DORNFELD LÁSZLÓ[1]

A KIBERBŰNÖZÉS ELLENI KÜZDELEM KIHÍVÁSAI

Absztrakt

Az internet megjelenése és széleskörű elterjedése alapvetően változtatta meg életünket. A bűnözők is hamar érdeklődni kezdtek az új technológia iránt. A határokon átívelő új bűnözési forma tömegessé válásával az államok és a nemzetközi szervezetek is felismerték a jogi szabályozás kialakításának fontosságát. Tanulmányomban e témakör büntetőeljárással kapcsolatos kérdéseit a legújabb angol és magyar szakirodalom alapján vizsgálom. Bemutatom a hagyományos nyomozási eszközök alkalmazásának lehetőségeit, és azt, hogy az eljárásjogban nem került sor gyökeres változásra, valamint új jogintézmények egy részének hibáit. Megvizsgálom továbbá a szabályozás kialakításának kérdéseit, melyben az önszabályozás bevezetésével is foglalkozom, amely megakadályozhatja a jogszabályok számának túlságos növekedését.

Kulcsszavak: büntető eljárásjog, kiberbűnözés, számítástechnikai bűnözés, nyomozás, Európai Unió.

BEVEZETÉS

Az internet az elmúlt évtizedben egyre inkább elérhetővé vált a számítógép tulajdonosok számára, és napjainkra a fejlett országokban élők mindennapi életének része lett. Jól mutatja ezt, hogy míg Press Freedom Survey 2001-es jelentése alapján Magyarországon csak a lakosság 6,4%-a rendelkezett interneteléréssel,[2] addig az Eurostat adatai alapján ez a szám 2011-re 68%-ra nőtt, vagyis megtízszereződött.[3] A digitális menetrend 2014-es eredménytáblája szerint az internethasználók aránya Dániában, Svédországban, Hollandiában és Luxemburgban a legmagasabb, számuk a lakosság 90%-át is meghaladja (az Egyesült Államokban 87%-os ez az arány).[4] A világháló, szemben a korábbi kommunikációs formákkal, nemcsak gyors és közvetlen adatátvitelre képes nagy távolságokon keresztül, de egyúttal többoldalú, interaktív kapcsolatot valósít meg a résztvevők között.[5] Fontos jellemző még, hogy az internetes tartalmak változatlanul hozzáférhetők a világ minden pontján a felhasználók számára.[6]

Ez a technológiai vívmány számos módon felhasználható, és könnyebbé, valamint szélesebb körben elérhetővé tehető rengeteg tevékenység az igénybevételével. Ide sorolható például az e-kereskedelem, a banki ügyek online intézése és a gazdasággal összefüggő egyéb fontos műveletek; az e-közigazgatás, amely gyorsabbá és mindinkább ügyfélbaráttá teszi az ügyintézést;[7] és az internet jelentős demokratikus potenciálja, amit e-demokráciaként is szoktak emlegetni. Számos téren van tehát szükség a megfelelő állami szabályozás kialakítására, amelyek megalkotása jelentős aktivitást igényel a jogalkotó részéről egy állandóan fejlődő és változó környezetben. Mindezek közül azonban talán a legfontosabb a kiberbűnözés elleni fellépés jogszabályi hátterének létrehozása, mivel az internet iránti bizalom jelentős csökkenésének komoly gazdasági következményei lehetnek. Ilyen lehet például, hogy egyre kevesebben vesznek részt az e-kereskedelemben.[8]

Az informatikai biztonság jogi szabályozás általi megteremtése lehetetlen feladatnak tűnik, és mint arra *Szádeczky* is rámutat, hamar anakronisztikussá válhatna a rendelkezések többsége. Az állami szabályozást azonban a megfelelő mértékben szükségesnek tartja annak kikényszeríthetősége miatt.[9]Az internetes bizton-

[1] A Miskolci Egyetem Állam- és Jogtudományi Kar frissen végzett jogász szakos hallgatója, aki tanulmányával a Batthyány Lajos Szakkollégium Batthyány-esszépályázatán második helyezést ért el.

[2] RÜTHER, WERNER: Az internet és az „informatikai bűnözés" a kriminológia számára is kihívás, in *Belügyi Szemle*, 2003/2-3. szám, 253. o.

[3] Az információs társadalomra vonatkozó statisztika – háztartások és magánszemélyek, elérhető: http://ec.europa.eu/eurostat/statisticsexplained/index.php/Information_society_statistics__households_and_individuals/hu (2015.07.30.).

[4] A digitális menetrend 2014. évi eredménytáblája: helyzetfelmérés, elérhető: http://europa.eu/rapid/press-release_IP-14-609_hu.htm (2015.08.10.).

[5] RÜTHER: *i. m.* 250–251. o.

[6] PARTI KATALIN: Nyomozás az interneten: együttműködés – korlátokkal, in *Belügyi Szemle*, 2004/11–12. szám, 204. o.

[7] Bővebben ld. TÓZSA ISTVÁN: Az elektronikus közigazgatás helyzete, in *Új magyar közigazgatás*, 2012/5. szám, 2–12. o.

[8] WARREN, PETER – STREETER, MICHAEL: *Az internet sötét oldala*, 2005, HVG Kiadó, Budapest, 79–82. o.

[9] SZÁDECZKY TAMÁS: Az IT biztonság szabályozásának konfliktusa, in *Infokommunikáció és Jog*, 2013/3. szám, 149. o.

ság létrehozásában a megelőző intézkedéseken túl nagyon fontos szerep jut még a bűnüldözésnek is, bár ultima ratio jellege miatt annak kizárólagos eszköze nem lehet. Közismert ugyanakkor az, hogy a bűncselekményt követő gyors és eredményes felderítés jelenti a prevenció egyik leghatékonyabb módját, és így hozzájárul a bűncselekmények számának csökkenéséhez. Célom a fogalmi alapok tisztázása után az internetes bűnözés jelentette kihívások elemzése, majd az erre a büntetőeljárás jogi szabályozás által adható lehetséges válaszoknak az áttekintése.

