

A kibertérben elkövetett bűncselekmények
nyomozásának kérdései

Tartalomjegyzék

Bevezetés.....	2
1. Az internetes nyomozás alapkérdései.....	5
1.1. Bizonyítási eszközök.....	10
1.1.1. IP-cím	10
1.1.2. Hagyományos eszközök	12
1.1.3. Új lehetőségek	13
1.2. Az együttműködés fontossága.....	16
2. Nemzetközi kitekintés	19
2.1. Az USA gyakorlata	19
2.2. Európai szabályozás	21
3. Hazai szabályozás.....	25
4. Összefoglalás.....	30
Irodalomjegyzék.....	33

A számítástechnika fejlődése és elterjedése sok változást hozott az emberek életében. Lassan felnövőben van egy olyan generáció, amelyet már születése óta körbevesznek a modern információtechnikai berendezések, amelyek használata napi rutint jelent számukra. Az új eszközök és különösen az internet adta lehetőségek sokszor könnyebbé teszik az emberek életét, és folyamatos bővülésük rohamosan folytatódik még az elkövetkező években.¹ Mára a lehetőségek növelése, a funkciók fejlesztése azonban fokozatosan másodlagossá vált a biztonsági szempontok mellett, ahogy mind a fejlesztők, mind a jogalkotók és mind a felhasználók elkezdtek felismerni az új kihívásokat.² A jog és az új technológiai vívmányok kapcsolata kezdettől fogva összetetten alakul: míg egy részről folyamatosan zajlik az új lehetőségek felmérése és előnyeinek felhasználása – elég csak az elektronikus közigazgatásra³ vagy e-kereskedelemre⁴ gondolni – addig más részről az internet kihívás elé is állítja az egyes nemzeti jogrendszereket azzal, hogy egyre inkább a bűnözés egyre nehezebben megfékezhető melegágyává válik, és az új környezetből kifolyólag komoly nehézségeket támaszt a büntetőeljárások során.⁵ Az elkövetett bűncselekmények palettája igen széles és sokszínű: a személyes adattal visszaéléstől a csaláson át az ipari kémkedésig, a szoftverkalózkodástól az internetes pedofiliáig és a cyberbullyingtól az öngyilkosságra rábírásig a terrorizmusig terjed.

Az internetes bűnüldözéssel kapcsolatos változások talán a büntetőeljárást érintik legjobban, melynek kimunkált rendszere többször évszázados múltra nyúlik vissza, és nem alkalmazható megfelelően ebben az új helyzetben. Maga a jelenség némileg régebbi, mint elsőre gondolnánk, már az 1970-es években követték el a mai hackertámadások előzményét – akkor még telefonhálózatok ellen. Az Amerikai Egyesült Államok először 1984-ben, a *Computer Fraud and Abuse Act*-tel (CFAA) szabályozta a számítógéppel elkövetett

¹ Az ún. Moore-törvény szerint a modern informatika alapját képező integrált áramkörök összetettsége körülbelül 18 hónaponként megduplázódik. A megállapítást napjainkban egyre többen kérdőjelezzik meg, de az informatika fejlődése ennek fennállásától függetlenül folyamatosan fejlődni fog. Forrás: *Még tíz évig lehet érvényes Moore-törvénye.* Index.hu 2012. május 2. Online: http://index.hu/tech/2012/05/02/meg_tiz_evig_lehet_ervenyes_moore_torvenye/ (Letöltés ideje: 2013. november 13.)

² Peter Warren–Michael Streeter: *Az internet sötét oldala*. HVG Kiadó, Budapest, 2005, 7. o.

³ Ezt a területet szabályozza többek között a 85/2012. (IV. 21.) Kormányrendelet az elektronikus ügyintézés részletes szabályairól

⁴ Fontos összefüggés, hogy maga az elektronikus kereskedelem növekvő mértéke igényli a pontos szabályozást és az elektronikus bűnözés visszaszorítását a felhasználói bizalom fenntartása érdekében. Lásd még: Warren–Streeter: i. m. 79-82. o.

⁵ Parti Katalin: *Nyomozás az interneten: együttműködés – korlátokkal*. In.: *Belügyi Szemle* 2004./11-12. szám 52. évf., 204. o.

csalásokat és adatlopásokat.⁶ A cselekmények számában folyamatos növekedés figyelhető meg: 1991 és 1994 között 500%-kal emelkedett, addig 1997 és 1998 között, egy év alatt duplájára, 3700-ról 8000-re nőtt a bejelentett kiberbűncselekmények száma, ezek pedig egyre több weboldalt és céget érintettek.⁷ Ez nemcsak világviszonylatban, de hazai statisztika alapján is kimutatható: a számítógépes csalások száma 9-ről 304-re, a bankkártyával visszaélések száma pedig 2-ről 379-re nőtt 1995 és 1999 között.⁸ A számítógépek száma ezalatt hét és félszeresére, 91 ezerről 678 ezerre nőtt.⁹ Az Európai Bizottság adatai szerint napjainkban naponta 1 millió ember válik számítástechnikai bűnözés áldozatává, és az okozott kár világviszonylatban elérheti a 388 milliárd dollárt is.¹⁰ A Google Inc. 2013-as átláthatósági jelentése már mintegy 90 000 rosszindulatú programot (ún. malware) terjesztő és adathalász weboldalt tartalmaz. A magyar szolgáltatónál létrehozott weblapok 15%-án található valamilyen káros program.¹¹ A 2011-es PCIPA törvényhez csatolt jelentésben az szerepel, hogy az amerikai Igazságügy Minisztérium adatai szerint a gyermekpornográfia kereskedelme szinte teljesen megszűnt az Egyesült Államokon belül a szigorú törvények miatt, és a folyamat megfordulása csak az internet elterjedésének köszönhető, és az esetek száma évi 150%-os növekedést mutat,¹² melynek gyermekkorú sértettjeit 2003-ban 1 millióra becsülték.¹³ Becslések szerint egy adott pillanatban 750 ezer pedofil található mindig legalább online.¹⁴ A legnagyobb számban azonban az illegális fájlcsere kerül sor, amiben becslések szerint csak az Egyesült Államokban 63 millióan vesznek rendszeresen részt.¹⁵

⁶ Warren–Streeter: i.m. 34. o.

⁷ Jonathan B. Wolf: *War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money*. In: 28 Am. J. Crim. L. 95 2000-2001, 96. o.

⁸ Nagy Zoltán András: *Informatikai bűncselekmények*. In: Magyar Tudomány, 2001/8. szám Online: <http://www.matud.iif.hu/01aug/nagy.html> (Letöltés ideje: 2013. 10. 09.)

⁹ Parti Katalin: *A számítógépes bűnözés és az internet*. Kriminológiai Tanulmányok 40., OKRI, Budapest, 2003, 181. o.

¹⁰ A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében. Európai Bizottság - IP/12/317 28/03/2012 Online: http://europa.eu/rapid/press-release_IP-12-317_hu.htm (Letöltés ideje: 2013. 10. 09.)

¹¹ A Google átláthatósági jelentése. Online: <http://www.google.com/transparencyreport/safebrowsing/> (Letöltés ideje: 2013. 09. 29.)

¹² 112th Congress Rept. 112–281. Online: <http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt281/pdf/CRPT-112hrpt281-pt1.pdf> (Letöltés ideje: 2013. 09. 29.), 5. o.

¹³ Paul Bocij-Leroy McFarlane: *The Internet: A Discussion of Some New and Emerging Threats to Young People*. In: 76 Police J. 3 2003. 7. o.

¹⁴ *How computer-generated 'Sweetie' snared 1000 pedophiles*. AFP, 2013. november 5. Online: <http://www.theaustralian.com.au/news/world/how-computer-generated-sweetie-snared-1000-pedophiles/story-e6frg6so-1226753220112> (Letöltés ideje: 2013. 11. 06.)

¹⁵ A fájlcséről bővebben lásd: Nagy Zoltán András: *A Pirate Bay-per tanulságai. De lege ferenda a fájlcséről*. In: Ügyészek lapja, 2010/2. 17. évf. 33-40. o.

Mielőtt rátérnénk az internetes környezetben elkövetett bűncselekmények felderítésének főbb jellemzőire és problémáira, fontos tisztázni az internetes nyomozás lehetséges jelentéseit és elhatárolni őket. Szűkebb értelemben jelentheti az interneten elkövetett bűncselekmények felderítését és az ahhoz kapcsolódó bizonyítékok begyűjtését, míg tágabb értelemben a nem internetes felületen elkövetett bűncselekmények nyomozása során is sor kerülhet erre, hiszen az itt tárolt adatok, információk fontos bizonyítékokat jelenthetnek. Magyarországon nagy port vert S. Ábel joghallgató ügye, akit az internetes blogjában megjelentetett írásai alapján gyanúsítottak meg 22 rendbeli emberölés előkészületével.¹⁶ Itt, bár a bűncselekmény színtere nem az internet lett volna, mégis fontos információkkal szolgált a nyomozás során. Legtágabb értelemben a nyomozások legnagyobb részében alkalmazásra kerülhet az internet, mint eszköz, hiszen a bűnüldöző szervek is egyre nagyobb részben támaszkodnak az új technológiai lehetőségekre; számos oldal könnyítheti az eljárás során az ügyész és a nyomozó hatóság munkáját.¹⁷ A dolgozatban elsődlegesen és főként a legszűkebb értelmezéssel kapcsolatos kérdések kerülnek bemutatásra és taglalásra. Ennek fő oka, hogy főleg itt érvényesülnek a terület sajátos vonásai, és ez sokkal speciálisabb, mint a másik két értelmezés.

Ezzel összefüggésben fontos meghatározni az internetes bűncselekmény fogalmát is, melyet szerintünk úgy lehet a legáltalánosabban (de nem a legpontosabban) megfogalmazni: minden olyan bűncselekmény, amelynek elkövetésére az interneten kerül sor. Ezzel kizártuk azokat a deliktumokat a vizsgálódásunk köréből, ahol az internet csak segítő vagy közvetítőszerepet lát el, de nem az elkövetés helyszíne. Kérdéses, hogy ennek fogalompárja vagy szinonimája-e a számítógépes bűncselekmény: ma nem olyan egyértelmű a határvonal, mint évekkel ezelőtt, és nem mondható igaznak, hogy minden internetes bűncselekmény egyúttal számítógépes is,¹⁸ leginkább az infokommunikációs eszközök (főleg az internetkapcsolatra képes okostelefonok) fejlődése és elterjedése miatt, amelyek ma már szintén képesek az internetre való rácsatlakozásra.

A dolgozat megírásának fő apropóját időszerűsége adta: napjainkban is folyamatosan növekvő tendenciát mutat az internetes bűncselekmények száma, és ezek egyre több személyt,

¹⁶ A 2011-ben indult ügy 2013. május 19-én első fokon elmarasztaló ítélettel végződött. http://hvg.hu/itthon/20130519_22_embert_akart_megolni_a_joghallgato_k (Letöltés ideje: 2013. 09. 29.)

¹⁷ Néhány hasznos lehetőség és szolgáltatás leírása a mindennapi nyomozásban: Hetényi Gábor: *Informatika a nyomozás szolgálatában*, Ügyészek lapja, 2008/1. szám 15. évf. 43-46. o.

¹⁸ Gergely Máté: *Nyomozás az interneten*. In: Belügyi szemle, 2002/10. 31. o.

vállalatot vagy akár egész államokat¹⁹ érintenek, nemcsak a fejlett országokban. Számos megoldatlan vagy elégtelenül megoldott probléma akad napjainkban az elkövetett bűncselekmények felderítésében, ami több okra vezethető vissza. Ezekre szeretnénk rávilágítani a dolgozatban, és bemutatni egyes más államokbeli megoldási kísérleteket. A fő buktatót ebben a technikai háttér jelenti, ami elmélyült IT ismereteket feltételez. Mivel a dolgozat elsődlegesen jogászoknak íródott, és annak szerzője is felhasználói szinttel rendelkező joghallgató, a szakmaiság megtartásával igyekszünk mellőzni a nehezen érthető technikai kifejezéseket. A téma fontosságán kívül fontos hajtóerő volt még az, hogy napi szintű internet felhasználóként mindig is érdekelték az internetes bűncselekmények és azokkal kapcsolatos jogi kérdések, és meggyőződése, hogy az idővel a bűncselekmények egyre nagyobb részét fogják itt elkövetni, ahogy egyre inkább megtörténik az átállás a papíralapról a számítástechnikai eszközökre.

1. Az internetes nyomozás alapkérdései

A legalapvetőbb kérdés a témakörben a helyszín, az internet működésének bemutatása és szemléltetése, hiszen ennek sajátosságai miatt vannak speciális kihívások az itt folytatott nyomozás során. Anélkül, hogy részletes, nehezen emészthető technikai fejtegetésekbe bocsátkoznánk, egy rövid mondatban megfogalmazhatjuk a lényegét: számítógépes hálózatok világhálózata (un. metahálózat). Ez a hálózat láthatatlan, és egy elkülönült, sajátos rendszert, az úgynevezett kibertérre alkotja, ami önállóan létezik a fizikai valóság mellett. Az ebben részt vevő, folyamatosan bővülő számú számítógépek állandóan kommunikálhatnak egymással, még hozzá kölcsönösen, adatsomagok formájában. Az internet igen fontos sajátossága, hogy azon az adatelérés nincs helyhez kötve, az információ szabadon áramlik a bolygó egyik végéből a másikba, nem törődve az államhatárokkal és jogi szabályozásokkal, így ugyanaz a tartalom elérhető bárhol. Ráadásul a kommunikáció nem egyoldalú – mint például a televízió esetén – hanem kölcsönösen zajlik a felek között.²⁰ Büntetőeljárás szemszögéből vizsgálva talán az egyik legfontosabb a bizonyítás kérdése: mivel minden a kibertérben zajlik, az elkövető nem hagy maga után ujjlenyomatot vagy más, a

¹⁹ Irán atomkutatását súlyosan érintette egy feltételezhetően izraeli-együtt államokbeli közös fejlesztésű vírus, és többek között Magyarországon is több gépet érintett a fertőzés. Pierre Klochender: *With New Malware Virus, Israel Fans A Virtual Flame Against Iran*. Centre for Research on Globalization
Online: <http://www.globalresearch.ca/with-new-malware-virus-israel-fans-a-virtual-flame-against-iran/31169>
(Letöltés ideje: 2013. 10. 09.)

