Hollósi Beatrix

joghallgató (PTE ÁJK), az ÓNSZ Bűnügyi Tagozatának tagja

A kiberbűncselekmények felderítési metodikája*

I. Bevezetés

Az elmúlt években a digitális technológiák robbanásszerű fejlődése egyben vele párhuzamosan növelte a kiberbűnözés mértékét, illetve annak komplexitását. A kiberbűnözés általánosságban eltér a hagyományos bűncselekményektől, hiszen az interneten vagy más digitális rendszerekben történik és a gyorsan változó technológiai környezetnek köszönhetően újabbnál újabb kihívások elé állítja a hatóságokat és a bűnüldöző szerveket.

A kiberbűncselekmények felderítése és megelőzése azonban kulcsfontosságú a digitális társadalmak biztonságának érdekében és az elkövetők azonosítása céljából, továbbá e cél érdekében specifikus és átfogó nyomozási módszerek szükségesek. Mindez többek között magában foglalja az új technológiákhoz alkalmazkodást, a digitális bizonyítékok gyűjtésének és elemzésének fejlesztését, valamint a nemzetközi együttműködés erősítését a kiberbűnözés elleni küzdelemben. Ezenkívül a kiberbűncselekmények felderítési metodikájának fejlesztése során kiemelt figyelmet kell fordítani az adatvédelmi és etikai szempontokra is.

A tanulmány célja, hogy bemutassa a kiberbűncselekmények felderítési metodikáit, kiemelve az alkalmazható módszereket és az elektronikus felderítés meghatározó részeit. Elsőként általánosan a kiberbűncselekmények főbb fogalmait és jellemzőit tekinti át, majd részletesen elemzi a felderítési folyamat fontosabb lépéseit, illetve a felmerülő nehézségeket. Végezetül az áttekintés kitér a kiberbűnözés elleni küzdelem érdekében folytatott nemzetközi együttműködésre.

II. Alapvetés

II.1. Kiberbűncselekmények

A kiberbűncselekmények az egyik Magyarországon is használt csoportosítás[1] alapján két fő kategóriába sorolhatóak:

- az egyik a kimondottan a számítógépes rendszerek ellen irányuló támadások (ún. *„cyber-dependent”* bűncselekmények),

* Ezúton szeretnék köszönetet nyilvánítani Prof. Dr. habil Fenyvesi Csabának dolgozatom lektorálásáért.

[1] Jonathan *Clough*: Principles of cybercrime. Cambridge University Press, Cambridge 2015. 10-11. o. Idézi: *Polt* Péter: A számítógépes bűnözés. Belügyi Szemle 1983/6. 60-64. o.

- míg a másik kategóriába azok a hagyományos bűncselekmények sorolhatóak, amelyek az információs rendszerek felhasználásával történnek (ún. *„cyber-enabled"* bűncselekmények), mint például a csalás vagy a zaklatás.[2]

A 2001-es Számítástechnikai Bűnözésről szóló Egyezmény (a továbbiakban: Budapesti Egyezmény) és egyéb Európai Uniós irányelvek[3] meghatározták a kiberbűncselekményekre vonatkozó jogi kereteket és szankciókat, melyről egy lentebbi pontban részletesebben lehet majd olvasni. Viszont már itt megemlítendő, hogy a magyar jogban is alkalmazott számítástechnikai fogalmak szilárd alapját képezték e nemzetközi rendelkezések, hiszen rendkívül fontos meghatározásokat dolgoztak ki a témát illetően.

Fontos megemlíteni, hogy bár számos tanulmány foglalkozik a kiberbűncselekmények jellemzőivel és csoportosításaival, azonban egyelőre nem alakult ki egy általánosan elfogadott és egységes definíciója a kiberbűncselekménynek, mint fogalomnak.

