Az online-térben terjedő deviancia, a cybercrime az információtechnológia tükrében

Information technology-based cybercrime, as expansive deviance of the online field

Készítette: Szabó Aliz, *Károli Gáspár Református Egyetem*

Témavezető: dr. Klein Tamás, *Infokommunikációs Jogi Tanszék*

Kézirat lezárása: 2016. december 1.

Tartalomjegyzék

Előszó ... **3**

1. A cybercrime fogalmi kérdései ... **3**

1.1. A jelenség első kutatói ... ***4***

1.2. Az internetes bűncselekmények csoportosítása ... ***4***

2. A számítógépes bűnözés történeti fejlődése ... **5**

2.1. Az első számítógépes bűncselekmények ... ***6***

2.2. A kiberbűnözés jellegzetes vonásai ... ***6***

2.2.1. Az elkövetői kör ... 6

2.2.2. A bűncselekmények érintettjeiről általában ... 7

2.2.3. A digitális bizonyíték ... 7

2.3. A technológiai fejlődés konzekvenciái ... ***8***

3. A Cybercrime- Egyezmény és újragondolása ... **9**

4. A Nemzeti Kiberbiztonsági Stratégia ... **9**

4.1. Magyarország Digitális Gyermekvédelmi Stratégiája ... ***10***

4.2. Magyarország Digitális Oktatási Stratégiája ... ***10***

4.3. Az európai biztonsági stratégia ... ***11***

4.4. A csúcstechnológiai bűnözés elleni harc régen és ma ... ***11***

4.5. A Nemzeti Kibervédelmi Intézet megalakulása ... ***12***

5. Új devianciák az online-térben ... **13**

5.1. Cyber-bullying ... ***13***

5.1.1. Cyber-stalking ... 14

5.1.2. Sexting ... 15

5.2. Adathalászat: phishing, pharming ... ***16***

5.2.1. A phishing szabályozásának új koncepciója ... 17

6. Az Európai Unió számítógépes bűnözésre vonatkozó jogforrásai ... **18**

6.1. Az ENISA szerepe ... ***19***

6.2. European Cybercrime Centre ... ***19***

6.3. További kiemelkedő nemzetközi dokumentumok ... ***20***

6.4. General Data Protection Regulation (GDPR) – a jövő ... ***21***

6.4.1. Reflekciók az általános adatvédelmi rendeletre ... 21

7. Mary esete a kiberbűnözéssel ... **22**

Megállapítások ... **25**

Forrásmegjelölés ... **27**

„Nincs a tulajdonunkban, amit létrehozunk – sőt, mi vagyunk az ő tulajdonában."
*(*McKenzie Wark: Hackerkiáltvány[1])

Előszó

A gyors technikai fejlődés, az informatika kiteljesedése és a hálózatok elterjedése következtében a számítástechnika árnyoldalának tartott számítógépes bűnözés[2] mára világméretűvé nőtte ki magát. A modern technika vívmányainak használatával számos bűncselekmény informatikai úton is megvalósíthatóvá vált. Napjainkban bárki játszi könnyedséggel lehet elkövető és áldozat egyszerre, akár legjobb tudomása nélkül is, ezért elengedhetetlen a megfelelő védelmi stratégia felállítása. Ennek megalapozásához viszont először magát a jelenséget kell körbejárnunk, annak fényében, hogy a védekezés mind emberileg, mind szakmailag nemzeti és nemzetközi együttműködést kíván. A számítógépes bűnözés történeti fejlődésének prezentálása után, a Cybercrime- egyezmény szemléltetésével és újragondolásával a kibertámadások elleni szervezettebb prevenció szükségességére világítok rá. A cybercrime-szabályozás lehetséges irányvonalainak bemutatására törekszem a kiberbiztonsági stratégiák és az uniós jogforrások részletezésével, ennek okán kutatómunkám során mind a hatályos Büntető Törvénykönyv rendelkezéseire, mind a cybercrime-ot specifikusan szabályozó jogszabályokra nagy hangsúlyt fektettem. Dolgozatomban arra szeretnék rámutatni, hogy milyen pozitív eredményekkel járhat, ha e két szélsőséges szemlélet egyes elemeit összefésüljük. A számítógépes bűnözési formák ismertetésekor az azok elleni védekezési formákat is részletezem annak érdekében, hogy életszerű segítséget nyújtsak egy lehetséges deviáns magatartás leküzdésében mind a felnőtt korosztály, mind a fiatalkorúak számára. Kiemelten vizsgálom az adathalászatot, melyre egy új szabályozási koncepciót is felépítek. A 2018-tól hatályba lépő uniós adatvédelmi szabályozást, a GDPR[3]-t is elemzem, majd reflektálok a rendeletre. Dolgozatomban végül a deviáns cselekmények hétköznapi értelmezésének elősegítésére áttekintettem Cameron S. D. Brown információs biztonsági szakértő 2015-ben befejezett, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*[4] címmel megjelent tanulmányát, nem csupán annak kiemelkedő aktualitása miatt, hanem mert véleményem szerint kifejezetten új, laikusok számára is jól érthető oldaláról vizsgálja ezt az egészen mai, rendkívül aktuális és kardinális problémát.

1. A cybercrime fogalmi kérdései

A definíció meghatározása előtt szükséges tisztázni, hogy a cybercrime még nem rendelkezik egységes, a szakirodalom által elfogadott definícióval. Ennek fő indoka az, hogy a jelenség rendkívül sokszínű és változékony, így könnyen lehet, hogy egy választott címszó nem fedné le annak teljes és valós tartalmát. Fontosnak tartom megjegyezni, hogy az elmúlt évtizedekben számos definiálási kísérlet zajlott, így most az általam legkiemelendőbbnek vélt két fogalom-meghatározást említem meg. Az Európa Tanács 1989-ben elkészítette 9. számú ajánlását a számítógéppel kapcsolatos bűncselekményekről, melyben az Európa Tanács által felállított szakértői testület kerüli a számítógépes bűncselekmény fogalomszintű meghatározását, helyette az eddig ismert, online környezetben megvalósítható deliktumokat vezeti listákra. A tanácsi javaslat egy minimum és egy fakultatív listát is tartalmaz. A minimum lista szereplői a számítógépes csalás, a számítógépes hamisítás, a számítógépes adatokban és programokban történő károkozás, a számítógépes szabotázs, a jogellenes behatolás, a jogellenes titokszerzés, a védett számítógépes programok jogellenes másolása és

[1] Mckenzie WARK: Hackerkiáltvány, Noran Libro kiadó, 2010. Fordította: NAGY Mónika Zsuzsanna.
[2] Ld. 2. A cybercrime fogalmi kérdései.
[3] General Data Protection Regulation.
[4] Ld. 7. Mary esete a kiberbűnözéssel.

a félvezető topográfiák jogellenes másolása. A fakultatív lista négy eleme a számítógépes adatok és programok megváltoztatása, a számítógépes kémkedés, a számítógép jogellenes használata és a védett programok jogellenes használata. Ettől eltérően, Kunos Imre 1999-es, a Belügyi Szemlében megjelent tanulmányában[5] a számítógépes bűnözést azon bűncselekmények összességeként definiálja[6], melyek esetén információtechnológiai eszközöket, rendszereket használnak a bűncselekmények elkövetésének eszközéül. Ez utóbbi fogalom ma is irányadó lehet azzal a kiegészítéssel, hogy a számítógép ma már nem csupán eszköz, hanem az internet segítségével az elkövetés helye is lehet. A cybercrime megjelenése az információtovábbítási eszközöknek köszönhető, így annak definíciója is e körben értelmezhető csupán.

1.1. A jelenség első kutatói

Hazánkban először Polt Péter hívta fel a figyelmet a virtuális kriminalitás létezésére és fontosságára 1983-as, *A számítógépes bűnözés* címmel a Belügyi Szemlében megjelent értekezésével[7], az Országos Kriminológiai és Kriminalisztikai Intézet (OKRI) munkatársaként. Az 1980-as évek végén fogott a cybercrime tanulmányozásához Pusztai László[8] jogtudós is, aki számos tanulmánnyal gyarapította tudásunkat a kiberbűnözésről, melyek közül az első igazán átfogó műve *A számítógép és bűnözés* címmel[9] jelent meg 1989-ben. Kutatásai során rendszerbe foglalta a korabeli számítástechnikai bűncselekményeket, számba vette a számítógépes bűnözés közös jellemzőit és rávilágított a jövőbeli tendenciákra is. További tudományos munkásságáról gazdag bibliográfiája árulkodik.

1.2. A számítógépes bűncselekmények csoportosítása

Pusztai László *a Számítógép és bűnözésben* négy alaptípusát különböztette meg az internetes bűncselekményeknek: a számítógépes visszaélést, az adatkikémlelést, a számítógépes szabotázst és a gépidőlopást. Tíz évvel később, a számítógépes bűncselekmények kodifikációjáról szóló tanulmányában[10] Nagy Zoltán András hasonló kategóriákat határozott meg. Eric Himpton Horder, Jr. amerikai ügyvéd szerint három csoportba sorolhatók a számítógépes bűncselekmények: az első csoportba a számítógép, mint szoftver és hardver együttese ellen irányuló bűncselekmények tartoznak, a második csoportot azok a bűncselekmények adják, melyeknél a számítógép médiumként az elkövetés eszközeként szolgál(számítógépes csalás, szerzői vagy szomszédos jogi jogsértések, illegális termékek vagy szolgáltatások online értékesítése, online zaklatás), a harmadikat pedig azok a tényállások teszik ki, amelyeknél a számítógép, mint tároló eszköz jelenik meg, amelyen lévő adatok bizonyítékként szolgálhatnak valamilyen más deliktumhoz. Szabó Imre professzor két kategóriába sorolja a bűncselekményeket[11]: az egyik kategóriát az internet, mint hálózat ellen megvalósuló bűncselekmények adják, a másikat pedig az interneten megvalósuló jogtalan cselekmények. Lényegesnek tartja az utóbbi csoport további kettéosztását, mivel az interneten hozzáférhetőek olyan adatbázisok, melyek esetleges elkövetési magatartások bizonyítékai lehetnek, s ezek kizárólag a személyiségi jogok korlátozásával lennének hozzáférhetők. A

---

[5] KUNOS Imre: A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. Belügyi Szemle, 1999, 47. évf. 11. szám., 28–42.

[6] KUNOS i.m. 28.

[7] POLT Péter: A számítógépes bűnözés. Belügyi Szemle, 1983, 21. évf. 6. szám, 60–64.

[8] Az OKRI igazgatója, valamint az Országos Bűnmegelőzési Tanács első elnöke volt.

[9] PUSZTAI László: Számítógép és bűnözés, Kriminológiai és kriminalisztikai tanulmányok. 1989, 26. kötet, 85–146.

[10] NAGY Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009. 5–6.

[11] SZABÓ Imre: Internetes bűncselekmények – különös tekintettel az internetes csalásra. E-akták. Tanulmányok az internetjog világából. Szerk.: Dr. KISS Daisy. Bibó István Szakkollégium Internetjogi Kutatócsoport, 2003. 301–324.

technológia személyiségi jogi és szerzői jogi jogsértések elkövetését is lehetővé teszi, de ezek nem kerülnek kifejtésre a dolgozatban. Marjie T. Britz[12] a 2013-ban, *Computer Forensics and Cyber Crime: An Introduction* címmel megjelent könyvében az informatikai bűncselekményekkel kapcsolatban négy fogalmat azonosít, Szabó Imréhez hasonlóan megkülönbözteti a számítógépes illetve a számítógéppel kapcsolatos bűncselekmény kategóriáját, illetve új fogalmakként említi a digitális bűncselekményt és a kiberbűncselekményt is. A digitális bűncselekmény-fogalmat minden olyan cselekményre használja, mely magában foglalja az elektronikusan tárolt adathoz való jogosulatlan hozzáférést, terjesztést, annak manipulálását, megsemmisítését vagy megmásítását. A kiberbűncselekmények Marjie szerint olyan számítógépes rendszerekkel vagy internetre csatlakoztatott számítógépekkel való visszaéléseket ölelnek fel, melyek közvetlenül vagy járulékosan veszteségeket okoznak. Úgy gondolom, hogy a digitális bűncselekmények és a kiberbűncselekmények új fogalmakként való bevezetése lényegesen fontos mind a hazai, mind a nemzetközi jogban, a technológiai változások előidézték ezek szükségességét. Mivel azonban sok az átfedés e két kategória között (hogy egy példát említsek, az adathalászat e csoportosítás szerint több fogalomkörbe is sorolható lenne), így szükségesnek tartom a két kategóriát egymással párhuzamba állítva vizsgálni, s ehhez mérten az így kialakuló vizsgálati eredményekre alapozva a fogalmakat pontosítani.

2. A számítógépes bűnözés történeti fejlődése

A számítógép egészen annak 1880-as feltalálása óta szolgál eszközként a virtuális bűnözéshez, így fontosnak tartom e kettő megszületésének történeti jelentőségű fordulópontjait egymással párhuzamba állítva taglalni. Az első modern komputer alapelveit Charles Babbage tudós dolgozta ki az angol kormány megbízásából, egyes források szerint Sir Humphrey Davyhez írt levelében.[13] Valamivel később, 1886-ban Herman Hollerith német származású amerikai feltaláló megépítette az első lyukkártya-feldolgozó gépet, melyet elektronikus számlálásra lehetett felhasználni, így azt a célt szolgálta, hogy az 1880-as népszámlálás adatait feldolgozza. A találmány nemcsak az USA-ban, de Európában is nagy sikert aratott, a statisztikai felmérések kedvelt eszköze lett. 1939-re Konrad Zuse német mérnök történelmet írva elkészítette az első, jelfogókkal működő számítógépet, a Z1-et. 1945-ig további prototípusokat[14] készített, így született meg az első kereskedelmi forgalomba került digitális számítógép[15] is. A fejlődés további lényeges állomásaiként megemlíteném még a Mark 1-est, az első nulladik generációs, valamint az ENIAC-ot, az első elektroncsöves, első generációs készülékeket is. Később, a tranzisztorok alkalmazásával létrejöttek második generációs gépezetek is, melyek által az eszközök mérete és energiafogyasztása is jelentősen csökkent. Az 1970-es évektől egészen napjainkig a számítógépek negyedik generációjáról beszélhetünk, melyek nagy integráltságúak, magas szintű nyelveken írják programjaikat és microprocesszorokkal működnek. Az ötödik generációs, mesterséges intelligenciával működő számítógépek fejlesztése kezdeti stádiumban van, így megjelenésük a jövő záloga.