²⁰ Werner Rüter: *Az internet és az „informatikai bűnözés” a kriminológia számára is kihívás*. In: Belügyi szemle, 2003/2-3. szám 51. évf., 250-251. o.

beazonosítására alkalmas fizikai nyomot a cselekmény elkövetése során, így erre támaszkodni nem lehet az azonosítása érdekében.²¹

A bizonyítást különösen nehezíti, hogy más számítógép biztonsági kiskapuit kihasználva, oda betörve akár más gépről is elkövetheti a deliktumot, ami tévútra is terelheti a nyomozó hatóságot a nyomozás kezdeti szakaszában. Ezt nevezik magyarul távoli támadásnak: ekkor az elkövető hozzá nagyon is közeli, ám az adatáramlás szempontjából már jóval távolabbi számítógépről követi el a bűncselekményt.²² Ehhez azonban még csak nem is szükséges feltörni más számítógépeket, elegendő egy olyan távol-keleti vagy harmadik országbeli szolgáltatót keresni, ahol az elégtelen szabályozás miatt jóval kedvezőbb a jogi környezet. Az innen végrehajtott támadások néha áthidalhatatlan akadályokat állítanak a nyomozás útjába. Az internet említett jellege, valamint az elkövetés és a célpont gyakran más helyszíne miatt olyan esetekben is nehéz lehet eldönteni a joghatóság kérdését egy adott ügyben, amikor egyébként kedvezőbb a jogi környezet az együttműködésre. De egy államon belül is nehéz eldönteni, hogy milyen szinten (pl. tagállami vagy szövetségi), illetve hol történjen az elbírálás: amely illetékességi területen a cselekmény elkezdődött, ahol azt elkövették vagy ahol az elkövető vagy a sértett található.²³

A kiberbűnözés, az internetes bűncselekmények általános jogi definíciójának kidolgozása még várat magára Magyarországon, és a jelenség igen színes volta és állandó változásai miatt nehéz is egy pontos és időtálló definíciót alkotni. A világban többször próbálkoztak már ezzel, például a Francia Belügyminisztérium meghatározása szerint ide tartozik minden olyan bűncselekmény, amit nagy valószínűséggel telekommunikációs eszközről követnek el. Az ENSZ definíciója szerint ide értendő minden olyan illegális tevékenység, amely az elektronikus biztonsági rendszerek és a továbbított adatok ellen irányul. A svájci rendőrség meghatározása szerint a modern információtechnológiai eszközökkel elkövetett bűncselekmények értendők ide. E definíciók egyike sem teljesen pontos azonban, és nem fedi le a témakör egészét.²⁴ Az amerikai Igazságügyminisztérium meghatározása szerint a büntetőtörvények minden olyan megszegése, amely az elkövetés, nyomozás és bünvádi eljárás során számítógépes technológia ismeretét feltételezi.²⁵ Ez a

²¹ Laczi Beáta: *A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései*. In: Magyar jog, 2001/12. sz. 48. évf. 726-727. o.

²² Bővebben lásd: Parti Katalin: *A számítógépes...* 199-201. o.

²³ Darin Walker-Deon Brock-T. Ramon Stuart: *Faceless-oriented Policing: Traditional Policing Theories Are Not Adequate in a Cyber World*. In: 79 Police J. 169 2006. 175. o.

²⁴ Ioan Radu-Minodora Ursacescu-Cleopatra Sendroiu-Mihai Cioc: *Computer Crime - A Threat to the International Society*. In: 2008 AGORA Int'l J. Jurid. Sci. 248 2008, 250. o.

²⁵ Chris Kim-Barrie Newberger-Brian Shack: *Computer Crimes*. In: 49 Am. Crim. L. Rev. 443 2012, 444. o.

definíció azonban túlságosan kiterjesztő értelmezésű, és már a dolgozat elején tisztázott értelmezési kérdések alapján sem állja meg a helyét, hiszen egy nem informatikai környezetben elkövetett, de arról ilyen bizonyítékokat felvonultató ügy is az informatikai bűncselekmények kategóriába esne.

Az egyes internetes bűncselekmények más-más aspektusait használják ki az internetnek, és ennek megfelelően szerintünk három nagy csoportra oszthatók: az internet nyilvánosságából fakadó bűncselekmények (pl. becsületsértés), mások adataihoz való jogosulatlan hozzáférés és mások megkárosítása vagyoni előnyök szerzésére (például csalás). SCHMÖLZER és SCHICH más felosztást alkalmaz, a cselekmény megvalósulása alapján. Az ő rendszerükben a felosztás szoftver, hardver és adat ellen irányuló bűncselekményeket foglalja magában.²⁶ QUÉMÉNER a szerint tesz különbséget a cselekmények között, hogy az egy konkrét számítógépes rendszert érint vagy az egész kibernetet.²⁷

Nagyon sokfajta cselekményt sorolhatunk az interneten keresztül elkövethetők közé, amelyek közül némelyik csak erre jellemző, hiszen az új technikai lehetőségeknek köszönhetően jöhetnek létre, és szinte kizárólag itt követhetők el. Ilyen például a hackelés és crackelés,²⁸ vagyis az idegen weboldalakra, programokba való jogtalan behatolás, és ott adatok megszerzése vagy károkozás. Sajátosság még az elosztott szolgáltatásmegtagadással járó támadás (*Distributed Denial of Service*, DDoS), ami a szervereket terheli túl, elérhetetlenné téve a tartalmat. Ehhez tradicionális bűncselekményként zsarolás társulhat, mikor a támadó közli, hogy a tartalom elérhetetlen marad egy bizonyos összeg megfizetéséig, de e nélkül teljesen újként azonosítható.²⁹ Új jellemző még a számítógépeket megfertőző rosszindulatú program készítése (malware írás), mások identitásának jogosulatlan megszerzése, az illegális fájlcsere stb. Ezek azonban leggyakrabban csak technikai szempontok alapján újak, korábban is léteztek a fizikai világban. Az esetek egy jelentős részében arról van szó, hogy már korábban is létező bűncselekményeket ültettek át az új

²⁶ Nagy Zoltán András: *Informatikai...*

²⁷ Hivatkozta Radu-Ursacescu-Sendroiu-Cioc: i. m. 249. o.

²⁸ A két fogalmat gyakran keverik, vagy hacker megnevezés alatt összevonják. A megkülönböztetést Eric Raymond kezdte el alkalmazni a Katedrális és a Bazar című művében. A hackerek ebben a felosztásban azok, akik a rendszerek gyengeségeit és saját képességeiket tesztelik és erről utóbb a sértettet is tájékoztatják, míg a crackerek, akik haszonszerzésre törekednek és károkat okoznak másoknak. (Eric S. Raymond: *Cathedral and the Bazaar*. Sebastopol, 2001) Más felosztásban a hacker számítógépes rendszerekbe hatol be, míg a cracker számítógépes programokat tör fel, például a másolásvédelem eltávolítására. Hogy morálisan bármelyik igazolhatóan cselekszik-e (pl. utóbb felhívja a tulajdonos figyelmét a védelmi hibákra vagy csak képességeit teszteli), az a mai napig vitás kérdés. (Gergely Máté: i. m. 33. o.)

²⁹ Susan W. Brenner: „*At Light Speed*”: *Attribution and Response to Cybercrime/Terrorism/Warfare*. In: 97 J. Crim. L. & Criminology 379 2006-2007. 385. o.

felületre, ahogy a technológia terjedése, vagyis a potenciális áldozatok számának folyamatos bővülése egyre jövedelmezőbbé tette ezt a formát az elkövetők számára. Ilyen például az interneten elkövetett zaklatás, csalás, illegális fájlmegosztás, zsarolás, kémkedés, terrorizmus stb.³⁰ Ezek egy része pusztán egy másik, fizikai világban elkövetett bűncselekmény elősegítésére is elkövethető, mint amikor orosz hackerek feltörték az ukrán rendőrség lopott autókkal foglalkozó adatbázisát, hogy könnyen értékesíteni tudják az általuk eltulajdonított járműveket.³¹ Bizonyos bűncselekmények azonban, mint a szexuális erőszak vagy emberrablás, amik kifejezett fizikai ráhatást igényelnek, valószínűleg nem ültethetők át a kibertérbe. Nem igaz ez azonban az emberölésre, elegendő csak arra gondolni, hogy elektronikus úton megbénítják valaki létfenntartó berendezését vagy átírják a szükségesen adagolandó gyógyszer mennyiségét egy kórház rendszerében. Bár a mai napig nem jelentettek be ilyen esetet, a gyakorlatban nem elképzelhetetlen.³²

Komoly veszélyt jelent az, hogy nemcsak a technikailag járatos személyek vihetik véghez a fentebb említettek tevékenységeket. Némelyik cselekmény minimális technikai ismerettel követhető el (például az internetes zaklatás vagy cyberbullying), és a nagyobb súlyú cselekmények elkövetése is egyre könnyebbé válik magának az internetnek a következtében, mivel például a hackerek megosztják egymással tudásukat, és a kísérletezni vágyó felhasználók számára egyre több technikai leírás válik elérhetővé.³³ Már 1997-ben lehetséges volt, hogy az Intel rendszerét feltörő hacker teljesen ingyenesen hozzáférhető programokat használhasson cselekménye elkövetéséhez.³⁴ Mindezekon túl ma már viszonylag olcsón, pár ezer forintnak megfelelő áron lehet rosszindulatú programokat vásárolni különböző, erre szakosodott internetes oldalakon. Ezeknél a cselekményeknél inkább az az új elem, hogy a fizikai világban történő megvalósításhoz képest jelentősen nagyobb anonimitással követhetők el, ami vonzóbbá is teszi ezt az elkövetők számára.³⁵ Ők nem csak profi bűnözők lehetnek, hanem egyszerű felhasználók is, a világ bármely pontjáról, kihasználva annak lehetőségét, hogy nemcsak szűkebb környezetükben, hanem a világ távoli pontjain követhetik el a cselekményt, ismeretlen emberek ellen.

A szervezett bűnözés is kezdi felismerni az ebben rejlő lehetőségeket, és igyekszik kihasználni az új lehetőségeket a nagyobb haszonszerzés reményében. Maga a vállalkozó

³⁰ A gyakori internetes bűncselekmények részletesebb felsorolását lásd: Warren–Streeter: i.m. 24. o.

³¹ Warren–Streeter: i. m. 46. o.

³² Susan W. Brenner: i. m. 384. o.

³³ Laczi Beáta: i. m. 727.; Warren–Streeter: i.m. 36. o.

³⁴ Johnatan B. Wolf: i. m. 99. o.

³⁵ Darin Walker-Deon Brock-T. Ramon Stuart: i. m. 169. o.

informatikusok toborzása is az interneten zajlik, ahol az általuk használt kommunikációs csatornákat figyelik, és a megfelelőnek vélt személyeket „megkönyékezik”. Többféle modell létezik a szervezett bűnözés és az informatikusok kapcsolatára: bevehetik tagjaik közé vagy bérelhetik pusztán a tudását pénzért, akár anélkül, hogy közölnék velük, kikkel kerültek kapcsolatba. De gyakran az is megesik, hogy saját tagjaik közül taníttatnak ki informatikusokat egyetemeken.³⁶ Az internetes pedofiliában igen jelentős még a szervezettség jelenléte és csoportok részvétele, amelyek több százezer kép cseréjét bonyolíthatják le, és akad köztük olyan, amelyik 7000 taggal bírt egy időben, különböző országokból.³⁷

A sikeres eljárás szempontjából igen fontos kérdésnek számít az elkövetett cselekmény észlelése, ami nélkül nem kerülhet sor a nyomozás megindítására, és így az ügy felderítésére sem. Az FBI becslése szerint az internetes adatlopással vagy károsítással kapcsolatos 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.³⁸ Hasonlóan nehéz lehet több más, látható nyommal nem járó cselekmény észlelése, például a mobiltelefon átprogramozása vagy a biztonsági kikapukat nyitó programok telepítése a sértett számítógépen, ami további bűncselekmények (pl. adatlopás) technikai megalapozója lehet.³⁹ Az internetes prostitúció szintén a nehezen észlelhető tevékenységek közé tartozik, hiszen az ebben résztvevők úgy álcázhatják magukat, hogy nem derül ki egyértelműen a szolgáltatás jellege (pl. masszőrszolgáltatás), és a fizetés is jóval könnyebb az ügyfél számára, például egy internetes oldal kívánságlistája (a felhasználó által megvásárolni kívánt termék)⁴⁰ valamely elemének a megvásárlásával.⁴¹ Cyberstalking esetén az online megfigyelés gyakran történhet a sértett tudta nélkül, és mint GILLESPIE is megjegyzi, nem érdemes a felelősségi kérdésekkel foglalkozni, amíg a sértett nem észleli a cselekményt, ami pedig sokszor nem jár látható nyomokkal, csak elszólásokból derülhet ki, hogy az elkövető olyan információk birtokában van, amikről egyébként nem lehetne tudomása.⁴² Az internetes pedofília esetén a leggyakrabban az Interpol megkeresése,

³⁶ A szervezett bűnözés informatikai módszereihez bővebben lásd: Warren–Streeter: i. m. 42-52. o.

³⁷ Paul Bocij-Leroy McFarlane: i. m. 8. o.

³⁸ Johnatan B. Wolf: i. m. 100. o.

³⁹ Laczi Beáta: i. m. 727. o.

⁴⁰ Ugyanez a funkció segíthet pedofiloknak a kiszemelt gyermekkorúak bizalmába férkőzni. Lásd: Paul Bocij-Leroy McFarlane: i. m. 11. o.

⁴¹ Darin Walker-Deon Brock-T. Ramon Stuart: i. m. 172. o.