1. FOGALMI NEHÉZSÉGEK: A KIBERBŰNÖZÉS ÉS A KIBERBŰNCSELEKMÉNY

Legelőször is fontos azt tisztázni, mit is ért a szakirodalom kiberbűnözés alatt, hiszen a jelenség, és az ebből a nyomozás során keletkező problémák értelmezése nélkül az erre válaszul létrejött új eszközök sem érthetők meg. Maga a kibertér kifejezés nem technológiai vagy jogi, hanem irodalmi eredetű, először 1984-ben, William Gibson *Neurománc* című kiberpunk regényében jelent meg. Az ebből képzett kiberbűnözés szó a kibertérben elkövetett bűncselekményeket jelöli, és napjainkban széles körben elterjedt.[10] Több, a jelenséget összefoglaló kifejezés jelent meg a magyar nyelvben az azóta eltelt időben, azonban ezek nem minden esetben azonos jelentésűek.

Korábban a számítógépes bűnözés kifejezéssel azonos értelemmel bírt,[11] azonban ez ma már egyértelműen szűkebb kategória, hiszen az új információtechnológiai vívmányok, így például az okostelefonok és a táblagépek elterjedése következtében ezen eszközök is a bűnözés célpontjaivá válhatnak vagy az elkövetés során használhatók. Ugyan a dogmatikailag jóval kevésbé kötött amerikai common law jogrendben próbálták a mobiltelefonokat is a számítógépek közé sorolni,[12] ám ez a megközelítés szerintem nem helyes, hiszen a számítógép a közbeszédben egyértelműen a személyi számítógépeket jelöli. Ezt a változást jogalkotó is felismerte, amit mutat, hogy a büntetőeljárásról szóló 1998. évi XIX. törvénybe (a továbbiakban: Be.) a 2002. évi I. törvénnyel bekerült a „*számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés" kényszerintézkedés elnevezését 2013-ban a ma is hatályos „információs rendszerben tárolt adatok megőrzésére kötelezés*"-re módosították, kifejezetten utóbbi tágabb jelentéstartalma miatt.[13] Használt kifejezések még az elektronikus, a csúcstechnológiás és az internetes bűnözés fogalmak is, amelyek többé-kevésbé azonos értelműek a kiberbűnözéssel. Jelen tanulmány során elsődlegesen utóbbi fogalmat fogom használni, annak nemzetközi elterjedtsége okán.[14]

A kiberbűncselekmény meghatározására nem létezik általánosan elfogadott definíció, hiszen annak tartalma, a bűnözők módszerei eddig soha nem látott gyorsasággal változnak,[15] így minden aspektusát nehéz összefoglalni egyetlen fogalomban. Az eddigi definícióalkotások során két fő megközelítési mód körvonalazódott: az egyik az elkövetés technológiai vonatkozásainak, míg a másik az elkövetés tárgyának tulajdonít nagyobb jelentőséget. Előbbihez sorolható például az Egyesült Államok Igazságügyi Minisztériumának meghatározása, amely szerint „számítógépes bűncselekmény a büntetőtörvények minden olyan megszegése, amely az elkövetés, a nyomozás vagy a bűnvádi eljárás során számítógépes technológia ismeretét feltételezi".[16] Ennek a meghatározásnak azonban nagy hátránya, hogy túlságosan is általános, így olyan bűncselekmények is alá tartoznának, amelyeknél az említett fázisok valamelyikénél szükséges számítógép használata,

[10] WALL, DAVID S.: *Cybercrime: The Transformation of Crimein the Information Age*, 2007, Polity, Cambridge, 9–10. o.

[11] GERGELY MÁTÉ: Nyomozás az interneten, in *Belügyi Szemle*, 2002/10. szám, 31. o.

[12] A 8. Körzeti Fellebbviteli Bíróságíróság a 10-1983 United States v. Neil Scott Kramer (2011) ügyben hozott ítéletében hivatkozza a Computer Abuse and Fraud Act azon rendelkezését, amely szerint számítógépnek minősül egy eszköz, ha az „számtani, logikai és tárolási műveleteket hajt végre", valamint az indokolásban idézi az egyik szakértőt, aki szerint „ma már mindenben van számítógép".

[13] CZINE ÁGNES: VIII. fejezet, in BELEGI JÓZSEF (szerk.): *Büntetőeljárás I–III - Kommentár a gyakorlat számára*, 2014, HVG-ORAC, Budapest, 806–808. o.

[14] Például az Interpol is ezt a fogalmat használja weboldalán. Lásd: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (2015. 08. 06.) Valamint az Europol részeként létrejött Európai Kiberbűnözés Elleni Központ (European Cybercrime Centre, EC3) is ezt a nevet viseli. Lásd: Frequently Asked Questions: the new European Cybercrime Centre, Európai Bizottság, elérhető: MEMO/12/221,http://europa.eu/rapid/press-release_MEMO-12-221_en.htm (2015.08.08.).

[15] WALL: *i. m.* 2-3. o.

[16] KIM, CHRIS – NEWBERGER, BARRIE – SHACK, BRIAN: Computer Crimes, in *American Criminal Law Review,* Vol. 49. Issue 2. (2012), 444. o.

de mégsem tekinthetők kiberbűncselekménynek, vagy nem ez a domináns bennük. Példaként említeném azon orosz hackerek ügyét, akik az ukrán rendőrség lopott autókkal kapcsolatos adatbázisát törték fel, hogy könnyebben értékesíteni tudják a járműveket,[17] de ma már a nyomozás is szinte elképzelhetetlen informatikai ismeretek nélkül.

A másik megközelítéshez sorolható például az ENSZ 2000-ben született definíciója, ami szerint a fogalom alatt értendő minden olyan illegális tevékenység, amely az elektronikus biztonsági rendszerek és a továbbított adatok ellen irányul.[18] Az osztrák *Schmölzer* és *Schich* szerint informatikai bűncselekmény az, ami hardver, szoftver vagy adat elleni támadással valósul meg.[19] *Nagy* ezzel szemben csak az adat szempontjából vizsgálja a kiberbűncselekményeket, amely szerinte egyaránt lehet az elkövetés célja, illetve annak eszköze is.[20] Ennél a definíciós megoldásnál a legnagyobb nehézséget az jelenti, hogy a kiberbűncselekmények köre túlságosan széles, és ezek mindegyike nem sorolható be a meghatározott kategóriákba, valamint a gyorsan kialakuló új módszerek hamar anakronisztikusakká tehetik őket. A fenti három meghatározásnál például nehéz lenne bárhol is elhelyezni az internetes zaklatást (*cyberbullying*).