A kiber(tér) függő és kiber(tér) által támogatott bűncselekmények egyaránt jellemzően határokon átívelő vagy más szóval nemzetközi jelleggel bírnak köszönhetően annak, hogy az egyes hálózathoz csatlakozó rendszerek között nincsenek fizikai határok, az információk és adatok pedig a felek között szabadon áramolhatnak.[4]

Mindemellett magas fokú anonimitás jellemzi az elkövetőket, hiszen a kommunikáció a technológiai lehetőségeknek köszönhetően könnyedén történhet titkosított csatornákon keresztül, mellyel az elkövetők elrejthetik tevékenységeiket a hatóságok látóköre elől[5], illetve a rendkívül gyors elkövetés és a sértettek magas száma miatt a hatóságoknak jelentős nehézséget okoz a felderítésük.[6] E bűncselekmények további jellemzőjeként említhető meg a fentiek miatt fennálló átlagosnál gyakoribb látencia is, hiszen az esetek többségében a hatóságok egyaltalán nem is szereznek tudomást az ilyesfajta bűncselekmények elkövetéséről.[7]

A kiber(tér) függő bűncselekmények kapcsán megemlítendő, hogy az *Internet of Things* (továbbiakban: IoT) eszközök térnyerése új lehetőségeket teremtett a bűnözők számára, mivel ezekre az esetek többségében nem vonatkoznak kötelező jogi védelmi követelmények. Ezenfelül a gyártók

---

[2] Továbbiakban a fent említett csoportosítás kapcsán a Gyaraki Réka „A közösségi média hatása a kiberbűncselekmények a kiberbűncselekmények elkövetésére" című tanulmányában is megjelenő kiber(tér) függő és kiber(tér) által támogatott bűncselekmények kifejezéseit fogom alkalmazni. *Ld.*: *Gyaraki* Réka: A közösségi média hatása a kiberbűncselekmények elkövetésére. Magyar Rendészet 2021/2. 73. o.

[3] Példaként az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv és a 2005/222/IB tanácsi kerethatározat

[4] *Miklós* Gellért: IoT és a kiberbűncselekmények szabályozása. Biztonságtudományi Szemle 2021/1. sz. 16-17. o.

[5] *Miklós:* i. m. 16. o.

[6] *Mezei* Kitti: ***A kiberbűncselekmények hazai szabályozásának aktuális kérdései.*** In: Magyar Jogászegyleti Értekezések (szerk. Sárközy Tamás). Magyar Közlöny Lap- és Könyvkiadó, Budapest 2018. 157. o.

[7] *Miklós*: i. m. 17. o.

sem helyeznek kellő hangsúlyt az eszközök megfelelő védelmi intézkedéseire, elsősorban a költséghatékonyság és az eszközök életciklusa miatt és így azok meglehetősen alacsony biztonsági szinttel rendelkeznek, melynek eredményeként könnyen sebezhetővé válnak az egyes informatikai támadásokkal szemben.[8]

II.1.1. A Budapesti Egyezmény

Az Európa Tanács által 2001. november 23-án elfogadott Budapesti Egyezmény jelentős mérföldkőnek számított a kiberbűnözéssel kapcsolatos nemzetközi szabályozásban. Az Egyezmény ugyanis alapvető definíciókat alkotott meg, illetve csoportosította a számítástechnikai bűncselekményeket, azokat négy kategóriába sorolva.

Az egyezmény a következő bűncselekménykategóriákat különböztette meg:

- I. Cím: Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények
- II. cím: Számítógéppel kapcsolatos bűncselekmények
- III. cím: Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények
- IV. Cím: Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.

Mindezen túl, az Egyezmény nemcsak egységes definíciókat és jogi keretet nyújtott, hanem rendszerezte a büntető anyagi jogi tényállásokat és már eljárásjogi kérdésekkel is foglalkozott.

II.2. Felderítés

A felderítés fogalma különböző jelentéssel bír a büntető eljárásjogban és a kriminalisztikában. Míg előbbiben a büntetőeljárásról szóló 2017. évi XC. törvény szerint a nyomozás egy szakasza értendő alatta, addig az utóbbi szakirodalmában adatgyűjtő és -feldolgozó tevékenységként értelmezik, mely kiterjedhet nem csak a (jogilag) releváns tényekre is. Ebből adódóan tágabb körben alkalmazható a második esetben (például háttérinformációk feltárása) és annak során bármilyen adatforrás felhasználható, illetve a felderítettséghez elégséges az önálló tisztánlátás és nem szükséges, hogy azt mások számára is lehetővé tegyük, tehát bizonyítottak legyenek a tények.[9]

A digitális felderítés a kiberbűncselekmények felderítésének kulcsfontosságú eszköze. Az elektronikus felderítés fejlődése szorosan összefügg a kiberbűncselekmények növekedésével és komplexitásával. A digitális nyomozások szakemberei egyre modernebb eszközökkel rendelkeznek

[8] Uo.
[9] *Székely* György László: A felderítésértelmezésitartományai a büntetőeljárásjogban és a kriminalisztikában. Belügyi Szemle 2021/10. sz. 1832-1833. o.