⁴² Alisdair A. Gillespie: *Cyberstalking and the Law: A Response to Neil MacEwan*. In: Criminal Law Review, 2013/1. 41. o.

lakossági bejelentés alapján vagy hivatalból észlelik a bűncselekményeket.⁴³ A nagy cégek azonban gyakran igyekeznek titokban tartani a hackerbetöréseket, még ha tudomásukra is jut: egy 1999-es amerikai felmérés szerint csupán a komoly hackertámadások 32%-át jelentették a hatóságoknak, így a legtöbb ügyben nem is indulhatott nyomozás.⁴⁴ Az együttműködés problémájával később még foglalkozni fogunk részletesebben, hiszen ez több fontos szempontból érinti a sikeres büntetőeljárást, amiből a legelső a cselekmény bejelentése.

Fontos még megjegyezni, hogy ha észlelnék is egy cselekményt, nehéz rögtön azonosítani annak jellegét, hiszen könnyedén lehet kiberbűncselekmény, kiberterrorizmus vagy kiberháború a cél. Míg az első két esetben a nyomozó hatóságra tartozik (de azon belül is eltérő szervezet lehet jogosult eljárni, ami hatásköri vitát szülhet), az utolsó esetben katonai választ igényel.⁴⁵ Jól megfigyelhető, hogy a korábban jól elhatárolható belső-külső fenyegetés közötti határvonal mennyire elhalványul az új technológiai vívmányok következtében, és végső soron ez is a büntetőeljárást késleltető tényezők között kell, hogy említésre kerüljön.

1.1. Bizonyítási eszközök

1.1.1. IP-cím

Mint fentebb már szó esett róla, a kibertérben elkövetett bűncselekményeknél az elkövető beazonosítása és a bizonyítási eszközök fellelése jóval nehezebb. Az azonosításnál nem lehet a hagyományos nyomokra támaszkodni például az ujjlenyomat hiánya miatt. Helyette az interneten úgynevezett IP-címek (*Internet Protocol*) kerülnek kiosztásra a felhasználóknak. Ezt a szolgáltatótól kapja az adott számítógép, amikor csatlakozik a szolgáltató szervergépére, vagyis az internetre. A szerver feljegyzi ezt az adatot minden adatküldésnél és fogadásnál, így ennek alapján visszakövethető az interneten folytatott kommunikáció. Mivel pedig az egyes IP-címek hozzátársíthatók az előfizető személyhez, így az IP-címek a legfontosabb nyomot jelenthetik egy nyomozás során.⁴⁶ Jelenleg az IPv4 privát címtartomány szerinti egyedi számsorok kerülnek kiosztásra az internetre csatlakozó felhasználóknak, ami négy 0-tól 255-ig terjedő számból áll. Ez azonban csak korlátozott számú IP-cím kiosztását teszi lehetővé, ami azonban lassan nem elegendő az összes felhasználó egyidejű kiszolgálására. Jelenleg az egyszerre több milliárd cím kiosztását

⁴³ Gergely Máté: i. m. 38. o.

⁴⁴ Johnatan B. Wolf: i. m. 102. o.

⁴⁵ Susan W. Brenner: i. m. 380. o.

⁴⁶ Bővebb technikai leírásért lásd: Kökényesi Attila: *Az internet útján elkövetett bűncselekmények vonatkozásában végzett házkutatás*. In: Ügyészek Lapja, 2008/Különszám 15. évf. 8. o. és Darin Walker-Deon Brock-T. Ramon Stuart: i. m. 173. o.

lehetővé tévő IPv6 fejlesztése folyik. Bár ez egyelőre sok esetben csak új biztonsági kockázatokat szül, és új lehetőséget ad a hackerek számára az IPv4-re szabott védelem megkerülésére, hosszú távon az internet biztonságosabbá válását jelentheti. Ugyanis míg jelenleg az IP-címek dinamikusan változnak minden egyes kapcsolódással, addig az új változat bevezetésével minden eszköz állandó címet kaphat, ami jelentősen megkönnyíti majd a nyomozó hatóság munkáját.

Mivel az internetszolgáltató tárolja a beazonosításhoz szükséges adatokat, a nyomozó hatóság azokat megkérheti, és felhasználásával elviekben eljuthat az elkövetőig. Azonban a helyzet korántsem ilyen egyszerű. Már az is nehézségeket okozhat, ha egy háztartásban többen élnek, vagy egy nagyobb közösség használ egyetlen internetkapcsolatot, nem is beszélve arról, ha vezeték nélküli internetkapcsolatot használnak, és azt egyáltalán nem védik jelszóval. Ilyenkor bárki rácsatlakozhat a hálózatra, és a szolgáltató számára úgy fog megjelenni, mintha az adott előfizető folytatná a hálózati kommunikációt, holott az illetéktelenül rácsatlakozó személy az.⁴⁷ A korábban már említett távoli támadások is részben az IP-cím, mint nyom eltüntetését szolgálják. Ezekben az esetekben nemcsak eltüntetik a nyomokat, de hosszabb időre akár tévútra is terelhetik az elkövetők a nyomozó hatóságot, hátráltatva a büntetőeljárást, és a határidők miatt akár el is lehetetlenítve azt. Mint LACZI megállapítja, ezen felül akár az is elképzelhető, hogy a továbbiakban már nem lehet teljes bizonyossággal a felhasználót kizárni az elkövetésből.⁴⁸ További nehézséget jelent a felderítésnél, hogy az IP-cím több országban, köztük Magyarországon is személyes adatnak minősül, így nehézségekbe ütközhet a nyomozó hatóság számára ennek megszerzése. 2008-ban Peter Shcarr német adatvédelmi biztos is így nyilatkozott az Európai Parlament meghallgatásán, főleg azon érv alapján, hogy ez az adat a használat időpontjával együtt egyértelműen egyetlen személyhez kapcsolható.⁴⁹ Finnországban egy esetben azért nem adta ki a közvetítő szolgáltató az elkövető IP-címét, mert kötötte „a telekommunikációs szolgáltatásokban érvényesülő bizalmi elv”.⁵⁰ A kérdés hazai vonatkozásáról és hatályos szabályozásáról részletesebben a magyar szabályozás részen belül lesz szó.

Ezen felül léteznek olyan anonimizáló eszközök, amiket tudatosan a kommunikáció titkosítására fejlesztettek ki. Ezek közül a legismertebb a Tor (*The Onion Router*), ami az

⁴⁷ Kökényesi Attila: i. m. 9-10. o.

⁴⁸ Laczi Beáta: i. m. 726. o. és Darin Walker-Deon Brock-T. Ramon Stuart: i. m. 174. o.

⁴⁹ Aoife White: *IP Addresses Are Personal Data, E.U. Regulator Says*. The Washington Post 2008. január 22. Online: <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html> (Letöltés ideje: 2013. 11. 14.)

⁵⁰ K.U. v. Finnország, 2872/02 ítélet, EJEB, 2009. március 2.

internethez hasonlóan amerikai katonai fejlesztésként indult el, majd a civil életben tett szert nagy jelentőségre. A program használatához egy klienst kell telepíteni, amin keresztül a kommunikáció folyik. A küldött adat végig titkosítva halad a két fél között, méghozzá úgy, hogy az egész adatsomag egy mesterkulcsot kap, míg minden részlete egy-egy első szintű kulcsot (innen kapta nevét is, hiszen többrétegű, akár csak egy hagyma). Ez kilenc véletlenszerűen választott közvetítőgépen is keresztülfut, és a program időről-időre megújítja ezt az útvonalat. Ezek a titkosítás miatt nem tudják visszafejteni az adat tartalmát, illetve azt sem, hogy pontosan honnan érkezett, és ezeket a nyomozó hatóságnak is szinte lehetetlen megtalálni. A bűnözők egyre jobban kezdik felismerni a technológia előnyeit, így számos tiltott tartalomhoz és szolgáltatáshoz hozzáférhetnek, mint például a Silk Road nevű kábítószer-árusító oldalhoz,⁵¹ vagy a Lolita City gyermekpornográf felvételeket tartalmazó weblaphoz, anélkül, hogy félniük kellene a lelepleződéstől. Az amerikai Nemzetbiztonsági Ügynökség (National Security Agency, NSA) nemrég nyilvánosságra került dokumentumai szerint egyelőre csak felhasználói hibák, és célzott, nagy erőfeszítéssel járó kerülőutak segítségével tudják a küldött azonosítani.⁵² Ez akár több száz munkaórát is igényelhet a nyomozó hatóság részéről, és ez a jelentős ráfordítás a nyomozásra csak nagyobb súlyú cselekményeknél lehet arányos a hatóság részéről, így akár az eljárás megszüntetéséhez is vezethet, ha más nyom nem áll rendelkezésre. Az anonimizálás nemcsak IP-címeknél képzelhető el, hanem a törvénysértő tartalom (pl. gyermekpornográfia) is elrejtethető más tartalomra, például más kép- vagy zenefájlokra belülről, hogy csak a megfelelő szoftverrel és jelszóval bírók érhessek azt el; ezt nevezik szteganográfiának.⁵³ Bár a módszer igen biztonságos módja a törvénysértő adatok titkos továbbításának, könnyedén észrevehető, ha egy fájl mérete jóval nagyobb, mint az egyébként indokolt lenne annak tartalma alapján.⁵⁴

1.1.2. Hagyományos eszközök

A hagyományos bizonyítási eszközök is alkalmazhatóak az internetes környezetben folytatott nyomozás során. A tanúvallomás, különösen a sértett vallomása, illetve a cselekmény technikai adatai nagy jelentőséggel bírhatnak a bizonyításban. Különösen igaz ez,

⁵¹ Az oldal feltételezett működtetőjét 2013. október 2-án tartóztatta le az FBI. USA v. Ross William Ulbricht. Online: <http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf> (Letöltés ideje: 2013. 10. 09.)

⁵² Az alkalmazott technikai módszerekről részletesebben: Bruce Schneier: *Attacking Tor: how the NSA targets users' online anonymity*. The Guardian, 2013. október 4. Online: <http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity> (Letöltés ideje: 2013. 10. 09.)

⁵³ Paul Bocij-Leroy McFarlane: i. m. 9. o.

⁵⁴ Warren–Streeter: i. m. 89. o.

ha a tanúvallomást olyan személytől szerzik be, aki a megtámadott rendszer informatikusa, biztonsági szakembere vagy rendszergazdája. Míg előbbi esetben a cselekmény körülményeiről derülhetnek ki fontos információk, utóbbi esetben a tanú speciális képzettsége lehet a nyomozó hatóság hasznára. Nagy jelentőséggel bírhat a terhelt vallomása is, azonban a büntetőeljárás alapelvei szerint erre senki sem kötelezhető, illetve a bűnösséget kell bizonyítani, nem az ártatlanságot, így csak erre egyértelműen nem építhető a bizonyítás.⁵⁵ Ráadásul egy kutatás szerint az internetes vonatkozású tiltott pornográf (mai terminológia szerint gyermekpornográf) felvétellel való visszaéléses ügyekben a gyanúsított félrevezető vagy irreleváns védekezése jobban hátráltatta az ügyet, mint az internetes vonatkozással nem rendelkező ügyeknél.⁵⁶ Minden ügynél fontos a szakértő kirendelése, mivel különleges, a felhasználói szintet meghaladó szakismeretre van szükség a technikai háttér komolyabb megértéséhez, a szoftverek működésének, az adott program elkövetéséhez alkalmasságának, a jogtisztaság és számos egyéb kérdésnek a megállapításához.⁵⁷ Mint PARTI is rámutat, itt a bizonyítékok megszerzése, értékelése már önmagában egy olyan tevékenység, ami nagyfokú szakértelmet igényel.⁵⁸ A szakértő kirendelése mellett azonban fontos, hogy az ügyészek és a nyomozó hatóság is valamennyire képzett legyen az informatikában, hiszen ők irányítják a nyomozást és nekik kell a kérdéseket megfogalmazniuk felé, illetve a bíróságon bizonyítaniuk a történetet, a szakértő csak támasz lehet ebben, nem helyettesíti a szaktudást.⁵⁹ Ezeken túl az elkövetési eszközön elektronikusan tárolt adatok jelenthetnek még fontos bizonyítékot, ez azonban komolyabb ügyeknél csak az eljárás későbbi szakaszában kerülhet elő. Bár a nyomait eltüntetni akaró hacker törölheti őket vagy szándékosan félrevezető módon módosíthatja, a számítógépek eredetileg tárolt adatait szakemberek vissza tudják nyerni különleges módszerrel, még ha meg is próbáltak tőlük szabadulni.⁶⁰

1.1.3. Új lehetőségek

A bizonyítás során számos új lehetőséget kínál fel maga az elkövetés helye, a kibertér. Ezek azonban nemcsak az itt elkövetett cselekmények nyomozásánál használhatóak, mint az IP-cím, hanem szinte bármilyen ügyben relevanciával bírhatnak. Tipikusan ilyennek

⁵⁵ Laczi Beáta: i. m. 727-733. o. nyomán

⁵⁶ Parti Katalin: *Tiltott pornográf felvétellel visszaélés az interneten - az empirikus kutatás adatai*. In: Kriminológiai tanulmányok 2007/44. 98. o.

⁵⁷ Laczi Beáta: *Tiltott...* 727-733. o. nyomán

⁵⁸ Parti Katalin: i. m. 97. o.

⁵⁹ Parti Katalin: *Újratervezés, avagy miért fontos az elektronikus bizonyítékszerzés?* In: Rendészeti szemle, 2010/3. 58. évf. 101-102. o.

