

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közsolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

A kibertér árnyoldala – a digitális világ kihívásai

Jelige: Támadás határ nélkül

Pályamunka lezárásának időpontja: 2025. január

2025.

TARTALOMJEGYZÉK

Előszó.....	5
I. Fejezet – Egyes kiberbiztonsági szervek és kiberbűncselekmények	7
1. A kiberbiztonság kérdésének aktualitása.....	7
2. Egyes hazai és külföldi szervek	8
2.1. <i>Hazai szervek</i>	8
2.1.1. Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI).....	8
2.1.2. Nemzeti Infokommunikációs Szolgáltató (NISZ).....	9
2.1.3. Nemzeti Kibervédelmi Intézet	9
2.1.4. Hun-CERT.....	10
2.1.5. KIFÜ CSIRT	10
2.2. <i>EU-ban</i>	11
2.2.1. ENISA	11
2.2.2. European Cybercrime Centre	11
2.3. <i>NATO-ban</i>	11
2.3.1. North Atlantic Council (NAC)	11
2.3.2. Military Committee (MC)	12
2.3.3. Cyber Defence Committee (CDC)	12
3. Kiberbűnözés.....	13
3.1. <i>Szervezett bűnözés</i>	13
3.1.1. Bűnszervezet	14
3.1.2. Bűnszövetség.....	15
3.2. <i>Kiberterrorizmus</i>	15
3.3. <i>Zaklatás</i>	16
3.4. <i>Gyermekepornográfia</i>	18
3.5. <i>Állatkínzás az online világ kihívásai közepette</i>	21
3.6. <i>Kábítószer-kereskedelem</i>	24
II. fejezet – A kibertérben elkövetett bűncselekmények nyomozásának kihívásai a büntetőeljárásban.....	25
1. Bevezető gondolatok	25
1.1. <i>Kiberbűncselekmények történetének alakulása hazánkban</i>	25
1.2. <i>Az online bűncselekmények sajátosságai</i>	25
2. Az előkészítő eljárás és a leplezett eszközök alkalmazása.....	26
2.1. <i>Az előkészítő eljárás</i>	26

2.1.1. Általános szabályok.....	26
2.1.2. Az előkészítő eljárás lefolytatására vonatkozó szabályok.....	27
2.2. <i>Leplezett eszközök</i>	29
2.2.1. Fizetési műveletek megfigyelése	30
2.2.2. Álvásárlás	31
2.2.3. Fedett nyomozó	31
2.2.4. Információs rendszer titkos megfigyelése.....	32
3. Az igazságügyi informatikai szakértő	32
3.1. <i>Kirendelése</i>	32
3.2. <i>Általános vizsgálati eljárás</i>	34
3.2.1. Vizsgálati tárgy azonosítása – megkülönböztetés, valamint a felismerés	34
3.2.2. Felmérés és megóvás.....	35
3.2.3. Vizsgálat	35
4. Felderítés	36
4.1. <i>A felderítés általános nehézségei</i>	36
4.2. <i>A törölt vagy módosított adatok helyreállításának a folyamata</i>	38
4.2.1. Adatmódosulás	38
4.2.2. Adattörlés	39
5. Kényszerintézkedések	39
5.1. <i>A kutatás</i>	39
5.2. <i>Az elektronikus adat lefoglalása és a megőrzésre kötelezés</i>	40
5.3. <i>Az elektronikus adat ideiglenes hozzáférhetetlenné tétele</i>	41
6. A bizonyítási eljárás	42
6.1. <i>Általános szabályok</i>	42
6.2. <i>Az elektronikus bizonyítékok beszerzése során felmerülő problémák</i>	43
6.2.1. Fizikai téri bizonyítékok.....	45
6.2.2. Digitális téri bizonyítékok.....	45
6.2.3. Az elektronikus adat és a tárgyi bizonyítékok közötti problematika.....	46
7. Az online elkövetett bűncselekmény esetén rendelkezésre álló bizonyítási eszközök	46
7.1. <i>Tanúvallomás</i>	46
7.1.1. Megfigyelési szakaszban történő torzulás a gyermekkorúaknál	47
7.1.2. Tárolási szakaszban történő torzulás a gyermekkorúaknál	48
7.1.3. Felidézés szakaszban történő torzulás a gyermekkorúaknál	49
7.2. <i>A szakvélemény</i>	50
7.2.1. Bizonyíték, mint alanyi oldal	50
7.2.2. Bizonyíték, mint tárgyi oldal.....	50
7.3. <i>Elektronikus adat</i>	50

8. Gyakorlati kihívások a nemzetközi bűnügyi együttműködésben.....	51
8.1. Gary McKinnon ügy.....	52
8.2. Ivanov és Gorshkov-ügy.....	52
9. Új jogi kihívások – metaverzum	53
10. Összegzés és 'de lege ferenda' javaslatok.....	55
III. Fejezet – A kiberbiztonság és a mesterséges intelligencia	57
1. Bevezetés.....	57
1.1. Az AI előnyei és hátrányai.....	57
1.2. Az AI és a kiberbiztonság kapcsolódása.....	57
2. AI használatával elkövethető egyes negatív megítélésű cselekmények.....	58
2.1. Adathalászat	58
2.2. Deepfake technológiák alkalmazása	59
2.3. Botnetek.....	60
2.4. Összegzés.....	61
3. Az AI használata a pénzügy, valamint a kiberbiztonság területén	61
3.1. Pénzügyi szektor	61
3.2. Kiberbiztonság területe	62
4. A DeepLocker, valamint a rajintelligencia mint kibertámadási modell	63
4.1. DeepLocker	63
4.2. A rajintelligencia	64
5. DDoS-támadások	65
5.1. DDoS meghatározása.....	65
5.2. Nemzetközi rendelkezések.....	66
6. IoT eszközök és az okosotthon.....	68
6.1. Meghatározása	68
6.2. Okosotthon	68
7. Összegzés és 'de lege ferenda' javaslatok.....	69
Felhasznált források.....	70

ELŐSZÓ

„Minden ember két univerzumba születik: a fizikai valóságba és a kibervilágba.”¹ Manapság egyre gyakrabban használjuk és halljuk a kibertér kifejezést. De tudjuk-e pontosan, hogy mit is jelent ez a kifejezés? Szinonimaként használhatjuk-e az online tér, illetve a virtuális tér kifejezésekkel? Összességében a 'virtuális' és a 'kiber' kifejezések a nemzetközi jogban, szakirodalomban elkülönül e két szóhasználat, de lényegileg nem fedezhető fel különbség.² A 'kiber' kifejezést cselekvésnek, navigálásnak fordítják. Ez tehát valamilyen aktív tevékenységet, mozgást feltételez, amelyet térben saját magunk irányítva végezhetünk. A 'virtuális' szó jelentés pedig látszólagos, elképzelt. „[...] a térnek azt a tulajdonságát jelenti, hogy a teret kialakító elemek fizikailag, tehát konkrét földrajzi térben nem megfoghatóak.”³ E két szó alkalmazása során tartalmilag különbség nem érzékelhető, ugyanis mindkettő ugyanarra a dologra vonatkozik, csak a térnek más jellemét ragadja meg. Így ezen kifejtettékre vonatkozóan jelen dolgozatomban szinonimaként használom a 'kiber', a 'virtuális' és az 'online' kifejezéseket.

A kiberbiztonság kifejezés definiálására nincs egyetemes meghatározás. Talán úgy tudnánk meghatározni, hogy „a kiberbiztonság azokra a tevékenységekre utal, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszerek, felhasználók és más személyek védelméhez szükségesek.”⁴

A közösségi médiát, az üzenetküldő szolgáltatásokat és az alkalmazásokat manapság egyre gyakrabban használják kommunikációra, munkára, szocializálódásra vagy információszerzésre. Ezeket a viselkedésbeli változásokat a bűnözők is átvették (ilyen technológiákon alapuló kiberbűncselekmények például a személyazonosság-lopás vagy az adathalászat terjedése), Ezen körülmények között a büntető igazságszolgáltatás szereplői alkalmazkodnak a kommunikációs és információs technológiák fejlődéséhez, követve a bűnözők módszereinek fejlődését.⁵

¹ Marcel DANESI kanadai nyelvész és antropológus

² MÉSZÁROS Rezső: *A kibertér világa*. 49442 tsz. OTKA. Megtekintés: 2024. október 10. <https://docplayer.hu/25087119-A-kiberter-vilaga-zarojelentes-49442-tsz-otka.html> 2

³ Uo.

⁴ EURÓPAI Unió: *Ellenőrzési kompendium. Kiberbiztonság az Európai Unióban és tagállamaiban*. 2020. Megtekintés: 2024. december 12. <https://bit.ly/3DeWP3W> 10

⁵ Chloé BRIÈRE: *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*. European Papers. 2021. Megtekintés: 2024. október 14. <https://bit.ly/4eGJtLG> 494

Az internetnek, és ezáltal az online térnek számos előnye és hátránya is van. Előnyök közé sorolható, hogy megjelentek olyan munkalehetőségek, amelyek otthonról is végezhetőek, megkönnyítheti a tanulást, különböző szórakozási formák jelentek meg, valamint a gyors kapcsolattartás lehetősége és adott számunkra, és még sorolhatnánk. Ezen dolgozatban a negatívumok lesznek hangsúlyban. A negatívumok közé sorolható az adatvédelem problematikája, a függőség, a veszélyeknek vagy vírusoknak való kitettség, valamint ki vagyunk téve olyan tartalomnak is, amelyeket személy szerint nem kívánunk megtekinteni.

I. FEJEZET – EGYES KIBERBIZTONSÁGI SZERVEK ÉS KIBERBŰNCSELEKMÉNYEK

1. A KIBERBIZTONSÁG KÉRDÉSÉNEK AKTUALITÁSA

A kiberbiztonság, kibervédelem kérdése napjainkban talán a legaktuálisabb kérdéskörök egyike. Ezt az aktualitást támasztja alá az elmúlt időszakban történt kiberbűncselekmény esete. 2024. októberében egy zsarolóvírus támadta meg a Védelmi Beszerzési Ügynökséget (a továbbiakban: VBÜ), ahol a „a hekkerek titkosították a magyar katonai és rendvédelmi szervek védelmi és biztonsági beszerzéséért felelős állami cég fájljait, és ötmillió dolláros váltságdíjat kérnek a feloldásukért, különben nyilvánosságra hozzák azokat.”⁶ Ezen támadás mögött egy *'Inc. Ransomware'* elnevezésű hekkercsoport áll, akik többnyire kormányzati és állami szerveket támadnak meg. A hekkercsoport széles körű hozzáférést nyert a VBÜ rendszereihez: „pénzügyi beszámolókat, honvédelmi szervezeti információkat, a honvédelmi és haderőfejlesztési program nem nyilvános aktualitásait, [...], belső ellenőrzésekről szóló dokumentumokat is megszerezték.”⁷

További esetként említeném meg a román elnökválasztás során felmerült kiberbiztonsági, kibervédelmi kérdését. A román alkotmánybíróság azt a döntést hozta, hogy egyhangúan érvényteleníti az elnökválasztásnak a folyamatát. Az első fordulót Georgescu, egyetemi oktató nyerte meg. Magának az érvénytelenítés oka hátterében a romániai hírszerzés véleménye szerint az áll, hogy Oroszország a választásokba beleavatkozott. Ez a mai fiatalok körében a legelterjedtebb alkalmazásnak, a TikTok-nak köszönhető. Több ezer álprofil vált aktívvá az elnökválasztási hetek során, köztük olyanok is, amelyeket 2016-ban regisztráltak, de azokat a fiókokat nem használták – egészen a választásokig. Továbbá influenszereket is fizettek Georgescu nézetei népszerűsítése érdekében. Végül pedig 85 ezer kibertámadást regisztráltak maga a választási rendszerek ellen. Ezen tevékenységek pedig nagyon hasonlítanak Oroszország módszereire, amiket 2022-ben, Ukrajnában alkalmazott.⁸

December 30-án látott napvilágot az a cikk, melyben több százezer személy személyes adatai szivárogtak ki. Az eset még 2024. júliusában történt, és röviden a lényege, hogy a Kütyübazár elnevezésű webáruházról kerültek ki a felhasználók személyes adatai, amelyek a Darkneten

⁶ BOLCSÓ Dániel – DEZSŐ András: *Meghekkelték a katonai és rendőrségi beszerzéseikért felelős állami céget, érzékeny adatok kerültek nyilvánosságra*. Telex. 2024. november 14. Megtekintés: 2024. november 27. <https://bit.ly/4eOsYfC>

⁷ Uo.

⁸ MOLNÁR Zoltán – VIG Emese: *A román alkotmánybíróság ledobta az atomot, példátlan helyzetet hozott az elnökválasztás megismételtetése*. Telex. 2024. december 6. Megtekintés: 2024. december 9. <https://bit.ly/3ZoXZkN>

megvásárolhatóak. A szakértő tippje alapján nagyjából nyolcszázezer magyar felhasználó az érintett.⁹

2. EGYES HAZAI ÉS KÜLFÖLDI SZERVEK

Jelen pont alatt röviden bemutatom az általam legfontosabbnak tartott kiberbiztonsággal foglalkozó egyes hazai, illetve a külföldi szerveket, a felsorolás így nem teljeskörű.

2.1. HAZAI SZERVEK

2.1.1. KÉSZENLÉTI RENDŐRSÉG NEMZETI NYOMOZÓ IRODA (KR NNI)

A rendőrség feladatát az 1994. évi XXXIV. törvény szabályozza. Ezen törvény alapján a Rendőrség feladatai közé tartozik a terrorizmus elleni küzdelem, valamint a bűnmegelőzési, bűnfelderítési célú ellenőrzések, feladatok ellátása. „A rendőrség fellép a kiberbűnözés valamennyi szegmense, így különösen a számítógépes rendszerek elleni támadások, a rosszindulatú számítógépes szoftverek, az adathalászat, az internetes csalások, [...], valamint a gyermekek online szexuális kizsákmányolása ellen.”¹⁰ A kibervédelem, kiberbiztonság körében fontos megemlíteni a Rendőrség ehhez kapcsolódó feladatokat ellátó Osztályait. A Korruptió és Gazdasági Bűnözés Elleni Osztály az Országos Rendőr-főkapitányság Bűnügyi Főosztályán belül működik. Az Osztály feladata elsősorban a korruptió, pénzhamisítás, pénzintézetek sérelmére elkövetett bűncselekmények, csúcstechnológia szakterületeire specializálódik. A kiberbűnözés elleni fellépés kiemelkedően fontos szerepének alapjául 2017-ben megalakult a Készenléti Rendőrség Nemzeti Nyomozó Iroda (a továbbiakban: KR NNI) Kiberbűnözés Elleni Főosztálya, amely Magyarország legnagyobb létszámú, kiberbűnözés elleni küzdelemre szakosodott rendvédelmi egysége. Ezen egység egészen 2007 és 2017 között nagy változásokon kellett, hogy átmenjen, míg főosztállyá alakuljon. „A KR NNI titkos információgyűjtést, titkos adatszerzést és nyomozási feladatokat ellátó, országos illetékességű szervezeti egység.”¹¹ A 25/2013. (VI. 24.) a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló BM rendelet meghatározza azon bűncselekmények körét, amelyek a Készenléti Rendőrség hatásköreibe tartoznak. A kiberbiztonság, kibervédelem szempontjából fontos bűncselekmény a Btk. 375. § (4) bekezdés a) pont szerinti „különösen jelentős kárt okozó információs rendszer felhasználásával elkövetett csalás, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja”¹², továbbá a Btk. 423. § (3) bekezdés

⁹ BOLCSÓ Dániel: *Több százezer magyar felhasználó személyes adatai szivároghattak ki a Kütyübazár oldaláról*. Telex. 2024. december 30. Megtekintés: 2025. január 3. <https://shorturl.at/MbAPv>

¹⁰ KISS Tibor: *Kibervédelem a bűnügyi tudományokban*. Dialóg Campus. Budapest, 2020. 78

¹¹ Uo.

¹² 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről. 2. melléklet, 19.7.

szerinti „közérdekű üzem ellen elkövetett információs rendszer vagy adat megsértése büntette”¹³, valamint a Btk. 424. § szerinti „közérdekű üzem ellen elkövetett információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétsége.”¹⁴ Ebből következően megállapítható, hogy a nyomozói tevékenység az interneten elkövetett bűncselekmények nyomozására, felderítésére, vizsgálatára is kiterjed (példának okáért tiltott online szerencsejáték szervezése vagy a későbbiekben említendő gyermekpornográfia).

2.1.2. NEMZETI INFOKOMMUNIKÁCIÓS SZOLGÁLTATÓ (NISZ)

A hazai állami és önkormányzati szektor kibervédelmét jelentősen befolyásolja az a központosított informatikai és elektronikus hírközlési szolgáltatások létrehozására irányuló folyamat, amelyet az elavult, széttagolt és költségesen fenntartható rendszerek egységesítése érdekében indítottak. A cél egy olyan integrált és biztonságos infokommunikációs rendszer kialakítása, amely magas színvonalú szolgáltatást nyújt az érintett szervezetek számára. A kormány a NISZ Zrt.-t jelölte ki a feladat ellátására, amely működését többek között a 309/2011. (XII. 23.), a 346/2010. (XII. 28.), a 186/2015. (VII. 13.) Korm. rendeletek, valamint egyéb vonatkozó jogszabályok szabályozzák.¹⁵

A NISZ Zrt. kiberbiztonsági feladatai közé tartozik például „az informatikai biztonsági irányítási rendszer kialakítása és működtetése”¹⁶, „kockázatértékelés végzése és ennek megfelelően a szükséges védelmi elemek kialakítása”¹⁷ vagy „a szükséges és megfelelő azonosítási, hozzáférés-kezelési és jogosultságkiosztási feladatok biztosítása.”¹⁸

2.1.3. NEMZETI KIBERVÉDELMI INTÉZET

A Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) 2015. október 1-jén került létrehozásra a Nemzetbiztonsági Szakszolgálat szervezetén belül. Az NKI ellátja „az eseménykezelési feladatokat a létfontosságú rendszerek [...], valamint a [...] 2001.évi CVIII. törvényben meghatározott bejelentés-köteles szolgáltatást – úgymint az online piactér [...] – nyújtó szolgáltatók esetében az eseménykezelési, valamint a hatósági felügyeletet.”¹⁹

Továbbá jogszabályi feladatai közé tartozik a nemzeti kapcsolattartó pont működtetése, melynek feladata az EU-n belüli bekövetkező jelentős kiber-incidensek hazai szintű

¹³ 25/2013. (VI. 24.) BM rendelet i. m. 22.2

¹⁴ 25/2013. (VI. 24.) BM rendelet i. m. 22.3.

¹⁵ KISS i. m. 80

¹⁶ Uo.

¹⁷ Uo.

¹⁸ Uo.

¹⁹ NEMZETI Kibervédelmi Intézet: *Magunkról.* Megtekintés: 2024. december 26.
<https://nki.gov.hu/intezet/tartalom/magunkrol/>

koordinálása, incidensekkel kapcsolatos jelentések fogadása, valamint nemzetközi partnerek részére történő küldése.²⁰

2.1.4. HUN-CERT

A Hun-CERT csoport az Internet Szolgáltatók Tanácsának a támogatásával jött létre és működik mind a mai napig. Ezen csoport a HUN-REN (melyet az Országgyűlés 2019. augusztus 1-én alapított) Számítástechnikai és Automatizálási Kutatóintézetben működik.

A csoport elsődleges feladata a hálózati incidensek felderítésénél, megelőzésénél, elemzésénél történő támogatás nyújtása. További feladatai körébe tartozik a biztonságos tudatosság növelés, valamint együttműködik hazai és nemzetközi szervezetekkel.²¹

Fő tevékenységei a következők:

- „Incidensek felderítése és elemzése
- Incidensek kezelése
- Biztonsági és kommunikációs gyakorlatok lebonyolítása
- Biztonsági tudatosság növelése”²²

2.1.5. KIFÜ CSIRT

„Az Innovációs és Technológiai Minisztérium irányítása alatt működő Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) az a Kormányzati Informatikai Fejlesztési Ügynökségről szóló [...] kormányrendeletben meghatározottak alapján végzi tevékenységét.”²³

Két fő tevékenységét különböztethetjük meg, melyek közül a második bír számunkra relevanciával. Ezen tevékenység a „hazai közoktatási, felsőoktatási, kutatási intézmények, közgyűjtemények számára informatikai infrastruktúra fejlesztése és üzemeltetése, valamint arra épülő szolgáltatások nyújtása.”²⁴ Ezen a tevékenységen belül lett létrehozva egy Információs Technológiai incidens-kezelő csoport, a CSIRT. „A KIFÜ CSIRT alapfeladata minden olyan kiberbiztonsági incidens kezelését és koordinációját segíteni, amelyben legalább egy KIFÜ által kiszolgált intézmény érintett.”²⁵

²⁰ Uo.

²¹ HUN-CERT csoport. <https://cert.hu/rolunk/huncert-csoport> Megtekintés: 2024. december 2.

²² Uo.

²³ Kiss i. m. 82

²⁴ Uo.

²⁵ Uo.

2.2. EU-BAN

2.2.1. ENISA

Az ENISA, azaz az Európai Hálózat- és Információbiztonsági Ügynökség az Európai Unió kiberpolitikájához hozzájárul. Az uniós országokkal és intézményekkel együttműködve támogatja, segíti őket abban, hogy felkészüljenek a jövő kiberbiztonsági kihívásaira.²⁶ „Egyik legfontosabb feladata ezen a területen az ismeretek és a bevált gyakorlatok terjesztése, valamint az információcsere biztosítása”²⁷

Az ENISA székhelyes Görögországban, Iráklionban található. Ezzel összefüggésben szervez kiberbiztonsági gyakorlatokat, továbbá a nemzeti kiberbiztonsági stratégiáknak a fejlesztéshez is hozzájárul. További tevékenységi körébe tartozik, hogy tanulmányokat készít (például számítógépes fenyegetések aktuális helyzetéről, e-igazolványokról, bizalmi szolgáltatásokról), építi a CSIRT-ek együttműködését.²⁸

2.2.2. EUROPEAN CYBERCRIME CENTRE

A Számítástechnikai Bűnözés Elleni Európai Központ 2013-ban kezdte meg működését. Annak érdekében jött létre, hogy „megerősítse az EU-ban a számítógépes bűnözésre adott bűnüldözési válaszokat, és ezáltal segítse az európai polgárokat, [...] az online bűnözés elleni védelemben.”²⁹

Feladata, hogy támogassa az EU tagállamait és intézményeit a kibertérben elkövetett bűncselekmények nyomozásához szükséges operatív és elemzői kapacitások fejlesztésében, valamint együttműködjön nemzetközi partnerekkel az európai kiberbűnözés felszámolásában. Tevékenységei közé tartozik a rosszindulatú szoftverek, rendszerfeltörések, adathalászat, jogosulatlan hozzáférések, manipulációk, személyazonosság-lopások, fizetőeszközökkel kapcsolatos csalások, valamint a gyermekek online csábítása és szexuális kizsákmányolása elleni küzdelem is.³⁰

2.3. NATO-BAN

2.3.1. NORTH ATLANTIC COUNCIL (NAC)

A NAC, vagyis az Észak-atlanti Tanács a NATO szervének az egyik legfontosabb politikai döntéshozó testülete. Felügyeli az egész Szövetséget érintő biztonsági kérdésekkel kapcsolatos politikai és katonai folyamatokat. Összehozza az egyes tagországok képviselőit, hogy

²⁶ EURÓPAI UNIÓ: *Európai Unió Kiberbiztonsági Ügynökség (ENISA)*. Megtekintés: 2024. december 12. <https://bit.ly/3VD1in8>

²⁷ KISS. i. m. 83

²⁸ Uo.

²⁹ KISS. i. m. 85

³⁰ KISS i. m. 86

megvitassák a kollektív döntéseket igénylő politikai vagy operatív kérdéseket. Az Észak-atlanti Tanács testülete legalább hetente – szükség esetén bármikor, különböző szinteken – ülésezik. A NATO valamennyi tagországának képviselői helyet kapnak a NAC-ban.³¹

2.3.2. MILITARY COMMITTEE (MC)

A Katonai Bizottság a NATO legfelső katonai testülete. Elnökét szokás a NATO „első katonájának” nevezni, bár ő nem tölt be hadszíntéri parancsnoki pozíciót. A bizottság az Észak-atlanti Tanács és a Védelmi Tervező Bizottság irányítása alatt működik. Tagjai a NATO-tagállamok vezérkari főnökei vagy az általuk kijelölt nemzeti katonai képviselők.³²

A Katonai Bizottság feladata a politikai döntések és útmutatások katonai irányvonalba ültetése, valamint a NATO-térség védelméhez szükségesnek ítélt intézkedések ajánlása és a katonai műveletekre vonatkozó döntések végrehajtása, továbbá stratégiai politikát és koncepciókat dolgoz ki, valamint éves hosszú távú értékelést készít a NATO érdekeit veszélyeztető országok és területek erejéről és képességeiről.³³

2.3.3. CYBER DEFENCE COMMITTEE (CDC)

A Szövetség biztonságát érintő kiberveszélyek összetettek, romboló hatásúak és kényszerítő jellegűek, ráadásul egyre gyakoribbá válnak. A kibertér folyamatosan vitatott terület, és minden nap történnek rosszindulatú kibertámadások, a kisebb szintű támadásoktól egészen a technológiailag kifinomult támadásokig. A NATO és szövetségesei erős és ellenálló kibervédelemre támaszkodnak a Szövetség három alapvető feladatának - az elrettentés és védelem, a válságmegelőzés és -kezelés, valamint az együttműködésen alapuló biztonság - teljesítése érdekében. A Szövetségnek fel kell készülnie arra, hogy megvédje hálózatait és műveleteit az egyre kifinomultabb kiberfenyegetésekkel szemben.³⁴

A NATO átfogó kibervédelmi politikáját a NATO politikai, katonai és műszaki hatóságai, valamint az egyes szövetségesek hajtják végre. Az Észak-atlanti Tanácsnak alárendelt Kibervédelmi Bizottság a politikai irányítás és a kibervédelmi politika vezető bizottsága. A NATO katonai hatóságai és a NATO Kommunikációs és Információs Ügynöksége konkrét felelősséggel tartozik a NATO kibervédelmi képességeinek operatív követelményeinek meghatározásáért, beszerzéséért, végrehajtásáért és működtetéséért.³⁵

³¹ NATO: *North Atlantic Council (NAC)*. Megtekintés: 2024. december 12. https://www.nato.int/cps/cy/natohq/topics_49763.htm

³² BLAHÓ András – PRANDLER Árpád: *Nemzetközi szervezetek és intézmények*. Akadémiai Kiadó. 2016. 256

³³ NATO: *Military Committee*. Megtekintés: 2024. december 12. https://www.nato.int/cps/ua/natohq/topics_49633.htm

³⁴ NATO: *Cyber defence*. Megtekintés: 2024. december 12. https://www.nato.int/cps/en/natohq/topics_78170.htm

³⁵ Uo.