2. A KIBERBŰNCSELEKMÉNYEK NYOMOZÁSÁNAK KIHÍVÁSAI

2.1. A látencia szerepe

Kim, Newberger és *Shack* megállapítása alapján a szakértők számára a kiberbűncselekmények által okozott kár megbecslése több tényező miatt okoz nehézséget. Felsorolásuk szerint szerepet játszik ebben a pontos fogalom meghatározás hiánya; az áldozatok vonakodása, hogy bejelentést tegyenek az elkövetett cselekményekről, félve a fogyasztói bizalom csökkenésétől, valamint a felderítés hiánya.[21] Mivel az első problémával már a korábbi szakaszban foglalkoztam, itt a másik kettőre fókuszálok csak. A sikeres eljárás szempontjából igen fontos kérdésnek számít az elkövetett cselekmény észlelése, valamint, hogy az a bűnüldöző szervek tudomására jusson, hiszen e nélkül nem kerülhet sor a nyomozás megindítására.

A kiberbűncselekmények kapcsán a kezdetektől fogva megfigyelhető jelentős látencia. Az FBI becslése szerint az internetes adatlopással vagy károsítással kapcsolatok ügyek 95%-a felderítetlen marad. Már 1986-ban is volt rá példa, hogy egy rendszerbe betörő, és ott adatokat manipuláló elkövető utóbb kitörölte a tevékenységét rögzítő fájlt, így tüntetve el saját nyomait.[22] Nagyon sok esetben az internetelérést biztosító eszköz használója nincs is annak tudatában, hogy kiberbűncselekmény áldozata lett, hiszen az nem jár látható nyomokkal. Példaként említeném itt a mobiltelefon átprogramozását vagy biztonsági kiskapukat nyitó programok telepítését a sértett számítógépen. Ezek igen gyakran további bűncselekmények (pl. adathalászat) technikai megalapozójaként szolgálnak,[23] például egy okostelefon segítségével ma már könnyedén meg lehet tudni az érintésmentes bankkártyák használatához szükséges adatokat.[24] Ugyanígy nehezen vehető észre, ha a sértett számítógépére billentyűleütéseket figyelő kémprogramot telepítettek vagy pedig egy, az eredetire nagyon hasonló, de adathalász csalók által üzemeltetett oldalra irányítják át (*pharming*).[25]

Azon ügyek jelentős részében sem értesítik a rendőrséget a sértettek, amelyek a tudomásukra jutnak. Különösen a nagy cégek igyekeznek gyakran titokban tartani a rendszereik ellen végrehajtott hackertámadásokat: egy 1999-es amerikai felmérés szerint a jelentős hackeléseknek mindössze a 32%-át jelentették be a

[17] WARREN, STREETER: *i. m.* 46. o.

[18] RADU, IOAN – URSACESCU, MINODORA – SENDROIU, CLEOPATRA – CIOC, MIHAI: Computer Crime - A Threat to the International Society, in *Agora International Journal of Juridical Sciences*, Vol. 2. No. 1. (2008), 250. o.

[19] Hivatkozza NAGY ZOLTÁN ANDRÁS: *Bűncselekmények számítógépes környezetben*, 2009, Ad Librum, Budapest, 38–39. o.

[20] Uo. 51–52. o.

[21] Felsorolásukban szerepel a duális (tagállami-szövetségi) igazságszolgáltatási rendszer is, de ez – amerikai sajátosságként – nem szerepel tanulmányom fókuszában. Ld. KIM – NEWBERGER – SHACK: *i. m.* 445. o.

[22] WOLF, JOHNATAN B.: War Games Meets the Internet: Chasing 21st Century Cyber Criminals With Old Laws and Little Money, in *American Journal of Criminal Law*, Vol. 28. Issue. 1. (2000), 100. o.

[23] LACZI BEÁTA: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, in *Magyar Jog*, 2001/12. szám, 727. o.

[24] GÁLFFY CSABA – VOITH HUNOR: *Nyitott pénztárcával sétálunk a világban*, elérhető: http://www.hwsw.hu/hirek/54283 /mastercard-visa-paypass-nfc-rfid-biztonsag-kartya-bank.html (2015.08.09.).

[25] LENGRÉ MÓNIKA: A XXI. század új típusú próbatétele: az informatikai biztonság, in *Belügyi Szemle*, 2012/5. szám, 5–21. o.

hatóságoknak, így a legtöbb ügyben nem is indulhatott nyomozás.[26] A sértettek vonakodása ugyanakkor érthető, hiszen míg sokszor nem sok előnyt remélnek a hatósági úttól, addig joggal tartanak tőle, hogy az ügyfelek a cég védelmének gyengeségeként és végső soron megbízhatatlanságaként fogják értékelni a rendszerükbe történt betörés tényét. Jól mutatja ezt az 1994-es Levin-ügy, mikor a Citibank a húsz legnagyobb befektetéssel bíró ügyfelét veszítette el, miután kiderült, hogy egy orosz hackertámadás miatt 10 millió dolláros kár érte az ügyfeleket.[27] Éppen ezért nagy felelőssége van abban a nyomozó hatóságoknak, hogy megfelelő diszkrécióval járjanak el az ilyen ügyek során, és kialakítsák a megfelelő kapcsolatokat.