az adatok gyűjtéséhez és elemzéséhez, ezáltal egy „külön forenzikus mező jött létre" az online nyomozásban. Bár a digitális adatok nagy mennyisége kihívást jelent, ugyanakkor a speciális technikák és módszerek segíthetnek áthidalni ezeket a nehézségeket. Az elektronikus felderítés továbbra is dinamikusan fejlődik annak érdekében, hogy lépést tartson a bűnözők által használt technológiák fejlődésével és a kibertér változásaival.[10]

II.3. Kriminálmetodika

A kriminálmetodika fogalma szerint azon eljárási módszerek és technikák összessége értendő alatta, amely nem csak általánosságban foglalkozik a bűncselekmények hatékony nyomozásával, hanem az egyes bűncselekmény-kategóriák felderítésére és bizonyítására összpontosít, miközben átveszi és alkalmazkodik mind a kriminál technika, mind a kriminál taktika alapvető ismereteihez. A kriminálmetodika lényegét tekintve szakkriminalisztika, melynek fő célja a bűncselekményfajták jellemző elkövetési módozataira, lehetséges információ forrásaira és általában a bűnügy sajátosságaira összpontosítani.[11]

III. A kiberbűncselekmények felderítése

A kiberbűncselekmények meglehetősen új és komoly kihívások elé állították a nyomozó hatóságokat, ugyanis a szükséges számítástechnikai, illetve egyéb online térrel kapcsolatos ismeretekből és erőforrásokból az esetek többségében jelentős hiány mutatkozik és a hagyományos nyomozási módszerek sem bizonyulnak hatékonyan alkalmazhatónak.[12]

A hagyományos bűncselekményekhez képest – ahol rendelkezésre állnak fizikális formában is megjelenő nyomok – jelentős eltérés, hogy itt számos esetben kizárólag digitális nyomok (pl. IP-cím[13], felhasználónév) állnak rendelkezésre. Ez tehát azt is jelenti, hogy nincsenek szemtanúk, DNS-minták vagy videófelvételek, melyek segíthetnek az azonosításban, ehelyett az internet-szolgáltatóktól és az eszközökből begyűjtött elektronikus adatokra támaszkodhatnak egyedül a nyomozó hatóságok.[14]

Jan-Jaap Oerlemans és Maša Galič *„Cybercrime investigations"* című tanulmánya az IP-címek digitális nyomként felhasználására remek példát mutatott be, mely jól szemlélteti a digitális nyomozás lépéseit. Ezt összefoglalva a következők mondhatók el:

---

[10] *Fenyvesi* Csaba: Kriminalisztikai világtendenciák – különös tekintettel a digitális felderítésre. In: A bűnügyi tudományok és az informatika (szerk. Mezei Kitti). Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, Budapest-Pécs 2019. 75-78. o.

[11] *Fenyvesi*: i. m. 30. o.

[12] Paul *Hunton*: The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Computer Law & Security Review 2011/1. sz. 61-62. o.

[13] Az IP cím az Internet Protokoll-cím rövidítése. Egy számsor, amely azonosításra szolgál az interneten.

[14] Jan-Jaap *Oerlemans* – Maša *Galič*: Cybercrime investigations. In: Essentials in cybercrime: A criminological overview for education and practice (szerk. Wytske van der Wagen, Jan-Jaap Oerlemans, Marleen Weulen Kranenbarg). Eleven International Publishing, Hága 2022. 197. o.

„Egy nemzetközi rendőri műveletet követően (amit az Europol koordinált) a holland hatóságok nagy számú IP-cím adatbázist kaptak az Europol-tól. Az Europol szerint az IP-címek egy olyan fórumról származnak, ahol gyermekpornográfiát osztottak meg egymással felhasználók. Emellett rendelkezésre állt egy másolat a szerverről, a hozzá tartozó üzenetekről és egyéb anyagokról is. A nyomozó hatóságoknak tehát össze kellett valahogy kapcsolniuk az IP-címeket a gyanúsítottakkal.

Hogyan működik ez?

1. Lépés:

A „Who is" adatbázisban keresés segíthet azonosítani, hogy melyik Internet Szolgáltatóhoz (ISP) tartozik az IP-cím. Abban az esetben, ha holland ISP-hez tartozik az IP-cím, akkor megvan az esély, hogy a gyanúsított is holland.