3. KIBERBŰNÖZÉS

Egyre növekvő tendenciát mutat a számítógépes bűnözés az olyan államokban, mint például az Európai Unió tagállamok, hiszen az internet-struktúra fejlett, továbbá az online módon történő fizetési rendszer is elérhető.³⁶

3.1. SZERVEZETT BŰNÖZÉS

„Az internet vonzó környezetté vált a különböző profit-orientált bűnelkövetők számára, különösen mert [...] nincs szükség arra, hogy jelen legyenek fizikailag a bűncselekmények elkövetésének a helyszínén [...]”³⁷ A fejlődő technikát kihasználó elkövetéseket kettő csoportra lehetne osztani. Az első csoportba azon büntetendő magatartások tartoznak, amelyek már a korábbi időben is léteztek, de „a kapcsolattartási és más lehetőségek a korábbiaknál jobban elősegítik azok terjedését, így akár nagyságrendileg is növelve társadalmi veszélyességüket.”³⁸ Ide lehet sorolni elsősorban a szervezett bűnözésnek a hagyományos üzletágait, mint például a kábítószer-kereskedelem, emberkereskedelem. A másik csoportba azon kriminális megnyilvánulások tartoznak, amelyek a technika fejlődése nélkül nem léteznének. Ilyen például a mások rendszerébe való behatolás különböző célok érdekében.³⁹

Az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény (2006. évi CI. törvény) meghatározza a szervezett bűnözői csoport fogalmát. Így szervezett bűnözői csoport „bizonyos ideig fennálló, három vagy több főből álló strukturált csoport, amely összehangoltan működik egy vagy több, a jelen Egyezményben meghatározott súlyos bűncselekmény elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve.”⁴⁰ A további fogalmi elemeket is meghatározza az Egyezmény. Súlyos bűncselekményként minősíti a legalább négy év szabadságvesztéssel vagy ennél súlyosabb büntetéssel büntetendő bűncselekményt megvalósító magatartást. A strukturált csoport az nem egyetlen bűncselekmény azonnali végrehajtására, és nem alkalomszerűen létrehozott csoport. Azonban a strukturált csoportban nem szükséges, hogy a tagjai pontosan meghatározott szerepekkel rendelkezzenek, vagy hogy a tagság az állandó legyen, illetve fejlett hierarchiával rendelkezzen.

³⁶ EUROPOL: *Cybercrime*. Megtekintés: 2024. október 29. <https://www.europol.europa.eu/crime-areas/cybercrime>

³⁷ Mezei Kitti: *A szervezett bűnözés az interneten*. A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar; MTA Társadalomtudományi Kutatóközpont. Budapest – Pécs. 2019. [07_buntetojog_informatika_MEZEIK.pdf](#) 125

³⁸ BORBÍRÓ Andrea – INZELT Éva – KEREZSI Klára – LÉVAY Miklós – PODOLETZ Léna: *A büntető hatalom korlátainak megtartása: a büntetés mint végső eszköz*. Elte Eötvös Kiadó. Budapest. 2014. 290

³⁹ BORBÍRÓ – INZELT – KEREZSI – LÉVAY – PODOLETZ i. m. 291

⁴⁰ 2006. évi CI. törvény az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről. 2. cikk (a) bekezdés. Megtekintés: 2024. november 27.

Vagyonnak minősíti az Egyezmény a bármilyen típusú vagyontárgyat, amely lehet anyagi vagy szellemi, ingó vagy ingatlan, tárgyi vagy eszmei, valamint az ilyen vagyontárgyak tulajdonjogát igazoló, vagy abban lévő érdekeltséget bizonyító jogi dokumentum vagy okirat.⁴¹

3.1.1. BŰNSZERVEZET

A 2012-es Büntető törvénykönyv (a továbbiakban: Btk.) is az Egyezményben meghatározott definíciót vette át, és meghatározza a bűnszervezet és a bűnszövetség fogalmát is, melyeket a 459.§ (1) bekezdésben határozza meg.

Így bűnszervezet a „legalább három személyből álló, hosszabb időre, hierarchikusan szervezett, konspiratíván működő csoport, amelynek célja ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekmények elkövetése.”⁴² A bűnszervezet alanyi oldali ismérvei között kell említeni, hogy legalább 3 főből kell állnia a szervezetnek (részesi magatartás lehetséges, de az elkövetési alakzatot egyértelműen meg kell tudni jelölni), azonban, ha az egyik személy nem büntethető (például gyermekkor miatt), a másik kettő személyre akkor is bűnszervezetben történő elkövetést meg kell állapítani. A szándékuknak legalább kettő szándékos bűncselekmény elkövetésére kell kiterjednie, amely öt vagy az ötét meghaladó szabadságvesztéssel büntetendő cselekmény. Az elkövetőknek nem kell tisztában lenniük azzal a ténnyel, hogy a Btk. hány év szabadságvesztéssel bünteti, hanem csak azzal kell tisztába lenniük, hogy az adott bűncselekmény súlyos bűncselekmény. Tárgyi oldali ismérvek körében említendő a szervezett elkövetés. A szervezett elkövetés jellemzője az, hogy az elkövetők a szerepeket elosztják, a lehetőségeket keresik, feltérképezik. A bűnözésnek hosszabb időre kell létrejönnie, továbbá hierarchikus jelleggel kell működnie. A hierarchikus jelleg azt jelenti, hogy legalább egy irányítói és legalább egy irányított szintnek kell lennie. Tehát két szint esetében is megállapítható a bűnszervezet, de általában több irányított szint a jellemző. Nem utolsó sorban említendő a konspiratív jelleg. A konspiratív jelentése titkosan szervezkedő, titokban megszervezett támadás.

A bűnszervezetben történő elkövetés esetén a Btk. nem sorolja fel a bűncselekménytípusokat, kizárólag annyit jelenít meg, hogy ötévi vagy ötét meghaladó szabadságvesztéssel büntetendő cselekmény esetében állapítható meg. Erre vonatkozóan felmerülhet a kérdés, hogy miként alkalmazhatóak a jogi szabályok azokra a bűnszervezetben történő elkövetésekre, amelyek az internet lehetőségeit kihasználva követik el illegális tevékenységüket, például az online piacokon keresztül folytatott kábítószer-kereskedelemre

⁴¹ 2006. évi CI. törvény i. m. 2. cikk (b) – (d) bekezdés. Megtekintés: 2024. november 27.

⁴² BTK. 459§ (1) 1.

vagy gyermekpornográf tartalmak terjesztésére.⁴³ Mezei Kitti álláspontjával egyetértve magam is azon az állásponton vagyok, hogy amennyiben a törvényi feltételek teljesülnek, és az elkövető tudata átfogja a bűnszervezetben történő cselekvést, akkor meg kell állapítani a bűnszervezetben történő elkövetést, feltéve természetesen, ha ötévi vagy ötévet meghaladó szabadságvesztéssel büntetendő bűncselekményről van szó.

3.1.2. BŰNSZÖVETSÉG

A bűnszövetség „akkor létesül, ha két vagy több személy bűncselekményeket szervezetten követ el, vagy ebben megállapodik, és legalább egy bűncselekmény elkövetését megkísérlik, de nem jön létre bűnszervezet”⁴⁴ A bűnszövetségben történő elkövetés megállapításához legalább két személy szükséges. Amennyiben az egyik elkövető nem büntethető (például gyermekkor miatt), a többi személyre akkor is a bűnszövetségben történő elkövetést kell megállapítani. Részesi magatartás ezen esetkörben is lehetséges, és ebben az esetben is meg kell tudni jelölni az elkövetési alakzatot. Tárgyi oldalon két dolognak kell teljesülnie. Az egyik feltétel, hogy két vagy több bűncselekményt ténylegesen végrehajtott legyen, vagy két vagy több bűncselekmény végrehajtásában előzetesen megállapodnak. Ekkor viszont fontos, hogy az egyik bűncselekményt legalább kísérleti szakaszba kell juttatni. A másik feltétel a szervezett elkövetés. A szervezett elkövetés jellemzői a bűnszervezetben történő elkövetés esetén leírtakkal megegyezik.

3.2. KIBERTERRORIZMUS

A kiberterrorizmus fogalmát úgy tudnánk röviden meghatározni, hogy a kibertérben elkövetett terrortámadások. A kiber szó jelentésére vonatkozó definícióra a korábban meghatározottak az irányadók. „A terrorizmus a latin *terrere* (megrémít) szóból ered, amelyet a francia -isme toldalékkal ellátva megkapjuk a *terrorisme*-et. Ez már a „rémületet okozni” jelentéssel bír.”⁴⁵ Azonban egységesen elfogadott fogalommeghatározás egyik szó esetében sem beszélhetünk. Magával a terrorizmussal 14 ENSZ egyezmény, valamint további 4 kiegészítő jegyzőkönyv is foglalkozik, azonban egyikben sem találhatunk egységes fogalommeghatározást. Ehelyett ezen dokumentumokban elkövetési mód fogalmakat határoznak meg. Ennek következtében ma már körülbelül ötven különböző elkövetési módot határoznak meg és rendelnek üldözendővé.⁴⁶

⁴³ MEZEI i. m. 129

⁴⁴ BTK. 459§ (1) 2.

⁴⁵ DORNFELD László: *Kiberterrorizmus – A jövő terrorizmusa?* A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi – MTA Társadalomtudományi Kutatóközpont. Budapest – Pécs. 2019. Megtekintés: 2024. december 04. [A_bunugyi_tudomanyok_es_az_informatika.pdf](#) 47

⁴⁶ DORNFELD i. m. 48

Kérdésként merülhet fel, hogy a kiberterrorizmus és a kiberbűnözés mennyire határolható el egymástól, a kiberterrorizmust a kiberbűnözés részeként lehet-e értelmezni. A legnagyobb különbség e kettő cselekmény között az elkövetők motivációjukban van. „Míg a bűnözők elsősorban vagyoni vagy más előny eléréseért, esetleg szórakozásból követnek el bűncselekményeket a kibertérben, addig a kiberterrorizmus mögött valamilyen politikai, vallási indíttatású cél húzódik meg.”⁴⁷ Különbségként említendő továbbá, hogy a terrorizmust elkövető személyek célpontjaikat szélesebb körben határozzák meg. A célban rejlő fő különbség pedig az „hogy a terroristák a megkülönböztetés nélküli fizikai károkozást kívánják elérni, míg a bűnözők esetén ez nem kifejezetten cél.”⁴⁸

A probléma viszont a kifejtettekkel az, hogy ezen éles elhatárolás a gyakorlatban szinte lehetetlen, ugyanis az eszközök, továbbá a cél homályossága miatt hatásköri viták keletkeznének.⁴⁹ Ugyanis egy bűnszervezetben történő elkövetés esetén a cél az ötévi vagy azt meghaladó szabadságvesztéssel büntethető bűncselekmény elkövetése, míg a terrorizmus, terrorista csoport elkövetésének célja például állam elleni, nemzetközi szervezet kényszerítése, alkotmányos rend erőszakos megváltoztatása, vagy e célok eléréseért más meghatározott bűncselekmények elkövetése céljából történő elkövetés.⁵⁰

Így a kifejtettek alapján Dornfeld Lászlóval egyetértek, miszerint a megkülönböztetés csak elméleti jellegű, továbbá az éles határvonal meghúzása nem lenne előnyös.

3.3. ZAKLATÁS

Az internet anonimitása gyakran felbátorítja az elkövetőket, így az internetes zaklatás széles körben elterjedt és kihívást jelentő problémává válik.⁵¹ A zaklatásnak sokféle arca van: a lányokat és fiatal nőket lelkileg lehúzzák a véleményük miatt, erőszakkal fenyegetik őket, nem kívánt pornográf képeket küldenek nekik.⁵² Sajnos kijelenthető, hogy az online zaklatás globális probléma.⁵³ Az Alkotmánybíróság a 8/1990 (IV.23.) és az 56/1994 (XI. 10.) AB határozataiban részletezte, hogy a „magánszférához való jogot” az Alkotmány konkrét,

⁴⁷ DORNFELD i. m. 51

⁴⁸ Uo.

⁴⁹ DORNFELD i. m. 52

⁵⁰ PAPP Zoltán István: *A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái*. Nemzeti Közszerológati Egyetem. Katonai Műszaki Doktori Iskola. 2018. Megtekintés: 2024. december 23 <https://bit.ly/4iStlZN> 60

⁵¹ Alexis GIRON: *Cyberbullying Laws: How Different Countries Address Online Harassment*. Megtekintés: 2024. október 14. <https://www.lawobrien.com/cyberbullying-laws-how-different-countries-address-online-harassment/>

⁵² Serap ALTINISIK: *Online harassment is silencing girls: EU and Member States can do more*. 2020. november 25. <https://plan-international.org/eu/blog/2020/11/25/online-harassment/>

⁵³ Sarita SCHOENEBECK – Amna BATOOL – Giang DO – Sylvia DARLING – Gabriel GRILL – Daricia WILKINSON – Mehtab KHAN - Kentaro TOYAMA: *Online Harassment in Majority Contexts: Examining Harms and Remedies across Countries*. University of Michigan. 2023. Megtekintés: 2024. október 14. <https://ar5iv.labs.arxiv.org/html/2301.11715>

szubjektív alapjogként nem nevezi meg, de a magánélet szabadságához való jog kétségkívül az egyén autonómiájának védelmére szolgáló olyan alapjog, amely az ember veleszületett méltóságából ered, amelynek tehát az általános személyiségi jog — az emberi méltósághoz való jog — szubszidiárius alapjoga. Tehát az úgynevezett általános személyiségi jogot anyajognak tekinti az Alkotmánybíróság. Ennek az alapjognak a megsértése, támadása eredményezi a zaklatás megvalósulását.

„Online zaklatást szenved el az a személy, aki többször is bántó, sértő, megalázó üzeneteket kap az interneten keresztül. A kiskorú felhasználóknak címzett szexuális tartalmú üzenet [...] is online zaklatás.”⁵⁴

A Btk. 222. § (1) bekezdésében megfogalmazott zaklatást az valósítja meg, aki rendszeresen vagy tartósan háborgat. Kutatásom során a legtöbb szerző a rendszeres vagy tartós háborgatást a bűncselekmény elkövetési magatartásának tekintette. Ambrus István rámutatott arra, hogy az elkövetési magatartás az valóban a háborgatás, viszont a rendszeres vagy tartós elkövetés az elkövetés módjaként értékelhető. Hiszen maga a *'háborgat'* ige is feltételez egy gyakoriságot, mert egy gyakorító képzővel van ellátva. Továbbá ezt az álláspontot a Kúria is elismerte, mégpedig, hogy „A háborgatás nyelvtanilag is bizonyos gyakoriságot, azaz többszörösséget feltételez. A törvény ezt kifejezetten nyomatékosítja a tényállásban, arra való utalással, hogy nem egyszeri, nem egymozzanatú, hanem folyamatos magatartásról van szó.”⁵⁵ A korábbi Legfelsőbb Bíróság pedig úgy fogalmazott, hogy „[...] Aki háborgat, az mást a nyugalmában zavarja meg a rendszeres vagy tartós, tolakodó, zaklató kapcsolatteremtő magatartásával.”⁵⁶ Ambrus István elemzését követve én sem tartom szerencsésnek, hogy a bírói gyakorlat, továbbá a szakirodalom összemossa a bűncselekmény elkövetési magatartását és elkövetési módját. Az, hogy a rendszeresség, tartósság és háborgatás egyazon törvényi tényállás tárgyi oldalán együtt jelenik meg, nyelvtani szempontból túlzott hangsúlyozásnak minősülhet. Ez a megközelítés a büntető törvénykönyvben nem biztos, hogy a legszerencsésebb megoldás, mivel a fogalmak ilyen módon történő párhuzamos használata szükségtelenül nyomatékosítja a cselekmények tárgyi oldalát. Ezért indokolt lehet ezen elemek együttes szerepeltetését a törvényi meghatározásokban fontolóra venni.⁵⁷

A rendszeresség kérdése is vitatott a legtöbb szerző esetében az előzőekben felvázolt problémakör miatt. A legtöbb szerző a rendszeres elkövetést egyszerűen többszöri

⁵⁴ NMHH: *Mi számít online zaklatásnak?* Megtekintés: 2024. október 12. https://nmhh.hu/cikk/190113/Mi_szamit_online_zaklatasnak

⁵⁵ BH 2014.6.169: Kúria Bfv. III. 802/2013. határozata zaklatás vétsége tárgyában

⁵⁶ BH 2011.11.302: Legf. Bír. Bfv. III. 818/2010. határozata zaklatás vétsége tárgyában

⁵⁷ AMBRUS István: *Digitalizáció és büntetőjog*. Wolters Kluwer Hungary Kft. Budapest, 2021. 117

elkövetésnek, rövid időközönkénti elkövetésnek definiálják. Ambrus István véleménye szerint a rendszeresség olyan tényállási ismérv, amely „előre nem meghatározható, de nagyobb számú, az alkalmosság kizáró, hosszabb időintervallumon belül, időről időre – akár nagyobb időközökkel is megszakítottan – visszatérő elkövetés.”⁵⁸ Ezen definícióból pedig következik, hogy a ’rendszeres háborgatás’ szókapcsolat kevésbé lehet tényállásszerű egyszerű ismétlődés. A második definíció helytállását bizonyítja az, hogy a Szegedi Ítéltábla a vádlottat zaklatás vétsége miatt emelt vád alól felmentette. A vádlott 2011. május 15-én 9 óra 47 perckor hívta fel a sértettet, ez alkalommal a feleségével beszélt. 2011. június 9-én 18 óra 34 perckor a sértett szüleit hívta fel, majd ugyanezen a napon 18 óra 35 perckor, és 19 óra 12 perckor beszélt telefonon a sértettel. A 18 óra 39 perckor kezdeményezett hívást a sértett nem fogadta. Ez összesen öt telefonhívás, melyből egy a sértett szüleit érintette. A Szegedi Ítéltábla a Fővárosi Ítéltábla rámutatására is hivatkozott, amely alapján „az értelmező kézi szótárak a rendszeresség fogalma alatt napi ismétlődést, más helyen meghatározott időközönként folyamatosan, vagy nagy számban, sok alkalommal”⁵⁹ történő elkövetést kell érteni. Ezeket figyelembevéve állapította meg a szegedi Ítéltábla, hogy „[...] ez a vádlotti magatartás nem tekinthető napi ismétlődésűnek, folyamatosnak, vagy nagy számúnak. A rendszeres háborgatás ezért nem állapítható meg a vádlott terhére.”⁶⁰

Ezen okfejtések következtében, mivel a rendszeres elkövetési módot nem lehetséges egzakt módon meghatározni, és így veszélyezteti a jogbiztonságot, ezért javasolható lenne a ’rendszeres’ kifejezés ’ismétlődő’ kifejezésre történő cserélése.

3.4. GYERMEKPORNOGRÁFIA

Első körben tisztázom azt, hogy mi számít gyermekpornográf tartalomnak. „Olyan felvételek tekinthetők gyermekpornográfoknak, amelyek gyermekeket ábrázolnak meztelenül vagy félmeztelenül, szexuális helyzetben azért, hogy felkeltsék másban a nemi vágyat.”⁶¹ Ahogy a Nemzeti Média- és Hírközlési Hatóság megfogalmazza, különösen az olyan felvétel minősül gyerekpornográf tartalomnak, amely „a nemiséget súlyosan szeméremszéttő módon ábrázolja [...] és abban kiskorút – akár aktív, akár passzív szereplőként – felhasználva, vagy amelyen kiskorú nemi szerve látszik.”⁶² Továbbá az Országgyűlés a 2021. évi LXXIX törvény elfogadásával a pedofil bűnelkövetőkkel szemben szigorúbb fellépést biztosít és ezzel

⁵⁸ Uo.

⁵⁹ ÍH 2010.97: Fővárosi Ítéltábla 3. Bhari. 158/2009/7. határozata zaklatás vétsége tárgyában.

⁶⁰ A Szegedi Ítéltábla Bf.505/2014/5. számú határozata terrorcselekménnyel fenyegetés büntette tárgyában.

⁶¹ NMHH: *Mi számít gyermekpornográf tartalomnak?* Megtekintés: 2024. október 12. https://nmhh.hu/cikk/190114/Mi_szamit_gyermekpornograf_tartalomnak

⁶² Uo.

egyidejűleg a 204. § (8) bekezdésében meghatározza a pornográf felvételt erre a szakaszra vonatkozóan. Tehát e szakasz alkalmazásában „pornográf felvétel: a másnak vagy másoknak a nemiséget súlyosan szeméremszéttörő nyíltsággal, célzatosan a nemi vágy felkeltésére irányuló módon történő ábrázolása, ideértve a nem létező személy vagy személyek valóságghű ábrázolását is.”⁶³

A gyermekpornográfiát nagyon sokan az internet megjelenéséhez kötik, azonban ki kell jelenteni, hogy ezen bűncselekmény nem az internet megjelenésekor jelent meg, ugyanis már a Csemegi-kódex 248. §-a is deklarálta a bűncselekményt. Ez a bűncselekmény a szemérem elleni vétség volt. Ekkoriban az követte el a szemérem elleni vétséget, aki „fajtalanságot tartalmazó iratot, nyomtatványt vagy képes ábrázolatot nyilvános helyen kiállított, árult vagy terjesztett.”⁶⁴

A hatályos törvényszöveg alapján a gyermekpornográfia passzív alanya kizárólag a 18. életévét be nem töltött személy lehet. Gyurkó Szilvia tett egy olyan javaslatot, melyben kifejtette, hogy dekriminalizálni kellene ezen törvényszöveg egyik esetét, nevezetesen a 204. § (5) bekezdés a) pontja szerinti tartást. Érvelésében arra helyezte a hangsúlyt, hogy egy teljesen jogszerűen két gimnazista (példájában két 17 éves kamasz) szexuális kapcsolatban van és vágykeltő, szexuális tartalmú képeket küldenek egymásnak saját magukról. Továbbá kifejtette, hogy ebből az esetből „egyértelműen látszik, hogy nem ez volt a jogalkotó szándéka, a gyermekpornográfia tényállását a szexuális predátorok ellen találták ki, nem az egymással csetelő tinikre.”⁶⁵ Ezen dekriminalizációval én sem értek egyet. Ugyanis akkor lenne egy legális útja annak, hogy a 14-18 év közötti fiatalkorúról készülhessen gyermekpornográf tartalmú fénykép. Ha a dekriminalizáció bekövetkezne, akkor megjelennének a felnőttek által legálisan nem használható, birtokolható képek az online térben, amelyek elkészítése viszont legális volt. Ezeket figyelembevéve Ambrus Istvánnal egyet tudok érteni, miszerint a dekriminalizáció szükségtelen, látható veszélyeket hordozna maga után, azonban ha a célszerűen értelmezés használatával, a konkrét esetben összehatásban megvizsgálva arra a következtetésre kerül a sor, hogy a cselekményt elkövető személy társadalomra veszélytelen, akkor büntetőjogi felelősségre vonásra ne kerüljön sor⁶⁶, tekintettel arra, hogy hiányzik a büntetőjogi felelősség megállapításának egyik alapvető eleme, nevezetesen a társadalomra veszélyesség.

A gyermekeket ábrázoló pornográf felvételeken gyakran nehéz az életkor, a felvétel készítésének helye és ideje pontos meghatározhatósága. Sok esetben ezek a felvételek gyenge

⁶³ BTK. 204. § (8)

⁶⁴ AMBRUS i. m. 103

⁶⁵ AMBRUS i. m. 104

⁶⁶ AMBRUS i. m. 106

minőségűek, eltorzítottak vagy akár hamisítványok is lehetnek, ami megnehezíti az áldozatok azonosítását, a jogi eljárásokat és a bűncselekmény bizonyítását.⁶⁷ Tehát a szakértő számára komoly feladatot jelent, hogy a rendelkezésre álló képi információk alapján bizonyítsa a gyermekpornográf anyagok jelenlétét. További nyomozási problémát okoz, hogy az elkövetők titkos, zárt közösséget alkotnak, sajátos nyelvezetet használnak, valamint ennél a bűncselekménynél jellemző a nemzetközi jelleg, tehát a határok nélkülsége.⁶⁸ A nemzetközi dokumentumok kifejezték a gyermekpornográfia elleni fellépés szükségességét és meghatározták ennek kereteit, azonban a szuverén jogrendszerek eltérő szabályozása akadályozza az egységes bűnüldözést és a nemzetközi együttműködést, valamint a büntetőeljárás sikerességét. Ezen körülmények miatt tisztázatlan például, hogy mi számít védett jogtárgynak; milyen ábrázolások lehetnek a bűncselekmény elkövetési tárgyai. További gondot jelent a passzív alany életkorának meghatározása, ugyanis az nem egységes a különböző országokban.⁶⁹

Sajnos ki kell jelenteni, hogy reális tendencia mutatkozik a gyermekpornográfia tovább terjedésére. Ennek oka lehet különösen, hogy üzletszerűvé válik a pornográfia egyes válfaja vagy növekszik az on-line dating, amikor közvetlenül lehet a bemutatott gyermekkel szexuális kapcsolatot létesíteni.⁷⁰

A gyermekpornográfia a nemzetközi és európai uniós dokumentumok szerint a gyermekek szexuális kizsákmányolásának egyik formája, amely olyan módozatokban jelenik meg, mint a prostitúció, az emberkereskedelem vagy a családon belüli bántalmazás.⁷¹ A büntetőeljárás során különböző problémák merülhetnek fel (a nyomozó hatóság szakmai és technikai felkészültsége, a szolgáltatók által végzett adatrögzítés és adatátadás, az elkövetés helyének meghatározása, az igazságügyi szakértő feladatainak ellátása, valamint a külföldi nyomozó hatóságok és internet-szolgáltatók együttműködése).⁷² „A legtöbb, felderítést, bizonyítást nehezítő tényező a nyomozást végző szerv technikai és személyi felkészültségéből eredt.”⁷³ A későbbiekben szó lesz az igazságügyi szakértőkről, előljáróban csak annyit jegyeznek meg ezzel kapcsolatban, hogy az igazságügyi szakértő kirendelése vitatott kérdés. Ugyanis a korábbi években különböző

⁶⁷ NAGY Zoltán András: *Bűncselekmények a számítógépes környezetben*. Ad Librum. Budapest, 2009. 205

⁶⁸ GYARAKI Réka Eszter: *A számítógépes bűnözés nyomozásának problémái*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar. Pécs, 2018. Megtekintés: 2024. október 13. <https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf> 178

⁶⁹ PARTI Katalin: *Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar. 2008 <https://bit.ly/4fdle7E> 268

⁷⁰ NAGY i. m. 206

⁷¹ PARTI i. m. 100

⁷² PARTI i. m. 187

⁷³ PARTI i. m. 189

problémák is felmerültek a szakértő kirendeléssel, például nem szakkérdésben kérték fel, hanem jogi kérdéseket tettek fel számára. Ezzel az a gond, hogy a jogkérdés eldöntése nem a szakértő feladata. Valamint olyan probléma is jelentkezett, hogy olyan kérdéseket tettek fel, amelyek abszolút nem relevánsak a bizonyítás szempontjából.⁷⁴

3.5. ÁLLATKÍNZÁS AZ ONLINE VILÁG KIHÍVÁSAI KÖZEPETTE

A kiinduló hipotézis az, hogy a kortárs állatjognak globálisnak vagy határokon átnyúlónak és többszintűnek kell lennie ahhoz, hogy hatékony legyen. A globalizáció idején az ember és az állat közötti interakciók minden aspektusa határokon átnyúló dimenzióval rendelkezik. Az állatjólét globális problémává vált, ami globális szabályozást igényel.⁷⁵ Sajnos azt kell mondani, hogy az állatkínzás bűncselekménye az elmúlt években nem mutat csökkenő tendenciát, sőt nap mint nap lehet az online térben olvasni az ehhez a bűncselekményhez kapcsoló híreket, és vannak olyanok is, akik ezt megörökítik videófelvétel formájában. Ezért gondoltam ezt a bűncselekményt is elemezni jelen dolgozatomban. „[...] a közösségi média használatának a mindennapi életünkben mára módfelett kiterjedt jelenléte számos bűncselekmény kapcsán a közhangulat megváltoztatása irányában is hatott [...]”⁷⁶ Jól mutatja, hogy pár évtizeddel korábban maga még az képezte a vita tárgyát, hogy az állatkínzás egyáltalán bűncselekménynek számít-e, addig a ma is hatályos Btk. egyértelműen bűncselekményként nyilvánítja a súlyosabban büntetendő deliktumok körében. Az elmúlt évek talán egyik legfelkavaróbb esete Fülöp, a nagycserkeszi németjuhász keverék. Gazdái az állat nyaka köré szorosan zsinórt tekertek, melynek következtében a feje felismerhetetlenségig eltorzult az ödémás megbetegedés következtében.⁷⁷ A beteg állatot egy mezőőr fedezte fel, majd ő értesítette az állatvédőket. Hiába került jó kezekbe, gondos ápolás alá Fülöp, pár hónap elteltével elpusztult. Az ügyész letöltendő börtönbüntetést, a védők pedig közérdekű munkát kértek. A Nyíregyházi Járásbíróság négy-négy hónap fogházbüntetésre ítélte a kutya gazdáit. Indokolása az volt, hogy a vádlottak büntetlen előéletűek, továbbá két kiskorú gyermekről is gondoskodnak. A tárgyalás napján az állatvédők ez alkalommal is békés tüntetéssel és "Börtönt az állatkínzóknak!" feliratú molinókkal mutatták ki az épület előtt, hogy elítélik az állatok bántalmazását, és szükségesnek tartják az állatkínzással kapcsolatos büntetések szigorítását.⁷⁸ Az állatkínzást mára már a legtöbb ember elítéli, és ezt az interneten is kifejti, ha ilyen esetben

⁷⁴ Uo.