---

[12] A Clemson University (USA) büntetőjogi professzora.

[13] Charles Babbage to Sir Humphrey Davy, July 3, 1822, Morrison and Morrison, Charles Babbage and His Calculating Engines, 305.

[14] A Z2 már relés elektromechanikus áramkörökkel működött, a Z3 pedig ennek továbbfejlesztéseként, az első programvezérlésű, kettes számrendszerben dolgozó számítógép volt.

[15] A Z3 utódjaként ZUSE elkészítette a Z4-et, melyet először a repülőgép-tervezésben, majd 1950-től a zürichi Műszaki Főiskolán használtak.

2.1. Az első számítógépes bűncselekmények

A számítógépeket már a kezdetekben is felhasználták csalásokhoz és adatállományok manipulálására, majd az első vírusok, trójai programok táptalajává váltak, melyeket főként károkozásra, információszerzésre hoztak létre. 1959-ben a Walston and Co. alelnöke hamis lyukkártyák segítségével 250 000 dollárt sikkasztott, ám ez az eset akkoriban még kivételesnek számított, így a tudományos élet és a nyomozó hatóságok nem tulajdonítottak különösebb jelentőséget a jelenségnek. Az integrált áramkör feltalálásával Jack S. Kilby[16] 1958-ban a harmadik generációs számítógépek tömegtermelését aktivizálta. 1963 és 1974 között az Equity Funding Corporation cég munkavállalói a szervezet készülékeit használva hamis kötvényeket készítettek fiktív kifizetések céljából, így 2 000 000 dollárt csaltak ki a vállalkozásból. Tettük olyan volumenű bűncselekmény-sorozatot eredményezett, melyet a Guiness Rekordok könyve is számon tart. A nyolcvanas évek elején megjelent az FBI számítógépes csalásról szóló jelentése, melyből kiderült, hogy míg egy átlagos fegyveres rablás alatt körülbelül 10 000 dollárt zsákmányoltak az elkövetők, addig egyetlen virtuális bűntettükkel ennek az összegnek akár a százszorosát is megkereshették. Magyarországon 2006 márciusában televíziós csatornák vételére szolgáló kódkártya hamisításával és terjesztésével a tettesek 64 milliárd forintot zsebeltek be.

2.2. A kiberbűnözés jellegzetes vonásai

Az internet nyitott, decentralizált, interaktív jellegéből adódóan a bűnözés ideális elkövetési területe. Az elkövetőknek előzetesen be kell szerezniük az eszközként szolgáló információkat, szoftvereket, valamint kellő szakmai tapasztalatot kell szerezniük az elkövetés sikerességéhez. A fejlődő technika és az internet világszintű elterjedése lehetővé teszik, hogy a bűntények egyre nehezebben ellenőrizhetőek, gyakran a sértett előtt is rejtve maradnak. E magas látencia leggyakrabban a bankokat, hitelintézeteket és biztosítókat érinti, ebben vélhetően közrejátszik az a tény is, hogy e szervezetek önös érdekeik miatt gyakorta nem jelentik a megtörtént káreseteket. A tettesek kiléte nehezen deríthető fel, mivel a kommunikációs csatornákon könnyedén rejtve maradhatnak. Az internet egy államhatárok nélküli virtuális világ, a bűncselekmények nemzetközi jellegűek, ami a visszaélések nyomon követését jelentősen megnehezíti. Egy újonnan megjelenő hardver, szoftver idővel általában az elkövetés új eszközévé válik, az így elkövetett cselekményeket azonban csak az elméleti alapvetések megalkotása révén lehetünk képesek megelőzni és csökkenteni.

2.2.1. Az elkövetői kör

Az internetes bűncselekmények elkövetőinek fő segédeszköze a számítógép, és mint olyan, a számítástechnika maga. Napjainkra bármely szakismerettel rendelkező személy a jogtalanság területére léphet szaktudása felhasználásával, s akár egy hozzá nem értő is képes olyan kártékony programot vagy vírust készíteni, mely a célszámítógépben nagy veszteségeket okozhat. Azt azonban fontos leszögeznünk, hogy az információtechnológia önmagában nem veszélyes tudomány, csupán annak nem megengedett célokra való felhasználásával válhat egy bűntény melegágyává. A 21. századi elkövetői réteg igen sokszínű.[17] Napjaink komputerundergroundjának tagjai közé tartoznak a hackerek és crackerek, akik védett rendszereket törnek fel (differenciálja őket, hogy a crackerek legtöbbször pénzszerzés céljából teszik ezt), az ártalmas kódokat készítő vírusírók, a kalózok, akik szoftverek védelmi rendszereinek feltörésével foglalkoznak, illetve az anarchisták, akik az információ szabad áramlását szándékoznak megakadályozni. E körbe tartoznak továbbá a phreakek, akik

[16] Jack St. Claire KILBY (1923. november 8.-2005.június 20.) Nobel-díjas amerikai fizikus, ő a kézi számítógép és a hőnyomtató feltalálója is.

[17] SZEGEDINÉ Lengyel Piroska: Számítógépes bűnözés, avagy fiatalok a cyber-térben, Hadmérnök, V. évfolyam 2. szám, 2010.június. 372.

telefonvonalakba próbálnak technológiai eszközök használatával behatolni, valamint a cypherpunkok, akik olyan programokat írnak, melyekkel más párhuzamos számítógépeket sajátos kódolással látnak el. Megemlítendők még azon terrorista szervezetek is, melyek adathalász rombolás és toborzás céljából követik el az erőszakos cselekményeket. Ezen elkövetői csoportokat számos tényező motiválhatja, többek közt a tapasztalatszerzés, a károkozás vagy a védett adatok megszerzése. Mivel az elkövetők leggyakrabban deviáns magatartású, érzelmileg labilis fiatalkorúak vagy fiatal felnőttek, így véleményem szerint nem csupán a virtuális világban kell védekeznünk ellenük, hanem biztosítanunk kell a serdülő gyermekek családcentrikus, információtudatos nevelését, mellyel a Z generációban csökkenthetjük a későbbi, elkövetésre irányuló hajlamot s így nagyobb eséllyel redukálhatjuk a jövőbeli jogsértések számát.

2.2.2. A bűncselekmények érintettjeiről általában

Az interneten elkövetett bűncselekményeknek naponta körülbelül egymillió áldozata van. A számítógépes bűnözők hozzávetőlegesen 750 milliárd eurót profitálnak Európában, és 4000 milliárd dollárt az Amerikai Egyesült Államokban. Világviszonylatban csaknem 50 milliárd internethez kapcsolt eszközről van tudomásunk. A számítógépes bűntények tulajdonképpen bárki ellen irányulhatnak, ám többségüket – adatok megszerzését, manipulálását célozva, vagy anyagi haszonszerzés végett - vállalatok ellen követik el. A PwC 2016-ban globális gazdasági bűnözés felmérést készített[18], melyben világszerte 6337, míg Magyarországon 95 vállalat vezető beosztású munkatársa válaszai alapján mérték fel a vállalatokat érintő bűnözési helyzetet. A megkérdezett szervezetek 46%-a szerint Magyarországon a deliktumok legelterjedtebb formája a hűtlen kezelés, bár ehhez hozzá tartozik az a tény is, hogy ez az egyik legkönnyebben felderíthető gazdasági bűncselekmény. Az elmúlt két évben a hazai cégek 25%-a legalább egyszer találkozott valamilyen gazdasági bűncselekménnyel. Magyarország öt leggyakoribb ilyen bűncselekménye a hűtlen kezelés (46%), a korrupció és vesztegetés (38%), az adócsalás (21%), a számítógépes bűnözés (17%) és a közbeszerzési csalás (17%). A számítógépes bűnözés régiós áldozatainak átlaga 22%, a globális átlag pedig 32%, vagyis jóval több, mint a hazai 17%-os átlag, így feltételezhetjük, hogy a magyar cégek egy része tudtán kívül válhatott online bűntény áldozatává. A vállalatoknak a pénzügyi veszteségen túlmenően egyéb járulékos kára is keletkezik, nem beszélve a vállalat jó hírnevére gyakorolt negatív hatásairól. A magyarországi válaszadók 42%-a nyilatkozott úgy, hogy a cégénél bekövetkezett csalást vállalati ellenőrzési mechanizmus segítségével leplezték le (a régiós arány 54%, míg globálisan 47%). A vállalatok az utóbb említett tényezők miatt gyakran tartják titokban az ellenük irányuló támadásokat, ezzel azonban a bűncselekmények elleni hatékony védekezést hátráltatják. Véleményem szerint a vállalatvezetőknek ezért szükséges lenne nagyobb hangsúlyt fektetniük a védekezési mechanizmusok elsajátítására, és egy ilyen helyzetben büszkeségüket félretéve, nem szégyellni segítséget kérni.

2.2.3. A digitális bizonyíték

A kiberbűncselekmény végrehajtásával előtérbe kerül a bűnüldözés egyik kiemelkedő problematikája, a digitális bizonyítékok kezelése. Ezek ugyanis rendkívül egyszerűen manipulálhatóak és beszerzésük komoly nehézségekbe ütközhet a hatóságok számára. Azokban az esetekben, ahol az ügyben informatikai tartalmak is érintettek, digitális bizonyítékok használata és szakértő bevonása is lehetséges. E tudományterület szülőhazája az Amerikai Egyesült Államok, mely szövetségi szabályozásában a bináris formában tárolt vagy továbbított bizonyító erejű információként határozza meg a digitális bizonyítékot. Egy

[18] http://www.pwc.com/hu/hu/kiadvanyok/globalis_gazdasagi_bunozes_felmeres/assets/Gazdasagibunozes2016_web.pdf [letöltve: 2016.09.05.]

digitális nyom akkor válhat bizonyítékká, amikor a nyomozó hatóság vagy az erre feljogosított szerv a büntetőeljárásban vagy más keretek között nyomozást indít. A házkutatás során jelenhet meg először a digitális bizonyíték és szakértő kettőse, ez a felállás azonban ritka: az esetek többségében a házkutatást végző szerv munkatársainak kell a kulcsfontosságú tevékenységeket (bizonyítékok tárolása, szállítása, stb.) elvégezni. A digitális bizonyítékok értelmezésénél a vizsgálati eljárás szabványok hiánya problémát okoz, mivel az egyes hordozó eszközök megtekintése és elemzése megfelelő készségeket kíván meg. Ez különösen a bírói testület munkáját nehezíti, ezért a szakértőknek nagyobb gondot kell fordítaniuk a bizonyítás digitális eszközeinek prezentálására. Máté István Zsolt igazságügyi informatikai szakértő szerint[19] a digitális bizonyítékoknak a büntetőeljárásban csak akkor lehet teljes bizonyító erejük, ha az eljárás valamennyi szereplője rendelkezik a szerepéhez mérten megfelelő szintű kompetenciával a digitális írástudás területén. A várhatóan 2018. január 1-jén hatályba lépő új büntetőeljárási törvény új bizonyítási eszközként határozza meg az elektronikus adatot, mellyel a jövő kihívásaira választ adni képes bizonyítási eszközök biztosítását célozza.

2.3. A technológiai fejlődés konzekvenciái

A technológiai fejlesztések szükségszerűen generálják a számítógépes bűncselekmények sokszorozódását és kezelhetetlenebbé válását, ezért lényeges hangsúlyt kell fektetni a megfelelő védelmi stratégiák kialakítására, ehhez pedig elengedhetetlen az internet-szolgáltatók és a bűnüldöző hatóságok szorosabb együttműködése, illetve a jogalkotás reakciójának gyorsítása és a joghatósági problémák kiküszöbölése. Az elkövetők gyakran használnak számítógépes banki rendszereket pénzügyi tranzakciók, illegális átutalások lebonyolítására, vagy a sértett zsarolása céljából. A számítástechnika rohamos innovációjának köszönhetően veszélybe kerülhetnek olyan nyílt rendszerek is, melyek pénzügyi, katasztrófavédelmi szervek vagy egyéb infrastruktúrák működését szolgálják. Ezért nemcsak a védekezés lényeges, hanem a megelőzés is: a kormánynak kiemelt figyelmet kell fordítania a megfelelő informatikai oktatás megszervezésére, hogy a holnap szakemberei minél alaposabban felkészülhessenek a társadalmat fenyegető veszélyre. Az IP címek a csatlakozás helyének és idejének beazonosítására szolgálnak, mára azonban egy egyszerű proxy szerverrel kijátszhatók, a hackerek pedig erre irányuló szolgáltatások, például az Onion network[20] ki- és továbbfejlesztésén dolgoznak. Aktuális probléma a szteganográfia[21] is, mellyel titkosított információ tárolására alkalmas helyhez juthatnak az elkövetők. Az internet globalitása miatt a nemzeti határoknak csekély a jelentősége, nem szükségszerű, hogy a sértettel azonos országban, kontinensen tartózkodjon az elkövető. A jogalkotóknak nincs könnyű dolguk, hiszen a technológiai környezet, amelynek szabályrendszerét ki kellene alakítaniuk állandó fejlődésben van, így a bűnelkövetők mindig egy lépéssel a jog előtt járnak. Mindezen nehézségek ellenére a tagállamok és a nemzetközi szervezetek felvették a kesztyűt, összehangolt munkájukkal egy átfogó szabályrendszer megalkotásán törekszenek. A technológia-semlegesség[22] elve segít a gyorsan változó technológiai környezet kezelésében, hiszen a szabályozás nem a szolgáltatásra, hanem magára a tevékenységre koncentrál. Ennek

---

[19] MÁTÉ István Zsolt: The Digital Evidence – A digitális bizonyíték., https://www.academia.edu/5105387/A_digit%C3%A1lis_bizony%C3%ADt%C3%A9k_The_Digital_Evidence [letöltve: 2016.10.10.]

