Pécsi Tudományegyetem Állam- és Jogtudományi Kar

Doktori Iskola

DOKTORI ÉRTEKEZÉS

(PhD)

Disszertáció

Dr. Szabó Barbara

2025.

Pécsi Tudományegyetem Állam- és Jogtudományi Kar

Doktori Iskola

Valóság és virtuális tér találkozása:

Büntető eljárásjogi és kriminalisztikai válaszok a XXI. századi bűncselekményekre

Konzulens:

Prof. Dr. Habil. Herke Csongor DSc.

Készítette:

Dr. Szabó Barbara

Pécs,

2025.

Tartalomjegyzék:

1. Bevezető gondolatok

A XXI. század dinamikus technológiai fejlődése, a digitalizáció térnyerése és az információs technológiák mindennapivá válása alapvető változásokat idézett elő a társadalom működésében, ezen belül a bűnözés természetében is. Ezen korszakban olyan új bűncselekmény-típusok jelentek meg, amelyek korábban nem léteztek, vagy a korábbi formáktól lényegesen eltérő sajátosságokat mutatnak. Az internet és a digitális technológiák globális elterjedése nem csupán a bűncselekmények elkövetésének módját alakította át, hanem a felderítés és üldözés módszertanát, valamint a jogi szabályozás egész szemléletét is új alapokra helyezte. A disszertáció középpontjában a modern, digitális környezetben megvalósuló bűncselekmények állnak, különös tekintettel azok strukturális sajátosságaira, valamint az e jelenségek kezelését célzó jogalkalmazási és jogalkotási kérdések. Az értekezés kiindulópontja a bűnözési formák megváltozott jellege, amelyet alapvetően a technológiai innovációk idéztek elő. A digitális platformok és a kibertér által kínált anonimitás és határokon átívelő jelleg új típusú kihívásokat támasztott mind a bűnüldöző szervek, mind a jogalkotók számára. A kutatás kiemelt figyelmet szentel azon kérdéseknek, hogy miként alakítja át a technológia a bűncselekmények elkövetési módját, hogyan reagálnak ezekre a jogalkotási szervek, és milyen gyakorlati eszközök állnak rendelkezésre a XXI. századi bűncselekmények felderítésére és bizonyítására.

1.1. A témaválasztás oka, a kutatás területe és aktualitása

1.2. Hipotézisek

Az értekezésben megfogalmazott és vizsgált hipotézisek a következő kérdéseket érintik:

1. Az elkövetési szándék önmagában nem elegendő a büntethetőséghez: Feltételezem, hogy a bűncselekmény elkövetésére irányuló szándék puszta kinyilvánítása önmagában nem minősül büntetendő cselekménynek, amennyiben nem kapcsolódik konkrét cselekményekhez vagy előkészületi magatartáshoz. Ez

különösen releváns a digitális térben megvalósuló fenyegetések és szándéknyilatkozatok értékelésekor.

2. Az internetes anonimitás és jogi felelősség hiánya elősegíti az online zaklatás terjedését: Hipotézisem szerint az online térben uralkodó anonimitás és a határokon átnyúló kommunikáció lehetősége növeli az ilyen típusú bűncselekmények elkövetésének gyakoriságát, továbbá jelentősen nehezíti a felelősségre vonást és a bizonyítást.

3. A digitális bűncselekmények számának növekedése összefügg az információbiztonsági tudatosság hiányosságaival: Feltételezem, hogy a személyes adatok fokozott sérülékenysége, valamint az online tranzakciókhoz kapcsolódó biztonsági rések növelik a digitális csalások, identitáslopások és adathalász támadások előfordulását.

4. A nemzetközi szabályozási keretek hatékonysága korlátozott: A Budapesti Egyezmény és hasonló nemzetközi jogi szabályozások bár szükségesek, önmagukban nem elégségesek a XXI. századi digitális bűncselekmények hatékony visszaszorításához. Feltételezem, hogy a jogharmonizáció nehézségei és a nemzetközi jogérvényesítés hiányosságai továbbra is jelentős kihívást jelentenek a bűnüldözés számára.

1.3. Módszertan

A kutatás módszertani keretét a társadalomtudományi empirikus megközelítés, azon belül a kvalitatív és kvantitatív elemeket ötvöző, szekunder elemzésre épülő dogmatikai kutatás alkotja. A vizsgálat alapját a szociálkutatás tudományos módszertani elvei adják, ahogyan azt Earl Babbie megfogalmazza: „a kutatási folyamat a problémafelvetés, a konceptualizálás, az operacionális meghatározás, az adatgyűjtés, majd az elemzés és értelmezés egymásra épülő szakaszaiból áll.”[1] A kutatás célja nem csupán leíró, hanem magyarázó és értelmező jellegű is, a jelenségek mögötti oksági, társadalmi és jogi

[1]Babbie, Earl: The Practice of Social Research. 14. kiadás. Boston, Cengage Learning, 2016. 592 o., 67–73. o.

összefüggések feltárására törekedve. Az értekezés elméleti dogmatikai típusú kutatás, mivel a vizsgált jelenségek a XXI. századi, technológiai alapú bűncselekmények elsősorban a jogrendszeren belül értelmezhetők. A módszertan ennek megfelelően normatív elemzést, komparatív jogösszehasonlítást, esettanulmány-feldolgozást és leíró statisztikai elemzést alkalmaz. A kutatás során szekunder forrásokra támaszkodtam, amelyek közé hazai és nemzetközi monográfiák, folyóiratcikkek, jogszabályok, bírósági döntések, valamint statisztikai jelentések tartoznak. A szakirodalmi áttekintés célja a kibertérben megvalósuló bűncselekmények dogmatikai értelmezése, valamint a technológiai fejlődés büntetőjogi implikációinak feltárása volt. A jogösszehasonlító módszer alkalmazása során az Európai Unió tagállamainak, továbbá az Egyesült Államok és Japán szabályozását is vetettem össze a magyar jogi környezettel, különös tekintettel a Budapesti Egyezményre (2001), a Digital Services Act-re (EU 2022/2065) és az EU e-Evidence Rendeletre (EU 2023/1543). A dogmatikai elemzés középpontjában a Btk. és a Be. releváns tényállásainak és eljárási szabályainak értelmezése, valamint a jogalkalmazási gyakorlatban felmerülő problémák feltárása állt. A leíró statisztikai módszerek alapját a Legfőbb Ügyészség és az Eurostat nyilvános adatai, továbbá az Europol SIRIUS Jelentés (2024) képezték. A módszertani megközelítés a „vegyes metódus” elvet követi, vagyis a kvantitatív adatok értelmezését kvalitatív szempontokkal egészíti ki, ahogy azt Alan Bryman javasolja a komplex társadalmi jelenségek vizsgálatánál.[2] A kvalitatív szemlélet elsősorban a szöveges tartalmak értelmezésére, a kvantitatív megközelítés pedig a statisztikai trendek és mintázatok feltárására irányult, ezáltal biztosítva az eredmények többdimenziós értékelését. A kutatási folyamat elméleti megalapozásánál Kovács Éva szerkesztésében megjelent „Közösségtanulmány, Módszertani jegyzet” ajánlásait is figyelembe vettem, amely hangsúlyozza, hogy a kvalitatív elemzés nem csupán adatgyűjtő, hanem értelmező és kontextusteremtő funkcióval is bír.[3] Ennek megfelelően az értekezés a jogi normák társadalmi beágyazottságát is vizsgálta, különös tekintettel az online bűnözés és a digitális szocializáció összefüggéseire.

[2]Bryman, Alan: *Social Research Methods.* 4. kiadás. Oxford, Oxford University Press, 2012**.** 766 o., 35–41. o.
[3] Kovács Éva (szerk.): Közösségtanulmány Módszertani jegyzet. Budapest 2007, pp. 11–18.

A kutatás feltáró elemző jellegű, és négy egymásra épülő szakaszra tagolható. Az első szakasz az elméleti és fogalmi keretek kialakítására irányult, melynek során meghatároztam a kutatás alapkategóriáit, definícióit és kérdésfelvetéseit. A második szakaszban sor került a jogforrások és a szakirodalom szisztematikus elemzésére, a deduktív kutatási modell alkalmazásával. A harmadik szakaszban a vizsgálat esettanulmány-alapú megközelítést követett, konkrét ügyek (például a Runescape-ügy, a WannaCry-támadás vagy az ILOVEYOU-vírus) elemzésén keresztül. A negyedik, záró szakasz az eredmények szintetizálását és a hipotézisek megerősítését célozta, valamint jogalkotási és jogalkalmazási következtetések levonásával zárult. A módszertani megoldások megválasztását az a törekvés határozta meg, hogy az értekezés tudományosan megalapozott, rendszerezett és reprodukálható módon járuljon hozzá a kiberbűnözés és a XXI. századi bűncselekmények nyomozásának elméleti és gyakorlati megértéséhez. A vizsgálat célja, hogy a társadalomtudományi kutatás racionalitását és a büntetőjogi dogmatika mélységét egyaránt figyelembe véve elősegítse a tudományos hitelesség és a gyakorlati relevancia összhangját.[4] A kutatás újszerűsége módszertani értelemben abban áll, hogy a klasszikus jogi-dogmatikai elemzést kiegészíti a technológiai és kriminológiai megközelítésekkel, ezáltal interdiszciplináris kutatási modellt hoz létre. Ez a megközelítés lehetővé tette, hogy a jogi normák és eljárási szabályok elemzése során figyelembe vegyem az informatikai, adatvédelmi és társadalomtudományi összefüggéseket is. A digitális bűncselekmények vizsgálata során ezért nem csupán a jogi szövegeket és joggyakorlatot elemeztem, hanem azokat a technológiai-forenzikus eszközöket és folyamatokat is, amelyek a bizonyítékok megszerzésében és értékelésében kulcsszerepet játszanak. A módszertani innováció lényege, hogy a kutatás a jogtudomány és az információtechnológia határterületén mozgó kérdéseket egységes elemzési keretbe vonta, ezáltal hozzájárulva a digitális bűnözés tudományos feldolgozásának fejlődéséhez.

2. Bevezetés

[4]Kovács Éva (szerk.): Közösségtanulmány Módszertani jegyzet. MTA Szociológiai Kutatóintézet, Budapest, 2007. 11–18. o.

A XXI. század bűncselekményeinek nyomozása egyre összetettebbé válik, mivel a bűnelkövetők olyan új technológiai eszközöket használnak, amelyek sokszor meghaladják a hagyományos nyomozási módszerek lehetőségeit. Az új bűncselekménytípusok, mint például a kibertámadások, az adathalászat, a zsarolóvírusok, valamint az online pénzügyi és gazdasági bűncselekmények jelentős kihívást jelentenek a hatóságok számára.

2.1. A XXI. századi bűncselekmények jellemzői

A bűnözés jellegének átalakulása a történelem során mindig is szorosan kapcsolódott a társadalmi, technikai és gazdasági átalakulásokhoz. A XXI. század elejére a digitális forradalom és a globalizáció, valamint az ezek nyomán létrejött új társadalmi és gazdasági struktúrák jelentős hatást gyakoroltak a bűnözés fejlődésére. Az új technológiai eszközök megjelenése, az internet globális hálózattá válása, valamint a nemzetközi kereskedelem átrendeződése lehetőséget teremtett új bűncselekmények megjelenésére, miközben a korábbi bűnözési módok is jelentős átalakuláson mentek keresztül. Ezek a bűncselekmények egyre inkább a technológia állandó változására, újítására, fejlesztésére ugyanakkor a globális jellegére és az adatközpontúságra is épülnek, amelyek mind új kihívásokat jelentenek a jogalkotás és a bűnüldözés számára egyaránt.

2.2. A digitális kor bűnözési formái és a társadalmi kihívások

A személyi számítógépek forradalmasították az elektronikus információ feldolgozását. Az IBM PC 5150-et 1981. augusztus 12-én mutatták be, és ez vált a későbbi „PC-kompatibilis” iparági szabvánnyá.[5] A személyi számítógép (PC) önálló, végfelhasználó által kezelt kisebb méretű gép volt, saját billentyűzettel, processzorral, operatív memóriával és monitorral rendelkezett. A PC elterjedése hihetetlen gyorsasággal zajlott,

[5]IBM: The IBM PC. https://www.ibm.com/history/personal-computer (letöltés dátuma: 2021. október 17.)

mindössze négy év alatt elérte a több száz millió felhasználót világszerte.[6] Az Internet, amely napjainkra globális hálózattá vált, és felhasználók milliárdjait kapcsolja össze, egy amerikai katonai kutatás eredményeként jött létre. Az ARPANET, a világ első nagy számítógépes hálózata, az Egyesült Államok Védelmi Minisztériumának kutatási részlege, a DARPA által 1969-ben indult el.[7] Kezdetben az UCLA, a Stanford Research Institute, a University of California Santa Barbara és a University of Utah voltak a hálózat első tagjai.[8] Ezen hálózat célja az egyetemek közötti kutatások és kommunikáció forradalmi átalakítása volt, ami alapot teremtett a világméretű oktatási reformok és tudományos együttműködések számára. Az európai internetes kapcsolatok kiépítése 1982-ben az EUNET hálózattal folytatódott, amely a kontinens első internetes szolgáltatásait biztosította.[9] Az 1980-as évek közepére az internet fokozatosan függetlenedett katonai eredetétől, és széles körben elérhetővé vált a civil felhasználók számára is. Az Internet mára világméretű hálózattá nőtte ki magát, amely az ún. World Wide Web (WWW) technológia segítségével biztosítja az információ gyors és hatékony megosztását.[10] A világméretű hálózat kialakulása új tereket nyitott meg az emberek egymás közötti kommunikációjában. A modern kommunikációs eszközök, mint a számítógépek, tabletek és okostelefonok, lehetővé tették az emberek számára, hogy bárhol és bármikor kapcsolatba léphessenek egymással, és információkat cserélhessenek. Az online kommunikáció forradalmasította a bűnözési módszereket, és új kihívásokat állított a jogalkotók és a bűnüldöző szervek elé. A közösségi platformok elterjedése szintén jelentős hatással volt a bűnözés alakulására a XXI. században. Az első közösségi hálózatok, mint például az amerikai „classmates.com” és a MySpace, az 1990-es évek végén jelentek meg, majd a Facebook hozta el a közösségi média világméretű áttörését. Mark Zuckerberg ötlete a Harvard Egyetemen született meg, és a Facebook hamarosan globális jelenséggé vált.[11] 2008 novemberében Magyarországon is megjelent a Facebook,

---

[6]Tarmo Virki (Reuters): Computers in use pass 1 billion mark: Gartner. https://www.reuters.com/article/technology/computers-in-use-pass-1-billion-mark-gartner-idUSL23245254/ (letöltés dátuma: 2025. október 17.)

[7]SRI International: ARPANET (History of Innovation). https://www.sri.com/hoi/arpanet/ (letöltés dátuma: 2021. október 17.)

[8] SRI International: ARPANET (2021).

[9]NLnet Foundation: Forty years of EUnet. https://nlnet.nl/press/20220401-fourtyyearsofeunet.html (letöltés dátuma: 2021. október 17.)

[10]CERN: Short history of the Web.https://home.cern/science/computing/birth-web/short-history-web (letöltés dátuma: 2021. október 17.)

[11]Encyclopaedia Britannica: Social network. https://www.britannica.com/technology/social-network (letöltés dátuma: 2021. október 17.)

amely azóta is az egyik legnépszerűbb online közösségi platform. A közösségi hálózatok lehetőséget biztosítanak a felhasználóknak arra, hogy kapcsolatot tartsanak egymással, információkat osszanak meg és különböző témákat vitassanak meg. Ugyanakkor ezek a platformok új lehetőségeket adnak a bűnözőknek is, hogy ezeket a platformokat felhasználva kövessék el a bűncselekményt. Szükségessé vált ezeknek a platformoknak az átfogóbb szabályozása, mivel az ilyen elkövetési eszközök használata miatt a bűncselekmények enyhébb szankciókkal járhatnak, noha a technológia alkalmazása nélkül, hagyományos értelemben véve, ugyanazon cselekmény súlyosabb bűncselekménynek minősülne, és ezáltal szigorúbb büntetést vonna maga után.

A XXI. századi bűnözés egyik legmeghatározóbb sajátossága a *digitalizáció* és az internetes technológiák széles körű elterjedése, amely új típusú bűncselekmények megjelenéséhez vezetett. A modern korban az elkövetők egyre inkább a digitális térre koncentrálnak, kihasználva az internet decentralizált jellegét és a virtuális környezetben rejlő lehetőségeket. Az elkövetés gyakran anonim módon és rendkívül gyorsan történik, miközben az olyan bűncselekmények, mint a kibertámadások, az adathalászat, a zsarolóvírus-támadások vagy a digitális eszközök feltörése, komoly kihívás elé állítják a bűnüldöző hatóságokat. A digitális bűnözés sajátossága, hogy az elkövetők földrajzilag egymástól távoli helyszínekről is képesek támadásokat indítani, amelyek hatásai globális szinten is érzékelhetők. A világméretű összekapcsoltság következményeként egyre gyakoribbak a több ország joghatóságát érintő ügyek, amelyek jelentősen megnehezítik a nyomozást és az igazságszolgáltatási együttműködést. A modern bűnözés másik meghatározó jellemzője az *adatalapúság*. A digitális társadalomban az adatok és az információk önálló gazdasági értékkel bírnak, így a bűncselekmények gyakran ezek megszerzésére, felhasználására, manipulálására vagy megsemmisítésére irányulnak. Ez a tendencia különösen aggasztó, mivel az adatokkal összefüggő jogsértések nem csupán anyagi károkat okozhatnak, hanem a személyes adatok védelmét és az azokba vetett társadalmi bizalmat is alááshatják, ez pedig a digitális gazdaság és a modern társadalom működésének egyik alapfeltétele. Ennek következtében a hatóságoknak és a szervezeteknek folyamatosan fejleszteniük kell az adatvédelem és a kiberbiztonság területén alkalmazott technológiáikat, hogy lépést tarthassanak az egyre kifinomultabb és gyorsan változó fenyegetésekkel.

2.3. A XXI. századi bűncselekmények új dimenziói: A kiberbűnözés aktuális kérdései

A XXI. század elejére a digitalizáció és az internet használat könnyen elérhetővé válása a bűnözés terén is új korszakot nyitott. Soha nem látott mértékben vált lehetővé az, hogy a bűncselekményeket földrajzi határok nélkül, anonim módon vagy álnéven, automatizált eszközökkel kövessék el. Ennek eredményeként a kiberbűnözés (vagyis az információs technológia eszközeivel megvalósított bűncselekmények köre) a bűnözés egyik legdinamikusabban növekvő területévé vált.[12] E tendenciát támasztják alá a statisztikai adatok is amelynek alapján megállapítható az, hogy Magyarországon az „információs rendszer vagy adat megsértése" néven nyilvántartott bűncselekményből 2018-ban alig 217 esetet regisztráltak, míg 2020-ban már 830-at, 2021-ben, 2022-ben, és 2023-ban pedig tovább emelkedett a regisztrált bűncselekmények száma míg 2024-re már 1488-ra növekedett az esetszám.[13][14] Hasonló arányban nőtt az információs rendszer felhasználásával elkövetett csalások száma is (2018-ban 1167 eset, 2020-ban 3400 eset, 2024-ben 15171 eset).[15] Magyarországon, a kiberbűncselekmények által okozott károk immár éves szinten elérik a tízmilliárdos nagyságrendet, mindamellett az sem elhanyagolható tény, hogy az áldozatok száma pedig mára már tízezres nagyságrendű.[16] Egy friss felmérés szerint hazánkban csupán egyetlen év alatt mintegy 30 milliárd forint kár keletkezett a kiberbűnözés következtében.[17] Mindez jól tükrözi azt, hogy a kiberbűnözés a XXI. századi bűnözés egyik legjelentősebb kihívásává vált, amelyre a nemzeti jogrendszereknek és a nemzetközi közösségnek egyaránt választ kell adnia.[18] A

---

[12]Noha a kibertér fogalmára vonatkozóan nem létezik egységesen elfogadott, általános definíció, a Nemzeti Média- és Hírközlési Hatóság (NMHH) értelmezése szerint a kibertér „globálisan összekapcsolt, decentralizált elektronikus információs rendszerek és az ezeken keresztül zajló társadalmi, gazdasági folyamatok összessége."