2. Lépés:

Hollandiában, valamint az EU más tagállamaiban is a nyomozó hatóságok adatokat kérhetnek az egyes IP-cím felhasználókról (általában az internetkapcsolatot fizető személy adatait) az ISP-től az adatszolgáltatási kötelezettségüknek köszönhetően. Ezen az úton már meglehet szerezni egy nevet és egyéb adatokat is, illetve akár a gyanúsított lakcímét, tartózkodási helyét.

3. Lépés:

A gyanúsított lakhelyén elvégzett helyszíni szemlével további bizonyítékokat lehet összegyűjteni a bűncselekményről. A nyomozó hatóságok ezután olyan adathordozókat, például számítógépeket és merevlemezeket foglalnak le, amelyeket feltehetően elkövetési eszközként használtak a gyermekpornográfia tárolására és terjesztésére.

4. Lépés:

A lefoglalt adathordozókon és kapcsolódó hálózatokon a nyomozó hatóságok a gyermekpornográf felvételeket és egyéb adatokat vagy más, illetve más elkövetőkhöz kapcsolódó bűncselekmények nyomait keresik (például elküldött üzenetek vagy használt becenevek)

5. Lépés:

Ezt követően az esetek többségében a szemtanúk vallomásaival folytatják és ha szükséges, a gyanúsítottat őrizetbe veszik és kihallgatják."

Fontos azonban tudni azt, hogy ez egy nyomozati szempontból idealizált eset, ugyanis a valóságban a kiberbűnözők gyakran különféle anonimizáló technikákat használnak, mint például VPN[15]-kapcsolatot, hogy elrejtsék az IP-címüket.[16]

A digitális nyomozások során a különböző adathordozók is fontos szerepet játszanak, mivel azok bizonyítékokat tartalmazhatnak a bűncselekményre**,** így már a nyomozás megkezdésekor másolatot kell készíteni a merevlemezekről vagy más adatforrásokról, majd a másolatot használják fel a továbbiakban.

Az adatmentéseknek alapvetően két esete van. Az egyik az adathordozók lefoglalása, elszállítása és azokról kikapcsolt állapotú adatmentés, míg a másik eset a helyszíni adatmentés., melynek további két esete a *„liveforensic"* és a *„mobil forensic"*. Előbbi esetén a számítógépeket bekapcsolt állapotban vizsgálják át, míg utóbbi a mobilkommunikációs eszközök adatmentésére vonatkozó eljárást foglalja magában.[17]

---

[15]Leslie F. *Sikos*: AI in digital forensics: Ontology engineering for cybercrime investigations. WIREs Forensic Science 2021/3. sz. 1. o.

[16]*Oerlemans – Galič*: i. m. 209. o.

[17]*Szabolcsi* Zsolt: Kibernyomozói munka terepen. Nemzeti Közszolgálati Egyetem. Budapest 2023. 42-50. o.

A *liveforensic* napjainkban igencsak elterjedt módszerré vált, hiszen meghatározható általa például, hogy mely felhasználók jelentkeztek be a számítógépre vagy egy fiókra a közelmúltban.[18] A modern forenzikai szoftverek lehetővé különböző fájltípusok szervezését, elemzését és akár a törölt fájlok is visszaállíthatóak. A *Netherlands Forensic Institute* (NFI) pedig kifejlesztett egy innovatív rendszert az adathalmazok közötti keresésre. A rendszer neve *"Hansken"* és nagy mennyiségű különböző típusú adat gyors és alapos elemzését teszi lehetővé. A nagy adatkészletekben gyorsan lehet keresni vele és kapcsolatokat lehet felállítani különböző attribútumok között (például felhasználói nevek, becenév, telefonszámok és e-mail címek), ezzel növelve a nyomozó hatóságok munkájának hatékonyságát és gyorsaságát. A szoftvert súlyos kábítószer-bűncselekmények és emberölési ügyek vizsgálatára használják fel Hollandiában, és fontos bizonyítékokat szolgáltatott már több ügyben is.[19]

A számítógépes rendszerek közötti kapcsolódás következtében előfordulhat, hogy sok adat nem az adott eszközön van tárolva, hanem egy arról "könnyen elérhető" egyéb adattárolásra alkalmas helyen (pl. felhőtárhely) Ugyanakkor a hálózati szintű keresésnek ("távoli keresés") köszönhetően lehetővé válik egy meglévő keresés kiterjesztése a gyanúsított informatikai berendezéseiről más eszközökre is, amelyek a belső hálózathoz (intranet) kapcsolódnak. A hálózati keresést példaként arra is használható, hogy távolról kutassanak egy vállalat levelező szerverén egy adatközpontban egy irodaházzal kapcsolatos nyomozás során. Ezenfelül a hálózati keresésnek köszönhetően a nyomozó hatóságok a gyanúsított eszközeinek lefoglalása után távolról hozzáférhetnek a gyanúsított egyes fiókjaihoz.[20]