⁶⁰ A technikai magyarázatra lásd: Warren–Streeter: i.m. 88. o.

tekinthető az ismertségi hálókön (angolul *social network*) vagy más néven közösségi oldalakon megosztott információk felhasználása. Az angol szabályozás szerint az ilyen közösségi oldalakon (például a Facebookon vagy a Twitteren) található információk kinyomtatva okiratnak minősülhetnek, amennyiben a bíróság elfogadja őket. Az innen származó információk hitelességét illetően nincs egységes gyakorlat, és egyértelmű, hogy csak nagy körültekintéssel lehet őket elfogadni bizonyító erejüként. Bárki készíthet más nevére szóló hamis felhasználói profilt vagy közzétehet más nevében, ha megszerezi a jelszavát vagy felhasználói gondatlanság révén hozzáférést szerez.⁶¹ A *Commonwealth v. Williams* ügyben a bíróság nem fogadta el az ismertségi hálókön történt kommunikációban részt vevők vallomását elegendőnek arra, hogy bizonyítsa a vádlott bűnösségét, arra hivatkozással, hogy akár más is hozzáférhetett az adott profilhoz.⁶² Az ismertségi hálók nyomozásbeli haszna ettől függetlenül igen nagy lehet, hiszen a felhasználók önként osztanak meg igen fontos információkat magukról. Ezek az oldalak akár az ismeretlen tettesek azonosításában is szerepet játszhatnak: egy esetben az elkövetőt úgy sikerült megtalálni, hogy barátnője, aki miatt a testi sértést féltékenységből elkövette, bocsánatkérő üzeneteket küldött a sértettnek, aki a Facebookon megtalálta a lány ismerősei között támadóját.⁶³ A holland *Terre des Hommes* gyerekjogi szervezet számítógépes programmal generált kiskorú segítségével 2013-ban tíz hét alatt 20 ezer pedofillal került kapcsolatba 71 országból, és közülük ezret a közösségi média segítségével azonosítani is tudtak.⁶⁴ A feltöltött képekből a tanúk is tájékozódni tudnak, és sok nyugati országban meg is teszik. Hosszú távon akár a felismerésre bemutatás is mellőzhetővé válhat személyek vonatkozásában, ha megfelelő képek állnak rendelkezésre róla a közösségi oldalakon. Azonban, mint arra az *O'FLOINN–ORMEROD* szerzőpáros is felhívja a figyelmet, míg a hagyományos esetben több gyanúsítottat mutatnak be, addig a közösségi oldalakon egyes személyeket keresnek, ami előítéletekhez vezethet.⁶⁵ Ez azonban könnyedén áthidalható, ha egy olyan elektronikus rendszert készítenek, ami az összes gyanúsított képét mutatja be egyszerre, és a sértett így választhat. A bizonyítékként való felhasználás szándéka esetén vigyázni kell arra is, hogy a nyomozó hatóság ne kényszerítse a terheltet a jelszava megadására, ez ugyanis több eljárási alapelvbe is ütközhet, például az önvádra kötelezés tilalmába. A szerzőpáros végkövetkeztetésével azonban nem

⁶¹ Micheál O' Floinn–David Ormerod: *Social networking material as criminal evidence*. In: *Criminal Law Review* 2012/7. szám 486-512. o.

⁶² Williams 456 Mass. 857

⁶³ O'Floinn–Ormerod: i. m. 499-500. o.

⁶⁴ *How computer-generated...* AFP.

⁶⁵ O'Floinn–Ormerod: i. m. 500. o.

érték egyet, mivel arra jutnak, hogy megbízhatatlansága miatt nem érdemes külön bizonyítási eszközként foglalkozni a közösségi oldalakra feltett tartalommal.

Ez a konzervativizmus igen kontraproduktívnek bizonyulhat egy olyan gyorsan változó és fejlődő területen, mint a kibertérben elkövetett bűncselekményeknél folytatott nyomozás esetén, hiszen a felhozott érvek alapján (más is hozzáférhetett, nem igazolható száz százalékosan, hogy ki írta, hamisítható stb.) minden internetes, sőt számítástechnikai úton tárolt bizonyíték megkérdőjelezhetővé válik. Ma már nem nehéz írott okiratokat sem hamisítani, csak kevésbé igényel több befektetést, mint egy elektronikus adaté vagy dokumentumé. A szerzők által idézett bírói vélemények azt mutatják, hogy nemcsak a jogalkotók, de a jogalkalmazók részéről is nagyfokú bizalmatlanság áll fenn az új technológiai vívmányok irányába. Való igaz, hogy az ilyen bizonyítékok önmagukban nem bizonyító erejűek, de más, egybevágó bizonyítékokkal együtt a sikeres bizonyítás alapját jelenthetik. Az internetes bizonyítékszerzésnél nagyon körültekintőnek kell lenni, különösen, ha az adott cselekményt a kibertérben követték el, és ezért a fizikai világban bizonyítékok jóval kisebb számban találhatók. Fontos, hogy a bizonyítás mindig kontextusban történjen, és a szükségesnek látszónál mindig több adat kerüljön megőrzésre.⁶⁶ Az új, internetes bizonyítékok kérdésben PARTI véleményével maradéktalanul egyetértünk, aki rámutat, hogy mint más esetknél, a hagyományos bizonyítékszerzés ideje is lassan lejár az egyre nagyobb fokú digitalizáció következtében. Az általa összeállított táblázat jól bemutatja a két forma közötti eltérésekből fakadó előnyöket. Ezek közül ki kell emelni a gyorsabb bizonyítást, a könnyebb együttműködést, a hitelesebben és hosszú ideig változatlanul megőrizhető bizonyítékokat, az új rendszerezési elvek bevezetésére való lehetőséget, és a környezettudatosabb hozzáállást, mivel így nem generálódik annyi, később szemétnek tekinthető anyag.⁶⁷

Nemcsak a közösségi oldalakra feltöltött képek jelenthetnek segítséget a nyomozásban, de akár maguk a bűncselekményt megvalósítók is, ha kellőképpen óvatlanok például egy gyermekpornográf felvétel elkészítésekor. Az Egyesült Királyságban 2002-ben úgy tudtak egy pedofil képeket készítő férfit elfogni, hogy analizálták a feltöltött képeket, a ennek alapján sikerült beazonosítani lakhelyét (például a háttérben az ablakon keresztül látható épületekről).⁶⁸ Ez a módszer időigényes, de sokszor az egyetlen lehetőséget jelentheti

⁶⁶ Parti Katalin: *Újratervezés...* 103. o.

⁶⁷ Parti Katalin: *Újratervezés...* 100-101. o.

⁶⁸ Paul Bocij-Leroy McFarlane: i. m. 7. o.

arra, hogy felkutassák az elkövetőt, különösen, ha a korábban már említett anonimizációt alkalmazza a cselekmény elkövetésénél.

Új bizonyítási eszközként merül fel a számítógép online történő átvizsgálása, más néven az online házkutatás, amely a legmodernebb informatikai eszközöket igényli, és jelentős sikereket ígér az alkalmazónak. Ezt a fajta eszközt akkor lehet alkalmazni, ha a beazonosítás olyan fokig jutott el, hogy akadnak konkrét személyek, akik kapcsolatba hozhatók az elkövetéssel. Ekkor ugyanis konkrét számítógépre kell rendőrségi kémprogramot telepíteni vagy közvetlenül, vagy az interneten keresztül, és annak adatai átkutathatóvá válnak. A számítógépen keresztül pedig a lakás megfigyelésére is lehetőség adódik, ha található hozzá csatlakoztatva vagy beépítve mikrofon és kamera. A módszer alkalmazásának elsősorban a szervezett bűnözéssel és terrorizmussal kapcsolatba hozható ügyeknél lenne nagy jelentősége, ahogy a tervezett német szabályozás is szerette volna, mert ezek olyan ügyek, ahol az online házkutatás okozta alapjogsérelem arányos lehet az elkövetett cselekménnyel. Gazdasági deliktumoknál és általános preventív célzattal is felmerült alkalmazása, és míg az előző talán megállná a helyét, utóbbi mögött nincs olyan jelentős érdek, hogy azzal magyarázható lenne az alapjogsérelem. Ugyanis a kibertérben sokkal inkább igaz, mint a fizikai világban, hogy bárki potenciális elkövető lehet, végső soron ez pedig az összes felhasználó megfigyeléséhez vezethetne.⁶⁹

1.2. Az együttműködés fontossága

Az internet fentebb vázolt sajátosságai és a bizonyítás nehézségei miatt együttműködésre van szükség. Ez több szereplő között is meg kell, hogy valósuljon az eredményes büntetőeljárás lefolytatásához. Egyrészt szoros együttműködésre van szükség több nemzet bűnüldöző szervei között, ha országhatárokon átnyúló bűncselekmények miatt kell nyomozni. Másrészről szükség van ezen hatóságok és az internetszolgáltatók közötti együttműködésre, az IP cím, mint fontos bizonyíték beszerzésére, amelyet csak innen lehet beazonosítani. Végül szükség van a magánszektor, a felhasználók és a nyomozó hatóság együttműködésére, hogy előbbieket az őket ért internetes bűncselekményeket bejelentsék, és azok ne maradjanak felderítetlenül abból az okból, hogy ismeretlenek maradnának a hatóságok számára.

⁶⁹ Az érintett alapjogok kapcsán részletesebben lásd: Mohácsi Barbara: *Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal*. In: Magyar Jog, 2008/12. 55. évf. 827-832. old.

A bűnügyi szervek együttműködését európai szinten az Europol és az Eurojust koordinálja, előbbi a nyomozó hatóság, utóbbi az ügyészség szintjén. Az Európai Bizottság az Europolon belül 2013. január 1-jével létrehozta a számítástechnikai bűnözés elleni európai központot (European Cybercrime Centre, a továbbiakban EC3), aminek feladata az Unión belül elkövetett kiberbűncselekmények országhatárokon átívelő felderítése érdekében folytatja működését. A központ feladata operatív és igazságügyi támogatás nyújtása az egyes tagállami rendőrségeknek, mivel felismerték, hogy ezek ereje önmagában sokszor nem elég a sikeres eljárás lefolytatására.⁷⁰ Fókuszában elsősorban az elektronikus banki szolgáltatásokat és egyéb internetes pénzügyi tevékenységeket érő hackertámadások, a gyermekek szexuális kizsákmányolása és az olyan bűncselekmények állnak, amelyek az EU-n belüli kritikus infrastruktúrákat és információs rendszereket érintik.⁷¹ A sikeres felderítésben fontos szerepe van európai szinten az Európa Tanács 2001-es egyezményének a számítástechnikai bűnözésről.⁷² Ennek aláírói a 25. cikk a „lehető legszélesebb körben” kötelezi jogsegély nyújtására a nyomozások és eljárások során. A cikk 3. pontja lehetővé teszi sürgős esetben a telefonos és faxes megkeresést is, amit a megkeresett fél kérelmére kell hivatalosan megerősíteni. A 4. pont szerint nem lehet az elutasítás oka, hogy az adott bűncselekményt a megkeresett fél a pénzügyi bűncselekmények közé sorolja, míg az 5. pont szerint teljesítettnek kell tekinteni a jogsegélynyújtás feltételeként kiköthető mindkét fél részéről fennálló büntethetőséget, ha az adott cselekmény bűncselekménynek minősül a megkeresett fél belső jogában, függetlenül az elnevezési és a besorolási kérdésektől. Ezek a rendelkezések nagyban könnyítik a nyomozó hatóságok munkáját, hiszen az időigényes és az eltérő jogi környezet miatt nehézkes jogsegélyi eljárást jelentősen megkönnyíti és meggyorsítja, például az eltérő besorolás és megnevezés figyelmen kívül hagyásával és a gyors megkeresés lehetőségének biztosításával.

Fontos európai szabályozás még a 2006/24/EK irányelv, amely az (5) pontjában megállapítja, hogy a szolgáltatásnyújtók számára bűnüldözési érdekből adatmegőrzést előíró nemzeti jogszabályok jelentősen eltérnek, és kötelezi a szolgáltatókat, hogy bizonyos ideig megőrizték, majd kérelem esetén a nyomozó hatóságnak átadják az irányelvben meghatározott adatokat. Az Unión kívül azonban csak különböző bilaterális és multilaterális

⁷⁰ Január 11-én megnyílik a számítástechnikai bűnözés elleni európai központ. Európai Bizottság - IP/13/13 09/01/2013 Online: europa.eu/rapid/press-release_IP-13-13_hu.htm (Letöltés ideje: 2013. 10. 13.)

⁷¹ A kritikus infrastruktúra itthoni megnevezése létfontosságú rendszer és létesítmény, melyek védelmével és meghatározásával a 2012. évi CLXVI. törvény foglalkozik. Ide tartozik minden olyan rendszerelem és létesítmény, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához.

⁷² Hazánkban a 2004. évi LXXIX. törvény hirdette ki.

egyezmények biztosítják az együttműködést. Így fordulhat elő, hogy míg Spanyolország könnyedén megkeresheti a latin-amerikai országokat az Iberred alapján, addig Ukrajnával csak közvetítőkön keresztül tud kapcsolatot teremteni.⁷³ Az együttműködés lehet informális (a common law országokban), illetve formális (kontinentális jog) jellegű is, amelyek azonban csak formájukban térnek el, és ettől függetlenül általában sikeresen végződnek.

Fontos kérdés még a jövőre nézve a magánszektor és az állam együttműködése is. A némileg mesészerű történet szerint akkor került sor az egyik legelső ilyen együttműködésre a nyomozás során, amikor egy clevelandi FBI ügynök kért segítséget cégektől. Miután az ügy nagy sikerrel zárult le, felhívta a figyelmet erre a lehetőségre az amerikai bűnüldöző szerveknél. Ebből született az InfraGard ötlete, amely az amerikai internetfigyelésbe a cégeket vonta be.⁷⁴ Az Egyesült Államok 2001-ben közzétett kiberbiztonsági nemzeti tervében is felismerte a magánszektor bevonásának fontosságát, mivel a kritikus infrastruktúra 80%-a magánkezelésben volt. Így a programban a partneri hozzáállást, és a szabályozás növelésének elkerülését tűzték ki célul, hogy ne kényszerítsék többletkiadásokra a cégeket. A program ezen kívül az önszabályozás felé mutató módon csak akkor helyezi kilátásba az állami beavatkozást, ha a cégek kudarcot vallanak a biztonság biztosításában. A 2002-es kiberbiztonsági stratégia is ezen az úton haladt tovább, 5 csoportra osztva a kiberbiztonságban érdekeltet az otthoni felhasználóktól a globális kérdésekig, szintenként eltérő feladatokkal.⁷⁵ Az üzleti élet szereplői azonban gyakran bizalmatlanok az állammal szemben, mivel a nyomozó hatóságot általában alkalmatlankodónak és túl merevnek tartják. Phil Karn szerint a biztonsági fejlesztések egy részét az állam beavatkozásának megelőzése miatt készítik, továbbá úgy kommentálta a nyomozó hatóság erőfeszítéseit, hogy „ha az egyetlen eszközöd a kalapács, az egész világ szögnek tűnik”.⁷⁶ Ennek a hozzáállásnak a fő oka WOLF szerint az, hogy míg nem sok előnyt remélnek a hatósági úttól, addig félnek attól, hogy az ügyfelek a cég védelmének gyengeségeként és végső soron megbízhatatlanságaként fogják értékelni a betörés tényét. 1994-ben a Citibank a húsz legnagyobb befektetéssel bíró ügyfelét veszítette el, amikor kiderült, hogy egy hackertámadás miatt 10 millió dolláros kár érte, bár ennek nagyobb részét utóbb sikerült visszaszerezni.⁷⁷ Ez volt az úgynevezett Levin-ügy,

⁷³ Parti Katalin: *Újratervezés...* 105-106. o.