[13]Belügyminisztérium Statisztikai Rendszere: Regisztrált bűncselekmények. Elérhető: https://bsr-sp.bm.hu/SitePages/ExcelMegtekinto.aspx, letöltés dátuma: 2024. 01. 10.

[14]Belügyminisztériumi statisztikák (2018-2020) közötti adatok: *Biztosítási Szemle* cikk, 2022.01.11. (MABISZ) adatai alapján (BSR): 2018: ~200; 2020: 830; 2021 (szeptemberig): 831 regisztrált eset; informatikai csalás 2018: ~1100, 2020: ~3400.

[15]Uo.: Regisztrált bűncselekmények. Elérhető: https://bsr-sp.bm.hu/SitePages/ExcelMegtekinto.aspx, letöltés dátuma: 2024. 01. 10.

[16]KiberPajzs (Mastercard kutatás, 2025): Éves szinten tízezres számú áldozat és tízmilliárdos nagyságrendű kár Magyarországon (2024-es adatok). Lásd: KiberPajzs hír (2025. február 20.)

[17] Uo., Magyarországon ~30 milliárd Ft kár egy év alatt a kiberbűnözés miatt (Mastercard felmérés).

[18] Szabó Barbara: Digital Crime: New Challenges for Criminal Justice Systems. Tomita, Mihaela – Ungureanu, Roxana (szerk.): Designing the Future of Criminal Justice System Under the Lens of Technology. International Conference "Multidisciplinary Perspectives in the Quasi-Coercive Treatment of

jelen fejezet célja, hogy átfogóan bemutassa a kiberbűnözés fogalmát és fejlődését, a vonatkozó jogszabályi hátteret (különös tekintettel a magyar szabályozásra és nemzetközi kitekintéssel), továbbá elemezze a kiberbűncselekmények főbb típusait.

2.4. A kiberbűnözés fogalma és fejlődése

A kiberbűnözés fogalmát egységesen nehéz meghatározni, mivel számos különböző jelenséget foglal magában ugyanakkor kijelenthető az, hogy a szakirodalomban a fogalom értelmezése sem egységes, eltérő megközelítések és definíciós kísérletek jellemzik, amelyek gyakran kontextusfüggően, különböző tudományos paradigmák mentén artikulálódnak.[19] Ugyanakkor általánosan elfogadott az megközelítés, miszerint kiberbűnözésnek tekintjük mindazon bűncselekményeket, amelyeket számítástechnikai eszközök vagy az internet felhasználásával követnek el.[20] A nemzetközi szakirodalomban bevett felosztás szerint megkülönböztethetünk „*cyber-dependent*" tehát „kiberfüggő" azaz a kizárólag információs rendszerek ellen irányuló, azokat célzó és „*cyber-enabled*" tehát „kiberrel támogatott" avagy „digitális eszközökkel elősegített" azaz informatikai eszközökkel megkönnyített, „hagyományos" bűncselekményeket.[21] Az előbbiek körébe tartoznak a számítógépes rendszerek működését vagy a bennük lévő adatok bizalmasságát, sértetlenségét veszélyeztető támadások (például a hackelés, károkozó programok terjesztése), míg az utóbbiak körében olyan klasszikus deliktumok jelennek meg új köntösben, mint a csalás, zsarolás, pénzmosás vagy zaklatás, amelyeket az információs technológia eszközei révén könnyebben, szélesebb körben lehet elkövetni.[22][23] A technológiai újítások által felmerülő új fenyegetések okán folyamatos

---

Offenders" (SPECTO – 8th Edition), 16–17 May 2024, Timișoara, Romania. Bologna, Filodiritto Editore, 2024. ISBN 979-12-80225-72-6, DOI: 10.26352/I516-SPECTO-2024. 122-132. p.

[19]1978-as évi IV. törvény 300/C. 1978. évi IV. törvény a Büntető Törvénykönyvről (Btk.) 300/C. § Számítógépes csalás (1989-ben beiktatott rendelkezés).

[20]Uo., Magyarországon ~30 milliárd Ft kár egy év alatt a kiberbűnözés miatt (Mastercard felmérés: Mastercard Research: Cybercrime in Hungary 2023 Annual Loss Estimation. https://www.mastercard.hu/hu-hu/consumers/saferfuture/cybercrime.html (letöltés dátuma: 2024. február 10.))

[21]Clough, Jonathan: *Principles of Cybercrime*. Cambridge University Press, Cambridge,. 10–11. o., 2015; (*hasonló felosztást alkalmaz az Europol is (cyber-dependent vs. cyber-enabled crime)).*

[22]U.o.

[23] Szabó Barbara: Crimes Committed on Online Surfaces. In: Tóth Dávid (szerk.), Az internet és a közösségi média jogi kihívásai – Konferenciakötet. Pécs: PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, 2022. pp. 80–87. 8 p. ISBN: 9789634299929

reakcióra kényszerül a jogalkotás amelyet a kibertérben elkövetett bűncselekmények történeti fejlődése is indokol.[24]Magyarországon már az 1980-as évek végén megjelent az igény a számítógépes bűnözés elleni fellépésre. Az 1978. évi IV. Büntető Törvénykönyvet ekkor egészítették ki a számítógépes csalás külön tényállásával (300/C.§ Számítástechnikai rendszer és adatok elleni bűncselekmény).[25] Azóta a hazai jogalkotás és joggyakorlat igyekezik összhangba hozni megoldásait a nemzetközi gyakorlattal. A korai számítógépes bűncselekmények (pl. illetéktelen hozzáférés egyszerű esetei vagy esetleges primitív vírusok) után napjainkra jóval szerteágazóbb illetőleg professzionálisabb módszerek jelentek meg. Az 1990-es évektől az internet elterjedése új dimenziót nyitott meg. Megjelentek az első online térben szerveződő csalások, hackercsoportok és vírusjárványok, mint például az ILOVEYOU vírus, amely 2000-ben komoly károkat okozott világszerte. Az ILOVEYOU-vírus, más néven a „Love Letter", egy számítógépes féreg (worm) típusú kártékony program, amely 2000. május 4-én jelent meg, és az informatika fejlődésének történetében az egyik legjelentősebb globális kibertámadását idézte elő. A vírus Visual Basic Script (.vbs) nyelven íródott, és elsősorban e-mail üzenet formájában terjedt, amelynek tárgya „ILOVEYOU" volt, a melléklete pedig „LOVE-LETTER-FOR-YOU.TXT.vbs" néven szerepelt.[26] Sok felhasználó számára a kettős kiterjesztés azt a látszatot keltette, hogy egy ártalmatlan szöveges fájlról van szó, azonban a megtévesztés egyik kulcseleme a melléklet elnevezésében rejlett és valójában egy végrehajtható szkriptet azaz parancsfájlt tartalmazott. A fertőzés exponenciálisan gyors ütemben terjedt világszerte, ugyanis aktiválódása után a féreg automatikusan továbbította önmagát a Microsoft Outlook levelezőprogram címjegyzékében szereplő minden e-mail címre. Emellett a vírus manipulálta a fertőzött rendszer fájljait is, többek között felülírta a multimédiás fájlokat (pl. JPEG, MP3) és más fájltípusokat, amely eredményképp adatvesztést okozott ezen tevékenység által.[27] A program egyes variánsai képesek voltak a jelszavak kinyerésére is, ezáltal még súlyosabb adatvédelmi kockázatokat generálva. A kártevő a megjelenését

[24]BH 1989.184. számú eset.
[25]Polt Péter: *A számítástechnikai bűnözés büntetőjogi megítélése.* Budapest, Közgazdasági és Jogi Könyvkiadó, 1983. p. 27.
[26]Schneier, Bruce: Secrets and Lies: Digital Security in a Networked World. New York, Wiley, 2000. 368 o. ISBN: 978-0471253112.
[27]Gerő Péter – Endersz Péter: *Biztonságosan és magabiztosan II. Az openSUSE operációs rendszer (GNOME kezelőfelülettel).* https://mek.oszk.hu/09300/09321/pdf/biztonsagosan2gnome.pdf (letöltés dátuma: 2021. április 14.)

követő 24 órán belül több millió számítógépet fertőzött meg, köztük kormányzati hivatalokat, multinacionális vállalatokat és pénzintézeteket is. A becslések szerint az ILOVEYOU-vírus által okozott közvetett és közvetlen gazdasági kár meghaladta az 5,5 milliárd amerikai dollárt, egyes források szerint pedig akár elérhette a 10 milliárd dollárt is.[28] A vírus készítőjeként a Fülöp-szigeteki Onel de Guzmant azonosították, aki feltehetően szakdolgozati projektként kezdett el foglalkozni a programozásával. Mivel a jogrendszer 2000-ben még nem rendelkezett konkrét szabályozással az ilyen típusú kiberbűncselekményekkel kapcsolatban, (kiváltképpen nem a Fülöp-szigeteki), így a készítőt végül nem vonták jogi felelősségre. Álláspontom szerint az eset jelentősége messze túlmutat egyetlen kibertámadás keretein, mivel jól példázza, hogy a digitális fenyegetések milyen súlyos hatással lehetnek nemcsak az érintettekre, hanem a társadalom szélesebb rétegeire is. Az eset bemutatása azért indokolt, mert világosan rávilágít az informatikai rendszerek sebezhetőségére, a felhasználók információbiztonsági tudásának hiányosságaira, valamint arra, hogy az e-mail alapú támadások még ma is rendkívül hatékony eszköznek számítanak a kiberbűnözők kezében. A nemzetközi közösség a problémára az elsők között az OECD iránymutatásaival reagált (1992), majd az Európa Tanács 1990. évi 9. sz. ajánlása sorolta fel a számítógépes bűncselekmények körét.[29][30] Mindezen tendenciák megalapozták a 2001-ben elfogadott Budapesti Egyezmény létrejöttét, amely az első átfogó nemzetközi jogi dokumentumként foglalkozik a cyberbűnözés egyes kérdéskörével.[31]

2.5. A XXI. századi technológiai változásokhoz igazodó szabályozási keretek kialakítása

2.5.1. A Számítástechnikai bűnözésről szóló Egyezmény és annak jelentősége

[28]CERT Advisory CA-2000-04: *Love Letter Worm.* United States Computer Emergency Readiness Team (US-CERT), 2000. https://www.cert.org/advisories/CA-2000-04.html (letöltés dátuma: 2024. december 14.)
[29]OECD: *Guidelines for the Security of Information Systems and Networks.* Paris, Organisation for Economic Co-operation and Development, 1992.
[30]Európa Tanács Miniszteri Bizottsága: R (89) 9. számú ajánlás a számítógéppel kapcsolatos bűncselekményekről. Strasbourg, 1990.
[31]Council of Europe: *Convention on Cybercrime (ETS No. 185).* Budapest, 2001. Magyarországon kihirdette: 2004. évi LXXIX. törvény.

A Számítástechnikai bűnözésről szóló Egyezmény, amelyet az Európa Tanács készített elő és 2001. november 23-án Budapesten fogadtak el, egy átfogó nemzetközi megállapodás, amelynek az a fő célja, hogy egységesítse a tagállamok jogrendszerét a számítástechnikai bűncselekmények elleni küzdelem terén.[32] Az Egyezmény, amely Magyarországon a 2004. évi LXXIX. törvény formájában került kihirdetésre és hatályba, nemcsak a bűncselekmények kriminalizálására, hanem azok felderítésére, nyomozására ugyanakkor a nemzetközi együttműködésre is vonatkozik, továbbá normatív törekvése, az egyes tagállamok büntetőjogi szabályozásának harmonizálása. Az Egyezmény meghatározza azokat a bűncselekményeket, amelyek különösen jelentős veszélyt jelentenek a digitális társadalom számára, és amelyek kriminalizálása szükséges a hatékony jogi védelem biztosításához. Az alábbiakban indokoltnak látom, hogy részletesen bemutassam azokat a bűncselekményeket, amelyek az Egyezmény hatálya alá esnek. Ennek során valamennyi releváns tényállást külön-külön, részletező módon kívánom tárgyalni, különös tekintettel azokra a jellegzetességekre, amelyek miatt ezek a cselekmények fokozott társadalmi veszélyességet hordoznak, és amelyek szükségessé teszik büntetőjogi szabályozásukat.

2.5.2. Büntető anyagi jog: Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sérthetetlensége és titkossága elleni bűncselekmények az Egyezmény tükrében

A jogosulatlan belépés alapvető védelmet biztosít a számítástechnikai rendszerek számára az engedély nélküli, illetéktelen hozzáférés ellen.[33] Súlyos következményekkel járhat a számítástechnikai rendszerek (amelyek lehetnek például vállalati hálózatok, állami rendszerek vagy akár személyes eszközök) elvesztése, módosítása vagy eltulajdonítása, ugyanis, rendkívül fontos és kritikus információkat tartalmazhatnak. Véleményem szerint ez kiemelt fontossággal bír a nemzetközi közösség számára a XXI.

[32]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), ETS 185. https://rm.coe.int/16802fa405 (letöltés dátuma: 2022. április 29.)
[33]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 2. cikk Jogosulatlan belépés, ETS 185. Elérhető: https://rm.coe.int/16802fa405 (letöltés dátuma: 2022. 04. 29.)

században, melyet az egyezmény rendelkezése is egyértelműen támogat, hiszen tükrözi, hogy a felelősségre vonás mellett a megelőzés támogatása is fontos elem. Előírja, hogy minden szerződő fél köteles olyan jogszabályokat és egyéb intézkedéseket elfogadni, amelyek alapján a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan, szándékos belépés bűncselekménynek minősül. Ez az előírás kiterjed a számítástechnikai rendszerek minden formájára, legyen az egyetlen eszköz vagy több eszköz összekapcsolt rendszere. Az illetéktelen, jogellenes behatolásokkal szemben, a potenciális károkozási tevékenységet és biztonsági fenyegetések esetleges bekövetkeztét, a jogszabályi intézkedés céljának megfelelve, a számítástechnikai rendszer védelmét megelőző módon kell biztosítani. Mindazonáltal a rendelkezés kifejezetten megköveteli, hogy a jogosulatlan belépés esetén szándékosság álljon fenn. Ez azt jelenti, hogy a cselekmény csak akkor minősül bűncselekménynek, ha cselekményeinek következményeit kívánja vagy e következményekbe belenyugszik az elkövető, más szóval tudatosan hajtotta végre az informatikai rendszerekbe való behatolást. A szándékosság hangsúlyozása azért lényeges, mert az egyén büntetőjogi felelősségre vonása elkerülhető, a véletlen vagy akaratlan módon történő hozzáférés esetén. Ugyanakkor a 2. cikk lehetőséget ad a szerződő felek számára, hogy meghatározzák, a jogosulatlan belépés bűncselekménynek minősítéséhez szükséges-e a biztonsági intézkedések megsértése. Ez azt jelenti, hogy vizsgálni kell, hogy az elkövető szándékosan megkerülte-e a rendszer védelmi intézkedéseit, mint például a jelszavakat, a tűzfalakat vagy egyéb más védelmi mechanizmusokat. Amennyiben az illetéktelen hozzáférés ezen biztonsági intézkedések megsértésével történik, az még súlyosabb bűncselekménynek minősülhet, ami tovább növeli az elkövető felelősségét. Továbbá biztosítja a feltételeket ahhoz, hogy a szerződő felek bűncselekménynek minősítsék azokat az eseteket is, amikor a jogosulatlan belépés célja számítástechnikai adatok megszerzése vagy más tisztességtelen célok elérése. Ez az opció lehetővé teszi a tagállamok számára, hogy az elkövetők motivációját is figyelembe vegyék a bűncselekmény súlyosságának megítélésekor. Példának okán, ha a jogosulatlan belépés célja az érzékeny adatok ellopása, a cselekmény súlyosabb minősítést kaphat, mint ha a behatolás csupán kíváncsiságból történt.

A jogosulatlan kifürkészés jelentősége abban rejlik, hogy védi a számítástechnikai rendszerekben tárolt, továbbított adatok titkosságát, integritását, illetve az onnan származó adatok jogosulatlan kifürkészésével kapcsolatos bűncselekményeket

szabályozza, valamint, hogy büntethetővé tegye az olyan cselekményeket, amelyek során valaki jogosulatlanul fér hozzá vagy figyeli meg a számítástechnikai rendszerekből származó adatokat, különösen, ha ezt technikai eszközök felhasználásával teszi.[34] A digitális korszakban a bizalmas adatok, (példának okán az üzleti titkok, személyes információk vagy állami titkok) jogosulatlan kifürkészése komoly károkat okozhat az individuumoknak, gazdasági szereplőknek és közigazgatási szerveknek egyaránt. Álláspontom szerint a rendelkezés hatékonyan hozzájárul a digitális információk védelméhez, mivel kriminalizálja azon jogellenes magatartásokat, amelyek során valamely személy jogosulatlanul fér hozzá vagy figyeli meg ezeket az adatokat. E körben különösen érzékenyek a titkosított vagy egyéb módon védett adatok, amely különösen hangsúlyos biztonsági rendszerek, távközlési hálózatok és adatbázisok esetében.

A cikk kimondja, hogy a bűncselekmény megvalósulásához a cselekménynek szándékosnak és jogosulatlannak kell lennie. Az elkövető tehát tudatosan és célzatosan kell, hogy hozzáférjen az adatokhoz, illetve figyelje meg azokat anélkül, hogy erre jogosultsága lenne. A kifürkészés alatt nemcsak az adatok közvetlen hozzáférése értendő, hanem az is, ha valaki technikai eszközök segítségével kifürkészi a számítástechnikai rendszerek által küldött adatokat, beleértve az elektromágneses sugárzást, amely az adatokat továbbítja. Az adatkommunikációs csatornák védelme szempontjából ez a rendelkezés különösen fontos. Továbbá hangsúlyozza a nem nyilvános, pontosabban titkos vagy bizalmas információk védelmét, másként fogalmazva a bűncselekmény akkor valósul meg, ha az elkövető ilyen típusú adatokat férkőz ki engedély nélkül, ezzel megsértve az adatok titkosságát. Ugyanakkor lehetőséget biztosít a szerződő felek számára, hogy meghatározzák, a jogosulatlan kifürkészés büntethetőségéhez szükséges-e bizonyos tisztességtelen célok megléte. Ez azt jelenti, hogy a nemzeti jogalkotás előírhatja, hogy a kifürkészés célja valamilyen tisztességtelen előny megszerzése legyen. Emellett a rendelkezések lehetővé tehetik a bűncselekmények szankcionálását akkor is, ha a kifürkészett adatok egy másik számítástechnikai rendszerből származnak.

A számítástechnikai adat megsértése a számítástechnikai adatokkal kapcsolatos jogellenes cselekményeket szabályozza, amelyek célja az adatok megsértése,

[34]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 3. cikk Jogosulatlan kifürkészés, ETS 185. Elérhető: https://rm.coe.int/16802fa405 (letöltés dátuma: 2022. 04. 29.)

megkárosítása vagy megsemmisítése.[35] Minden olyan cselekmény bűncselekménynek minősül e rendelkezés szerint, amelynek során jogosulatlanul törölnek, megrongálnak, megváltoztatnak, megsemmisítenek vagy szándékosan megkárosítanak számítástechnikai adatokat. Az adatok megsértése kiterjedhet az adatok tartalmának, formátumának, vagy elérhetőségének megváltoztatására, amelyek következtében az adatok elveszíthetik megbízhatóságukat vagy használhatóságukat. A cikk elősegíti, hogy a szerződő felek meghatározzák azt, hogy csak akkor minősül a cselekmény bűncselekménynek, ha az jelentős kárt okoz. Ez a rendelkezés lehetővé teszi, hogy a jogszabályok különbséget tegyenek a kisebb, esetleg nem szándékos adatkárosítások és a súlyos, szándékos cselekmények között. Megítélésem szerint, a modern információs társadalomban az elektronikus adatok sérülése vagy elvesztése jelentős gazdasági, társadalmi, valamint biztonsági kockázatot jelenthet ezért az adatok biztonságának biztosítása és az adatok megbízhatósága rendkívül fontos mindamellett, hogy az integritása alapvető követelmény.