⁷⁵ Anne PETERS: *Global Animal Law: What It Is and Why We Need It*. Cambridge University Press. 2016. március 10.

⁷⁶ AMBRUS i. m. 257

⁷⁷ AMBRUS i. m. 258

⁷⁸ KOVÁCS Tünde: *Fülöp kutya megkínzói letöltendő fogházbüntetést kaptak*. 2017. november 29. <https://www.nyirport.hu/2017/11/fulop-kutya-megkinzoi-letoltendo-foghazbuntetest-kaptak-13356>

ütközik. Továbbá szintén megfigyelhető, hogy „[...] a kirívóan durva állatkínzásos esetekben rendre az elkövető(k) azonnali kézre kerítését, továbbá [...] letöltendő szabadságvesztésben megnyilvánuló megbüntetését követelik, szintén az interneten.”⁷⁹ Tehát az interneten, közösségi médiában történő véleménynyilvánításnak nagy hatása van arra, hogy a társadalmi felfogást átalakítsa.

Az Alkotmánybíróság 8/2017. (IV. 18.) AB határozatában részletesen foglalkozott az állatvédelemmel. Részletesen taglalja, hogy a '*ne bis in idem*' elvét sérti az az eset, ha az elkövetőt az állatkínzás büntettének elkövetése miatt – amely ugyanazon állatkínzásban megjelenő cselekménye – állatvédelmi bírsággal sújtanak (állatvédelmi hatósági eljárás keretében), illetve az állatkínzás büntetőjogi felelősség megállapítása eredményeként szankciót szabnak ki. Azonban helyes szabályozási módnak gondolnám, ha a büntetőjogi és a közigazgatási szankcióval (jelen esetünkben állatvédelmi bírsággal) fenyegetett cselekmény esetén lehetőség legyen a '*ne bis in idem*' elvének a kiküszöbölése. Ezen véleményen volt az említett AB határozatban Dr. Czine Ágnes, Dr. Salamon László, valami Dr. Szabó Marcel alkotmánybírók. Dr. Czine Ágnes különvéleményében kifejtette, hogy a kétszeres eljárás alkotmányos tilalma nem akadályozza meg, hogy a büntetőeljárás jogerős lezárását követően azonos tényállás alapján közigazgatási eljárásban a közigazgatási hatóság olyan szankciót alkalmazzon, amelynek nincs büntető jellege, hanem inkább preventív célú [például az állattartástól való eltiltás kiszabható (az Átv. 43. § (9)-(10) bekezdései alapján)]. Az állatvédelmi bírság viszont nem preventív, hanem büntető jellegű szankció, amelyet a közigazgatási szervek alkalmaznak. Ezért a büntetőeljárás során hozott felelősség megállapítás vagy felmentés után, ha ugyanazon személy ellen és ugyanazon tényállás alapján a hatóság ismét büntető jellegű szankciót (bírságot) szabna ki, az ütközik a '*ne bis in idem*' elvével. Dr. Szabó Marcel különvéleményében arra mutatott rá, hogy míg a büntetőjog ultima ratio jelleggel próbálja érvényre juttatni az ember-állat együttélés alapvető szabályait, és a jogsértésre a társadalom erkölcsi felfogását tükrözve, a vétkesség és a büntetés hangsúlyozásával reagál, addig a közigazgatási jog az állattartásra vonatkozó tevékenységeket szélesebb körben szabályozza. Emiatt olyan elemeket is magában foglal, amelyek a büntetőjogi eszközrendszerbe nem illeszthetők be. Mivel a két szabályozás célja csak részben azonos, funkciói és szankciórendszerei jelentősen eltérnek, ezért a kapcsolódási pontok ellenére nem fedik le egymást teljesen.⁸⁰ További javaslatom egy külön fejezet szentelése az

⁷⁹ AMBRUS i. m. 259

⁸⁰ 8/2017. (IV. 18.) AB határozat az állatok védelméről és kíméletéről szóló 1998. évi XXVIII. törvény 43. § (1) és (4) bekezdésének alkalmazásával kapcsolatos alkotmányos követelmény megállapításáról

állatvédelemnek, melyben az eredmény súlyosságától függően egyre szigorúbb szankciók lennének hozzárendelve. Továbbá a jelenlegi szabályozás általános jelleggel a zoofiliát – tehát az állatok iránt érzett nemi vonzalmat – nem bünteti a Btk., azonban indokolt lenne egy *'sui generis'* tényállást alkotni.⁸¹ Ha nemzetközileg kitekintünk, más országokban azonban szabályozott a zoofília kérdése. A francia büntető törvénykönyv 521. § (1) bekezdése deklarálja, hogy a házasított, szelídített vagy fogságban tartott állat szexuális zaklatása három évig terjedő szabadságvesztéssel és 45 000 eurós pénzbírsággal büntetendő. Minősített esetként értékeli a francia büntető törvénykönyv ugyanezen szakasza, ha a bűncselekményt csoportosan, kiskorú jelenlétében vagy az állat tulajdonosa vagy tartója követi el és ekkor a büntetések négy év szabadságvesztésre és 60 000 eurós pénzbírságra emelkednek.⁸² Számos ország az erről a cselekményről készült pornográf felvételek terjesztését is büntetni rendeli (példának okáért a német törvénykönyv 184a. §, a svéd büntetőtörvény 10. fejezet 10c. §, norvég büntetőtörvény 317. §).⁸³

Ha a nyomozást nehezítő tényezőkről kellene szólni, mindenképpen meg kell említeni az időmúlást. Ugyanis minél később jut a hatóságok tudomására a károsítás, vagy a pusztulás ténye, annál kevesebb a valószínűsége az eredményes és biztos szakértői vizsgálatnak. Ugyancsak nem segíti a nyomozást, hogy ezen vizsgálatok magas költséggel rendelkeznek, ami megterhelést okoz a nyomozó hatóságok számára, vagy hogy ezen bűncselekmény esetén sokszor tanúhiányról is szó lehet. További nehezítő tényező a kapacitáshiány, ugyanis a leterheltség miatt sokszor a határidőt meg kell hosszabbítani, ezzel a szakvélemény akár hónapokat is késleltethet. Végül pedig a hatósági állatorvosi vizsgálatok megfelelő dokumentálása is hátráltathatja az eredményes nyomozást.⁸⁴ „Az állatkínzás-gyanús helyzetek megítéléséhez a bűncselekmény helyszíneléséhez egységes protokoll és módszertani útmutató kidolgozására lenne szükség.”⁸⁵ Szintén elengedhetetlen a lakosság széles körű, érthető tájékoztatása arról, hogy mely cselekmények minősülnek állatkínzásnak és ezekhez milyen törvényi szankciók kapcsolódnak. Továbbá a kellő elrettentés érdekében fontos, hogy a büntetőjogi felelősségre vonás nagyobb hangsúlyt kapjon a médiában.⁸⁶

⁸¹ AMBRUS i. m. 287

⁸² CODE PÉNAL: Titre II: Autres dispositions. Article 521-1-1

⁸³ AMBRUS i. m. 276

⁸⁴ TILKI Katalin: *Az állatkínzás nyomozását nehezítő és segítő tényezők*. Ügyészek Lapja. Megtekintés: 2024. október 27. <https://ugyeszeklapja.hu/?cat=31>

⁸⁵ Uo.

⁸⁶ Uo.

3.6. KÁBÍTÓSZER-KERESKEDELEM

A kábítószer-kereskedelem az egyik, ha nem a legnagyobb illegális piaca az online térben megjelenő bűncselekményeknek. A kábítószer-kereskedelem bűncselekménye legtöbb esetben szervezett bűnözői csoportokban jelenik meg a különböző online felületeken. Ezen ponton szükségesnek tartom megemlíteni a Darknetet. A Darknet az internetnek az egyik titkosított hálózata, melyhez csak egy böngésző telepítése után – a Tor böngésző – férhetünk hozzá, így az anonimitást lehetővé teszi. Magát a hálózatot legális célokra is használhatják, de sokunkban a Darknet hallatán a feketepiacra összpontosítunk. Nem véletlen, hiszen a Darknet oldalán számtalan illegális tevékenység működik (például fegyverkereskedelem vagy az egyéb kábítószerrel kapcsolatos bűncselekmények).

2017-ben, az Europol által kiadott statisztikák alapján a kábítószer-kereskedelem a legelterjedtebb illegális tevékenység a Darkneten. Ezen statisztika alapján az első nyolc Darknet piactérnek 10,6 millió és 18,7 millió euró bevétele származott csupán a kábítószer-kereskedelemből.⁸⁷

A Btk. 176. §-a alapján kábítószer-kereskedelmet követ el, aki kábítószerrel kínál, átad, forgalomba hoz, vagy azzal kereskedik. A kínálás az sikertelen átadás, hiszen, ha a megkínált személy a kábítószerrel átveszi, már egy másik elkövetési magatartás, nevezetesen az átadás valósul meg. Az átadás tehát akkor valósul meg, ha a megkínált személy a kábítószerrel átveszi. A forgalomba hozatal az, amikor az elkövető több személynek juttat kábítószerrel. A kereskedelem pedig egy rendszeresen ismétlődő cselekvést jelent, amely anyagi haszonszerzésre irányul. Az alapeset büntetendősége kettőtől nyolc évig terjedő szabadságvesztés.

A kábítószer-kereskedelem mellett még számos tiltott szerrel összefüggő cselekményt rendel büntetni a Btk. Így büntetni rendeli a kábítószer birtoklását (Btk. 178. § - 180. §), a káros szenvedélykeltést (Btk. 181. §), a kábítószer készítésének elősegítését (Btk. 182. §), a kábítószer-prekurzorral visszaélést (Btk. 183. §), az új pszichoaktív anyaggal visszaélést (184. § - 184/D. §), a teljesítménycsökkentő szerrel visszaélést (Btk. 185. §), valamint a gyógyszerhamisítást (Btk. 185/A. §).

⁸⁷ EUROPOL: *Drugs and the Darknet. Perspectives for enforcement, research and policy*. 2017. Megtekintés: 2024. december 29. <https://shorturl.at/fngUF51>

II. FEJEZET – A KIBERTÉRBEN ELKÖVETETT BŰNCSELEKMÉNYEK NYOMOZÁSÁNAK KIHÍVÁSAI A BÜNTETŐELJÁRÁSBAN

1. BEVEZETŐ GONDOLATOK

1.1. KIBERBŰNCSELEKMÉNYEK TÖRTÉNETÉNEK ALAKULÁSA HAZÁNKBAN

Magyarországon az online bűncselekmények az 1990-es évek hajnalán jelentek meg, és ahogy a számítógépek egyre gyorsabb ütemben terjedtek el és fejlődtek, a bűncselekmények száma is ezzel párhuzamosan növekedett. A legelső tényállások a szerzői joghoz kapcsolódtak. A korábbi „büntető törvénykönyvet módosító 1993. évi XVII. törvény iktatta be a szerzői és szomszédos jogok megsértése tényállást”⁸⁸, amelyet a ma hatályos 2012-es Btk. szerzői vagy szerzői joghoz kapcsolódó jogok megsértése elnevezéssel illet. Külön számítástechnikára vonatkozó bűncselekmény 2004 májusában jelent meg. Ez a tényállás a számítógépes csalás volt. Ez a törvényi tényállás az 1994. évi IX. a büntető jogszabályok módosításáról szóló törvény hatálybalépését követően jelent meg. Új bűncselekmény jelent meg a korábbi Btk-ban 1997-ben, melyet a kiskorúak védelme érdekében deklarált a jogalkotó. A bűncselekmény megnevezése a tiltott pornográf felvételek készítése, mely bűncselekmény „a kiskorúakról készített pornográf felvételek készítőjével, forgalmazóival szemben lép fel.”⁸⁹ 2000. márciusi hatállyal az 1999. évi CXX. törvény 6. § (2) a „[...] nagy nyilvánosság fogalmát kiterjeszti a bűncselekmény elektronikusan rögzített információ távközlő hálózaton való közzététele útján történő elkövetésre is.”⁹⁰ Ezen ponttól mondhatjuk azt, hogy az internet végleg részese lett a büntetőjognak. Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezmény aláírására ezt követően került sor. 2002. áprilisi hatállyal pedig kialakultak a ma is létező számítástechnikai bűncselekmények törvényi tényállásai.⁹¹

1.2. AZ ONLINE BŰNCSELEKMÉNYEK SAJÁTOSSÁGAI

A jelen korban kiemelkedik azon bűncselekmények felderítési nehézségei a bűnüldöző szerveknél, amelyeket az online térben követnek el. Ez a probléma – tehát a felderítési nehézségek – sajnos a büntetőeljárás jelentős lassításában vagy sikeres befejezésében is megjelenik. „A kiberbűncselekmények különböző kategóriáinak felderítési nehézségei azonosak, legyen szó akár egy egyszerűbb, [...] akár egy szofisztikált módon kivitelezett kibertámadást érintő eljárásról.”⁹² Ezen nehézségek legtöbbször a technikai újdonságokhoz,

⁸⁸ CHRISTIÁN László: *Az információs társadalom jogi vetületei. Alkalmazott jogi informatika*. Pázmány Press. Budapest, 2013. 108

⁸⁹ CHRISTIÁN i. m. 109

⁹⁰ Uo.

⁹¹ Uo.

⁹² HERÉDI István: *A kiberbűncselekmények felderítési nehézségei*. Belügyi szemle. 2022/1. szám 47

online identitást elfedő szolgáltatások használatához kapcsolódik. Az ilyen jelleggel elkövetett bűncselekményeknek csupán elenyésző számban jut a hatóságok tudomására. Azonban a hatóságok számára a bűncselekmények elkövetőinek felderítése gyakran összetett és kihívásokkal teli feladat. Az elkövetőkre vonatkozó lényeges információk megszerzése nemcsak alapos nemzetközi együttműködést igényel, hanem a nyomozás folyamata is időigényes lehet.⁹³

A nemzetközi szakirodalom általánosságban a kiberbűncselekmények esetén a következő két elhatárolást használja: az egyik csoportba azon bűncselekmények tartoznak, amelyeket kizárólag a kibertérben követhetők el, azok az esetek, amelyek egy információs rendszert közvetlenül érintenek – tehát a bűncselekmény csak ezeken a rendszereken valósulhat meg. Ilyen cselekmény lehet például a rosszindulatú kódsorok alkalmazása. A másik csoportba tartoznak azok a bűncselekmények, amelyeket az informatikai rendszer vagy kibertér felhasználásával követnek el, többek között ilyen az online csalás vagy a zsarolás.⁹⁴

2. AZ ELŐKÉSZÍTŐ ELJÁRÁS ÉS A LEPLEZETT ESZKÖZÖK ALKALMAZÁSA

A következő pontokban részletesen kitérek az előkészítő eljárás és a leplezett eszközök alkalmazásának feltételeire.

2.1. AZ ELŐKÉSZÍTŐ ELJÁRÁS

2.1.1. ÁLTALÁNOS SZABÁLYOK

Ezen jogintézmény egy új intézménynek minősül, hiszen eddig egyetlen egy korábbi büntetőeljárás törvény sem tartalmazott ehhez hasonló rendelkezéseket. A Büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) kilencedik része szól az előkészítő eljárás szabályairól. Ez az előkészítő eljárás egy úgynevezett „opcionális eljárás”, ugyanis csak abban az esetben lesz elrendelve, ha a törvényben meghatározott feltételek fennállnak. Előkészítő eljárás elrendelése esetén arra keresik a választ a nyomozó hatóság tagjai, hogy egyáltalán a bűncselekmény elkövetésének a gyanúja fennáll-e. Úgy is fogalmazhatunk, hogy a „gyanú gyanúját keresik”. Kronológiai sorrendet nézve tehát az előkészítő eljárás a nyomozási szakaszt megelőzi. Az előkészítő eljárás abból a célból folytatható le, ha „a rendelkezésre álló adatok a bűncselekmény gyanújának megállapítására nem elegendőek és megalapozottan feltehető, hogy az előkészítő eljárás lefolytatása alapján el lehet dönteni, hogy a bűncselekmény gyanúja fennáll-e.”⁹⁵

⁹³ HERÉDI i. m. 49

⁹⁴ Katarzyna CHALUBIŃSKA-JENTKIEWICZ – Filip RADONIEWICZ – Tadeusz ZIELIŃSKI: *Cybersecurity in Poland*. Springer. 2022. <https://link.springer.com/content/pdf/10.1007/978-3-030-78551-2.pdf> 39

⁹⁵ BE. 340. § (2)

Az előkészítő eljárás lefolytatására a nyomozó hatóság vagy ezzel a hatáskörrel rendelkező ügyészség jogosult. A rendőrségről szóló 1994. évi XXXIV. törvény alapján szintén jogosult az előkészítő eljárás lefolytatására a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust ellátó szerve.⁹⁶ Ezen eljárás során alkalmazhatóak a törvényben meghatározott kényszerintézkedések, ezeket a törvény 341. §-ban taxatívén felsorolja (például bírói engedélyhez kötött leplezett eszköz, rejtett figyelés, 221. § a) pontja szerinti álvásárlás). Azonban „csak abban az esetben kerülhet sor leplezett eszközök alkalmazására, így előkészítő eljárásra (a kettő feltételezi egymást), ha a bűncselekmény gyanújának megállapítására nyílt eszközök alkalmazásával nem kerülhet sor.”⁹⁷ Szintén hosszasan, taxatívén felsorolva találhatjuk meg azon lehetőségeket, amelyek alapján az előkészítő eljárás alatt adatszolgáltatás kérhető – ilyen lehetőség például a vámhatóság, a szabálysértési nyilvántartási rendszer vagy esetleg a körözési nyilvántartási rendszer.

2.1.2. AZ ELŐKÉSZÍTŐ ELJÁRÁS LEFOLYTATÁSÁRA VONATKOZÓ SZABÁLYOK

Főszabály szerint hat hónap áll rendelkezésre az előkészítő eljárás lefolytatására, azonban a bírói engedélyhez kötött leplezett eszközök alkalmazásakor, ha a büntetendő szándékos cselekmény öt évig vagy ennél súlyosabb szabadságvesztéssel büntetendő, akkor ez a határidő kilenc hónapra módosul. Ha a gyanúval fenyegető cselekmény három évig terjedő szabadságvesztéssel büntetendő, akkor is elrendelhető a leplezett eszközök alkalmazása azokban az esetekben (ezen esetköröket a Be. 234. § (2) bekezdésében taxatívén felsorolja), ha az például üzletszerűen vagy bűnszövetségben elkövetett cselekmény, szexuális visszaélés, kerítés, prostitúció elősegítése, kitarthatóság, gyermekprostitúció kihasználása, gyermekpornográfia bűncselekménye. A gyermekeket ábrázoló pornográf felvételeken gyakran nehéz az életkor, a felvétel készítésének helye és ideje pontos meghatározhatósága. Sok esetben ezek a felvételek gyenge minőségűek, eltorzítottak vagy akár hamisítványok is lehetnek, ami megnehezíti az áldozatok azonosítását, a jogi eljárásokat és a bűncselekmény bizonyítását.⁹⁸ Tehát a szakértő számára komoly feladatot jelent, hogy a rendelkezésre álló képi információk alapján bizonyítsa a gyermekpornográf anyagok jelenlétét. További nyomozási problémát okoz, hogy az elkövetők titkos, zárt közösséget alkotnak, sajátos nyelvezetet használnak, valamint ennél a bűncselekménynél jellemző a nemzetközi jelleg, tehát a határok nélkülsége.⁹⁹ A nemzetközi dokumentumok kifejezték a gyermekpornográfia elleni fellépés szükségességét és

⁹⁶ BE. 339. § (3)

⁹⁷ FARKAS Ákos – RÓTH Erika: *A büntetőeljárás (negyedik, átdolgozott kiadás)*. Wolters Kluwer Kft. 2019. 321

⁹⁸ NAGY Zoltán András: *Bűncselekmények a számítógépes környezetben*. Ad Librum. Budapest, 2009. 205

⁹⁹ GYARAKI i. m. 178

meghatározták ennek kereteit, azonban a szuverén jogrendszerek eltérő szabályozása akadályozza az egységes bűnüldözést és a nemzetközi együttműködést, valamint a büntetőeljárás sikerességét. Ezen körülmények miatt tisztázatlan például, hogy mi számít védett jogtárgynak; milyen ábrázolások lehetnek a bűncselekmény elkövetési tárgyai. További gondot jelent a passzív alany életkorának meghatározása, ugyanis az nem egységes a különböző országokban.¹⁰⁰ Sajnos ki kell jelenteni, hogy reális tendencia mutatkozik a gyerekpornográfia tovább terjedésére. Ennek oka lehet különösen, hogy üzletszerűvé válik a pornográfia egyes válfaja vagy növekszik az on-line dating, amikor közvetlenül lehet a bemutatott gyermekkel szexuális kapcsolatot létesíteni.¹⁰¹ A gyermekpornográfia a nemzetközi és európai uniós dokumentumok szerint a gyermekek szexuális kizsákmányolásának egyik formája, amely olyan módozatokban jelenik meg, mint a prostitúció, az emberkereskedelem vagy a családon belüli bántalmazás.¹⁰² A büntetőeljárás során különböző problémák merülhetnek fel (a nyomozó hatóság szakmai és technikai felkészültsége, a szolgáltatók által végzett adatrögzítés és adatátadás, az elkövetés helyének meghatározása, az igazságügyi szakértő feladatainak ellátása, valamint a külföldi nyomozó hatóságok és internet-szolgáltatók együttműködése).¹⁰³ „A legtöbb, felderítést, bizonyítást nehezítő tényező a nyomozást végző szerv technikai és személyi felkészültségéből eredt.”¹⁰⁴

Abban az esetben, ha nem az ügyészség végzi az előkészítő eljárást, akkor az eljáró hatóság kettő havonta be kell számolnia az ügyészségnek az addig beszerzett adatokról, illetve kérésre az ügyiratok bemutatásáról. Viszont, ha az eljárást az ügyészség folytatja le, akkor

- „az ügyészség bármely nyomozó hatóságot annak illetékességi területén eljárási cselekmény elvégzésére utasíthatja, illetve a nyomozó hatóság tagja a legfőbb ügyész kezdeményezésére a nyomozó hatóság országos parancsnoka egyetértésével az előkészítő eljárás során határozott időtartamra igénybe vehető,
- felkérésére az eljárási cselekmény elvégzésében közreműködik
 - a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, illetve
 - a rendőrségről szóló törvény szerint hatáskörébe tartozó bűncselekmény miatt folytatott eljárásban a rendőrség terrorizmust elhárító szerve.”¹⁰⁵

¹⁰⁰ PARTI i. m. 268

¹⁰¹ NAGY i. m. 206

¹⁰² PARTI i. m. 100

¹⁰³ PARTI i. m. 187

¹⁰⁴ PARTI i. m. 189

¹⁰⁵ BE. 347. § (3)

Meg kell szüntetni az előkészítő eljárást azokban az esetekben, ha a rendelkezésre álló idő letelt (tehát a hat – egyéb esetekben kilenc – hónap jogvesztő határidőt jelent), az előkészítő eljárás alatt bizonyos lett, hogy a bűncselekmény gyanúja nem áll fenn, illetve, ha eredmény az előkészítő eljárástól nem várható. Amennyiben megszüntetésre kerül az eljárás, akkor az eljárásban beszerzett adatok a büntetőeljárásban nem használható fel bizonyítékként.

Ha a bűncselekmény elkövetésének gyanúja beigazolódik, akkor nyomozást kell elrendelni. A nyomozás elrendelésével az előkészítő eljárás befejeződik. Ezen esetben viszont az előkészítő eljárásban szerzett adatokat haladéktalanul át kell adni az ügyészségnek vagy a nyomozó hatóságnak.¹⁰⁶

2.2. LEPLEZETT ESZKÖZÖK

A leplezett eszközök alkalmazhatóságát több törvény, illetve rendelet is szabályozza – például az 2017. évi XC. törvény a büntetőeljárásról, a 100/2018. (VI. 8.) Korm. rendelet, az 1994. évi XXXIV. törvény a Rendőrségről. A leplezett eszközök az információs, technikai rendszerek titkos megfigyelését jelenti, így kifejezetten fontos szerepe van az online, digitális térben elkövetett bűncselekmények kapcsán.

„A leplezett eszközök alkalmazása olyan, a magánlakás sérthetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő alapvető jogok korlátozásával járó, a büntetőeljárásban végzett különleges tevékenység, amelyet az erre feljogosított szervek az érintett tudta nélkül végeznek.”¹⁰⁷

A leplezett eszközök akkor alkalmazhatóak, amennyiben

- „megalapozottan feltehető, hogy a megszerezni kívánt információ, illetve bizonyíték a büntetőeljárás céljának eléréséhez elengedhetetlenül szükséges és más módon nem szerezhető meg,
- annak alkalmazása nem jár az azzal érintett vagy más személy alapvető jogának az elérendő bűnüldözési célhoz képest aránytalan korlátozásával, és
- annak alkalmazásával bűncselekménnyel összefüggő információ, illetve bizonyíték megszerzése valószínűsíthető.”¹⁰⁸

Ezen alkalmazhatósági feltételekből jól kiolvasható az alkotmányjogban is ismert alapjogi korlátozási feltételek. Az Alaptörvény I. cikke mondja ki ezen feltételeket, tehát „alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges

¹⁰⁶ BE. 345. § (1)

¹⁰⁷ BE. 214. § (1)

¹⁰⁸ BE. 214. (5)

tartalmának tiszteletben tartásával korlátozható.”¹⁰⁹ Tehát a három elv, amit tiszteletben kell tartani és amelynek megsértése esetén jogellenes tevékenység lesz a leplezett eszközök alkalmazása, az a szükségesség, az arányosság és a célszerűség elve.