III.1. Nyílt forrású adatgyűjtés

Az IP-cím alapján végzett vizsgálatok sikertelensége esetén más digitális nyomok is akadhatnak egy nyomozás során, amelyeket az illetékes hatóságok meg kell vizsgálni. Ilyen módon különösen fontosak azok a digitális nyomok, amelyeket az internetet használó személyek hagynak maguk után az online térben.

Mint más emberek, a kiberbűnözők is aktívak a közösségi médiában. Ilyenkor viszont a hatóságok is nyomon követhetik az emberek "digitális morzsáit" az interneten annak érdekében, hogy többet megtudjanak a gyanúsítottról, az áldozatról és a gyanúsított környezetéről vagy több információt gyűjtsenek be magáról a bűncselekményről.

Az adatok nyílt forrásból gyűjtése OSINT (*Open-source intelligence*) néven ismert. A nyílt forrású adatok alatt olyan információkat értendők, amelyeket bárki legálisan beszerezhet megfigyeléssel,

[18] *Oerlemans – Galič*: i. m. 217. o.
[19] *Oerlemans – Galič*: i. m. 217-218. o.
[20] *Oerlemans – Galič*: i. m. 220. o.

lekéréssel vagy vásárlással, mint például az interneten bármikor könnyedén elérhető információk. Bár a legtöbb kiberbűnöző szigorúan elválasztja valódi személyazonosságát a bűnözői személyazonosságától, – akár egy egyedi felhasználónév használatával – mégis a bűnözők is követhetnek el hibákat (például ugyanazokat a kifejezéseket vagy idézeteket használják mindkét helyen, melynek segítségével összekapcsolhatóvá válnak valódi személyazonosságukkal) és előfordulhat az is, hogy a kiberbűnözők egymásról szivárogtatják ki a személyes adataikat (erre a *„doxing"* kifejezés használatos). Mindezekkel pedig meglehetősen hasznos nyomokat közölnek a nyomozó hatóságok számára.[21]

Az OSINT technikák esetében megkülönböztethető az adatok manuális- és automatizált gyűjtése. A nyilvánosan elérhető online adatok manuális gyűjtése során az adatokat olyan keresőmotorokba (például Google) bevitt keresőszavakra kattintva gyűjtik össze, amelyek bárki számára elérhetőek. Bár ez a fajta keresési módszer igencsak egyszerűnek tűnhet, ennek ellenére a feltételezett hackerek becenevének beírása a Google-be valójában már eredményezte azt, hogy a beazonosítás sikeres megtörténjen.

Az adatgyűjtés ugyanakkor részben vagy teljesen automatizálható szoftverek segítségével is történhet, melyek lehetővé teszik, hogy egy előre megadott kifejezés alapján gyűjtsenek adatokat több különböző (nyílt) adatforrásból egyszerre, majd megjelenítsék azokat összefoglalt és átlátható formában és ennek köszönhetően kapcsolatokat, linkeket hozhatnak létre az információk között: például egy személy, aki különböző felhasználóneveket használ, de mindig ugyanazt a titkosítási kulcsot használja az üzenetek küldéséhez (például PGP kulcsok a *darknet* piacokon) vagy ugyanazokat a *bitcoin* címeket használja pénz átutalásokra.[22]

Mindemellett a fedett nyomozók alkalmazása az online térben értékes lehetőséget kínál a hatóságok számára. Az internet ugyanis nemcsak a bűnözők számára egy határtalan közeg a bűncselekmények (viszonylagos) névtelenséggel végrehajtására, de alkalmas a bűnözés elleni küzdelemre is. Ennek eredményeképp a nyomozók is anonim módon kommunikálhatnak úgy, mint mások, anélkül, hogy (közvetlen) fizikai kockázatot vállalnának. Például illegális árut vagy szolgáltatást vásárolhatnak online piactereken annak érdekében, hogy bizonyítékokat gyűjtsenek be. A nyomozó hatóságok ezáltal információkat kaphatnak arról, hogy ki küldi/küldte a csomagot, amely az árut vagy más adatokat tartalmaz. Ha a gyanúsított maga végzi a szállítást akár az is előfordulat, hogy például egy csomagon ujjnyomokat vagy DNS-anyagot (pl. bélyegzőnyalás útján) találjanak, amelyek alapján további vizsgálatokat folytathatóak Az áru vagy adatok internetes vásárlását pedig online kommunikáció előzi meg, mely során lehetséges egyéb adatok megszerzése is a gyanúsítottról, mint

