konklúzió

Az angol kollégák összességében nagyon impresszív és hatékony rendszert mutattak be, és bár az eltérő jogrendszer másfajta lehetőségeket nyújt, mégis érdemes elgondolkodni némely jogi (például az elkobzott vagyon visszaáramoltatása a rendőrség részére) és gyakorlati (már a házkutatáskor is figyelnek a vagyon felkutatására) példa átvételén.

Az elkobzott vagyon visszaáramoltatása mindenképpen ösztönző jellegű a vagyonfelderítésben részt vevő szervek számára, hiszen abból lehet a munkavégzéshez szükséges eszközöket megvásárolni, például korszerűsíteni a számítógépes rendszert, a gépjárműparkot. Magyarországon jelenleg erre nincs lehetőség, de úgy véljük, hogy hasonlóan ösztönző jellegű lenne ennek bevezetése. Nálunk jelenleg az sem gyakorlat, hogy például kábítószerrel összefüggő házkutatás során a banki átutalások, megtakarítások dokumentációit is keressék a nyomozók, illetve hogy a nyomozáskor megtörténjen a nagy értékű gépjárművek vagy akár luxus kozmetikai cikkek vagy ruházat dokumentálása.

Azt gondoljuk, hogy a kontinentális jogi hagyományokon alapuló német jogi megoldások könnyebben átvehetők, jobban közelítenek a magyar büntetőjogi szabályozási rendszerhez. Jelenleg is már több azonosság felfedezhető

a vagyon-visszaszerzési lehetőségeken belül, elsősorban ami a jogi szabályozást illeti – például az elkobzásra vonatkozó rendelkezések szinte teljes egészében azonosak –, gyakorlati téren azonban ezeket a lehetőségeket a német kollégák sokkal jobban alkalmazzák és hasznosítják.

Az egyértelmű, hogy a bizonyítási teher megfordítása – amely mindkét ország példájában látható volt – alapvető és megkerülhetetlen a vagyonvisszaszerzés hatékonyságához. Magyarországon jelenleg egyetlen esetben van a bizonyítási teher megfordítására lehetőség a büntető törvénykönyvről szóló 1978. évi IV. törvény 77/B § (1) bekezdés b) pontja, valamint a (4) bekezdés alapján, azaz amennyiben a vagyonelkobzást arra a vagyonra rendelik el, amelyet az elkövető a bűnszervezetben való részvétele ideje alatt szerzett. Távlati célként megfogalmazható, hogy az angol példához hasonlóan minden egyes esetben, amikor vagyonelkobzás elrendelésére kerül sor, forduljon meg a bizonyítási teher.

Az is nyilvánvaló, hogy a meglehetősen szigorú szankciórendszer és a felderítési gyakorlat tudatosságának erősítése és a jogszabályok maradéktalan alkalmazása terén mindkét ország gyakorlata példaértékű számunkra. Mindkét országban nagy hangsúlyt helyeznek a képzésekre és továbbképzésekre, nemcsak rendőri, hanem ügyészi és bírói szinten is, illetve a gyakorlati tapasztalatokat is rendszeresen megosztják egymással a különböző fórumokon. Különösen hangsúlyozzák, hogy a rendőri munkán belül ez egy speciális, elkülönült terület, ahol ennek megfelelő tudásra van szükség, és ehhez igazodva Angliában például ezt ügyészi szinten is érvényesítik, így napi kapcsolatban, sőt egy irodában dolgozik a vagyonfelderítéssel foglalkozó nyomozó és ügyész. A szigorú szankciórendszernek az az alapvető feladata, hogy az elkövetőnek „ne érje meg” bűncselekményeket elkövetni, ne lehessen bűncselekmények elkövetéséből vagyonokat felhalmozni, elrejteni.

Mindkét országban nagyon jó az együttműködés a különböző rendőri szervek és szintek között, és felismerték, hogy az adó- és a vámhivatallal való együttműködés elengedhetetlen az eredményességhez. Magyarországról ez sajnos nem mondható el, ami részben a jogi szabályozásra vezethető vissza, például az adótitokra vonatkozó szabályok esetében.

Magyarország esetében elmondható, hogy ezt a speciális területet és a jogi lehetőséget nem használják megfelelően a gyakorlatban, ezt támasztja alá a vagyonvisszaszerzés igen alacsony statisztikai aránya, holott már a szabályok szélesebb körű alkalmazásával nagymértékben növelhető lenne a hatékonyság.

A későbbiekben a munkánk során felmerülő hazai jogi és gyakorlati nehézségeket és azok megoldási javaslatait ismertetjük.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp116-129

SZIKINGER ISTVÁN

Al Capone karrierjének vége

Al Capone nevét két dolog miatt szokták emlegetni. Az egyik: ő volt a XX. század szervezett bűnözésének egyik „alapító atyja". A másik: soha nem tudták felelősségre vonni az általa vélhetően elkövetett igen súlyos bűncselekmények többsége miatt. Az ártatlanság vélelme őt is megilleti, ezért a bűnösségéről a jogerős ítéletben megállapítottakon túlmenően nem illik, nem is szabad szólni. Mindazonáltal megjegyzendő, hogy a korabeli szakmai és társadalmi tapasztalat és megítélés szerint a „vélhetően" szó helyett inkább a „nyilvánvalóan", illetve „köztudottan" kifejezéseket kellene használni. De nem tehetjük. Végül „csupán" adócsalás miatt tudták keményebben megbüntetni. Azért az sem valami csekélység volt: tizenegy év szabadságvesztésre ítélték.

Az FBI 2000-ben oldotta fel az Al Capone ügyeiben keletkezett anyagok titkosítását, egyben a világhálón is hozzáférhetővé téve őket.[1] Tanulságos dokumentumok ezek, megerősítik a közfelfogást az erőszakos bűncselekményekkel, valamint az illegális üzletekkel (szerencsejáték, prostitúció, szeszkereskedelem) kapcsolatos eljárások sikertelenségének okáról. Azt tudniillik, hogy a maffiavezér lefizette, markában tartotta az egész chicagói rendőrséget. Nem arról van tehát szó, hogy nem tudták: valójában legtöbbször nem is akarták elfogni, vonakodtak attól, hogy eljárást indítsanak ellene. Igaz persze az is, hogy jellemzően tanúk sem akadtak, akik a gengsztervezér ellen tettek volna vallomást. Az adócsalás miatti elítélésre is megvan a magyarázat: abban ugyanis nem a helyi rendőrség, hanem a szövetségi adóhatóság járt el, annak az embereit pedig – úgy tűnik – már nem sikerült „megdolgoznia".

A huszadik századi gengszter prototípusa

Al Capone azért lehetett a maga kategóriájában kiemelkedő és meghatározó személyiség, mert a megfelelő ember volt a megfelelő helyen és időben. 1920-ban hatályba lépett az Egyesült Államokban a Volstead Act, amelyben

1 http://foia.fbi.gov/foiaindex/capone.htm

a Kongresszus megtiltotta az alkoholtartalmú italok előállítását, forgalmazását, az országba történő behozatalát, onnan való kivitelét, valamint a szövetségi állam területén való szállítását is. Ezzel a továbbra is nyilvánvalóan meglévő kereslet és a hivatalosan elismert kínálat között olyan ellentmondás keletkezett, amely törvényszerűen megnyitotta a lehetőséget az illegális termelés, valamint kereskedelem előtt. Mivel pedig ezek a tevékenységek nyereségesen csak vállalkozási formákban valósulhatnak meg, gyakorlatilag a törvény által el nem ismert tömeges szükséglet vezetett a huszadik századi szervezett bűnözés jellemző kereteinek kialakulásához.