A leplezett eszközök engedélyük alapján lehetnek szerven belüli engedélyhez kötöttek, ügyészi engedélyhez kötöttek, valamit bírói engedélyhez kötöttek. A következőkben azon leplezett eszközöket fejtem ki, amelyek egy online térben elkövetett bűncselekmény esetén relevánsak lehetnek.

2.2.1. FIZETÉSI MŰVELETEK MEGFIGYELÉSE

A fizetési műveletek megfigyelése egy ügyészi engedélyhez kötött leplezett eszköz. Az ügyészség engedélyével a leplezett eszközöket alkalmazására feljogosított szerv elrendelheti, hogy a pénzügyi szolgáltatást végző szervezet egy meghatározott időszakban rögzítse, megőrizze, és továbbítsa az elrendelőnek a fizetési műveletekkel kapcsolatos adatokat. Különösen ilyen fizetési műveletek megfigyelésének tekinthető a pénzforgalmi törvény „szerinti fizetési számlával kapcsolatos valamennyi fizetési művelet; meghatározott feltételeknek megfelelő fizetési műveletekre vonatkozó adatok rögzítése, illetve továbbítása.”¹¹⁰

A fizetési műveletek megfigyelésének főszabályi határideje három hónap, amely egyszer az ügyészség engedélyével három hónappal meghosszabbítható. Annak érdekében, hogy a nyomozás sikerrel záródjon, a szolgáltatónak kötelessége mindezt a megfigyelést titokban tartania, senkinek sem adhat tájékoztatást. Abban az esetben, ha a fizetési műveletek megfigyelésével érintett személy kéri a saját adatainak kezeléséről szóló tájékoztatást, olyan választ kell adnia szolgáltatónak, melyből nem derül ki, hogy az adatai a megfigyelés céljából lettek továbbítva. Ismét a megfigyelés sikeressége érdekében erről a szolgáltatót minden esetben tájékoztatni szükséges.¹¹¹

„A fizetési műveletek megfigyelése esetén a (kiegészítő) pénzügyi szolgáltatási tevékenységet végző szervezet az érintett adatokat köteles tárolni és köteles azokat az ügyésznek megküldeni.”¹¹²

¹⁰⁹ ALAPTÖRVÉNY I. cikk (3)

¹¹⁰ FARKAS – RÓTH i m. 296

¹¹¹ BE. 216. § - 218. §

¹¹² NAGY Klára: *A titkos információgyűjtés az új büntetőeljárási törvénytervezet tükrében*. Belügyi Szemle. 2017/4. 61

2.2.2. ÁLVÁSÁRLÁS

Az álvásárlás szintén egy ügyészi engedéllyel alkalmazható leplezett eszköz. Az álvásárlásról a Be. 221. §-a szól. Mint az elnevezésből is kiderül, az álvásárlás egy színlelt megállapodás. Ez a színlelt megállapodás abban az esetben köthető, illetve teljesíthető, amennyiben az

- „a bűncselekménnyel feltehetően összefüggésbe hozható dolog vagy annak mintája megszerzésére vagy szolgáltatás igénybevételére,
- az eladó bizalmának erősítése céljából a bűncselekményre vonatkozó tárgyi bizonyítási eszközt eredményező dolog megszerzésére vagy szolgáltatás igénybevételére,
- a bűncselekmény elkövetőjének elfogása, illetve tárgyi bizonyítási eszköz biztosítása érdekében dolog megszerzésére vagy szolgáltatás igénybevételére irányul.”¹¹³

2.2.3. FEDETT NYOMOZÓ

A fedett nyomozó alkalmazása egy ügyészi engedélyhez kötött leplezett eszköz. A fedett nyomozó alkalmazásának ideje legfeljebb hat hónap lehet, azonban, ha a fedett nyomozó alkalmazásának feltételei továbbra is fennállnak, ügyészi engedélyre alkalmanként szintén hat hónapra meghosszabbítható. A Be. rendelkezik a fedett nyomozó alkalmazásának eseteiről. Ilyen lehet a bünszervezetben történő beépülésének, a rejtett figyelés végrehajtásának vagy az álvásárlásnak az esete.¹¹⁴ Ha a fedett nyomozó eljárása során bűncselekményt, illetve szabálysértési vagy közigazgatási bírsággal sújtandó cselekményt követ el, nem lesz büntetendő, ha az a cselekményének az eredményességéhez vezet (például kábítószer vesz a fedett nyomozó annak érdekében, hogy a kábítószer kereskedelemben részt vevő tagokat fel tudja térképezni, be tudja azonosítani), vagy a lelepleződésének a megakadályozásához szükséges.¹¹⁵ Azonban fennáll az a szabály, hogy a fedett nyomozó cselekménye közben nem bírhat más bűncselekmény elkövetésére.

A fedett nyomozó alkalmazása kifejezetten alkalmas lehet például a gyermekpornográfia bűncselekményének a felderítésében, ahol ugyanis titkos, zárt csoportokban kommunikálnak az elkövetők. Ebben az esetben a fedett nyomozó feladata legfőképpen a tagoknak a megismerése, a csoportba történő beilleszkedése, valamint az elkövetők tartózkodási helyének a beazonosítása.

¹¹³ Be. 221. §

¹¹⁴ Be. 222. § (2) a), c), d)

¹¹⁵ Be. 224. § (1) a), b)

2.2.4. INFORMÁCIÓS RENDSZER TITKOS MEGFIGYELÉSE

Az információs rendszer titkos megfigyelése elnevezésű leplezett eszköz bírói engedélyhez kötött. Tagadhatatlan tény, hogy a bírói engedélyhez kötött leplezett eszközök a magánélethez vagy az információs önrendelkezési joghoz való alapjogokat sértik, de ahogy korábban említettem, a bűncselekmény eredményes felderítéséhez szükséges és arányos mértékben korlátozhatóak ezen alapjogok.

„Információs rendszer titkos megfigyelése során a leplezett eszközök alkalmazására feljogosított szerv bírói engedéllyel információs rendszerben kezelt adatokat titokban megismerhet, az észlelteket technikai eszközzel rögzítheti.”¹¹⁶ Továbbá, azon adat, amely ennek érdekében szükséges, az elhelyezhető az információs rendszerben, technikai eszköz esetén pedig lakásban, gépjárműben vagy egyéb helyiségben helyezhető el. Az ilyen elhelyezett adatokat vagy technikai eszközöket a leplezett eszköz alkalmazása befejezését követően haladéktalanul el kell távolítani.

3. AZ IGAZSÁGÜGYI INFORMATIKAI SZAKÉRTŐ

3.1. KIRENDELÉSE

A hatályos Be. alapján „ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni.”¹¹⁷ Fontos kritérium azonban, hogy meg kell különböztetni a jogkérdést a ténykérdéstől. A szakértő kizárólag ténykérdésben dönthet, hiszen a jogkérdés eldöntése a bíróságra hárul. Tehát minden olyan döntés, ami nem jogkérdés és különleges szakértelmet kíván meg szakkérdésnek minősíthető. „A szakértő a bíróság különleges szakértelmét pótolja, feladata releváns szakkérdések megvilágítása és értékelése.”¹¹⁸ A szakértő feladata tehát „hogy a hatóság kirendelése vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását.”¹¹⁹ A kirendelés során általában a szokásjog játszik fontos szerepet. A szakértőtől elvárható az a magatartás, hogy úgy járjon el, mintha a kirendelő maga végezné el a szükséges feladatot, feltéve, ha rendelkezne azzal a különleges szakértelemmel, amelynek hiányában szükségesnek látta a szakértőt az eljárásba bevonni. „[...] a szakértő kötelessége a számára átadott tárgyak, eszközök, adatok eredetiségének a megőrzése és a szakértői vélemény elkészítésével együtt a hatóság számára történő visszaadása.”¹²⁰ A szakértőnek meg kell

¹¹⁶ Be. 232. § (1)

¹¹⁷ Be. 188. § (1)

¹¹⁸ KISS i. m. 143

¹¹⁹ 2016. évi XXIX. törvény az igazságügyi szakértőkről

¹²⁰ KISS i. m. 146

ismernie azon adatokat, amelyek feltétlenül szükségesek a feladatának az ellátásához (pl. eljárás ügyiratai, jelen lehet az eljárási cselekménynél stb).¹²¹ „Az igazságügyi informatikai szakértő az elektronikus/digitális bizonyítékok felkutatása, azonosítása során jut szerephez, jellemzően a házkutatások alkalmával.”¹²²

Fontos hangsúlyozni, hogy egy online térben elkövetett bűncselekmény vagy annak a gyanúja fennállása esetén (tehát az előkészítő eljárásban) az igazságügyi informatikai szakértő mindig jelen van, ugyanis ő rendelkezik – remélhetőleg – olyan szaktudással, kompetenciával, amelyekkel más, az eljárásban résztvevő személyek nem. Merülhet fel a kérdés, ha egy általánosnak nevezhető igazságügyi informatikai szakértő nem rendelkezik azzal a kompetenciával, amire szükség van, akkor azt milyen „eszközzel” helyettesítik. Ebben az esetben, ha nincs meg a megfelelő kompetencia (mert például egy olyan bűncselekményről van szó, amelynél egy gazdasági társaság egy saját szoftvert fejlesztett és azon keresztül lett elkövetve a bűncselekmény), akkor eseti szakértő kerül kirendelésre. Azért lényeges mindenképpen egy szakember kirendelése, mert a szaktudás egy sikeres eljáráshoz elengedhetetlen. Azonban az eseti szakértő legtöbb esetben sokkal több kiadással jár, valamint sokkal bonyolultabb megfelelő időpontot egyeztetni személyével, hiszen az ilyen különleges szaktudást igénylő szakterületekből elenyésző számban találhatók meg a megfelelő szakemberek. Ezért az eljárás akár hónapokkal is eltolódhat.

Az eljárás során általa tapasztalt adatokat rögzíti, és arra a szakvéleményre támaszkodik a bíróság. A szakértő tehát egy online térben elkövetett bűncselekmény esetén kulcsfontosságú szerepe van, hiszen, ha az adatokat nem a valóságnak megfelelően, nem helyesen rögzíti, akkor akár a büntetőeljárás felmentéssel is zárulhat, hiszen a bíró a rendelkezésére álló adatokra támaszkodik, a védelem pedig hivatkozhat arra, hogy az adatok nem felelnek meg a valóságnak.

A szakértő bevonásának szükségessége a kiberbűncselekmények nyomozása vagy bármely eljárási cselekmény során gyakran vitatott kérdés. Sem a büntetőeljárás egyéb résztvevői, sem a hatóságok között nincs egyöntetű vélemény arról, hogy szükséges-e szakértőt kirendelni, és ha igen, mikor. Egyesek felesleges kiadásnak tekintik, hiszen a szakértő által végzett vizsgálatokat gyakran el tudná végezni egy helyi informatikus vagy rendszergazda is.¹²³ „Hazánkban a helyi rendőrkapitányságokon nem működik elkülönült részleg a

¹²¹ BE. 192. § (1) a–b)

¹²² MÁTÉ István Zsolt: *A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban*. Magyar Rendészet 2014/2.

¹²³ KISS i. m. 147

számítástechnikai bűncselekmények nyomozására. A nyomozók csak szakértőktől, szaktanácsadóktól [...] kaphatnak útmutatást.”¹²⁴

3.2. ÁLTALÁNOS VIZSGÁLATI ELJÁRÁS

A következőkben az általános vizsgálati eljárás menetét tartom szükségesnek részletezni. Az általános vizsgálati eljárás szakaszai sorrendben a vizsgálati tárgy azonosítása, a vizsgálati tárgy állapotának felmérése, a vizsgálati tárgy állapotának megóvása, valamint a vizsgálat.

3.2.1. VIZSGÁLATI TÁRGY AZONOSÍTÁSA – MEGKÜLÖNBÖZTETÉS, VALAMINT A FELISMERÉS

Mind a megkülönböztetésnek, mind a felismerésnek vannak általános elvei. Az eszközök felismerése elsődlegesen fizikai tulajdonságuk alapján történik, majd ezt követően kell „az adott eszköz osztály általános megjelenési jellemzőit [...] összevetni a kérdéses eszköz jellemzőivel, majd a hasonlóság alapján kell elvégezni az elsődleges besorolást.”¹²⁵ Megkülönböztetés esetén az eszközök műszaki címkéi, gyári iratai vehetők elsősorban figyelembe.

A felismerés és a megkülönböztetés gyakorlati alkalmazásakor a „szakértői vizsgálatot megelőzően a vizsgálatra átvett tárgyakról és azok csomagolásáról, illetőleg a csomagolás bontási folyamatáról képi [...] dokumentáció készülhet.”¹²⁶ Ledokumentálandó a dokumentáció során az eszköznek a márkája, azonosítója, általános állapota, jellege, típusa. Miután a tárgyak azonosítása megtörtént, meg kell állapítani, hogy „a szakértőt kirendelő dokumentumban feltüntetett és a ténylegesen átvett tárgyak egymásnak megfelelnek-e [...]”.¹²⁷ Ezt követően azt a kérdést kell megválaszolni, hogy a vizsgálatra átvett tárgyakban lévő adatok mentése szükséges-e. Fontos kérdéskör szintén, hogy a vizsgált eszköz roncsolás nélkül szétszerelhető-e vagy sem. Amennyiben roncsolás nélkül a szétszerelés meg tud valósulni, akkor magáról a folyamatról szintén készülhet digitális képi dokumentálás, majd a szétszerelt eszközt eredeti állapotába szükséges helyreállítani. Azonban, ha roncsolással valósítható meg csak az eszköz vizsgálata, úgy szükséges a megbízó vagy a kirendelő írásos felhatalmazása.¹²⁸

¹²⁴ PARTI i. m. 188

¹²⁵ MÁTÉ István Zsolt – DARABOS Zoltán – MORBER Szilárd Krisztián – SÁNDOR Gábor: Módszertani levél. Az elektronikus adatok vizsgálatának általános alapelveiről. Magyar Igazságügyi Kamara. 6/2020. https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf 22

¹²⁶ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 19

¹²⁷ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 20

¹²⁸ Uo.

3.2.2. FELMÉRÉS ÉS MEGÓVÁS

Az eszközfelmérés legfőbb célja „az adathordozók, illetve az azokat működtető eszközök mechanikai, elektronikai és informatikai ellenőrzése.”¹²⁹ Az eszközfelmérés az adatmentés megkezdése előtt történő folyamat.

„A megóvás az a folyamat, melynek során megvédik és fenntartják a digitális adat hordozó és a lehetséges digitális adat eredeti állapotát.”¹³⁰ A megóvás során figyelemmel kell lenni az elektromágneses mezők, a fizikai szennyeződések, mechanikai károsodások, adatmódosulások hatásaira, körülményeire.

3.2.3. VIZSGÁLAT

A kirendelt és eljáró szakértő a szükséges vizsgálatot elvégzi, amely során négy módszert alkalmaz, nevezetesen a digitális nyomrögzítés, vizuális adatrögzítés, adattartalom hozzáférhetőségének biztosítása és az adatok elemzése. Az, hogy a szakértő mely módszert vagy módszereket alkalmazza, az a saját felelősségi körébe tartozik.¹³¹

A digitális nyomrögzítés a „digitális adat kinyerése az adatok meghatározott köréről készített másolat létrehozásának folyamata.”¹³² Az adatkinyerésnek három alapvető esete van, ezek a következők: bekapcsolt digitális eszközről történő adatkinyerés, kikapcsolt digitális eszközről történő adatkinyerés, valamint nem leállítható bekapcsolt digitális eszközről történő adatkinyerés.

A vizuális adatrögzítés alkalmazása elsősorban akkor történik, amikor „a vizsgált digitális eszköz működőképes, azonban informatikai szempontból alkalmatlan a digitális nyomrögzítésre.”¹³³ E módszer alkalmazásával lehetséges a képernyőkép, képernyőfelvétel, kijelzőfotó, videófelvétel készítése.¹³⁴ Ami esetlegesen magyarázatot igényel, az a kijelzőfotó. A kijelzőfotó a „digitális eszköz képernyőjén vagy kijelzőjén működés közben megjelenő adattartalomról optikai fényképezés útján készített analóg vagy digitális fénykép.”¹³⁵ A képernyőfotó annyiban különbözik ezen módszertől, hogy szoftveres úton készítendő digitális fénykép.

¹²⁹ Uo.

¹³⁰ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 21

¹³¹ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 23

¹³² Uo.

¹³³ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 31

¹³⁴ Uo.

¹³⁵ Uo.

„Az adattartalom hozzáférhetősége biztosítására szolgáló metódus kiválasztása az eszközfeldmérés eredményének, valamint az adattartalom feldolgozási módszer alkalmazása során felmerülő adathozzáférési akadályok figyelembe vételével történik.”¹³⁶

Az adatok elemzését „oly módon kell elvégezni [...], hogy a digitális adat módosulásának lehetősége minimális legyen.”¹³⁷ Azonban történhet olyan eset, amely során az eredeti dokumentum mégis megsérül vagy megváltozik. Ekkor a helyes eljárás az, hogy ennek a tényét, okát, valamint a hatását a vizsgálatról szóló dokumentumba ismertetni kell.¹³⁸

4. FELDERÍTÉS

A felderítés általános szabályait a Be. LX. fejezete tartalmazza. E fejezeten belül a törvény meghatározza azon személyek körét, akik a felderítés folyamán jelen lehetnek, részletesen szól a gyanúsított kihallgatásának szabályairól, valamint az ügyiratok kezeléséről.

4.1. A FELDERÍTÉS ÁLTALÁNOS NEHÉZSÉGEI

Egy online térben elkövetett bűncselekmény felderítése jelentősen nehezebb egy fizikai térben elkövetett bűncselekményhez képest. Ugyanis elsősorban, ami ezt a nehézséget különösen megnöveli, hogy az elkövetett bűncselekmények csupán töredéke jut a hatóságoknak a tudomására.¹³⁹ Azonban, ha a bűncselekmény elkövetése a hatóságok tudomására jut, akkor a következő nehézséget az elkövető személyének a felderítése okozza. Legtöbb esetben egy online bűncselekménynél a nemzetközi jelleg a jellemző. Ahhoz, hogy az elkövetőről bármilyen érdemi információt sikerüljön beszerezni a nyomozó hatóságnak, mindenképpen egy nemzetközi együttműködést igényel e tevékenység. Azonban még tovább nehezíti a felderítést, hogy nincs egy nemzetközileg egységes szabályozás. Kérdésként felmerülhet, hogy mi számít az elkövetés helyének. Ezt később egy magyar gyakorlati példával is szemléltetni fogom, hogy a két bíróság másképp állapította meg az elkövetés helyét. A nemzetközileg elfogadott joghatósági elv az elkövetés helyére vonatkozóan a területi elv. Mi lesz az elkövetés helye, ha például az elkövető Kanadában él, és az általa kifejtett online bűncselekmény sértettjei argentin, illetve chilei állampolgárok? A területi elv alapján Kanada lesz az elkövetés helye, hiszen a bűncselekményt a elkövető ott fejtette ki, de Kanadában nem volt sértettje az általa elkövetett deliktumnak, így ott a büntetőeljárás megindítására nem kerülhet sor. A két sértett a saját országában feljelentést tud tenni, de ők nem tudnak a területi elvre alapozni, hiszen nem az ő

¹³⁶ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 34

¹³⁷ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 41

¹³⁸ Uo.

¹³⁹ HERÉDI i. m. 49

országukban lett kifejtve a deliktum. Ezen példa alapján pedig megállapítható, hogy a területi elv nem nyújt teljeskörű megoldást.¹⁴⁰

A mindennapi gyakorlatban a kiberbűncselekmények egyik legjellegzetesebb vonása az a magas szintű anonimitás, amelyet a kibertér biztosít az elkövetők számára. Az anonimitás ugyanakkor csak egy lehetőség, amit az elkövetők kihasználhatnak, de gyakran előfordul, hogy valamilyen módon, akár közvetlenül, akár közvetve, felfedhetik saját személyazonosságukat a jogsértések során.¹⁴¹ A személyiség elrejtésének egyik legáltalánosabb esete az online avatároknak a használata. „Az avatár egy olyan, kizárólag az online világban létező személyes profil, amely nem a tulajdonosának valós adataira építkezik.”¹⁴² Viszont a legtöbb felhasználó gyakran lustaságból vagy figyelmetlenségből olyan elemeket is beépít avatárjaikba, amelyek közvetve vagy közvetlenül utalhatnak valódi személyazonosságukra vagy korábbi profiljaikra. Ezek az információk lehetőséget adnak arra, hogy további adatokat gyűjtsenek a felhasználó kilétéről. Emellett a hatóságok számára rendelkezésre állnak a szolgáltatóktól történő adatkérések is, amelyek alapján a felhasználó hálózati tevékenységeire és az általa megadott személyes adatokra vonatkozó információkhoz juthatnak hozzá.¹⁴³ Nemzetközi szinten lévő együttműködés tekintetében az előző pontban említett Számítástechnikai Bűnözésről szóló Egyezmény kimondja, hogy egy tagállam bármikor, a hét minden napján és a nap 24 órájában kapcsolatba léphet egy másik, az egyezményben részes tagállam hatósági kapcsolattartó pontjaival, hogy kérje az adott ország területén működő szolgáltatót, az ügghöz kapcsolódó elektronikus adatok megőrzésére, legfeljebb 90 napig, vagy a jogsegélykérelem megérkezéséig. Hazánkban a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya lett kijelölve kapcsolattartási pontként. Egyes tagállamok nemcsak az adatok megőrzéséről értesítik hatóságunkat, hanem gyakran már a kért elektronikus adatokat – például előfizetői adatokat – is megküldik válaszukban. Ez jelentősen felgyorsíthatja az eljárást, mivel a válaszban megkapott adatok alapján további lépések tehetők, anélkül, hogy meg kellene várni a jogsegélykérelem hivatalos válaszát. Lényeges, hogy a külföldi hatóságok általában akkor nyújtanak gyors adatot, ha az közvetlenül hozzájárul az elkövető azonosításához. Amennyiben azonban a bűncselekmény és a kért információ közötti kapcsolat csak közvetett, vagy a megkeresésben szereplő tényállásból nem egyértelműen felismerhető, a megkeresett állam

¹⁴⁰ Tóth Dávid – Gáspár Zsolt: *Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén*. Büntetőjogi Szemle. 2020/2. https://ujbtk.hu/wp-content/uploads/lapszam/BJSZ_202002_140-150o_TothDavid_GasparZsolt.pdf 144

¹⁴¹ HERÉDI i. m. 50

¹⁴² Uo.

¹⁴³ Uo.

megtagadhatja az információ szolgáltatását, vagy felhívhatja a megkereső államot a kérés pontosítására, hivatkozva saját jogi előírásaira.¹⁴⁴

További felderítési probléma, hogy az online bűncselekményeket olyan térben követik el, ahol nincs szükség papírokra vagy nyomtatott példányokra, hanem a számítástechnikához és az internethez kapcsolódó virtuális világban. Ez pedig megkönnyíti az elkövető számára, hogy a bűncselekmény elkövetése után pillanatokkal megbabrálja az adatokat és a programokat, így eltörölve minden lehetséges bizonyítékot. Ez megnehezíti a nyomozók számára a bizonyítékok összegyűjtését.¹⁴⁵

A felderítést jelentősen megnehezíti, hogy „a kibertérben elkövetett bűncselekmények [esetén] [...] az online szolgáltatások bővülésével, a technológiai újítások felszínre kerülésével új elkövetési magatartások jelennek meg, valamint az elkövetők is új eszközökhöz jutnak.”¹⁴⁶ Ezen okok miatt a felderítést végző szervezetnek elképzelhetetlen az, hogy ne legyenek naprakész ismereteik a technológiai fejlődés szempontjából.¹⁴⁷ Sajnos azonban kijelenthető, hogy egy online térben elkövetett bűncselekmény esetén az elkövetőnek felfoghatatlan lépéselőnye van a nyomozó hatóságokkal szemben, ugyanis egy ilyen bűncselekmény elkövetője legtöbb esetben egy profi, a számítástechnikához nagyon értő személyről van szó. Ezért tartom szükségesnek, hogy a felderítést végző személyeknek legyen egy rendszeres továbbképzés, ugyanis a „bűnözőket nem utol kell érni, hanem előttük kellene lenni”, ez pedig képzések nélkül nem valósítható meg.

4.2. A TÖRÖLT VAGY MÓDOSÍTOTT ADATOK HELYREÁLLÍTÁSÁNAK A FOLYAMATA

4.2.1. ADATMÓDOSULÁS

Minden esetben meg kell akadályozni az adatmódosulás lehetőségét élő számítógépes rendszer esetén. Azonban, ha fennáll ennek a veszélye (pl. távoli hozzáférés, vagy adattörölő eljárás elindulása), akkor el kell különíteni az adott eszközt a számítógépes rendszer többi elemétől el kell mihamarabb különíteni, valamint a rendszernek az áramellátását meg kell szüntetni azonnali beavatkozás révén. Amennyiben a folyamat megszakítása után káros beavatkozás történt, azt dokumentálni kell a rendelkezésre álló adatok alapján.¹⁴⁸

Amennyiben az adatkinyerést követően a forrás az adathordozó vagy átviteli csatorna működése miatt olvashatatlan, a hiba kiterjedését dokumentálni szükséges, valamint „hogy a

¹⁴⁴ HERÉDI i. m. 52

¹⁴⁵ Ahmad Fekry MOUSSA: *Electronic evidence and its authenticity in forensic evidence*. Megtekintés: 2024. október 14. <https://ejfs.springeropen.com/articles/10.1186/s41935-021-00234-6>

¹⁴⁶ Herédi i. m. 52

¹⁴⁷ Uo.

¹⁴⁸ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 19

mérettartó másolatok (lemezképek) esetében a hibás forrásadatok milyen logikai értékkel lettek helyettesítve (bitmintázat)”¹⁴⁹

4.2.2. ADATTÖRLÉS

„Amennyiben a szakkérdés megválaszolása azt indokolja, szükség lehet a törölt állományok helyreállítására és / vagy a fájlrendszer által nem nyilvántartott digitális adatok kinyerésére.”¹⁵⁰ A törölt adatok csak abban az esetben állíthatók vissza, amennyiben azt az operációs rendszer vagy a fájlrendszer működési elve ezt lehetővé teszi. „Egy törölt állomány helyreállítása gyakorlatilag a fájlrendszer nyilvántartásában meglévő inaktív (allokátlan) állománybejegyzések aktívvá (allokálttá) módosítása útján történik meg.”¹⁵¹

5. KÉNYSZERINTÉZKEDÉSEK

„A kényszerintézkedések minden esetben valamilyen alapjogot korlátoznak, ezért meg kell felelniük a szükségesség-arányosság Alkotmánybíróság által kidolgozott kritériumnak.”¹⁵² A digitális környezethez kapcsolódóan a következő kényszerintézkedéseket tudjuk megkülönböztetni: a kutatás (Be. 302. § - 305. §), az elektronikus adat lefoglalása és a megőrzésre kötelezés (Be. 315. § - 317. §), valamint az elektronikus adat ideiglenes hozzáférhetetlenné tétele (Be. 335. § - 338. §).