2.2. Pontos jogszabályalkotás szükségessége

A kiberbűncselekmények kapcsán kiemelkedően fontos a jól érthető, világos büntető anyagi normák kialakítása, hogy a jogalkalmazás során a lehető legkevesebb probléma merüljön fel. Ezek megalkotása során nagyon lényeges, hogy eredményeképp egyébként jogszerű magatartások ne kerüljenek kriminalizálásra. Ez ugyanis nem csak paradox jogi helyzetet eredményez, de visszavetheti a technikai fejlődést is.[28] Példaként említeném itt a fájlcserélő oldalak üzemeltetői ellen indított jogi eljárásokat (a leghírhedtebb közülük a Pirate Bay-per), hiszen ezeken nem tárolnak jogsértő adatokat, csak ezek elérési útját; az ezek segítségével lebonyolított fájlcsere egy része teljesen legális, és nehezen megállapítható, hogy a felhasználó általi elérhetővé tétel jogszerű-e.[29]

Másik példaként említhetném a United States v. Drew ügyet,[30] ahol az áldozat közösségi oldalon történő zaklatás hatására öngyilkosságot követett el. Az ehhez vezető üzenetet egy olyan hamis felhasználói profilról küldték, amely Lori Drew-hoz volt köthető. A tagállami cyberstalking törvény alapján végül nem indult eljárás a bizonyítékok hiánya miatt. Szövetségi bíróság előtt elsőfokon négy vádpontban indult eljárás, amelyek közül az egyik a CFAA 18 USC § 1030 (a)(2)(C)-be ütköző „államközi vagy külföldi kommunikációban érintett számítógéphez információszerzés céljából történő felhatalmazás nélküli vagy a felhatalmazás mértékét túllépő hozzáférés" volt. Az esküdtszék három vádpontban ártatlannak, a fentebbi vétség elkövetésében bűnösnek találta Drew-t, míg egy vádpontban nem tudott döntésre jutni. Ezzel tulajdonképpen a közösségi oldal felhasználási feltételeinek megszegése miatt ítélték el a vádlottat. Az esküdtszék 2008-as ítéletét felülbírálva az eljáró bíró, George H. Wu helyt adott a vádlott felmentési kérelmének. Indoklásában kifejtette, hogy Drew elítélése olyan magánfelek közötti jogviszony megsértésének kriminalizálását jelentette volna, amelynek alapja egy bármikor, külön értesítés nélkül megváltoztatható megállapodás.[31]

A büntetőeljárásjogi rendelkezések esetén az anyagi jogihoz hasonlóan fontos, hogy a szabályozás megfelelően pontos legyen. E mellett adatvédelmi és személyiségi jogi érveket lehet felsorakoztatni, hiszen az átvizsgált eszközökön található információk egy része nemcsak személyes, de különleges adat is lehet. A látogatott weboldalak vagy a tárolt fájlok vizsgálata közben például kiderülhet a felhasználó politikai véleménye, vallásos meggyőződése vagy szexualitása, de akár az egészségi állapota is. Szinte a gyanúsított teljes személyiségének megismerésére lehetőséget ad a nyomozó hatóságnak, és ahogy a technikai lehetőségek egyre bővülnek, úgy nő az állam lehetősége is arra, hogy beavatkozzon az állampolgárok életébe.[32]

3. A HAGYOMÁNYOS NYOMOZÁSI ESZKÖZÖK SZEREPE A KIBERTÉRBEN

Ahogy a kiberbűncselekmények túlnyomó többsége valamely, a fizikai világban már kialakult bűncselekmény – mint például csalás, zsarolás, zaklatás stb. – digitalizált formája, és a büntető anyagi jog számára nem tartalmaz kihívásokat, úgy az eljárásjog eddig bevett nyomozási eszközeinek is helyük van ezek felderítésében. A legelső kiberbűnözés elleni törvények, – mint például a Computer Abuse and Fraud Act (a tová-

[26] WOLF: *i. m.* 102. o.
[27] Uo. 102. o., WARREN – STREETER: *i. m.* 43. o.
[28] DORNFELD LÁSZLÓ: Fájlmegosztás: a szellemi tulajdonjog legújabb kihívása, in *Diskurzus*, 2014/1. szám, 54–61. o.
[29] Bővebben ld.: NAGY ZOLTÁN ANDRÁS: A Pirate Bay-per tanulságai. De lege ferenda a fájlcseréről, in *Ügyészek Lapja*, 2010/2. szám, 33–40. o.
[30] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
[31] THAW, DAVID: Criminalizing Hacking, Not Dating: Reconstructingthe CFAA Intent Requirement, in *The Journal of Criminal Law and Criminology*, Vol. 103. No. 3. (2013), 921–922. o.
[32] MOHÁCSI BARBARA: Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal, in *Magyar Jog*, 2008/12. szám, 830. o., BERECZ PÉTER: A Német Szövetségi Alkotmánybíróság „számítógép-határozata", in *Studia Juvenum*, 2009, Debrecen, 71–78. o.

biakban: CFAA) – megalkotása idején ez még nem volt egyértelmű. *Wolf* cikkében azt rója fel az amerikai jogalkotónak, hogy számos elégtelenül szabályozott kérdést hagyott meg, és sok esetben csupán a már meglévő szabályokat duplikálta. A szerző a törvény egyik legnagyobb hibájának azt tartja, hogy teljesen külön próbálja kezelni az internetes bűncselekményeket más deliktumoktól.[33]

A bizonyítási eszközök és kényszerintézkedések jelenlegi törvényi szabályozása alkalmas arra, hogy azok bizonyosan alkalmazhatók legyenek a kiberbűncselekmények esetén. A fő probléma ugyanis nem a hiányos jogszabályi háttér, hanem a nyomozó hatóság és az ügyészek technikai járatlansága és képzetlensége, amelyek gyakran negatívan hatnak a nyomozásra. Több bizonyítási eszköz kapcsán is felmerül ez a probléma, így a tanúvallomásnál, a terhelt vallomásánál és a szakértői véleménynél. Előbbi kettőnél a fő gondot az okozhatja, hogy a vallomástevő – például tanúként a sértett cég rendszergazdája vagy a gyanúsított – a legtöbbször jóval járatosabb az informatikában az őt kérdezőnél. Egy 2001-es felmérés szerint az elkövetők 85%-a belső munkatárs, és csupán 11%-a hacker vagy cracker.[34] Ennek különösen a terhelti vallomásnál van jelentősége, ahol a törvények nem írnak elő igazmondási kötelezettséget, így a kihallgatott könnyedén félrevezetheti a nyomozó hatóságot.[35] A szakértői vélemény esetén a fő problémát azt jelenti, ha a nyomozó hatóság nem képes a megfelelő kérdéseket feltenni. A *Parti* által vizsgált 2002 és 2005 közötti magyar gyermek pornográf ügyek majdnem felében a szakértőt olyan feladat elvégzésére rendelték ki, mint például a képek leválogatása, amit maga a nyomozó hatóság is könnyedén el tudott volna végezni.[36]