Alphonse Gabby May Capone 1899-ben született a New York állambeli Brooklynban. Édesapja és édesanyja hat évvel korábban vándorolt ki Olaszországból az Egyesült Államokba. A család nem nyomorgott, de szerény körülmények között élt. Alphonse-nak hat testvére volt. Iskolai tanulmányait 14 éves korában abbahagyta, mert összetűzésbe keveredett az egyik tanárnővel. A rendelkezésre álló források szerint[2] sérelmezte a származása miatti hátrányos megkülönböztetést, amellett érzékelte az „amerikai álom", vagyis a jólét és az őt körülvevő valóság közötti ellentmondást. Egy *Johnny Torrio* nevű bűnözőnek kezdett dolgozni. Adósságokat hajtott be, és egy bárban tevékenykedett kidobóemberként. Itt vágta meg valaki késsel az arcát, ezért kapta a *Sebhelyes arcú* gúnynevet.

1918-ban megnősült. A következő évben – egy emberölési ügy vádját elkerülendő – Chicagóba ment, ahová Torrio is áttette székhelyét. Az „ötpontos" (Five Points Gang) bandában Al Capone gyorsan haladt előre a ranglétrán, gyakorlatilag a vezér: Torrio jobbkeze volt. Itt tapasztalta meg az ügyek „elsikálásának" lehetőségét is: többször őrizetbe vették, de Torrio mindig el tudta intézni, hogy szabadon bocsássák. Néhány év múlva a főnök úgy döntött: visszatér Olaszországba, ezért az akkorra már igen nagy hatalomra szert tevő bandát Alphonse-ra hagyta.

Al Capone az alvilági erények – kegyetlenség, célratörés, a vesztegetés képessége stb. – mellett elsősorban szervezőkészségével emelkedett ki. Ezzel nőtt a bűnözői világ átlaga fölé, valóban jelentős mértékben hozzájárulva a vállalkozásszerűen működő kriminális csoportok megszületéséhez. Tevékenysége átfogta a gengsztervilág szokásos ügyleteit: a prostitúció és a szerencsejátékok szervezését, no meg „természetesen" az erőszak alkalmazását, a gyanú szerint beleértve szükség esetén az emberölést is. Mindamellett az elsők között ismerte fel a legális üzletek fenntartásának szükségességét. Ez

2 http://www.notablebiographies.com/Ca-Ch/Capone-Al.html

egyrészt a bűnös úton megszerzett pénz tisztára mosását szolgálta. Szinte a szó szoros értelmében, mivel Al Capone automata mosodákat üzemeltetett, nyilván a gépekbe dobandó készpénz elszámolhatósága miatt. Népszerű magyarázat szerint innen ered a „pénzmosás" kifejezés. Valójában azonban ez a megjelölés csak jóval később, a XX. század második felében terjedt el. A törvényes üzletek másrészt az elismert társadalmi státust, a „szalonképességet" is előmozdították. Al Capone esetében közismert volt ugyan valódi foglalkozása, üzletemberként mégis megjelenhetett olyan rendezvényeken, részt vehetett olyan megbeszéléseken, ahol elvárható volt a jelenlét indokolása. Jó kapcsolatokat ápolt Chicago polgármesterével is, aki azonban a húszas évek végén már úgy látta: karrierjének nem tesz jót az alvilági vezérrel fenntartott szívélyes viszony. Új rendőrfőnököt alkalmazott, aki nem tartozott Al lefizetett emberei közé. A gengszter 1928-ban Floridában vásárolt házat, és oda költözött, de tovább folytatta chicagói tevékenységét.

Al Capone már életében legendává vált. Az általa és emberei részéről – vélhetően – elkövetett bűncselekmények érthetően nagy publicitást kaptak. Ráadásul olyan deliktumokról van szó, amelyek a korabeli nyomozási módszerekkel is feltárhatók, bizonyíthatók lettek volna. Egy vele szemben terveket kovácsoló banda vezéreit például fogadásra hívta meg, majd az ajándék módjára becsomagolt bunkóval a senki által nem cáfolt gyanú szerint szétverte a fejüket. Leghírhedtebb akciója a Valentin-napi mészárlásként elhíresült leszámolás volt. 1929. február 14-én rendőri akciónak álcázott, egyenruhás bandatagok által végrehajtott kivégzés áldozatává vált egy – sőt akkor már lényegében az egyetlen – rivális csoport hét tagja. Érdekes, hogy sokan elhitték: valóban a rendőrség követte el a gyilkosságokat. A fegyverszakértő azonban megállapította: nem a testületnél rendszeresített fegyverekből dördültek el a lövések.

A szervezett bűnözés történetében jelentős esemény volt az 1929-es Atlantic City-beli konferencia, amelyet azért hívtak össze, hogy egyeztessék a különböző bandák tevékenységét. *Nucky Johnson*, a helyi csoportok elismert főnöke készítette elő a rendezvényt. A gengszterek álnéven jelentkeztek be a szállodába, Al Caponét azonban felismerték, így őt és társait nem engedték be. Egy másik hotelba ment az egész társaság, ahol azután meg tudták tartani a tanácskozást. Valójában egy nagy nemzeti bűnözői szindikátus létrehozására irányuló kezdeti lépésekről volt szó. A résztvevők megbeszéléseket folytattak az együttműködés különböző lehetőségeiről, az akkor már nyilvánvalóan kudarcot szenvedő szesztilalom feloldása (ami csak öt évvel később következett be) utáni helyzet kezeléséről, a profit legalizálásának módozatairól.

A Szövetségi Nyomozó Iroda hatásköre a múlt század első felében igen korlátozott volt, az Al Capone nevével fémjelzett leszámolások ügyeiben például nem járhatott el. Az intenzívebb felderítő tevékenység akkor kezdődött el, amikor Al Capone idézés ellenére nem jelent meg egy szövetségi nagyesküdtszék *(Grand Jury)* előtt. Itt meg kell jegyezni, hogy az Egyesült Államokban a közhatalom különösen érzékenyen reagál az igazságszolgáltatással szemben tanúsított jogellenes magatartásokra. A bandavezérnek 1929 márciusában kellett volna egy szövetségi nagyesküdtszék elé állnia, amit azonban elmulasztott. Ügyvédei segítségével igazolta távolmaradását, másodszor azonban már nem engedhette meg magának ugyanazt. Akkor elrendelték őrizetbe vételét, de óvadék ellenében megúszta a fogva tartást.

A nagyesküdtszék 25 tagból álló testület (ellentétben az általában 12 fős „kisesküdtszékkel"), és lényegében a bűnösség kérdésében dönt. Feladata, hogy határozzon a bírósági eljárás megindításáról, vagyis a vádemelés megengedhetőségéről.

A pénzügyi nyomozás és a bírósági eljárások

Az adócsalás gyanúja miatti szövetségi nyomozást az tette lehetővé, hogy az Egyesült Államok legfelsőbb bírósága elvi éllel kimondta: a jövedelem keletkezésének jogellenessége nem mentesít a pénzügyi kötelezettségek teljesítése alól. Az önvád tilalma nem jelenti azt, hogy bárki megtagadhatná a valóságosan keletkezett jövedelmének a bevallását arra hivatkozva, hogy ellenkező esetben bűncselekmény elkövetésével vádolná magát. Az ügyben konkrétan a szesztilalmi törvény megszegésével keletkezett bevételek adóalapba tartozásáról volt szó[3].