Az 5. cikk, azaz *a számítástechnikai rendszer megsértése* a számítástechnikai rendszerek működésének jogosulatlan megzavarását és akadályozását szabályozza, és kiterjed minden olyan cselekményre, amely szándékosan és jogosulatlanul befolyásolja a számítástechnikai rendszer rendeltetésszerű működését, ezzel veszélyeztetve a rendszer stabilitását és megbízhatóságát.[36] A digitális infrastruktúra kritikus elemei körében ahol úgy vélem, hogy a stabilitás és a folyamatos működés alapvető kritérium súlyos következményekkel járhatnak az ilyen cselekmények. Az akadályozás többféle módon is megvalósulhat, többek között számítástechnikai adatok bevitelével, adatok továbbításával, adatok megkárosításával, törlésével, megrongálásával vagy megváltoztatásával is.

Számítástechnikai adatok bevitelével például a túlterheléses támadás (úgynevezett: DDoS) során, a fő cél az, hogy a rendszer leállítása vagy annak működésének lelassítása következzen be. Ezt az elkövető azáltal tudja elérni, hogy a rendszerbe nagy mennyiségű adatot küld. Tegyük fel azt, hogy a szolgáltatás teljes leállítása az elkövető célja. Ebben

---

[35]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 4. cikk. Számítástechnikai adat megsértése, ETS 185. Elérhető: https://rm.coe.int/16802fa405 (letöltés dátuma: 2022. 04. 29.)

[36]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 5. cikk Számítástechnikai rendszer megsértése, ETS 185. Elérhető: https://rm.coe.int/16802fa405 (letöltés dátuma: 2022. 04. 29.)

az esetben illetőleg a digitális infrastruktúra elleni támadások során ezen módszer különösen gyakran használt, közkedvelt eszköz az elkövető által. Distributed Denial of Service azaz DDoS, magyar nyelvi megfogalmazásban elosztott szolgáltatás megtagadásos támadás, amely kiberbiztonsági támadási forma. A fő célja az, hogy megbénítsa az adott számítógépes rendszer, hálózat vagy weboldal működését oly módon, hogy azt hatalmas mennyiségű forgalommal túlterhelik. A támadó egy úgynevezett "botnetnek" nevezett eszközhalmazt használ a támadás indításához. Az említett "botnet" eszközhalmaz olyan fertőzött számítógépek vagy okoseszközök, amelyeket korábban rosszindulatú szoftverrel kompromittált a támadó. [37]Levonható az a következtetés, hogy a támadást nem egyetlen számítógépről aktiválja a támadó, hanem a botnet gépei egyidejű és szervezett módon, terhelési céllal, jelentős mennyiségű adatot zúdítanak a célrendszerre, ami ezáltal nem elérhető a felhasználók számára, lelassul, strukturálisan túlterheltté válik.[38] Reprezentatív példaként említhető azon esetkör, amikor egy adott, igazán népszerű webáruház honlapját kifejezetten a karácsonyi vagy az úgynevezett „black friday" (fekete péntek) vásárlási időszakban DDoS-támadás éri, és a túlterhelés miatt a valódi vásárlók nem tudnak hozzáférni az oldalhoz, amely azon túl, hogy kellemetlen mindkét félnek, az adott cégnek jelentős bevételkiesést és reputációs károkat okozhat. A probléma érdemi kibontakozása akkor veszi kezdetét amikor ezen támadások kritikus szolgáltatásokat, például banki rendszereket, állami hatáskörbe tartozó intézmények digitális platformjait, illetve alapvető infrastruktúrát biztosító szolgáltatókat vesznek célba és a lelassulás vagy a teljes megbénításból adódó gazdasági kár okozásán túl a támadók pénzköveteléshez kötik a cselekmény befejezését. (ún. ransom DDoS: zsarolójellegű elosztott szolgáltatás-megtagadás). [39] A védekezés azért különösen nehéz ezen esetekben, mivel a hatékony védelem különféle technológiák és módszerek együttes alkalmazását igényli, mint például terheléselosztók, felhőalapú DDoS-védelmi szolgáltatások (pl. Cloudflare), tűzfalak, forgalomszűrők, valamint a viselkedéselemzésen alapuló védelmi megoldások, amelyek alkalmasak az atipikus

[37]Ahmad, R. – Shah, M. A. – Wahid, A. – Khan, M. A.: Botnets Unveiled: A Comprehensive Survey on Evolving Threats, Detection Techniques, and Future Directions. = *International Journal of Communication Systems* 2024/3, e5056. o. DOI: 10.1002/ett.5056.
[38]Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. = *Pro Futuro* 2018/1, 66–83. o.
[39]Gelgi, Metehan – Guan, Yueting – Arunachala, Sanjay – Rao, Maddi Samba Siva – Dragoni, Nicola: Systematic Literature Review of IoT Botnet DDoS Attacks and Evaluation of Detection Techniques. = *Sensors* (Basel, Switzerland) 2024/11, p. 3571.

adatforgalmi mintázatok detektálására, és lehetővé teszik azok proaktív szűrését még a célrendszer elérését megelőzően.[40]

Adatok továbbításával a rendszerben tárolt adatok jogosulatlan továbbítása, amely megzavarja a rendszer működését. Különösen veszélyes lehet ezen tevékenység, amennyiben a továbbított adatok bizalmasak vagy kritikus jelentőségűek az informatikai rendszer működése szempontjából.

Adatok megkárosításával, törlésével, megrongálásával vagy megváltoztatásával történik, ha az adatok szándékos manipulációja, amely miatt a rendszer nem tud megfelelően működni. Ez magában foglalhatja az adatbázisok vagy egyéb létfontosságú információk szándékos módosítását vagy törlését, amelyek súlyosan károsíthatják a rendszer működését.

Az eszközökkel való visszaélés (6.cikk) azokat a cselekményeket szabályozza, amelyek során valaki jogosulatlanul és szándékosan használ, előállít, terjeszt vagy birtokol olyan eszközöket, amelyek kifejezetten számítástechnikai bűncselekmények elkövetésére szolgálnak. Ezek az eszközök lehetnek szoftverek, hardverek vagy más technológiai eszközök.[41]

A számítástechnikai bűncselekmények elleni küzdelemben számos szoftveres, hardveres és egyéb technológiai eszköz kiemelt szerepet tölt be. Az esetleges manipulációs mintázatok felderítése és jogosulatlan hozzáférések megelőzése mellett a fő cél az adatvédelem valamint a rendszer integritás megőrzése. Az illetéktelen hálózati hozzáféréseket a szoftveres védelem egyik alappillérével, azaz a tűzfalak alkalmazásával korlátozzák. Meghatározó funkciót töltenek be az úgynevezett betörésérzékelő és megelőző rendszerek (IDS/IPS), amelyek folyamatos auditálás és felügyelet alatt tartják a hálózati forgalmat és riasztást adnak ki, ha gyanús tevékenységet észlelnek. A rendszerbe való bejutás illetőleg az adatok manipulálását elősegítő kártékony programok ellen további védelmet képeznek az antivírus és antimalware szoftverek.[42] Szükségszerű

---

[40]Douligeris, C. – Mitrokotsa, A.: DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. = *Computer Networks* 2004/5, pp. 643–666. o. DOI: 10.1016/j.comnet.2003.10.003.
[41]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 6. cikk. Eszközökkel való visszaélés. ETS 185. Elérhető: https://rm.coe.int/16802fa405, letöltés dátuma: 2022. 04. 29.
[42]Firewalls, Intrusion Detection/Prevention, Encryption, and Multi-Factor Authentication in Cybersecurity Solutions. All Academic Research, 2023. Elérhető: https://allacademicresearch.com, letöltés dátuma: 2022. 04. 29.

és hatékony eszközként szolgálnak az adatintegritás-ellenőrző megoldások is, ide sorolandó többek között a hash-értékeken alapuló rendszerek, amelyek képesek észlelni a fájlok vagy adatok jogosulatlan módosítását.[43] A hardveres védelem területén fontos eszközök a hardveres biztonsági modulok (HSM-ek), amelyek kriptográfiai műveleteket hajtanak végre, és biztonságosan tárolják az érzékeny adatokat, például titkosítási kulcsokat. Hasonlóképpen ide sorolhatóak a biztonságos adattárolók, például az olyan SSD-k, amelyek beépített titkosítással és törlésvédelemmel rendelkeznek. Javítják a rendszerhozzáférés biztonsági szintjét a biometrikus azonosító rendszerek, többek között az ujjlenyomat- vagy arcfelismerésen alapuló megoldások, amelyek jelentősen csökkentik az illetéktelen felhasználás kockázatát. A blockchain-alapú adattárolás a legfrissebb technológiai tendenciák részét képezi, amely a digitális adatok módosíthatatlanságát és visszakövethetőségét garantálja, így kiválóan alkalmazható például digitális szerződések vagy pénzügyi tranzakciók esetén.[44] A rendelkezés szerint, ide tartozik az olyan eszközök *előállítása, értékesítése, megszerzése, behozatala, forgalomba hozatala vagy más módon történő hozzáférhetővé tétele*, amelyek kifejezetten számítástechnikai bűncselekmények elkövetésére szolgálnak. A cikk továbbá konkretizálja, hogy mely eszközök számítanak jogellenesnek, beleértve a kifejezetten bűncselekmények elkövetésére létrehozott vagy átalakított eszközöket, mint például azok, amelyek jogosulatlan belépést vagy adatlopást szolgálnak. E körben fontos kiemelni, hogy a számítógépes jelszavak és belépési kódok jogosulatlan birtoklása is bűncselekménynek minősül, ha azokat számítástechnikai bűncselekmények elkövetésére szánják. A cselekmények bűncselekménynek minősüléséhez szándékosság szükséges, azaz az elkövetőnek tisztában kell lennie azzal, hogy az eszközöket jogellenes célokra használják fel. Emellett fontos kiemelni azon tényt, hogy az eszközök tényleges felhasználása nem szükséges a bűncselekmény megállapításához tehát már a birtoklásuk is elegendő, ha azzal a szándékkal történik, hogy a bűncselekmény elkövetésére használják fel őket. Ez alól kivételt képeznek azon esetek, amikor az eszközöket

[43]Stallings, S.: Hash Functions and Their Applications. = *International Journal of Computer Applications* 2011, Elérhető: https://www.researchgate.net/publication/325090921_Hash_Functions_and_Their_Applications, letöltés dátuma: 2022. 04. 29.

[44] Taylor, Paul J. – Dargahi, Tooska – Dehghantanha, Ali – Parizi, Reza M. – Choo, Kim-Kwang Raymond: Blockchain for Cybersecurity: Systematic Literature Review and Directions for Future Research. = Journal of Computer Information Systems 2021, online megjelenés. DOI: 10.1080/08874417.2021.1995914.

engedéllyel végzett kutatásokra vagy rendszerek védelmére használják, ezáltal biztosítva, hogy a jogszabályok ne korlátozzák indokolatlanul a jogos tevékenységeket.

2.6. A számítógéppel kapcsolatos bűncselekmények

A Budapest Egyezmény 7. cikke a számítógépes hamisítás bűncselekményét szabályozza, amely az olyan szándékos és jogosulatlan cselekményekre vonatkozik, amelyek során valaki számítástechnikai adatokat hamisít meg, hoz létre, vagy módosít abból a célból, hogy azokat valódiként ismerjék el vagy használják fel.[45] A cikk célja a számítástechnikai rendszerek és az azokban tárolt adatok integritásának védelme, megelőzve a digitális információk manipulációjából eredő károkat és visszaéléseket. Számítógépes hamisításnak minősül az *adatok jogosulatlan bevitele* olyan számítógépes rendszerbe, amelyek hamis vagy félrevezető információkat eredményeznek, például pénzügyi rendszerekben, csalárd előnyök szerzése céljából. Meglévő *adatok* ***megváltoztatása***, oly módon, hogy azok hamis információkat tükrözzenek, ilyen lehet például egy digitális szerződés feltételeinek módosítása. Véleményem szerint a számítógépes hamisítás tényállásának gyakorlati alkalmazhatóságát kiválóan példázza az az eset, amikor az elkövető az ETR rendszerben módosította egy sikertelen vizsga eredményét, aminek következtében a rendszer azt a látszatot keltette, mintha a vizsga sikeres lett volna, megfelelő érdemjeggyel együtt. Hasonlóképpen ide sorolható annak az informatikusnak az esete is, aki a rábízott informatikai hálózatot kihasználva jogosulatlanul vitt be olyan adatokat a hallgatói nyilvántartásba, amelyek szerint egy hallgató sikeresen teljesített egy vizsgát, noha valójában részt sem vett rajta. E két eset jól szemlélteti, hogy a számítógépes hamisítás bűncselekményi tényállása a gyakorlatban is egyértelműen alkalmazható olyan beavatkozásokra, amelyek súlyosan sértik az információs rendszerek integritását és megbízhatóságát.[46][47]

Adatok szándékos törlése vagy megsemmisítése, amely példának okán valótlan adatok megjelenéséhez vagy elrejtéséhez vezethet. Az adatok integritásának védelme érdekében,

---

[45]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. 7. cikk Számítógéppel kapcsolatos hamisítás. ETS 185. Elérhető: https://rm.coe.int/16802fa405, letöltés dátuma: 2022. 04. 29.
[46] EBH 2009.2033. I.
[47] BH 2009.264. I.

álláspontom szerint a 7. Cikk által szabályozott számítógépes hamisítás elleni rendelkezések kulcsfontosságúak, azonban a gyorsan fejlődő technológiai környezetben önmagukban nem feltétlenül elegendőek a kellően hatékony intézkedéshez.A jogszabályi keretek ugyan lefedik a leggyakoribb visszaélési formákat (mint például az adatok jogosulatlan bevitele, módosítása vagy törlése) azonban a gyakorlat azt mutatja, hogy a bűnelkövetők sok esetben technológiai előnyben vannak a hatóságokkal szemben. A számítógépes bűncselekmények jellege ugyanis egyre komplexebb. A bűnözők gyakran használnak titkosított kommunikációt, elosztott hálózatokat, hamis digitális identitásokat, valamint nemzetközi szervereket, amelyek megnehezítik a nyomozást és a jogérvényesítést.[48] Emellett az is probléma, hogy a bizonyítékgyűjtés technikai és jogi szempontból is kihívást jelent, különösen akkor, ha több ország joghatósága is érintett.

A 8. Cikk *a számítógéppel kapcsolatos csalás* bűncselekményét szabályozza, amely olyan cselekményekre vonatkozik, amelyek során valaki jogosulatlanul és szándékosan használ fel számítástechnikai adatokat vagy rendszereket annak érdekében, hogy anyagi haszonra tegyen szert, vagy másnak anyagi kárt okozzon.[49] A csalás egyik formája során az elkövető jogosulatlanul hozzáfér a rendszer adataihoz és *adatokat visz be, megváltoztatja vagy törli azokat*, hogy anyagi előnyhöz jusson, vagy kárt okozzon másoknak. Példának okán ilyen cselekmények történhetnek banki adatbázis manipulálásával, amelynek esetében lehetővé teszi jogosulatlan átutalások végrehajtását. A másik formája a *számítástechnikai rendszer működésébe való bármilyen beavatkozás,* amelybe beletartozik a rendszer működésének akadályozása, amely révén az elkövető jogtalan előnyhöz jut. Ilyen például bizonyos rendszer blokkolása, ami akár váltságdíj fizetésére kényszeríthet egy szervezetet, mint ahogyan az ransomware támadások esetében történik.

A zsarolóvírus-támadások (úgynevezett ransomware-támadások) olyan rosszindulatú kibertámadások, amelyek során a támadó valamilyen módon (például e-mailes mellékleteken vagy fertőzött weboldalakon keresztül) kártékony programot juttat a célpont számítógépes rendszerébe, amely titkosítja a felhasználó adatait. A támadó a zsarolási célból kriptográfiai úton hozzáférhetetlenné tett adatok visszafejtéséért

[48]Dornfeld László: Fájlmegosztás: a szellemi tulajdonjog legújabb kihívása. Diskurzus 2014/1. szám 4. évfolyam, 54–61. o. Online: http://blszk.sze.hu/iv- evfolyam-2014 (Letöltés ideje: 2023. 07. 07.)
[49]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 8. cikk Számítógéppel kapcsolatos csalás. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)

pénzügyi kompenzációt követel, amelyet rendszerint kriptovaluta formájában kér (pl. Bitcoinban).[5051] Ezek a támadások jellemzően két fázisból állnak. Először a rosszindulatú szoftver beszivárgása következik be az informatikai rendszerbe, amely a fájlokat titkosítja, majd a felhasználónak megjelenik egy üzenet, amelyben a támadó a követelését közvetíti. Az üzenetben a támadó egyértelművé teszi, hogy az adatok visszaállítására kizárólag abban az esetben kerül sor, amennyiben a felhasználó teljesíti az előírt pénzügyi követelést.[52]

Magyarországon is történtek hasonló támadások, többek között önkormányzatok, kórházak és kisvállalkozások váltak célponttá, amit a Nemzeti Kibervédelmi Intézet éves jelentései is dokumentálnak.[53] Ugyanakkor a zsarolóvírusos támadások egyik legismertebb esete a „WannaCry" elnevezésű globális kibertámadáshoz kötődik. A 2017-ben, bekövetkezett incidens világszerte több mint 150 országot érintett, és hozzávetőleg 200 000 informatikai rendszert fertőzött meg, beleértve egészségügyi intézményeket, közfeladatot ellátó szerveket, valamint gazdasági társaságokat is.[54] Megítélésem szerint a digitális rendszerek elleni támadások nem csupán gazdasági és anyagi veszteségeket okoznak, hanem hosszabb távon alapjaiban rendítik meg a felhasználók technológiába vetett bizalmát. Az ilyen incidensek egyre összetettebb jogi, etikai és adatvédelmi kérdéseket vetnek fel, amint arra a releváns szakirodalom is rámutat.[55] Különösen aggasztónak tartom, hogy az áldozatok jelentős része nem fordul a hatóságokhoz, mivel tartanak attól, hogy a pénz követelés kifizetése ellenére sem kapják vissza az adataikat, illetve hogy a bejelentéssel további kockázatokat vállal. Meglátásom szerint a leghatékonyabb védekezés a megelőzésben és a felhasználók tudatosságának

---

[50]Anderson, Ross – Barton, Chris – Böhme, Rainer – Clayton, Richard – van Eeten, Michel J. G. – Levi, Michael – Moore, Tyler – Savage, Stefan: Measuring the Cost of Cybercrime. In: Böhme, Rainer (szerk.): *The Economics of Information Security and Privacy*. Berlin–Heidelberg, Springer, 2013. pp. 265–300. Elérhető: https://doi.org/10.1007/978-3-642-39498-0_12 (letöltés dátuma: 2025. március 13.)

[51]Kaspersky: Ransomware: *What is it and how to protect yourself*. [n.d.]. Elérhető: https://www.kaspersky.com/resource-center/threats/ransomware, letöltés dátuma: 2024. 03. 13.

[52]Europol: *Internet Organised Crime Threat Assessment* (IOCTA) 2020. [n.d.]. Elérhető: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020, (letöltés dátuma: 2024. január 16.)

[53]Nemzeti Kibervédelmi Intézet: Éves kiberbiztonsági jelentés. Elérhető: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf, (letöltés dátuma: 2024. április 16.)

[54]Greenberg, Andy: *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York, Doubleday, 2019.

[55]Axon, Louise – Erola, Arnau – Agrafiotis, Ioannis – Uuganbayar, Ganbayar – Goldsmith, Michael – Creese, Sadie: Ransomware as a Predator: Modelling the Systemic Risk to Prey. = *Digital Threats: Research and Practice* 2023/4, pp. 1–38.

növelésében rejlik. Ennek része kell, hogy legyen az operációs rendszerek és szoftverek rendszeres frissítése, a gyanús e-mailek elkerülése, valamint az adatok rendszeres mentése is.[5657] Úgy gondolom, hogy ezek a lépések nem csupán technikai intézkedések, hanem alapvető felelősségvállalást is jelentenek a digitális biztonság érdekében.