[20] Másik elnevezése a Tor hálózat, az internet láthatatlan részét képezi, az e területen futó hálózati kapcsolatok és szolgáltatások nem azonosíthatóak.

[21] Az adatelrejtés egyik kedvelt módszere, a felhasználó háromdimenziós képekbe menti el adatait, a képek eredeti méretének megtartásával.

[22] A technológia-semlegesség értelmében nem részesíthető előnyben és nem zárható ki egyetlen technológia vagy hálózati platform sem a szélessávú szolgáltatásokat nyújtók közül.

értelmében 2015-től, az ITU[23] által hozott döntés alapján Európában, Afrikában és Ázsia egyes részein (Region 1) is digitálisan történik a műsorszórás. E tekintetben kivételes, hogy egy nemzetközi szervezet hozott döntést egy technológiai kérdés kapcsán. A szabályozás a technológia-semlegesség és a kommunikáció szabadsága kiterjedtebb érvényesülését eredményezi.

3. A Cybercrime- Egyezmény és újragondolása

Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye[24] 2004. július 1-jén lépett hatályba. Elsődleges célja, hogy megvédje a társadalmat a kiberbűnözéssel szemben, s megteremtse a részt vevő tagállamok között az ehhez elengedhetetlen összhangot. Az Egyezmény számos megállapodás eredményeit viszi tovább, ezek közé sorolható a korábbi 1950-es Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezmény, az 1960-ban elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya, valamint az 1989-ben ratifikált Gyermekek Jogairól szóló Egyezmény. A Cybercrime- egyezmény egy jól működő nemzetközi együttműködés, azonban az esetek többségében reaktív jellegű, tehát a bekövetkezett támadás esetére nyújt megoldást. A tagállamok megkívánják, hogy ne csak a már megtörtént támadások elbírálására adjon jogi keretet, hanem preventív jelleggel is bírjon. A jelenlegi szabályozás némely esetekben eltér a kor és a technológiai színvonal követelményeitől, mivel akár egy mit sem sejtő felhasználó számítógépével is végrehajtható olyan támadás, amit a jog szankcionál. A támadó hálózatok napjainkra oly mértékben elterjedtek, hogy egy átlagos anyagi helyzetben lévő polgárnak sem kell mélyen a zsebébe nyúlnia ahhoz, hogy botnet[25] üsse a markát, sőt, hozzáértőnek sem kell feltétlenül lennie annak használatához. Ezek a tények félelemre adnak okot, annak tudatában, hogy a nyelvi korlátok lehullásának is köszönhetően a világ más régióiból érkező adathalász, célzott adathalász támadások már nincsenek többé határok közé szorítva. Mindazonáltal szükségesnek tartom megjegyezni, hogy a Cybercrime- egyezmény a jelenlegi legsikeresebb kibervédelmi nemzetközi együttműködés, és a 2018-ban hatályba lépő GDPR adatvédelmi rendelettel társítva a kibervédelem egy új fejezetét nyithatja meg az online világban[26].

4. A Nemzeti Kiberbiztonsági Stratégia

Magyarország Nemzeti Kiberbiztonsági Stratégiája az 1139/2013. (III.21.) Kormányrendeletben született meg. Fő célja, hogy – illeszkedve a biztonságos és innovatív 21. századi nemzetközi környezetbe –, hazánk nemzeti érdekei a magyar kibertérben is érvényesülhessenek. Ehhez elengedhetetlen a kibertérből eredő fenyegetések kezelése, a kormányzati összhang és eszköztár előremozdítása. A rendelet megalkotásához az 1035/2012. (II.21.). Kormányrendeletet vették alapul, valamint az Európai Unió kiberbiztonsági előírásait követték. Fontos volt, hogy illeszkedjen továbbá a NATO csúcs- dokumentumaiban foglalt elvekhez is. Az így megalkotott jogszabály számos betartandó követelményt meghatározott a biztonságos világháló megteremtéséért, így elsődlegessé vált az egyéni és közösségi személyes adatvédelem, az innovativitás a gazdaságban, a kiber-fenyegetések elhárítása és az állami szolgáltatások fejlesztése. A Nemzeti Kiberbiztonsági Stratégia bemutatását nem csupán azért tartom fontosnak, mert kiemelten sok pozitív változást eredményezett az internetes fenyegetések megelőzésére és elhárítására vonatkozóan, hanem mivel a kormányrendelet hatására számos új szervezet és sikeres együttműködés született. Első

[23] Nemzetközi Távközlési Egyesület.
[24] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400079.TV [letöltve: 2016.09.01.]
[25] A botnet ebben az értelemben olyan hálózatra kapcsolt gépek (botok) összessége, amelyek felett malware programok által átvették az irányítást.
[26] Ld. 6.4. General Data Protection Regulation (GDPR) – a jövő

lépésként, a kormányzati koordináció gyümölcseként létrejött a Nemzeti Kiberbiztonsági Koordinációs Tanács, a 484/2013. (XII.17.) Kormányrendelet nyomán. Célkitűzéssé vált olyan szakosított intézmények létrehozása is, melyekben specifikus szakértelmű személyek kerültek az adat-és titokvédelmi területek élére. A Stratégia egyik fő eredményeként megszületett a Gyermekvédelmi Internet-kerekasztal, mely 2014 óta a Nemzeti Média-és Hírközlési Hatóság tanácsadó testületeként kiemelt figyelmet fordít a gyermekbarát internetezés megvalósítására és a szűrőszoftverek átható fejlesztésére. A kerekasztal elnöke Koltay András Médiatanács-tag, akit a Médiahatóság elnöke, Karas Monika két másik taggal együtt saját jelölés alapján nevezett ki, a testület további 8-8 tagját gyermekvédelmi szervezetek, valamint szakmai szövetségesek ajánlásai alapján, további 2 tagját pedig a Nemzeti Fejlesztési Minisztérium javaslata alapján választották meg. Megbízatásukat 3 évre nyerték el, munkájuk önzetlen, díjazásban nem részesülnek. A grémium egyedi ügyeket is vizsgál, nagy hangsúlyt fektet a kiskorúak szellemi és lelki fejlődésére, valamint a gyermekek és szüleik médiatudatosságra való nevelésére.

4.1. Magyarország Digitális Gyermekvédelmi Stratégiája

A 2015. évi InternetKon nemzeti konzultáció keretében a magyar polgárok véleménye egyöntetű volt: a világháló ne fenyegesse a gyermekek biztonságát. Így 2016-ban, a Digitális Jólét program részeként elkészült Magyarország Digitális Gyermekvédelmi Stratégiája, mely aktuális megoldásként szolgál a gyermekeket fenyegető új típusú veszélyforrások kezelésére, elhárítására. Az 1488/2016. (IX.2.) számú Kormányhatározat a biztonságos internetszolgáltatás megteremtéséről, a tudatos internethasználatról és Magyarország digitalizált gyermekvédelmi stratégiájáról szól. A 2016 szeptemberétől induló program a magyar nemzetgazdaság digitális fejlesztését célozza, elsődleges célkitűzése, hogy megvédje a gyermekeket az internet veszélyes, káros tartalmaitól és tudatos, értékteremtő internethasználatra nevelje őket. Mindez nem valósulhatna meg a gyermekek védelmét szolgáló szabályok és intézkedések kiemelt érvényesülése és érvényesítése nélkül. A stratégia további célja, hogy a védelmi mechanizmusok megfelelően funkcionáljanak, kiküszöbölve a gyermekekre leselkedő veszélyeket és káros hatásokat. A Kormány a magyarországi internetszolgáltatókkal kötött megállapodás keretében a „Gyermekek Számára Biztonságos Internetszolgáltatás" új feltételeit kívánja megteremteni. Ingyenesen hozzáférhető, magyar nyelvű gyermekvédelmi szűrőszoftverek kifejlesztését kezdeményezi, célkitűzése továbbá egy kiskorúak számára biztonságos tartalmakat bemutató honlap létrehozása és működtetése is. Átfogó tájékoztatási programokat kíván indítani a gyermekek megóvását célzó jogszabályi rendelkezések megismertetése és a digitális világban megjelenő sérelmekkel szembeni fellépési lehetőségek bemutatása érdekében. Ingyenes képzési és továbbképzési programokat indít, melyek célja a szülők, pedagógusok, valamint a gyermekekkel foglalkozó más szakemberek médiaműveltségének fejlesztése.

4.2. Magyarország Digitális Oktatási Stratégiája

Deutsch Tamás[27] szerint a digitalizáció ma már nem választás kérdése, a 21. században Magyarországon nincs olyan ember, aki kizárhatja életéből a digitális világot, hiszen valamilyen szinten mindenkit érint. Ennek fényében 2016 nyarán elkészült Magyarország Digitális Oktatási Stratégiája (DOS), mely minden elemében illeszkedik a kormányzati elképzelésekhez. E stratégiában jóval nagyobb szerepet kap az oktatás területén a digitalizálás, s ez nagymértékben kihat az oktatás szemléletmódjára, módszertanára, az új tanulási folyamatokra és az oktatási környezetre is. A stratégia foglalkozik a pedagógusok digitális felkészültségének fejlesztésével, az oktatási tananyagok újragondolásával, a fizikai

[27] Miniszterelnöki biztos, a Digitális Jólét Program felelőse.

infrastruktúrával és az intézmények eszközellátásával is. 2020 lesz az az év, amikor befejeződik a magyar oktatási rendszer digitális átalakítása. Mind az állampolgároknak, mind az oktatóknak, cégvezetőknek lehetősége lesz a digitális tudásuk megszerzésére, formálására. Az új nemzeti alaptantervben (Nat) a digitális képességek és eszközök használata kiemelt szerepet kap majd. Cél továbbá az informatikai képzéseken részt vevők számának növelése, a jelenlegi 25%-os jelentkezési arányt 40%-ra szeretnék emelni. A miniszterelnöki biztos a magyar állampolgárok véleményére alapozva dolgozta ki és építette fel ezt a programot, ez európai szinten egyedülálló és példaértékű. A világban kevés helyen készült olyan digitális oktatási stratégia, mely az oktatási rendszer egészére kiterjed. [28]A köznevelés, a szakképzés, a felsőfokú oktatás és a felnőttkori képzés teljes rendszerének digitális fejlesztését, digitális átalakítási programját fogalmazza meg a stratégia.

4.3. Az európai biztonsági stratégia

2015. április 28-án az Európai Bizottság által közzétételre került a 2015-2020-ig terjedő időszakra szóló európai biztonsági stratégia, amely támogatja a tagállamok együttműködését a biztonsági fenyegetések kezelése során, és fokozza közös erőfeszítéseiket a terrorizmus, szervezett bűnözés és számítástechnikai bűnözés elleni küzdelemben. A stratégia szerint a három legjelentősebb cél a terrorizmus megelőzése, a szervezett bűnözés elleni küzdelem és a kiberbűnözés elleni küzdelem. E fenyegetések ellen többek között az informatikai ágazattal folytatott párbeszéd fokozásával és az Európai Unió eszközeinek megerősítésével lehet fellépni. Így a Bizottság 2015-ben uniós szintű fórumot indított a fő informatikai vállalatokkal az interneten és a médiában folytatott terrorista propaganda megfékezése, és az új titkosítási technológiákkal kapcsolatos módszerek felkutatása érdekében. Prioritást élvez az online bűnügyi nyomozás akadályainak, és az internetalapú bizonyítékokhoz és információkhoz való hozzáférés szabályainak a megállapítása. Deres Petronella[29] szerint a közelmúlt eseményei rávilágítottak annak szükségességére, hogy fokozzuk az erőfeszítéseket, és felgyorsítsuk a stratégiában meghatározott konkrét intézkedések végrehajtását. Erre szolgál a FIDUCIA kutatási projekt[30] 9. munka-csomagja is, mely a számítógépes bűnözés jogi, kriminológiai és szociológiai vonatkozásait tárja fel, elemzi az egyes bűncselekményeket, az ezekhez kapcsolódó adatgyűjtést, felülvizsgálja a jogi szabályozást és a megelőzés érdekében tett intézkedéseket.

4.4. A csúcstechnológiai bűnözés elleni harc régen és ma

A csúcstechnológiai bűnözés elleni egység legkorábbi elődje az Országos Rendőr-főkapitányság (ORFK) sajtófigyelő csapata volt. Az ő feladatuk a rendőrségi sajtómegjelenésekhez kapcsolódó tartalmak követésére terjedt ki. Később hatáskörük bővült az internetes jogsértések monitorozásával, majd 2007 februárjában nyomozati jogkört kapott az egység, ekkor hozták ugyanis létre a témával jelenleg foglalkozó osztályt, akkor már a Nemzeti Nyomozó Iroda részeként. Jelenleg Magyarországon inkább számítógépes bűnözésről lehet beszélni, de a technika fejlődési irányai és üteme tekintetében átfogóbb a csúcstechnológia kifejezés. A kiberbűnözők ellen harcoló rendőrök az internetes jogsértések mellett bejelentések, feljelentések, illetve saját nyomozásaik alapján értesülnek egy-egy újabb esetről. Bár a teljes internet monitorozása lehetetlen feladat, a már megismert

---

[28] Elkészült a Digitális Oktatási Stratégia, http://www.kormany.hu/hu/hirek/elkeszult-a-digitalis-oktatasi-strategia [letöltve: 2016. szeptember 20.]

[29] Tanszékvezető docens, KRE-ÁJK Büntetőjogi, Büntető Eljárásjogi és Büntetés-végrehajtási Jogi Tanszék.