1928-ban el is rendelték a nyomozást, amely az adóhivatal hatáskörébe tartozott. Az ügy előadója a rámenősségéről ismert *Frank J. Wilson* lett. A chicagói gengszter elleni ügyön kívül a Lindbergh-bébi elrablásával kapcsolatos felderítésben vált ismertté a neve, egyebek mellett azzal, hogy feljegyezte a váltságdíjként átadott bankjegyek számát, ami azután igen jelentős bizonyítékokhoz vezetett. Mivel a jövedelmek keletkezése elválaszthatatlan volt Al Capone más, kriminálisnak tekintett tevékenységeitől, ezért az eljárásban sok olyan cselekményt is fel kellett deríteni, amelyek kapcsolódtak ugyan a nyomozás tárgyához, de vizsgálatuk nem tartozott az adóhatóság

3 United States v. Sullivan, 274 U.S. 259 (1927)

jogkörébe. Az már valószínűleg nem lepi meg az olvasót, hogy Al Capone meg akarta öletni Wilsont, erről azonban végül társai lebeszélték.

Wilson először 1931. március 27-én levélben foglalta össze az ügy állását a washingtoni vezetésnek. Ebben leírta, hogy az egyik bizonyítandó tény egy szerencsejáték-barlang tulajdonlása volt. A létesítmény két év alatt több mint félmillió dollár nyereséget termelt. A beszámoló utalt azokra a vallomásokra, amelyekben a tanúk elmondták: Al Capone saját tulajdonaként beszélt a játékteremről. Wilson egy 1925-ös vizsgálati jelentésre is hivatkozott. Abban egy *David A. Morgan* nevű városi tisztviselő számolt be arról, hogy ellenőrizni kívánták a helyet, ezért razziát tartottak a seriff segítségével. A jelentés szerint az akció megkezdése után néhány perccel megjelent Al Capone, és közölte: ő itt a tulajdonos, több razzia pedig nem lesz. Egy hónappal később a gengszter emberei otthona előtt lelőtték Morgant, ő azonban nem halt bele a sérüléseibe. A történtekből viszont levonta a tanulságot, és kijelentette: nem egészséges dolog Al Capone játéktermében razziázni. Nem is volt ott több ellenőrzés és kutatás.

1931. április 8-án Wilson újabb levelet írt főnökének, amelyben azt latolgatta, hogy a célszemélyt szükséges-e, célszerű-e bűnszövetség *(conspiracy)* létrehozásával és fenntartásával is megvádolni. Az ügynök kifejtette, hogy egy *Louis Alterie* nevű ember segítségével talán bizonyítani tudják ezt a társas elkövetői alakzatot. Ő ugyanis az említett, Hawthorne Smoke Shop nevű játékbarlang működtetéséhez kapcsolható. Korábban valótlannak bizonyuló nyilatkozatot tett, ezért hamis tanúzás miatt folyt ellene eljárás. Frank Wilson megemlítette a levélben, hogy a terheltet egy *Hess* nevű ügyvéd védi, aki korábban ügyészként tevékenykedett. Ő nem gengszter-ügyvéd, jegyezte meg a levél írója, ezért remélhető, hogy betartja ígéretét: az igazság elmondására ösztönzi védencét. Ebben az esetben lehet szó a hamis tanúzás miatti vád elejtéséről.

1931. július 8-án *Hodgins*, *Westrich* és *Clagett* ügynökök írtak egy összefoglaló jelentést a nyomozás vezetőjének. A bevezetőben kifejtették, hogy Al Capone az Egyesült Államok leghírhedtebb gengsztere. Egy bűnözői szindikátus vezetőjeként közreműködött sör és más alkoholtartalmú italok előállításában, játéktermeket üzemeltetett, valamint bordélyházak működtetésében is szerepet játszott. Az anyag szerzői kiemelték, hogy Al Capone neve a megelőző években minden jelentősebb bűncselekmény kapcsán felmerült. Ezek egy része igaz lehet – tették hozzá. Leírták, hogyan emelkedett a gengszter-vezér az alvilági ranglétrán. A jelentés szerint nem kétséges, hogy Al Capone Chicagóban az egész rendőrséget lefizette, ezért nem fogták el soha. Egy

alkalommal csavargás miatt őrizetbe vették, de el kellett engedniük, mert az derült ki, hogy a városban egyetlen rendőr sem ismeri. Pénzügyi oldalról is nehéz volt megfogni, mert soha nem volt bankszámlája. Tranzakcióit is jórészt tanúvallomásokkal kellett felderíteni és bizonyítani.

1933. december 21-én Wilson összefoglaló jelentésben rögzítette az Al Capone elleni adócsalási vádat megalapozó tényeket, kitérve a gengszter egyéb tevékenységére is. Leírta, hogy az 1924-es választásoktól kezdődően a bűnszervezet gyakorlatilag zavartalanul működhetett Chicago egyik külvárosában: Ciceróban. 1926. április 26-án meggyilkoltak egy *William McSwiggen* nevű államügyészt, aki korábban az Al Capone nevéhez kapcsolt emberölések ügyében hallgatott ki tanúkat. Akkor házkutatást is végeztek, amelynek során megtalálták a játékbarlang bevételeit tartalmazó feljegyzéseket. Ezt a nyomozás anyagához csatolták, egyebekben azonban érdemben nem foglalkoztak vele. Sikerült megállapítani, hogy a bejegyzések részben egy *Leslie A. Shunway* nevű embertől származtak, aki a (feltételezett) bűnszervezet tagja volt. Wilson felkutatta őt, és vallomást is tett. Ez volt az első jelentős bizonyítási eszköz az adócsalás miatti eljárásban. 1931 februárjában Shunway megjelent Chicagóban a nagyesküdtszék előtt, és azonosította az említett bevételi adatokat. Kiderült, hogy a tanú valójában pénztárosként dolgozott a bandának, ezért az általa mondottak különösen értékesek voltak a bizonyítási eljárásban. Vallomásában részletesen elmondta, hogy a játékteremben lóversenyfogadásokat lehetett kötni, rulett és kockajátékok, huszonegyezés, valamint pókerjátszmák folytak.

Beszámolt arról is, hogy 1925-ben egy alkalommal éppen a helyszínen tartózkodott, amikor razziát tartottak. A rendőröket *Hoover* tiszteletes (nem azonos az FBI vezetőjével, Edgar Hooverrel) is elkísérte. Le kívánták foglalni azt a pénzt, amely akkor az ottani ügyletekkel kapcsolatban ott feltalálható volt. Ekkor megjelent Al Capone, pizsamanadrágban és egy kabátban. Utasította Shunwayt, hogy vegye magához az összegeket. Az utasítást a pénztáros teljesítette. Véleménye szerint a bejegyzések pontosak voltak, hiszen emlékezett: a „könyvelést" részletesen, az egyes játékfajtákra lebontva kellett végeznie, a bevételből levonták a bér- és egyéb költségeket.

Wilson az összefoglaló jelentésben rögzítette: McSwiggen államügyész meggyilkolásának éjszakáján Al Capone eltűnt. A rendőrség összefüggésbe hozta őt az emberöléssel, körözést adtak ki ellene, és intenzíven keresték. Hónapokkal később került elő, akkor viszont már a rendőri vezetők úgy nyilatkoztak, hogy nincs ok az őrizetbe vételére, nincs bizonyíték arra, hogy bármilyen szerepe lett volna a súlyos bűncselekményben. Mivel egyértelműen a bandát

tartották felelősnek az államügyész haláláért, és kilátásba helyezték a fellépést a csoport ellen, a játékbarlang működését azonnal megszüntették, Shunway pedig kollégáival gondoskodott a megmaradt készpénz biztonságba helyezéséről. A hullámok elültével azután a vállalkozás visszatért Ciceróba, és ugyanott folytatták, ahol abbahagyták. Vallomásában Hoover tiszteletes szintén beszámolt a razziáról. Visszaemlékezett arra, hogy annak során Al Capone félrehívta, és félreérthetetlen ajánlatot tett. Először busás adományokról beszélt, amelyeket természetesen az egyháznak nyújtana, később pedig arról, hogy az egyik területről visszavonulna, ha cicerói működését nem zavarnák a továbbiakban.