⁷⁴ Warren–Streeter: i.m. 65-67. o.

⁷⁵ Pergel Józsefné: *A biztonságosabb információs társadalom érdekében tett nemzetközi lépések*. Online: <http://www.jit.hu/dok/doku/biztrov4.pdf> (Letöltés ideje: 2013. 11. 17.) 8-10. o.

⁷⁶ Johnatan B. Wolf: i. m. 102. o.

⁷⁷ Johnatan B. Wolf: i. m. 102. o.

amelynél a betörést a rendszerbe Szentpétervárról követték el.⁷⁸ Európai szinten az Európai Parlament és a Tanács 460/2004/EK rendeletével létrehozott Európai Hálózat- és Információbiztonsági Ügynökség feladata a köz- és magánszektor közötti együttműködés megteremtése. Ez az együttműködés mindkét fél érdekeit szolgálja, így kiemelten fontos feladatot végez ennek alapjait megteremtve.

Mivel az internetet szabályozó jogszabályok számos kérdésben eltérőek, szükség lenne arra is, hogy ne csak a jogalkalmazók között valósuljon meg együttműködés, hanem a jogalkotói szinten is közeledjenek a szabályozások egymáshoz. Komoly problémát jelent a mindenhol eltérő jogi környezet, az egymást sokszor nem fedő szabályok, aminek következtében ugyanaz a kibertérben elkövetett cselekmény egyik államban büntetendő, a másikkban pedig nem. Különösen a határokon átvélő elektronikus kereskedelemnél fontos kérdés ez, és talán e téren a legfontosabb a jogalkotók közötti nemzetközi együttműködés.⁷⁹ A témakörben született nemzetközi megállapodások egyike a korábban már említett Európa Tanács 2001-es számítástechnikai bűnözésről szóló egyezménye. Ez egyaránt foglalkozik büntető anyagi- (2-13. cikk) és eljárásjogi kérdésekkel (14-21. cikk), amely a rendszerek és adatok lefoglalásának és átadásának biztosítása érdekében kötelez a megfelelő jogalkotási aktusokra.

2. Nemzetközi kitekintés

2.1. Az USA gyakorlata

Más államok szabályozásának áttekintésénél fontos kiemelt figyelemmel kezelni az Amerikai Egyesült Államokat, ahol igen komoly mértékben jelentkezik a kiberbűnözés, és az első országok között van, amelyek jogszabályi úton igyekeztek az internetet szabályozni. Ezért a dolgozat a világ többi részéről külön, részletesebben is áttekinti a fontosabb vonatkozó törvényeket. Itt született az internetes bűncselekmények visszaszorítására a legelső törvény, a *Computer Fraud and Abuse Act* (CFAA) 1984-ben, és azóta mind szövetségi mind tagállami szinten számos intézkedés követte. A CFAA-t több alkalommal is kiegészítették: 1986-ban, 1989-ben, 1994-ben, 1996-ban, 2001-ben (Patriot Act), 2002-ben és 2008-ban, így két évtizedes jogalkotói munka eredménye. A törvény elsősorban azokat a számítógépeket védi, amelyek szövetségi érdekkörbe tartoznak, így a közigazgatási, a banki, a katonai és a

⁷⁸ Warren–Streeter: i. m. 43. o.

⁷⁹ Radu-Ursacescu-Sendroiu-Cioc: i. m. 254. o.

kereskedelmi rendszereket.⁸⁰ WOLF cikkében azt rója fel az amerikai jogalkotónak, hogy számos elégtelenül szabályozott kérdést hagytak, és sok esetben a meglévő szabályokat duplikálták. A törvény egyik legnagyobb hibájának tartja, hogy teljesen külön próbálja kezelni az internetes bűncselekményeket más deliktumoktól.⁸¹

Bár elsődlegesen a büntetőjogi tényállásokat fogalmazza meg, több büntetőeljárás, elsősorban hatásköri rendelkezés is található benne. A 18 USC § 1030 (d) pont (1) bekezdése alapján a törvényben kriminalizált cselekményekben nyomozhat az Egyesült Államok titkosszolgálat is. Ez valószínűleg annak tudható be, hogy több bűncselekmény komoly nemzetbiztonsági kockázatot jelenthet, és más államok vagy csoportok megbízásából, illetve állampolgárai vagy tagjai követhetik el. A (2) bekezdés alapján az (a) pont (1) bekezdésében részletezett bűncselekmények esetén azonban az FBI-nak van elsőbbsége, így például a kémkedés, különösen az atomtikok kikémlelése, a külföldi kémelhárítás, a nemzetvédelem és a külföldi kapcsolatok miatt védett információk engedély nélküli közzététele ügyében, kivéve, ha ezek más jogszabály alapján a titkosszolgálat hatáskörébe tartoznak. Az FBI-on belül a törvényben nevesített bűncselekményeknél történő nyomozásra létrehozták a National Computer Crime Squadot (NCCS).⁸² A törvény, bár számos hibával küzdött megszületése pillanatától kezdve,⁸³ több más államnak példaként szolgált az adatokhoz való jogosulatlan hozzáférés és módosítás szabályozása kérdésében.⁸⁴ A CFAA hatályát 2011-ben a 8. Körzeti Fellebbviteli Bíróság mobiltelefonokra is kiterjesztette a *United States v. Neil Scott Kramer* ügyben hozott ítéletével.⁸⁵ Ez hivatkozza a törvény azon rendelkezését, hogy számítógépnek minősül egy eszköz ha „számítási, logikai és tárolási műveleteket hajt végre”, valamint az ítélet indokolásában idézi az egyik szakértőt, aki szerint „ma már mindenben van számítógép”. Ezzel a törvény nemcsak a személyi számítógépekkel elkövetett cselekményeket, hanem a más infokommunikációs eszközökkel elkövetett deliktumokat is bünteti, azonban szerintünk hibás az ilyen, technológiai, vagyis ténykérdési szempontból megkérdőjelezhető kiterjesztés alkalmazása, helyett tisztább lett volna a szövegezés

⁸⁰ Charles Doyle: *Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws*. Congressional Research Service, 2010. december 27. Online: <http://www.fas.org/sgp/crs/misc/RS20830.pdf> (Letöltés ideje: 2013. 10. 06.)

⁸¹ Johnatan B. Wolf: i. m. 97. o.

⁸² Az NCCS honlapja. Online: <http://www.tscm.com/comperim.html> (Letöltés ideje: 2013. 11. 15.)

⁸³ Bővebben a CFAA kritikájáról lásd: Scott Zambo: *Digital La Cosa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime*. In: 33 New Eng. J. on Crim. & Civ. Confinement 551 2007 551-575. o.

⁸⁴ Kim-Newberger-Berrie: i. m. 487. o.

⁸⁵ 10-1983 *United States v. Neil Scott Kramer*

módosítása és pontosítása a változó időknek megfelelően, még ha az angolszász jogrendszerhez az előbbi megoldás közelebb is áll.

A 2011-ben elfogadott *Protecting Children from Internet Pornographers Act* (PCIPA) 4. szakaszának (a) pontja szerint a kereskedelmi internetszolgáltatók kötelesek megőrizni legalább egy évig az ügyfeleknek kiosztott IP címeket, olyan módon, hogy a felhasználó beazonosítható legyen. Ezek az adatok csak a kormányzati szerveknek elérhetőek. Ez a törvényi rendelkezés azt szolgálja, hogy internetes bűncselekmények esetén az egyik legfontosabb nyom, az IP cím könnyen elérhető legyen a nyomozó hatóság számára, és ne töröljék őket túlságosan hamar, néhány napon vagy héten belül, amikor valószínűleg még nem is észlelték az adott bűncselekményt. A törvény (b) pontja arra vonatkozik, hogy adatlopás esetén a felhasználók megfelelő értesítést kapjanak, hogy a szükséges lépéseket meg tudják tenni, így például az illetékes szervekhez forduljanak. Ezzel az intézkedéssel valószínűleg az is cél, hogy áthidalják a sértettek és a nyomozó hatóság közötti elégtelen kapcsolatot.

2.2. Európai szabályozás

Bár az internetet az Egyesült Államokban találták fel, az európai hatalmak ismerték fel először jelentőségét a civil életben, különös tekintettel az e-kereskedelemre (amely, mint már utaltunk rá, az eredője a kiberbűnözésnek és a biztonság iránti igénynek) és elterjedése a CERN technikusainak köszönhető. Európa, még ha nem is a leghamarabb kezdett a megalkotásához, szintén elől jár az internet szabályozásában, ezért fontos az európai, különösen a több országra kiható jogszabályokat is megfigyelnünk, főleg mivel az Európai Unió jogszabályai hazánkra nézve is kötelezőek. Ennek megfelelően ebben a fejezetben elsősorban az EU kapcsolódó irányelveit elemezzük, másrészt az Európa Tanács által elfogadott egyezményeket, határozatokat. Bár utóbbiak nem feltétlenül csak a szűkebb értelemben vett Európában érvényesülnek, az európai szabályozás fontos részét képezik.

Az Európa Tanács már igen hamar felismerte a számítástechnikai úton elkövetett bűnözés elleni küzdelem fontosságát és több ehhez kapcsolódó ajánlást is kiadott, többek között 1985-ben,⁸⁶ 1987-ben,⁸⁷ 1988-ban,⁸⁸ 1989-ben⁸⁹ és 1995-ben.⁹⁰ A Miniszteri Bizottság

⁸⁶ A Miniszteri Bizottság R (85) 10. számú Ajánlása a bűnügyi jogsegélyről szóló európai egyezmény alkalmazása a távközlés hálózatok lehallgatására vonatkozó megkeresések kapcsán

⁸⁷ A Miniszteri Bizottság R (87) 15. számú Ajánlása a személyes adatok rendőrségi felhasználására vonatkozó szabályozásról

⁸⁸ A Miniszteri Bizottság R (88) 2. számú Ajánlása a szerzői és szomszédos jogokkal kapcsolatban elkövetett jogsértések elleni küzdelem érdekében hozandó intézkedésekről

1989-ben kiadott ajánlása több eljárásjogi problémára is rámutatott az új környezetben elkövetett bűncselekmények kapcsán. Ezek három fő témakört érintettek: a nyomozó hatóságok kényszerítő ereje a bizonyítékgyűjtésnél, a bizonyítékok összegyűjtése, tárolása és személyekhez történő társításának jogszerűsége az eljárás során és a számítógépes bizonyítékok felhasználása a bíróság előtt. Az ajánlásban a bizonyítás kapcsán felmerült az adattovábbító rendszerekben tárolt adatok átkutatásának és lefoglalásának lehetősége, a tanúk aktív együttműködésre kötelezése az általános jóval nagyobb körben, a telekommunikációs rendszerek figyelése és a számítógépek adatforgalmának lehallgatása. Az Európa Tanács további jelentős lépéseket tett a kibertérben fellelhető káros tartalmak ellen az ezredforduló óta, és létrejöttek a korábban már említett számítógépes bűncselekmények (2001)⁹¹ és a gyermekek szexuális kizsákmányolása és szexuális bántalmazása elleni (2007)⁹² egyezmények is.

Az Európai Unió szabályozás fontos része a korábban már említett 2006/26/EK irányelv, mellyel már korábban foglalkoztunk. Ez az adatok megőrzésével foglalkozik, melyeket később felhasználhat a nyomozó hatóság a nyomozás során. Az Európai Parlament és a Tanács korábban már említett 460/2004/EK rendelete rendelkezik az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, melynek feladata a magas szintű szakértelem kifejlesztése és az együttműködés elősegítése az internetbiztonságban érintettek között. A számítógépes rendszerek elleni támadásokkal foglalkozik a Tanács 2005/222/IB kerethatározata, amelynek célja a tagállamok igazságügyi és egyéb hatóságai közötti együttműködés javítása a tagállamok büntető jogszabályainak az információs rendszerek közelítése révén. A kerethatározat a joghatóság kérdésében hoz fontos intézkedéseket, így ezeknél a bűncselekményeknél joghatóság állapítható meg, ha egészben vagy részben az adott állam területén követték el (fizikailag ott tartózkodott az elkövető vagy ottani információs rendszer ellen irányult), adott állampolgársággal rendelkezik az elkövető, vagy olyan jogi személy javára követték el, amelynek tevékenysége végzésének központja a tagállam területén található. Ezek között sorrend is van, így az elkövetés helye az elsődleges a joghatóság szempontjából, azt követi az állampolgárság és végül az az ország, ahol az elkövetőt megtalálták. A Tanács 2008/114/EK irányelve foglalkozik az európai kritikus

⁸⁹ A Miniszteri Bizottság R (89) 9. számú Ajánlása a számítógéppel kapcsolatos bűncselekményekről

⁹⁰ A Miniszteri Bizottság R (95) 13. számú Ajánlása az információs technológiával összefüggő büntető eljárásjogi problémákról

⁹¹ ETS 185 Az Európa Tanács Egyezménye A számítástechnikai bűnözésről (Budapest, 23.XI.2001.)