5.1. A KUTATÁS

A kutatás elrendelésének szabályait a Be. 302. §-ban részletezi. Eszerint tehát „a kutatás a büntetőeljárás eredményes lefolytatása érdekében a lakás, az egyéb helyiség, a bekerített hely vagy a jármű átkutatása. A kutatás információs rendszer, illetve adathordozó átvizsgálására is kiterjedhet.”¹⁵³ A kutatást abban az esetben lehet elrendelni, az megalapozottan feltehető, hogy információs rendszer, illetve adathordozó átvizsgálására vezet.¹⁵⁴ Ha az információs rendszer átvizsgálására kerül a sor, akkor fontos garanciális szabály, hogy „biztosítani kell az információs rendszer útján [...] hozzáférhető adatok megismerését és rögzítését is, függetlenül az adatok elhelyezkedésétől.”¹⁵⁵ Mivel nem minden rendőrkapitányság rendelkezik a kényszerintézkedések végrehajtásához szükséges eszközökkel, és bizonyos szakkérdésekben a rendőrségi állomány gyakran nem rendelkezik megfelelő szaktudással, ezért sok esetben külső

¹⁴⁹ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 30

¹⁵⁰ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 45

¹⁵¹ Uo.

¹⁵² DORNFELD i. m. 115

¹⁵³ Be. 302. § (1)

¹⁵⁴ Be. 302. § (2) e)

¹⁵⁵ 100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól 86. § (1)

segítséget vesznek igénybe.¹⁵⁶ Ebben az esetben az a személy fogja a helyszínen elvégezni azon teendőket, amelyek az eljárási cselekményhez elengedhetetlenek, akit küldőleg segítségül rendelnek – ő lehet például szakértő, illetve szaktanácsadó. Amikor a kutatás kényszerintézkedését megkezdik, azon személyeket, akiket az intézkedés alá vontak, az eszköz közeléből el kell távolítani (természetesen azért, hogy a kényszerintézkedés alatt ne tehessenek kárt az esetleges bizonyítékokban).

5.2. AZ ELEKTRONIKUS ADAT LEFOGLALÁSA ÉS A MEGŐRZÉSRE KÖTELEZÉS

Ha a büntetőeljárás sikeres lefolyása szükségessé teszi az elektronikus adat lefoglalását, akkor általában magát az információs rendszert (például számítógépet) lefoglalni, mert a büntetőeljárás során relevanciája az elektronikus adatnak van, amit természetesen másféle módon is ki lehet nyerni az adathordozóból vagy információs rendszerből – példának okáért átmásolással, áthelyezéssel. Ha maga a nyomozó hatóság teljes pontossággal tudja, hogy mely adatokra van szüksége, akkor csak azon adatokat másolják le. Ellenkező esetben – tehát ha abban az időpontban, amikor a lefoglalás történik, nem határozható teljes pontossággal, hogy mely adatokra van szükség – a teljes tartalom átmásolására nyílik lehetőség. Fontos kritérium, hogy az átmásolás csak „utólag meg nem változtatható adathordozóra történhet.”¹⁵⁷ Továbbá biztosítani szükséges, hogy ne változzanak meg az eredeti adatok az átmásolás során. Az átmásolás megtörténte után a hatóság jegyzőkönyvet készít, és a jegyzőkönyvben fel kell tüntetni a rögzítésre használt adathordozó gyártási számát, típusát, továbbá az adathordozón tárolt adat jellegét és tartalmát fel kell tüntetni. Azonban az adathordozó fizikai lefoglalására is sor kerülhet. Ez azon esetekben történhet, ha felmerül a gyanú, hogy az adathordozón vannak esetleg törölt adatok, és ezek a törölt adatok egyszerű másolással nem foglалhatóak le, vagy ha maga az adathordozó bizonyítási eszköz, továbbá elkobzást vagy vagyonelkobzást rendelvek el. A Be. 315. § (4) bekezdése alapján „Az elektronikus adat lefoglalását úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse.”¹⁵⁸ Ezen bekezdés miatt, ha az adathordozó fizikai lefoglalására sor kerül, azt meg kell indokolni, hogy mi az oka, miért nem volt elegendő a teljes vagy egyszerű másolatnak a készítése.¹⁵⁹ Ha az elektronikus adat fizetésre használt, akkor a lefoglalást úgy is végre lehet hajtani, hogy azt az elszenvető fél a lefoglalt adatot fizetésre használja (például rossz kódok megadásával zárva). Ez a szabály

¹⁵⁶ KISS i. m. 134

¹⁵⁷ HEKRE Csongor: *A digitalizáció szerepe a büntetőeljárásban* A bűnügyi tudományok és az informatika. MTA TK Jogtudományi Intézete és a Pécsi Tudományegyetem Állam- és Jogtudományi Kar. Budapest-Pécs, 2019. 118

¹⁵⁸ BE. 315. § (4)

¹⁵⁹ HEKRE i. m. 119

kiterjed a virtuális fizetőeszközökre is. Továbbá olyan eset is lehetséges elektronikus adat esetében, hogy a lefoglalást se másolással, se fizikai hordozó lefoglalásával fogatosítják, hanem az adat megőrzésre kötelezettjének az elektronikus adat feletti rendelkezési jogát korlátozzák. Ilyenkor a kötelezettnek kell ügyelnie arra, hogy az adat ne sérüljön, ne törölődjön, illetve, hogy ne továbbítsa.¹⁶⁰ Azonban indítványra az is elrendelhető, hogy az őrzésre kötelezettnek ne kelljen fizikailag megőriznie ott, ahol elrendelte a hatóság, hanem arról másolatot készítsen és azt a másolatot őrizze. Ilyenkor természetesen az eredeti elektronikus adatok megváltoztatására már sor kerülhet – ha az engedélyt adnak – a megőrzésre kötelezett által. Azonban a mai technológiai világban így is sok veszélynek ki van téve a megőrzésre kötelezett. Tehetjük fel a kérdést, hogy abban az esetben történik-e felelősségre vonás, amikor ő mindent megtett annak érdekében, hogy például ne férjen hozzá más illetéktelenül az adatokhoz – mert például hackertámadás áldozata lett? Természetesen ebben az esetben nem fog sor kerülni felelősségre vonásra, hiszen a kötelezettől nem várható el olyan magatartás, amely az általánosan elvárt mértéket meghaladja. Ebben az esetben viszont köteles a lehető legrövidebb időn belül jelezni a megőrzésre kötelezést elrendelőt.¹⁶¹ A megőrzésre kötelezés kizárólag büntetőeljárás alatt rendelhető el és leghosszabb időtartama három hónap lehet.

5.3. AZ ELEKTRONIKUS ADAT IDEIGLENES HOZZÁFÉRHETETLENNÉ TÉTELE

Ezen kényszerintézkedés a Btk. 77. §-át, azaz az elektronikus adat végleges hozzáférhetetlenné tételét biztosítja, és kizárólag a bíróság rendelheti el. Ez magába foglalja az adat ideiglenes eltávolítását, az elektronikus adathoz való hozzáférés ideiglenes megakadályozását és az elektronikus adat önkéntes eltávolítására történő felhívást. „A három intézkedési lehetőség alkalmazása egyfajta fokozatosságon alapul [...]”¹⁶² A legalsóbb szinten az önkéntes eltávolításra történő felhívás. Ezen intézkedés körében a tárhelyszolgáltató és a tárhelyszolgáltatást végző közvetítő mellett a médiatartalom-szolgáltató is kaphat ilyen felhívást. Ezt a gyakorlatban egy hatósági figyelmeztetésként lehet értékelni. A lépcsőfok második fokán az ideiglenes eltávolítás áll. Ennek lényege, hogy az adott tartalom elérhetetlen lesz az online térben, ezért a kötelezettek köréből kiesik a médiatartalom-szolgáltató. Amikor viszont a hozzáférés megakadályozása történik, akkor az adott weblapot teszik elérhetetlenné a magyar felhasználók számára, ezért ennél a körnél a kötelezettek száma egyel ismét csökken, és a kötelezett ennél az intézkedésnél az elektronikus hírközlési szolgáltató. Természetesen ez

¹⁶⁰ Uo.

¹⁶¹ HEKRE i. m. 120

¹⁶² BÉKÉS Ádám – GÉPÉSZ Tamás: *A bűncselekmény helyszíne: az internet. Bizonyítási és eljárási nehézségek az interneten elkövetett bűncselekmények kapcsán*. In Medias Res. 2024/1. 13. évfolyam. Megtekintés: 2024. október 13. <https://inmediasresfolyoirat.hu/imr/article/view/298> 122

nem azt jelenti, hogy az adott elektronikus adat lekerül a világhálóról, mert az lehetetlen volna, hanem csak azt eredményezi, hogy a magyar felhasználók nem férnek hozzá. A hozzáférés megakadályozása egy „drasztikusabb intézkedés, így csak bizonyos, kizárólag közvéder üldözendő bűncselekmények esetében és csak akkor van helye, ha az ideiglenes eltávolításra való kötelezés [...] nem vezetett eredményre.”¹⁶³ Ez azonban mint már korábban említettem, nem jelent megoldást, hiszen a jogellenes tartalom továbbra is a világhálón marad. Maga az intézkedés csökkenteni tudja a jogellenes tartalom országon belüli hozzáférhetőségét, azonban mivel nem szűnik meg a jogsértés, ezért külföldről vagy egy speciális böngésző használatával ismét hozzáférhetőek ezen tartalmak.¹⁶⁴ Ebből pedig az következik, hogy az intézkedés csak egy félmegoldást tud adni.

6. A BIZONYÍTÁSI ELJÁRÁS

Szükségesnek tartom megemlíteni a fizikai térben és a digitális térben lévő bizonyítékoknak a komplexitását. Attól, hogy egy bűncselekmény az online térben lett elkövetve, nem jelenti azt, hogy a fizikai térben ne legyenek az ehhez a bűncselekményhez szorosan kapcsolódó fizikai téri bizonyítékok. Gondoljunk például a számítógépre vagy a mobiltelefonra, amik a fizikai térben jelennek meg, és az azon az eszközön tárolt adatok pedig digitális téri bizonyítékként szolgálhat a joghatóság számára. A fizikai és a digitális téri bizonyítékok ezek alapján szervesen nem tud elválni.

6.1. ÁLTALÁNOS SZABÁLYOK

„A bizonyítás azokra a tényekre terjed ki, amelyek a büntető és a büntetőeljárás jogszabályok alkalmazásában jelentősek. A bizonyítás a büntetőeljárás járulékos kérdéseinek elbírálásában jelentős tényekre is kiterjedhet.”¹⁶⁵ Garanciális szabályként mutatkozik meg a Be-ben, hogy csak olyan bizonyíték használható fel a büntetőeljárás során, amely bizonyítottan a valóságnak megfelelnek.

A bíró a tényállás keretein belül mozoghat. Ez a vádhoz kötöttség elve. Ez azt jelenti, hogy a bíró csak a tényállásban megállapított tényekre alapozhat és azon nem terjeszkedhet túl. Például egy adott ügyben hiába nyilvánvaló, ha a sértett lopást követett el, ha az a tényállásban nem szerepel – tehát az ügyészség nem emelt ellene vádat –, akkor azért a cselekményért a sértettet a bíró nem vonhatja felelősségre. Azonban a vádhoz kötöttséget nem sérti, ha a bíró a tényállást feldolgozva arra a következtetésre jut, hogy a tényállásban meghatározott elemek közül nem mind bír relevanciával, így figyelmen kívül hagyja azokat. Tehát összefoglalva, a

¹⁶³ BÉKÉS – GÉPÉSZ i. m. 123

¹⁶⁴ BÉKÉS – GÉPÉSZ i. m. 124

¹⁶⁵ Be. 163. § (1)

bíró a tényálláson túl nem terjeszkedhet, viszont a tényállást szűkíthet, figyelmen kívül hagyhat a mérlegelése alapján információkat.

Természetesen nem kell azokat az tényeket bizonyítani, amelyek mindenki számára köztudottak, amelyekről a bíróságnak, ügyészségnek, illetve a nyomozó hatóságnak tudomása van, valamint amelyeknek a valóságát a vádló, a terhelt, valamint a védő együttesen elismernek. Ez az úgynevezett valónak elismerés lehetősége. Itt nem arról van szó, hogy egy adott ügyben a terhelt a vádnak megfelelően beismeri cselekményét, hanem annak csak bizonyos pontjait ismeri el a valóságnak megfelelően. „A vád bizonyításához szükséges tények feltárása, az alátámasztásukra szolgáló bizonyítási eszközök rendelkezésre bocsátása, illetve beszerzésének indítványozása a vádlót terheli.”¹⁶⁶

6.2. AZ ELEKTRONIKUS BIZONYÍTÉKOK BESZERZÉSE SORÁN FELMERÜLŐ PROBLÉMÁK

Elektronikus bizonyítéknak számít minden olyan digitálisan tárolt, feldolgozott vagy továbbított adat, amely bizonyító értékkel bír.¹⁶⁷ Az egyik legjelentősebb nehézséget az adja, hogy legtöbb esetben az elkövető sokkal nagyobb informatikai tudással rendelkezik, mint a nyomozó hatóság tagjainak, bíróknak, ügyészeknek, ezzel is nehezítve a büntetőeljárás gyors és sikeres lefolyását, hiszen félrevezető információkat használhatnak védekezésre. További nehézséget okozza, hogy a büntetőeljárás kezdetén a kriminalisztika hagyományos módszerei (például a daktiloszkópia) nem kap szerepet, hiszen az elektronikus adaton kívül nem áll más a rendelkezésre a hatóságoknak. Nem szabad elmenni azon információ mellett sem, hogy az elektronikus adatok nagyon könnyen megsemmisíthetőek, módosíthatóak, így a nyomozó hatóság részéről a bizonyításhoz elengedhetetlen a magas szakmai ismerettel rendelkező technikai, informatikai rendszerek iránt.¹⁶⁸ Ugyanakkor „[...] a bizonyítási eszközök beszerzésének a digitális térben is törvényesnek és szakszerűnek kell lennie. Megfelelően kell dokumentálni, és biztosítani kell a zárt lánc meglétét a megszerzéstől egészen az értékelésig.”¹⁶⁹ Shiuh-Jeng Wang szerint a következő három kritériumot kell betartani a nyomozások során: (1) a bizonyítékok megszerzése az eredetinek megváltoztatása vagy megrongálása nélkül, (2) a visszaszerzett bizonyítékok hitelesítése az eredetileg lefoglalt adatokkal megegyezőnek, (3) az

¹⁶⁶ Be. 164. § (2)

¹⁶⁷ Antonela GROPEANU – Adrian IACOB: *Investigative issues regarding cybercrime*. European Journal of Public Order and National Security, no. 2, 2016. 10

¹⁶⁸ DORNFELD László: *A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések*. Belügyi Szemle, 2018/2. <https://real.mtak.hu/114280/1/DornfeldBelugyiSzemle2018.evi2.szam115-135.pdf> 118

¹⁶⁹ PESZLEG Tibor: *A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük*. Ügyészek Lapja. 2010/2. bit.ly/4eGQLiu 25

adatok elemzése azok módosítása nélkül.¹⁷⁰ „Az adatok bizonyító erejüket csak akkor tartják meg, ha megőrzi a beszerzésüket közvetlenül megelőző állapotukat, és így a vizsgálati eredmény reprodukálható marad.”¹⁷¹

Az interneten elkövethető bűncselekmények csoportosításánál az egyik csoportot a közléssel megvalósított deliktumok képezik (például rágalmozás, zaklatás, online csalás). Ebben az esetben ellentmondásos a bírói gyakorlat. A BH2011. 332. számú eseti döntésében azt olvashatjuk, hogy „[...] megtévesztés ugyanis akkor történt, amikor az adott (konkrét) sértett az interneten szembesült a vádlott megtévesztő szándékkal internetre feltett és azáltal közvetített eladási ajánlatával. Ehhez képest a károkozó magatartás kifejtése (a pénzátutalás) és az eredmény (a kár) bekövetkezte is értelemszerűen a sértett lakóhelyén történt. Ekként valamennyi esetben ez (az adott sértett lakóhelye) az elkövetés helye.”¹⁷² Egy másik ezzel ellentétes eseti döntés (BH2016.167) szerint az online térben elkövetett rágalmozás vagy becsületsértés esetén „[...] a közzététel helye az elkövetés helye. Következésképp az interneten és egyúttal nagy nyilvánosság előtt elkövetett rágalmozás, illetve becsületsértés esetén a weboldalt működtető szerver helye jelenti az elkövetés helyét; és így a bíróság illetékességét az elkövetés helyére tekintettel megalapozó körülményt.”¹⁷³ Látható az ellentmondás a két eseti döntés között. Ezen okfejtések után érdemes megemlíteni, hogy a Be. 765. § (3) bekezdése „[...] a magánvádló feljelentése kapcsán kizárja a 21. § (3) bekezdés b) pontjának alkalmazását, vagyis a sértett lakcíme, tényleges tartózkodási helye nem lehet illetékességi ok.”¹⁷⁴ Tehát ha valóban külföldön található a weboldalt működtető szerver helye, akkor a magánvádlónak ismernie kellene a terhelt lakóhelyét is, nemcsak a kilétét. Erre próbál megoldás nyújtani a Be. 767. §-a, amely alapján lehetővé teszi, hogy a bíróság magánvádas eljárás esetén „[...] nyomozást rendeljen el a feljelentett kilétének, személyes adatainak, elérhetőségeinek felderítésére.”¹⁷⁵ Azonban egy probléma itt is felmerül, mégpedig az általános határidő. Az általános határidő két hónap, ami kétszer két hónappal meghosszabbítható. Ha a maximális hat hónap nem hoz eredményt, a bíróság az eljárást megszünteti. Tehát legfeljebb hat hónap áll

¹⁷⁰ Shiuh-Jeng WANG: *Measures of Retaining Digital Evidence To Prosecute Computer Based Cyber-Crimes*. Department of Information Management, Central Police University, Taoyuan 333Taiwan. 2006. március 25.. Megtekintés: 2024. október 13. <https://bit.ly/3NnqhGv> 218

¹⁷¹ DORNFELD i. m. 119.

¹⁷² BH 2011.12.332: Legf. Bír. Bkk. III. 473/2011. Internetes hirdetéssel megvalósított csalás esetén az elkövetési magatartás - a megtévesztés - akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot

¹⁷³ BH 2016.7.167: Kúria Bkk. III. 336/2016. Az interneten közléssel megvalósult rágalmozás vagy becsületsértés esetén a bűncselekmény elkövetésének helye - amely egyben az általános illetékességi oknak felel meg - a weboldalt működtető szerver helye.

¹⁷⁴ BÉKÉS – GÉPÉSZ i. m. 118

¹⁷⁵ Uo.

rendelkezésre, hogy a nyomozóhatóság minden közzététellel kapcsolatos adatot megszerezzen a külföldi szolgáltatótól, és ezeket követően beazonosítsa az elkövetőt. „Először is bizonytalan, hogy a külföldi szolgáltatónál rendelkezésre állnak-e a megfelelő információk, és ha igen, akkor hajlandó-e azokat kiadni [...]”¹⁷⁶ Továbbá, ha meg is érkeznek a kért adatok ezen a relatíve szűk határidőn belül, akkor egy tapasztaltabb elkövető esetében az azonosításhoz egyáltalán nem lesznek elégségesek és ezért további keresésekre lesz szükség. Problémaként merül fel, hogy a Be. 786. § (5) bekezdése alapján a magánvádló „[a] távollévő terhelttel szemben vagy külföldön tartózkodó terhelt távollétében bírósági eljárást nem indítványozhat [...]”¹⁷⁷ Tehát egy objektív akadályba ütközhet és a büntetőeljárás felelősségre vonás nélkül véget érhet. Szathmáry Zoltán véleménye alapján az internet jogi helyének meghatározása továbbra is nehézségekbe ütközik, mivel a jogalkalmazás nem képes következetesen kezelni ezek online aspektusait. A technológiai fejlődés miatt a jelenlegi jogi megközelítések elavulttá válhatnak, és a probléma megoldásához egy egységes – legalább az Európai Unió területén –, nemzetközi szabályozásra lenne szükség, amely rendezné a joghatósági kérdéseket, javítva ezzel a jogalkalmazás hatékonyságát.

6.2.1. FIZIKAI TÉRI BIZONYÍTÉKOK

Attól, hogy egy digitális térben elkövetett bűncselekményről van szó, a fizikai térben ugyanúgy jelen vannak fontosabbnál fontosabb fizikai bizonyítékok, melyeket a büntetőeljárás során felhasználhatnak. Ilyen fizikai bizonyítékként említhető meg maga a számítógép (ami talán az egyik legfontosabban begyűjtendő bizonyíték), a periféria vagy egyes adathordozók, valamint a mobiltelefon (szintén nagy jelentőséggel bír, hiszen ma már szinte mindegy egyes embernek van legalább egy mobiltelefonja, és a mobileszközöket talán többet is használják, mint a számítógépeket, nem beszélve arról, hogy a mobiltelefonok esetében felmerülhetnek olyan bizonyítékok is, mint a híváslista, esetleg fényképek).

6.2.2. DIGITÁLIS TÉRI BIZONYÍTÉKOK

A bizonyítékoknak a beszerzése egy hagyományosnak mondható bűncselekmény esetén is alapos megfontolást és mérlegelést igénylő feladatnak tekinthető. „Mérlegelni kell, hogy mit kell bizonyítéknak tekinteni [...], hogy az evidenciákat milyen módszerrel szerzik meg [...] annak érdekében, hogy azok minden kétséget kizáróan az eljárás végéig alkalmasak legyenek a bíróság előtti bizonyításra.”¹⁷⁸ Ezen hagyományos bűncselekmények (példának okáért emberölés vagy lopás) esetén is készülhetnek olyan bizonyítékok, amelyeket a büntetőeljárás

¹⁷⁶ Uo.

¹⁷⁷ Uo.

¹⁷⁸ KISS i. m. 132

során digitális bizonyítékként fel tudnak használni. Nem kizárt, hogy az adott esetről készül kép- és hangfelvétel. Gondoljunk bele, hogy a mai világban, mivel szinte mindenki rendelkezik mobiltelefonnal, ha szemtanúja lesz egy bűncselekménynek, mi az első teendője (megáll, elkezdi bémésködni és a telefonjával videófelvételt kezd el készíteni). Ezen bizonyítékoknál is elengedhetetlen az, hogy egyértelműen, kétséget kizáróan tudjanak a szakértő kérdéseire válaszok adni.¹⁷⁹

6.2.3. AZ ELEKTRONIKUS ADAT ÉS A TÁRGYI BIZONYÍTÉKOK KÖZÖTTI PROBLEMATIKA

A Be. meghatározza, hogy mi számít tárgyi bizonyítási eszköznek. E törvény szerint „tárgyi bizonyítási eszköz minden olyan tárgy [...], amely a bizonyítandó tény bizonyítására alkalmas.”¹⁸⁰ Továbbá ezen szakasz második bekezdése az iratot is a tárgyi bizonyítási eszközök közé sorolja, függetlenül attól, hogy az papíralapú vagy elektronikus adatként létező szöveg, ábra vagy rajz.

Azonban a következő, 205. § az elektronikus adatról szóló rendelkezésének második bekezdése szerint, „ahol e törvény tárgyi bizonyítási eszközt említ, azon e törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell.”¹⁸¹

Ebből látható, hogy a törvény nem tud pontos kifejezést adni az elektronikus adat és a tárgyi bizonyítási eszköz közti különbségre.

7. AZ ONLINE ELKÖVETETT BŰNCSELEKMÉNY ESETÉN RENDELKEZÉSRE ÁLLÓ BIZONYÍTÁSI ESZKÖZÖK

A Be. 165. §-ban meghatározza a bizonyítási eszközöket, melyek közül egy online térben elkövetett bűncselekmény esetén a tanúnak, az elektronikus adatnak és a szakértői véleménynek van kifejezetten hangsúlyos szerepe, mondhatni, csak ezen bizonyítási eszközök állnak rendelkezésre.

7.1. TANÚVALLOMÁS

„A büntetőeljárás sikerét a bűncselekmény teljeskörű felderítése, bizonyítása jelenti.”¹⁸² Bizonyítási eszközök közül kijelenthetjük, hogy talán az egyik legfontosabb a tanúvallomás. Pontosan ezért a fontossága miatt nagy jelentősége van annak, hogy a tanúvallomás által rögzített információk megfelelnek-e a valóságnak. A bírónak minden esetben figyelmeztetnie kell a kihallgatásra váró tanút, hogy köteles a legjobb tudomása és lelkiismerete szerint az igazat

¹⁷⁹ Uo.

¹⁸⁰ Be. 204. § (1)

¹⁸¹ Be. 205. § (2)

¹⁸² NAGY Zoltán András: *A joghatóság problémája a kiberbűncselekmények nyomozásában*. Nagy Ferenc 70. születésnapjára. Acta Universitatis Szegediensis: acta juridica et politica 2018. https://acta.bibl.u-szeged.hu/54018/1/juridpol_081_755-765.pdf 757

elmondani, továbbá, hogy a hamis tanúvallomás tételét vagy a tanúvallomás jogosulatlan megtagadását a törvény büntetni rendeli. Annak a tájékoztatásnak is el kell hangoznia, hogy a vallomása jelen vagy más ügyben bizonyítékként akkor is felhasználható, ha később a vallomástételt megtagadja. Tehát összességében azt kell elmondania a tanúnak, amire emlékszik és kitalálni és elhallgatni semmit sem szabad. Hamis adatok sajnos nem csak akkor tudnak születni, amikor valaki szándékosan hamis információval szolgál a büntetőeljárás során. Ugyanis az információk torzulhatnak a személy akarata ellenére is.¹⁸³ A korábbi büntetőeljárásról szóló 1998. évi XIX. törvényben főszabályként azt lehetett kihallgatni, aki a tizennegyedik életévét betöltötte. Viszont tizennegyedik életévét be nem töltött személyt csak akkor lehetett kihallgatni, ha a vallomásától várható bizonyíték mással nem pótolható. További szabályként szerepelt, hogy a kihallgatása esetén a hamis tanúzás következményeire való figyelmeztetést mellőzni kell.¹⁸⁴ A hatályos Be. a tizennegyedik életévét be nem töltött személyeket a különleges bánásmód körébe tartozó személyekhez sorolja. A korábbi törvényhez hasonlóan fenntartja azt a szabályt, hogy csak akkor lehet kihallgatni, ha az attól várható bizonyíték mással nem pótolható. Igaz csekély számban, de ilyen esetek is sajnálatos módon előfordultak és előfordulnak. Ez az eset azért is különösen bonyolult, mert a kihallgató személyre nagy kihívásokat jelentő feladat hárul, ha a pontos esemény leírásra törekszik. „A nehézségek a gyerek speciális jellemzőiből adódnak, amelyeket jól kell ismernie ahhoz a kérdezőnek, hogy megfelelő eredményeket tudjon elérni.”¹⁸⁵ A kihallgatás szempontjából három szakaszt tudunk megkülönböztetni, nevezetesen a megfigyelés, az emlékezetben történő tárolás és a visszaidézés. A nehézség, hogy a torzulás bármelyik szakaszban létrejöhét, akár mindhárom szakaszban is.

7.1.1. MEGFIGYELÉSI SZAKASZBAN TÖRTÉNŐ TORZULÁS A GYERMEKKORÚAKNÁL

Ebben a szakaszban is háromféleképpen tud károsodni az információ: egyes részleteket a személy nem figyel meg a figyelme szelektivitása miatt, másik eset amikor a rövidtávú memóriából a hosszú távú memóriába nem a látottaknak megfelelően raktározódik el az információ, valamint az, hogy nem egyforma az emléknymok erőssége.