[30] A FIDUCIA – „New European Crimes and Trust-based Policy" egy európai finanszírozású (EU FP7) projekt, amely kifejezetten a büntető-igazságszolgáltatás és az intézményi bizalom összefüggéseit vizsgálja. Célja, hogy kidolgozza a bizalomalapú közpolitika-csinálás modelljét, és ez alapján ajánlásokat fogalmazzon meg a kriminológia új területein, így a kiberbűnözésről is.

bűncselekmények kapcsán felmerülő területeket visszatérően vizsgálják. Kisebb ügyekben megyei, városi illetve a Budapesti Rendőr-főkapitányság és a kerületi szervek is nyomozhatnak. A Nemzeti Nyomozó Irodához (NNI) a nagyobb felkészültséget igénylő ügyek kerülnek. 2008 óta a Budapesti Rendőr-főkapitányságon is van egy kiberbűnözés elleni fellépésre specializált egység. A nyomozók munkáját a hagyományos rendőri kellékek mellett speciális felkészültségű nyomozók, illetve „law enforcement" eszközök segítik. Utóbbiak nagy teljesítményű szoftverek és hardverek, melyeket kifejezetten igazságszolgáltatási célokra alakítottak ki. A nyomozók a jól felkészült bűnözők ellen így is lépéshátrányban vannak technológiai szempontból, de ezt a hátrányt igyekeznek minél kisebb szintre szorítani. Egyre több a bejelentett számítógépes bűntény, a jelentősebb ügyek száma 1% körüli hazánkban. Gazdag Tibor[31] szerint a legjellemzőbb bűncselekmények az internetes csalások, a pornográf felvételek, valamint a személyes adatokkal való visszaélések. Jellemzőek még a szerzői jogsértések, ezekkel viszont 2011. január 1. óta a Nemzeti Adó-és Vámhivatal (NAV) foglalkozik.

4.5. A Nemzeti Kibervédelmi Intézet megalakulása

A 2013. évi L. törvény[32] módosításával 2015. október 1-én megalakult a Kormányzati Eseménykezelő Központ (GovCERT-Hungary[33]), a Nemzeti Elektronikus Információbiztonsági Hatóság, és a koordináltabb információáramlást lehetővé tevő Nemzeti Kibervédelmi Intézet[34]. Az Intézet az elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan feladatkörrel rendelkezik, feladata annak nyomon követése és segítése, a tervezési szakasz koordinálása, a szabályozás, ellenőrzés és incidenskezelés megvalósítása. Ennek céljából együttműködik az Információbiztonsági Hatósággal, az Eseménykezelő Központtal, valamint a Biztonságirányítási és Sérülékenység vizsgálati területtel[35]. Kapcsolatot ápol továbbá számos nemzetközi kibervédelmi szervezettel, úgymint az ENISA, a FIRST[36], a TI[37], az IWWN[38], illetve a Central European Cyber Security Platform[39]. Feladata az ügyfelek és rendszerek nyilvántartása, a biztonsági osztályba és szintbe sorolás ellenőrzése, sérülékenység vizsgálat elrendelése, javaslattétel létfontosságú rendszer kijelölésére valamint információbiztonsági felügyelő kirendelésére. A napjaink információs társadalmát érintő fenyegetések miatt kiemelten fontos a nemzeti elektronikus adatvagyon és az ezt kezelő információs rendszerek és rendszerelemek biztonsága. Az alapvető elektronikus információbiztonsági követelmények közé tartozik a kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer és elemeinek sértetlensége és rendelkezésre állása. A szervezeteknek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, melyek támogatják a megelőzést, a reagálást, az észlelést és a biztonsági események kezelését. A Nemzeti Elektronikus Információbiztonsági Hatóság feladatai közé tartozik az Európai Unió tagállamaiban történő elektronikus információs rendszer üzemeltetése, az EU tagállamokon

[31] Az NNI Csúcstechnológiai Bűnözés Elleni Osztályának vezetője.
[32] 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról.
[33] A magyar kormányzat információ-megosztó és incidens-kezelő szervezete, szolgáltatásait a kormányzati szervezetek és az önkormányzatok részére nyújtja. Főbb feladatai a biztonsági események kezelése, ügyeleti szolgálat, elemzés/értékelés, kibervédelmi gyakorlat, képzés, tudatosítás, sérülékenység vizsgálat.
[34] A Nemzeti Kibervédelmi Intézet a korábbi, E-biztonsági Intelligencia Központot (NBF-CDMA) egységes keretben magába foglalja, ezáltal hatékonyabb feladat-végrehajtást biztosít.
[35] Feladata a sérülékenység vizsgálat és a biztonsági események kivizsgálása, valamint az EMIR / FAIR rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása.
[36] Forum of Incident Response and Security Teams.
[37] Trusted Introducer.
[38] International Watch and Warning Network.
[39] Visegrádi Négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform.

kívül eső információs rendszerek ellenőrzése, és az információtechnológiai fejlesztési projektekben megjelölt követelmények érvényesülésének ellenőrzése. A Hatóság továbbá kormányzati információtechnológiai és hálózatbiztonsági információ-megosztási, incidens-kezelési munkacsoportot működtet, melynek fő profilja az információbiztonság növelése. A munkacsoport tagjait a Hatóság által felkért szervezetek, a szakhatóság és a kormányzati eseménykezelési központ delegálják.

5. Új devianciák az online-térben

Mára mind a személyes használatban lévő, mind az üzleti vagy állami célra használt számítógépek és számítástechnikai rendszerek az elkövetők keresett eszközei, célpontjai lettek. Az internet technológiája nemcsak új bűncselekmények megjelenését idézte elő, hanem új teret adott a már létező és a büntetőjog által fenyegetett cselekményeknek is. Ezzel egyetemben számos újszerű deviáns magatartás tűnt fel az információs társadalomban, olyanok is, amelyek a társadalom egy korábbi szintjén meghatározásuknál fogva nem létezhettek, és olyanok is, amelyek más formában, de jelen voltak a társadalomban.
Az elkövetők indítéka, valamint az elkövetés célja, módja és célzott személyi köre alapján eltérő zaklatási típusokról beszélhetünk. Eszerint a zaklatás munkahelyi, szexuális, faji-etnikai alapú vagy személyes indíttatású cselekvésként kategorizálható. A munkahelyi, szexuális zaklatók főként olyan férfiak, akik pozícióféltésből vagy szexuális kapcsolat létesítésére keresik áldozataikat. Az Európai Parlament és a Tanács társjogalkotásából született 2002/73/EK irányelv tartalmazza a diszkriminációval és szexuális zaklatással kapcsolatos legújabb rendelkezéseket. A faji-etnikai megkülönböztetés elleni küzdelem fegyvere az Európai Tanács 2000/43/EK irányelve, mely a faji- vagy etnikai származásra való tekintet nélküli egyenlő bánásmódot hirdeti. A legtöbb zaklatásról elmondható, hogy a sértett és a tettes közt valamilyen kapcsolat áll vagy állt fenn, így gyakori, hogy az elkövető már a kapcsolatuk kezdetétől molesztálja áldozatát. Hazánkban először a 2003. évi CXXV. törvény[40] említette a zaklatást, olyan magatartásként, mely az egyenlő bánásmódot, az emberi méltóságot sértő, szexuális vagy egyéb természetű jelenség, amelynek célja valamely személlyel szemben ellenséges, megfélemlítő, megszégyenítő vagy támadó környezet kialakítása. A jogalkotó célja azon súlyosabb jogsértések pönalizálása volt, melyek más személy rendszeres vagy tartós háborgatását eredményezik, jelentős érdeksérelmet okozva a magánéletébe való önkéntes beavatkozással. A törvény indokolása szerint általános tapasztalat, hogy a zaklató magatartása az idő múlásával egyre fenyegetőbb, durvább lesz, ami súlyos pszichés zavarokhoz, de akár tulajdon vagy személy elleni erőszakos bűncselekmények elkövetéséhez is vezethet. A hatályos jogi szabályozást a 2012. évi C. törvény paragrafusai között találjuk. Az információs társadalom devianciáinak jelenléte nagymértékben az infokommunikációs technika elterjedt használatához köthető. A devianciák a társadalmi értékrendek, szokások változását is példázzák. Amíg egy-egy új magatartás nem rendelkezik egységes társadalmi megítéléssel, addig a hazai büntetőjog sem mutathat megfelelő szankcionálást. Mivel az infokommunikációs eszközök könnyen elérhetők, így a fiatal generációk nagyobb része birtokolja, és napi rendszerességgel használja őket. Meglátásom szerint a technológia terjedésének jelentős hatása van az interneten elkövetett bűncselekmények növekedésére.

5.1. Cyber-bullying

A zaklatás napjainkra mindennapossá nőtte ki magát az internetes világban. A cyber-bullying egy új típusa az elsősorban tinédzser korúak közt tapasztalható iskolai kiközösítésnek.

[40] 2003. évi CXXV. törvény az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról.

Megvalósulhat fenyegető üzenetek formájában, grooming[41] során, az áldozat nevében vagy akár személyes adataival való visszaéléssel is. A gyermekekre káros internetes tartalmak kiszűrését támogató Biztonságos Böngészés Programhoz (BBP) már több száz iskola csatlakozott, illetve több ezer munkaállomás programtag. A BBP projekt során a diákok által használt komputerekre olyan szűrőszoftvereket telepítenek, melyek kiszűrik a fiatalokra káros tartalmakat és az internetes zaklatást. Magyarországon a gyerekközösségekben megnyilvánuló erőszakra egyre több figyelem vetődik. A Nemzeti Média- és Hírközlési Hatóság 2011-től elrendelte az Eu Kids Online I-III projekteket, melyek átfogó célja a gyerekek internethasználati jellegzetességeinek, illetve az ezekhez kapcsolódó kockázatok és veszélyek megismerése, megértése. A felmérés szerint a magyar gyerekek 19%-át érte a kérdezést megelőző évben a kortársai részéről zaklatás. Az érintettek 73%-át személyesen érte a sérelem, és csupán 30%-ukkal fordult elő az interneten (is). Az internetes zaklatások helyszínei nagyrészt a közösségi oldalak és az azonnali üzenetküldők. A zaklatottak 49%-a említette ezt a két alkalmazást a zaklatás „helyszínéül". A gyerekek 15%-a maga is viselkedett már zaklatóan a világhálón. A projekt eredményei azt mutatják, hogy bár a magyar gyerekeket viszonylag kis számban érintik a vizsgált kockázatos tevékenységek, a tanácsadóknak és szülőknek fel kell készülniük a veszélyeztetettség eme új dimenzióira. A cyber-bullyingnak számos alfaja ismert, ezek közül kiemelendő a flaming, az identitáslopás, a stalking illetve a sexting. A flaming[42] során a fórumokon trágár hozzászólások kerülnek a nyilvánosság elé, a vita gyakran vallási, ideológiai vagy politikai kérdésen alapszik. Az identitáslopás gyakran jár az áldozat e-mail fiókjának vagy közösségi oldalának feltörésével, legtöbbször azzal a szándékkal történik, hogy a nevében kompromittáló üzenetet továbbítsanak ismerősei számára. A cyber-stalkingot elszenvedettek folyamatos fenyegetés alatt állnak, adataik vagy online szokásaik rendszerint erőszakos tartalmú üzenetek formájában kerülnek nyilvánosságra, ezáltal az elkövetők a veszélyeztetettség érzését keltik bennük. Végül, de nem utolsó sorban a sexting provokatív, szexuális tartalmú fényképek, videók készítését és terjesztését jelenti, melyek napvilágra kerülése akár egy életen át üldözheti a szégyenbe hozott személyt.

Fontosnak tartom hangsúlyozni, hogy minden korosztály válhat internetes bűncselekmények áldozatává, életkortól függetlenül. A megfelelő szakértelemmel, technológiai ismeretek elsajátításával, helyzetük mihamarabbi felismerésével viszont jelentősen mérsékelhető a bűnelkövetési ráta. Konkrét segítséget jelenthet, ha a lehető leggyorsabban eltávolítják a veszélyes tartalmakat, ezért fontos, hogy a hatóságok és civil szervezetek együttműködjenek az áldozatokkal és azok hozzátartozóival. Sosem lehetünk eléggé felkészültek az internetes kockázatok és ártalmak semlegesítésében. A megfelelő kezeléshez először a probléma létezésének tudatosítására kell rávilágítanunk.

5.1.1. Cyber-stalking

J. Reid Meloy napjaink egyik kiemelkedő pszichológus professzora, aki az Egyesült Államok tagállamaiban megjelenő zaklató magatartásokat kutatja. Kutatásai szerint a stalking fogalma tagállamról tagállamra változik, néhány fogalmi elem azonban minden definícióban megtalálható. Eszerint a stalking olyan másra irányuló, nem kívánt, háborgató viselkedés, amely burkoltan vagy kifejezetten fenyegető és hatására a megfenyegetett komoly félelmet

[41] Bár a grooming, azaz az online behálózás önmagában nem bűncselekmény, alkalmas a gyermekek személyes adatainak kicsalására, „szexuális játékokba" való bevonására, az áldozatok szégyenérzetének erősítésére.

[42] A flaming vagy másnéven flame war során szándékosan jogsértő, ellenséges, témához nem kapcsolódó hozzászólásokat küld az elkövető az internetes fórumra. A kifejezés mára bizonyos fokig elavult, pontosabb definíció lehet a problémakörre a trolling, mely azonban valamivel tágabban, a teljes provokatív, vitagerjesztő magatartást leírja.