[21] *Oerlemans – Galič*: i. m. 225-226. o.
[22] *Oerlemans – Galič*: i. m. 226-227. o.

például név, telefonszám és/vagy e-mail cím. Ezeknek az adatoknak köszönhetően pedig további nyomozási lépésekre kerülhet sor, mint például a már említett ISP adatok lekérésére.[23]

IV. Kiberbűncselekményekkel kapcsolatos felderítési nehézségek

A kibernyomozás során Jan-Jaap Oerlemans és Maša Galič *„Cybercrime investigations"* megnevezésű tanulmánya szerint 3 fő probléma merül fel újból és újból: „a joghatóság, anonimitás és titkosítás". Ezek pedig jelentősen befolyásolták a kialakult nyomozási módszereket.

A joghatósággal kapcsolatosan Budapesti Egyezmény 19. cikk (2) bekezdése lehetővé teszi az igazságügyi hatóságok számára, hogy a már elérhető számítógépről kiterjesszék a keresést a kapcsolt hálózatokra, de csak akkor, ha azok a joghatósági területükön találhatóak.

A kutatási és lefoglalási jogosultságokat az emberi jogok és szabadságok tiszteletben tartásával kell meghatározni és gyakorolni. Egy számítógép lefoglalása és a rajta tárolt információk elemzése komoly adatvédelmi beavatkozást jelent. Az Emberi Jogok Európai Bírósága egyértelműen megjegyezte, hogy a helyszíni keresés és a számítógépek lefoglalása súlyos beavatkozást jelent a magánéletbe és az adatvédelem jelentőségéből adódóan részletes szabályozások és specifikus eljárási garanciák szükségesek.[24]

Azon bűncselekmények elkövetőinek felderítése sem egyszerű feladat sokszor, amelyek a hatóságok tudomására jutottak, ugyanis nem csupán komoly nemzetközi együttműködést igényel bármilyen releváns információ beszerzése, hanem a nyomozás egyben igazi türelemjáték is, a nemzetközi jogi aktusokon alapuló eljárások akár több hónapig is eltarthatnak. Ezenfelül ennél komolyabb problémát jelent, hogy online bűncselekmények áldozatai gyakran nem is jelzik az esetet a hatóságoknak akár félelemből vagy egyszerűen figyelmetlenségből, hiszen az ilyen cselekmények skálája rendkívül széles és egy online hirdetésben vagy álprofilban megjelenített személyes adattal visszaélés esetén, ha nem jár el a sértett kellő figyelemmel az is megtörténhet, hogy tudomást sem szerez róla.[25]

Az adatok titkosítása és a kriptográfia alkalmazása elengedhetetlen az információhoz való jogosulatlan hozzáférés megakadályozásához, amely matematikai algoritmussal teszi az adatokat olvashatatlanná titkosított szöveggé alakítva azokat. Az így titkosított adatokat egy dekriptáló kulccsal lehet csak újra olvashatóvá tenni. Ez a módszer kimondottan alkalmas a felek közötti titkosított kommunikációra. Ellenben a kriptográfia használatának egyben negatív vonzatai is vannak. Az adatok titkosítása jelentős problémát jelent a bűnüldözés számára, mind a kommunikációk lehallgatása, mind pedig a számítógépeken tárolt adatok elemzése során. A bűnüldöző hatóságok már az 1990-es évek

[23] *Oerlemans – Galič*: i. m. 228-229. o.
[24] *Oerlemans – Galič*: i. m. 219-220. o.
[25] *Herédi* István: A kiberbűncselekmények felderítésének nehézségei. Belügyi Szemle 2022/1. sz. 48-49. o.

elejétől felhívták a figyelmet rá, hogy a bűnözők által használt kriptográfia (az úgynevezett „sötétségbe vonulás") megbénítja a bűnüldözést, melynek nyilvános hozzáférését azóta próbálják korlátozni különböző megoldásokkal.[26]

Az informatika területein bekövetkező változások és fejlesztések rendkívül gyorsan történnek és így fontos, hogy a bűnüldözésben résztvevő szakemberek naprakészek legyenek, melyben segítséget nyújthat az automatizáció és a gépi tanulás. Az eszközeik, kereséseik automatizálásával a nyomozók felgyorsíthatják folyamatukat és hatékonyságukat.[27] Így az is elképzelhető, hogy a mesterséges intelligencia a jövőben komoly fegyver lehet a nyomozó hatóságok kezében a kiberbűnözés elleni harcban.