⁹² ETS 201 Az Európa Tanács Egyezménye A gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen. (Lanzarote, 25.X.2007.)

infrastruktúra kijelölésével, melyeket olyan létfontosságú rendszerelemként határoz meg, amelyek kiesése legalább két tagállamot súlyosan érintene. Egyértelműen ide sorolhatók olyan alapvető informatikai rendszerek is, melyek támadás alá kerülése esetén az e-kereskedelem, és így az összes tagállam gazdasága veszélybe kerülne. Ezek védelmére a 10. cikk alapján kapcsolattartó pontot kell kinevezni, amely koordinálja a hazai védelmet a tagállamon belül, a Bizottsággal és a többi tagállammal. Fontos előrelépés volt a már említett EC3 létrehozása 2013. január 1-jétől kezdve, mely az Europolon belül jött létre, és annak infrastruktúráját használja. A központ három fő területen végez tevékenységet: az internetes szervezett bűnözés, az áldozatnak komoly sérelmet okozó ügyek (pl. gyermekpornográfia) és a kritikus infrastruktúrát célzó támadások elleni küzdelemben. A központ egyik fő célja a Hálózat- és Információbiztonsági ügynökséghez hasonlóan az együttműködés elősegítése a tagállamok, harmadik államok, a tudományos szakértők, az internetbiztonságban érdekelt cégek, civil szervezetek stb. között.⁹³ Az EC3 honlapján továbbmutató linkek találhatóak azon tagállami weboldalakra, ahol online jelenthetőek be kiberbűncselekmények.⁹⁴ A magyar nyelvű honlapot, a <http://www.biztonsagosinternet.hu>-t a Nemzeti Hálózatbiztonsági Központ üzemelteti. Idén született meg az Európai Parlament és a Tanács irányelvjavaslata a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről, amelynek deklarált célja az egységesen magas szintű hálózat- és információbiztonság megteremtése. A javaslat három alapcél tűzött ki: 1) a hálózat- és információbiztonság területén tevékenykedő hatóságok létrehozása 2) az illetékes hatóságok együttműködése az összehangolt információcsere, valamint az uniós szinten történő felderítés és reagálás érdekében és 3) a magán- és a közszféra közötti információ megosztás gyakorlattá tétele. Ezzel együtt hozták nyilvánosságra az Európai Unió kiberbiztonsági stratégiáját, amely a nyílt, biztonságos és megbízható kibertér létrehozását célozza.⁹⁵

A közvetítő szolgáltató a hozzáférést, információtovábbítást, tárhelyet, gyorsítótárat és keresőszolgáltatást biztosítás a felhasználó számára.⁹⁶ Felelősségének kérdését Európai Unió szinten a 95/46/EK irányelv az adatvédelemről és a 2000/31/EK irányelv szabályozza, amelyek rendelkezései alapján az ilyen szolgáltató sem büntetőjogi, sem polgári jogi

⁹³ *A collective EU response to cybercrime*. Europol. Online: <https://www.europol.europa.eu/ec3> (Letöltés ideje: 2013. november 13.)

⁹⁴ <https://www.europol.europa.eu/content/report-cybercrime-online> (Letöltés ideje: 2013. 11. 17.)

⁹⁵ *Cyber Security strategy and Proposal for a Directive*. Európai Bizottság. Online: <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security> (Letöltés ideje: 2013. 11. 17.)

⁹⁶ Parti Katalin - Marin, Luisa: *Foltvarrással az on-line illegális tartalom ellen: a tartalomblokkolás, a közvetítő szolgáltató felelőssége és az értesítési-levélteli eljárás*. Infokommunikáció és Jog, 2012/49. 59. old.

felelősséggel nem bír a jogsértő tartalom miatt, hacsak nem ő maga tette közzé, ő választotta ki a fogadó feleket vagy módosította, esetleg szűrte a tartalmat. A 2009/136/EK irányelv is leszögezi, hogy a közvetítő szolgáltatónak nem feladata döntenie az adott tartalom jogszerűsége felől, és nem felel a felhasználó által közzétett információ továbbításáért.⁹⁷ Főszabály szerint azonban a tartalom feltöltője felel a jogsértésért és neki kell viselnie annak jogi következményeit. Az Emberi Jogok Európai Bírósága 2013-ban hozott ítéletet a Delfi AS v. Észtország ügyben.⁹⁸ A Delfi a legnagyobb észt internetes hírportál, melynek cikkeihez naponta 10 ezer kommentet fűznek az olvasók. 2006-ban az egyik cikkhez számos sértő, fenyegető hangvételű hozzászólás érkezett, és a sértett cég kártérítést követelt az oldaltól, valamint a sértő üzenetek eltávolítását, ami még aznap megtörtént. Első fokon a Delfinek kedvező ítélet született, másodfokon és a legfelsőbb bíróság előtt azonban a fellebbező cégnek adtak igazat. Az EJEK nem találta szólásszabadságot sértőnek az ítéletet, mivel indoklásuk szerint a Delfinek kellett volna biztosítania, hogy ezek a felhasználói hozzászólások nem jelennek meg és válnak publikussá. Bár ez az ítélet egy polgári jogi ügyben keletkezett, a büntetőjogon belül is nagy vita van arról, felelőssé tehető-e a szolgáltató az oldalán a felhasználók által közzétett törvénysértő tartalomért, főleg ha azt valamilyen elv alapján szelektálta. Különösen az olyan oldalak esetén kérdéses ez, ahol úgynevezett felhasználói tartalommal találkozhatunk, vagyis az adott oldal tartalmát teljesen annak felhasználói határozzák meg. A Társaság a Szabadságjogokért az ügygel kapcsolatban hangot adott azon véleményének, hogy a tartalomszolgáltató és a közvetítő szolgáltató bizonyos esetekben egybe esik, ha egy szolgáltató saját tárhelyen saját tartalmat tesz közzé, de egyébként elválík egymástól.⁹⁹ Ez az ítélet abba az irányba mutat, hogy legalábbis a polgári jogi igény szempontjából az adott szolgáltató is felelőssé tehető, ám az EJEK jelen esetben az EU szabályozással szembemenő döntést hozott, ami hosszú távon komolyan érinti a jogbiztonságot. A szolgáltatóknál közzétett jogsértő tartalom eltávolítására két lehetőség kínálkozik: az adott tartalom blokkolása a hivatalos szervek megkeresésére (hazánkban elektronikus adat hozzáférhetetlenné tétele), illetve az önszabályozáshoz kapcsolódó értesítési-eltávolítási eljárás (notice-and-takedown, N&TD). Előbbi esetén a tervezett német szabályozás kudarca mutatja jól, milyen nehéz megfelelően szabályozni a kérdést: az alkalmazott módszerrel nem lehetett volna jól elkülöníteni a legális és illegális tartalmakat,

⁹⁷ Parti Katalin - Marin, Luisa: i. m. 59. o.

⁹⁸ Delfi AS v. Észtország, 64569/09 ítélet, EJEK, 2013. október 10.

⁹⁹ Dojcsák Dalma: *No comment*. A Társaság a Szabadságjogokért blogja Online: http://ataszjelenti.blog.hu/2013/10/16/no_comment_453 (Letöltés ideje: 2013. 11. 17.)

így ártalmatlan oldalak is törlésre kerültek volna, valamint a blokkolás csak a 10 ezer felhasználó feletti német internetszolgáltatókat érintette volna, így aki nem ezek valamelyikénél fizetett elő az internetre, továbbra is elérte volna a tartalmakat.¹⁰⁰ Ezzel szemben az N&TD eljárás jóval kevesebb problémát vet fel és gördülékenyebben alkalmazható, mivel nem közvetlenül a rendőrséget, hanem az online forrádrótokat használja fel, amelyek felszólítják a közvetítő szolgáltatót a tartalom eltávolítására.¹⁰¹

A nemzeti szabályozások áttekintésénél érdemes megemlíteni a számítógépek online átvizsgálásának lehetőségét, ami több országban is elfogadott gyakorlattá vált. Ezzel ellentétes eredményre jutott a német Legfelsőbb Bíróság 2007-es StB 18/06 számú ítéletében, amely a számítógépek titkos átvizsgálását megtiltotta a német nyomozó hatóság számára. A bíróság szerint alapvető jogokat érintő garancia, hogy miként házkutatást sem lehet titokban végezni, a számítógép átvizsgálására se kerülhessen így sor (mint ahogy arra magyar vonatkozásban SZÁDECZKY is rámutat).¹⁰² 2008. február 27-én a Szövetségi Alkotmánybíróság megsemmisítette Észak-Rajna–Vesztfália alkotmányának online házkutatást lehetővé tevő rendelkezéseit, miután alkotmányellenesnek minősítette.¹⁰³ A kategorikus tiltás véleményünk szerint nem jó irány, hiszen a gyanúsítás közlése előtt sok fontos adat kerülhetne így a nyomozást végző szerv birtokába. Éppen ezért célszerű lenne elválasztani az elektronikusan tárolt adat és az elektronikus úton folytatott kommunikáció megítélését a kérdésben: előbbinél a házkutatás, utóbbinál az engedélyhez kötött titkos adatszerzés és információgyűjtés szabályait lenne célszerű alkalmazni.

3. Hazai szabályozás

A hazai szabályozást tekintve a legfontosabb a Be. rendelkezéseit áttekinteni és értelmezni, hiszen ez a törvény szabályozza a nyomozást, amely a dolgozat témáját képezi. Elsőként vizsgálva a nyomozó hatóság kérdését, a törvény nem tartalmaz speciális rendelkezést a kiberbűncselekmények vonatkozásában, így általános szabályként itt is érvényesül, hogy a rendőrség jár el nyomozó hatósággént (Be. 38. §). Ez alól a szerzői jogok terén van eltérés a (2) bekezdés (c) pont második fordulatóban, ahol a Nemzeti Adó- és Vámhivatal jogosult eljárni, de itt sem tesz a jogalkotó különbséget, hogy az interneten vagy máshol valósul meg.

¹⁰⁰ Bővebben a német szabályozásról lásd: Parti Katalin - Marin, Luisa: i. m. 60-61. o.

¹⁰¹ Bővebben a német szabályozásról lásd: Parti Katalin - Marin, Luisa: i. m. 62-63. o.

¹⁰² Parti Katalin: *Kerekasztal-beszélgetés az online terrorizmusról*. In: Ügyészek Lapja, 2010/2. 17. évf. 43-51. o.

¹⁰³ Mohácsi Barbara: i. m. 827. o.

Fontos kérdés, hogy milyen bizonyítási eszközökről és kényszerintézkedésekről rendelkezik a törvény, amit az internetes nyomozásban is fel lehet használni. Korábban már foglalkoztunk ezekkel a dolgozatban, így itt csupán a hatályos magyar szabályozást ismertetjük. A kibertérben elkövetett cselekményeknél lehetséges bizonyítási eszközök lehetnek: a tanúvallomás (Be. 79. §), a terhelt vallomása (Be. 117. §), szakértői vélemény (Be. 99. §), a tárgyi bizonyítási eszköz (Be. 115. §) és az okirat (Be. 116. §). A kényszerintézkedések közül a házkutatás (Be. 149. §), a lefoglalás (Be. 151. §), az információs rendszerben tárolt adatok megőrzésére kötelezés és az elektronikus adat ideiglenes hozzáférhetetlenné tétele (Be. 158/A. §) alkalmazható. Továbbá a nyomozás során lehetőség van bírói engedélyhez kötött titkos adatszerzésre (Be. 200. §) is.

A 79. § (1) bekezdés alapján tanúként bárki kihallgatható, akinek a bizonyítandó tényről tudomása lehet. Mivel az interneten két eszköz között folyik a kommunikáció, nehezen elképzelhető, hogy a tanú ne legyen sértett vagy a sértettel kapcsolatban álló személy, például egy cég rendszergazdája. Ők főleg a bűncselekmény számítástechnikai eszközön található adataival járulhatnak hozzá a sikeres nyomozáshoz. A terhelt vallomása még mindig igen fontos bizonyítási eszköz a nyomozó hatóság számára, azonban több szempontból is óvatossá kell lenni értékelésénél. Legelőször figyelembe kell venni, hogy a terhelt személye gyakran nem ismert a nyomozás során, csak más bizonyítékok megszerzése után válik azonosíthatóvá (sőt, az IP-címnél ismertetett esetekben akár vakvágányra is kerülhet a nyomozás) és ha ismert is, a törvény nem köt ki a vallomásánál igazmondási kötelezettséget, csupán annyi korlátozást tesz, hogy mást bűncselekmény elkövetésével hamisan nem vádolhat (Be. 117. § (4)). A terhelt szándékosan félrevezető vallomásával összezavarhatja a nyomozást végzőt, aminek lehetősége az internetes vonatkozású ügyeknél nagyobb.¹⁰⁴ Főleg elképzelhető ez, ha az elkövetők képzetesebbek, mint a bűnüldöző szervek állománya, és egy 2001-es felmérés szerint az elkövetők 85%-a belső munkatárs, 11%-a pedig hacker vagy cracker.¹⁰⁵ Beismerő terhelti vallomás esetén is kiköti a Be, hogy az egyéb bizonyítékokat meg kell szerezni.

A szakértő szerepét már korábban hangsúlyoztuk a kibertérben történő nyomozás során. PARTI korábban említett adataira támaszkodva látható, hogy míg internetes szállal nem rendelkező ügyekben 21 alkalommal rendeltek ki számítástechnikai szakértőt, addig az internetes vonatkozású ügyeknél ez a szám 112 volt.¹⁰⁶ Ahogy azt már szintén említettük, nem

¹⁰⁴ Parti Katalin: *Tiltott...* 98. o.

¹⁰⁵ Laczi Beáta: i. m. 729. o.