Bizonyos esetekben vita alakult ki annak kapcsán, hogy egy-egy új technológiai eszközzel kapcsolatos eljárás hova is sorolható. Így például *Laczi* szerint a számítógépek nyomozás során történő átvizsgálása sokáig kérdéses volt, hogy szemlének vagy pedig házkutatásnak tekinthető-e,[37] és csak 2002 óta kerül egyértelműen Be. 149. § (1) alatt szabályozásra. A legtöbb esetben azonban az új technikai lehetőségekre vonatkozó külön implementálás nélkül is egyértelműen alkalmazhatóak lesznek. Így például az sosem volt vitatott, hogy az egyes illegális tartalmakat tároló adathordozók, klónozott telefonok és más, a kiberbűncselekmények eredményeként a fizikai világban létrejövő dolgok a Be. 115. § alatti tárgyi bizonyítási eszköznek tekintendők.[38] Ugyanígy nem volt szükséges a magyar jogban arra, hogy új normát alkossanak a számítógépek távoli átvizsgálását lehetővé tévő online házkutatás alkalmazására, hiszen az könnyedén beilleszthető volt a bírói engedélyhez kötött titkos adatszerzéshez. Ez a döntés, a körülötte Németországban kialakult alapjogi jellegű vitáknak is betudható, amelynek részeként előbb 2007-ben a Legfelsőbb Bíróság, egy évre rá pedig az Alkotmánybíróság semmisített meg rá vonatkozó jogszabályi rendelkezéseket.[39] A felmerült súlyos aggályok alapján valóban szükség van a bírói kontrollra ennek alkalmazásánál.

Mint fentebb látható, a jelenlegi jogi szabályozás máris megteremtette az elektronikus adattal kapcsolatos nyomozási feltételeket. Míg az elektronikusan tárolt adatnál a házkutatás, addig az elektronikus úton folytatott kommunikációnál az engedélyhez kötött titkos adatszerzés és információgyűjtés szabályait kell alkalmazni, vagyis mindkét esetben már előtte is létező normák részeként került szabályozásra. Persze ez a kiterjesztés jóval egyszerűbb az angolszász jogrendszerben, amelynek mobiltelefonokkal kapcsolatos megoldásáról már szót ejtettem. A magyar büntető eljárásjogban nehezen tudnánk olyan érvelést elfogadni, amely szerint a közösségi médiák (pl. Facebook) felületén található információk kinyomtatva okiratként bizonyítéknak fogadhatók el, mint azt teszik Nagy-Britanniában.[40] Az eljárásjogban tehát csak a legritkább esetben volt szükség teljesen új eljárási szabályok kidolgozására, mindössze egy új bizonyítási eszköz és egy új kényszerintézkedés került be a Be-be az elmúlt években a kiberbűncselekményekkel összefüggésben.

---

[33] WOLF: *i. m.* 97. o.

[34] LACZI: *i. m.* 729. o.

[35] PARTI KATALIN: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai, in VIRÁG GYÖRGY (szerk.): *Kriminológiai tanulmányok 44. kötet*, 2007, OKRI, Budapest, 98. o.

[36] A 225 ügyből 88-ban tudta volna a nyomozó hatóság a szakértő feladatát ellátni a megfelelő technikai tudás birtokában. Ld. Uo. 97. o.

[37] LACZI: *i. m.* 730. o.

[38] Uo. 728–729. o.

[39] Bővebben ld.: BERECZ PÉTER: *i. m.* 71–78. o.

[40] O'FLOINN, MICHEÁL – ORMEROD, DAVID: Socialnetworking materialas criminal evidence, in *Criminial Law Review*, Vol. 7. (2012), 486–512. o.

4. FELLÉPÉS AZ ILLEGÁLIS TARTALOM ELLEN: ÖNSZABÁLYOZÁS ÉS INTERNETBLOKKOLÁS

Amennyiben egy jogsértő tartalom egyszer már felkerült az internetre, onnantól a világ bármely részéről elérhetővé válik, még ha nem is minden felhasználó számára.[41] Hogy az ilyen tartalmak ne maradjanak letölthetők, amíg a gyakran elhúzódó büntetőeljárás tart, szükség van egy olyan mechanizmusra, amellyel elérhetetlenné tehetők az internetezők védelme érdekében. Erre két elterjedt megoldás kínálkozik: az egyik az önszabályozás, a másik a koreguláció alkalmazása. *Parti* ezzel összefüggésben három szintet különböztet meg: az elsődleges szint a felhasználói, ahol a számítógépet használó vagy az azt üzemeltető intézmény állítja be a szűrés mértékét; a második szint az internet-szolgáltató által alkalmazott szűrés; míg a harmadik szint pedig az állam által előírt tartalom blokkolása.[42]