Hoover tiszteletes a saját vallomása szerint határozottan visszautasította a korrupciós közeledést, és a gengsztert jogtisztelő magatartás tanúsítására szólította fel. Közölte: mindent átad a seriff helyettesének. A gengszter a játékterem berendezési tárgyaira mutatva kijelentette: „ez mind az enyém". Mire Hoover: „azok is mennek".

Hoovernek a városban betöltött tisztségénél fogva joga lett volna őrizetbe vételi engedélyt *(warrant)* kérni, és úgy emlékezett – bár ebben nem volt biztos –, hogy ezt meg is tette. Elmondása szerint annyi bizonyos, hogy a rendőrök nem akadályozták meg Al Capone eltávozását a helyszínről. Azt is elmondta, hogy a gengszterek a razzia részt vevői közül többeket tettleg bántalmaztak. A támadókat őrizetbe vették, ez azonban nem akadályozta meg a banda tagjait a további tettlegességben.

Egy *Chester Bragg* nevű ingatlanügynököt ugyancsak tanúként hallgattak ki a razzia lefolyása ügyében. Elmondta, hogy a rendőrök lezárták az épület közvetlen környékét, őt pedig azzal bízták meg, hogy őrizze a bejáratot: senkit ne engedjen ki vagy be. Al Capone azonban közölte vele, hogy ő itt a tulajdonos, ezért az őr nem gátolta meg, hogy belépjen. A továbbiakban a szerencsejáték-berendezések elszállítása zajlott, majd a razziában részt vevők távoztak a helyszínről. Bragg szerint ekkor került sor a bántalmazásokra a bandatagok részéről, ő maga is kapott ütéseket. Vérző orral sikerült elmennie. A bandavezér és Hoover közötti beszélgetésről csak hallomásból tudott, azt azonban megerősítette, hogy ő több fenyegetést kapott az akció folyamán. Valamennyiszer arra szólították föl, hogy hagyja ott a helyszínt, fejezze be az ottaniak zaklatását. Az épületben a hatósági emberek a falhoz állították a játékbarlang személyzetét, ezért nekik Al Capone ott nem tudott parancsokat adni, a helyzetből és a bandavezér magatartásából, valamint szavaiból is egyértelműen az tűnt ki azonban, hogy általa működtetett intézményről van szó. Leslie A. Shunway ismertetett nyilatkozatából azonban tudjuk, hogy Alnak mégis sikerült kiadnia néhány fontos utasítást.

Bragg beszámolt arról, hogy a későbbiekben jelen volt az ügy bírósági tárgyalásán, ahol Al Capone és társai – többek között a testvére, Ralph – az igazságszolgáltatás előtt magabiztosan, tulajdonosként viselkedtek. Nyomatékosan közölték vele, hogy olasz barátaik jelentek meg hallgatóságként, ezzel adva tudtára: jobban tenné, ha elmenne.

Vallomást tett a már említett David Morgan is. Közölte, hogy felismerte Al Caponét. Davidson hadnagyhoz, az akció rendőri parancsnokához kísérte, ott hangzottak el azok a fenyegető szavak, amelyekről Wilson nyomozó már korábbi levelében is beszámolt. Morgan egyébként szintén felidézte, hogy a razzián orrba vágták, orvoshoz kellett mennie.

Az összefoglaló jelentés rögzítette, hogy a létesítmény mintegy fél órával a razzia után már ismét üzemelt anélkül, hogy a városi hatóságok ez ellen bármit tettek volna, egészen az államügyész meggyilkolásáig. A Morgan elleni későbbi emberölési kísérlet tetteseit nem sikerült felderíteni. Amint arról szó volt, a McSwiggen elleni merénylet után néhány hónap szünet következett, majd újra indult a biznisz. Ekkor egy *Fred Ries* nevű embert alkalmaztak pénztárosnak, vezető szerepet játszott továbbá *Jack Guzik*, aki Al Capone személyes pénzügyi megbízottja volt. Riest nem volt könnyű felkutatni, mert – mint utólag kiderült – a szervezet Kaliforniába akarta küldeni annak megakadályozása céljából, hogy a vád tanúja legyen. Éppen Los Angelesbe indult volna, amikor Wilson nyomozó rátalált a Missouri állambeli St Louisban. A jelentés szerint Ries halálfélelemben volt, és közölte: retteg attól, hogy vallomása miatt a szervezet utoléri, és megtorolja az igazságszolgáltatás segítését. Ebből adódóan azután ügyesen tagadott minden olyan tényt, amelyet Al Capone és a bűnözői csoport más vezetői ellen fel lehetett volna használni. Wilson ekkor úgy döntött, hogy őrizetbe veszi Riest. Erre az úgynevezett fontos tanúkról *(material witnesses)* szóló törvény adott lehetőséget. Az Egyesült Államok büntetőeljárásába már az 1789-es igazságszolgáltatási törvény bevezette ezt a sajátos felhatalmazást. Amennyiben egy nyilatkozatot tartalmazó hitelesített okirat *(affidavit)* áll rendelkezésre arról, hogy valakinek a tanúvallomása lényeges lehet az ügy eldöntése szempontjából, emellett valószínűsíthető, hogy idézésre nem jelenne meg a nagyesküdtszék vagy a bíróság előtt, akkor őrizetbe vehető. Van lehetőség arra, hogy biztosíték letétele mellett a tanú szabadlábra kerüljön. Ries esetében ezt tizenötezer dollárban határozták meg, de képtelen volt a megfizetésére. Szabadságelvonását mindazonáltal titokban tartották, mert a bűnüldöző szervek attól féltek, hogy Capone vagy emberei leteszik a szükséges összeget, Ries pedig nem jelenik meg a meghallgatásokon, illetve a tárgyalásokon.

Fogva tartása alatt Riest meglátogatta Wilson nyomozó egy kollégájával. Sikerült rávenniük arra, hogy azonosítsa a rendelkezésre álló pénzügyi dokumentumokat, és elmondja, hogy azok milyen összefüggésben álltak Al Capone és bandája tevékenységével. Ries beszélt a szervezet felépítéséről, a vezetők szerepéről, valamint arról, hogy a tiszta nyereséget Guziknak adta át. Esküvel megerősített, igen részletes vallomásában tényszerűen leírta a játékterem működtetésének mechanizmusát, a pénzügyi elszámolások rendjét. Megjelölte az egyes feladatköröket, valamint a hozzájuk tartozó személyeket is.

A találkozó után a bűnüldöző hatóság munkatársai intézkedtek a tanú szabadon bocsátásáról, mivel a tárgyalásig igen sok idő volt még hátra. Wilsonék azonban attól tartottak, hogy a hosszú bennlét alatt Ries ellenük, illetőleg az igazságszolgáltatás ellen fordul, és az ügy szempontjából ismét használhatatlanná válik. Mindazonáltal természetesen a védelméről is gondoskodni kellett, hiszen semmilyen szempontból nem volt kívánatos, hogy volt munkatársaival, illetőleg azok főnökeivel találkozzon. Ezért – miután megtette a társaira és főnökeire terhelő vallomását, Dél-Amerikába küldték, fedezve az utazás és az ottani tartózkodás költségeit.