érez. [43]Pszichiátriai- klinikai értelemben a stalking meghatározott személy rendellenes vagy tartós fenyegetése vagy nyugtalanítása. Akkor tekinthető egy fenyegetés komolynak, ha az egy ésszerűen gondolkodó személyben nagymértékű aggodalmat kelt, ha az áldozat hisz abban, hogy az elkövető beváltja fenyegetéseit, vagy ha azok jelentős érdeksérelemmel jártak. A zaklatás nem kizárólag az áldozatra korlátozódik, érintheti annak barátait, családtagjait, tulajdonát, és az elkövetőnek tisztában kell lennie tettei súlyával. A személyes jellegű inzultálás elkövetője rendszerint hosszabb ideje, visszatérően molesztálja áldozatát az infokommunikációs környezetben. Az internet és a mobiltechnológia alapvetően két lehetőséget teremt az elkövető és áldozata kapcsolatát tekintve: a távoli hozzáférést és az állandó hozzáférhetőséget. A távoli hozzáférés annak lehetőségét biztosítja, hogy az elkövető bárhol is tartózkodjon, elérje áldozatát. Az állandó hozzáférhetőség az áldozat helyzetétől független. Egyes kommunikációs módok, például az e-mail vagy a chat csak írásbeli alapúak, az észlelés más módon nem valósul meg. A kommunikáció során nincs hang, mely segítene a közlő nemének, életkorának felismerésében, nem értelmezhetők reakciói, mimikája. Ugyanakkor az üzenetek mellé csatolt képek, zenék, linkek árulkodóak lehetnek a zaklató szándékait illetően. Emocionális és fizikai távolságot létesít az elkövető és áldozata között a közvetlen kapcsolat hiánya, mely az elkövetés érzelmi megkönnyítéséhez vezet. A stalking nem kizárólag e két fél között zajlik, példának okáért a proxy-stalking megvalósításával a tettes más online résztvevőket befolyásolva érheti el egy személy zaklatását. J. Reid Meloy szerint az internetnek sokoldalú szerepe van a zaklatás során. Egyrészt eszközként szolgál az elkövetőnek az információgyűjtéshez, másrészt olyan kommunikációs csatorna, melyen keresztül az áldozat könnyen megfenyegethető, inzultálható. Nem utolsó sorban, az időhöz fűződő függetlensége miatt azt az érzetet keltheti a sértettben, hogy zaklatója bárhol, bármikor a közelében van. Az anonimitás az áldozat alávetettségét fokozza, azt az érzetet kelti benne, hogy az elkövető a környezetéből bármely személy lehet.

5.1.2. Sexting

Félelem, depresszió, szorongás, önértékelési problémák: csak néhány olyan következmény, melyeket a zaklató magatartások okoznak. A sexting során a felhasználók önmagukról készített erotikus tartalmú fényképeket, videókat és szexuális töltetű üzeneteket küldenek egymásnak infokommunikációs eszközeikkel, vagy e felvételeiket internetes közösségi oldalakon közzéteszik. A jelenség a tinédzser korosztályt érinti a legszámottevőbben, ennek valószínűsíthető oka a serdülő korosztály szexuális túlfűtöttsége, kísérletező magatartása, illetőleg tetteik súlyosságának fel nem ismerése. Míg a cyber-bullying más magánszférájának a semmibe vételét jelenti, addig a sexting a felhasználó saját magánszférájának teljes nyitottságát eredményezi. A magyar társkereső oldalakra évente több ezer gyermekpornográfiával kapcsolatos hirdetés kerül fel. A Pew Internet&American Life Project nevű, független Egyesült-államokbeli szervezet 2009-es kutatása alatt összegyűjtött adatokból az derül ki, hogy a 12 és 17 év körüli korosztály 15%-a kapott már erotikus jellegű képet Amerikában. Az Eu Kids Online felmérés[44] második projektjének adataiból kiderült, hogy a 9-16 éves magyar gyerekek csaknem 16%-a találkozott már szexuális jellegű képpel vagy videóval. [45]Az érintettek 4%-a mondta, hogy napi szinten találkozik ilyen felvételekkel, 13%-uk egyszer-kétszer a héten, 19%-uk egyszer-kétszer a hónapban, míg 49%-uk ennél

---

[43] J. Reid MELOY: Stalking – An Old Behaviour, A New Crime, 1999, http://drreidmeloy.com/wp-content/uploads/2015/12/1999_Stalking_anOldB.pdf [letöltve: 2016. november 10.]

[44] Ld. 5.1. Cyber-bullying

[45] EU Kids Online II. A magyarországi kutatás eredményei – Készült a Nemzeti Média- és Hírközlési Hatóság megrendelésére. Szerkesztő: ITHAKA Nonprofit Kft., 2011. szeptember, http://nmhh.hu/dokumentum/3886/ITHAKA_EU_KIDS_Magyar_Jelentes_NMHH_Final_12.pdf [letöltve: 2016. 08.20.] 3.

ritkábban.[46] Ez azt jelenti, hogy a teljes 9-16 éves korosztály 10%-a szembesült ilyen jellegű tartalommal az interneten. Ugyanakkor a pornográf felvételek még mindig fontos forrása a televízió illetve a filmek, az érintettek csaknem fele és a teljes korosztály 8%-a ezeken a csatornákon jutott hozzá a tiltott tartalmakhoz. Az érintettek csaknem harmada állította, hogy automatikusan felugró lapokon látott ilyeneket, 29%-uk videómegosztó-oldalakon, negyedük pedig felnőtteknek szóló, korhatáros oldalakon látta a képanyagokat. A szexuális jellegű üzenetekkel kapcsolatos kérdések csupán a 11 éves és annál idősebb gyerekek kérdőívében szerepeltek. A 11-16 év közötti fiatalok 7%-a állította, hogy a kérdezést megelőző egy évben kapott szexuális jellegű üzeneteket az interneten keresztül. 62%-uk a havi gyakoriságnál ritkábban kapott ilyen üzeneteket, 21%-uk havonta, 7%-uk hetente, 4%-uk pedig naponta szembesült ilyen levelekkel.[47] A fiúknak és az idősebbeknek nagyobb esélyük van arra, hogy ilyen üzeneteket kapjanak. Minél régebben használja valaki a világhálót, annál valószínűbb, hogy érkezik hasonló üzenete. A szexuális jellegű tartalmak legtöbbször vagy véletlenül jutnak el a fiatal korosztályhoz, vagy üzenetküldőn keresztül kapják azokat. A legtöbb esetben konkrét üzenetről van szó, de előfordul az is, hogy valakit arra kérnek, vegyen részt szexuális jellegű párbeszédben vagy intim testrészéről osszon meg fotókat. Gyakori még, hogy az érintett fiatal másvalakik szexuális aktusának lesz tanúja valamiképp az interneten. A megkérdezett gyermekek csupán 1%-a állította, hogy sextingelt már. A magyar gyerekek csaknem negyede került már kapcsolatba olyan emberrel a világhálón, akit nem ismert. Harmaduk személyesen is találkozott valamilyen ismeretségével. Ez azt jelenti, hogy a 9-16 évesek 7%-a vett már részt ilyen találkozón. Már a 13-14 évesek körében is átlag feletti az ismerkedők aránya, ami azonban a 15-16 éves korosztálynál 43%-ra ugrik. Az internetet tapasztaltabban, napi szinten használói nagyobb arányban alakítanak ki ilyen kapcsolatokat.[48]A 15-16 éves, online ismeretséget kötő lányok csaknem fele találkozott már interneten megismert személlyel. Érdekes tény, hogy Új-Mexikóban legálissá tették a sextinget, így a serdülő korosztály is szabadon oszthat meg szexuális tartalmakat egymás között. George Muñoz szenátor szavaival élve, a gyerekek mindig gyerekek maradnak, és el fognak követni hibákat. Az államfő szerint nem lehet életük végéig büntetni őket azzal, hogy gyermekpornográfia terjesztésével vádoljuk őket. Az állampolgárok többsége osztja Muñoz szenátor véleményét, egyesek szerint azonban ezzel egy kiskaput nyitottak a pedofilok számára, akik így egyszerűbben és gyakrabban követhetnek majd el gyermekpornográfiával kapcsolatos tevékenységeket. Az Európai Parlament az interneten terjedő pedofil tartalmak alaposabb kivizsgálását, az elkövetők bíróság elé állítását, az áldozatok védelmét és az illegális tartalmak eltávolítását szorgalmazza.

5.2. Adathalászat: phishing, pharming

A cybercrime elkövetésének egy másik lehetséges esete az adathalászat. A phishing támadások során kiberbűnözők potenciális áldozatok millióinak küldenek levelet világszerte, amelyekkel átverik vagy támadják őket. Az üzenetek látszólag megbízható forrásból érkeznek, gyakran sürgető határidővel egybekötve, és a mit sem sejtő online felhasználók személyes adatainak, banki azonosítóinak, jelszavainak megszerzését célozzák. A pharming során, ezt tetézve a levelek általában egy káros kódot tartalmazó, támadó honlapra mutatnak. Támadónak nevezzük az olyan weboldalakat, melyek megpróbálják rosszindulatú szoftverrel (malware) megfertőzni a látogatók számítógépét. A malware-eket személyes adatok elsajátítására, levélszemét küldésére, számítógép és cserélhető meghajtóinak megfertőzésére, illetve további hasonló szoftverek terjesztésére használják. Az is előfordulhat, hogy az adathalász levél egy fertőzött mellékletet tartalmaz, mely megpróbálja beszennyezni gépünket

[46] ITHAKA i. m. 3-4.
[47] ITHAKA i. m. 5.
[48] ITHAKA i. m. 7.

és átvenni felette az irányítást. A spear phishing, vagyis célzott adathalász támadás során a támadók jóval célirányosabb leveleket küldenek, az áldozatok listája ez esetben igen rövid, körülbelül 5-10 tagból áll. Ennek célja a kiszemelt 'célpontok', felhasználók online szokásainak tanulmányozása, például Google- vagy Facebook fiókjaik átolvasásával, fórumokon közölt üzeneteik vizsgálatával. Ezt követően a támadók egy személyre szabott, relevánsnak tűnő levelet készítenek a kiszemelt személy számára, így az még nagyobb valószínűséggel válhat áldozattá. A célzott adathalászat sokkal veszélyesebb fenyegetés az egyszerű adathalász támadásoknál, mivel e támadások felfedése is jóval nehezebb. A támadásokkal szembeni védekezés első lépése annak megértése, hogy mi magunk is lehetünk célpontok. Mi, illetve a cégünk is birtokolhat olyan bizalmas információt, amelyet valaki más szeretne megszerezni. Minél több személyes információt osztunk meg magunkról az online-térben, annál kiismerhetőbbek, egyúttal támadhatóbbak leszünk a támadók számára. A legelterjedtebb webböngészők már felveszik a harcot az adathalászok ellen, a biztonsági csomagokból ismert phishing szűrő vészjelzést ad a gyanús oldalak meglátogatásakor. Eszerint elkülöníthetjük a megbízható oldalak fehér listáját és az ismert phishing oldalak fekete listáját, melyek ezután automatikusan frissülnek a számítógépen. A rendszeresen frissített operációs rendszer és tűzfal jó alapjai a támadások elkerülésének. Lényeges továbbá a homográf[49] weboldalak elkerülése, és gyanakvásunk állandó fenntartása.

5.2.1. A phishing szabályozásának új koncepciója

Az adathalászat elleni védelmi stratégiák alulszabályozottsága az online felhasználók együttműködéseinek hézagosságában mutatkozik meg. Ennek orvoslását a hazai internet-szolgáltatókra vonatkozó jogszabályok módosításában látom, úgy gondolom, hogy lényeges lenne a strukturált adatszolgáltatási kötelezettség előírása számukra. Az általuk alkalmazott kéretlen levél-szűrő rendszerekre implementált adatfeldolgozó alkalmazások készítését javaslom. Az adatgyűjtés kulcsfontossága megkívánja egy ennek folytatására szakosodott szerv életre hívását, esetleg egy már működő szervezet kijelölését erre a feladatra. Úgy vélem, hogy a Nemzeti Kibervédelmi Intézet erőforrásai és képességei tekintetében alkalmas lehet erre a pozícióra. A vállalatok kötelességévé javaslom tenni a kockázatok tudatosítását a társadalmi szférával, oktatási és egyéb kezdeményezéseiken keresztül. Ennek azért látom szükségét, mert a cybercrime legsérülékenyebb szereplője maga a felhasználó, ezért fogékonyabbá kell tenni a kiberéberségre. AZ IT-cégek ehhez szoftvereik biztonságosabbá tételével járulhatnak hozzá. Egyre több szervezet beszél nyíltan az elszenvedett adatlopásokról, online támadásokról, az Egyesült Államokban erre már törvény is kötelezi őket. Hogy egy példát említsek, a CNN Money oldalán megjelent cikk szerint 2016 szeptemberében amerikai olimpiai bajnokok egészségügyi adatait is hackertámadás érte.[50] Egy erre irányuló törvényi kezdeményezés a hazai szabályozásra is pozitív hatással lenne, a piaci szereplők körében redukálódna az elhallgatott biztonsági események száma. A vállalatok és intézmények rendszerei sérülékenyek, feltörhetők, ezt nem szabad elhallgatni, hiszen az információk megosztása mindannyiunk biztonságát növelheti. Európai uniós fejleményként említhető, hogy a 2016-os holland uniós elnökség idején a tagállamok elfogadtak egy törvényjavaslatot, amely a szervezeteket a biztonsági események felelősségteljes nyilvánosságra hozatalára kötelezné, ez pedig kedvezően hatna a következmények kezelésére és elhárítására. Kiváló védekezési módszernek tartom az egyre ismertebb kiberhírszerzést is, mely a fenyegetési környezetet világszinten elemzi, és az összegyűjtött információkból regionális sajátosságokat azonosít, melyekkel a biztonsági cég akár egy kibontakozó támadás

[49] A számítástechnikában a homográfia olyan webcímet jelent, amely látszólag ismert cím, de valójában eltér attól. Az adathalászat során használt hamis webhivatkozások célja az áldozat megtévesztése.

[50] Ivana KOTTASOVA: Hackers steal medical data of US Olympic stars, http://money.cnn.com/2016/09/13/news/wada-hacked-russian-spies/index.html [letöltve: 2016. november 20.]

kivédésére is képes lehet. Ennek naprakész működéséhez szükséges lenne az ügyféloldalon is felállítani egy biztonsági műveleti központot. A threat intelligence[51] szolgáltatások hazai bevezetését a vállalatok korlátozott pénzügyi lehetőségei is nagyban befolyásolják, ezek azonban rendkívül hasznos eszközök lehetnek a kibertámadások kivédésében. Támogatom továbbá az ún. bug bounty programok[52] létrehozását, melyek a hibakereső magánszemélyek elismerésével és jutalmazásával a szervezetek sérülékenységének vizsgálatát és fejlesztését indukálhatják. Az etikus hackereket[53] anyagi megfontolásból csupán alkalmanként veszik igénybe a szervek, de jó, ha róluk sem feledkezünk meg: az Óbudai Egyetemen és a KÜRT Akadémián már képzésük is zajlik, mely az EC Council által kiadott Certificied Ethical Hacker képzettség megszerzésével jár együtt. Összességében mind felhasználói, mind vállalati szinten szükség van módosításokra, melyek alkalmazásával az adathalászat egy sokkal áttekinthetőbb és könnyebben leküzdhető jelenséggé válhat.