Az, hogy egy gyermek milyen mértékben észlel vagy figyel meg egy eseményt, nagyban függ attól, hogy milyen előzetes tudással rendelkezik. Egy vizsgálat eredménye azt mutatta, hogy „[...] 3-10 éves gyerekek pontosan be tudtak számolni egy súlyos orvosi beavatkozásról

¹⁸³ GÁL István László – NAGY Zoltán András: *Informatika és büntetőjog*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar. Pécs, 2006. 119

¹⁸⁴ 1998. évi XIX. törvény a büntetőeljárásról. 86. § (1)

¹⁸⁵ GÁL – NAGY i. m. 120

[...], ami a kutatók szerint annak volt köszönhető, hogy előzetes tudással rendelkeztek arról, hogy mi fog velük történni.”¹⁸⁶ Ebből azt a következtetést lehet levonni, hogy ha egy gyermek egy adott eseményről keveset tud előzetesen, akkor kevesebb információt fog megjegyezni. Azonban ez a figyelemhiány a stressz miatt is bekövetkezhet.

„A rövidtávúból a hosszú távú memóriába történő átvitel során az információ azért módosulhat, mert a rövidtávú memória rendelkezik azzal a tulajdonsággal, hogy két oldalról kapja az információkat.”¹⁸⁷ Ezáltal az észlelt események egyfajta értelmezése kerül a hosszú távú memóriába.

Az emlékenyom erőssége több tényezőtől függ. Függ az életkoról, továbbá attól, hogy a gyermek megfigyelő vagy részes volt az adott eseménysorozatban. Természetesen ez azért nagyon fontos tényező, hiszen mindenki sokkal jobban emlékezik vissza pontosan az eseményekre, ha annak az eseménynek a részese, vele történik. Továbbá szintén függhet, hogy a hasonló ingerek hányszor érik az adott gyereket. Az ismétlődő átélés esetében kevésbé torzul az információ, mintha csak egyszer élné át az élményt.¹⁸⁸

7.1.2. TÁROLÁSI SZAKASZBAN TÖRTÉNŐ TORZULÁS A GYERMEKKORÚAKNÁL

A tárolási szakaszban történő információtorzulásnak két alapvető tényező befolyásolja: az esemény megtörténte és felidézése között eltelt időszak, valamint az eseményt követő tapasztalatok.

Általánosságban kijelenthető, hogy ha egy tanúvallomás az eseményt követően pár héten belül történik, akkor sokkal nagyon részletességgel és pontossággal lehetséges felidézni a történeteket. Azonban tudjuk, hogy sokszor egy adott bűncselekmény sokkal később jut a hatóságok tudomására, illetve a büntetőeljárás is évekig elhúzódhat. Ezen problémakörök nagyban befolyásolják a pontos visszaemlékezés. Azonban egy kutatás ezt az állítást is cáfolja, hiszen a kutatásukban azt állapították meg, hogy a 26. hónapot betöltött gyerekek, akik súlyos balesetet szenvedtek, – tehát részese volt az eseménynek – két év elteltével is megfelelő verbális visszaemlékezést nyújtottak.¹⁸⁹

¹⁸⁶ GÁL – NAGY i. m. 121

¹⁸⁷ GÁL – NAGY i. m. 122

¹⁸⁸ GÁL – NAGY i. m. 123

¹⁸⁹ Carole PETERSON – Regina RIDEOUT: *Memory for Medical Emergencies Experienced by 1- and 2-Year-Olds*. Memorial University of Newfoundland. 1998. <https://pubmed.ncbi.nlm.nih.gov/9779751/>

7.1.3. FELIDÉZÉS SZAKASZBAN TÖRTÉNŐ TORZULÁS A GYERMEKKORÚAKNÁL

A kihallgatáson történő pontos felidézést szintén több tényező tudja befolyásolni. Ilyen befolyásoló tényezőként lehet számon tartani a külső körülmények hatását, az átélt események jellemző hatásait, a gyermek saját (belső) tulajdonságait.

Egy tanulmány harmincnégy 8-10 év közötti gyerek vizsgálatában történő részvételéről számol be, hogy a külső hatás mennyire is tudja befolyásolni az emlékezést. A vizsgálat arról szólt, hogy a gyerekeket két csoportra osztották, és a gyerekek egyik felét egy nagyobb egyetem jogi karának próbabírószági termében, felét pedig az iskolájában kérdezték ki. Fontos, hogy mindkét helyszínen ugyanaz a személy volt a kérdező. Az eredmény az lett, hogy akiket a tárgyalóteremben kérdeztek ki, ők gyengébb memóriateljesítményt mutattak, mint azok, akiknél az iskolában történt a kikérdezés. A bírósággal kapcsolatos bizonyos élményeket stresszesebbnek értékelték, mint az iskolában megkérdezett társaik.¹⁹⁰ Mivel a tanú kihallgatása – mint már az előzőekben írtam – az egyik legfontosabb bizonyítási eszköz, ennek érdekében a Be. is rendelkezik a tanú kihallgatásánál arról, hogy „Az egyesbíró vagy a tanács elnöke a különleges bánásmódot igénylő tanú védelme érdekében [...] a tárgyalóteremből eltávolíttatja azt a vádlottat vagy a hallgatóságot közül azt, akinek jelenléte a különleges bánásmódot igénylő tanút a kihallgatása során zavarná [...]”.¹⁹¹ További nagyon fontos körülmény tud lenni maga a kihallgatás módja, a kihallgatási technikája. Torzuláshoz vezethet az, ha nem a megfelelő módon történik a kérdezés.¹⁹²

Nagy jelentősége van annak, hogy a tanúvallomástételkor milyen fejlődési áll (például hogyan tudja kifejezni magát stb). Tudjuk, hogy a gyermekek által használt szavak nem minden esetben jelentik azt, amire mi felnőttek elsőre gondolnánk. Ezért, ha a gyerek a kihallgatás során ugyan rendelkezik a megfelelő nyelvtani készségekkel és megfelelően ki tudja magát fejezni, érdemes megkérdezni, hogy pontosan, egy általa használt kifejezés alatt mit ért.¹⁹³

Összességében tehát elmondható, hogy egy gyermekkorú viszonylag hosszú időn keresztül képes felidézni eseményeket, azonban a büntetőeljárás sikeressége érdekében olyan szakembereket kell alkalmazni, akik az ezen pont alatt lévő helyzeteket megfelelően kezelni tudják.¹⁹⁴

¹⁹⁰ Karen J. SAYWITZ – Rebecca NATHANSON: *Children's testimony and their perceptions of stress in and out of the courtroom*. USA. 1993. 613 <https://www.sciencedirect.com/science/article/pii/014521349390083H>

¹⁹¹ Be. 526. § (3)

¹⁹² GÁL – NAGY i. m. 126

¹⁹³ GÁL – NAGY i. m. 129

¹⁹⁴ GÁL – NAGY i. m. 132

7.2. A SZAKVÉLEMÉNY

7.2.1. BIZONYÍTÉK, MINT ALANYI OLDAL

Mint az összes bizonyítási eszköz, úgy maga a szakvélemény is felfogható részbizonyításként.¹⁹⁵ Megkülönböztethetünk funkcionális és strukturális oldalt. A funkcionális oldalról már szoltam korábban, ez esetben csak annyit kívánok megjegyezni, hogy akkor kerül sor szakértő alkalmazására, ha az különleges szakértelmet igényel az ügy eldöntéséhez szükséges tény megállapítása. Ebből a funkcionális megközelítéséből pedig látható, hogy a szakértő szerepe, funkciója közel áll a bíróéhoz (szokták is a szakértőt nevezni ténybírónak).¹⁹⁶ „A szakértőnek különleges a feladata és a helyzete, hogy a részletek, szakmai mozzanatok feltárásában is közreműködjék.”¹⁹⁷ Azonban a szakértő átfoghat ügyészi tevékenységet is, hiszen gyakran csak a szakértő fedez fel az ügy szempontjából releváns tényeket.

7.2.2. BIZONYÍTÉK, MINT TÁRGYI OLDAL

„Maga a szakértés önmagában olyan közvetett és összetett megismerési folyamat, amelynek során a szakértő vizsgálatot végez, szakmai tényeket állapít meg és következtetéseket von le.”¹⁹⁸ A szakértői vizsgálat eredménye, azaz a szakvélemény, tulajdonképpen csak egy bizonyíték a bűnügy szempontjából, amelynek két oldala van: a formai és a szakmai. Formai szempontból fontos, hogy a szakvélemény törvényes forrásból származzon, ami jelenti azt is, hogy a szakértőt szabályosan vegyék igénybe, legyen megfelelő akkreditációja, és tágabb értelemben különleges műszerekkel, felszerelésekkel rendelkezzen. Tartalmilag a szakértő általában vizsgálati anyagot kap, amelyet elemez, kimutatásokat és értékeléseket készít, hogy alapos megállapításokhoz tudjon jutni.¹⁹⁹

7.3. ELEKTRONIKUS ADAT

Szükségnek tartom pár alapvető fogalom tisztázását, melyeknek egy elektronikus térben elkövetett bűncselekmény esetében elkerülhetetlen az ismeretük.

Az adat informatikai értelemben „egy vagy több jeltől álló sorozat, amelynek értelmét meghatározott értelmezési folyamat(ok) adják meg [...]”.²⁰⁰ A digitális adat pedig egy adott „információ diszkrét, nem folytonos ábrázolása.”²⁰¹ Ezen digitális adatokat binárisan – kettes számrendszeren – ábrázolják, és a digitális adatok a magyar jogi nyelvben elektronikus adatok.

¹⁹⁵ TREMMEL Flórián: *Bizonyítékok a büntetőeljárársban*. Dialóg Campus Kiadó. Budapest-Pécs. 2006. 129

¹⁹⁶ Uo.

¹⁹⁷ Uo.

¹⁹⁸ Uo.

¹⁹⁹ TREMMEL i. m. 130

²⁰⁰ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 8

²⁰¹ Uo.

A digitális vagy elektronikus bizonyíték minden olyan digitálisan tárolt, feldolgozott vagy továbbított adat, amely bizonyító értékkel bír.²⁰² Digitális eszköznek számít minden „digitális adatok feldolgozására és / vagy tárolására használt (elektronikus) berendezés [...]”.²⁰³

Egy digitális térben elkövetett bűncselekmény esetén is megjelennek azon alapelvek, melyeknek minden körülmény között érvényesülniük kell. Ezen alapelvek a következők: átláthatóság, eredetiség, megbízhatóság, megismételhetőség, ismételt előállíthatóság. Az átláthatóság egy olyan elvárás, amely „a nyitottság, a nyomonkövethetőség, és az ellenőrizhetőség követelményeit foglalja magában.”²⁰⁴ Az eredetiség úgy gondolom egyértelmű, tehát hogy az adott tárgyat, amelyet vizsgálat tárgyává kell tenni, azt eredeti állapotában megőrizve szükséges vizsgálni. A megbízhatóság alapelve akkor fog teljes körűen teljesülni, ha „az adott vizsgálati eljárások eredménye megismételhető és ismételt előállítható.”²⁰⁵ Megismételhetőség és az ismételt előállíthatóság közös jellemzője, hogy azonos eredmény fog születni a vizsgálat során, a különbség e két alapelv között az, hogy míg a megismételhetőség azonos környezetben, addig az ismételt előállíthatóság különböző vizsgálati környezetben ad azonos eredményt.²⁰⁶

Elektronikus adatnak minősül „a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”²⁰⁷

8. GYAKORLATI KIHÍVÁSOK A NEMZETKÖZI BŰNÜGYI EGYÜTTMŰKÖDÉSBEN

Az IP cím „egy egyedi azonosító számsor, amelyet a számítógépes eszközökhöz rendelnek, hogy az interneten keresztül képesek legyenek felismerni egymást és adatokat küldeni egymás között.”²⁰⁸ Ezek az IP címek általában földrajzi területekhez köthetőek. Ebből következőleg meghatározhatóak lehetnének egy-egy bűncselekményeknek az elkövetési helye. Viszont a probléma, hogy a bűncselekmény elkövetője vagy nem a saját IP címét használja, valamint az IP címet nagyon könnyen ki lehet cserélni egy másik IP címre, ezzel „támadás úgy tűnik, mintha más helyről érkezne, mint ahonnan valójából származik.”²⁰⁹ Az a megoldás is rendelkezésre áll az elkövetők számára anonimitásuk megőrzésére, hogy privát vagy publikus proxy szervert

²⁰² GROPENEANU – IACOB op. cit. 10

²⁰³ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 9

²⁰⁴ MÁTÉ – DARABOS – MORBER – SÁNDOR i. m. 12

²⁰⁵ Uo.

²⁰⁶ Uo.

²⁰⁷ Be. 205. § (1)

²⁰⁸ TÓTH – GÁSPÁR i. m. 145

²⁰⁹ Uo.

használnak. A publikus proxy szerverek könnyen elérhetőek, azonban mivel sokan használják, ezért nagyon leterhelt a szerver, lassúak és nem megbízhatóak. „A leggyakrabban használt és a leghatékonyabb technika az előbbieket mellett, amikor távvezérléssel átveszik az irányítást egy idegen országban található eszköz felett és erről indítják meg a támadást a harmadik fél irányába.”²¹⁰

8.1. GARY MCKINNON ÜGY

Gary McKinnon, egy munkanélküli számítástechnikai adminisztrátor az Egyesült Királyságból, jogosulatlanul hozzáfért 97 amerikai kormányzati számítógéphez londoni otthonából. Műveletei során adatokat törölt ezek operációs rendszereiből, aminek következtében több mint 2000 washingtoni számítógépet kellett leállítani az amerikai hadseregben 24 órára. 2002 novemberében New Jersey és Virginia állam vádat emelt McKinnon ellen. Az amerikai kormány vádalkut ajánlott, amelyben McKinnon bűnösnek vallotta volna magát, és kiadatását elfogadta volna. Ennek részeként 37-46 hónapos börtönbüntetést kapott volna, amelyből 6-12 hónap letöltése után hazatérhetett volna, hogy büntetése hátralévő részét az Egyesült Királyságban töltsse le. Ezt követően az angol jogszabályok alapján 18-24 hónapot kellett volna ténylegesen letöltenie. Ha azonban nem működött volna együtt, akkor 8-10 év börtönbüntetés várt volna rá, a hazatérés lehetősége nélkül, amelyet egy magas biztonságú börtönben kellett volna letöltenie, és ebből a büntetésnek csak 15%-át engedhették volna el.²¹¹ Azonban 2004-ben McKinnon visszautasította a vádalkut, ezért Virginia és New Jersey állam is elfogatóparancsot adott ki ellene, és a külügyminisztertől kérvényezték a kiadatását. A kérvények elfogadása után, 2005. június 7-én McKinnont letartóztatták. A meghallgatások sorozata után, 2006-ban a külügyminiszter kiadta a parancsot a kiadatására. McKinnon 2008-ban fellebbezett a kiadatási döntés ellen, de a Lordok Háza elutasította a fellebbezését.²¹² 2012-ben azonban Theresa May belügyminiszter visszavonta a kiadatási parancsot, mivel McKinnonnál Asperger-szindrómát diagnosztizáltak, és a szakértők szerint fennállt az öngyilkosság veszélye, ha kiadatják az Egyesült Államoknak.²¹³

8.2. IVANOV ÉS GORSHKOV-ÜGY

„Az amerikai kormány állítása szerint Aleksey Vladimirovich Ivanov 2000-ben feltörte az Online Information Bureau, Inc. (OIB) számítógépes rendszerét és megszerezte azon

²¹⁰ Uo.

²¹¹ Nicola PADFIELD: *Shining the Torch on Plea-Bargaining*. The Cambridge Law Journal 2009/1. <https://bit.ly/3zSNSMs>

²¹² TÓTH – GÁSPÁR i. m. 146

²¹³ Megtekintés: 2024. október 29. <https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition>

kulcsfontosságú jelszavakat, amelyekkel irányítása alá tudta vonni az OIB teljes rendszerét.”²¹⁴ A vád szerint Ivanov ezután azzal fenyegett, hogy teljesen tönkreteszi a számítógépes rendszerét a vállalatnak, és körülbelül 10 000 amerikai dollárt követelt annak fejében, hogy ezt ne tegye meg. Miután a követelését elutasították, ismét fenyegető üzenetet küldött az OIB-nek, amelyhez az oroszországi tartózkodása alatt a Washington államban, Kirkland városában működő Lightrealm internetes szolgáltatórendszerét használta fel, és az e-mailt egy Connecticut államban, Vernonban dolgozó OIB-alkalmazottnak címezte.²¹⁵ „Az FBI ügynökei úttörő módon derítették fel az elkövetőket, aminek részeként üzletembernek álcázva Seattle-be csalogatták a két orosz hackert egy állásinterjúra.”²¹⁶ Az interjú során egy olyan számítógépen kellett bizonyítaniuk informatikai tudásukat, amelyre előzetesen kémprogramokat (spyware) telepítettek. Ezzel a programmal megszerezték a hackerek jelszavait, amelyekkel hozzáfértek saját számítógépükhöz. Később a szövetségi ügynökök ezeket az adatokat lementették, és a büntetőeljárás során bizonyítékként használták fel ellenük.²¹⁷ Ivanov és Gorshkov ellen online elkövetett számítógépes csalás, összeesküvés, zsarolás, továbbá eszközökhöz való jogosulatlan hozzáférés miatt emeltek vádat az USA-ban. „Ivanov azzal érvelt, hogy mivel az említett bűncselekmények elkövetésének idején Oroszországban tartózkodott, így nem terhelhetik az Egyesült Államok törvényeinek megszegésével.”²¹⁸ A bíróság viszont azt állapította meg, hogy az ügy kapcsán rendelkezik joghatósággal, tehát ezért az Oroszországban elkövetett cselekményei szándékosak és ezen cselekményeinek negatív hatása az USA területén következtek be. Továbbá a Kongresszus azzal is érvelt, hogy „minden anyagi jogi tényállás [...] területtől függetlenül alkalmazandóak.”²¹⁹ Természetesen a Kongresszus döntésével az orosz hatóságok nem értettek egyet, mert véleményük szerint ezen döntés a joghatósági alapelveket megsérti, továbbá kifogás tárgya lett a nyomozási események és a bizonyítékok megszerzése is.²²⁰

9. ÚJ JOGI KIHÍVÁSOK – METAVERZUM

„A metaverzum egy megosztott, virtuális világ, amit a felhasználók bármilyen platformról képesek elérni az interneten keresztül, és ahol a virtuális avatárjaikkal tudnak kapcsolatba lépni

²¹⁴ TÓTH – GÁSPÁR i. m. 145

²¹⁵ Megtekintés: 2024. október 19. <https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/>

²¹⁶ TÓTH – GÁSPÁR Uo.

²¹⁷ Önder Kutay ŞEKER: *International Regulation of National Cybercrime Jurisdiction*. Tilburg Law School. 2012. <https://arno.uvt.nl/show.cgi?fid=127475> 10

²¹⁸ TÓTH – GÁSPÁR Uo.

²¹⁹ Uo.

²²⁰ TÓTH – GÁSPÁR i. m. 146

egymással.”²²¹ Az, hogy az emberek hogyan tudják a metaverzumon keresztül elérni egymást, két módon történhet: vagy virtuális valóság útján, vagy kiterjesztett valóság útján. Azonban ezek kombinációja is felléphet, például VR szemüveg használatával. Lényeges jellemzője, hogy saját gazdasággal rendelkezik, amely valós értéket képvisel, és összefüggésben áll a valós világ gazdasági folyamataival. „A metaverzumot a gyakorlatban használják a számítógépes játékokban, közösségimédia-platformokon, [...] digitális könyvtárakra, és az e-kereskedelmet is forradalmasítja a virtuális bevásárlóközpontokkal.”²²² A metaverzum jelenség több jogi kérdést is felvet (adatvédelem, polgári jogi szabályok, hogyan kell egy metaverzum világában elkövetett bűncselekmény esetén eljárni stb). A kibertámadások megelőzésére speciális intézkedéseket kell alkalmazni. „A hiányos adatbiztonsági intézkedések növelik az adatvédelmi incidensek kockázatát – ezeknek az egyik legsúlyosabb következménye pedig a felhasználó avatarjával való visszaélés és a személyiséglopás.”²²³

A virtuális erőszak fogalma nem újkeletű dolog. Már 1993-ban felmerült ez a fogalomhasználat, amikor is egy *'LambdaMoo'* elnevezésű felhasználó más avatárokat kényszerített arra, hogy szexuális cselekményeket írjanak le és szexuális módon viselkedjenek. A károkozás megtörtént, azonban büntetőjogi felelősségre vonásra nem került sor, hiszen hiányoztak a nemi erőszak tényállási elemei, mint például magának a behatolás ténye.²²⁴ Általában egy női avatar jelenik meg az áldozati oldalon. Az elkövetők viszont az online térben úgy érzik, hogy bármit megtehetnek, hiszen hatalomra tesznek szert, ahol pedig korlátlanul cselekedhetnek – legalábbis azt hiszik. Felmerülhet a kérdés, hogy ezek a személyesen átélt esetek szexuális erőszaknak vagy zaklatásnak minősíthetők-e büntetőjogi szempontból, mert igazából fizikailag érintkezés nem történik.

A virtuális és a valós világ közötti határok egyre inkább elmosódnak. Nina Jane Patel a kutatásai részeként 2021 decemberében létrehozott egy profilt a Metaversen. A belépést követő 60 másodpercen belül három-négy férfi verbálisan és szexuálisan zaklatta. Amikor női avatarját megérintették a játékban, érezte, hogy a kézi vezérlője vibrál. A VR-headsetek és a kézi vezérlők által biztosított panorámakép, a hang és az érintésszimuláció multiszenzoros élményt nyújt, elmosva a virtuális és a fizikai közötti elválasztást.²²⁵ Azonban sajnos ez nem ér véget,

²²¹ HORVÁTH Katalin: *A metaverzum jogi kérdései – 1. rész*. Wolters Kluwer. 2022. június 22. Megtekintés: 2024. október 15. <https://jogaszvilag.hu/szakma/a-metaverzum-jogi-kerdesei-1-resz/>

²²² Uo.

²²³ DOMOKOS Márton: *A metaverzum jogi kérdései – 2. rész*. Wolters Kluwer. 2022. június 23. Megtekintés: 2024. október 15. <https://jogaszvilag.hu/szakma/a-metaverzum-jogi-kerdesei-2-resz/>

²²⁴ Carlotta RIGOTTI - Gianclaudio MALGIERI: *Sexual violence and harassment in the metaverse: A new manifestation of gender-based harms*. Megtekintés: 2024. október 15. <https://bit.ly/3BlzgZn> 8

²²⁵ Junmo YOON: *Can We Do Anything About Sexual Crimes in the Metaverse?* Loyola University Chicago School of Law. 2022. október 6. <https://blogs.luc.edu/compliance/?p=4849>

amikor a felhasználók leveszik a headsetet. Az áldozatokat ugyanaz a szorongás, pánikroham és esetleg depresszió éri, mint a valós áldozatokat.²²⁶ Naivitás lenne azt gondolni, hogy a fizikai világ legsötétebb részei nem fognak tükröződni a virtuális világban. A hatások nagyobbak, mint egy vállalat szolgáltatási feltételeinek megszegése, és a következményeknek súlyosabbaknak kell lenniük, mint a platformról való kitiltás. A platformoknak és a jogalkotóknak meg kell osztani a jogi felelősséget, ha valami rosszul sül el. Ha az avatarok a valós világ embereit képviselik, akkor a valós világ biztonsági intézkedéseit is be kell vezetni minden felhasználó védelme érdekében.²²⁷ A nők jogainak védelméért elsődlegesen egyértelműen az államnak kell felelősséget vállalnia, Szükség van továbbá olyan nemzetközi jogra, amely előírja az államok számára, hogy nemzeti jogszabályokat és mechanizmusokat fogadjanak el, amelyek kötelezik a technológiai vállalatokat arra, hogy biztosítsák az emberi jogok előmozdítását és védelmét a különböző platformjaikon.²²⁸

Végezetül pedig pár nyitott kérdés: Perelhető-e és ki a metaverzumban egyik avatárral a másik avatar ellen elkövetett jogsértésekért? Milyen jogai vannak a metaverzumban virtuális telket/területet/ingatlant vásárló felhasználóknak ezeken a területeken? Beléphet-e más felhasználó az avatarjával engedély nélkül az ilyen területekre a metaverzumban? Sérül-e az avatárt létrehozó természetes személy személyhez fűződő joga, ha az avatarja jóhírnevét sértik a metaverzumban?²²⁹ Megannyi kérdés van, amelyekre még nincsenek sem jogszabályok, sem bevett joggyakorlatok, és ezek közül csak néhányat lehet rendezni a metaverzum szolgáltatói által meghatározott általános felhasználási feltételekben.

10. ÖSSZEGZÉS ÉS 'DE LEGE FERENDA' JAVASLATOK

Amint látható volt, számos problémával kell megküzdenie a büntetőeljárásnak az online térben elkövetett bűncselekmények esetén. A teljesség igénye nélkül a '*de lege ferenda*' javaslatok a következők lennének:

- az online térben elkövetett bűncselekmények elkövetési helyének egységes, nemzetközi meghatározása a joghatóság részére az egyértelműbb megállapítás céljából
- az online bűncselekmények határon átvétele okán egységes szabályozásra törekvés nemzetközi szinten

²²⁶ Uo.

²²⁷ Uo.

²²⁸ RIGOTTI – MALGIERI i. m. 23

²²⁹ HORVÁTH K. i. m.

- a büntetőeljárási törvényben egy külön fejezet az online térben elkövetett bűncselekményeknek (ezzel megakadályozva az analógia alkalmazását – például lopás esetén kiterjeszteni az értelmezést az online lopásra)
- folyamatos, korral és változásokkal, az elkövetőkkel lépést tartó képzés biztosítása az erre a területre specializálódott személyeknek
- a digitális tudatosságra törekvés fejlesztése a felhasználók számára

III. FEJEZET – A KIBERBIZTONSÁG ÉS A MESTERSÉGES INTELLIGENCIA

1. BEVEZETÉS

Elsősorban fontosnak tartom, hogy valamiféle definíció legyen megfogalmazva a mesterséges intelligenciára. A mesterséges intelligencia (a továbbiakban: AI) egy számítógépes programnak tekinthető, mely rendelkezik emberi magatartásokkal, mint például a tanulással, gondolkodással, vélemények megfogalmazására.

1.1. AZ AI ELŐNYEI ÉS HÁTRÁNYAI

Az AI használatának számos előnyét tudjuk felsorakoztatni egymás mellé. Előnyök közé tartozik, hogy a nap 24 órájában a rendelkezésünkre áll (például az online ügyfélszolgálati chatrobotok). Egy embernek, hogy produktív tudjon maradni, kellenek szünetek, kellenek szabadnapok, míg az AI-nak erre nincs szüksége. Ebből következően, az AI használata csökkenteni tudja az ember által okozott hibák számát, erre „csak” a megfelelő programozás szükséges. Egy, a mai modern világban elképzelhetetlen lenne, hogy egy autógyárban ne dolgozzanak robotok, melyek a megfelelő programozás után ugyanazt a mozdulatsort képesek végrehajtani. További előnyként említendő, hogy segítséget vagy tanácsot tudunk kérni, érzelemmentesen tud egy dönteni, míg ugye az embert el tudják ragadni az érzelmei.²³⁰

Azonban az érzelemmentes döntések hátrányként is jelentkezhetnek, ugyanis az emberek közötti kapcsolatot egyszerűen nem lehet gépekkel helyettesíteni. Hátrányként jelentkezhet, hogy egyes szakterületek, munkaterületek végzését teljes mértékben a robotok veszik át, ezzel a munkanélküliség is megnövekedhet. Természetesen meg kell említenem a dolgozat témájából kifolyólag is, hogy AI használatával számos bűncselekmény áldozatai lehetünk, ha nem vagyunk elég körültekintőek.