Természetesen magát Al Caponét is meghallgatták, először csupán adóügyi eljárásban. Mindazonáltal megtörtént a figyelmeztetés (bár akkor az még nem volt törvény által előírt feltétel, különösen nem a büntetőeljáráson kívül): amit mond, az adott esetben ellene is felhasználható a bűnüldöző hatóságok és bíróságok előtt. Az adózó jogi képviselőt hatalmazott meg, és közölte: majd ő fog válaszolni minden kérdésre. *Lawrence P. Mattingly* ügyvéd a meghallgatáson mindenekelőtt kifejezte abbéli reményét, hogy az adóügyi eljárás minél előbb lezárul. Készségesnek mutatkozott a szükséges adatok rendelkezésre bocsátására. Miután teljesen nyilvánvaló volt a büntetőeljárás lefolytatására irányuló szándék, a jogi képviselő valószínűsíthetően annak elhárítása vagy a lehetséges következmények enyhítése céljából egy levelet csatolt. Ebben Al Capone beismerte, hogy 1925 és 1928 között (az utóbbi évet is magába foglalva) igen jelentős adóköteles jövedelme volt. A levél ezen túlmenően tartalmazta azt is, hogy a bevételeket és nyereséget megalapozó tevékenységben kik voltak az üzlettársai. Közülük *Jack Guzik*, *Frank Nitto* és a testvére, *Ralph Capone* neve érdemel említést. Egy másik feljegyzés az ügyvédtől származik, abban az 1929-es jövedelmekre vonatkozóan találhatók fontos adatok.

Ezeket az iratokat a későbbiekben a vád eredménnyel használta fel az Al Capone ellen adócsalás miatt induló eljárásban.

A nyomozás során megállapították, hogy a terhelt jelentős jövedelme részben a prostitúció szervezéséből és működtetéséből származott. Az egyik

nagyobb bordélyház az Illinois államban lévő Stickney város területén működött Harlem Inn néven. Megjegyzendő, hogy Al Capone éppen erre vonatkozóan mondta az említett razzia idején Hoover tiszteletesnek: hajlandó onnan kivonulni, ha a cicerói játékbarlangját békén hagyják.

Az államügyész megölése után az említett nyilvánosházban is kutatást tartottak azért, hogy megtalálják a bűncselekménnyel gyanúsítható Caponét. A férfi nem volt ott, de lefoglaltak lőfegyvereket, dinamitot, szeszes italokat, valamint a prostitúcióból származó jövedelemre vonatkozó feljegyzéseket. Bírósági eljárás is indult, amelynek következtében megtiltották a Harlem Inn további működtetését. Ennek azonban az érintettek nem tettek eleget az adónyomozás időszakában. Sikerült felderíteni egy *John Grigus* nevű tanút, akinek fűtésszerelési vállalkozása volt. Azonosított egy megtalált számlát, határozottan kijelentve, hogy azt Al Capone egyenlítette ki.

A nyomozás folyamán megállapították, hogy a közelben egy Shadow Inn nevű másik bordély is működött, ugyanazon üzemeltetői körrel. A lányokat időnként cserélték is a két ház között. Bizonyítékok támasztották alá – de enélkül ez egyébként is elképzelhetetlen lett volna másképp –, hogy az intézményekről a helyi rendőrség tudott, sőt védettséget nyújtott nekik. 1931. május 30-án egyidejűleg tartottak razziát a két nyilvánosházban, ennek nyomán fontos bizonyítási eszközöket foglaltak le. Wilsonék a telefonlehallgatások anyagából tudták, hogy a Harlem Inn területén még az előző napon is volt egy géppisztoly, ezt azonban a razzia idején már nem sikerült fellelni. Az összefoglaló jelentés itt megjegyzi, hogy a titkos felvételeket nem az adott ügyben nyomozó hatóság rögzítette, de azt a társszervektől törvényes keretek között kapták meg. A prostitúciós ügyben a bírósági tárgyaláson egyébként *Louis Constantino*, a Harlem Inn vezetője beismerő vallomást tett, hasonlóképpen bűnösnek vallotta magát négy kéjhölgy.

Ügyészi kihallgatásakor Al Capone beismerte, hogy a szerencsejátékok szervezéséből jelentős jövedelemre tett szert. Elmondta azt is, hogy számos pénzügyi tranzakcióját *A. Costa* álnéven bonyolította le. Ezt megerősítette egy *Parker Henderson* nevű tanú, a gengszter által lakott Ponce de Leon Hotel tulajdonosa is. Henderson elmondta, hogy gyakran kaptak átutalást a már akkor is működő Western Union útján. A pénzek jelentős részét Al Capone a feleségének továbbította. A tanú arról is beszámolt, hogy ő vásárolt Capone részére hat revolvert. Ez azért lényeges, mert az egyiket megtalálták a banda számláját terhelő egyik áldozat mellett. A fegyver azonosítása alapján akkor Hendersonhoz jutottak el, és emberölés miatt vádat emeltek ellene. Capone és emberei azonban akkor megnyugtatták: nem fogják elítélni. Így is történt:

a későbbiekben ejtették az ellene felhozott vádat. A pénzátutalásokkal kapcsolatos kijelentéseket egy *Catherine Gaines* nevű tanú is alátámasztotta.

Wilson az általa írt jelentésekben nem utalt arra, hogy az említetteken túlmenően is szereztek volna információt. A *Collier's* magazin 1947. április 26-i számában azonban felfedte, hogy az Al Capone köreiben mozgó informátor, *Edward J. O'Hare* régóta segítette a munkájukat. Az informátor ügyvéd volt, amellett üzleti érdekeltségei miatt is szükségesnek látta, hogy jó kapcsolatokat építsen ki a Chicagót uraló bandával. 1939-ben gépkocsijában agyonlőtték. A két tettes elhajtott, az ügy máig felderítetlen maradt. Érdekes tény mindenesetre, hogy néhány hónappal a gyilkosság után Frank Nitto, Al Capone jobbkeze feleségül vette az informátor menyasszonyát. Még egy dolgot érdemes megemlíteni O'Harével kapcsolatban: fia, *Edward Henry* („Butch") *O'Hare* a második világháború egyik légi csatájában életét vesztette. Róla nevezték el a chicagói nemzetközi repülőteret.

Az adónyomozók széles körben felderítették, mire fordította Al Capone az illegálisan megszerzett jövedelmét. Az ingatlanvásárlásoktól kezdve egészen a bútorok vételéig igen sok ügyletet azonosítottak és bizonyítottak. A szervezet vezetéséhez tartozó Frank Nittót is megvádolták adócsalással. Elrendelték letartóztatását is, ő azonban eltűnt. A sajtó nevetségesnek tartotta, hogy a hatóságok ennyire képtelenek érvényt szerezni a törvénynek. A chicagói kereskedelmi kamara díjat ajánlott a nyomravezető számára. Végül Wilsonék derítették fel a keresett személy tartózkodási helyét.

1931 februárjában bírálták el Al Capone igazságszolgáltatás elleni ügyét (amiért nem jelent meg a szövetségi nagyesküdtszék előtt), majd ugyanazon év októberében került sor az adócsalás miatti vád miatti bírósági tárgyalásra.

Az Al Capone és társai elleni adónyomozás egyértelműen sikeresnek minősíthető. Hangsúlyozni kell, hogy nem csupán a „nagyfőnök", hanem a társai ellen is igen kiterjedt, részletekbe menő adatgyűjtést, elemzést és értékelést végeztek a hatóság képviselői. A lefolytatott eljárások alapján végül 47 ember ellen emeltek vádat.