¹⁰⁶ Parti Katalin: *Tiltott...* 108. o.

elegendő, ha az eljárásban résztvevők közül egyedül csak ő ért az informatikai szakterülethez, hiszen nem a szakértő az ügy ura, hanem csak egy - bár kétségtelenül rendkívül fontos - szereplő a sikeres bizonyításban.¹⁰⁷ 2002 és 2005 között 36 esetben fordult elő, hogy a szakértőnek feltett kérdések nem voltak alkalmasak arra, hogy a bizonyítást szolgálják. IT-szakértő alkalmazása jelenleg nem kötelező a Be. 99. § (2) bekezdés alapján, azonban a jövőre nézve érdemes lenne megfontolni ennek bevezetését (természetesen annak mérlegelésével, hogy ez jelentős összeggel terheli meg a büntetőeljárás költségét) a számítástechnikai félreértésekből, rossz felszerelésből és a képzetlenségből fakadó elégtelen bizonyítások elkerülésére. A kör szűkíthető is lenne, nem minden esetben lenne indokolt a szakértő bevonása: az említett időszakban például 88 esetben lett volna lehetőség arra, hogy a rendőrség elvégezze a szakértőnek kiadott feladatokat, ha rendelkezik a megfelelő eszközökkel.¹⁰⁸ Így tehát a rendőrség eszközeinek modernizálása és szakirányú képzése sok esetben ki tudná váltani a szakértő alkalmazását a nyomozás során. A Be. 105. § (2) bekezdés alapján a szakértő megismerheti az ügy iratait, jelen lehet eljárási cselekményeknél, a kirendelőtől adatokat kérhet. Ennek megfelelően igazán jelentős szerepe a házkutatásnál, információs rendszerben tárolt adatok megőrzésére kötelezés idején – annak ideje alatt folyik azon adatok átvizsgálása, amelyeket később lefoglálnak – és a lefoglalás előkészítésénél és végrehajtásánál lehet, hiszen ő tudja, pontosan milyen adatokra van szükség, hogy megfelelően elkészíthető legyen a szakvéleménye. Az elkészült szakvéleményt a Be. 108. § alapján szóban kell előadni vagy írásban előterjeszteni, a Be. 110. § szerint pedig a szakértő a bíróságon meghallgatható. Itt LACZI megállapítása tűnik helytállónak, vagyis, hogy az írásban történő véleményadás és a meghallgatás együttesen történő alkalmazására lenne szükség a technikai részletek bonyolultsága, és az ezzel kapcsolatban felmerült kérdések tisztázása, magyarázata miatt.¹⁰⁹

A tárgyi bizonyítási eszköz olyan dolog, amely bizonyítandó tény bizonyítására alkalmas. Az informatikában ilyen lehet például a hardver, melyen a törvénysértő tartalmat tárolják, a klónozott, hamis telefonkártya vagy bankkártya stb.¹¹⁰ Ettől azonban sokkal lényegesebb a bizonyítás szempontjából az az adat, amely magához a bűncselekményhez kapcsolódik (pl. naplófájlok a felkeresett weboldalakról) vagy tárolása bűncselekményt valósít meg (pl. gyermekpornográfia). Ezeknek az adatoknak azonban közvetítőre van

¹⁰⁷ Parti Katalin: *Újratervezés...* 102. o.

¹⁰⁸ Parti Katalin: *Tiltott...* 97. o.

¹⁰⁹ Laczi Beáta: i. m. 728. o.

¹¹⁰ Laczi Beáta: i. m. 729. o.

szükségük, hogy tárolhatók legyenek: ezek tipikusan az adathordozók (pl. merevlemez, DVD, pendrive). A Be. 115. § (2) bekezdés úgy rendelkezik, hogy tárgyi bizonyítási eszköz az irat, a rajz és minden olyan tárgy, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Így az adathordozók is tárgyi bizonyítási eszköznek minősülnek és bizonyítékként felhasználhatók. Az okirat valamely adat, tény valóságának, esemény megtörténtének bizonyítására alkalmas irat. Mivel a Be. 116. § (3) bekezdés kimondja, hogy a számítástechnikai rendszerre és az ilyen rendszer útján rögzített adatokat tartalmazó adathordozóra nem alkalmazhatóak az okirat szabályai a (2) bekezdés szerint, így e bizonyítási eszköz jelentősége a bizonyítási eszközök között nem túl jelentős, relevanciája a kibertéren kívül keletkező bizonyítékoknál lehet, például egy telefon híváslistája lehet okiratként felhasználható.

A kényszerintézkedések közül elsőként tekintsük át a házkutatást. Korábban nem volt egyértelmű, hogy egy számítógép átkutatása bizonyítékok után ennek vagy pedig szemlének minősül-e,¹¹¹ ma már azonban egyértelműen nevesíti a Be. 149. § (1) bekezdés a házkutatásnál számítástechnikai rendszer vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozó átvizsgálását. A (2) c pontja pedig deklarálja, hogy házkutatásnak helye van bizonyítási eszköz megtalálása érdekében. Házkutatást bíróság, az ügyész és a nyomozó hatóság is elrendelhet, illetve a bíróság és az ügyész igénybe veheti a nyomozó hatóságot a lefolytatásához. Amennyiben a házkutatás sikerrel jár, további alkalmazható kényszerintézkedés a lefoglalás és az információs rendszerben tárolt adatok megőrzésére kötelezés. A bíróság, az ügyész, illetőleg a nyomozó hatóság rendelheti el annak a dolognak, illetőleg számítástechnikai rendszernek vagy ilyen rendszer útján rögzített adatokat tartalmazó adathordozónak a lefoglalását, amely bizonyítási eszköz. Az adathordozó esetén maga a merevlemez, DVD stb. kerül lefoglalásra, és az ezeken található adatok később felhasználhatók bizonyítékként. Ha magára az adatra rendelnek el lefoglalást, akkor a végrehajtás során gondoskodni kell olyan másik számítástechnikai rendszerről vagy adathordozóról, amelyre az átmásolható. Az információs rendszerben tárolt adatok megőrzésére kötelezést (korábban számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés) a Be. 158/A. § szabályozza. A kényszerintézkedés alkalmazása során a bűncselekmény felderítése és a bizonyítás érdekében az információs rendszerben tárolt adat birtokosának, feldolgozójának, illetőleg kezelőjének az így rögzített meghatározott adat feletti rendelkezési joga ideiglenes korlátozásra kerül. Ide értendő minden korábban már felsorolt bizonyítási eszköz, vagy bizonyítási eszköz felderítéséhez, a gyanúsított kilétének,

¹¹¹ Laczi Beáta: i. m. 730. o.

tartózkodási helyének a megállapításához szükséges adat. A törvény rendelkezése alapján a megőrzésre kötelezettnek gondoskodnia kell a fokozott biztonságú elektronikus aláírással is ellátható adat változatlan megőrzéséről és biztonságos tárolásáról. A kényszerintézkedés értelme az, hogy nincs minden esetben szükség a lefoglalásra, hiszen szemben sok fizikai bizonyítékkal, a számítástechnikai eszköz útján tárolt adat sokkal nehezebben károsodik. Mivel az átvizsgálás így is könnyedén elvégezhető, nem kell feleslegesen lefoglalni később a bizonyítás szempontjából értéktelennek minősülő adathordozókat, és a paragrafus (7) bekezdése lehetővé teszi, hogy az átvizsgálás után lefoglalásra kerüljenek az adatok más rendszerbe vagy adathordozóra történő átmásolással, illetve megszüntetésre kerüljön a megőrzésre kötelezés.

Az utolsó a kényszerintézkedések közül az elektronikus adat ideiglenes hozzáférhetetlenné tétele (korábban elektronikus hírközlő hálózat útján közzétett adatok ideiglenes hozzáférhetetlenné tétele), amely a legújabb is egyben, ugyanis a 2013. évi LXXVIII. törvény vezette be a büntetőeljárás törvénybe. A törvény az új Btk-val együtt lépett hatályba, annak 77. §-ában meghatározott intézkedés, az elektronikus adat végleges hozzáférhetetlenné tétele büntetőeljárásjogi „párjaként”. A kényszerintézkedés az elektronikus adat feletti rendelkezési jogot ideiglenesen korlátozza, és az ahhoz való hozzáférést ideiglenesen megakadályozza. Közvádra üldözendő bűncselekmények esetén a bíróság rendelheti el olyan elektronikus adatra, amelyre a Btk. 77. §-ban meghatározott intézkedésnek van helye, és a hozzáférhetetlenné tétel szükséges a bűncselekmény folytatásának megakadályozásához. A kényszerintézkedés megvalósulhat elektronikus adat ideiglenes eltávolításával és elektronikus adathoz való hozzáférés ideiglenes megakadályozásával, előbbi esetben pedig a fentebb már tárgyalt megőrzésre kötelezés is elrendelhető a hozzáférhetetlenné tétellel együtt. A fő különbség a kettő között, hogy míg az ideiglenes eltávolítás esetén az adat lekerül a tárhelyről, addig a hozzáférés megakadályozása esetén rajta marad, ám az nem elérhető a megtekintők számára. Az eltávolításra a 158/C. § alapján a tárhelyszolgáltató kötelezhető, akinek a határozat közlését követő egy munkanapon belül intézkednie kell ez iránt. Amennyiben a nyomozás vagy hozzáférhetetlenné tétel elrendelésének oka megszűnik, intézkedni kell az elektronikus adat visszaállításáról, amely szintén egy munkanapon belül végrehajtandó. Hozzáférhetetlenné tételnek akkor van helye a 158/D. § szerint, ha a tárhelyszolgáltató nem tett eleget az ideiglenes eltávolításnak vagy külföldi hatóság jogsegély iránti megkeresése a kibocsátástól számított 30 napig eredménytelen maradt; gyermekpornográfia, állam elleni bűncselekmény vagy terrorcselekmény miatt indult büntetőeljárásban, ezekhez kapcsolódó elektronikus adatok

esetén. Mint ebből látható, a főszabály az elektronikus adat eltávolítása, a hozzáférhetetlenné tételre csak kivételes esetben kerül sor. Az eljárás ebben az esetben az, hogy a hatóság határozattal kötelezi a hírközlési szolgáltatókat az elektronikus adathoz való hozzáférés ideiglenes megakadályozására. Ez a kényszerintézkedés a korábban már részletezett internetblokkolás hazai bevezetése, ám tényleges alkalmazhatósága még kérdéses. A törvénysértő tartalom eltávolítása iránti megkeresés sokszor még nyugati tárhelyszolgáltatóknál sem vezetett eredményre (mint például az USA-ban működő kuruc.info szélsőséges portál esetén), és ilyen esetben a tartalom hozzáférhetetlenné tételének technikai kérdései is felmerülnek, például, hogy külföldi IP-címet biztosító nyílt proxyra való rácsatlakozás esetén továbbra is elérhetőek-e ezek a tartalmak.

Utolsóként foglalkozunk a titkos adatszerzéssel, amelynek tekintetében a magyar nyomozás elkövetőspecifikus, hiszen az konkrét személyre irányul.¹¹² A titkos adatszerzést az ügyész és a nyomozó hatóság végzi bírói engedély alapján az elkövető kilétének, tartózkodási helyének megállapítása, elfogása, valamint bizonyítási eszköz felderítése érdekében, a nyomozás elrendelésétől a nyomozás iratainak ismertetéséig az érintett tudta nélkül. A 200. § (1) b) pontjának második fordulata alapján az elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmát megismerheti, az észlelteket technikai eszközzel rögzítheti, valamint a c) pont szerint számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat megismerheti, rögzítheti és felhasználhatja. Mivel a titkos adatszerzésbe belefoglalták a számítástechnikai eszközön tárolt adatokat, így ez a korábban már elemzett online házkutatás hazai meghonosításának tekinthető. Mivel ennek lehetősége csak súlyosabb cselekményeknél áll fent, ez a korlátozás arányban állónak tekinthető a sérelemmel, főleg ha az ilyen nagyobb súlyú kiberbűncselekmények felderítéséhez fűződő társadalmi érdeket vesszük figyelembe.

Az IP-cím kapcsán utaltunk már rá, hogy az hazánkban személyes adatnak minősül. A személyes adatok védelméhez való jog már az Alkotmány 59. §-ban is jelen volt, és az Alaptörvény VI. cikkének (2) bekezdésében is nevesített alapjog, ahol kimondásra kerül, hogy „mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.” Az Országgyűlés sarkalatos törvényben, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben szabályozza az Alaptörvény VI. cikkben megfogalmazott jogokat. A törvény 3. §-a meghatározza a személyes adat fogalmát, ami az érintettel kapcsolatba hozható adat, valamint

¹¹² Parti Katalin: A számítógépes... 196. o.

az adatból levonható, az érintettre vonatkozó következtetés. Ennek alapján az érintettnek közvetve vagy közvetlenül beazonosíthatónak kell lennie. A 4. § (3) bekezdés első fordulata alapján az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A második fordulat meghatározza, hogy akkor tekinthető az érintettel akkor helyreállíthatónak a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek. Ez a korábbi adatvédelmi törvénnyel¹¹³ szemben előrelépés, hiszen ott még nem tett különbséget a jogalkotó aközött, hogy helyreállításnak mi tekinthető és nem szűkítette a kört az adatkezelőre.¹¹⁴

4. Összefoglalás

Mint láthattuk, a kibertérben elkövetett bűncselekmények köre igen széles, és ezek olyan sajátos feladatok elé állítják a nyomozó hatóságot, amelyet csak megfelelő felkészültséggel lehet megoldani. Az internet és az információs technológia fejlődése és elterjedése alapvető változásokat hozott a kommunikációban és a gazdaságban, amelynek eredményeképp jöhetett létre a kiberbűnözés, hiszen kialakulásában fontos szerepe volt a potenciális áldozatok számának és a lehetséges haszon mértéke jelentős növekedésének, a viszonylagos anonimitásnak és annak, hogy saját közvetlen közösségén kívül, a világ bármelyik másik pontján követheti el valaki ezeket a cselekményeket. Ahogy a 460/2004/EK rendelet is leszögezi, az internet mára a társadalmi és gazdasági fejlődés alapjává vált, és így a védelme is egyre fontosabb a társadalom számára. Megfigyelhető, hogy miként több funkció elérhető az internet segítségével, úgy fognak egyre inkább szaporodni az ezek megsértésére irányuló cselekmények. PARTI nagyon találóan fogalmazta meg azt, hogy miként a navigációs eszközök átvették a papíralapú térképek helyét, úgy fogja idővel az elektronikus bizonyítás is a hagyományosát.¹¹⁵ Természetesen, amíg akadnak olyan bűncselekmények, melynek nem ültethetők át a kibertérbe, addig ez az átállás nem lehet teljes, a távoli jövő lehetőségeinek és kihívásainak találgatása pedig már a tudományos fantasztikum körébe tartozik. Az azonban bizonyosan kijelenthető, hogy amíg az informatika ilyen rohamosan fejlődik, úgy állnak elő újabb és újabb kihívások, melyeknek meg kell felelni. Az internetes nyomozásra feltétlenül igaz, hogy örök versenyfutás a bűnözők és a nyomozó hatóság között.