6. Az Európai Unió számítógépes bűnözésre vonatkozó jogforrásai

Az Európai Unió Bizottsága kiemelt fontosságú veszélyként tekint az információs rendszerek elleni támadásokra, célkitűzése egy biztonságon és jogérvényesülésen alapuló térség megvalósítása. A Tanács 2005. február 24-én megalkotta a 2005/222/IB. számú kerethatározatot, mely lényegét tekintve közel azonos a Cybercrime- Egyezmény számítástechnikai bűncselekményekre vonatkozó tényállásaival. A kerethatározat uniós jogforrás, így kötelező erővel bír az unió valamennyi tagállamára nézve, tehát jelentős lépésnek tekinthető az informatikai bűncselekmények elleni uniós együttműködésben. A jogforrások közé sorolható még a 2001/413/IB. számú kerethatározat a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről, valamint a 2002/58/EK elektronikus hírközlési adatvédelmi irányelv is. Utóbbi arra kötelezi a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, hogy biztosítsák szolgáltatásaik biztonságát, továbbá rendelkezéseket tartalmaz a kéretlen levelek és kémprogramok ellen is. Az internethasználat biztonságosabbá tétele érdekében a hálózat-és információbiztonsági politika számos fellépéssel lett gazdagabb, például a biztonságos információs társadalomra irányuló stratégiáról szóló közleménnyel (COM(2006) 251.), valamint a kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről szóló közleménnyel (COM(2006) 688.). A 460/2004/EK rendelet az Európai Hálózat-és Információbiztonsági Ügynökség (ENISA) létrehozásáról szól. A nemzetközi bűnügyi együttműködés fejlesztése érdekében számos egyezmény született és több kiváló nemzetközi szervezet jött létre, köztük az Interpol, az Europol és az Eurojust. E szervezetek mindegyike a határon átnyúló valamennyi bűnözési forma visszaszorítására jött létre, így többek között a számítógépes bűnözés visszaszorítására is kiterjed a tevékenységük. A bűnügyi együttműködés egyszerűsítésére a 2006/960/IB. kerethatározat is tett lépéseket, célként tűzte ki, hogy a bűnüldözési operatív információkhoz való gyors és pontos hozzáférést biztosítson. A kerethatározat érvényesülésének érdekessége, hogy amennyiben valamely tagállam a beszerzett információt vagy bűnüldözési operatív információt bíróság előtt bizonyítékként kívánja felhasználni, be kell szereznie az információt vagy bűnüldözési operatív információt szolgáltató tagállam beleegyezését a tagállamok között hatályban lévő, az igazságügyi együttműködésre vonatkozó eszközök alkalmazása útján. A beleegyezés beszerzése nem szükséges, amennyiben a megkeresett tagállam az információ vagy bűnüldözési operatív információ átadásakor beleegyezését adta annak bizonyítékként történő használatához. A

[51] E szolgáltatások célja, hogy a vállalatok proaktívan részt vegyenek a fő infrastruktúrájukban, adataikat és vezetőiket célzó kibertámadások felismerésében, azonosításában és az ellenük való védekezés során.
[52] Hibafelderítési jutalomprogram, mely biztonsági rések felkutatására szolgál.
[53] Speciálisan képzett informatikai biztonsági szakértő, aki képes a vállalati informatikai rendszerek sérülékeny pontjainak felderítésére, a csalások felfedésére, és megoldási javaslatokat tesz e problémák kezelésére.

Tanács 2009/316/IB. határozatában döntött az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) [54]létrehozásáról. Az EU Stockholmi Programja[55] a 2011-2015. közötti időszakra vonatkozóan előirányozta az európai bizonyítékgyűjtési rendszer kidolgozását.

6.1. Az ENISA szerepe

Az Európai Hálózat- és Információbiztonsági Ügynökség székhelye a görögországi Iráklioban van. A 2004-től működő szervezet célja, hogy az Európai Unió, a tagállamok és az üzleti szféra fokozottabb mértékben legyen képes a hálózat-és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra. Továbbá, felkérés esetén segíti a Bizottságot az uniós jogszabályok korszerűsítését és kidolgozását szolgáló technikai előkészítő munkájában. Ezen felül fokozza az együttműködést az állami és a magánszektor szereplői között, hogy kielégítően magas szintű biztonság valósulhasson meg az EU-tagállamokban. Ezen célkitűzések elérése céljából az ENISA összegyűjti a megfelelő információkat a jelenlegi és jövőbeni kockázatok elemzéséhez, és kutatási eredményeiről tájékoztatja a tagállamokat és a Bizottságot. Az Európai Parlament, a Bizottság és az illetékes európai és nemzeti szervek számára tanácsot ad, segítséget nyújt, valamint fokozza az ágazati szereplők közötti együttműködést. Célja még, hogy elősegítse a Bizottság és a tagállamok közötti együttműködést a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozása során, s hozzájáruljon a tudatosság növeléséhez és a naprakész, átfogó információk szolgáltatásához valamennyi felhasználó számára. Segíti a Bizottságot és a tagállamokat az iparról, illetve hardver-és szoftvertermékek biztonságáról folytatott párbeszédek során, nyomon követi a biztonsági termékek és szolgáltatások szabványainak kialakítását, előmozdítva a kockázatértékelési és kockázatkezelési tevékenységeket. Az ENISA hozzájárul az EU-n kívüli országokkal és nemzetközi szervezetekkel folytatott együttműködéshez azzal, hogy elősegíti a biztonsági kérdésekre vonatkozó globális szemlélet terjedését, és megfogalmazza saját következtetéseit, iránymutatásait, tanácsot ad a segítségkérőknek.

6.2. European Cybercrime Centre

Az Europol Kiberbűnözési Központ testesíti meg az Európai Unió informatikai bűnözés elleni küzdelmét, tevékenységével hozzájárul a határon átnyúló bűncselekményekre való gyors reagáláshoz. Elsősorban a bűnszervezetek, bűnszövetségek általi kibertámadásokra összpontosít, ennek céljából együttműködik a számítógépes bűnözésben eljáró hatóságokkal, a tagállamok nyomozati szerveivel, nemzetközi bűnüldöző hatóságokkal, illetve a civil szférával. Adatokat gyűjt a számítógépes bűnözésről, kiberbűnözési helpdesket üzemeltet, támogatja a közös nyomozócsoportok létrehozását egy vagy több tagállam együttműködésével, összhangot teremt az Európai Unión kívüli tagokkal, és koordinálja a nemzetközi ügyek nyomozását. Értékeli a kibertérből érkező fenyegetéseket, elemzi a trendeket és előrejelzi a legújabb fejleményeket a kiberbűnözés alakulásában. Szoros együttműködést épített ki az Európai Rendőr-akadémiával, képzéseket szervez a nyomozó hatóságok tagjainak, a bíráknak és ügyészeknek, emellett forenzikus eszközöket fejleszt ki. Egy olyan információs infrastruktúra kialakításán dolgozik, melyben a vele együttműködő

[54] Az ECRIS egy egységes elektronikus hálózat, információcsere-rendszer, amely az egyes tagállami bűnügyi nyilvántartások információinak elektronikus cseréjét, így az unió polgárainak védelmét szolgálja. Alapját az egyes tagállamok bűnügyi nyilvántartásai képezik. Gyakorlati szempontból az összes tagállam bűnügyi nyilvántartásának elektronikus úton történő összekapcsolását jelenti. A büntetőjogi felelősséget megállapító ítéletekre vonatkozó információk cseréjére gyorsan, egységesen és számítógép útján könnyen továbbítható formában kerül sor.

[55] A Stockholmi Program meghatározza az Európai Unió által a jog érvényesülésén, a szabadságon és a biztonságon alapuló térségre vonatkozóan a 2010 és 2015 közötti időszakra megállapított prioritásokat.

szervezetektől származó minden adatot rögzítenek, melyek ez által visszakereshetőek lesznek a kiberbűnözésre vonatkozóan. A Kiberbűnözési Központ mellett speciális feladatokra felállított munkacsoport (European Cybercrime Task Force[56]) jött létre. Az Europol rendelkezik egy több elemből álló kiberbűnözési platformmal, melynek része többek közt az internetes bűncselekmények bejelentésére szolgáló online rendszer (Internet Crime Reporting Online System), melyre a világhálón észlelt deliktumokkal kapcsolatos információk tölthetők fel; egy kiberbűnözési munkafájl (AWF), valamint a technikai szakismeret bővítését ellátó internetes kriminalisztikai szakértői platform (Internet Forensic Expertise Platform). A Központ szervezetén belül három fókuszpont működik, az első az FP Cyborg (Kiberbűncselekményekkel foglalkozó fókuszpont), mely a tisztán informatikai jellegű bűncselekmények nyomozásával foglalkozik, illetve a számítógépes bűntények megelőzését és az ellenük való küzdelmet támogatja. A második az FP Twins, mely a gyermekek szexuális kizsákmányolásával foglalkozik, célja az elkövetők azonosítása és a tagállamok közötti kapcsolatok kialakítása. A határon átnyúló esetekben feladata még az elkövetési mód, a modus operandi feltárása, illetve a bűnelkövetői hálózatok kommunikációs módszereinek elemzése azok felbontása érdekében. A harmadik fókuszpont az FP Terminal, mely támogatja az EU tagállamok nyomozásait számos bankkártyás csalással kapcsolatban.

6.3. További kiemelkedő nemzetközi dokumentumok

A számítógépes bűncselekmények tekintetében irányadó nemzetközi dokumentumként elsőként az 1986-os OECD jelentést szeretném megemlíteni. A Gazdasági Együttműködési és Fejlesztési Szervezet[57] (OECD) iránymutatást adott az európai igazságszolgáltatás tapasztalatairól, segítve ezzel a számítógépes környezetben elkövetett bűncselekmények megismerését és kodifikálását. 1989-ben megjelent a strasbourgi székhelyű Európa Tanács 9. számú ajánlása, mely a cybercrime definiálása során már említésre került. Később, 1995-ben megjelent 13. számú ajánlása is, mely eljárásjogi problémákra reflektál. 1997-ben a G-8 fórum által Bűnözés elleni alcsoport alakult, és elfogadásra került a számítógépes bűnözés elleni harc tíz alapelve. 2001-ben létrejött a korábbiak során már említett Számítástechnikai Bűnözésről szóló Egyezmény is. Tíz évvel később, 2011-ben megszületett az Európai Parlament és Tanács 2011/92/EU számú irányelve a gyermekek szexuális bántalmazásáról, szexuális kizsákmányolásáról és a gyermekpornográfia elleni küzdelemről, mely büntetni rendeli a gyermekkel való, szexuális céllal történő internetes kapcsolatfelvételt. Két évvel később, az információs rendszerek elleni támadásokról született meg a 2013/40/EU irányelv, melynek célja, hogy bizonyos minimumszabályok megállapításával egymáshoz csiszolja a tagállamok büntetőjogát és javítsa a tagállamok hatóságai, a rendőrség, a bűnüldözési szakszolgálatok és az Unió ügynökségei és szervei közti együttműködést. Az irányelv felhívja a tagállamok figyelmét arra, hogy azonos büntetőjogi tényállási elemeket fogalmazzanak meg, szankcionálásuk során a szervezett bűnözés legyen minősítő körülmény, a jogosulatlan adatszerzés, a rosszindulatú szoftverek használata és személyiség-lopás legyen büntetendő, tilalmazandó. Cél továbbá, hogy a szankciók legyenek arányosak a bűncselekmény súlyával és legyen megfelelő visszatartó erejük, s nem utolsó sorban az alkalmazottak által végrehajtott cselekmények essenek súlyosabb elbírálás alá.

---

[56] Az EUCTF kurzusok szervezésével és technikai eszközökkel támogatja a tagállamok hatóságait, valamint a magánszektorral és a tudományos világgal is kapcsolatot tart a nyomozások fellendítése érdekében. Az internetes szervezett bűnözésről évente ad ki stratégiai elemzéseket (iOCTA), amelyek főként a kiberbűncselekmények értékeléseit tartalmazzák.

[57] Az OECD párizsi székhelyű nemzetközi szervezet, melynek célja, hogy segítse a tagállamok kormányait a lehető legjobb gazdasági és szociális politika kialakításában és értékelésében. Fő profilja a tagállamok gazdasági, kereskedelmi és pénzügyi tevékenységének összehangolása. Magyarország 1996 óta tagja.

6.4. General Data Protection Regulation (GDPR) – a jövő

Az Európai Parlament és a Tanács 2016/679. adatvédelmi rendelete[58] 2018. május 25-én lép hatályba, s lényegében minden olyan személyre, szervezetre vagy online szolgáltatásra irányadó lesz, ami kapcsolatban van a digitálisan tárolt személyes adatokkal. Az adatkezelőknek általánosan megfogalmazott szabályoknak kell megfelelniük az Európai Unió lakosairól tárolt adatok kezelése során, az állampolgárok pedig hivatalosan elismert jogokat szereznek saját adataik kezelése felett. Az előírások megszegése akár 20 millió eurós (több mint 6 milliárd forintos), vagy az éves árbevétel 4%-kát is elérő büntetéssel járhat. A GDPR kötelezővé teszi az adatkezelő számára a 72 órán belüli incidens bejelentést, minden érintett számára biztosítja a helyesbítéshez és törléshez való jogot és a hordozhatósághoz való jogot is. A személyek külön hozzájárulását kell kérni az adatgyűjtéshez, s ezt a hatóságok felé bizonyítani is kell, nem vélelmezhető. Az érintetteknek jogot kell biztosítani az adatkezelő vagy adatfeldolgozó által használt automatikus elbíráló rendszer döntése elleni fellebbezésre. Az elszámoltathatóság tükrében az adatkezelőnek ténylegesen bizonyítania kell, hogy megfelel a GDPR elvárásainak. Az ICO[59] 2016. március 14-én közzétett egy útmutatót[60], amely 12 lépésben segít felkészülni az új adatvédelmi rendeletre. A magyar Infotv.[61] kapcsán más alapokból kell majd kiindulni s ezért mások lesznek a prioritások is, de a listára így is érdemes figyelmet fordítani. Az ICO által javasolt 12 lépés:

1. Tudatosság
2. A meglévő információ
3. Az adatvédelmi információk átadása
4. A személyhez fűződő jogok
5. Az érintettek hozzáférési kérvényei
6. A személyes adatok feldolgozásának jogalapja
7. Beleegyezés
8. Gyermekek
9. Az adatokat érő jogsértések
10. Beépített adatvédelem és adatvédelmi hatásvizsgálatok (DPIA)
11. Adatvédelmi munkatárs
12. Nemzetközi szint.