A megfelelő digitális nyomozási módszer kiválasztása érdekében meghatározott szempontok mentén kell elvégezni azok összehasonlítását. Elsőként is meg kell vizsgálni a módszer összetettségét, komplexitását. Ez azt mutatja meg, hogy mennyire egyszerű elvégezni, mennyibe kerül és mennyi időt vesz igénybe a folyamat. Fontos felmérni azt is, hogy az igazságügyi adatok integritása mennyiben sérül az adott metódus alkalmazása során és figyelembe venni, hogy mennyiben arányos ez a sérelem az elérni kívánt céllal.[28]

V.1 A közvetítő szolgáltatók felelőssége a nyomozás során

A kiberbűncselekmények felderítése kapcsán fontos megvizsgálni a felelősség kérdését is. Az elmúlt években felmerülő igények arra ösztönzik ugyanis a techcégeket, hogy ők is járuljanak hozzá az internet jogszerű működéséhez. Viszont az ezzel kapcsolatos ígéretek gyakran nem a remények szerint teljesülnek, hiszen az internet egy nemzetek felett álló, globális hálózatként működik, így nehéz, illetve szinte lehetetlen egyetlen és egységes szabályrendszert megalkotni rá. Az infrastruktúra helyes működését is fontos ugyan biztosítani, de még inkább fontosabb a megfelelő figyelem ráfordítása a használat során tanúsított magatartásokra.

Az internet működésének fontos szereplői a különböző szolgáltatók, akik lehetnek hálózati infrastruktúra üzemeltetői, tárhelyszolgáltatók vagy keresőmotorok. Ugyanakkor a szolgáltatók felelőssége a nyomozás során meglehetősen fontos kérdéseket vet fel. Egyelőre a büntetőjogi felelősségük tisztázatlan és inkább a polgári jogi felelősséggel kapcsolatos szabályokat lehet sikeresen alkalmazni. Különösen a jogsértő tartalmakért önként vállalt vagy előírt felelősségük generál sok vitát napjainkban. Az informatikai bűncselekmények különböző típusai miatt tágabban kell értelmezni ezt a felelősségi alakzatot. A közvetítő szolgáltatók ugyanis nem csak a tartalommal kapcsolatos

[26] *Oerlemans*, *Galič*: i. m. 236-237. o.
[27] Cecelia *Horan* – Hossein *Saiedian*: Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. Journal of Cybersecurity and Privacy 2021/1. sz. 595-596. o.
[28] *Horan* – *Saiedian*: i. m. 582. o.

jogsértésekért lehetnek felelősek, hanem például a rosszindulatú számítógépes programok terjesztése esetén is.[29]

Az Európai Unió irányelvei és a hazai jogszabályok folytán rögzített kimentési lehetőségek meglehetősen széles körűek és a szolgáltatók tevékenységétől függően differenciálják a felelősséget. Fontos megérteni azonban azt is, hogy az nem csupán a tartalom jogsértő mivoltára vonatkozik, hanem a kifejtett tevékenységeik során tanúsított magatartásokra is kiterjed. Viszont a jogszabályoknak és az irányelveknek megfelelően eljáró szolgáltatók mentesülhetnek a felelősség alól, míg azok, akik nem tesznek eleget kötelezettségeiknek felelősségre vonhatók a jogsértésekért.[30]

III. Nemzetközi Együttműködés

A felderítés során az egyik fő nehézséget a nemzetközi jelleg és az abból adódó joghatósági kérdések jelentik, így elkerülhetetlen a hatékony nyomozás érdekében a hatóságok közötti internacionális együttműködés.

Az Európai Unióban az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv (továbbiakban: Irányelv) a 2005/222/IB tanácsi kerethatározatot váltotta fel. Ez az irányelv minimumszabályokat határozott meg az információs rendszerek elleni bűncselekményekre és elősegítette az együttműködést tagállami hatóságok között.