2.7. Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények

A 9. cikk a számítástechnikai rendszerek és hálózatok felhasználásával elkövetett, *gyermekpornográfiával kapcsolatos bűncselekményeket* szabályozza, különös hangsúlyt helyezve a gyermekek védelmére.[58] Az internet és a digitális technológiák rohamos terjedésével párhuzamosan nőtt a gyermekpornográf tartalmak előállításának, terjesztésének és birtoklásának kockázata. Megítélésem szerint ezen rendelkezés kiemelt jelentőséggel bír, mivel a gyermekek online biztonságának garantálása a digitális környezetben is alapvető társadalmi és jogi kötelezettség.[59] Gyermekpornográfiának minősül minden olyan vizuális ábrázolás, amely kiskorú személyt mutat be szexuális tevékenység közben, kiskorúnak tűnő személyt ábrázol hasonló helyzetben, vagy valósághű képeket jelenít meg, amelyek kiskorúakat mutatnak be szexuális magatartásban. A cikk szerint kiskorúnak minősül minden olyan személy, aki még nem töltötte be a 18. életévét, de a szerződő felek dönthetnek úgy, hogy ezt a korhatárt 16 évre csökkentik. A digitális korszakban, ahol a technológiai fejlődés a lehetőségek mellett új veszélyeket is teremtett, különösen fontosnak tartom ezen szabályozás bevezetését. A gyermekek védelme kiemelt társadalmi érdek, hiszen az online térben még kiszolgáltatottabbá váltak, mint korábban. A gyermekpornográfia előállítása, terjesztése és birtoklása a digitális eszközök elérhetőségével és anonimitásával együtt jóval

[56]Nemzeti Kibervédelmi Intézet (2023). *Éves kiberbiztonsági jelentés*. 2023. Elérhető: https://nki.gov.hu (letöltés dátuma: 2024. április 16.)
[57]European Union Agency for Cybersecurity (ENISA): *ENISA Threat Landscape 2022*. 2022. november 3. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, (letöltés dátuma: 2022. április 16.)
[58]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet 9. cikk. Gyermekpornográfiával kapcsolatos bűncselekmények. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)
[59]Szabó Barbara: Problematic internet use, endangering children and minors. In Jámborné, Róth Erika (szerk.) Doktoranduszok fóruma, 2022 Miskolc-Egyetemváros, Magyarország : Miskolci Egyetem, Állam- és Jogtudományi Kar (2023) 232 p. pp. 185-189. , 7 p. ISBN: 9789633583272

könnyebbé vált, ami a védelem fokozását teszi indokolttá. A rendelkezés hangsúlyozza, hogy minden olyan vizuális ábrázolás, amely valódi vagy valósághűen megjelenített kiskorút mutat be szexuális tevékenységben, büntetendő. Különösen előremutatónak tartom, hogy a cikk egységesíti a kiskorúság fogalmát, ugyanakkor lehetőséget ad arra, hogy a tagállamok saját döntésük alapján a tizennyolcadik életévről tizenhatodik életévre csökkentsék a korhatárt. Álláspontom szerint ez a megoldás biztosítja a rugalmas, de egyúttal szigorú védelmet a gyermekek online kizsákmányolásával szemben.

2.8. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

A 10. Cikk a *szerzői vagy szomszédos jogok védelmét* szabályozza, különösen azokra az esetekre összpontosítva, amikor a jogsértést számítástechnikai rendszerek, például az internet használatával követik el.[60] A rendelkezés célja, hogy megerősítse a szellemi tulajdon védelmét a digitális korban, ahol a jogsértések könnyebben elkövethetők, és az internetes környezetben nehezebben kontrollálhatók és megelőzhetők. A szerzői vagy szomszédos jogokat az elkövetőnek tudatosan és nyereségszerzési szándékkal kell megsértenie a bűncselekmény elkövetéséhez. A kereskedelmi cél különösen fontos, mivel ez teszi egyértelművé, hogy az ilyen jogsértések elsősorban a haszonszerzésre irányulnak, és ennek következtében jelentős gazdasági károkat okozhatnak a jogtulajdonosoknak illetőleg kifejezetten azokra az esetekre vonatkozik, amikor a jogsértést számítástechnikai rendszerek útján követik el. Az ilyen cselekmények, mint például a szerzői joggal védett zenei vagy filmes tartalmak engedély nélküli terjesztése, különösen veszélyesek, mivel gyorsan és széles körben terjedhetnek az interneten, jelentős bevételkiesést okozva a jogosultaknak. Fontos hangsúlyozni, hogy csekély súlyú jogsértések esetén amikor a cselekmény nem okoz jelentős gazdasági kárt vagy társadalmi veszélyt a nemzeti jogrendszerek mérlegelési jogkörükben eljárva dönthetnek enyhébb szankciók alkalmazásáról, illetve a büntetőjogi felelősségre vonás mellőzéséről. A 10. Cikk véleményem szerint, rendkívül fontos a szellemi tulajdon védelme szempontjából a digitális korban, hiszen hozzájárul a digitális gazdaság fenntartható működéséhez azáltal, hogy megvédi a szellemi tulajdonjogok birtokosait a jogellenes kizsákmányolástól. A

[60]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 10. cikk Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)

szakirodalom rámutat, hogy a szellemi tulajdonjogok hatékony érvényesítése kulcsfontosságú a tudásalapú gazdaság versenyképességének megőrzése érdekében, és ezzel az állásponttal magam is egyetértek, hiszen a szellemi alkotások megfelelő jogi védelme ösztönzőleg hat az innovációra, a kreativitásra, továbbá biztosítja a gazdasági szereplők számára a befektetéseik megtérüléséhez szükséges biztonságos környezetet. [61]Továbbá, a jogellenes tartalomterjesztés elleni fellépés nemcsak az egyéni jogosultak érdekeit szolgálja, hanem hozzájárul az általános piaci transzparenciához és az igazságos versenyfeltételek fenntartásához is.

2.9. Egyéb felelősségi és büntetési formák

A V. Cím alatt található rendelkezések célja a számítástechnikai bűncselekmények hatékony üldözésének és szankcionálásának biztosítása különféle kiegészítő felelősségi és büntetési formákon keresztül. Ezek a rendelkezések kiterjednek a bűncselekmények előkészítésére, a bűnsegélynyújtásra, a jogi személyek felelősségére, valamint a büntetések típusaira és mértékére. Ezek a rendelkezések azért fontosak, mert biztosítják, hogy a jogrendszer ne csak a ténylegesen megvalósult károkat szankcionálja, hanem már a veszélyeztető magatartásokat is, ráadásul hatékonyan léphessen fel mind az egyéni, mind a szervezett bűnözéssel szemben, a digitális tér kihívásaihoz igazodva. A 11. cikk szerint, bűncselekménynek kell minősíteni a számítástechnikai bűncselekmények elkövetésére irányuló kísérletet is, még akkor is, ha a bűncselekmény nem valósul meg teljes mértékben.[62] Ez a rendelkezés lehetővé teszi azt a hatóságok számára, hogy még a bűncselekmény teljes megvalósulása, befejezése előtt közbelépjenek, ennek következtében már a kísérleti szakaszban megakadályozhatják az elkövetőket a cselekményeik bevégzésével, és megelőzhető a tényleges kár vagy bűncselekmény bekövetkezése. A számítástechnikai bűncselekmények elkövetésében való bűnsegélynyújtás vagy felbújtás magában foglalja azokat a magatartásokat, amelyeknél

[61]Spránitz Gergely: Digitális tartalmak szerzői jogi védelme online környezetben II. rész. = *Iparjogvédelmi és Szerzői Jogi Szemle,* 2007/4 (112. évf. 4. sz.), 73–84. o. Elérhető: https://www.sztnh.gov.hu/kiadv/ipsz/200708-pdf/05.pdf, (letöltés dátuma: 2024. március 16.)
[62]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 11. cikk Kísérlet és bűnsegély vagy felbujtás. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)

technikai támogatást nyújtanak, eszközöket biztosítanak, vagy bármilyen módon elősegítik a bűncselekmény elkövetését. Fontos kiemelni azt is, hogy a jogi személyek is felelősségre vonhatók (12.cikk) a számítástechnikai bűncselekményekért, ha azok a jogi személy érdekében, annak vezetői vagy alkalmazottai által kerülnek elkövetésre.[63] Jogi személyekkel szemben pénzbírság, tevékenységük korlátozása vagy felfüggesztése, illetve súlyosabb esetekben a jogi személy felszámolása is kilátásba helyezhető szankcióként. A büntetések és intézkedések vonatkozásában kiemelendő, hogy a számítástechnikai bűncselekmények esetén kiszabott szankcióknak arányban kell állniuk az elkövetett cselekmény súlyosságával, továbbá megfelelő visszatartó erővel kell rendelkezniük annak érdekében, hogy megelőzzék a jövőbeni jogsértéseket. Súlyosabb bűncselekmények elkövetése esetén jellemzően szabadságelvonással járó büntetéseket szabnak ki. Emellett lehetőség van pénzbírság, vagyonelkobzás, valamint egyéb büntetőjogi szankciók és intézkedések alkalmazására is.[64]

2.10. Büntetőeljárási jog értelmezése az Egyezmény tükrében

A Büntetőeljárásjogi rendelkezések alkalmazási körét illetően a 14. cikk második bekezdése előírja, hogy a szerződő felek kötelesek meghatározott jogköröket és eljárásokat alkalmazni az Egyezmény 2-11. cikkeiben meghatározott bűncselekményekkel kapcsolatban, a számítástechnikai rendszerek útján elkövetett egyéb bűncselekmények esetében, valamint a bűncselekményekkel összefüggő elektronikus bizonyítékok összegyűjtésével kapcsolatban ellenkező rendelkezés hiányában.[65] A harmadik bekezdés olyan szabályokat, valamint korlátozásokat határoz meg, amelyek lehetőséget adnak a szerződő feleknek arra, hogy bizonyos intézkedéseket ne alkalmazzanak teljeskörűen, hanem csak a meghatározott feltételek mellett. Mindazonáltal, hogy a szerződő felek fenntarthatják maguknak azt a jogot, hogy a 20.

[63]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 12. cikk – Jogi személyek felelőssége. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.).
[64]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 13. cikk Büntetések és Intézkedések. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)
[65]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), I. Fejezet, 12. cikk Jogi személyek felelőssége. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)

cikkben meghatározott intézkedéseket (mint például bizonyos nyomozati eszközöket) csak a fenntartásban kifejezetten megjelölt bűncselekmények esetében alkalmazzák. Egy adott ország, példának okán dönthet akként, hogy ezeket az intézkedéseket csak a súlyos bűncselekmények esetén használja, nem pedig minden típusú bűncselekménynél. Másfelől fenntarthatja magának a jogot, hogy ne alkalmazza ezeket az intézkedéseket azonban ez abban az esetben történhet meg ha az adott ország jogi szabályozása nem teszi lehetővé azt, hogy a 20. és 21. cikkekben foglalt intézkedéseket alkalmazzák bizonyos zárt kommunikációs rendszerekre, mint például olyan hálózatokra, amelyek csak egy szűk, meghatározott felhasználói csoport számára elérhetők, és nem kapcsolódnak más rendszerekhez. Fontos kiemelni azt, hogy ugyanakkor ezen esetekben a jogszabály arra is ösztönzi az országokat, hogy ezeket a korlátozásokat minimálisra csökkentsék, és törekedjenek arra, hogy az intézkedések a lehető legszélesebb körben alkalmazhatók legyenek.

A 15. Cikk kulcsszerepet játszik a jogállamiság és az emberi jogok védelmének biztosításában a számítástechnikai bűncselekmények elleni fellépés során.[66] Azáltal, hogy előírja a jogkörök és az eljárások alkalmazásához szükséges biztosítékokat és garanciákat, hozzájárul a jogszerűség, arányosság és az emberi jogok tiszteletben tartásához. Az első bekezdés célja az arányosság elvének érvényesítése, valamint az emberi jogok és szabadságok megfelelő védelme különös tekintettel az olyan jogokra, amelyeket az Európa Tanács Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezményében (1950), az Egyesült Nemzetek Polgári és Politikai Jogok Nemzetközi Egyezségokmányában (1966), valamint más nemzetközi emberi jogi szerződésekben rögzítettek.[67][68] Az emberi jogok nemzetközi védelme a második világháborút követően kapott különös hangsúlyt, amikor a nemzetközi közösség felismerte, hogy az állampolgárok jogainak védelmét nem lehet mindössze az nemzetállamok belügyeinek tekinteni.[69] Ennek eredményeként létrejött az Európa Tanács Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezménye (EJEE, 1950) és az Egyesült Nemzetek

[66]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), II. Fejezet, 15. cikk Jogi személyek felelőssége. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)
[67]Európa Tanács: *Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezmény*. Róma, 1950.
[68]Egyesült Nemzetek Szervezete: *Polgári és Politikai Jogok Nemzetközi Egyezségokmánya.* New York, 1966.
[69]Blutman László: Az Európai Unió joga a gyakorlatban. Budapest, *HVG-ORAC Lap- és Könyvkiadó*, 2014 351. o.

Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (ICCPR, 1966), amelyek egészen napjainkig meghatározzák az emberi jogok nemzetközi védelmi rendszerét.[70] [71]Ezen dokumentumok noha különböző földrajzi régiókban illetőleg intézményi keretekben működnek, közös bennük az a célkitűzés, hogy egységes és hatékony válaszokat biztosítsanak a felmerülő kihívásokra, valamint elősegítsék az összehangolt fellépést a közösen meghatározott célok elérése érdekében, (mint például az emberi méltóság, szabadság és egyenlőség biztosítása) nemzetközi szinten.

Az EJEE-t 1950-ben fogadták el Rómában, és 1953-ban lépett hatályba.[72] Az Egyezmény különlegessége, hogy létrehozta az Emberi Jogok Európai Bíróságát (EJEB), amely lehetővé teszi azt, hogy az egyének közvetlenül panaszt tegyenek az őket ért emberi jogi sérelmek esetén, miután a nemzeti jogorvoslati lehetőségeket kimerítették.[73] Az Egyezmény rögzíti többek között az élethez való jogot, a kínzás tilalmát, a szabadsághoz és biztonsághoz való jogot, a tisztességes eljáráshoz való jogot, valamint a magán- és családi élet tiszteletben tartásához való jogot.[74] Az EJEB ítélkezési gyakorlata az ún. „élő jog" elve alapján dinamikusan fejlődik, azaz az Egyezmény rendelkezéseit a társadalmi változások fényében értelmezi, és ezáltal az emberi jogvédelem tartalma folyamatosan bővül.[757677] A nemzetközi emberi jogvédelem kulcsfontosságú dokumentuma a már említett ICCPR, amelyet az ENSZ Közgyűlése fogadott el 1966-ban, és 1976-ban lépett

---

[70]Európa Tanács: *Emberi Jogok és Alapvető Szabadságok Védelméről szóló Egyezmény.* Róma, 1950.
[71]Európa Tanács: *Az Emberi Jogok Európai Egyezményének egyszerűsített változata (magyar nyelvű kivonat).* Elérhető: https://www.echr.coe.int/documents/d/echr/Simplified_Conv_HUN (letöltés dátuma: 2022. április 28.)
[72]Európa Tanács: Az Emberi Jogok Európai Egyezményének egyszerűsített változata (magyar nyelvű kivonat). Elérhető: https://www.echr.coe.int/documents/d/echr/Simplified_Conv_HUN (letöltés dátuma: 2022. április 28.)
[73]Emberi Jogok Európai Bírósága: Kérdések és válaszok az Emberi Jogok Európai Bíróságáról. Strasbourg. Elérhető: https://www.echr.coe.int/documents/d/echr/Questions_Answers_HUN (letöltés dátuma: 2022. április 28.)
[74]1993. évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99300031.tv, (letöltés dátuma: 2022. április 28.)
[75]Letsas, George: A Theory of Interpretation of the European Convention on Human Rights. Oxford, Oxford University Press, 2007. pp. 15–48.
[76]Kiss Valéria: Az élő jog koncepciójának empirikus vizsgálata. A jogtudatkutatások módszertani problémái. In: Fazekas Marianna (szerk.): Jogi tanulmányok. Jogtudományi előadások az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskoláinak jubileumi konferenciáján: 20 éves a doktori képzés az ELTE Jogi Karán. ELTE ÁJK Doktori Iskola, Budapest, 2014, 238–248. o. Elérhető: https://edit.elte.hu/xmlui/bitstream/handle/10831/35689/Jogi_tan_2014_Kiss_Valeria_238-248.pdf, (letöltés dátuma: 2023. április 28.)
[77]Rainey, Bernadette – McCormick, Pamela – Ovey, Clare (szerk.): Jacobs, White and Ovey: The European Convention on Human Rights. Oxford, Oxford University Press, 2021. 792 o.

hatályba.[78] Az Egyezségokmány a polgári és politikai jogok nemzetközi garanciáit foglalja magában. E körben kiemelhető például az élethez való jog, a kínzás, valamint kegyetlen bánásmód tilalma, a véleménynyilvánítás szabadsága, a vallásszabadság és így tovább, a teljesség igénye nélkül.[79] Az ENSZ Emberi Jogi Bizottsága felügyeli a dokumentumba foglaltak végrehajtását, amely az állami jelentések vizsgálata mellett egyéni beadványokat is elbírál, ez utóbbi az első fakultatív jegyzőkönyv révén vált lehetővé.[8081] Herke Csongor hangsúlyozza, hogy az emberi jogok nemzetközi védelme egyre nagyobb szerepet játszik a nemzeti büntetőeljárások során is.[82] A nemzetközi egyezmények (különösen az EJEE) normái a nemzeti jogalkalmazásra is közvetlen hatást gyakorolnak, hiszen az Emberi Jogok Európai Bíróságának ítéleteit a nemzeti bíróságoknak figyelembe kell venniük.[83] A magyar büntető eljárásjog rendszerében is megfigyelhető, hogy az EJEE 6. cikkében foglalt tisztességes eljárás követelménye visszahat a büntetőeljárási törvények értelmezésére is, különös tekintettel a védelemhez való jogra, az ártatlanság vélelmére, valamint az eljárás ésszerű időn belüli lefolytatására.[8485] Kifejezetten előremutatónak tartom, hogy az EJEE és az ICCPR nem pusztán deklarációk, hanem tényleges garanciákat és gyakorlati biztosítékokat nyújtanak az emberi méltóság védelmének érdekében. Az EJEB működése példátlan lehetőséget teremt arra, hogy az egyének a konkrét ügyeikben nemzetközi fórumhoz fordulhassanak, ami véleményem szerint jelentős mértékben hozzájárult az európai jogállamiság és jogbiztonság fejlődéséhez. Az Egyezmények normatív jelenléte a nemzeti jogrendszerekben pedig erősíti az emberi jogok univerzális érvényességének tudatát, és

---

[78]International Covenant on Civil and Political Rights. United Nations General Assembly, 1966. december 16. United Nations Treaty Series, vol. 999, p. 171. Elérhető: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (letöltés dátuma: 2022. április 28.)

[79]CCPR Centre: *Simple Guide on the International Covenant on Civil and Political Rights (ICCPR) an overview of Articles 1–27*. Elérhető: https://ccprcentre.org/files/media/ICCPR_easy_to_read_commentary_WEB.pdf, (letöltés dátuma: 2022. április 28.)

[80]Manfred Nowak – William A. Schabas (szerk.): *U.N. Covenant on Civil and Political Rights: CCPR Commentary*. 3. kiadás. Kehl, N.P. Engel Verlag, 2019

[81] Philip Alston – Ryan Goodman (szerk.): *International Human Rights*. Oxford, Oxford University Press, 2013. 1580 o.

[82]Herke Csongor: Az előzetes letartóztatás végrehajtása az emberi jogok európai egyezménye tükrében. = *Jogtudományi Közlöny* 2000/3., 90–98. o.

[83]Herke Csongor: *Büntető eljárásjog Az új büntetőeljárási törvény főbb rendelkezései*. Budapest, Ludovika Egyetemi Kiadó, 2022. 327 o.

[84]Herke Csongor: *Magyar büntető eljárásjog*. *Egyetemi jegyzet.* Pécs, Baufirma Kiadó, 2021. 327 o.