Az önszabályozás egyik formája az értesítési-eltávolítási eljárás (vagy egyszerűen csak eltávolítási eljárás,[43] *notice & takedown*), amelynek segítségével maga a jogsértő adat is eltávolítható a szerverekről. Ennek során a nyomozó hatóság közvetlenül, nemzetközi forródrótok segítségével vagy közvetett módon, a forródrótok igénybevétele nélkül értesíti a tartalmat tároló közvetítő szolgáltatót. Míg utóbbi esetben a szolgáltatónak vizsgálnia kell, hogy valóban bűncselekményt valósít-e meg a tárolt tartalom, addig a közvetlen eljárás nagy előnye, hogy a forródrótok által jelentett tartalom jogellenességét nem kell vizsgálni, vagyis az eljárás felgyorsul.[44] Magyarországon az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 13. §-a lehetőséget teremt a szerzői jog szerinti jogosultaknak, hogy a jogsértő tartalom eltávolítását kérjék, aminek kötelező tartalmi elemeit rögzíti is. A szolgáltató ekkor az értesítés átvételét követő 12 órán belül köteles a megjelölt információhoz való hozzáférés nem biztosítása vagy a tartalom eltávolítása felől intézkedni. Az értesítési eljárással együtt felmerül a szolgáltató büntetőjogi felelősségének kérdése, hiszen a tudomásra jutást követően a továbbiakban passzívan segítséget nyújt a jogsértés folytatásához. *Szabó* remekül érvel amellett, hogy ennek megállapítására csak a sikertelen eltávolítási eljárás után kerülhet sor. Ellenkező esetben ugyanis nemcsak a büntetőjog ultima ratio jellegével kerülne összeütközésbe a szabályozás, de magát az eltávolítási eljárást is teljesen feleslegessé tenné.[45]

A másik megoldás az állami szervek által megállapított jogsértő tartalom elérésének megakadályozása, vagyis az internetblokkolás. Számos nemzetközi példa mutatkozik alkalmazására Európától Ázsiáig, amelyek egyike sem váltotta be azonban a hozzá fűzött reményeket. Legutoljára 2015 augusztusának elején India próbálkozott a közerkölcs védelmében 857 pornográf tartalmú oldal blokkolásával, hogy azokat fiatalkorúak ne érjék el. A felemás intézkedés (a felnőttek számára továbbra is technikai lehetőséget biztosítottak volna e tartalmak elérésére) azonban komoly társadalmi ellenállást váltott ki, és csak növelte a pornográf tartalmak iránti érdeklődést, így alig pár nap múlva a kormány rendelete visszavonására kényszerült.[46]

Alapvetően kétféle megoldás alakult ki a jogsértő tartalmak blokkolása kapcsán: 1) általános tartalomszűrési és monitorozási kötelezettséget írnak elő a közvetítő szolgáltatók számára 2) a nyomozó hatóság tudomására jutott egyedi esetekben fordulnak a szolgáltatókhoz és élnek blokkolással. Az első eset alapjogilag igen aggályos lehet, hiszen a gyakorlatban azt jelenti, hogy minden internetes adatforgalom ellenőrzésen esik át,[47] valamint nagy rá az esély, hogy túlszűrés folytán legális tartalmakhoz való hozzáférést is blokkolnak vagy pedig alulszűrés miatt illegális tartalmak maradnak továbbra is elérhetők.[48] A második megoldás jellemző a magyar Be. törvényre, amelynek 158/B-D. szakasza lehetőséget nyújt az elektronikus adat ideiglenes hozzáférhetetlenné tételére. Szemben a 2009-es német megoldással, amely egy, állandóan frissülő listán

[41] Példaként említhetők a pedofíliában érdekeltek által létrehozott zárt csoportok, amelyekben gyakran több százezer gyermek pornográf felvétel cseréje zajlik. Ezek túlnyomó többségében több országból is jelen vannak tagok. Ld.: BOCIJ, PAUL – MCFARLANE, LEROY: The Internet: A Discussion of Some New and Emerging Threats to Young People, in *Police Journal,* Vol. 76. No. 3. (2003), 8. o.

[42] PARTI KATALIN – MARIN, LUISA: Foltvarrással az on-line illegális tartalom ellen: a tartalomblokkolás, a közvetítő szolgáltató felelőssége és az értesítési-levételi eljárás, in *Infokommunikáció és Jog*, 2012/49. szám, 58. o.

[43] SZABÓ IMRE: A fájlcserélő honlapot üzemeltető közvetítő szolgáltatók felelőssége, in *Ügyészek Lapja*, 2010/1. szám, 10. o.

[44] Az eljárás részleteiről bővebben ld.: PARTI – MARIN: *i. m.* 62–63. o.

[45] SZABÓ: *i. m.* 12–13. o.

[46] MAJUMDER, SANJOY: India pornban: How the government was forced to reverse course, BBC Asia, elérhető: http://www.bbc.com/news/world-asia-india-33810775 (2015.08.09.).

[47] DORNFELD: *i. m.* 58. o.

[48] PARTI – MARIN: *i. m.* 60–61. o.

szereplő oldalak blokkolását írta elő,[49] itt olyan közvádra üldözendő bűncselekmények esetén rendelheti el a bíróság elektronikus adat hozzáférhetetlenné tételét, amelynél a Btk. 77. § szerinti elektronikus adat végleges hozzáférhetetlenné tételének van helye, és a hozzáférhetetlenné tétel szükséges a bűncselekmény folytatásának megakadályozásához. Az internetes tartalmak blokkolását azonban nem csak bíróság rendelheti el, hanem bizonyos esetekben az állami közigazgatás szervei is. A Nemzeti Adó- és Vámhivatal a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény 36/G. §-a alapján a tiltott szerencsejáték-szervezést megvalósító elektronikus adathoz; az Országos Gyógyszerészeti Intézet pedig az emberi alkalmazásra kerülő gyógyszerekről és egyéb, a gyógyszerpiacot szabályozó törvények módosításáról szóló 2005. évi XCV. törvény 20/A. §-a alapján a hamis vagy nem engedélyezett gyógyszer elérhetővé tételével összefüggő elektronikus adathoz való hozzáférést ideiglenes korlátozza.