1.2. AZ AI ÉS A KIBERBIZTONSÁG KAPCSOLÓDÁSA

Az AI és a kiberbiztonság szorosan összefonódott az évek során, hiszen az AI hozzájárult a hatékony védekezési rendszerek kialakításához, valamint támogatta az elemzők munkáját a folyamatosan változó globális fenyegetettségi környezetben. Az AI első generációja szabályalapú rendszerekre épült, amelyek az emberi operátorok által előre meghatározott szabályok alapján figyelték a hálózati forgalmat és a felhasználói tevékenységeket. Ezek a rendszerek ugyan képesek voltak riasztásokat generálni, de számos korláttal rendelkeztek.²³¹

²³⁰ Megtekintés: 2024. december 23. <https://bit.ly/4iS8TIw>

²³¹ VALTER Krisztián – VADÁSZ Gábor: *A mesterséges intelligencia szerepe a kiberbiztonságban: hogyan észleljük és előzzük meg a támadásokat?* BDO Magyarország. 2024. április 15. Megtekintés: 2024. december 23. <https://bit.ly/3ZR9S2V>

Az AI második hulláma, amely a 20. század végén vált elterjedtté, a gépi tanulás fejlődésének köszönhetően jelentős előrelépést hozott a kiberbiztonságban. Ez az új megközelítés lehetővé tette, hogy az AI saját maga állítsa be a szabályok határértékeit, csökkentve az emberi beavatkozás szükségességét. A gépi tanulás mellett a deep learning algoritmusok integrációja is tovább növelte az AI hatékonyságát a fenyegetések felismerésében és kezelésében.²³²

A jelenlegi, harmadik generációs AI új szintre emelte a kiberbiztonságot. A harmadik generációs AI képes automatizálni az ismétlődő feladatokat, csökkenteni az emberi hibákat, és prediktív analitikát alkalmazva segíti a fenyegetések korai felismerését, továbbá lehetővé teszi a kiberbiztonsági csapatok számára, hogy gyorsan reagáljanak a támadások elhárítására.²³³

2. AI HASZNÁLATÁVAL ELKÖVETHETŐ EGYES NEGATÍV MEGÍTÉLÉSŰ CSELEKMÉNYEK

Az AI a sok új lehetősége mellett jelentős számú kihívásokat is teremtett a kiberbiztonság tekintetében. Ide sorolhatóak az ezen pont alatt tárgyalandó esetek is – például a deepfake. Azonban adatvédelmi szempontból is jelentős kihívásokkal kell szembenéznünk, ugyanis egy AI rendszer által kezelt óriási adathalmaz esetleges kiszivárgása komoly kockázatokat hordoz maga után – gondoljunk csak az egészségügyi vagy a pénzügyi adatokra. Ez pedig adatvédelmi incidensekhez vezethet, amely veszélyeztetheti az emberek magánéletét, valamint társadalmi és gazdasági károkat is okozhatnak.

Az AI rendszert kártékony programoknak a fejlesztésében is alkalmazzák, melyből következik, hogy újfajta veszélyek megjelenését hordozza magával.

2.1. ADATHALÁSZAT

A mai, harmadik generációs AI esetében már nem nagyon tudjuk megkülönböztetni egy ember, vagy egy gép által írt adathalász emailt vagy üzenetet. Az adathalászattól évről évre növekvő tendenciát mutató cselekmény. Egy 2023-es információ alapján a bejelentett adathalász tartalmak 2021-hez képest 2022 végéig 61%-kal nőttek meg.²³⁴ Az AI-val egyszerűen, nagyon gyorsan lehet egy adathalász email megírni, ugyanis különböző utasítások alapján írja meg azt, valamint bármely más nyelvre le is tudja fordítani, valamint a hackerek több megfogalmazásban lévő emailt hozhatnak létre az AI segítségével, hiszen korlátlanul a rendelkezésükre áll.

²³² Uo.

²³³ Uo.

²³⁴ CYBER Report: *Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them.* 2023. január 7. Megtekintés: 2024. december 23. <https://www.cnn.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html>

Az Amerikai Egyesült Államokban 2023-ban messze kiemelkedően az adathalászat volt a leggyakoribb típusa a kibertámadások közül. Ez számokkal leírva azt jelenti, hogy az adathalászat közel háromszázezer, míg a második helyen álló cselekmény nagyságrendileg ötvenötezer bejelentett elkövetést jelent.²³⁵

Véleményem szerint ez a szám nem fog csökkenni mindaddig, amíg az internet felhasználók zöme nem tudatosan használja az egyes platformokat, és amíg a legtöbb esetben igaznak vélnek, amit az interneten találnak. Ezt az emberi hiszékenységet a támadók, hackerek előszeretettel használják ki.

2.2. DEEFAKE TECHNOLÓGIÁK ALKALMAZÁSA

„A deepfake olyan digitális manipuláció, amellyel kép- illetve hangfelvétel tartalmakat állítanak elő a mesterséges intelligenciát alkalmazó technológia segítségével a valóságtól eltérő tartalommal és valamely szándékolt hatás elérése érdekében.”²³⁶

Ezen jelenség terjedése leggyorsabban az egyes közösségi platformokon valósul meg. Gondoljunk csak bele, hogy manapság mikor megnyitjuk a Meta alkalmazását, találkozni fogunk AI által generált képpel, amelynek a felhasználóközösség egy része elhiszi a valódiságát. Maga a „deepfake-jelenség 2017-ben indult hódító útjára a Reddit fórumon, ahol az egyik felhasználó egy pornósztár arcát egy híres színésznőével helyettesítette.”²³⁷

A deepfake technológiát jelenleg elsősorban pornográf tartalmak előállítására használják, amelyeket a készítők különböző nyílt és darkwebes platformokon kereskednek. Deepfake áldozatául bárki válhat, azonban leggyakrabban ismert, celeb személyekre nézve jelent veszélyeket.²³⁸

Egy 2022-es esetről egy hacker csoport az egyik legnagyobb kriptovaluta (Binance) tőzsdéjének főigazgatójáról – Patrick Hillmanról – készített deepfake felvételt. Ezzel a deepfake felvétellel több, Binance ügyfelet tévesztettek meg.²³⁹ 2022 márciusában egy videó jelent meg, amelyen Volodimir Zelenszkij ukrán elnök beszédet mond. A felvétel gyorsan elterjedt az ukrán és orosz közösségi médiában, azonban a zavaros képsorokon Zelenszkij szokatlan

²³⁵ STATISTA: *Most commonly reported cybercrime categories in the United States in 2023, by number of individuals affected*. Megtekintés: 2024. december 23. <https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-us/>

²³⁶ SZALAY Klára: *Deepfake, azaz mélyhamisítás: technológia és jog*. Infojegyzet. 2024/20. Megtekintés: 2024. december 23. https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog

²³⁷ NMHH: *Egyéni és társadalmi kockázata is van a deepfake-nek*. 2023. január 13. <https://bit.ly/3Pa4IKw>

²³⁸ NEMZETI Kibervédelmi Intézet: *Mekkora fenyegetést jelentenek valójában a deepfake-ek?* CTI jelentés. 2022 <https://bit.ly/40i3bst> 13

²³⁹ NEMZETI i. m. 15

arckifejezéssel arra szólítja fel az ukrán katonákat, hogy tegyék le a fegyvert. Ez a videó elérhető, látható, azonban még is deepfake technológiával készült.²⁴⁰

Az Európai Parlament idén elfogadott [A mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról] szabályozásának 52. cikkének 3. bekezdése vonatkoztatható a deepfake technológiával készült tartalmakra. Ezen jogszabályhely alapján:

„Azon MI-rendszerek felhasználói, amelyek olyan, meglévő személyekre, tárgyakra, helyekre vagy más szervezetekre vagy eseményekre érzékelhetően hasonlító képet, audio- vagy videotartalmat generálnak vagy manipulálnak, amely egy személy számára megtévesztő módon eredetinek vagy valóságosnak tűnhet („deepfake”), közlik, hogy a tartalmat mesterségesen hozták létre vagy manipulálták.”²⁴¹

A szabályozás fokozatosan lép majd hatályba, 2026-ra a teljes szabályrendszer hatályos lesz.

2.3. BOTNETEK

A Botnet „egy fertőzött informatikai eszközökből álló hálózat, amelyet a botnet gazdája többféle károkozásra is alkalmazhat.”²⁴² A fertőzött munkaállomások főként kényszerű levelek kiküldésére, szolgáltatásmegtagadási támadások indítására, valamint szenzitív adatok, például banki információk eltulajdonítására használhatók.

A támadónak először hozzáférést kell szereznie az áldozat eszközéhez, amit számos módon megvalósíthat. Az egyik gyakori módszer az ún. exploit kitekkel történő fertőzés, amely során a támadó egy weboldal sérülékenységeit kihasználva automatikusan telepíti a káros kódot (botot) a weboldalt meglátogatók eszközeire. Egy másik elterjedt technika a rosszindulatú programokat tartalmazó kényszerű e-mailek használata. Bár a célpontok hagyományosan asztali számítógépek, egyre gyakrabban kerülnek célkeresztbe IP-kamerák, mobiltelefonok és routerek is.²⁴³

Védekezni úgy tudunk, hogy rendszeresen frissítjük szoftvereinket, tűzfalat vagy egyéb vírusvédelmi szoftvert telepítünk, valamint biztonság tudatos magatartást tanúsítunk az internet használata során.²⁴⁴

²⁴⁰ GOSZTONYI Gergely – LENDVAI Gergely: *Deepfake és dezinformáció. Mit tehet a jog a mélyhamisítással készített álhírek ellen?* Médiakutató. 2024 tavasz, XXV. évf. 1. szám. <https://bit.ly/3ZRteF5> 43

²⁴¹ EURÓPAI Bizottság: *A mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról*. IV. cím, 52. cikk, (3) bekezdés. Megtekintés: 2024. december 23. <https://bit.ly/3P9OQrr> 77

²⁴² NEMZETI Kibervédelmi Intézet: *Robothálózat (Botnet)*. 2020. március 9. Megtekintés: 2024. december 23. https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/?utm_source=chatgpt.com

²⁴³ Uo.

²⁴⁴ Uo.

2.4. ÖSSZEGZÉS

Mint látható, számos módon kiszolgáltathatjuk úgy az adatainkat, hogy nem tudtunk róla, figyelmetlenek voltunk. Gyakran mondják, hogy egy adott platformra történő regisztrálás ingyenes, azonban valójában a regisztrációkor „fizetünk”, méghozzá a személyes adataink megadásával. Fokozott figyelmet kell szentelni, hogy kinek, hol, milyen körülmények között adjuk meg adatainkat, az internet felhasználókban ezen digitális tudatosságot növelni kell.

3. AZ AI HASZNÁLATA A PÉNZÜGYI, VALAMINT A KIBERBIZTONSÁG TERÜLETÉN

3.1. PÉNZÜGYI SZEKTOR

Az AI használata a pénzügyi, illetve a kibervédelmi szektorban meglehetősen előnyös támogatási lehetőséget nyújt. A csalások elleni küzdelem – amely az elmúlt időszakban meglehetősen elszaporodottnak mondható -, az adatvédelem és a kibertámadások megelőzése is olyan területnek mondható, amelyeknél az AI, valamint az automatizált rendszerek segítséget biztosíthatnak.²⁴⁵ „A kiberbiztonság az egyik legfontosabb kihívás az információs technológia korában, amely különösen fontos a pénzügyi szektorban, ahol a biztonság kulcsfontosságú az ügyfelek és az intézmények számára egyaránt.”²⁴⁶

Vannak olyan ajánlottan követendő szabályok a pénzügyi szektorban., mint például a kétlépcsős azonosítás alkalmazása, a megfelelő, azaz az erős jelszó alkalmazása, vírusvédelmi szoftverek alkalmazása és még lehetne sorolni. Az AI meglehetősen sok területen képes segíteni a pénzügyi szektoron. Megemlítenéd e körben a jelentéskészítést (az AI képes elemzéseket készíteni, amelyek a kiberbiztonsági csapatokat támogatja a rendszerek sebezhetőségeinek megértésében vagy ezen területek azonosításában), adathalászat észlelése, gyorsabb válaszreakció, vagy esetleg az automatizált válaszok (lehetőség van automatizált válaszok létrehozására, amelyek reagálnak egy biztonsági fenyegetésre).²⁴⁷

Az elmúlt években több elemző beszámol arról, hogy az AI egyre több teret kap a kiberbiztonságban – így a pénzügyi szektorban is. Így sok intézmény most már az AI használatával végzik el a rendszereik védelmének az erősítését. A fejlődő gépi intelligencia egyszerre nagy mennyiségű adatot képes elemezni, így képes észrevenni az esetlegesen felmerülő problémákat, amelyek a kiberfenyegetésekre utalhatnak. Természetesen ezen rendszerek napjainkban folyamatosan fejlődnek, tanulnak az újonnan megjelenő fenyegetésekből, és így hatékonyabbá válnak a támadások felismerésében. Továbbá valós idejű

²⁴⁵ BAGÓ Péter: *Kiberbiztonság és a mesterséges intelligencia kapcsolata*. Gazdaság és pénzügy. 10. évfolyam. 2. szám. 2023. június. Megtekintés: 2023. december 25. <https://bankszovetseg.hu/Public/gep/2023/196-221%20Bago.pdf> 196

²⁴⁶ Uo.

²⁴⁷ BAGÓ i. m. 196-198

információkat biztosítanak a fenyegetésekről, amely lehetővé teszi a pénzügyi intézetek számára a gyors reagálási lehetőséget. Automatizálásra is kiválóan alkalmazhatóak, így a rutinszerűvé vált feladatok elvégzésével a szakembereket tehermentesíti, így több idő jut az emberi szakértelmet igénylő, összetettebb problémák megoldására. Azonban felmerülnek aggodalmak is az AI használatával, elsősorban a megbízhatóságával. Így, mivel az AI olyan adatokkal képes „dolgozni”, amelyeket korábban az emberek vittek fel a rendszerbe, ezért ezen adatoknak a helyessége (mert az adatok változhatnak), védettsége nagyfokú felelősségvállalást kíván meg. Összességében tehát elmondható, hogy számos előnyt nyújt a pénzügyi szektorban az AI alkalmazása, azonban ehhez adatvédelmi, valamint felelősségbiztosítási intézkedéseket kíván meg.²⁴⁸

3.2. KIBERBIZTONSÁG TERÜLETE

Tagadhatatlan, hogy a kiberbiztonság területén az AI használata értékes eszköz lett, ugyanis segíthet jelezni, megelőzni, valamint beazonosítani egy adott fenyegetést.²⁴⁹ A következőkben az egyes kapcsolódási területeket fejtem ki.

Csalások felderítése: maga az AI mintázatokat, kapcsolódási pontokat tud beazonosítani valamennyi adat között, amelyek egy ember által történő vizsgálat esetén elkerülhetik a figyelmet. Ennek folyamán az AI hozzájárul a csalási kísérleteknek a gyorsabb felismeréséhez.

Támadásdetektálás: ahogy korábban is szó esett róla, egy AI alapú rendszer elképesztően nagy adatállományt képes elemezni, ezzel különbséget tud tenni egy átlagos, ismétlődő cselekmény és egy gyanús, veszélyeztető cselekmény között. A második fordulat bekövetkezte esetén pedig képesek riasztást generálni.

A riasztáskezelési kapcsolódási terület összefügg az előzőkben vázoltakkal, ugyanis egy AI rendszer képes minimalizálni a téves riasztások számát. Tehát a riasztások szűrésében segítségre lehet, és beazonosíthatja a valódi fenyegetéseket, amelyek viszont sürgős beavatkozást igényelhet.

Hálózati behatolásérzékelés és megelőzés: Az AI rendszerek folyamatosan tanulmányozzák a hálózati adatforgalmat, hogy felismerjék a mintázatokat, amelyek behatolási kísérletet jelezhetnek. A támadók viselkedésének elemzésével képesek megkülönböztetni a különböző hackercsoportokat.

²⁴⁸ BAGÓ i. m. 199-200

²⁴⁹ KOLLÁR Csaba: *A mesterséges intelligencia megjelenése a biztonságstudományban*. What will our Future be Like? Sozial und Wirtschafts Forschungsgruppe. Großpetersdorf. 2023. Megtekintés: 2024. december 25. <https://real.mtak.hu/170988/1/tarstudkotet2023.pdf> 249

Biztonságos felhasználói azonosítás: az AI fejlett (biometrikus) azonosításokat képes alkalmazni – példának okáért arcfelismerés vagy ujjlenyomat-azonosítás.

Spam üzenetek szűrése: az AI rendszerek mivel tanulnak, így megismerhetik a spam üzeneteknek a mintázatait, ezáltal képesek a nem kívánt tartalmat, üzenetet kiszűrni.

Eseményvizualizáció: egy harmadik generációs AI rendszer képes fénykép, - video, - hangfájl készítésére, így az AI segítségével a kiberbiztonsági eseményeket vizuális formában meg lehet jeleníteni, amely a szakemberek számára megkönnyíti az adott helyzet átlátását.²⁵⁰

4. A DEEPLCKER, VALAMINT A RAJINTELLIGENCIA MINT KIBERTÁMADÁSI MODELL

4.1. DEEPLCKER

Az IBM Research által fejlesztett DeepLocker egy új generációs, AI-alapú malware, amely több nyílt forráskódú AI-modellt kombinál ismert rosszindulatú technikákkal. A malware jelentése valamilyen rosszindulatú számítógépes program. „Ez az MI-alapú kibertámadási eszköz az úgynevezett kitérő támadások [...] új, erősen célzott fajtáját implementálja.”²⁵¹ Ezek a kitérőtechnikák olyan módszerek, eljárások, amelyeket a számítógépes támadások alkalmaznak a rosszindulatú tevékenységek leplezésére.²⁵²

A DeepLocker különlegessége abban rejlik, hogy a cél azonosításhoz olyan eseményindítókat (triggert) használ, mint például arcfelismerés, hangfelismerés, vagy esetleg helymeghatározás alapján is aktiválódhat. A DeepLocker rejtve marad ezen tevékenységek közben, továbbá még hatékonyabban is tud működni, mivel több millió rendszert tud megfertőzni úgy, hogy azt valaki észrevenné. Azonban csak akkor fog működésbe lépni, ha bármely cél közül bármelyiket beazonosítja (például, ha az adott fertőzött eszköz az adott helyre kerül).²⁵³

A DeepLocker három összetevője, amivel el tudja fedni magát:

- Az első réteg azt rejti el, hogy magát a támadást mi váltja ki (arcfelismerés, helymeghatározás stb.), így ennek a réteg feladata az, hogy a célnak a típusát elrejtse
- A második rétegnek a feladata a konkrét célnak az elrejtése (tehát például, hogy ki pontosan a támadásnak a célja, vagy hol következzen be)

²⁵⁰ KOLLÁR i. m. 249-250

²⁵¹ FEHÉR András Tibor – NÉGYESI Imre: *Mesterségesintelligencia-alapú kibertértámadási modellek*. Műszaki Katonai Közlöny. 2021. 31. évf. 3. szám. Megtekintés: 2025. január 3. https://real.mtak.hu/131737/1/05_Feher-Negyesi_73-87_MKK_2021_3.pdf 75

²⁵² Uo.

²⁵³ Uo.

- A harmadik réteg pedig a történetet fogja elrejtetni, akkor, ha a támadás bekövetkezik. Ennek a réteg feladata tehát annak az álcázása, hogy maga a támadás hogyan hajtodik végre.²⁵⁴

A DeepLockerben ezt a három rétegű elrejtést az AI modell végzi. Csak akkor fogja a triggerrel előállítani, amikor a szükséges körülmények fennállnak. Továbbá olyan sokféle módot használhat magának a cél azonosításához, hogy nagyjából lehetetlen kitalálni az AI modell ismeretében is, hogy mi a pontos kiváltási körülmény: az arc, egy adott hely vagy rendszerinformáció, vagy esetleg több kiváltási körülmény együttes fennállása.²⁵⁵

4.2. A RAJINTELLIGENCIA

„A raji intelligencia lényege, hogy nem sejtekből épül fel, mint az élő szervezetek vagy a többi MI – hanem egyedekből áll, amelyek önmagukban is működő entitások. Ezek az entitások együtt [...] hatékonyabban képesek a környezeti kihívásoknak megfelelni.”²⁵⁶ A számítástechnikai modelleknek is ugyanez a célja – tehát hogy egymást segíteni tudják. A raj hatékonysága abban rejlik, hogy nem számít, melyik entitás éri el a célt; ha valamelyik sikerrel jár, az az egész közösség eredményének tekinthető.²⁵⁷

Amikor ezt a raji modellt, elvet az online térben alkalmazzák, olyan víruskódok jönnek létre, amelyek képesek alkalmazkodni a környezetükhöz. A vírusraj egyes elemei megosztják egymással az akadályozó tényezőkre vonatkozó információkat, a szükséges módosításokat pedig maga az AI hajtja végre. Továbbá képes a rajintelligencia kollektív tudását felhasználni a kártékony kódok elrejtésére is.²⁵⁸

Így ebből megállapítható, hogy egy tömeges károkozásra hatékony tud lenni egy ilyen vírusraj, hiszen egyrészt a központi vezérlőegysége hiányzik, másodrészt a raj tanul a korábban elért sikeres és sikertelen támadásokból, harmadrészt rejtőzködésre kiválóan hasznosítható a raj alkalmazkodási tulajdonsága, és végül a raj minden tagja különböző módokon kommunikál egymással, hiszen a raj egy közösségi kommunikáció hoz létre saját maga részére.²⁵⁹ Tehát még ha a védelmi rendszernek sikerül is észlelnie és eltávolítania néhány víruspéldányt, ez nem befolyásolja a raj egészének működését.

²⁵⁴ FEHÉR – NÉGYESI i. m. 76

²⁵⁵ FEHÉR – NÉGYESI i. m. 77

²⁵⁶ Fehér – Négyesi i. m. 78

²⁵⁷ Uo.

²⁵⁸ Fehér – Négyesi i. m. 79

²⁵⁹ Uo.

5. DDoS-TÁMADÁSOK

5.1. DDoS MEGHATÁROZÁSA

Miközben a zsarolóvírusokkal, valamint a pénzügyi csalásokkal foglalkozó csoportok a legnagyobb fenyegetést jelentik a felhasználók számára, újabb fenyegetések is kezdenek megjelenni. Csak idő kérdése volt, hogy az Internet of Things (a továbbiakban: IoT) eszközöket érintő támadások megjelenjenek, elterjedjenek. 2016-ban következett be az első jelentős támadás a Mirai megjelenésével. A Mirai egy IoT-eszközökből, például routerekből és biztonsági kamerákból álló botnet. A gyenge biztonsági intézkedések miatt ezek az eszközök könnyű célpontot jelentettek a támadók számára, akik egy akkora botnetet hoztak létre, hogy az minden idők legnagyobb DDoS-támadását hajtotta végre. A Symantec 2016 során kétszeres növekedést tapasztalt az IoT-eszközök elleni támadások számában, és a csúcsidőszakokban egy átlagos IoT-eszközt kétpercenként támadás ért.²⁶⁰

A DDoS elnevezés az angol rövidítéséből ered. DoS (mint Denial of Service) során a támadás csak egyetlen egy számítógéptől származik. Viszont, ha ez a támadás összetettebb, tehát több, összekapcsolt rendszert foglal magába, egyszerre több helyről indul, akkor beszélünk DDoS-ról (azaz Distributed Denial of Service). Ebben az esetben több, a rendszert alkotó eszközök végzik párhuzamosan az adott feladatot, melyek lehetnek akár mobileszközök, számítógépek is. Az eszközök egymástól nagyobb távolságban is lehetnek.²⁶¹

„A szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat.”²⁶² Ezen szolgáltatásmegtagadással járó támadás használandó a DDoS esetében is.

A DDoS-támadás során a támadó egy hálózatot alkotó számítógépek adatcsomagjait használja fel arra, hogy túlterhelje a célba vett, általa fertőzni kívánt szervert. A támadás következtében a szerver nem lesz képes az adatcsomagok megfelelő fogadására és feldolgozására (a generált hatalmas forgalom miatt), ami akár a rendszer teljes leállítását is okozni tudja. Azonban már a jelentős lassulás is elegendő lehet ahhoz, hogy a rendszer működése megbénuljon, ugyanis a megnövekedett válaszidő jelentős zavarokat eredményez. Ezeknek a számítógépeknek, amelyeket a felhasználó tudta nélkül fertőznek meg, zombinak nevezik. A másik elnevezés a korábban kifejtett botnet, amely több botnak az

²⁶⁰ SYMANTEC: *Internet Security Threat Report*. 2017. április. Megtekintés: 2024. december 26. <https://docs.broadcom.com/doc/istr-22-2017-en> 8

²⁶¹ MEZEI Kitti: *A kibertűnözés egyes büntetőjogi szabályozási kérdései*. Doktori (PhD) értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. Pécs, 2019. <https://shorturl.at/HqnWF> 55

²⁶² Uo.

összekapcsolásával keletkező hálózatot jelenti. A botnet irányítóját egy személy esetén botmasternek, több személy esetén botherdernek nevezik. Ő az, ki a feladatokat kiosztja a megfertőzött eszközöknek.²⁶³

A botnet fertőzések ugyanúgy jutnak el az adott felhasználó számítógépére, mint bármely más fertőzés, így hangsúlyozni szükséges, hogy a korábban felvázolt biztonsági előírások igenis fontosak a biztonságos számítástechnika alkalmazásához, hiszen bármely felhasználó eszköze zombigéppé tud válni. Már az nagyon sok veszélyt rejt magában, hogy a számítógépek az internetre csatlakoznak, továbbá a következő pontban részletesebben kifejtendő IoT eszközök megjelenésével és terjedésével meglehetősen megnövekedett a kockázat.²⁶⁴

5.2. NEMZETKÖZI RENDELKEZÉSEK

A kiberbűnözés elleni küzdelem egyik alapvető nemzetközi egyezménye a Budapesti Egyezmény. Ezen dokumentum büntetendővé nyilvánítja a DDoS-támadásokat. A 4. cikk a számítástechnikai adat, míg az 5. cikk a számítástechnikai rendszer megsértésével fogalmaz meg rendelkezést. Így, a 4. cikk szerint büntetendő cselekmény a „számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése.”²⁶⁵ A rendelkezés célja, hogy a digitális világban az adatok és programok ugyanolyan védelemben részesüljenek, mint a fizikai dolgok. Az 5. cikk értelmében továbbá bűncselekménynek minősül a „számítástechnikai rendszer működésének számítástechnikai adatok bevitelével, [...] megváltoztatásával vagy megsemmisítésével való, jogosulatlan és szándékos, jelentős mértékű akadályozása.”²⁶⁶ A cikk kimondja, hogy az akadályozásnak jelentős mértékűnek kell lennie, ugyanakkor az, hogy mi számít jelentősnek, a szerződő felek határozzák meg. Például jelentős akadályozás lehet az olyan nagymértékű adatforgalom, amely lényegesen rontja a rendszer működőképességét – mint a DDoS-támadások esetében.