[85]Emberi Jogok Európai Egyezménye, 6. cikk Tisztességes tárgyaláshoz való jog (hivatalos magyar fordítás). Elérhető: https://www.echr.coe.int/documents/d/echr/convention_hun, (letöltés dátuma: 2022. április 28.)

hozzájárul egy méltányosabb jogalkalmazáshoz. A második bekezdés arról rendelkezik, hogy bizonyos esetekben, amennyiben a jogkör vagy eljárás természete által indokolt, a biztosítékok és a garanciák különféle korlátozásokat és feltételeket tartalmazhatnak. Ezek a korlátozások lehetnek az eljárás vagy a jogkör alkalmazási időtartamának és körének a restrikciója, az alkalmazást alátámasztó indokok megléte, valamint a bírói vagy más független szervezet általi felülvizsgálat biztosítása. Ezen biztosítékok továbbá arra szolgálnak, hogy minimalizálják a visszaélések lehetőségét, és ugyanakkor garantálják, hogy a jogkörök, valamint az eljárások jogszerűsége, és arányossága is megmaradjon. Ez különösen fontos, mivel biztosítja, hogy az ilyen eljárások ne legyenek túlzott mértékűek, és ne sértsék indokolatlanul az érintettek jogait. A harmadik bekezdés hangsúlyozza, hogy a közérdekkel összhangban, különösen az igazságszolgáltatás megfelelő működésének biztosítása érdekében, minden szerződő félnek meg kell vizsgálnia azt, hogy a jelen fejezetben meghatározott jogkörök valamint eljárások milyen hatással vannak a harmadik személyek jogaira, jogos érdekeire és felelősségére. Ez a bekezdés továbbá kiemeli a jogszerűség és az igazságosság fontosságát az eljárások során, valamint a jogi érintettek védelmét.

A 16. cikk a tárolt számítástechnikai adatok gyors megőrzésével kapcsolatos szabályokat és kötelezettségeket foglalja magában.[86] Ennek a cikknek az a célja, hogy a szerződő felek biztosítsák a számítástechnikai rendszerekben tárolt adatok gyors és hatékony megőrzését, különösen olyan esetekben, amikor ezek az adatok módosítás vagy megsemmisülés veszélyének vannak kitéve. Minden szerződő fél köteles olyan jogalkotási illetőleg egyéb intézkedéseket hozni, amelyek lehetővé teszik az illetékes hatóságok számára, hogy elrendelhessék a számítástechnikai rendszerben tárolt meghatározott adatok, beleértve a forgalmi adatokat, gyors megőrzését, különösen akkor, ha fennáll a veszélye annak, hogy az érintett adatok módosulnak vagy megsemmisülnek. Az adatok *megőrzésének időtartama* legfeljebb kilencven napig tarthat, biztosítva, hogy az adatok a hatóságok rendelkezésére álljanak, és fontos kiemelni azt is, hogy szükség esetén az intézkedés ismételten elrendelhető.[87] Mindemellett az adatokat őrző vagy az adatok megőrzésére kötelezett személynek *titokban kell tartania az eljárást* az adott

[86]Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), II. Fejezet. 16. cikk Tárolt számítástechnikai adatok gyors megőrzése. ETS 185. Elérhető: https://rm.coe.int/16802fa405, (letöltés dátuma: 2022. április 29.)
[87]Számítástechnikai Bűnözésről Szóló Egyezmény. II. Cím, 16. cikk (2) bekezdés

ország belső jogszabályai által meghatározott időtartamig, ezáltal garantálva az adatok biztonságát és integritását.[88] A forgalmi adatok gyors megőrzésére és részbeni átadására vonatkozó szabályokat a 17. cikk határozza meg, kiegészítve az előző, 16. cikkben foglaltakat, és speciálisan a forgalmi adatokkal kapcsolatos eljárásokat szabályozva. Ez magában foglalja, hogy a kommunikációval kapcsolatos összes forgalmi *adatot meg kell őrizni*, függetlenül a hálózat vagy a szolgáltató komplexitásától.[89] Emellett a szerződő félnek biztosítania kell, hogy a megfelelő számú forgalmi adatot *gyorsan átadják* az illetékes hatóságoknak vagy az általuk kijelölt személyeknek.[90] Ez az átadás elengedhetetlen ahhoz, hogy a kommunikáció továbbítására használt esteleges útvonalat és a szolgáltatót azonosítani lehessen. A 18. cikk a számítástechnikai adatok és előfizetői információk közlésére vonatkozó kötelezettségeket szabályozza annak érdekében, hogy a szerződő felek jogi alapot teremtsenek az illetékes hatóságok számára a számítástechnikai rendszerekben tárolt adatokhoz, valamint a szolgáltatók birtokában lévő előfizetői adatokhoz való hozzáféréshez.[91] A szabályozás alapján minden szerződő félnek lehetővé kell tenni a hatóságok számára, hogy kötelezhessék az adott területen tartózkodó személyeket a birtokukban vagy ellenőrzésük alatt lévő számítástechnikai adatok közlésére, valamint a területükön szolgáltatást nyújtó szolgáltatókat az előfizetőkre és a szolgáltatásokra vonatkozó adatok közlésére.[92] Továbbá meghatározza azt is, hogy mit értünk "előfizetőre vonatkozó adatok" alatt, beleértve az adott kommunikációs szolgáltatás típusát, az előfizető személyazonosságát, valamint a szolgáltatásra vonatkozó technikai illetőleg számlázási adatokat, amelyek nélkülözhetetlenek az eljárás alatt.[93] A tárolt számítástechnikai adatok átvizsgálására és lefoglalására vonatkozó eljárásokat szabályozza a 19. cikk, amelyeket a szerződő feleknek biztosítaniuk kell az illetékes hatóságok számára.[94] Ezen szabályozás biztosítja azt, hogy a hatóságok hozzáférhessenek a nyomozás szempontjából fontos számítástechnikai rendszerhez vagy annak egy részéhez és az abban tárolt számítástechnikai adatokhoz, a számítástechnikai adatok tárolását lehetővé tevő számítástechnikai adattároló-egységekhez, amennyiben a hatóságok egy adott rendszert

[88]Számítástechnikai Bűnözésről Szóló Egyezmény. II. Cím, 16. cikk (3) bekezdés.
[89]Számítástechnikai Bűnözésről Szóló Egyezmény. II. Cím, 17. cikk (1) a) bekezdés.
[90]Számítástechnikai Bűnözésről Szóló Egyezmény. II. Cím, 17. cikk, 1. b. bekezdés.
[91]Számítástechnikai Bűnözésről Szóló Egyezmény. III. cím, 18. cikk, 1. a. bekezdés.
[92]Számítástechnikai Bűnözésről Szóló Egyezmény. III. cím, 18. cikk, 1. b. bekezdés.
[93]Számítástechnikai Bűnözésről Szóló Egyezmény. III. cím, 18. cikk, 3. a. bekezdés.
[94] Számítástechnikai Bűnözésről Szóló Egyezmény. IV. cím, 19. cikk.

vizsgálnak át, és feltételezhető az, hogy a keresett adatok egy másik vagy ugyanazon joghatóság alá tartozó rendszerben találhatók, akkor az átvizsgálást kiterjeszthessék erre a másik rendszerre is.[95] Továbbá olyan intézkedéseket is előír, amelyek feljogosítják a hatóságokat a számítástechnikai adatok lefoglalására, *másolatuk készítésére és megőrzésére,* valamint az *adatok épségének megóvására*, az átvizsgált számítástechnikai rendszer fenti számítástechnikai adatainak *hozzáférhetetlenné tételére vagy eltávolítására*.[96] A hatóságok továbbá kötelezhetik a számítástechnikai rendszerek működését vagy az adatok védelmét *ismerő személyeket*, hogy szükség esetén *megadják a nyomozáshoz szükséges tájékoztatást.*[97] A 20. cikk a számítástechnikai rendszerek útján továbbított forgalmi adatok valós idejű összegyűjtésére és rögzítésére vonatkozó jogköröket és kötelezettségeket határozza meg, amelyek célja, hogy a szerződő felek biztosítsák a hatóságok számára a szükséges eszközöket és jogi hátteret a forgalmi adatok valós idejű nyomon követésére és a rögzítésére, amelyek kulcsfontosságú szerepet tölthetnek be a bűnügyi nyomozások során.[98] A cikk előírja, hogy minden szerződő félnek olyan jogalkotási és egyéb intézkedéseket kell bevezetnie, amelyek lehetővé teszik a hatóságok számára, hogy a területükön található technikai eszközökkel valós időben összegyűjtsék vagy rögzítsék a számítástechnikai rendszerek útján továbbított, meghatározott kommunikációhoz kapcsolódó forgalmi adatokat. Emellett kötelezhetik a szolgáltatókat arra, hogy a meglévő technikai képességeik keretein belül működjenek együtt a hatóságokkal az ilyen adatok összegyűjtésében vagy rögzítésében. A cikk rugalmasságot is biztosít azáltal, hogy ha egy szerződő fél jogrendszere nem teszi lehetővé az 1. bekezdés szerinti intézkedések bevezetését. Ebben az esetben alternatív jogszabályokat vezethet be, amelyek szintén biztosítják a forgalmi adatok valós idejű összegyűjtését a területükön található technikai eszközök segítségével. A titoktartásra vonatkozó rendelkezések pedig garantálják, hogy a szolgáltatók titokban tartják az adatok összegyűjtésére vonatkozó tevékenységeket, megőrizve a nyomozások hatékonyságát illetőleg biztonságát. Végül, a cikk hangsúlyozza, hogy az itt meghatározott jogköröket

[95]Számítástechnikai Bűnözésről Szóló Egyezmény. IV. cím, 19. cikk, 1. a., b. bekezdés.
[96]Számítástechnikai Bűnözésről Szóló Egyezmény. IV. cím, 19. cikk, 3. bekezdés.
[97]Számítástechnikai Bűnözésről Szóló Egyezmény. IV. Cím, 19. cikk, 4. bekezdés.
[98]Számítástechnikai Bűnözésről Szóló Egyezmény. V. Cím, 20. cikk

és eljárásokat az arányosság, jogszerűség, és az emberi jogok védelmének követelményei szerint kell alkalmazni, mint ahogy azt a 14. és 15. cikkek előírják.

2.11. A technológiai fejlődés hatásai és az uniós jogi keretek és a XXI. századi bűnüldözésben

A XXI. században a bűnüldözés egyre inkább támaszkodhat az információs rendszerek adataira, mint bizonyítékokra, mivel jelenleg szinte minden bűncselekmény valamilyen formában kapcsolódik a digitális térhez. Amikor egy gyanúsított vagy áldozat okostelefonját vizsgálják, olyan információkat és adatokat találhatnak, mint például a szöveges üzenetek, az e-mailek, a fényképek, a videók, a közösségi média bejegyzések, valamint az utóbbi időben használt helymeghatározások vagy például egy térképes keresés egy adott címre, lokációra. Ez kifejezetten előnyös ugyanis ezek az adatok segítségül szolgálhatnak a bűncselekmény időpontjának és helyszínének a rekonstruálásában.[99] A résztvevő személyekről is részletesebb információkhoz jutunk hiszen ezáltal teljes képet kaphatunk az elkövetés utáni és az megelőző tevékenységekről, az elkövető esetleges szándékai és cselekményeiről továbbá lehetőség adódik az elkövető és áldozat közötti okozati viszonyok, kapcsolatok feltárására is.[100] Ezenkívül a digitális eszközökön található adatok összevethetők más forrásokkal is mint, például banki tranzakciós adatokkal, biztonsági kamerafelvételekkel, vagy tanúk vallomásaival, így átfogóbb és megbízhatóbb képet nyújtanak a bűncselekmény körülményeiről és jelentősen hozzájárulhatnak az igazság kiderítéséhez és az elkövetők felelősségre vonásához.[101] Az okostelefonok azonban csak a jéghegyének csúcsát képezik. Számos más eszköz is, mint például laptopok, táblagépek, GPS rendszerek, hordható technológiák (pl. Fitbitek[102]), zárt láncú televíziók, és az „Internet of Things" (IoT) eszközök értékes,

---

[99]Antonela Gropeneanu, - Adrian Iacob: Investigative issues regarding cybercrime. = European Journal of Public Order and National Security, no. 2., 2016/2, p. 10.

[100]A személyes adatok és a magánszféra védelme. A Rendőrség hivatalos honlapja. Elérhető: https://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag/a-szemelyes-adatok-es-a-maganszfera-vedelme (letöltés dátuma: 2021. március 6.)

[101]Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesítésük. *Ügyészek Lapja*, 2010/2., 25–26. o.

[102](A Fitbit egy viselhető fitneszkövető eszköz, amely lehetővé teszi a felhasználók számára, hogy nyomon kövessék fizikai aktivitásukat, egészségi állapotukat és alvási szokásaikat. Az eszköz különféle szenzorok segítségével méri a napi lépésszámot, a megtett távolságot, az elégetett kalóriákat, a szívritmust, valamint az alvás minőségét és időtartamát. A Fitbit készülékek okostelefon alkalmazással is összekapcsolhatók,

digitális adatokat tartalmazhatnak, amelyek relevánsak lehetnek a nyomozás szempontjából, mint „digitális bizonyíték”.

A digitális bizonyíték fogalma a magyar jogtudományban több szerző értelmezésében is megjelenik, különböző megközelítésekben. Gácsi Anett Erzsébet szerint, a digitális vagy elektronikus adatok a büntetőeljárásban második generációs bizonyítékoknak tekinthetők, amelyek új dogmatikai kérdéseket vetnek fel. A hagyományos bizonyítási eszközökön túl ezek az adatok önálló bizonyítási eszközként jelennek meg, és mind a büntetőeljárásjog, mind a kriminalisztika számára kihívást jelentenek. Álláspontja szerint ezek az adatok önálló bizonyítási eszközként jelennek meg, amelyek a hagyományos eljárásjogi keretek közé már nem minden esetben illeszthetők be.[103] Sorbán Kinga szintén a digitális bizonyítékok sajátosságaira hívja fel a figyelmet, különösen a forrásuk tekintetében. Értelmezése szerint a magyar jogrendszer nem rendelkezik egységes állásponttal arra vonatkozóan, hogy mi tekinthető digitális bizonyíték forrásának ugyanis az egyik megközelítés szerint az adathordozó, míg a másik szerint maga az információs rendszerben tárolt adat minősül annak.[104] A jogalkotó igyekezett mindkét értelmezést lehetővé tenni, azonban a szabályozás hiányosságai miatt a gyakorlatban értelmezési nehézségek adódhatnak. Róth Erika a 2017. évi XC. törvény jelentőségét emeli ki, amely bevezette az „elektronikus adat” fogalmát, mint új bizonyítási eszközt. Véleménye szerint ez a változás azért volt indokolt, mert az elektronikus adatok nem minden esetben kezelhetők a fizikai dolgok analógiájára, így sajátos szabályozást igényelnek megszerzésük, kezelésük és megőrzésük során.[105] Dornfeld László szerint a digitális bizonyíték olyan bizonyító erővel bíró adat, amelyet digitális formában tárolnak, dolgoznak fel vagy továbbítanak.[106] A szerző hangsúlyozza, hogy a digitális korszak új jogi kihívásokat teremtett, különösen a nemzetközi vonatkozású bizonyítékszerzés terén, és szükséges a jogi szabályozás korszerűsítése annak érdekében, hogy ezekre a kihívásokra adekvát válasz születhessen. Herke Csongor a digitális bizonyítékok kérdését

---

amely részletes elemzéseket és visszajelzéseket nyújt a felhasználók számára, elősegítve az egészségesebb és aktívabb életmód kialakítását.)

[103]Gácsi Anett Erzsébet: *A digitális bizonyíték és a kriminalisztika fejlődése a XXI. században*, Magyar Rendészet, 2022/3., 45–55. o.

[104]Sorbán Kinga: *Az elektronikus bizonyítékok elméleti és gyakorlati kérdései a büntetőeljárásban*, Belügyi Szemle, 2016/11., 81–96. o.

[105]Róth Erika: A büntetőeljárás újraszabályozása a 2017. évi XC. törvény főbb újításai, Magyar Jog, 2017/10., 577–589. o.

[106]Dornfeld László: Az elektronikus bizonyítékszerzés aktuális kérdései, in: Kriminológiai Tanulmányok 56., 2019, 215–232. o.

elsősorban a büntetőeljárás digitalizációjának szélesebb összefüggésében vizsgálja. Véleménye szerint a digitalizáció célja az eljárások hatékonyságának növelése, a költségek csökkentése és a cselekmények gyorsabb, egyszerűbb lefolytatása. A digitális bizonyítékokat ennek részeként értelmezi, és hangsúlyozza, hogy ezek kezelése speciális eljárási szabályokat igényel. Továbbá kiemeli, hogy a digitális adatokkal kapcsolatban alapvető fontosságú azok hitelessége, integritása és bizalmassága, hiszen ezek nélkül nem biztosítható a tisztességes eljárás.[107] Véleménye szerint tehát az elektronikus bizonyítékok nem egyszerűen a korábbi tárgyi bizonyítékok digitális megfelelői, hanem önálló eljárásjogi jelentőséggel bíró eszközök, amelyekkel szemben a büntetőeljárásnak külön biztosítékokat kell nyújtania. Ugyanakkor felhívja a figyelmet arra is, hogy a digitalizáció nem csupán előnyökkel jár, hanem kihívásokat is hordoz, például a személyes jelenlét hiányából fakadó bizonyítási nehézségeket vagy a technikai eszközök megbízhatóságának kérdését.[108] Végül, Tóth Marcell Máté a digitális bizonyítékot olyan bináris formában tárolt vagy továbbított információként határozza meg, amely bizonyító erővel bír. Kiemeli az informatikai szakértők jelentőségét, akiknek közreműködése gyakran elengedhetetlen a bizonyítékok hiteles összegyűjtéséhez, elemzéséhez és bemutatásához, mivel ezek a bizonyítékok technikai jellegükből adódóan csak szakértői értelmezéssel válhatnak értelmezhetővé illetőleg jogilag felhasználhatóvá.[109] A digitális bizonyítékok természetükből fakadóan rejtetten vannak jelen, hasonlóan az ujjlenyomatokhoz vagy a DNS-hez, amelyek csak speciális eszközök és módszerek alkalmazásával hozhatók felszínre, válnak észlelhetővé, valamint értelmezhetővé.[110]

Miután megvizsgáltuk a digitális bizonyítékok különféle értelmezését, technikai jellemzőit, fontos kitérni azokra a jogi kihívásokra is, amelyek az adatok kezelésével járnak. Ezen bizonyítékok egyik ilyen jellemzője, ahogy már említésre került az az, hogy rendkívüli gyorsasággal átléphetik a joghatósági határokat, mivel az internet és a digitális kommunikáció globális jellege lehetővé teszi, hogy az adatok egy szempillantás alatt egyik országból a másikba kerüljenek. Ez komoly kihívásokat jelent a nemzetközi jogi

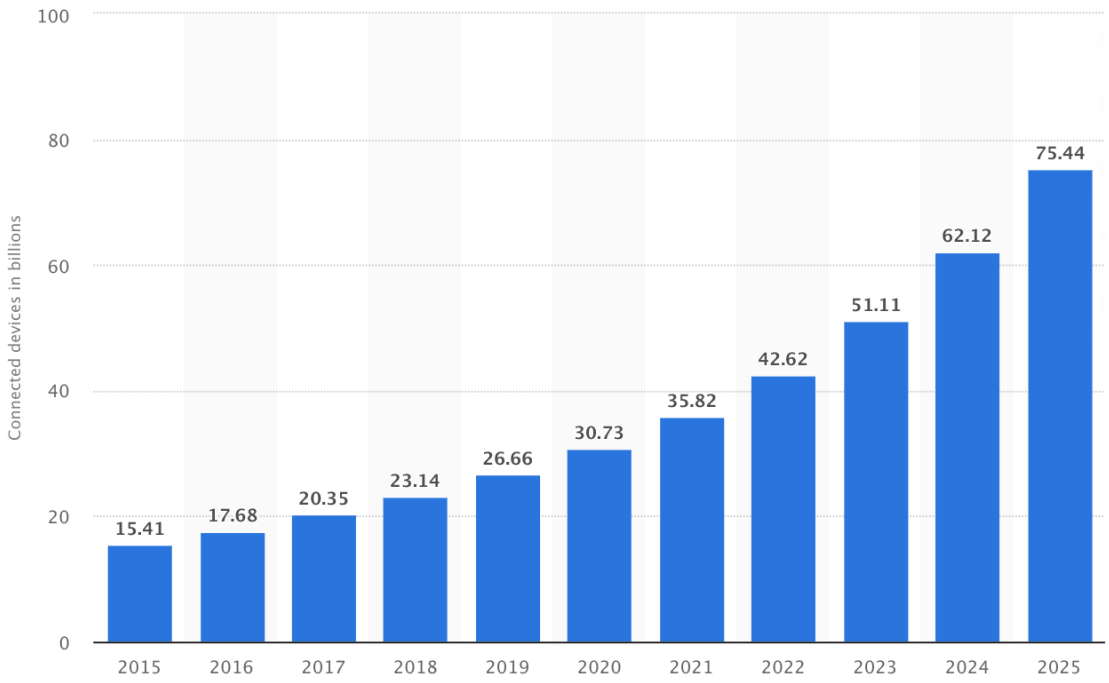
[107]Herke Csongor: A digitalizáció szerepe a büntetőeljárásban, in: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika, PTE ÁJK, Pécs, 2019, 104–113.
[108]Herke Csongor: *Büntető eljárásjog Egyetemi jegyzet*, PTE ÁJK, Pécs, 2018.
[109]Tóth Marcell Máté: A digitalizáció egyes kihívásai a büntetőeljárásban. = *Belügyi Szemle*, 72. évf. 2. sz. (2024), 185–210. o. DOI: https://doi.org/10.38146/BSZ.2024.2.1
[110]Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: *Kriminalisztika* – Tankönyv és atlasz. Dialóg Campus Kiadó, Budapest–Pécs, 2005.

együttműködés és a bűnüldözés számára, mivel a különböző joghatóságok közötti eltérő jogszabályi keretek akadályozhatják a hatékony nyomozást és a bizonyítékgyűjtést. A másik kihívás a digitális adatok módosíthatósága, formázási lehetősége mivel ezek az adatok rendkívül érzékenyek bármilyen beavatkozásra. További kihívást jelent a technológiai fejlődés is amely jelentős hatással van a digitális bizonyítékok kezelésére. Egy apró változtatás (akár szándékos, akár gondatlan) jelentősen befolyásolhatja az adatok integritását, így azok megbízhatóságát és felhasználhatóságát a bírósági eljárásokban.[111] A módosítás és megsemmisítés kockázata (különösen az olyan új technológiai eszközök, mint a mesterséges intelligencia (a továbbiakban: MI) megjelenésével összefüggésben) fokozott aggodalomra adhat okot azokban az esetekben, amikor az elkövetők tudatosan törekednek nyomaik eltüntetésére vagy módosítására, illetve amikor az adatokat tároló eszközök műszaki meghibásodása, vagy akár az idő múlásából eredő adatvesztés veszélye áll fenn.[112] Az időérzékenység szintén olyan lényeges tényező, amely nem hagyható figyelmen kívül, hiszen a bizonyítékok megőrzésének és érvényesítésének feltétele a gyors és hatékony beavatkozás, még mielőtt azok bizonyítóereje csökkenne vagy véglegesen elveszne.