Az internetblokkolás olyan kérdéskör, amely a technikai és büntetőjogi vonatkozásain túl fontos alapjogi kérdéseket is felvet. Különösen a szólásszabadsággal összefüggésben merülhetnek fel konfliktusok, hiszen a diktatúrák gyakran élnek az internetes tartalomszűrés eszközével, igyekezve eltüntetni a számukra kellemetlen tartalmakat. Itt megemlíteném a Kínában működő Aranypajzs projektet, amely például a Tibet függetlenségével vagy a Falun kung vallási meditáció követőivel kapcsolatos oldalak elérését akadályozza meg;[50] de a török szabályozás is gyakran mutat autoriter jelleget: 2013-ban összesen mintegy harmincezer weboldalhoz blokkolták a török felhasználók hozzáférését, ezek egy részénél politikai indokból.[51] Ugyanakkor demokratikus társadalmakban is megvalósítható az internetszűrés, az olyan jogszabályi biztosítékok beiktatásával, mint például a bírói függetlenség, és a szélesebb társadalom bevonása a szabályozás megalkotásába.[52] Jelenleg azonban az Európai Parlament és a Tanács által megalkotott a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól szóló 2000/31/EK irányelv 15. cikke kimondja azt, hogy a tagállamok nem állapíthatnak meg általános tartalomszűrési kötelezettséget a közvetítő szolgáltatókra nézve.

Összességében elmondható, hogy az internetblokkolás nemcsak komoly alapjogi aggályokat vet fel, hanem emellett alacsony hatásfokú is, és könnyedén kijátszható, így demokratikus országokban nem képes a neki szánt szerepet betölteni. Az önszabályozás jobb lehetőségeket kínál az illegális tartalom elérhetetlenné tételére, ezek sem lehetnek azonban hatékonyak az állami és szupranacionális szervezetek támogatása és a koreguláció általi egységesítése nélkül.[53] Ahogy *Békés* is megjegyzi, az önszabályozásnak nem az állami szabályozás helyett kell létrejönnie, hanem annak kiegészítéseként.[54] *Szádeczky* véleménye szerint az önszabályozás akkor működőképes, ha a gazdasági szereplők felismerik a kisebb működési kockázattal együtt járó versenyelőnyt, és ezzel együtt az állampolgárok és a non-profit szervezetek is belátnák pozitív hatásait.[55]

ÖSSZEGZÉS

Az internetes bűnözés jelensége az 1970-es évektől van jelen, és mára globális problémává vált. Számos próbálkozás történt az ellene való fellépésére a legelső kiberbűnözésről szóló amerikai törvény, a CFAA 1984-es megalkotása óta.[56] Mára – ahogy az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelet is leszögezi – az internet a társadalmi és gazdasági fejlődés alapjává vált, így a védelme is kiemelt fontosságú a társadalom számára. Mivel a jognak relatíve igen fiatal, és a többi életviszonyhoz képest jóval dinamikusabb részterületéről van szó, ennek a védelemnek a kialakítása gyakran tartogat buktatókat mind a jogalkotó, mind a jogalkalmazó számára. A nemzetközi tendenciák némelyike

[49] PARTI – MARIN: *i. m.* 60. o.
[50] A komplex rendszer fejlesztésében részt vevő amerikai Cisco Systems ellen az Egyesült Államokban indított jogi eljárás megszüntetését sokan kritizálták. Ld. COHN, CINDY – REITMAN, RAINEY: Court Lets Cisco Systems Off the Hook for Helping China Detain, Torture Religious Minorities, Electronic Freedom Foundation, elérhető: https://www.eff.org/deeplinks/2014/09/court-lets-cisco-systems-hook-helping-china-detain-torture-religious-minorities (2015.08.09.).
[51] Bővebben ld.: A Freedom House 2013-as jelentése az internetszabadságról, elérhető: https://freedomhouse.org /report/freedom-net/2013/turkey#.VcfHsPm6LIU (2015.08.09.).
[52] DORNFELD: *i. m.* 58. o.
[53] PARTI – MARIN: *i. m.* 63–64. o.
[54] BÉKÉS GERGELY: Internetszolgáltatók a fájlcsere ellen? in *Infokommunikáció és Jog* 2009/5. szám, 194–200. o.
[55] SZÁDECZKY: *i. m.* 149. o.
[56] WARREN – STREETER: *i. m.* 34. o.

nem nyújt valódi megoldást a problémákra, mint az az internetblokkolás kudarcából is kitűnik. Más esetekben a pontatlan, nehezen értelmezhető fogalmazás jelenthet problémát, és így egyébként legális tevékenységek felesleges kriminalizációjához vezethet. Fontos, hogy e hibák tanulságait felhasználva próbáljunk meg minél inkább időtálló szabályozást kialakítani.

A túlságosan szerteágazó, minden részletre kiterjedő állami szabályozás azonban kontraproduktívnak bizonyulna, hiszen ez olyan áttekinthetetlen joganyagot jelentene, amin még a piaci szereplők is nehezen ismernék ki magukat, nem is beszélve az egyszerű felhasználókról. Emellett jelentős terhet róna nem csak a jogalkalmazóra, de a jogalkotóra is, akinek rendszeresen felül kéne vizsgálnia a technika fejlődése miatt folyamatosan elavuló jogszabályokat. Az állami szabályozásnak a legfontosabbakra kell kiterjednie, és minden másban teret kell biztosítania a világháló szereplőinek arra, hogy ezt kiegészítsék és a sajátos viszonyokhoz igazíthassák önszabályozó rendszereikkel.

Mint azt bemutattam, az eljárásjogi szabályozás korántsem járt olyan jelentős változással, mint azt elsőre gondolni lehet a technika jelentős fejlődése alapján. A bevált megoldások, illetve a kudarcok tanulságainak levonása, valamint jogszabályi átültetése nagyon fontos feladat, ugyanakkor ugyanilyen fontos az állomány megfelelő továbbképzése, amely elengedhetetlen ahhoz, hogy az állam sikerrel vehesse fel a harcot a kiberbűnözés jelentette fenyegetéssel szemben.

FELHASZNÁLT IRODALOM

[1] BÉKÉS GERGELY: Internetszolgáltatók a fájlcsere ellen? in *Infokommunikáció és Jog*, 2009/5. szám, 194–200. o.

[2] BERECZ PÉTER: A Német Szövetségi Alkotmánybíróság „számítógép-határozata". in *Studia Juvenum*, 2009, Debrecen, 71–78. o.

[3] BOCIJ, PAUL – MCFARLANE, LEROY: The Internet: A Discussion of Some New and EmergingThreats to Young People, in *Police Journal*, Vol. 76. No. 3. (2003), 3–13. o.