Mivel a büntetőeljárás jelenlegi formája évszázados hagyományokra tekint vissza, nehezen tud alkalmazkodni az új kor kihívásaihoz. Számos feladat vár még elvégzésre a

¹¹³ 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

¹¹⁴ Bővebben lásd: Parti Katalin: *Nyomozás...* 210. o.

¹¹⁵ Parti Katalin: *Újratervezés...* 99. o.

jövőben az eredményesség növelése érdekében. Ilyen a bizonyítási rendszer korszerűsítése, az új technikai vívmányok útján keletkező bizonyítékok teljes körű felhasználása érdekében. Bizonyos új lehetőségek már megvalósultak hazánkban, így az online házkutatás lehetősége, amely bizonyos körülmények között elfogadható módszer lehet, mint ahogy az elektronikus úton továbbított információkról titkos adatszerzés is. Ezek mellett érdemes lehet még kidolgozni a közösségi médiában közzétett információk felhasználását és értékelését a bizonyítási eljárás során, a jelenleg nagy problémákat okozó anonimizáló berendezések feltörésére kidolgozott módszer kidolgozása mellett az IP-cím bizonyítékként való felhasználását is. A jövőben akár olyan tevékenységek is megkönnyíthetők elektronikus úton, mint a felismerésre bemutatás, de a tanúvédelem is egyszerűbbé tehető általa. Ezek mellett fontos az egyes nemzetek jogszabályainak összehangolása, annak felismerésével, hogy a kiberbűnözés nem bír jelentős nemzeti sajátosságokkal, hanem globálisan hasonló jegeket mutat, és a jelentős szabályozásbeli eltérések segítik ezen bűnözési forma terjedését. A bűnügyi együttműködés és megfelelő szabályozás kiterjesztése a harmadik világ, különösen Ázsia országaira elengedhetetlen ahhoz, hogy a jövőben ne maradhassanak büntetlenek az ezen országokban található szolgáltatókon keresztül elkövetett bűncselekmények.¹¹⁶ Sokat segíthet egy kibertámadás jellegének eldöntésénél, és a megfelelő bűnügyi fellépés meghatározásánál, ha sikerül kizárni a lehetséges opciók között a kiberháborús cselekményt, melynek érdekében nemzetközi egyezményrel kellene szabályozni e területet a hadviselés más formáihoz hasonlóan.¹¹⁷ Az együttműködést ki kell terjeszteni a magánszektorra is, különösen mivel a cégek és magánszemélyek a leginkább érintettek és érdekelték a kiberbiztonság megteremtésében és fenntartásában, és ezt kezdik a jogalkotók is felismerni. Ennek kapcsán érdemes megfontolni az önszabályozó rendszerek bevezetését is, hogy a szabályozások ne a felhasználókat és a szolgáltatókat terheljék feleslegesen, és ténylegesen elérjék a céljukat. Ennek során az állam a keretet és a kényszerítő eszközöket biztosítja, és csak a nagyobb súlyú jogsértéseknél lép közbe a büntetőjog eszközével, míg egyébként a szolgáltatók saját eszközeikkel szankcionálnak. A szabályozás egy ilyen rendszerben a felhasználóktól indulva a szolgáltatók közvetítésével jut el az államhatalmi szintig.¹¹⁸

¹¹⁶ Mint történt az például a Fülöp-szigeteken a Love Bug vírus ügyében, ahol a szabályozás hiánya miatt nem tudták elítélni a hatalmas kárt okozó számítógépes vírus készítőjét. Bővebben lásd: Parti Katalin: *Nyomozás...* 207. o.

¹¹⁷ Különösen igaz ez annak fényében, hogy hatalmas pusztítást lehet okozni kiberháborús eszközökkel, akár teljes gazdasági rendszereket összeomlasztva a kritikus infrastruktúra támadásával.

¹¹⁸ Parti Katalin: *Nyomozás...* 209. o.

Mindezeket figyelembe véve elmondható, hogy a kiberbűnözés üldözése terén a jövőt az eddig megszokottól eltérő megoldások és módszerek jelentik, amelynek során az internetes környezetben gyakran nehézkesen érvényesíthető és sokszor eltérő nemzeti szabályozások fokozatos egységesítésére, a bűnüldöző szervek szoros nemzetközi együttműködésére, valamint a magánszektorral való jó viszonyára van szükség az eredményes fellépés érdekében.

Irodalomjegyzék

Nyomtatott források

- Bocij, Paul-McFarlane, Leroy: *The Internet: A Discussion of Some New and Emerging Threats to Young People*. In: 76 Police J. 3 2003. 3-13. o.
- Brenner, Susan W.: „At Light Speed”: *Attribution and Response to Cybercrime/Terrorism/Warfare*. In: 97 J. Crim. L. & Criminology 379 2006-2007. 379-476. o.
- Gergely Máté: *Nyomozás az interneten*. In: Belügyi Szemle, 2002/10. 31-38. o.
- Gillespie, Alisdair A.: *Cyberstalking and the Law: A Response to Neil MacEwan*. In: Criminal Law Review, 2013/1. 39-45. o.
- Hetényi Gábor: *Informatika a nyomozás szolgálatában*, Ügyészek Lapja, 2008/1. szám 15. évf. 43-46. o.
- Kim, Chris-Newberger, Barrie-Shack, Brian: *Computer Crimes*. In: 49 Am. Crim. L. Rev. 443 2012, 443-488. o.
- Kökényesi Attila: *Az internet útján elkövetett bűncselekmények vonatkozásában végzett házkutatás*. In: Ügyészek Lapja, 2008/Különszám 15. évf. 7-15. o.
- Laczi Beáta: *A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései*. In: Magyar Jog, 2001/12. sz. 48. évf. 726-738. o.
- Mohácsi Barbara: *Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal*. In: Magyar Jog, 2008/12. 55. évf. 827-832. old.
- Nagy Zoltán András: *A Pirate Bay-per tanulságai. De lege ferenda a fájlcséről*. In: Ügyészek Lapja, 2010/2. 17. évf. 33-40. o.
- Nagy Zoltán András: *Informatikai bűncselekmények*. In: Magyar Tudomány, 2001/8. szám 946-957. o. Online: <http://www.matud.iif.hu/01aug/nagyz.html> (Letöltés ideje: 2013. 10. 09.)
- Parti Katalin: *A számítógépes bűnözés és az internet*. Kriminológiai Tanulmányok, 40. OKRI, Budapest, 2003, 199-201. o.
- Parti Katalin - Marin, Luisa: *Foltvarrással az on-line illegális tartalom ellen: a tartalomblokkolás, a közvetítő szolgáltató felelőssége és az értesítési-levélteli eljárás*. Infokommunikáció és Jog, 2012/49. 59. old.
- Parti Katalin: *Kerekasztal-beszélgetés az online terrorizmusról*. In: Ügyészek Lapja, 2010/2., 17. évf., 43-51. o.
- Parti Katalin: *Nyomozás az interneten: együttműködés – korlátokkal*. In.: Belügyi Szemle 2004./11-12. szám 52. évf.
- Parti Katalin: *Tiltott pornográf felvétellel visszaélés az interneten - az empirikus kutatás adatai*. In: Kriminológiai tanulmányok 44. Budapest 2007 89-110. o.
- Parti Katalin: *Újratervezés, avagy miért fontos az elektronikus bizonyítékszerzés?* In: Rendészeti Szemle, 2010/3. 58. évf. 99-106. o.
- Radu, Ioan-Minodora Ursacescu, Minodora-Sendroiu, Cleopatra-Cioc, Mihai: *Computer Crime - A Threat to the International Society*. In: 2008 AGORA Int'l J. Jurid. Sci. 248 2008, 248-256. o.
- Rütther, Werner: *Az internet és az „informatikai bűnözés” a kriminológia számára is kihívás*. In: Belügyi Szemle, 2003/2-3. szám 51. évf. 249-262. o.
- O' Floinn, Micheál–Ormerod, David: *Social networking material as criminal evidence*. In: Criminal Law Review 2012/7. szám 486-512. o.

- Walker, Darin–Brock, Deon–Stuart, T. Ramon: *Faceless-oriented Policing: Traditional Policing Theories Are Not Adequate in a Cyber World*. In: 79 Police J. 169 2006. 169-176. o.
- Warren, Peter–Streeter, Michael: *Az internet sötét oldala*. HVG Kiadó, Budapest, 2005
- Wolf, Johnatan B.: *War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money*. In: 28 Am. J. Crim. L. 95 2000-2001, 95-116. o.
- Zambo, Scott: *Digital La Cosa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime*. In: 33 New Eng. J. on Crim. & Civ. Confinement 551 2007 551-575. o.

Online források

- 12th Congress Rept. 112–281. Online: <http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt281/pdf/CRPT-112hrpt281-pt1.pdf> (Letöltés ideje: 2013. 09. 29.)
- *A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében*. Európai Bizottság - IP/12/317 28/03/2012 Online: http://europa.eu/rapid/press-release_IP-12-317_hu.htm (Letöltés ideje: 2013. 10. 09.)
- *A collective EU response to cybercrime*. Europol. Online: <https://www.europol.europa.eu/ec3> (Letöltés ideje: 2013. november 13.)
- A Google átláthatósági jelentése. Online: <http://www.google.com/transparencyreport/safebrowsing/> (Letöltés ideje: 2013. 09. 29.)
- Az NCCS honlapja. Online: <http://www.tscm.com/compkrim.html> (Letöltés ideje: 2013. 11. 15.)
- Cyber Security strategy and Proposal for a Directive. Európai Bizottság. Online: <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security> (Letöltés ideje: 2013. 11. 17.)
- *How computer-generated 'Sweetie' snared 1000 pedophiles*. AFP, 2013. november 5. Online: <http://www.theaustralian.com.au/news/world/how-computer-generated-sweetie-snared-1000-pedophiles/story-e6frg6so-1226753220112> (Letöltés ideje: 2013. 11. 06.)
- *Január 11-én megnyílik a számítástechnikai bűnözés elleni európai központ*. Európai Bizottság - IP/13/13 09/01/2013 Online: http://europa.eu/rapid/press-release_IP-13-13_hu.htm (Letöltés ideje: 2013. 10. 13.)
- *Még tíz évig lehet érvényes Moore-törvénye*. Index.hu 2012. május 2. Online: http://index.hu/tech/2012/05/02/meg_tiz_evig_lehet_ervenyes_moore_torvenye/ (Letöltés ideje: 2013. november 13.)
- Dojcsák Dalma: *No comment*. A Társaság a Szabadságjogokért blogja Online: http://ataszjelenti.blog.hu/2013/10/16/no_comment_453 (Letöltés ideje: 2013. 11. 17.)
- Doyle, Charles: *Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws*. Congressional Research Service, 2010. december 27. Online: <http://www.fas.org/sgp/crs/misc/RS20830.pdf> (Letöltés ideje: 2013. 10. 06.)
- Klochender, Pierre: *With New Malware Virus, Israel Fans A Virtual Flame Against Iran*. Centre for Research on Globalization Online: <http://www.globalresearch.ca/with-new-malware-virus-israel-fans-a-virtual-flame-against-iran/31169> (Letöltés ideje: 2013. 10. 09.)

- Pergel Józsefné: *A biztonságosabb információs társadalom érdekében tett nemzetközi lépések*. Online: <http://www.jit.hu/dok/doku/biztrov4.pdf> (Letöltés ideje: 2013. 11. 17.)
- White, Aoife: *IP Addresses Are Personal Data, E.U. Regulator Says*. The Washington Post 2008. január 22. Online: <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html> (Letöltés ideje: 2013. 11. 14.)

Hivatkozott jogforrások

- 18 USC Protecting Children from Internet Pornographers Act
- 18 USC § 1030 Computer Fraud and Abuse Act
- Az Európai Parlament és a Tanács 95/46/EK irányelve
- Az Európai Parlament és a Tanács 2000/31/EK irányelve
- Az Európai Parlament és a Tanács 2006/24/EK irányelve
- Az Európai Parlament és a Tanács 2009/136/EK irányelve
- Az Európai Parlament és a Tanács 460/2004/EK rendelete
- Az Európai Unió Tanácsa 2008/114/EK irányelve
- Az Európai Unió Tanácsa 2005/222/IB kerethatározata
- Az Európai Parlament és a Tanács irányelvjavaslata a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről 2013/0027 (COD)
- A Miniszteri Bizottság R (85) 10. számú Ajánlása a bűnügyi jogsegélyről szóló európai egyezmény alkalmazása a távközlés hálózatok lehallgatására vonatkozó megkeresések kapcsán
- A Miniszteri Bizottság R (87) 15. számú Ajánlása a személyes adatok rendőrségi felhasználására vonatkozó szabályozásról
- A Miniszteri Bizottság R (88) 2. számú Ajánlása a szerzői és szomszédos jogokkal kapcsolatban elkövetett jogsértések elleni küzdelem érdekében hozandó intézkedésekről
- A Miniszteri Bizottság R (89) 9. számú Ajánlása a számítógéppel kapcsolatos bűncselekményekről
- A Miniszteri Bizottság R (95) 13. számú Ajánlása az információs technológiával összefüggő büntető eljárásjogi problémákról
- ETS 185 Az Európa Tanács Egyezménye A számítástechnikai bűnözésről (Budapest, 23.XI.2001.)
- ETS 201 Az Európa Tanács Egyezménye A gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen (Lanzarote, 25.X.2007.)
- Magyarország Alaptörvénye (2011. április 25.)
- 1949. évi XX. törvény a Magyar Köztársaság Alkotmánya
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
- 1998. évi XIX. törvény a büntetőeljárásról
- 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 2013. évi LXXVIII. törvény egyes büntető tárgyú törvények módosításáról

Hivatkozott ítéletek

- 10-1983 United States v. Neil Scott Kramer
- Delfi AS v. Észtország, 64569/09 ítélet, EJEB, 2013. október 10.
- K.U. v. Finnország, 2872/02 ítélet, EJEB, 2009. március 2.
- 456 Mass. 857 Commonwealth v. Williams
- BGH, 31.01.2007 - StB 18/06