Az Európai Parlament 2013/40/EU irányelve az információs rendszerek elleni támadásokról továbbá meghatározza és kiegészíti a Budapesti Egyezményt. Az irányelv (4) bekezdése a kritikus infrastruktúra elleni támadásokat szintén büntetendővé nyilvánít, ugyanis azokban esetleg bekövetkező működési zavar, illetőleg azok megsemmisítése a tagállamokban komoly következményekkel járna. Kritikus infrastruktúra alatt érteni kell például az erőműveket, a vízellátó rendszereket, vagy az ipari vezérlőrendszereket (például SCADA rendszerek). Így

²⁶³ MEZEI (2019a) i. m. 55-56

²⁶⁴ Uo.

²⁶⁵ 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről. 4. cikk

²⁶⁶ 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről. 5. cikk

ezen különösen szigorú megítélés alá esnek. Az irányelv (5) bekezdése pedig a botnetek létrehozását, illetőleg azok használatát rendeli büntetni, ugyanis „[b]izonyított az olyan, egyre veszélyesebb, ismétlődő és átfogó támadások előfordulása, amelyeket a tagállamok szempontjából [...] gyakran kulcsfontossággal bíró információs rendszerek ellen intéznek.”²⁶⁷ Az irányelv szerint az ilyen támadásokkal szembeni védekezés és a felelősök megbüntetése kiemelt fontosságú.²⁶⁸ Ezen irányelv 4. és 5. cikke deklarálja, hogy legalább a súlyosabb esetekben minősüljön bűncselekménynek a rendszert érintő jogellenes beavatkozás, valamint az adatot érintő jogellenes beavatkozás.

Súlyosabban kell büntetni a cselekményt, ha a támadást bűnszervezetben követik el, ha az jelentős kárt okoz, vagy ha kritikus infrastruktúra ellen irányul. Az irányelv alapján a tagállamoknak kell biztosítani a büntetési tételeket. Így a büntetési tételek a következőképpen alakulnak:

- a tagállamoknak kell biztosítaniuk, hogy az irányelv 3-7. cikkében megfogalmazott bűncselekmények, legalább a súlyosabb esetekben szabadságvesztéssel legyen büntetendő, és amelynek felső határa legalább két év;
- a tagállamoknak kell biztosítaniuk, hogy az irányelv 4-5. cikkében megfogalmazott bűncselekmények – amennyiben szándékosan követték el és jelentős számú információs rendszert érintettek – szabadságvesztéssel legyenek büntetendők, melynek felső határa legalább három év;
- a tagállamoknak kell biztosítaniuk, hogy az irányelv 4-5. cikkében megfogalmazott bűncselekményeket, ha azokat bűnszervezetben követték el, súlyos kárt okoztak vagy kritikus infrastruktúra részét képező információs rendszer ellen követték el, szabadságvesztéssel legyen büntetendő, melynek felső határa legalább öt év.²⁶⁹

A jogi személyek felelőssége is szabályozott. A Budapesti Egyezmény és a 2013-as irányelv előírja, hogy ha a jogi személy érdekében, annak képviselője által, vagy annak felügyeletének hiánya miatt követnek el kiberbűncselekményt, akkor a jogi személyt is felelősségre kell vonni. Ez magában foglalhat büntetőjogi szankciókat, például pénzbüntetést vagy egyéb jogi intézkedéseket. Fontos, hogy a természetes személyek büntethetősége nem zárja ki a jogi

²⁶⁷ Az Európai Parlament és a Tanács 2013/40/EU Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (5) bekezdés <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040>

²⁶⁸ MEZEI (2019a) i. m. 63-64

²⁶⁹ Az Európai Parlament és a Tanács 2013/40/EU Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról 9. cikk (2)-(4) bekezdés <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040>

személyek elleni eljárás lehetőséget. Az ilyen szabályozás különösen releváns a digitális korban, ahol az adatok és információk a vállalatok legértékesebb eszközeivé váltak. Az adatlopások és a rendszerek biztonsági réseinek kihasználása jelentős károkat okozhat a szervezeteknek, legyen szó üzleti titkok elvesztéséről vagy anyagi károkról.²⁷⁰

6. IoT ESZKÖZÖK ÉS AZ OKOSOTTHON

6.1. MEGHATÁROZÁSA

Az IoT az angol Internet of Things kifejezés kezdőbetűiből tevődik össze, magyarra fordítva a „dolgok internete” kifejezést használhatjuk. „Az [...] olyan internetre csatlakoztatott eszközök összessége, amelyek képesek kommunikálni más eszközökkel és hálózatokkal, de funkcionalitásuktól függően sokféle feladatra képesek.”²⁷¹

Ahogy a dolgozatom elején lévő idézet is jól szemlélteti, nem lehet manapság élesen elválasztani a digitális és a fizikai világot, az IoT eszközöknek köszönhetően folyamatos közeledés tapasztalható ezen két világ között. „Így a kibertámadás már nem csupán számítógépet bénít, adatot manipulál, hanem a rosszindulatú programok megfertőzhetik okos-eszközökkel teli fizikai valóságot is [...]”²⁷²

Az, hogy az IoT eszközökhöz mely eszközök is tartoznak valójában, megosztott megközelítéseket szül. Egyes megközelítések alapján a mobileszközök és a számítógépek is ebbe a körbe tartoznak, mások véleménye szerint viszont csak azon eszközök, amelyeknek van IP címe és azt nem Windows, Android, IOS vagy ehhez hasonló operációs rendszer futtatja, és amely nem tárol személyes adatokat. Korábbi adatok szerint 2021-ben több mint 20 milliárd eszköz csatlakozott az internetre.²⁷³

A technológia folyamatos fejlődését nézve ez a szám a további években is növekedni fog. Minden egyes eszköz csatlakozása az internetre biztonsági kockázatot jelent, illetve jelenthet. Ugyanis „[n]em az IoT „okossága”, hanem inkább „butasága” veszélyes (elavult, olcsó vagy rosszul beállított elemei).”²⁷⁴

6.2. OKOSOTTHON

Tehetjük fel a kérdést, hogy mikor beszélhetünk okosotthonról. Legtöbb esetben akkor, amikor az otthon legnagyobb része egy hálózatra, WIFI-re felcsatlakoztatott berendezésekkel,

²⁷⁰ MEZEI (2019a) i. m. 64-66

²⁷¹ NEMZETI Kibervédelmi Intézet: *IoT eszközök biztonsági kérdései – Az okosotthon. CTI jelentés. 2022.* Megtekintés: 2024. december 29. <https://shorturl.at/iZigh> 3

²⁷² FEHÉR András Tibor – NÉGYESI Imre: *A mesterséges intelligencia alapú kibertámadások lehetőségei.* Studia Mundi – Económia. 8. évfolyam 5. szám. 2021. Megtekintés: 2024. december 29. <https://journal.uni-mate.hu/index.php/stm/article/view/3256/3638> 28

²⁷³ NEMZETI Kibervédelmi Intézet i. m. 4

²⁷⁴ FEHÉR – NÉGYESI i. m. 29

eszközökkel van felszerelve. Ilyen népszerű berendezések az otthoni hangvezérlők, okos ajtócsengők kamerával felszerelve, okosvillanykapcsoló, okosfüstjelző, illetve termosztát, okosizzók, okoshűtők és még lehetne sorolni.²⁷⁵

Mivel az IoT eszközök száma növekvő tendenciát mutat, ezzel összefüggésben a kibervédelmi kérdés is fokozatosan nő, hiszen a hackerek, kiberbűnözők előszeretettel keresik az olyan eszközöket, amelyek nem a megfelelő biztonsággal rendelkeznek.²⁷⁶ Ezáltal egy nem megfelelő biztonsági beállítás következtében a személyes adataink a kiberbűnözők kezébe kerülhet, és esetleg zsarolás áldozatai is lehetünk. Korábban már kifejtettem, hogy milyen biztonsági intézkedéseket szükséges megejteni, így itt ezen pont alatt nem térek ki rá, az ott leírtak az irányadók.

A digitális és a fizikai valóság közeledése abban is megfigyelhető, hogy egy IoT eszközeinkhez történő illetéktelen hozzáférés esetén a magánéletünket is megismerheti a hacker, vagy kiberbűnöző:

„Ha például reggel 8-kor a kiszemelt áldozat elmegy dolgozni, és akár manuálisan, akár automatikusan lejjebb viszi a maximális hőmérsékletet, majd délután hazaérkezéskor vagy nem sokkal még azelőtt visszaemeli azt, akkor ez egyértelmű indikátor lesz a támadó számára, hogy adott esetben mikor tud zavartalanul betörni az áldozat lakásába.”²⁷⁷

Összefoglalva, az IoT eszközök tagadhatatlanul hasznosak, előszeretettel használjuk őket, kényelmeinket szolgálják, a mindennapjaink részévé váltak. Ezért elengedhetetlen, hogy oly módon használjuk ezeket az eszközöket, amelyek a lehető legnagyobb biztonságot nyújtsák számunkra, hogy a saját hasznunkra váljanak, ne pedig a kárunkra.²⁷⁸

7. ÖSSZEGZÉS ÉS 'DE LEGE FERENDA' JAVASLATOK

Összességében úgy gondolom, hogy látható a mesterséges intelligencia fejlődésének a hátránya. Számos olyan probléma van, amelyre már most, vagy majd a jövőben a jogalkotónak megoldást kell találnia. Néhány 'de lege ferenda' javaslat az ebben a fejezetben történt kifejtések következtében:

- AI-t használó bűncselekmények büntetési tételeinek pontosítása.
- Az AI kiberbiztonsági alkalmazásának szabályozása.
- Külön jogi keretek az AI által elkövetett bűncselekmények kezelésére.
- Nemzetközi megállapodások kidolgozása az AI-t érintő kiberbűnözésről.

²⁷⁵ NEMZETI Kibervédelmi Intézet i. m- 6-8

²⁷⁶ Uo.

²⁷⁷ NEMZETI Kibervédelmi Intézet i. m. 10

²⁷⁸ NEMZETI Kibervédelmi Intézet i. m. 15

FELHASZNÁLT FORRÁSOK

- 100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól. (dátum nélk.).
1998. évi XIX. törvény a büntetőeljárásról. (dátum nélk.).
2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről. (dátum nélk.).
2006. évi CI. törvény az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről. (dátum nélk.).
2012. évi C. törvény a Büntető Törvénykönyvről. (dátum nélk.).
2016. évi XXIX. törvény az igazságügyi szakértőkről. (dátum nélk.).
2017. évi XC. törvény a büntetőeljárásról. (dátum nélk.).
- 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről. (dátum nélk.).
- 8/2017. (IV. 18.) AB határozat az állatok védelméről és kíméletéről szóló 1998. évi XXVIII. törvény 43. § (1) és (4) bekezdésének alkalmazásával kapcsolatos alkotmányos követelmény megállapításáról. (dátum nélk.).
- A Szegedi Ítéltábla Bf.505/2014/5. számú határozata terrorcselekménnyel fenyegetés büntette tárgyában. (dátum nélk.).
- Ahmad, F. M. (dátum nélk.). Electronic evidence and its authenticity in forensic evidence. Forrás: <https://ejfs.springeropen.com/articles/10.1186/s41935-021-00234-6>
- Alexis, G. (dátum nélk.). Cyberbullying Laws: How Different Countries Address Online Harassment. Forrás: <https://www.lawobrien.com/cyberbullying-laws-how-different-countries-address-online-harassment/>
- Ambrus, I. (2021). *Digitalizáció és büntetőjog*. Budapest: Wolters Kluwer Hungary Kft.
- Anne, P. (2016. március 10). *Global Animal Law: What It Is and Why We Need It*. Cambridge University Press.
- Antonela, G., & Adrian, I. (2016). *Investigative issues regarding cybercrime*. European Journal of Public Order and National Security.
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2013/40/EU IRÁNYELVE (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. (dátum nélk.).
- Bagó, P. (2023. 10. évf. 2. szám). Kiberbiztonság és a mesterséges intelligencia kapcsolata. *Gazdaság és pénzügy*, 196-200. Forrás: <https://bankszovetseg.hu/Public/gep/2023/196-221%20Bago.pdf>
- Békés, Á., & Gépész, T. (2024/1, 13. évfolyam). A bűncselekmények helyszíne: az internet. Bizonyítási és eljárási nehézségek az interneten elkövetett bűncselekmények kapcsán. *In Medias Resz*, 122. Forrás: <https://inmediasreszfolyoirat.hu/imr/article/view/298>
- BH 2011.11.302: Legf. Bír. Bfv. III. 818/2010. határozata zaklatás vétsége tárgyában. (dátum nélk.).
- BH 2011.12.332 I. Internetes hirdetéssel megvalósított csalás esetén az elkövetési magatartás - a megtévesztés - akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot. (dátum nélk.).
- BH 2014.6.169: Kúria Bfv. III. 802/2013. határozata zaklatás vétsége tárgyában. (dátum nélk.).
- BH 2016.7.167 I. Az interneten közzététel megvalósult rágalmozás vagy becsületsértés esetén a bűncselekmény elkövetésének helye - amely egyben az általános illetékességi oknak felel meg - a weboldalt működtető szerver helye. (dátum nélk.).
- Blahó, A., & Prander, Á. (2016). *Nemzetközi szervezetek és intézmények*. Akadémia Kiadó.

- Bolcsó, D. (2024. december 30). Több százezer magyar felhasználó személyes adatai szivároghattak ki a Kütyübazar oldaláról. Magyarország. Forrás: <https://telex.hu/techtud/2024/12/30/kutyubazar-adatszivargas-adatvedelmi-incidens-szemelyes-adatok-kiberbiztonsag>
- Bolcsó, D., & Dezső, A. (2024. november 14). Meghekkelték a katonai és rendőrségi beszerzésekért felelő állami céget, érzékeny adatok kerültek nyilvánosságra. Magyarország. Forrás: <https://telex.hu/techtud/2024/11/14/vedelmi-beszerzesi-ugynokseg-vbu-hekkertamadas-zsarolovirus-inc-ransomware-kibertamadas-adatlopas>
- Borbíró, A., Inzelt, É., Kerezsi, K., Lévy, M., & Podoletz, L. (2014). *A büntető hatalom korlátainak megtartása: a büntetés mint végső eszköz*. Budapest: ELTE Eötvös Kiadó.
- Carlotta, R., & Gianclaudio, M. (dátum nélkül.). Sexual violence and harassment in the metaverse: A new manifestation of gender-based harms. Forrás: <https://bit.ly/3BlzgzN>
- Carole, P., & Regina, R. (1998). Memory for Medical Emergencies Experienced by 1- and 2-Year-Olds. Memorial University of Newfoundland. Forrás: <https://pubmed.ncbi.nlm.nih.gov/9779751/>
- Chiristían, L. (2013). *Az információs társadalom jogi vetületei*. Budapest: Pázmány Press.
- Chloé, B. (2021). EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments. European Papers. Forrás: https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2021_1_13_Articles_SS1_8_Chloe_Briere_00479.pdf
- Code Penal: Titre II: Autres dispositions. Article 521-1-1. (dátum nélkül.).
- Cyber, R. (2023. január 7). Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them. Forrás: <https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html>
- Domokos, M. (2022. június 23). A metaverzum jogi kérdései - 2.rész. Wolters Kluwer Kft. Forrás: <https://jogaszvilag.hu/szakma/a-metaverzum-jogi-kerdesei-2-resz/>
- Dornfeld, L. (2018/2). A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi szemle*, 118. Forrás: <https://real.mtak.hu/114280/1/DornfeldBelugyiSzemle2018.evi2.szam115-135.pdf>
- Dornfeld, L. (2019). Kiberterrorizmus - A jövő terrorizmusa? In *A bűnügyi tudományok és az informatika* (old.: 47-52). Budapest-Pécs: Pécsi Tudományegyetem Állam-és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont. Forrás: https://jog.tk.hun-ren.hu/uploads/files/A_bunugyi_tudomanyok_es_az_informatika.pdf
- Európai Bizottság. (dátum nélkül.). A mesterséges intelligenciára vonatkozó harmonizált jogszabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról.
- Európai, U. (2020. december). Ellenőrzési kompendium - Kiberbiztonság az Európai Unióban és tagállamaiban. Forrás: https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_HU.pdf
- Európai, U. (dátum nélkül.). Európai Unió Kiberbiztonsági Ügynökség (ENISA).
- EUROPOL. (2017). Drugs and the Darknet. Perspectives for enforcement, research and policy. Forrás: <https://shorturl.at/fngUF>
- EUROPOL. (dátum nélkül.). Cybercrime. Forrás: <https://www.europol.europa.eu/crime-areas/cybercrime>
- Farkas, Á., & Róth, E. (2019). *A büntetőeljárás (negyedik, átdolgozott kiadás)*. Budapest: Wolter Kluwer Kft.

- Fehér, A. T., & Négyesi, I. (2021. 31. évf. 3. szám). Mesterségesintelligencia-alapú kibertámadási modellek. *Műszaki Katonai Közlöny*, 75-79. Forrás: https://real.mtak.hu/131737/1/05_Feher-Negyesi_73-87_MKK_2021_3.pdf
- Fehér, A. T., & Négyesi, I. (2021. 8. évf. 5. szám). A mesterséges intelligencia alapú kibertámadások lehetőségei. *Studia Mudi - Economica*, 28. Forrás: <https://journal.unimite.hu/index.php/stm/article/view/3256/3638>
- Gál, I. L., & Nagy, Z. A. (2006). *Informatika és büntetőjog*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar.
- Gosztonyi, G., & Lendvai, G. (2024 tavasz, XXV. évf. 1. szám). Deepfake és dezinformáció. Mit tehet a jog a mélyhamisítással készített álhírek ellen? *Médiakutató*, 43. Forrás: <https://bit.ly/3ZRteF5>
- Gyaraki, R. E. (2018). A számítógépes bűnözés nyomozásának problémái. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs. Forrás: <https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf>
- Hekre, C. (2019). A digitalizáció szerepe a büntetőeljárásban. In K. Mezei, *A bűnügyi tudományok és az informatika* (old.: 118-120). Budapest-Pécs: MTA TK Jogtudományi Intézete és a Pécsi Tudományegyetem Állam- és Jogtudományi Kar.
- Herédi, I. (2022/1). A kiberbűncselekmények felderítési nehézségei. *Belügyi Szemle*, 47.
- Horváth, K. (2022. június 22). A metaverzum jogi kérdései - 1. rész. Wolters Kluwer Kft. Forrás: <https://jogaszvilag.hu/szakma/a-metaverzum-jogi-kerdesei-1-resz/>
- Hun-CERT. (dátum nélk.). Forrás: <https://cert.hu/rolunk/huncert-csoport>
- ÍH 2010.97: Fővárosi Ítéltábla 3. Bhari. 158/2009/7 határozata zaklatás vétsége tárgyában. (dátum nélk.).
- Junmo, Y. (2022. október 6). Can We Do Anything About Sexual Crimes in the Metaverse? Loyola University Chicago school of law, Chicago, USA. Forrás: <https://blogs.luc.edu/compliance/?p=4849>
- Karen J., S., & Rebecca, N. (1993). Children's testimony and their perceptions of stress in and out of the courtroom. USA. Forrás: <https://www.sciencedirect.com/science/article/abs/pii/014521349390083H>
- Katarzyna Chałubińska-, J., Filip, R., & Tadeusz, Z. (Springer). *Cybersecurity in Poland*. Poland: 2022. Forrás: <https://link.springer.com/content/pdf/10.1007/978-3-030-78551-2.pdf>
- Kiss, T. (2020). Kibervédelem a bűnügyi tudományokban. Budapest: Dialóg Campus.
- Kollár, C. (2023). A mesterséges intelligencia megjelenése a biztonságstudományban. *What will our Future be Like?* Großpetersdorf. Forrás: <https://real.mtak.hu/170988/1/tarstudkotet2023.pdf>
- Kovács, T. (2017. november 29). Fülöp kutya megkínzói letöltendő fogházbüntetést kaptak. Forrás: <https://www.nyirport.hu/2017/11/fulop-kutya-megkinzoi-letoltendo-foghazbuntetest-kaptak-13356>
- Magyarország Alaptörvénye (2011. április 25.). (dátum nélk.).
- Máté, I. Z. (2014/2). A bizonyítékok kezelése. Az igazságügyi informaticai szakértő a büntetőeljárásban. *Magyar Rendészet*.
- Máté, I. Z., Darabos, Z., Morber, S. K., & Sándor, G. (6/2020). Módszertani levél. Az elektronikus adatok vizsgálatának alapelveiről. Magyar Igazságügyi Kamara. Forrás: https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf
- Mészáros, R. (2016). A kibertér világa. Magyarország. Forrás: <https://docplayer.hu/25087119-A-kiberter-vilaga-zarojelentes-49442-tsz-otka.html>

- Mezei, K. (2019). A kiberbűnözés egyes büntetőjogi szabályozási kérdései. Doktori (PhD) értekezés. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Magyarország. Forrás: <https://shorturl.at/HqnWF>
- Mezei, K. (2019). A szervezett bűnözés az interneten. In K. Mezei, *A bűnügyi tudományok és az informatika* (old.: 125). Budapest-Pécs: Pécsi Tudományegyetem Állam-és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont.
- Molnár, Z., & Vig, E. (2024. december 6). A román alkotmánybíróság ledobta az atomot, példátlan helyzetet hozott az elnökválasztás megismételtetése. Magyarország. Forrás: <https://telex.hu/kulfold/2024/12/06/calin-georgescu-lasconi-tiktok-romania-alkotmanybirosag-ervenytelenites-hibrid-hadviseles-elnokvalasztas-oroszorszag>
- Nagy, K. (2017/4). A titkos információgyűjtés az új büntetőeljárás törvénytervezet tükrében. *Belügyi Szemle*, 61.
- Nagy, Z. A. (2009). *Bűncselekmények a számítógépes környezetben*. Budapest: Ad Librum.
- Nagy, Z. A. (2018). A joghatóság problémája a kiberbűncselekmények nyomozásában. *Acta Universitatis Szegediensis : acta juridica et politica*, 757. Forrás: https://acta.bibl.u-szeged.hu/54018/1/juridpol_081_755-765.pdf
- NATO. (dátum nélkül.). Cyber defence. Forrás: https://www.nato.int/cps/en/natohq/topics_78170.htm
- NATO. (dátum nélkül.). Military Committee. Forrás: https://www.nato.int/cps/ua/natohq/topics_49633.htm
- NATO. (dátum nélkül.). North Atlantic Council (NAC). Forrás: https://www.nato.int/cps/cy/natohq/topics_49763.htm
- Nemzeti Kibervédelmi Intézet. (2020. március 9). Robothálózat (Botnet). Forrás: https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/?utm_source=chatgpt.com
- Nemzeti Kibervédelmi Intézet. (2022). IoT eszközök biztonsági kérdései - Az okosotthon. CTI jelentés. Forrás: <https://shorturl.at/iZigh>
- Nemzeti Kibervédelmi Intézet. (2022). Mekkora fenyegetést jelentek valójában a deepfake-ek? CTI jelentés. Forrás: <https://bit.ly/40i3bst>
- Nemzeti Média- és Hírközlési Hatóság. (2023. január 13). Egyéni és társadalmi kockázata is van a deepfake-nek. Forrás: <https://bit.ly/3Pa4IKw>
- Nemzeti Média- és Hírközlési Hatóság. (2024). Mi számít online zaklatásnak? Forrás: https://nmhh.hu/cikk/190113/Mi_szamit_online_zaklatasnak
- Nemzeti Média- és Hírközlési Hatóság. (dátum nélkül.). Mi számít gyermekpornográf tartalomnak? Forrás: https://nmhh.hu/cikk/190114/Mi_szamit_gyermekpornograf_tartalomnak
- Nemzeti, K. I. (dátum nélkül.). Magunkról. Forrás: <https://nki.gov.hu/intezet/tartalom/magunkrol/>
- Nicola, P. (2009/1). Shining the torch on Plea-Bargaining. *The Cambridge Law Journal*, 11-14. Forrás: <https://www.cambridge.org/core/journals/cambridge-law-journal/article/abs/shining-the-torch-on-pleabargaining/84A8C53F3DCEEFE80B3ECB089E686BCE>
- Önder, K. S. (2012). *International egulation of National Cybercrime Jurisdiction*. Tilburg: Tilburg Law School.
- Papp, Z. I. (2018). A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái. Nemzeti Közszerológati Egyetem, Katonai Műszaki Doktori Iskola. Forrás: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13335/papp_zoltan_doktori_ertekezes.pdf?sequence=14&isAllowed=y

- Parti, K. (2008). Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs. Forrás: <https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/parti-katalin/parti-katalin-vedes-ertekezes.pdf>
- Peszleg, T. (2010/2). A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. *Ügyészek Lapja*, 25. Forrás: https://www.ugyeszek.hu/ftp/tartalom/ugyeszek_lapja/2010/ul2010_2_all.pdf?phpMyAdmin=5e79130c4a2a408b3f002bed9c4d2fba
- Sarita, S., Amna, B., Giang, D., Sylvia, D., Gabriel, G., Daricia, W., . . . Kentaro, T. (2023). Online Harassment in Majority Contexts: Examining Harms and Remedies across Countries. University of Michigan. Forrás: <https://arxiv.labs.arxiv.org/html/2301.11715>
- Serap, A. (2020. november 25). Online harassment is silencing girls: EU and Member States can do more. Forrás: <https://plan-international.org/eu/blog/2020/11/25/online-harassment/>
- Shiuh-Jeng, W. (2006. március 25). Measures of Retaining Digital Evidence To Prosecute Computer Based Cyber-Crimes. Department of Information Management, Central Police University, Taoyuan 333, Taiwan. Forrás: <https://www.scribd.com/document/332332873/Measures-of-Retaining-Digital-Evidence-to-Prosecute-Computer-Based-Cyber-crimes>
- Statista. (dátum nélk.). Most commonly reported cybercrime categories in the United States in 2023, by number of individuals affected. Forrás: <https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-us/>
- Symantec. (2017. április). Internet Security Threat Report. Forrás: <https://docs.broadcom.com/doc/istr-22-2017-en>
- Szalay, K. (2024/20). Deepfake, azaz mélyhamisítás: technológia és jog. *Infojegyzet*, 1. Forrás: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog
- Theresa May statement on Gary McKinnon extradition. (2012. október 16). Forrás: <https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition>
- Tilki, K. (dátum nélk.). Az állatkínzás nyomozását nehezítő és segítő tényezők. *Ügyészek Lapja*. Forrás: <https://ugyeszeklapja.hu/?cat=31>
- Tóth, D., & Gáspár, Z. (2020/2). Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. *Büntetőjogi Szemle*, 144-146. Forrás: https://ujbtk.hu/wp-content/uploads/lapszam/BJSZ_202002_140-150o_TohtDavid_GasparZsolt.pdf
- Tremmel, F. (2006). *Bizonyítékok a büntetőeljárásban*. Budapest-Pécs: Dialóg Campus Kiadó.
- United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001). (2001. december 6). Forrás: <https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/>
- Valter, K., & Vadász, G. (2024. április 15). A mesterséges intelligencia szerepe a kiberbiztonságban: hogyan észleljük és előzzük meg a támadásokat? Magyarország. Forrás: <https://bit.ly/3ZR9S2V>