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.