E tényezők együttesen rávilágítanak a digitális bizonyítékokhoz kapcsolódó kihívások komplexitására, valamint arra az igényre, hogy a hagyományos nyomozási módszerek kiegészítéseként olyan speciálisan kialakított eljárások és technikai eszközök is előtérbe kerüljenek, amelyek adott esetben elősegíthetik, könnyíthetik a digitális bizonyítékokban rejlő lehetőségek hatékonyabb érvényesítését az igazságszolgáltatás során. A nyomozó hatóság a digitális bizonyítékokat hasonló módon alkalmazhatja, mint a „hagyományos" tárgyi bizonyítékokat, azzal a céllal, hogy összekapcsolják az adott személyeket, helyeket, eseményeket, valamint ezáltal megalapozzák a bűncselekmények okozati összefüggéseit. A digitális bizonyítékok azonban meglehetősen gyakori módon, sokkal szélesebb körű információt tartalmaznak, és a megszerzésük is sokkal összetettebb folyamattá válhat, mint a „hagyományos" bizonyítékoké.[113] Az adatok, adatállományok

[111]Herke Csongor: A digitalizáció szerepe a büntetőeljárásban, in: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika, Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2019, 104–113.o.
[112]Herke Csongor: Mesterséges intelligencia a büntetőjogi döntéshozatalban. = *Jogtudományi Közlöny*, 2023/4., 165–176. o. Elérhető: https://szakcikkadatbazis.hu/doc/1207285 (letöltés dátuma: 2024. január 5.)
[113] Az Európai Unió Tanácsa: E-bizonyítékok Elektronikus bizonyítékok a büntetőeljárásokban. Elérhető: https://www.consilium.europa.eu/hu/policies/e-evidence/ (letöltés dátuma: 2024. május. 06.)

mennyiségének robbanásszerű növekedése tovább súlyosbítja ezeket a kihívásokat. Az internethez csatlakozó eszközök száma 2021-re elérte az átlagosan 4,3 eszközt személyenként, ami globálisan körülbelül 12,2 milliárd eszközt jelent.[114] Ezek az eszközök jelentős mennyiségű adatot generálnak, amelyek közül sok létfontosságú a modern élet működése szempontjából. A jövőre nézve ezek a trendek várhatóan tovább gyorsulnak, és véleményem szerint 2027-re ezen adatmennyiség a tízszeresére növekszik világszerte.[115]



1. ábra

A Statista által készített előrejelzés, amely szerint 2025-re több mint 75 milliárd IoT-eszköz lesz használatban világszerte.[116]

[114]Statista: Number of Internet of Things (IoT) connected devices worldwide from 2022 to 2033. Elérhető: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (letöltés dátuma: 2022. május 06.)

[115] (*Már 2025-ben is 30,9 milliárd internethez csatlakoztatott eszköz van világszerte, ami alátámasztja a 2021-ben megfogalmazott előrejelzésemet: az adatmennyiség valóban rohamosan növekszik, és a 2027-re várt tízszeres szorzó egyre reálisabbnak tűnik.)*

[116]Archana Bachhav – Vilas Kharat – Madhukar Shelar: Processing Distributed Internet of Things Data with Query Optimization in Cloud. = International Journal of Computer Applications, 2019. Elérhető: https://www.researchgate.net/figure/oT-connected-devices-from-2015-to-2025-in-billions-3_fig1_331285113
Statista: Number of Internet of Things (IoT) connected devices worldwide from 2022 to 2033. Elérhető: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Az adatok és információk efféle áramlása ugyanakkor nem csupán a potenciális bizonyítékok számának növekedését eredményezi a nyomozó hatóságok számára, hanem egyúttal jelentősebb nehézségeket is támaszt a feldolgozás, értékelés és felhasználhatóság terén. Nehezebbé válik a releváns információk kiszűrése a hatalmas adatmennyiségből, valamint a megkülönböztetése a felhasználhatatlan, nyomozás tekintetében jelentéktelen adatoktól és információktól. Ezen túlmenően, az adatmennyiség gyors növekedésével a nyomozóknak nem kizárólag a felelősségük, hogy az óriási adathalmazból kiszűrjék a releváns információkat, hanem az is, hogy biztosítsák ezeknek az adatoknak, információknak a megfelelő kezelhetőségét és elemzését. Ez a folyamat komoly technológiai és emberi erőforrásokat igényel, hiszen az adatokat nem csupán összegyűjteni, hanem értelmezni és a bűnügyi nyomozás kontextusába helyezni is szükséges. Az adatfeldolgozás során a nyomozóknak figyelembe kell venniük az adatokat érintő rendelkezéseket és adatvédelmi szabályokat is, ami tovább növeli a kihívások mértékét, nem említve ezek időigényességét.[117] Ahogy az adatok mennyisége és komplexitása növekszik, úgy válik egyre elengedhetetlenebbé a fejlett elemző eszközök és technológiák alkalmazása, amelyek képesek automatizálni az adatok feldolgozását és segítenek a nyomozóknak a leglényegesebb információk azonosításában. Ennek ellenére a technológiai eszközök sem képesek minden kihívást megoldani.

Az új titkosítási technológiák alkalmazása egyre bonyolultabbá teszi a digitális eszközökből származó adatokhoz való hozzáférést. Még abban az esetben is, ha a nyomozó hatóságok törvényes úton megszerzik a szükséges engedélyeket, ugyanis az adatok titkosítása következtében sokszor nehézségekbe ütköznek azok visszafejtése és elemzése során. Ezt a jelenséget a szakirodalom „elsötétedésként” (going dark) említi, amely komoly akadályokat gördít a digitális bizonyítékok gyakorlati felhasználása elé, és számos (elsősorban adatvédelmi) jogi kérdést is felvet kifejezetten az adatvédelem területén.[118] Noha a korszerű titkosítási eljárások kétségkívül jelentős előrelépést jelentenek az adatbiztonság és a személyes adatok védelme terén, a büntetőeljárások szempontjából egyidejűleg komoly nehézségeket is generálhatnak. Bizonyos esetekben e

[117]Mándi Veronika: A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata. = Büntetőjogi Szemle, 2023/1., 54–63. o. Elérhető: https://ujbtk.hu/mandi-veronika-a-szemelyes-adatok-kezelese-a-buntetoeljarasban-es-a-nyilvanossag-kapcsolata/ (letöltés dátuma: 2023. 05. 19.)

[118] Europol Eurojust: First Report of the Observatory Function on Encryption. The Hague, 2019. Elérhető: https://www.europol.europa.eu/cms/sites/default/files/documents/final_report_of_the_observatory_function.pdf (letöltés dátuma: 2022. 03. 06.)

technológiák nem csupán megnehezítik, de akár ellehetetleníthetik is a hatóságok számára a releváns információk elérését.[119] E technológiák elsődleges célja az adatok integritásának, bizalmasságának és hitelességének megőrzése (különösen a digitális kommunikáció és adatátvitel vonatkozásában), ami viszont azzal a következménnyel járhat, hogy a nyomozó hatóságok számára lényegesen nehezebbé válik a releváns információkhoz való hozzáférés, illetve a bizonyítékok beszerzése és felhasználhatóságuk biztosítása.[120]

Az egyik legfontosabb újítás a kvantumtitkosítás, amely a kvantummechanika elveit használja az adatok védelmére, és várhatóan rendkívül biztonságossá válik a jövőben, mivel képes ellenállni a hagyományos és a kvantumszámítógépek általi támadásoknak is. Továbbá, a homomorfikus titkosítás szintén figyelemre méltó fejlesztés, amely lehetővé teszi az adatok titkosított állapotban történő feldolgozását anélkül, hogy azok dekódolásra kerülnének.[121] Ez különösen fontos az olyan területeken, mint a felhőalapú számítástechnika, ahol az adatok feldolgozása harmadik fél szerverein keresztül történik. Ezek mellett, a blokklánc technológián alapuló elosztott főkönyvi rendszerek is új irányt képviselnek a titkosításban, mivel decentralizált és átlátható módon biztosítják az adatbiztonságot, amelyet már széles körben alkalmaznak a kriptovaluták, intelligens szerződések és más pénzügyi technológiák területén.[122] A technológiai innovációk ilyen gyors ütemű fejlődése közvetlen és egyre intenzívebb hatással van az uniós jogalkotásra és joggyakorlatra is, amelyet az alábbiakban bemutatott esetek is szemléletesen példáznak.

A C-203/15 (Tele2 Sverige AB) ügy középpontjában az állt, hogy a tagállamok jogszabályai mennyiben felelnek meg az uniós adatvédelmi előírásoknak, különös tekintettel a 2006/24/EK irányelv (a hírközlési adatmegőrzési irányelv) alapján bevezetett adatmegőrzési kötelezettségekre ugyanis a 2006/24/EK irányelv előírta, hogy az

---

[119]Digital Watch Observatory: Encryption. Elérhető: https://dig.watch/topics/encryption (letöltés dátuma: 2024. 05. 06.)

[120]Europol Eurojust: Third Report of the Observatory Function on Encryption. The Hague, 2021. Elérhető: https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf(letöltés dátuma: 2022. 03. 06.)

[121]Konstantinos Christidis – Michael Devetsikiotis: Blockchains and smart contracts for the internet of things. = IEEE Access 4, 2016. 05. 10., 2292–2303. o. Elérhető: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408, letöltés dátuma: 2022. 04. 07. DOI: 10.1109/ACCESS.2016.2566339

[122]Mi az a blokklánc technológia és hogyan működik? Kriptomat. Elérhető: https://kriptomat.io/hu/blockchain/mi-az-a-blockchain-technologia/ (letöltés dátuma: 2022. 05. 06.)

elektronikus hírközlési szolgáltatók kötelesek megőrizni bizonyos adatokat a szolgáltatásaik felhasználóiról, beleértve a forgalmi adatokat és a helymeghatározási adatokat.[123] A cél az volt, hogy ezek az adatok elérhetők legyenek a bűnüldöző hatóságok számára súlyos bűncselekmények megelőzése, felderítése és üldözése érdekében. Azonban az Európai Bíróság 2014-ben megsemmisítette ezt az irányelvet a Digital Rights Ireland ügyben, mert úgy ítélte meg, hogy az irányelv sérti a magánélethez és a személyes adatok védelméhez való jogot.[124] Az Európai Bíróságnak el kellett döntenie, hogy a tagállamok, a nemzeti jogukban továbbra is fenntarthatnak-e olyan adatmegőrzési kötelezettségeket, amelyek hasonlóak a megsemmisített irányelvhez. A Tele2 Sverige AB ügyben kulcskérdésként merült fel az, hogy mennyiben jelent beavatkozást a magánélethez való jogba, ha egy tagállam általános adatmegőrzést ír elő? Hogyan kell egyensúlyt teremteni a bűnmegelőzés és a magánélet védelme között? Továbbá az is, hogy általános és különbségtétel nélküli adatmegőrzési kötelezettség összhangban van-e az uniós joggal, különösen az Alapjogi Chartával ugyanis a svéd jogszabály előírta az elektronikus hírközlési szolgáltatók számára, hogy őrizzék meg a felhasználók forgalmi és helymeghatározási adatait egy meghatározott ideig. Az Európai Unió Bíróságának egyik legfontosabb megállapítása az volt, hogy a tagállamok nem írhatnak elő általános és különbségtétel nélküli adatmegőrzést. Az ilyen intézkedések súlyos beavatkozást jelentenek az Alapjogi Charta által biztosított alapvető jogokba, különösen a magánélet tiszteletben tartásához való jogba (7. cikk) és a személyes adatok védelméhez való jogba (8. cikk).[125] Az ítélet rávilágított arra, hogy az általános adatmegőrzési gyakorlat nem felel meg az arányosság és a szükségesség követelményeinek, amelyeket az uniós jog előír. Továbbá azt is megállapította, hogy bizonyos körülmények között, amikor a nemzeti jogszabályok célzott adatmegőrzést írnak elő, az uniós joggal összhangban lehet. Az ilyen célzott adatmegőrzés akkor elfogadható, ha pontosan meghatározott célokra irányul, például súlyos bűncselekmények megelőzésére vagy a nemzetbiztonság

[123]Európai Unió Bírósága: C-203/15. és C-698/15. sz. egyesített ügyek – Tele2 Sverige AB kontra Post- och telestyrelsen és Secretary of State for the Home Department kontra Watson és társai. Ítélet, 2016. december 21. Elérhető: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=HU (letöltés dátuma: 2022. 05. 06.)

[124]Európai Unió Bírósága: C-293/12. sz. ügy Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai. Ítélet, 2014. április 8. Elérhető: https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=HU(letöltés dátuma: 2022. 05. 06.)

[125] Európai Unió*:* Az Európai Unió Alapjogi Chartája, 7. cikk, 8.cikk (2016/C 202/02). Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:12016P/TXT (letöltés dátuma: 2022. 05. 06.)

védelmére, és ha megfelelő garanciákkal van ellátva. Ebben az esetben is azonban szigorú feltételeket kell alkalmazni annak érdekében, hogy a magánélethez és a személyes adatok védelméhez való jogok ne sérüljenek. Az adatmegőrzési időszak korlátozásának szükségességének kiemelése esetében az adatmegőrzési intézkedések csak a feltétlenül szükséges ideig tarthatók fenn, és alkalmazásukat célzottan kell végrehajtani. Ez azt jelenti, hogy az adatmegőrzés időtartamát a minimumra kell csökkenteni, hogy a személyes adatok indokolatlanul hosszú ideig ne maradjanak a hatóságok birtokában. A bíróság továbbá hangsúlyozta, hogy a bűnüldöző hatóságok hozzáférése a megőrzött adatokhoz szigorú feltételekhez kötött. Ez a hozzáférés csak akkor engedélyezhető, ha objektív kritériumok alapján szükséges, és ha a hozzáférést egy független hatóság előzetesen engedélyezi.

A C-698/15 (Watson és társai**)** ügy az Európai Unió Bíróságának (EUB) egy másik jelentős döntése, amely szorosan kapcsolódik a C-203/15 (Tele2 Sverige AB) ügyhöz. Ebben az ügyben brit állampolgárok, köztük David Davis és Tom Watson, kérdőjelezték meg a brit adatmegőrzési szabályozás jogszerűségét.[126] [127] A brit jogszabály, a 2014-es Data Retention and Investigatory Powers Act (DRIPA) (Adatmegőrzésről és nyomozati hatáskörökről szóló törvény), előírta, hogy a távközlési szolgáltatók kötelesek megőrizni a felhasználók forgalmi és helymeghatározási adatait, és azokat a bűnüldöző hatóságok rendelkezésére bocsátani.[128] Watson és társai úgy vélték, hogy ez a törvény sérti az Európai Unió Alapjogi Chartájában biztosított jogokat, különösen a magánélethez és a személyes adatok védelméhez való jogot. Ez esetben is abban kellett dönteni, hogy a brit jogszabály, amely általános adatmegőrzést ír elő, összhangban van-e az uniós joggal, különösen az Alapjogi Chartával és az EU irányelveivel. Ez a kérdés arra vonatkozott, hogy az általános és különbségtétel nélküli adatmegőrzés összeegyeztethető-e az uniós adatvédelmi követelményekkel. A bíróság előtt állt az a kérdés, hogy milyen feltételek

---

[126]Európai Unió Bírósága: C-698/15. sz. ügy – Secretary of State for the Home Department kontra Tom Watson és társai. Ítélet, 2016. december 21. Elérhető: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=HU (letöltés dátuma: 2022. 05. 06.)

[127]*Az Egyesült Királyság hivatalosan 2020. január 31-én lépett ki az Európai Unióból. A kilépés után egy átmeneti időszak következett, amely 2020. december 31-én ért véget. Ez alatt az átmeneti időszak alatt az Egyesült Királyság továbbra is alkalmazta az Európai Unió szabályait, miközben a jövőbeli kapcsolatokra vonatkozó tárgyalások zajlottak. Az átmeneti időszak lezárultával az Egyesült Királyság teljes mértékben elhagyta az Európai Unió egységes piacát és vámunióját.*

[128]*Data Retention and Investigatory Powers Act 2014*. Elérhető: https://www.legislation.gov.uk/ukpga/2014/27/contents, letöltés dátuma: 2023. 04. 18

mellett férhetnek hozzá a hatóságok a megőrzött adatokhoz. Különösen fontos volt meghatározni, hogy a hozzáférés mennyiben felel meg az uniós jog által megkövetelt garanciáknak, beleértve a független felülvizsgálat szükségességét és a hozzáférés célhoz kötöttségét. Az Európai Bíróság megerősítette korábbi álláspontját, miszerint az általános és különbségtétel nélküli adatmegőrzés összeegyeztethetetlen az uniós joggal. Az ilyen jellegű adatmegőrzés jelentős beavatkozást jelent a magánélethez való jogba, és nem igazolható a szükségesség és arányosság elveinek megfelelően. A hozzáférésnek célhoz kötöttnek kell lennie, és csak súlyos bűncselekmények esetében engedélyezhető. Emellett az adatkezeléshez független hatóság előzetes engedélye szükséges, ami biztosítja az adatvédelmi jogok megfelelő védelmét továbbá hangsúlyozta, hogy az adatmegőrzésre és a hozzáférésre vonatkozó nemzeti szabályozásnak megfelelő garanciákat kell biztosítania annak érdekében, hogy a személyes adatok védelme ne sérüljön. Ilyen garanciák közé tartozik az adatmegőrzési időszak minimalizálása, a célhoz kötöttség elvének betartása, valamint a független felügyelet biztosítása.