6.4.1. Reflekciók az általános adatvédelmi rendeletre

Az Európai Parlament és Tanács 2016/679 rendelete elsőre egyszerűnek és távolinak tűnhet, ám a helyzet mást mutat. Bár a GDPR mind az adatkezelőket, mind az adatfeldolgozókat érinti, a szerepek gyakran felcserélődhetnek, és könnyen megeshet, hogy az adatkezelő egyben adatfeldolgozóvá is válik. Véleményem szerint az adatok kezelése szintén problémákat okozhat. Az adatkezelőknek többek között előzetesen vizsgálniuk kell a tárolandó adatok megfelelőségét, a tárolás jogszerűségét, az arra irányadó helyet, időt, és a lehetséges másolatokat, kivonatokat is. Mindez egy nagyobb szervezetnél, ahol az adatok áramlanak és feldolgozásuk esetenként kiszervezésben történik, igen körülményes feladat. A rendelet szinte kizárólag általánosan megfogalmazott pontokat tartalmaz, technikai részleteket nem – így komoly feladatot okoz majd az érintetteknek, hogy megfelelően implementálják az új rendelkezéseket. A GDPR komoly pénzbüntetés kiszabásával rendeli büntetni az előírások

---

[58] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.HUN&toc=OJ:L:2016:119:TOC [letöltve: 2016.09.10.]

[59] Az Egyesült Királyság adatvédelmi hivatala.

[60] https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/03/preparing-for-the-gdpr-12-steps.pdf [letöltve: 2016.09.25.]

[61] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV [letöltve: 2016.10.01.]

megszegőit, ez azt sugallja, hogy nem csupán opcionális ajánlásról van szó: 2018 májusa az adatkezelés új korszakának nyitányát hordozza magában.

7. Mary esete a kiberbűnözéssel

2015-ben született tanulmányában[62] Cameron S. D. Brown információs biztonsági szakértő egészen új oldaláról mutatta be a cybercrime-ot. Kutatásában egy kitalált személy, Mary esetén keresztül összegzi a kibertérben megjelenő felderítési folyamatokat, kérdéseket, nyomozati és infrastrukturális problémákat. Mary egy húszas évei végén járó egyetemista lány Ausztráliában, aki szexuális tartalmú e-maileket és sms-eket kap, melyek a lány magánéletének részleteit tartalmazzák. Véleményem szerint az eset azért különleges, mert aktuális képet mutat a 21. századi jelenségekről, ráadásul globálisan érvényesül, számos országban megjelenő és egészen aktuális problémakört vet fel. A következőkben Mary történetét szeretném részletesen bemutatni, párhuzamba állítva Brown kutatási eredményeivel és az olvasóközönségben felmerülendő kérdésekre adott válaszaival.

„Miután Mary jelentős mennyiségű szexuális tartalmú e-mailt és sms-t kap, szüleitől kér segítséget. Az üzenetekből kiderül, hogy a küldő tudja, Mary hova jár egyetemre, ismeri a baráti körét és egyéb személyes adatait. A zaklató a személyazonosságát nem fedi fel a lány előtt. Mary apja online kutatásba kezd, mely során felfedez néhány külföldi, erotikus tartalmú weblapon közzétett kommentet, melyekben lányát említik. Mind Mary, mind a szülei vonakodnak jelenteni az esetet a rendőrségen, mivel nem hisznek annak megfelelő felderítési képességeiben. Mi több, a lány nem tartja elég komolynak az esetet a rendőrségi feljelentéshez.”[63]

A műszaki szakértők, a rendőrség, a jogászság, a kriminológusok és a nemzetbiztonsági szakértők más-más módokon értelmezik a számítógépes bűnözés koncepcióját. Egyre nehezebben eldönthető, hogy a cybercrime jogi, szociológiai vagy műszaki fogalomként határozható-e meg. Brown szerint a jognak tartózkodnia kell a számítógépes bűnözés ’sui generis’ jogi kategóriájának megalkotásától és a jogi hézagpótlástól annak érdekében, hogy abba beleférjenek az új technológiai vívmányok. A kutató azt az elvet vallja, hogy a jognak a már meglévő hagyományos bűncselekmény-kategóriákat kellene kiszélesítenie, mivel az általa említett eljárásjogi és felderítési problémák nagy látenciát és alacsony nyomozati eredményességet okoznak. Mivel számos internetes bűncselekmény határokon átívelő, ezért a létező nemzeti jogszabályok nem képesek megfelelő számú eszközt biztosítani az elkövető felderítéséhez. Az anonimitás szintén a nyomozás eredménytelenségéhez vezethet, hiszen a világ bármely pontjáról bárki elkövetheti az adott cselekményt. Így Mary reakciója nem okoz nagy meglepetést az olvasónak, hiszen konzisztens a nyomozati szervek felderítési potenciáljába vetett alacsony bizalommal.

„Egy héttel később Mary elmeséli szüleinek, hogy ismeretlen hívása volt egy idegentől, aki szexuális fantáziálásra invitálta őt a vonal másik végéről. Valamivel később egy online hirdetőn talál egy, a nevében írt és telefonszámát is tartalmazó bejegyzést azzal a tartalommal, hogy arról fantáziál, hogy megrontsák őt. A lány kap egy e-mailt is, amely fenyegető stílusban íródott, és amelyhez mellékletként több személyes jellegű fényképet is csatoltak, többek között a lány lakhelyéről, illetve róla készült pillanatképekről, melyeken barátaival a kávézóban vagy az egyetemen tölti idejét. Van még egy fotó, mely a lány egyik

---

[62] Cameron S. D. BROWN: Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology. Szerk.: K.Jaishankar. 2015, http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf [letöltve: 2016.08.10.]

[63] S. D. BROWN op. cit. 58.

olyan ruhadarabját ábrázolja, amit úgy hiszi, hogy a ruhásszekrényéből vihettek el. Mary és szülei még aznap jelentik az esetet a rendőrségen."[64]

Mary esetében az eljáró hatóság a Police Central E-crime Unit[65] lenne, mely azonban csak a legsúlyosabb e-bűnözési incidenseket vizsgálja és az online zaklatást nem tartja keretrendszerébe tartozónak. Érdekességként, az FBI például 5000 dollárban állapította meg a nyomozás megindításának küszöbét. Ha a lány mégis a hatóságokhoz fordul és az E-crime Unit megindítja a nyomozást, a szerző szerint két irányba indulhat el a nyomozati szerv. Vizsgálhatja a cselekmények informatikai oldalát, vagy koncentrálhat a lányt körülvevő körülményekre és a hagyományos felderítési módszereket alkalmazva keresheti meg az elkövetőt. A tapasztalatok azonban azt mutatják, hogy e két módszer inkább együtt vezethet eredményre.

„Miután a rendőrség felvette Marytől a jegyzőkönyvet, továbbítja azt az E-crime Unitnak. Lyon rendőrfőnököt bízzák meg az üggyel. A sürgető fenyegetések az eset kiemelt fontosságú kezelését eredményezik. Lyon kapcsolatba lép Maryvel és interjút szervez a lánnyal, melynek során megkapja tőle az összes elektronikus levelezés másolatát, melyet a zaklatóval folytatott, valamint Mary minden számítógépes és egyéb adatát. Lyon figyelmezteti a lányt, hogy az online zaklatás kinyomozása nehéz feladat, főleg ha a tettes vagy a bizonyítékok más ország területén vannak. Lyon továbbá érdeklődik arról is, hogy a lány szakította-e meg mostanában a kapcsolatot valakivel az ismerősei közül, vagy van-e valamilyen elképzelése a zaklató személyazonosságáról. Azt a választ kapja, hogy a lánynak nemrég volt egy rosszul végződő szakítása előző barátjával, Paullal, miután rajtakapta őt, hogy megcsalja az egyik barátnőjével."[66]

Brown hisz abban, hogy a nyomozás sikerességéhez a nyomozó hatóság elkötelezettségére, 'soft' és 'hard' képességeire és a technikai kompetenciák megfelelő alkalmazására van szükség. A 'soft' kompetenciákkal meghatározható az elkövetők viselkedésprofilja, melyből már kikövetkeztethető az elkövető lehetséges magatartása, célja, motivációja. A 'hard' képességek a számítógépek és hálózatok ismeretét, a mérnöki és informatikai tudást képezik. Mary ügyében a hatóság megfelelően jár el, egyszerre kezdi meg a Maryhez érkező képek és üzenetek forrásának keresését és a lány környezetének kriminalisztikai módszerekkel történő átvizsgálását.

„Lyon felkeresi az E-crime Unitot, hogy lássa, sikerült-e már dekódolniuk Paul telefonját. Bár a Blackberry biztonsági rendszerét még nem sikerült teljesen feltörniük, felfedeztek rajta olyan fotókat, melyek megegyeznek a Marynek küldöttekkel. Lyon levelet küld az Ügyészi Hivatalnak, majd pár héttel később James Keller ügyész informálja őt arról, hogy levél érkezett Paul ügyvédjétől, mely szerint a férfi tagadja az ellene felhozott vádakat. Lyon továbbra is úgy gondolja, hogy Paul telefonját kiberzaklatásra használta. A rendőrfőnök Kellertől azt a tanácsot kapja, hogy nyújtson be egy keresetet a bíróságon, melyben követeli a gyanúsítottól a Blackberry biztonsági jelszavainak megadását."[67]

A vizsgálati eredmények a lány egykori barátjához, Paulhoz vezetnek, így a hatóság lefoglalja a férfi infokommunikációs eszközeit. A felderítés során kiderül, hogy különböző maszkolási módszerek alkalmazásával a szexuális tartalmú képeket Moldovában, a fórumüzeneteket az Egyesült Államokban, az e-maileket Szerbiában, az sms-eket pedig Oroszországban továbbították. Közülük csak az USA volt hajlandó kiadni a szükséges információkat a küldő IP címéről és egyéb ismert adatairól, ez megnehezítette a nyomozó hatóság munkáját. Az államok segítőkészségének hiányát egyrészről a nemzetközi együttműködés

[64] S. D. BROWN op. cit. 59.

[65] Ausztrál Szövetségi Rendőrség.

[66] S. D. BROWN op. cit. 63.

[67] S. D. BROWN op. cit. 83.

keretrendszerének hiánya okozza, másrészt a hatóságra háruló adminisztratív teher. Az időveszteség miatt megsérülhetnek, rosszabb esetben hozzáférhetetlenné válhatnak a bizonyítékok, ami szintén megnehezíti a felderítést. A szerző szerint a moldovai, szerb és orosz példa elkerülése végett nyílt konferenciákat kellene tartaniuk és több informális kapcsolat kiépítésére törekedniük, melyek a transznacionális bűnelkövetés során nagyobb kooperációt teremtenének az egyes szervek, például az Europol vagy az Interpol között.

„Az ügyész bemutatja az esetet a bíróságon, minden addig ismert bizonyítékkal együtt. Úgy véli, nincs más értelmes magyarázat, minthogy Paul követte el a zaklató magatartást Mary ellen. Azt állítja, hogy a vádlott anonim módon követte el a bűncselekményt, hogy elrejtse személyazonosságát és egy olyan, adatok végleges törlését szolgáló szoftvert töltött le a számítógépére, mellyel eltüntethette böngészési előzményeit, melyek bizonyítékul szolgálhattak volna. Továbbá a vádlott késleltette a rendőrség munkáját azzal, hogy minden előzményt kitörölt mobiltelefonjáról, szintén a szóban forgó szoftverrel. A továbbiakban egy információs biztonsági szakértőt kérnek fel arra, hogy ismertesse az eset lehetséges aspektusait. A védelem felteszi a kérdést a szakértőnek, hogy a talált digitális fényképek megegyeznek-e a sértett számítógépén találtakkal. A szakértő ismerteti, hogy a fotók metaadatai egymásnak megfelelőek, így azok a vádlott Blackberry készülékéről származnak. A szakértő elmondja továbbá, hogy Mary személyes adatain és fényképein kívül nem talált egyéb olyan információt, mely összekötné a vádlottat az áldozattal. A védelem ezután egy magán biztonsági cég szakemberét szólítja, aki tanúsítja, hogy eltérőek a Mary telefonján talált fényképek idejére vonatkozó adatok a vádlott számítógépén találtaktól. A szakember elmondja még, hogy a fényképeket egy, a vádlott telefonjánál frissebb szoftvert alkalmazó Blackberryn tárolták, így a készülék nem lehet a vádlotté. A szakértői vizsgálatból az is kiderül, hogy minden rejtett adat megtalálható egy megosztott mappában Paul számítógépén, mely összeköttetésben áll a férfi által letöltött szoftverrel, azonban nem bizonyítható, hogy e mappát a férfi hozta létre. A bíróság ezután a vádlottat szólítja, aki állítása szerint azért hátráltatta a nyomozást, mert nem akarta, hogy kitudódjon katolikus családja előtt még titkolt homoszexualitása. Ezt követően a vádlottat számítástechnikai készségeiről kérdezik, amire azt a választ adja, hogy átlagos felhasználói tudással rendelkezik, építészetet tanult az egyetemen, ott ismerte meg Maryt is, aki mesterképzésben informatikát tanult. Elmondása szerint még számítógépe telepítésében is a lány segédkezett a számára. Paul azt állítja, ő szakított a lánnyal, miután rájött, hogy a férfiak iránt vonzódik, és elmondja a bíróságon, hogy ez a lányt nagyon megviselte, hűtlennek állította be barátját, amiért az felvállalta másságát. A felhozottakra az ügyészségnek több ellenvetése is támadt."[68]