A chicagói vezér védői vádalkut ajánlottak. Az ügyészséget tájékoztatták arról, hogy védencük hajlandó beismerő vallomást tenni, ha a büntetés mértéke számukra elfogadható lesz. A vádhatóság belement a megállapodásba. Azt ígérték az ügyészek, hogy kettő és öt év közötti szabadságvesztés kiszabására tesznek majd indítványt. Ennek az volt az oka, hogy az igen alapos nyomozás, a rendelkezésre álló számos bizonyíték ellenére voltak aggályok az ügy kimeneteléről. Felvetődött például egyes cselekmények büntethetőségének elévülése, a nagyesküdtszék az utolsó pillanatban szakította meg azt az

1924-es tényállásokra vonatkozóan. Az is tudott volt, hogy a védelemben részesített két tanú, Shumway és Reis fejére Al Capone vérdíjat (mindegyikük esetében ötvenezer dollárt) tűzött ki, márpedig az ő vallomásuk rendkívül fontos volt a bizonyítási eljárásban. A vádhatóság pedig nem akart kockáztatni. A megállapodásról a sajtó tudomást szerzett, a közvéleményt felháborította az alku.

Tudni kell, hogy a vádalku nem törvényben szabályozott intézmény. Az eljáró bíró a vádlott legnagyobb megrökönyödésére kijelentette, hogy ilyen egyezségnek a szövetségi bíróság előtt nincs helye. Ez után Al Capone visszavonta a beismerő vallomását. Az ítélet: tizenegy év szabadságvesztés.

1931-ben arra derített fényt a nyomozás, de a bíróság is észlelte, hogy Al Capone tanúkat vett rá hamis vallomások megtételére. Ezen túlmenően személyi testőre, *Phillip D'Andrea* tiltott fegyverviseléssel volt gyanúsítható, mivel a tárgyalóteremben is töltött pisztolyt tartott magánál. D'Andrea hat hónap letöltendő szabadságvesztést kapott. A bizonyítékok hatására az ítélet indokolásában a bíróság úgy fogalmazott: vak lett volna, ha nem veszi észre a tanúkra nehezedő nyomást, megfélemlítésüket.

Büntetésének letöltését Al Capone Atlantában kezdte meg, viszonylag jó körülmények között. 1934-ben átszállították a hírhedt Alcatrazba, ahol már nem élvezte a korábbi kedvezményeket. 1939-ben jó magaviselete miatt szabadult. Ekkorra egészségi állapota már nagyon rossz volt. Szifilisze miatt részlegesen lebénult, elmeállapotában is leépülés volt érzékelhető. Először egy Baltimore-i kórházban kezelték, majd floridai birtokán töltötte élete utolsó éveit. Volt bűntársai felvették vele a kapcsolatot, de ő már soha nem tért vissza a szervezett bűnözés világába. 1947-ben agyvérzést kapott, majd tüdőgyulladásban halt meg.

A nyilvánosság

Amint arról szó volt, Al Capone a XX. század szervezett bűnözésének a maga módján kiemelkedő alakja, egyik alakítója. A média természetesen mindig érdeklődött a kriminalitás és a bűnüldözés világa iránt, korszakunkra azonban a végbement technikai fejlődés olyan új lehetőségeket nyitott, amelyek szinte az egyidejűség élményét adták a közönségnek. Al Capone egyébként megpróbálta kihasználni és a maga javára fordítani a tömegtájékoztatás eszközeit. Közszerepléseket vállalt (például az elsők között üdvözölte Lindberghet az óceán átrepülése után, jótékonysági akciókat szervezett), tudato-

san építette üzletemberi imázsát. Az elkövetett cselekmények, és a hozzá, valamint a bandájához kapcsolódó gyanúsítások miatt azonban nem sikerült elfogadtatnia magát a társadalommal. Különösen a Valentin-napi mészárlás után fordult ellene a közvélemény. Így nem okozott nehézséget, hogy a Chicagói Bűnüldözési Bizottság 1930-ban „első számú közellenséggé" nyilvánította. Még életében filmeket készítettek róla.

A média egyben óriási üzlet volt, ahol természetesen konkurenciaharc is zajlott. Ezért a jó (vagy annak tűnő) értesülések gyakran az újságokban jelentek meg. Jellemző, hogy az FBI által publikált, a titkosítás alól feloldott anyagok között igen sok hírlapi közlemény, tudósítás található. Ez mindenesetre mutatja, hogy az amerikai hatóságok minősítési gyakorlata sem problémamentes. A nyilvánosságra hozott adatok titkosítása nem indokolt. Az viszont tény, hogy a bűnüldözéssel foglalkozó szervek figyeltek a megjelent írásokra, továbbá a képi anyagokra is, azokat fontos forrásként használták tevékenységük során.

A tanulságokról

Megdöbbentő az a kontraszt, amely az Al Capone elleni rendőri, illetve pénzügyi nyomozói fellépés között érzékelhető. Az előbbiről alig tudni valamit. Annyit mégis meg lehet állapítani, hogy a hírhedt gengszter nevéhez – már akkor is – kapcsolt kiemelkedően súlyos erőszakos bűncselekmények teljes mértékben felderítetlenek maradtak. Ahogyan arról szó volt, megfelelő források hiányában és jogerős bírói határozat nélkül nem állítható, hogy a sikertelen nyomozások minden esetben az általa vagy társai által elkövetett törvényszegések megtorlását akadályozták meg. Ettől függetlenül tény, hogy igen sok áldozattal járó emberölések maradtak homályban, ami teljességgel elfogadhatatlan. A múlt század húszas éveinek végére a chicagói városi vezetés is „bekeményített", határozott harcot hirdetett a kriminalitás ellen. Valódi áttörést Al Capone és bandája ügyeiben azonban még ekkor sem tudtak elérni.

Ezzel szemben a pénzügyi nyomozás bravúrosnak nevezhető. Az adott körülmények között, a bűnözői csoporton belüli konspiráció miatt, valamint a legális, követhető tranzakciók hiányában az adócsalás bizonyítása elismerésre méltó szakmai teljesítmény. Wilson és munkatársai emberfeletti erőfeszítésekkel gyűjtötték be és dolgozták fel az eredményes vádemeléshez szükséges bizonyítékokat. Kiemelést érdemel, hogy – ez a jelentésekből világosan kitűnik – végig nagy hangsúlyt helyeztek a törvényesség követelményének érvényesítésére.

A kétfajta nyomozás közötti különbség azért is figyelmet érdemel, mert teljesen nyilvánvaló: egy (vagy több) emberölés után – főleg, ha ismert az áldozat és megalapozott a gyanú a tettesek lehetséges körét illetően – mindig maradnak értékelhető nyomok. Az úgynevezett „áldozat nélküli" cselekmények („vice"; például tiltott szerencsejáték, prostitúció) esetében pedig a jogsértés a dolog lényegénél fogva olyan tömeges méretű, hogy ezért nem jelenthet igazán nagy nehézséget a bizonyítás. Az adócsalás esetében mindez már kevésbé jellemző.

Kézenfekvő, de elhamarkodott volna az a következtetés, hogy a korrupt helyi rendőrséggel szemben a szövetségi bűnüldözés határozottsága, célratörő munkája és szakmai felkészültsége hozott eredményt az adócsalási ügyben. A centralizált szervezeteken belül ugyanis szintén előfordulhat a romlottság, a központi irányítás semmire nem garancia. Jól példázza ezt, hogy éppen a maffia őshazájában, Olaszországban és éppen a szervezett bűnözéssel fenntartott kapcsolatok miatt több volt miniszterelnök ellen folyt büntetőeljárás. Magyarországon a Szervezett Bűnözés Elleni Központ volt vezetőjét ítélték el és fokozták le tábornoki rangjából.

Nem a centralizáció–decentralizáció dilemmája körül kell tehát a választ keresni. A rendőri korrupció leküzdésére mindkét struktúrában vannak eszközök, azokkal messzemenően élni kell. Olyan következtetés levonható, hogy az adónyomozók szakmai felkészültsége messze meghaladta a helyi rendőrökét, de ez sem következik automatikusan a szervezeti felállás és az irányítás különbségéből.