Ezek az esetek vezettek a C-207/16.[129] számú ügyhöz, amely az Európai Unió Bírósága elé került és ezzel jelentős precedenst teremtett a személyes adatokhoz való hozzáférés és az adatvédelem területén, különös tekintettel a bűnüldözési tevékenységek során felmerülő kihívásokra. A központi kérdés az volt, hogy a bűnüldöző hatóságok milyen jogi feltételek mellett férhetnek hozzá a személyes adatokhoz a nyomozás részeként, figyelembe véve az európai alapvető jogok védelmét, különösen a magánélet tiszteletben tartását és a személyes adatok védelmét. Az ügy egy spanyolországi jogvitából indult, ahol a helyi bűnüldöző hatóságok egy elektronikus hírközlési szolgáltatót kötelezték arra, hogy a nyomozás részeként adjon át bizonyos személyes adatokat. Ezek között szerepeltek a hívások időpontjai, időtartamai, a hívó és hívott felek azonosítói, valamint cellainformációk, amelyek lehetővé tették a hívások földrajzi helyének meghatározását. A nyomozás tárgya egy viszonylag kisebb súlyú bűncselekmény, egy telefonlopás volt, amelynek felderítése érdekében kívánták felhasználni ezeket az adatokat. A spanyol bíróság előtt álló fő kérdés az volt, hogy a személyes adatokhoz való hozzáférés a Charta 7. és 8. cikke által biztosított alapvető jogokkal összhangban megengedhető-e a kisebb súlyú bűncselekmények esetén is, vagy csak súlyosabb bűncselekmények nyomozása

[129] Bot, M.: Főtanácsnoki indítvány: Polbud – Wykonawstwo ügy (C-106/16). In: *EUR-Lex*, 2017. 1-22. o. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:62016CC0207&from=EN.

indokolhatja ezt a beavatkozást. [130][131] Az Európai Unió Alapjogi Chartájának 7. és 8. cikke az Európai Unió alapvető jogi keretében központi szerepet játszik az egyének alapvető jogainak védelmében, különös tekintettel a magánélet és a személyes adatok védelmére, amelyek a digitális korban kiemelt jelentőséggel bírnak. A magán- és családi élet tiszteletben tartásához való jog, azaz a 7. cikk szilárdan rögzíti, hogy minden egyénnek joga van a magánéletének, családi életének, otthonának és kapcsolattartásának tiszteletben tartásához.[132] Ez a jog nem csupán az egyén fizikai terének védelmét jelenti, hanem kiterjed minden olyan területre, amely az egyén magánszféráját érinti. Ide tartozik például a személyes kommunikáció védelme, amely különösen fontossá vált a digitális technológiák térnyerésével, ahol az online kommunikáció biztonsága és a magánélet tiszteletben tartása különösen sérülékeny. A 7. cikk alapvetően biztosítja, hogy az egyének magánszférája, amely a modern világban mind inkább összefonódik a digitális tevékenységekkel, megfelelő védelmet élvezzen az állami és magánszektor beavatkozásaival szemben. A 8.cikk kifejezetten a személyes adatok védelmének fontosságára összpontosít, és több kulcsfontosságú rendelkezést is tartalmaz.[133] Először is, minden egyénnek joga van a rá vonatkozó személyes adatok védelméhez, ami azt jelenti, hogy az adatkezelés során tiszteletben kell tartani az érintett személy jogait és méltóságát. Az ilyen adatokat csak tisztességesen, jogszerűen és kizárólag meghatározott célból lehet kezelni, amelyhez az érintett személy előzetes beleegyezése szükséges, vagy más törvényes alap megléte indokolhatja az adatkezelést, továbbá mindenkinek joga van a róla gyűjtött adatokat megismerni, kijavítani. Ezen szabályok tiszteletben tartását független hatóságnak kell ellenőriznie. A spanyol bíróság előzetes döntéshozatal iránti kérelmet nyújtott be az Európai Unió Bíróságához, hogy tisztázza az uniós jog értelmezését ebben a kontextusban. Az Európai Unió Bírósága az ítéletében hangsúlyozta, hogy a személyes adatokhoz való hozzáférés komoly beavatkozást jelent az érintettek alapvető jogainak védelmébe, különösen a magánélet tiszteletben tartásának jogába. A bíróság ugyanakkor megállapította, hogy a bűnüldözés érdekében ilyen

[130]Európai Unió Alapjogi Chartája: 7. cikk. Az Európai Parlament, a Tanács és a Bizottság közös nyilatkozata. 2000.
[131]Európai Unió Alapjogi Chartája: 8. cikk. Az Európai Parlament, a Tanács és a Bizottság közös nyilatkozata. 2000.
[132]Európai Unió Alapjogi Chartája: 7. cikk. Az Európai Parlament, a Tanács és a Bizottság közös nyilatkozata. 2000.
[133]Európai Unió Alapjogi Chartája: 8. cikk. Az Európai Parlament, a Tanács és a Bizottság közös nyilatkozata. 2000.

beavatkozás indokolt lehet, feltéve, hogy az arányos és szükséges a nyomozás céljának eléréséhez. A bíróság továbbá kifejtette, hogy az arányosság elvének betartása kulcsfontosságú ugyanis a hatóságoknak csak olyan esetekben szabad hozzáférniük a személyes adatokhoz, ahol a bűncselekmény súlya ezt indokolja, és ahol a hozzáférés valóban szükséges a bűncselekmény felderítéséhez vagy megelőzéséhez. Fontos kiemelni a főtanácsnok véleményét, amely szintén kiemelt jelentőséggel bírt az ügy megítélése szempontjából. A főtanácsnok rámutatott arra, hogy bár a személyes adatokhoz való hozzáférés súlyos beavatkozást jelent, mindemellett a kisebb súlyú bűncselekmények esetén is indokolt lehet, ha az adatokhoz való hozzáférés arányos és elengedhetetlen a nyomozás sikeréhez. Ugyanakkor hangsúlyozta, hogy a jogszerűség és az alapvető jogok védelmének biztosítása minden esetben elsődleges szempont kell, hogy legyen. Az Európai Unió Bíróságának ítélete véleményem szerint eredendően befolyásolta az adatvédelem és a bűnüldözés közötti egyensúly megteremtését az Európai Unióban. A bíróság világosan rögzítette, hogy bár a személyes adatok védelme alapvető jog, a bűnüldözés érdekében történő hozzáférés megengedhető, ha az megfelel az arányosság és a szükségesség követelményeinek. Ez az ítélet iránymutatást nyújt a tagállami bíróságok számára az ilyen típusú ügyek elbírálásakor, különösen abban, hogy mikor indokolt a személyes adatokhoz való hozzáférés engedélyezése. Rámutatott arra is, hogy az új technológiák, további kihívásokat jelentenek ezenkívül az ilyen technológiák által felvetett kérdések jövőbeli jogalkotási és jogalkalmazási, értelmezési bizonytalanságokat kelthetnek, amelyeket megfelelően kell kezelni annak érdekében, hogy biztosítani lehessen a bűnüldözés hatékonyságát és az egyének alapvető jogainak védelmét.

A kiberbűnözést az Európai Unió kiemelt prioritásaként kezeli. Ezt igazolja az is, hogy 2013-ban olyan irányelvet adott ki az információs rendszerek elleni támadások tárgyában (2013/40/EU irányelv), amely a tagállamok számára előírta a főbb „cyber-bűncselekmények" büntetendővé tételét illetőleg a büntetések szigorítását.[134] Az uniós jogalkotás keretében több olyan jogszabály is született, amely közvetlenül érinti a tárgyalt problémakört. Példaként említhető a 2011/93/EU irányelv, amely a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni fellépést célozza, és amelynek nyomán a tagállamok (így Magyarország is) szigorították e cselekmények büntetőjogi megítélését.

[134]Európai Parlament, Tanács: 2013/40/EU irányelv az információs rendszerek elleni támadások elleni büntetőjogi intézkedésekről, 2013. augusztus 12. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32013L0040 (letöltés dátuma: 2022. 04. 06.)

Emellett kiemelendő a 2019/713/EU irányelv is, amely a fizetési eszközökkel kapcsolatos csalásokkal szembeni fellépést szabályozza, különös tekintettel a bankkártya csalásokra és a kibertérben elkövetett pénzügyi visszaélésekre, ezzel korszerűsítve a terület büntetőjogi szabályozását.[135] Továbbá az is ezt igazolja, hogy az EU Biztonsági Unió Stratégia részeként külön program által foglalkozik a kibertér biztonságával és a bűnüldözés erősítésével, amely 2020-ban került elfogadásra.[136] E körben kell kiemelni azt is, hogy 2021-ben az Európai Unió Tanácsa elfogadta a Kiberbiztonsági Stratégiát, amely a kiberbűnözés elleni fellépést is magában foglalja, továbbá folyamatban van egy új, egységes európai e-Evidence (azaz elektronikus bizonyíték) szabályozás kialakítása, amely lehetővé tenné, hogy a hatóságok közvetlen megkeresésekkel jussanak hozzá a más tagállamban lévő szolgáltatóknál tárolt adatokhoz, ezáltal jelentőssen felgyorsítva a nyomozást.[137][138][139] Fontos még megemlíteni, hogy globális szinten is zajlik egy új, átfogó ENSZ kiberbűnözési egyezmény kidolgozása, bár ennek elfogadása jelen disszertáció készültekor még folyamatban van. A nemzetközi szervezetek közül az Interpol és az EUROPOL is lényeges funkciót tölt be a kiberbűnözés elleni küzdelem keretében. A tagállamok rendőrségei közötti információk gyors áramlását, átadását továbbá a koordinációs feladatokat segíti elő az INTERPOL cyber egysége.[140] 2013-ban az EUROPOL, Hágában létrehozta az Európai Kiberbűnözés Elleni Központ EC3 nevű részlegét, amelynek fő célja az, hogy operatív támogatást adjon a tagállami nyomozásoknak, összehangolja a kiterjedt nemzetközi műveleteket, és az éves jelentéseiben (IOCTA: Internet Organized Crime Threat Assessment) átfogóan vizsgálja

---

[135]Európai Parlament és Tanács: Az Európai Parlament és a Tanács (EU) 2019/713 irányelve (2019. április 17.) a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról. Hivatalos Lap: L 123, 2019.5.10., 18–29. o. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32019L0713 (letöltés dátuma: 2022. 05.01)

[136]Európai Bizottság: A Biztonsági Unió Stratégiája A biztonság erősítése a fizikai és digitális térben (2020–2025). COM(2020) 605 final. Brüsszel, 2020. július 24. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020DC0605 (letöltés dátuma: 2022. 05. 06.)

[137] Európai Bizottság – Külügyi Szolgálat: EU Cybersecurity Strategy for the Digital Decade. JOIN(2020) 18 final. Brüsszel, 2020. december 16. Elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2020%3A18%3AFIN (letöltés dátuma: 2022. 05. 01.)

[138]Európai Bizottság: Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. COM(2018) 225 final. Brüsszel, 2018. április 17. Elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0225 (letöltés dátuma: 2022. 05. 01.)

[139]E-evidence cross-border access to electronic evidence. = European Commission, [n.d.]. Elérhető: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en,

[140]Interpol: Cybercrime Directorate. Elérhető: https://www.interpol.int/en/Crimes/Cybercrime (letöltés dátuma: 2022. 05. 06.)

az aktuális fenyegetéseket.[141][142]Az Eurojust, az EU igazságügyi együttműködési ügynöksége szintén aktív.[143] Megfigyelhető, hogy egyre több, kiberbűnözéssel kapcsolatos ügyet koordinál, közös nyomozócsoportokat (JIT: Joint Investigation Team) hoz létre és támogatást nyújt a határokon átnyúló nyomozásokban is.[144]

2.12. A magyar büntetőjog és büntetőeljárás

A magyar büntetőjog viszonylag korán felismerte a kiberbűnözés jelentette kihívásokat, és mára a hatályos Büntető Törvénykönyv 2012. évi C. törvény, (a továbbiakban: Btk.) külön fejezetben szabályozza a tiltott adatszerzést és az információs rendszer elleni bűncselekményeket. A Btk. XLIII. fejezete alatt találhatóak meg a tipikusan "cyber-dependent" (azaz a kizárólag információs rendszerek ellen irányuló bűncselekmények), mint a Tiltott adatszerzés (Btk. 422. §), az Információs rendszer vagy adat megsértése (Btk. 423. §), valamint az Információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424. §).[145][146][147] Az információs rendszerek megfelelő működéséhez, valamint az azokban tárolt adatok biztonságához fűződő közérdeket védő, jogi tárgyú büntetőjogi tényállások az előző fejezetben már tárgyalt 2001-es Budapesti Egyezmény előírásainak való megfelelést szolgálják.[148] A 422. § tiltott adatszerzés bűncselekménye példának okán lefedi az információs rendszerbe való jogosulatlan belépést és az ott elhelyezett védelemmel ellátott adatok megszerzését (voltaképpen a már említett klasszikus "hacking" tevékenységet), míg a 423. § az információs rendszerben vagy adatban okozott károkozó műveleteket (adatok törlése, módosítása, hozzáférhetetlenné

[141]Nemzeti Kibervédelmi Intézet Europol EC3 szerepe https://nki.gov.hu/it-biztonsag/nemzetkozi-kapcsolatok/europol
[142]Europol: Internet Organised Crime Threat Assessment (IOCTA) 2024. Elérhető: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (letöltés dátuma: 2024. 08. 06.)
[143]Eurojust: Az Eurojust bemutatása Tények és adatok (tájékoztató kiadvány), 2020. Elérhető: https://www.eurojust.europa.eu/sites/default/files/2020-12/2020-08_Generic-factsheet_public_Final4_HU.pdf (letöltés dátuma: 2024. 02. 04.)
[144] Eurojust – European Judicial Network: Joint Investigation Teams – Practical Guide, 2021. Elérhető: https://www.eurojust.europa.eu/sites/default/files/assets/joint_investigation_teams_practical_guide_2021_en.pdf (letöltés dátuma: 2024. 05. 06.)

[145]Mezei Kitti, *Ügyészek Lapja* 2020/3., 54–55. o.
[146]Clough, Jonathan: Principles of Cybercrime. Cambridge University Press, Cambridge,. 10–11. o., 2015
[147]Btk. 422. §, Btk. 423. §, Btk. 424. §
[148]Mezei Kitti, *Ügyészek Lapja* 2020/3., 54–55. o.

tétele) rendeli büntetni.[149][150] A 424. § pedig a védelmi intézkedések kijátszását, azaz tipikusan a számítógépes biztonsági rendszerek feltöréséhez használatos programok, jelszavak jogosulatlan megszerzését, forgalomba hozását és terjesztését kriminalizálja. [151]

Mindazonáltal fontos kiemelni azt, hogy nem kizárólag ezen külön fejezet tartalmaz olyan deliktumokat, amelyek a kiberbűnözés körébe tartoznak. Számos hagyományos bűncselekmény különös részi tényállása is alkalmazható, ha az elkövetés eszköze az informatikai rendszer. Ezt jól illusztrálja például az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §), amikor a „hagyományos" csalás (Btk. 373. §) digitális vagy informatikai eszközökön keresztül történik.[152][153] Általánosan ide sorolható például az online banki csalás, az automatizált, robotikás programmal használt csalás, a rendszerekbe való betörés és adatmanipuláció. Ugyancsak ide sorolható a készpénz-helyettesítő fizetési eszközzel visszaélés (Btk. 393. §) (pl. bankkártyával elkövetett visszaélések).[154] A nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények között találjuk a gyermekpornográfia tényállását (Btk. 204. §), amely a gyermekekről készült tiltott pornográf felvételek megszerzését, tartását, kínálását, átadását, hozzáférhetővé tevését, készítését, forgalomba hozását, kereskedését, ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tételét bünteti, a jelenlegi technológiai környezetben tipikusan online környezetben, elektronikus platformokon zajló cselekmények esetében is alkalmazva.[155] A zaklatás (Btk. 222. §) törvényi tényállása is kiterjed az elektronikus kommunikáció útján történő rendszeres vagy tartós háborgatásra.[156] Emellett a kábítószer-kereskedelem (Btk. 176–177. §) és az emberkereskedelem (Btk. 192. §) „tradicionális" deliktumai is új árnyalatot kapnak, amikor az elkövetők az internetes eszközökkel vagy az interneten (pl. darknet piacokon vagy közösségi médián) keresztül bonyolítják tevékenységüket.[157] [158]

[149]Btk. 422. §
[150]Btk. 423. §
[151]Btk. 424. §
[152]Btk. 373. §
[153]Btk. 375. §
[154]Btk. 393. §
[155]Btk. 204. §
[156]Btk. 222. §
[157]Btk. 176–177. §
[158]Btk. 192. §

A büntető anyagi jog mellett a büntetőeljárás (2017. évi XC. törvény, a továbbiakban: Be.) szabályai is alkalmazkodtak az információs társadalom jelenlegi igényeihez illetőleg fejlődéséhez. Az új Be. bevezette az elektronikus adat fogalmát, mint önálló bizonyítási eszközt, és részletes rendelkezéseket tartalmaz az elektronikus adatok lefoglalásának a végrehajtására és megőrzésére vonatkozóan.[159][160][161] A változások hatására többek között az is lehetővé vált, hogy a hatóságok az elektronikus adatok ideiglenes hozzáférhetetlenné tételét rendeljék el (ilyen lehet példának okán az illegális tartalmat hordozó honlapok blokkolása), illetve hogy a nemzetközi jogsegély keretében külföldi szervereken tárolt adatokat is beszerezzenek.[162] A Be. emellett szabályozza a titkos információgyűjtés eszközeit, amelyek kulcsfontosságúak a kiberbűnözés felderítésében (ilyen például a telekommunikációs eszközök lehallgatása vagy az információs rendszer titkos megfigyelése bírói engedéllyel).[163][164] Mindemellett fontos hangsúlyozni, hogy a digitális bizonyítékok kezelése során a hatóságoknak kötelességük biztosítani azok hitelességét és sértetlenségét, miközben maradéktalanul tiszteletben kell tartaniuk az adatvédelemhez és a magánélethez fűződő jogokat is, amelyek részletes kifejtésére a későbbi fejezetekben kerül sor.

A XXI századi bűncselekménytípusok rendszerezése különös tekintettel a kiberbűnözés formáira és megvalósulási módjaira

Az alábbiakban áttekintjük a kiberbűnözés, legjellemzőbb típusait és megjelenési formáit, különös tekintettel a már említett „kiberfüggő” (cyber-dependent) és „kiberrel támogatott” avagy digitális eszközökkel elősegített (cyber-enabled) kategóriákat.