A bizonyítékok begyűjtésében fontos szerepet játszanak az internetszolgáltatók. Ugyanis ők bocsáthatják rendelkezésre az adatáramlással illetve a konkrét tartalommal kapcsolatos információkat. Az információ kinyerése a mobil adathordozók fejlődésével még nehezebb lett. A kereskedelmi és a civil eszközök egyaránt nagy mennyiségű adatot tárolnak különböző e-mail profilokon, a közösségi hálón és egyéb applikációkban, melyekhez a hozzáférés lehetősége egyre korlátozottabb. A 2016-os előrejelzések szerint egy átlagos háztartás 3.3 terabyte adatot tárol majd különböző adathordozókon. Ehhez pedig olyan humánpolitikai és technológiai beruházásokra lesz szükség, melyek többletterhet jelentenek az államnak, magas látenciához vezetnek és csökkentik a nyomozás hatékonyságába vetett társadalmi bizalmatlanságot. A bizonyítási szakaszban problémát jelent még a bizonyítékok és a gyanúsított közötti kapcsolat felderítése. Bár Mary esetében sikerül a számítógépéről és mobiltelefonjáról a bűncselekményhez köthető adatokat letölteni, a nyomozó hatóságok feladata annak bizonyítása, hogy a részben gyermekpornográfiával kapcsolatos tartalmak Paul tudtával és nem a tudta nélkül kerültek technikai eszközeire. Ehhez a közvetlen és közvetett

[68] S. D. BROWN op. cit. 90.

bizonyítékok megfelelő együtthatása szükséges, annak bizonyítására, hogy a vádlott az adott időben és helyen az eszközt használta. Ez a tevékenység a bűnfelderítés hatáskörébe tartozik.
„A bíróság Mary lakcímére elfogatóparancsot ad ki és megbíz egy, a felektől pártatlan szakértőt, hogy egy újabb teljes körű vizsgálatot folytasson le a készülékeken. Erre azért van szükség, mert az E-crime Unit szakértőjének véleményével szemben bizalmatlan. Pár nappal később keresést folytatnak Mary házában. Találnak egy Android vezérlésű másik készüléket, és egy másik Blackberry mobiltelefont is, mely típusában megegyezik a Paultól lefoglalttal. Amikor megkérdezik a lányt a Blackberry hollétéről, Mary szenvtelenül állítja, hogy elvesztette a telefont. A rendőrség talál még jó néhány összezúzott merevlemezt is az alagsorban. A lemezek olyannyira sérültek, hogy nincs esély az adatok helyreállítására. Eközben a készülékeket vizsgáló szakértő azt a megállapítást teszi, hogy minden egyes eszközön frissítve lettek az operációs rendszerek és a firmware programok. Mary Androidján a szoftvert szintén újratelepítették, és egy új beállítás került rá, amely automatikusan törli a telefon böngészési előzményeit. Amikor Lyon rendőrfőnök megkérdezi a lányt, hogy miért állított be a készüléken efféle megsemmisítő tevékenységet, Mary védekezni kezd és visszautasítja a kérdés megválaszolását, személyes tényezőkre hivatkozva. Pault felmentik a vád alól és Mary ügyét a bizonyítékok hiánya miatt ejtik.”[69]
Az eszközök alacsony szoftveres védelme gyengíti a tartalmakra alapozott bizonyító erőt a bíróság előtt, főként mivel az elektronikus bizonyítékokat a szakértők legtöbbször inkább valószínűnek, semmint relevánsnak tartják. A hozzáférés a „chain-of-custody”[70] által bizonyítható, mely egy olyan protokoll, ami biztosítja a kinyert adat útjának követhetőségét és a segíti a hatóság munkavégzésének ellenőrzését. A hatékonyság növelésére Brown több megoldást is ajánl. Szerinte a Számítástechnikai Bűnözésről Szóló Egyezményt szükséges lenne kiterjeszteni az ENSZ tagállamokra, és az egyes nemzetközi együttműködések is összehangolásra szorulnának ahhoz, hogy az adatszolgáltatás és információáramlás előrelendüljön. A szerző a bürokratikus teher csökkentését egy folyamatosan üzemelő kommunikációs háló megvalósításában látja, mellyel azonnal kivizsgálhatók az olyan eszközök, melyeknél a bizonyíték megrongálódhat. Brown szerint hasonlóan jelentős a büntetőeljárás szereplőinek informatikai képzésének támogatása is. Esetükben elsősorban a digitális bizonyíték feldolgozás, az online bűnözés és ezek bírói, rendőri, ügyészi állománnyal való megismertetésére lenne szükség. A büntető-igazságszolgáltatás innovációja még sürgetőbb cél, hiszen egyre több egyedi jellemző nehezíti meg az online környezetben elkövetett jogsértések felderítését. Véleményem szerint Brown a modern kori informatika egyik nagy úttörője. Cybercrime-ról szóló átfogó tanulmányában tökéletesen elemzi a rendszer hiányosságait, univerzális megoldásaival, javaslataival pedig aktualizálni szeretné a bűncselekmények nyomozati fázisát. A tanulmány tanulságaként, számos olyan egyedi jellemző nehezíti az online környezetben elkövetett jogsértések felderítését, mely a büntető-igazságszolgáltatás innovációját igényli. Szükségszerű lenne a büntetőeljárás szereplőinek informatikai képzése is, továbbá a digitális bizonyíték feldolgozás fejlesztése, valamint az online bűnözés és a Darknet[71] sajátosságainak mind a rendőri, mind az ügyészi, bírói állománnyal való megismertetésére is szükség lenne.

Megállapítások
Összefoglalóan megállapítható, hogy az informatikai bűnözés szabályozásának jelenségével foglalkozó tudományos nézetek között két határozott szemlélet azonosítható, az egyik nézet szerint a Büntető Törvénykönyv rendelkezéseinek irányadónak kell lenniük az elektronikus

[69] S. D. BROWN op. cit. 97.
[70] A bizonyíték dokumentálására, begyűjtésére és védelmére irányuló folyamatok összessége.
[71] Azokat az internetes szolgáltatásokat és helyeket nevezik így, amelyeket már kifejezetten illegális célokkal rejtenek el a hagyományos internetről.

úton elkövetett bűncselekményekre is, és ezekkel a konvencionális eszközökkel kell a technológiai változás következtében felmerülő kihívásokat kezelni, míg a másik szemlélet a cybercrime specifikus szabályozását kívánná. Véleményem szerint mindkét felfogás mellett lehet érvelni. A magyar szabályozásra tekintve a Büntető Törvénykönyvről szóló 2012. évi C. törvény a bűnelkövetési tényállások átfogó, kódexjellegű, dogmatikus egészet alkotó rendszerét összesíti, ám nem tarthatjuk távol magunkat az új hazai és nemzetközi jogalkotási megoldásoktól, stratégiáktól sem. Nem tartom szükségszerűen kényszerítőnek a két szemlélet közötti választást, mivel a meglévő számítógépes bűncselekmények folyamatos változása, fejlődése és az új bűntények nagyszámú megjelenése megkívánja mind a stabil háttérszabályozást, mind az új módszerek kutatását, a regulálás új lehetőségeinek megteremtését is. A klasszikus büntetőjogi elveket érvényesítő szabályozás mellett helye lehet az infokommunikációs technológiára tekintettel lévő szabályoknak csakúgy, mint az ön-és társszabályozás szabályainak is. Sőt, a jelenlegi, biztos alapokon álló cybercrime-szabályozás arra szolgáltat bizonyítékot, hogy a két kibékíthetetlennek látszó teória egyes elemeinek összefésülése pozitív eredményekkel jár. Összességében azt tapasztaltam a források elemzése során, hogy a kiberbűncselekmények elbírálására nagyobb hangsúlyt fektet mind a hazai, mind a nemzetközi jogalkotás, mint az azokat megelőző lépések megtételére, valószínűsíthetően abból kifolyólag, hogy az cybercrime elkövetője egy lépéssel mindig a jogi szabályozás előtt jár, a folyton változó technológiai kritériumok végett. A számítógépes bűnözés a számítógép-használat konzekvenciája, bár tudatos szabályozással visszaszorítható, az online élet résztvevőiként mindig az életünk része marad. Kutatásom zárásaként ezért ismételten a prevenció szükségességére hívom fel a figyelmet, annak reményében, hogy ez a következő üzenet megannyi embertársamhoz eljut: elsődlegesen mi, felhasználók tehetünk a saját biztonságunkért, informatikai felkészültségünk megalapozza jelenlétünket az online-térben. Az áldozattá válás a téma iránti fogékonysággal, illetve folyamatos önfejlesztéssel elkerülhető lehet.

Forrásmegjelölés

Parti Katalin - Kiss Anna: A számítógépes bűnözésről akkor és most. Szerkesztők: Bárd Petra – Hack Péter – Holé Katalin. Pusztai László emlékére, 2014. OKRI- ELTE ÁJK, Budapest, 297–310.

Szegediné Lengyel Piroska: Számítógépes bűnözés, avagy fiatalok a cyber-térben. Hadmérnök, V. évfolyam 2. szám, 2010.június.

Deres Petronella: Internetes bűnözés - Cybercrime. Technológiai jog – Új globális technológiák jogi kihívásai. Szerkesztő: Tóth András. KRE ÁJK: Budapest, 2016. 243–250.

Domokos Andrea: Cybercrime. Technológiai jog – Új globális technológiák jogi kihívásai. Szerkesztő: Tóth András. KRE ÁJK: Budapest, 2016. 251–260.

Varga Árpád: Hogyan deríthető fel az internetes zaklatás, melyet moldovai proxy szervereken és orosz email klienseken keresztül követnek el? MTMI Blog. 2016.07.19., http://mtmi.hu/cikk/931/Hogyan_deritheto_fel_az_az_internetes_zaklatas_melyet_moldovai_proxy_szervereken_es_orosz_email_klienseken_keresztul_kovetnek_el [letöltve: 2016.08.10.]

Cameron S. D. Brown: Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology. Szerkesztő: K. Jaishankar, 2015. 9. kötet, 55–119.

Parti Katalin: A számítógépes bűnözés és az internet. Szerkesztő: dr. Irk Ferenc. Kriminológiai tanulmányok 40., OKRI, Budapest, 2003. 179–204.

Dr. Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009.

Kunos Imre: A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. Belügyi szemle. 1999/11. 28–42.

Tóth Tamás: Az Europol tevékenysége – Nemzet és Biztonság 2012/6. szám, 59–78.

Mckenzie Wark: Hackerkiáltvány. Fordította: Nagy Mónika Zsuzsanna. Noran Libro kiadó, 2010.

Szabó Imre: Internetes bűncselekmények, különös tekintettel az internetes csalásra. E-akták. Tanulmányok az internetjog világából. (Studia Collegii De Stephano Bibo Nominati) Szerkesztő: Dr. Kiss Daisy. Bibó István Szakkollégium Internetjogi Kutatócsoport, Budapest, 2003. 301–324.

Kulcs a net világához! A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról. Szerkesztette: Sziklay Júlia, 2013., http://www.naih.hu/files/2013-projektfuzet-internet.pdf [letöltve: 2016.08.20.]

EU Kids Online II. A magyarországi kutatás eredményei – Készült a Nemzeti Média- és Hírközlési Hatóság megrendelésére. Szerkesztő: ITHAKA Nonprofit Kft., 2011. szeptember,

http://nmhh.hu/dokumentum/3886/ITHAKA_EU_KIDS_Magyar_Jelentes_NMHH_Final_12.pdf [letöltve: 2016. 08.20.]

Máté István Zsolt: The Digital Evidence – A digitális bizonyíték., https://www.academia.edu/5105387/A_digit%C3%A1lis_bizony%C3%ADt%C3%A9k_The_Digital_Evidence [letöltve: 2016.10.10.]

Makay József: GDPR- Hatalmas változásra készül a digitális világ, 2016.10.17., https://androbit.net/articles/1055/gdpr_hatalmas_valtozasra_keszul_a_digitalis_vilag.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Androbit+%28Androbit+technol%C3%B3giai+%C3%A9s+tudom%C3%A1nyos+magazin%29[letöltve: 2016.10.20.]

Kis Endre: Kiberéberség adatlopások idején, 2016. 09.21., http://computerworld.hu/computerworld/kibereberseg-adatlopasok-idejen.html [letöltve: 2016.09.25.]

Szathmáry Zoltán: Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban, doktori értekezés. Témavezető: Balogh Zsolt György. Budapest, 2012.

2012/2015. (XII. 29.) Korm. határozat: Az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról.

Nemzeti Fejlesztési Minisztérium: A Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) szerepe a nemzeti kibervédelemben a 2013. évi L. tv. alapján. Előadó: Nagy Zoltán Attila CISM elnök., http://www.kurt.hu/wp-content/uploads/2013/11/NEIH_szerepe.pdf [letöltve: 2016.08.22.]

1744/2013. (X. 17.) Korm. határozata a Nemzeti Bűnmegelőzési Stratégiáról (2013–2023) Magyar Közlöny, 2013. évi 172. szám.

Alábecsült veszélyek? 2016. évi felmérés a globális és magyar gazdasági bűnözésről, Globális Gazdasági Bűnözés felmérés, pwc, 2016., http://www.pwc.com/hu/hu/kiadvanyok/globalis_gazdasagi_bunozes_felmeres/assets/Gazdasagibunozes2016_web.pdf [letöltve: 2016.08.30.]

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016.április 27.)

Marjie T., Britz: Computer Forensics And Cyber Crime: An Introduction(Third Edition), Pearson, 2013.