Az viszont sajnálatos, hogy Al Capone gyakran említett példája a felderítetlen gyilkosságokkal és az elítélés alapját jelentő adócsalással olyan téves konklúzióra is vezethet, amely szerint az emberi élet védelménél sokkal fontosabb az állam pénzügyi érdekeinek érvényesítése. Ez csak az eredményt tekintve igaz, valójában nincs adat arra, hogy ilyenfajta értékkülönbség lehet a háttérben. A rendelkezésre álló dokumentumok szerint ugyanis a helyi rendőrség a pénzügyi nyomozáshoz sem nyújtott érdemi segítséget (amelyet elvárható módon megtehetett volna), az adóhatóságnak pedig nem volt hatásköre eljárni az erőszakos és az „áldozat nélküli" bűncselekmények ügyeiben.

DOI:10.38146/bsz-ajia.2011.v59.i2.pp130-134

A hónap eseményei az EU bel- és igazságügyi együttműködése terén

(január–február)

A MAGYAR EU-ELNÖKSÉG TERVEI A BELÜGYI SZAKPOLITIKÁKBAN. 2011. január 1-jétől hat hónapig Magyarország tölti be az Európai Unió Tanácsának soros elnöki tisztségét. A trió utolsó tagjaként hazánk igyekszik befejezni, illetve továbbgondozni minden olyan ügyet, amelyek a korábbi elnökségektől ránk maradtak. Természetesen az uniós elnökség elsősorban arra jó alkalom, hogy napirendre vegyük azokat a kérdéseket, amelyek kapcsán speciálisan magyar érdekeket akarunk érvényesíteni, vagy amely területeken mi tartunk szükségesnek, fontosnak gyors, európai szintű előrelépést. A belügyi területet érintően a magyar elnökség vezető kérdése a szervezett bűnözés elleni harc terén való előrelépés. Építve a bizottság és a belga elnökség által elért eredményekre, a magyar elnökség a belső biztonság elemei közül leginkább erre az aspektusra koncentrál. Emellett elnökségi időszakunk kiemelt feladata Románia és Bulgária schengeni csatlakozásának kérdése, ez elsősorban a csatlakozással érintett tagállamokon múlik ugyan, mindazonáltal Magyarország ezt igyekszik lehetőségeihez mérten támogatni. Céljaink között szerepel a közlekedésbiztonság területén történő előrelépés is, az elnökségünk időszakában jelentős haladást szeretnénk elérni a tagállamok egyes jogsértések esetén történő hatékony információcseréjét elősegítő irányelv tárgyalásában. Ezek mellett számos kiemelt kérdés lesz napirenden, amelyekről ebben a rovatban igyekszünk e fél évben folyamatosan beszámolni.

A BEL- ÉS IGAZSÁGÜGYI TANÁCS JANUÁRI INFORMÁLIS ÜLÉSÉNEK EREDMÉNYEI. Január 20–21-én került sor a bel- és igazságügyi tanács magyar elnökség alatti első, egyúttal informális ülésére Gödöllőn. A belügyi ülésnap napirendjén alapvetően három téma szerepelt, a diskurzus a magyar elnökség által készített vitadokumentumok alapján zajlott. Az ülésen a legtöbb tagállam miniszteri szinten képviseltette magát, jelen volt *Cecilia Malmström* belügyi biztos, *López Aguilar*, a LIBE elnöke, az érintett uniós ügynökségek (Europol, Cepol, Frontex) igazgatói, a schengeni és a tagjelölt országok delegációi, valamint külön meghívottként az Interpol főtitkára és a SECI Központ igazgatója. Az informális ülések sajátossága, hogy csupán néhány, az elnökség által fontos-

nak vélt téma kerül a napirendre, így a minisztereknek alkalmuk nyílik az adott kérdés részletes megvitatására, arra, hogy a szokásosnál bővebben kifejtsék álláspontjukat. A magyar elnökség az informális ülés egyik témájaként a szervezett bűnözés elleni harc egyes aspektusainak megvitatását választotta, tekintettel arra, hogy ez a téma elnökségi prioritásaink között is hangsúlyosan szerepel. A téma kapcsán igencsak tartalmas vita alakult ki a résztvevők között, az elnökségi vitaindító anyagának megállapításai közül egyebek között az információcsere és a vagyonvisszaszerzés hatékonyságának további erősítése, valamint a szervezett bűnözés multidiszciplináris megközelítése fontosságának hangsúlyozása széles körű támogatásra talált. Az Europol, Interpol, SECI Központ részéről komplex, átfogó értékelések hangzottak el a szervezett bűnözés jelentette aktuális fenyegetésről. A bizottság kérésére felkerült a napirendre a következő többéves uniós költségvetés belügyi vonatkozásának megvitatása is, amelynek keretében az ebéd folyamán a tagállami belügyminiszterek véleménye alapján körvonalazódott a bizottság számára, mire helyeznék a hangsúlyt a tagállamok a következő többéves pénzügyi keret meghatározásakor. Jelen pillanatban az éves uniós költségvetés csupán egy százalékát fordítják a belügyi együttműködés céljainak megvalósítására, ami nem túl impozáns adat, de tudomásul kell venni azt is, hogy minden egyes kiadás indokoltságát igazolni kell, és biztosítani a ráfordítás által teremtett hozzáadott értéket. A pénzügyi válság időszakában bármilyen területen nehéz növelni az anyagi ráfordítás nagyságát, mindamellett Európa biztonságának garantálása sem sérülhet. A belügyi együttműködés területén még jobban ki kell használni az ügynökségekben lévő potenciált. A belügyminiszterek a délután folyamán a határigazgatás témakörével foglalkoztak, a vitaanyag kapcsán valamennyi delegáció kiemelte a kérdés aktualitását, és megköszönte a magyar elnökségnek a téma napirendre vételét. A vita célja az volt, hogy a tagállamok még az Európai Bizottság júniusra tervezett, az integrált határellenőrzéssel és a határbiztonsággal foglalkozó reformjavaslat-csomagja előtt ötletekkel szolgáljon, és rávilágítson arra, hogy a tagállamok álláspontja szerint melyek azok a területek, ahol változás, előrelépés, fejlesztés szükséges. A tagállamok többsége a Frontex szerepének erősítése, illetve a schengeni értékelési mechanizmus reformja mellett tette le a garast, mindazonáltal abban is egyetértettek, hogy a huszonegyedik század biztonsági próbatételeinek való megfeleléshez elengedhetetlen az új technikák bevonása a határmenedzsment területén. Utóbbi kapcsán azonban figyelemmel kell lenni a rendszerek közötti interoperabilitás megteremtésére, és el kell kerülni az ahhoz hasonló fiaskókat, amelyek például a SIS és a VIS rendszerek fejlesztésekor felmerültek.