[4] COHN, CINDY – REITMAN, RAINEY: *Court Lets Cisco Systems Off the Hook for Helping China Detain, Torture Religious Minorities, Electronic Freedom Foundation*, elérhető: https://www.eff.org/deep links/2014/09/court-lets-cisco-systems-hook-helping-china-detain-torture-religious-minorities (2015.08.09.).

[5] CZINE ÁGNES: VIII. fejezet, in BELEGI JÓZSEF (szerk.): *Büntetőeljárás I–III - Kommentár a gyakorlat számára*, 2014, HVG-ORAC, Budapest, 806–808. o.

[6] DORNFELD LÁSZLÓ: Fájlmegosztás: a szellemi tulajdonjog legújabb kihívása, in *Diskurzus*, 2014/1. szám, 54–61. o.,

[7] GÁLFFY CSABA – VOITH HUNOR: Nyitott pénztárcával sétálunk a világban, elérhető: http://www.hwsw.hu/hirek/54283/mastercard-visa-paypass-nfc-rfid-biztonsag-kartya-bank.html (2015.08.09.).

[8] GERGELY MÁTÉ: Nyomozás az interneten, in *Belügyi Szemle*, 2002/10. szám, 31–38. o.

[9] KIM, CHRIS – NEWBERGER, BARRIE – SHACK, BRIAN: Computer Crimes, in American *Criminal Law Review*, Vol. 49. Issue 2. (2012), 443–488. o.

[10] LACZI BEÁTA: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, in *Magyar Jog*, 2001/12. szám, 726–738. o.

[11] LENGRÉ MÓNIKA: A XXI. század új típusú próbatétele: az informatikai biztonság, in *Belügyi Szemle*, 2012/5. szám, 5–21. o.

[12] MAJUMDER, SANJOY: *India pornban: How the government was forced to reverse course, BBC Asia*, elérhető: http://www.bbc.com/news/world-asia-india-33810775 (2015.08.09.).

[13] MOHÁCSI BARBARA: Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal, in *Magyar Jog*, 2008/12. szám, 827–832. o.

[14] NAGY ZOLTÁN ANDRÁS: A Pirate Bay-per tanulságai. De lege ferenda a fájlcseréről, in *Ügyészek Lapja*, 2010/2. szám, 33–40. o.

[15] NAGY ZOLTÁN ANDRÁS: *Bűncselekmények számítógépes környezetben*, 2009, Ad Librum, Budapest.

[16] PARTI KATALIN – MARIN, LUISA: Foltvarrással az on-line illegális tartalom ellen: a tartalomblokkolás, a közvetítő szolgáltató felelőssége és az értesítési-levételi eljárás, in *Infokommunikáció és Jog*, 2012/49. szám, 58–65. o.

[17] PARTI KATALIN: Nyomozás az interneten: együttműködés – korlátokkal, in *Belügyi Szemle*, 2004/11–12. szám, 204–220. o

[18] PARTI KATALIN: Tiltott pornográf felvétellel visszaélés az interneten - az empirikus kutatás adatai, in VIRÁG GYÖRGY (szerk.): *Kriminológiai tanulmányok 44. kötet*, 2007, OKRI, Budapest, 89–110. o.

[19] RADU, IOAN – URSACESCU, MINODORA– SENDROIU, CLEOPATRA– CIOC, MIHAI: Computer Crime - A Threat to the International Society, in *Agora International Journal of Juridical Sciences*, Vol. 2. No. 1. (2008), 248–256. o.

[20] RÜTHER, WERNER: Az internet és az „informatikai bűnözés" a kriminológia számára is kihívás, in *Belügyi Szemle*, 2003/2-3. szám, 249–262. o.

[21] SZABÓ IMRE: A fájlcserélő honlapot üzemeltető közvetítő szolgáltatók felelőssége, in *Ügyészek Lapja*, 2010/1. szám, 5–14. o.
[22] SZÁDECZKY TAMÁS: Az IT biztonság szabályozásának konfliktusa, in *Infokommunikáció és Jog*, 2013/3. szám,149–153. o
[23] THAW, DAVID: Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement, in *The Journal of Criminal Law and Criminology*, Vol. 103. No. 3. (2013), 906–948. o.
[24] TÓZSA ISTVÁN: Az elektronikus közigazgatás helyzete, in *Új magyar közigazgatás*, 2012/5. szám, 2–12. o.
[25] O'FLOINN, MICHEÁL – ORMEROD, DAVID: Socialnetworking materialas criminal evidence, in *Criminial Law Review*, Vol. 7. (2012), 486–512. o.
[26] WALL, DAVID S.: *Cybercrime: The Transformation of Crime in the Information Age*, 2007, Polity, Cambridge.
[27] WARREN, PETER – STREETER, MICHAEL: *Az internet sötét oldala*, 2005, HVG, Budapest.
[28] WOLF, JOHNATAN B.: War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money, in *American Journal of Criminal Law*, Vol. 28. Issue. 1. (2000), 95–116. o.

FELHASZNÁLT INTERNETES FORRÁSOK

[1] A digitális menetrend 2014. évi eredménytáblája: helyzetfelmérés, http://europa.eu/rapid/press-release_IP-14-609_hu.htm (2015.08.10.).
[2] A Freedom House 2013-as jelentése az internetszabadságról, https://freedomhouse.org/report/freedom-net/2013/turkey#.VcfHsPm6LIU (2015.08.09.).
[3] Az információs társadalomra vonatkozó statisztika – háztartások és magánszemélyek, Eurostat, http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/hu (2015.07.30.).
[4] Frequently Asked Questions: the new European Cybercrime Centre, Európai Bizottság - MEMO/12/221, http://europa.eu/rapid/press-release_MEMO-12-221_en.htm (2015.08.08.).
[5] Január 11-én megnyílik a számítástechnikai bűnözés elleni európai központ, Európai Bizottság - IP/13/1309/01/2013, europa.eu/rapid/press-release_IP-13-13_hu.htm (2015.08.08.).