Az Európai Tanács 2005. február 24-én fogadta el a 2005/222/IB kerethatározatot, mely szintén fontos lépés volt az információs rendszerek elleni támadásokkal kapcsolatos jogszabályok harmonizációja terén. Ez a kerethatározat az információs rendszerekre helyezte a hangsúlyt, szemben a számítástechnikai rendszer fogalmával.

Az Irányelv célja a büntetőjog harmonizációja és az együttműködés erősítése volt a tagállamok között. Az Irányelv hivatkozott a Budapesti Egyezményre, amelynek követte jogi keretét, továbbá szabályozta az információs rendszerekhez való jogellenes hozzáférést, a rendszert és adatot érintő jogellenes beavatkozást, valamint a jogellenes adatszerzést is.

Az EMPACT (*European Multidisciplinary Platform Against Crime Threats*) az Európai Unió révén kezdeményezett, tagállamok által támogatott program, amely a szervezett és nemzetközi bűnözés elleni küzdelemre összpontosít. Az EMPACT a stratégiai prioritások meghatározásától kezdve az operatív cselekvési tervek kidolgozásán keresztül, az eredmények értékeléséig terjedő folyamatokat öleli fel. Az EMPACT az az együttműködési keret, amely lehetővé teszi a tagállamok, az uniós intézmények és más szereplők számára, hogy stratégiai és operatív szinten is együttműködjenek a

[29] *Sorbán* Kinga: Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában: Felelősség és kötelezettségek. In Medias Res: Folyóirat sajtószabadságról és a médiaszabályozásról 2019/1. sz. 86-87 o.

[30] *Sorbán*: i. m. 88. o.

bűnözés elleni küzdelemben.

Az EMPACT létrehozásának célja az volt, hogy elősegítse az előre meghatározott uniós bűnüldözési célok elérését, biztosítsa a tagállamok közötti hatékony együttműködést az információk és ismeretek megosztása terén és strukturált platformot biztosítson a prioritásként meghatározott súlyos és szervezett nemzetközi bűncselekmények elleni küzdelemben.

Az EMPACT keretében végzett tevékenységek eredményeként több sikeres felderítés történt és számos gyanúsítottat fogtak el. Az együttműködés hatékonyan támogatja a bűnüldözést, és jelentős eredményeket érnek el az adott bűnözési területeken.[31]

IV. Konklúzió

Összegzésképpen elmondható, hogy a kiberbűncselekmények felderítése komoly kihívások elé állítja a nyomozó hatóságokat, ugyanis a hagyományos nyomozási módszerek gyakran nem alkalmazhatóak kellően hatékonyan az online térben. A nyomozás során a digitális nyomok – például IP-címek és felhasználónevek – jelentik a fő adatforrásokat és a hatóságok számára szükségszerű a speciális szakértelem és az eszközök rendelkezésre állásának növelése az azonosítás és az adatok elemzésének érdekében.

Az IP-címek nyomként felhasználása segíthet a gyanúsítottak azonosításában, de gyakran szükség van egyéb nyomokra is, mint például internetes szolgáltatóktól származó adatokra, viszont az adatok gyűjtése és elemzése csak az első lépés a digitális nyomozás során és a nyomozóknak helyszíni szemlékkel és más módszerekkel kell a rendelkezésre álló adatok megerősítése és a bűncselekmények bizonyíthatósága érdekében eljárniuk.

Ezenkívül a nyílt forrású adatgyűjtés is fontos szerepet játszik a nyomozásokban, amivel a nyomozók figyelemmel kísérhetik a gyanúsítottak online tevékenységét és információkat gyűjthetnek a bűncselekményekről, noha a kiberbűnözők gyakran anonim módon léteznek és működnek az online térben, ehhez különféle technikákat alkalmazva, mint például a VPN-k.

Végezetül, bár nem utolsó sorban az információs rendszerek elleni támadások és más kiberbűncselekmények nemzetközi jellege miatt elengedhetetlen az együttműködés a hatóságok között, melyet az Európai Unió irányelvei és más nemzetközi egyezmények próbálnak létrehozni, ámde továbbra is sok jogi és technikai kihívás áll fenn a hatékony kiberbűnözés elleni küzdelem érdekében.

[31] *Vetter* Da□ niel: Az EMPACT szerepe a kiberbűncselekme□ nyek elleni küzdelemben. Belügyi Szemle, 2023/8. sz. 1343. o.