EURÓPAI UNIÓ

IRÁNYELVTERVEZET AZ UTAS-NYILVÁNTARTÁSI ADATOK FELHASZNÁLÁSÁRÓL AZ EURÓPAI UNIÓBAN. Az Európai Bizottság február 2-án fogadta el az úgynevezett EU PNR *(Passenger Name Record)* irányelvtervezetet. A tervezet célja, hogy harmonizálja a tagállamok rendelkezéseit, amelyek kötelezettségeket állapítanak meg a légi fuvarozók számára, hogy bűnüldözési célból továbbítsanak PNR-adatokat a tagállamok illetékes hatóságainak. A kezdeményezés célja a terrorizmus és a súlyos bűncselekmények megelőzése és az ellenük folytatott harc hatékonyságának növelése. A rendszer működésének lényege, hogy a légi fuvarozók továbbítják a foglalási rendszerükben meglévő adatokat az illetékes nemzeti utasinformációs hatóságoknak. Ezek a hatóságok a számukra létrehozott saját adatbázisban kezelik és megőrzik az adatokat. Az utasinformációs hatóságok a PNR-adatokkal végzett automatizált kockázatelemzés után – ha szükséges – az adatok manuális elemzése révén kiszűrik az utasok közül azokat, akiknek adatai arra utalnak, hogy érintettek lehetnek a tervezet céljai között meghatározott bűnözési formákban. A PNR-adatokból az egyes bűnözési formák jellegzetességeivel való összevetés révén akár az utasok személyes adatainak ismerete nélkül is azonosítani tudják a gyanús személyeket. A közös európai megközelítés elfogadásának azonban jelentős gazdasági és társadalmi vetületei vannak. Nagy valószínűséggel az irányelv által meghatározott követelmények teljesítése növeli a légitársaságok költségeit és ezen keresztül az utasokéit is. A légi fuvarozókra rótt kötelezettségek tovább növelik a különböző közlekedési ágazatok közötti megkülönböztetést a légi közlekedés terhére. A társadalmi hatások közül a legfontosabb a rendszer működésének viszonya az adatvédelem követelményeivel és a személyiségi jogok érvényesülésével. Minden tagállam sokat vár az irányelvtől. Elsősorban az adatvédelmi és a költségvetési hatásokat fogják vizsgálni az új szövegváltozat esetében is. A belügyi biztos az irányelvtervezet megjelenésekor kibocsátott sajtóanyagában kétéves vitát irányzott elő a közös európai megközelítésről, tekintettel arra is, hogy az Európai Parlament kiemelt figyelmet fordít az irányelv tárgyalására, hiszen az ott illetékes biztosság már több esetben vitatta a rendszer szükségességét és arányosságát.

AZ EMBERI JOGOK EURÓPAI BÍRÓSÁGÁNAK A DUBLINI RENDELET ALKALMAZÁSÁRA VONATKOZÓ ÍTÉLETE. Az Európa Tanács emberi jogi bírósága január 21-én hozott döntést egy az úgynevezett dublini rendelet alapján kiutasított menedékkérő beadványa alapján (M.S.S. v. Belgium and Greece). Az Emberi Jogok Európai Bírósága elmarasztalta mind Görögországot, mind Belgiumot az Emberi jogok európai egyezményének 3. (embertelen vagy megalázó bánásmód vagy büntetés tilalma) és 13. (jog a hatékony jogorvoslathoz) cikkelyeinek megsértése miatt.

A menedékkérő afgán állampolgár 2008 elején hagyta el Kabult, és Iránon és Törökországon keresztül Görögországban lépett az EU területére. A belga hatóságok az ott beadott menedékkérelmet nem vizsgálták meg, hanem a Dublin–II rendelet alapján átadták Görögországnak. A bíróság szerint a belga hatóságok tisztában voltak a görögországi menekültügyi eljárás hiányosságaival, hibáival, illetve az ottani életkörülményekkel, amikor kiutasították a kérelmezőt. Az ENSZ Menekültügyi Főbiztosának Hivatala fel is hívta a belga hatóságok figyelmét a görögországi helyzetre. Belgium a kiutasítást úgy hajtotta végre, hogy nem követelte meg a görög hatóságok általi egyedi garanciákat, nem győződött meg a menekültügyi szabályozás gyakorlati alkalmazásának megfelelőségéről, noha a dublini rendszer lehetőséget adott volna az átadás visszautasítására.

Az ítélet nyomán az Európai Bizottság sürgeti a menekültügyi rendszer átfogó reformjának mielőbbi végrehajtását (közös menekültügyi rendszer felállítása, a Dublin–II rendelet módosítása).

NYILVÁNOS KONZULTÁCIÓ A BELÜGYI TERÜLET FINANSZÍROZÁSÁRÓL. Az Európai Bizottság nyilvános konzultációt hirdetett a következő többéves pénzügyi keret előkészítéséhez kapcsolódóan a belügyi szakpolitikák finanszírozásának jövőjéről. A tagállamok, EU-intézmények, hatóságok mellett a nem kormányzati szervezetek, tudományos intézmények, magánszemélyek is véleményt formálhatnak 2011. március 6-ig a prioritásokról és a végrehajtási mechanizmusokról a belügyi szakpolitikák (biztonság, migráció és a külső határok igazgatása) területén.

A konzultáció annak a folyamatnak a része, amellyel a bizottság a jelenlegi EU-költségvetés felülvizsgálatát és a következő, 2013-tól hatályos pénzügyi keretet készíti elő. Célja, hogy minden érdekelt (gyakorlati tapasztalatokkal is bíró személyek és szervezetek) bevonásával megvizsgálja, az alkalmazott pénzügyi eszközök megfelelnek-e a szükségleteknek, mennyire hatékonyak és hogyan fejleszthetők tovább. A konzultációs kérdőív az unió valamennyi hivatalos lapján elérhető, kitölthető: http://ec.europa.eu/your-voice/ipm/forms/dispatch

AZ EURÓPAI BIZOTTSÁG MÁSODIK JELENTÉSE A KISHATÁRFORGALMI SZABÁLYOK ALKALMAZÁSÁRÓL. Az Európai Bizottság február 9-én fogadott el jelentést* a

* COM(2011) 47 final. Communication from the commission to the European Parliament and the Council. Second report on the implementation and functioning of the local border traffic regime set up by Regulation. No 1931/2006.

tagállamok külső szárazföldi határain való kishatárforgalom szabályainak meghatározásáról, valamint a schengeni egyezmény rendelkezéseinek módosításáról szóló 1931/2006/EK rendelet (a továbbiakban: kishatárforgalmi rendelet) végrehajtásáról.

A kishatárforgalmi rendszer kivételt képez a schengeni határ-ellenőrzési kódexben (562/2006/EK rendelet) foglalt, az Európai Unió tagállamainak külső határait átlépő személyek határokon történő ellenőrzésének általános szabályai alól: a tagállamok a szomszédos harmadik országokkal kétoldalú megállapodást köthetnek a határ menti területeken jogszerűen tartózkodó személyek határátlépésének megkönnyítése érdekében.

Jelenleg ilyen megállapodás van hatályban Magyarország és Ukrajna (2008), Szlovákia és Ukrajna (2008), Lengyelország és Ukrajna (2009) és Románia és Moldova (2010) között, a felsoroltak közül azonban csak az utolsó felel meg teljes mértékben a kishatárforgalmi rendelet előírásainak. Hamarosan hatályba lép négy hasonló megállapodás, lengyel–fehérorosz, lett–fehérorosz, litván–fehérorosz és norvég–orosz viszonylatban is. A lett–orosz, litván–orosz, román–ukrán megállapodások előkészítés alatt állnak.

Az első bizottsági jelentés (2009. július 24.) arról számolt be, hogy a kishatárforgalmi megállapodások szigorúbb feltételeket támasztanak, mint a kishatárforgalmi rendelet, illetve egyik megállapodás sem használja a könnyítést szolgáló intézkedések mindegyikét. A helyzet e tekintetben a második jelentés szerint nem változott.

A bizottság szerint a kishatárforgalmi rendszer alapvetően jól működik, jelentősen megkönnyíti a külső szárazföldi határok közelében élő emberek életét. A bizottság nem tervezi a rendelet felülvizsgálatát, mindazonáltal felhívja a tagállamokat a megállapodások módosítására annak érdekében, hogy teljes mértékben megfeleljenek a rendeletben foglaltaknak.

Összeállította:
Asztalos Erika és Szabó Adrienn

Ára: 470 Ft