3.1. Adatlopás és adathalászat

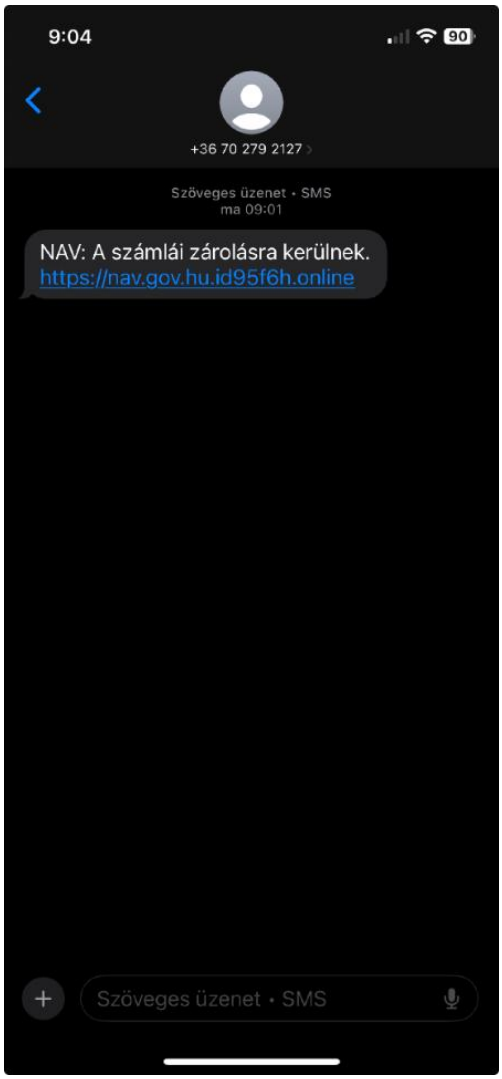
[159]Be. 165 §
[160]Be. 205 §
[161]Be. 315.-316 §
[162]Be. 335.-338 §
[163]Be 231. §
[164]Btk. 256.-260 §

A kiberbűnözés leggyakoribb formái közé tartozik az adatlopás és az adathalászat (phishing). Adatlopásról akkor beszélünk, amikor egy elkövető jogosulatlanul megszerez valamilyen védett adatot, amely adott esetben lehet személyes adat, üzleti titok, pénzügyi információ vagy akár belépési jelszó is.[165] Az adathalászat esetén a támadó megtévesztés útján arra veszi rá az áldozatát, hogy önként adja ki bizalmas adatait, információit. Általánosságban véve mindez történhet hamis e-mailek, weboldalak vagy üzenetek segítségével. Az úgynevezett „phishing" támadások rendszerint bankok, közszolgáltatásokat ellátó gazdasági szereplők vagy széleskörben ismert cégek „nevében" küldenek elektronikus üzenetet, amelyben sokszor valamilyen sürgős esetre vagy teendőre hivatkozva (pl. jelszó-újítás, számlaegyeztetés) csalják ki az áldozat bejelentkezési adatait vagy bankkártya-információit. Az alábbiakban öt konkrét esetet mutatok be, amelyek során Magyarországon ismert gazdasági szereplők, intézmények nevében történtek „phishing" (adathalász) támadások. Ezen esetek bemutatásával a célom, hogy jól szemléltessem az adathalász támadások változatos módszereit és az általuk célzott adatköröket.

2025 tavaszán több magyar állampolgár is kapott olyan SMS-eket, amelyek látszólag a Nemzeti Adó- és Vámhivataltól (továbbiakban: NAV) származtak. Az SMS-ek arról értesítették a címzetteket, hogy a számláik zárolásra kerültek, vagy az adott ügyfélnek adóhátraléka van és ennek lehívásához egy linkre kattintva kellett megadniuk a banki vagy ügyfélkapus belépési adataikat. Az üzenetekben található link azonban egy, a NAV valódi honlapját utánzó, hamis weboldalra vezetett. Az esetek kapcsán a NAV hivatalos közleményt is kiadott, figyelmeztetve az adózókat az adathalász támadásokra.[166]

[165]Varga Árpád: Az adathalászat általános jellemzői, trendjei és észlelési kérdései napjainkban. Infokommunikáció és Jog, 2020/1. (74.), 14–20. o. Elérhető: https://szakcikkadatbazis.hu/doc/1134438 (letöltés dátuma: 2021 01. 14.)

[166]Nemzeti Adó- és Vámhivatal: *Kamuüzenetek a NAV nevében*. Elérhető: https://nav.gov.hu/sajtoszoba/hirek/Kamuuzenetek_a_NAV_neveben (letöltés dátuma: 2025. 05. 06.)



2. ábra

Nemzeti Adó- és Vámhivatal: Kamuüzenetek a NAV nevében. Elérhető: https://nav.gov.hu/sajtoszoba/hirek/Kamuuzenetek_a_NAV_neveben

From: ertesites@tarhely.gov.hu <escconf2022@mke.org.hu>
To: sales@bhe-mw.eu
Date: 2025. 03. 19 03:27
Subject: [virus a variant of MSIL/TrojanDownloader.Agent.RWE trojan] Adóbevallási értesítés (Feladó: NAV, Bizonylat: Adóbevallási okmány: 94 - 022835271202502122332871983)

Adóbevallási értesítés

Tisztelt Ügyfelünk!

Mellékletben megküldtük az adóhatóság által készített bevallási tervezetet, kérjük, vizsgálja felül, szükség esetén módosítsa.
Az adóbevallások benyújtásának határideje 2025. május 20. Ez a határidő azonos az online és offline benyújtásnál.

Ennek a dokumentumnak nincs másolata az Ön tárhelyére ezért kérjük, most mentse el a számítógépére

Értesítő kiállításának időpontja: 2025.03.18. 00:48:46

Feladó: **Nemzeti Adó- és Vámhivatal** (NAV)

Dokumentum főbb adatai
Bizonylat nyugta száma: **022835271202502122332871983**
Dokumentum típusa: **Adóalany adóbevallási tervezet**
Elküldött fájl neve: **Adóbevallási.img**
Dokumentum küldésének ideje: **2025.03.18. 00:49:36**

Üdvözlettel:
IdomSoft Biztonságos Kézbesítési Szolgáltatás

Magyarországról hívható telefonszám: 1818, külföldről: +36 1 550 1858
E-mail: 1818@1818.hu
Honlap

3. ábra

Nemzeti Adó- és Vámhivatal: Kamuüzenetek a NAV nevében. Elérhető: https://nav.gov.hu/sajtoszoba/hirek/Kamuuzenetek_a_NAV_neveben

Hasonló támadások érintették 2022-ben az OTP Bank ügyfeleit is. Ebben az esetben az ügyfelek tömegesen kaptak ugyancsak SMS-eket, amelyek arról számoltak be, hogy a bankkártyájukat zárolták és az üzenetben szereplő linkre kattintva tudják feloldani.[167] A támadók által üzemeltetett weboldal rendkívül pontos másolata volt az OTP Bank netbankos felületének, így számos felhasználó adta meg gyanútlanul belépési adatait.[168] Az OTP Bank szintén figyelmeztette ügyfeleit az ilyen jellegű csalásokra, továbbá fontos kiemelni azt, hogy ezen csalások ellen összefogott a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, a Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitánysággal együtt amelynek révén különböző

[167]HVG: Vigyázzon az OTP nevében küldött SMS-sel! – csalók írogatnak. 2022. december 6. Elérhető: https://hvg.hu/gazdasag/20221206_OTP_SMS_csalas (letöltés dátuma: 2022. 12. 06.)

[168]24.hu: Legyen óvatos, ha ilyen SMS-t kap!. 2022. december 9. Elérhető: https://24.hu/tech/2022/12/09/sms-csalas-adathalaszat-otp-bankkartya-veszelyes/ (letöltés dátuma: 2022. 12. 10.)

kommunikációs kampányt indítottak a hasonló támadások kivédése érdekében és a pénzügyi fogyasztók védelmében (Kiberpajzs).[169]

4. ábra

Képernyőkép (www.facebook.com)

A Magyar Posta nevében is számos adathalász támadást követtek el 2021 és 2023 között. Ezek során a csalók SMS-ekben vagy e-mailekben jelezték, hogy a címzett csomagját nem sikerült kézbesíteni, és egy kisebb összegű díj kifizetésével kezdeményezhetik az újrakézbesítést. A megtévesztő weboldalon bankkártya-adatokat kellett megadni, amelyeket később jogosulatlan tranzakciókra használtak fel a támadók. A Magyar Posta rendszeresen felhívta ügyfelei figyelmét az ilyen csalások veszélyeire és kommunikációs kampányokban tájékoztatta őket arról, hogy a Magyar Posta ilyen módon sose kéri el a bankkártya-adataikat.[170]

2022 nyarán a magyarországi internetes kereskedelmi platformok sem maradtak ki az ilyen jellegű támadásokból. Az eMAG webshop nevében a közösségi médiában széles körben terjedő kampány során ígértek 57 250 forint helyett 745 forintért szerszámot. A

[169]KiberPajzs: Csalástípusok: telefonos, számítógépes, SMS-es és e-mailes csalások áttekintése. Elérhető: https://kiberpajzs.hu/csalastipusok (letöltés dátuma: 2023. 05. 30.)
[170]Magyar Posta Zrt.: FIGYELEM! Továbbra is adathalász levelet és SMS-t vagy közösségi médiában álfelhívásokat küldenek a Magyar Posta nevében. Elérhető: https://www.posta.hu/aktualitasok/adathalasz_levelet_es_smst_kuldenek_a_magyar_posta_neveben_20230628 (letöltés dátuma: 2023. 09. 29.)

megtévesztett vásárlók bankkártya-információi ezzel a módszerrel kerültek az illetéktelenek birtokába.[171]

5. ábra

Képernyőkép (www.facebook.com)

A korábban ismertetett hazai esetek mellett érdemes kitérni egy nemzetközi esetre is, amely jól mutatja, hogy a phishing jelensége globális léptékű problémát jelent. A PayPal Holding Inc. közismert nemzetközi vállalat, amely online fizetési szolgáltatásokat nyújt világszerte. Nem meglepő tehát, hogy a vállalat nevével visszaélve nemzetközi szinten kezdeményeztek adathalász tevékenységeket. A csalók hamis biztonsági

[171] HVG: -99% akció, de +100% átverés az eMAG nevében hirdetett 745 forintos ajánlat. 2022. július 18. Elérhető: https://hvg.hu/tudomany/20220718_emag_csempeszett_makita_utvefuro_lefoglalt_57_250_forint_helyett_745_forint_akcio_atveres (letöltés dátuma: 2022. 07. 18.)

figyelmeztetésekkel ijesztették meg az ügyfeleket, sürgetve őket, hogy adják meg fiókjuk belépési adatait egy látszólag hiteles PayPal-felületen, amelynek URL-je megtévesztően hasonlított a hivatalos PayPal domainre. Ezek a támadások több ezer PayPal felhasználó adatait kompromittálták, komoly pénzügyi károkat okozva. [172] Magyarországon ezen bűncselekmények büntetőjogi megítélése számos büntetőjogi tényállás alá eshet. Amennyiben a támadó technikai eszközökkel hatol be egy rendszerbe, hogy onnan adatot szerezzen meg, úgy a Btk. tiltott adatszerzés (Btk. 422. §) vagy információs rendszer vagy adat megsértésének (Btk. 423. §) tényállása is alkalmazható.[173][174] Ha „social engineering" folytán, (azaz manipulációval való bizalmas információ szerzésével, egyszerűbben kifejezve, megtévesztéssel éri el ugyanezt az elkövető) tehát például ha egy banki ügyfél adatait csalja ki és ezzel kárt okoz, akkor minősíthető elsősorban csalásnak (Btk. 373. §), rendszerint információs rendszer felhasználásával elkövetett csalásnak (Btk. 375. §).[175][176] A megszerzett adatok típusa további tényállásokat is felvethet, mint például a személyes adattal visszaélés (Btk. 219. §) vagy vállalati, céges adatoknál akár gazdasági titok megsértése (Btk. 413. §) is releváns lehet.[177][178] Mind nemzetközi, mind hazai szinten ugrásszerűen nőtt az adathalász támadások száma az elmúlt években, amit az előzekben bemutatott esettanulmány is alátámaszt. A vállalati és az intézményi szféra ellen irányuló phishing különösen veszélyes, mivel gyakran a munkavállalók hiszékenységén vagy éppen a jóhiszeműségén keresztül jutnak be a támadók a nagyobb rendszerekbe, ezzel veszélyeztetve sok ezer ügyfél vagy partner adatait is. A magyar tapasztalatok szerint a kibertámadások között az információs rendszer védelmét biztosító technikai intézkedés kijátszásának számában (amely lefedi az adathalász tevékenységet) több mint harmincszoros növekedés mutatkozott.[179] Nem egy esetben közel 8 millió forintot meghaladó összegeket is kicsaltak már ilyen módszerrel mit sem sejtő

[172]Ionut Arghire: PayPal Phishing Campaign Employs Genuine Links to Take Over Accounts. SecurityWeek, 2025. január 10. Elérhető: https://www.securityweek.com/paypal-phishing-campaign-employs-genuine-links-to-take-over-accounts/ (letöltés dátuma: 2025. 01. 13.)
[173] Btk. 422. §
[174] Btk. 423. §
[175] Btk. 373. §
[176] Btk. 375. §
[177] Btk. 219. §
[178] Btk. 413. §
[179] A Legfőbb Ügyész Országgyűlési beszámolója, az ügyészség 2023. évi tevékenységéről. B/8995. szám Elérhető: https://www.parlament.hu/irom42/08995/08995.pdf (letöltés dátuma: 2024. 09. 27.)

áldozatoktól.[180] A bűnözők az ellopott adatokkal közvetlenül vagy közvetve visszaélnek. Közvetlenül, amikor az ellopott jelszavakkal megpróbálnak további rendszerekbe illetéktelenül behatolni, vagy felhasználói fiókokhoz hozzáférni, esetlegesen, feltörni. Közvetve, amikor a már megszerzett adatokat tovább értékesítik olyan internetes felületeken vagy piactereken, amelyeken a felhasználók azonosítása kifejezetten nehéz.

3.2. Deepfake

A „deepfake" (magyarul „mélyhamisítás") olyan mesterségesintelligencia-alapú technika, amely generatív neurális hálózatokkal (elsősorban deep learning és GAN-modellek (generatív adverzális hálózatok)) manipulál vagy hoz létre audio- és vizuális tartalmakat.[181] A Képviselői Információs Szolgálat (az Országgyűlés Hivatala Közgyűjteményi és Közművelődési Igazgatóságának keretében működő szakmai egység) 2024-ben kiadott infojegyzete szerint a deepfake-technológia 2017 végén vált szélesebb körben ismertté, amikor egy Reddit-felhasználó pornográf videói nyomán került a figyelem középpontjába. [182] A generatív ellenfelek hálózatának (GAN) alkalmazása ekkor jelentős minőségi ugrást eredményezett a manipulált tartalmak előállításában. A deepfake eszközeinek elérhetősége és a felhasználás egyszerűsége miatt már nemcsak filmstúdiók, hanem bárki képes a hitelesnek tűnő hamis felvételek előállítására. Megállapítható, hogy ez a jelenség szoros összefüggést mutat a kiberbűnözés különböző formáival, így a hamis hírek terjesztésével, az identitáslopással, a zsarolóvideók előállításával és terjesztésével, valamint a bírósági bizonyítás manipulálásával.[183] Herke Csongor Pro Futuro-tanulmánya (2023) rávilágít arra, hogy a deepfake nemcsak kockázat, hanem bizonyos szituációkban, mint például oktatásban, kultúrában vagy művészetben hasznos eszköz is lehet.

---

[180]Zala Vármegyei Rendőr-főkapitányság: Megint nem nyert. Police.hu, 2025. március 5. Elérhető: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/megint-nem-nyert (letöltés dátuma: 2025. 03. 05.)

[181]Országgyűlés, Képviselői Információs Szolgálat: Deepfake technológia és jog. *Infojegyzet* 2024/20. Elérhető:https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog (Letöltés: 2024. 08. 11.)

[182]Országgyűlés, Képviselői Információs Szolgálat: Deepfake technológia és jog. *Infojegyzet* 2024/20. Elérhető:https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog (Letöltés: 2024. 08. 11.)

[183]Lendvai, Gergely Ferenc: Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából. In: Aczél, Petra – Veszelszki, Ágnes (szerk.): *Deepfake: a valótlan valóság*, Gondolat Kiadó, Budapest, 2023, 121–138.o.Elérhető: https://www.researchgate.net/publication/373737686_Deepfake_a_szolasszabadsag_tukreben_-_reflexiok_a_jog_perspektivajabol (letöltés dátuma: 2024. 08. 11.)

Ugyanakkor hangsúlyozza a „hazug osztalék” veszélyét, vagyis azt, hogy a hamis felvételek tömegtermelése aláássa a hitelességbe vetett társadalmi bizalmat.[184]A szerző a technológia történeti áttekintése után bemutatja az észlelési (detekciós) eszközöket és ismerteti a lehetséges jogi válaszokat. Újabb tanulmányában (Magyar Jog, 2024) Herke Csongor a büntető igazságszolgáltatás nézőpontját helyezi előtérbe, és hangsúlyozza, hogy a deepfake jelenség következtében a bizonyítékok hitelességét újra kell értékelni, továbbá a bíróságoknak fel kell készülniük a manipulált felvételek felismerésére.[185]Ezek a tanulmányok a hazai jogirodalomban úttörő módon kapcsolják össze a technológiai ismereteket a büntetőeljárás elméletével. A deepfake-tartalmak a 21. századi kiberbűnözésben több bűnözési kategóriában jelennek meg, így például a személyiségi jogokat sértő tartalmak, a politikai és közéleti manipuláció, a gazdasági bűncselekmények, a bizonyítás és igazságszolgáltatás ellenes bűncselekmények. A személyiségi jogokat sértő tartalmak kategóriájába esik a bosszúpornó, a pornográf deepfake-ek és az identitáslopás. E körben kiemelendő, hogy a deepfake anyagok mintegy 98%-a pornográf jellegű, amelyet a magyar Országgyűlés Képviselői Információs Szolgálata által készített infojegyzet is megerősít.[186] A jelenség kriminológiai és büntetőjogi jelentőségére Herke Csongor tanulmányai hívják fel különösen a figyelmet. Munkásságában a bosszúpornó elleni hatékony fellépés érdekében a Büntető Törvénykönyv rendelkezéseinek felülvizsgálatát, valamint a tartalomszűrési technológiák fejlesztését is szükségesnek tartja[187]Tanulmányai nem csupán a probléma súlyát tárják fel, hanem iránymutatást is adnak a jogalkotás és a jogalkalmazás számára. Ezen nemkívánatos felvételek terjesztése ugyanis súlyosan sértik az emberi méltóságot, a magánélethez való jogot és a képmáshoz fűződő jogot, ami indokolja a jogalkotói és szakpolitikai válaszok sürgető szükségességét.

---

[184]Herke Csongor: Deepfake: áldás vagy átok? Jogi szabályozási szempontok. *Pro Futuro*, 13(1), 2023, 157–178. DOI: 10.26521/profuturo/2023/1/13334 (Letöltés: 2023. 11. 11.)

[185]Herke Csongor: A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra. *Magyar Jog*, 71. évfolyam, 6. szám (2024) 321–332.

[186]Országgyűlés, Képviselői Információs Szolgálat: Deepfake technológia és jog. *Infojegyzet* 2024/20. Elérhető:https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog (Letöltés: 2024. 08. 11.)

[187]Herke Csongor: Deepfake: áldás vagy átok? Jogi szabályozási szempontok. *Pro Futuro*, 13(1), 2023, 157–178. DOI: 10.26521/profuturo/2023/1/13334 (Letöltés: 2023. 11. 11.)

Politikai és közéleti manipuláció közé sorolhatók a hamis kampányvideók illetőleg az álhírek. Az Európai Parlament kutatószolgálata 2025-re, 8 millió deepfake-tartalom megosztását prognosztizálja, és a technológia már elérte a szofisztikáltság olyan szintjét, hogy egyre nehezebb a hamis és valódi felvételek megkülönböztetése.[188]Herke Csongor álláspontja alapján a demokratikus diskurzust fenyegető manipulációk elleni védekezés a „detekciós eszközök és jogi szankciók kombinációját" igényli. A gazdasági bűncselekmények körében külön figyelmet érdemel a nemzetközi szakirodalomban az úgynevezett vezetői csalás (CEO fraud) néven ismert jelenség. Ennek lényege, hogy az elkövetők a célzott átverés keretében cégvezetőnek vagy felsővezetőnek adják ki magukat, és jellemzően egy sürgős pénzátutalás teljesítésére igyekeznek rábírni az áldozatot. E körben egyre nagyobb kockázatot jelentenek a hangszintetizálással megvalósított csalások is, amikor az elkövető a mesterséges intelligencia segítségével utánozza vagy lemásolja egy adott személy hangját, majd ezt felhasználva próbálja manipulálni az áldozatot valamilyen haszonszerzés vagy anyagi előny megszerzése érdekében. A deepfake-hangokkal elkövetett első ismert csalás 2019-ben történt, és azóta rohamosan nő az ilyen jellegű incidensek száma.[189]A hanghamisítás különösen veszélyes, ugyanis a telefonbeszélgetések autentikusságába vetett hitet és bizalmat használja ki. A fényképek és videófelvételek kiemelt szerepet játszanak a bizonyításban, így a deepfake technológia közvetlenül érinti az igazságszolgáltatás hitelességének megőrzését. A bizonyítás és az igazságszolgáltatás elleni bűncselekmények körében említhető a hamis bizonyíték előterjesztése, illetve az ún. deepfake-védekezés, amikor a vádlott azzal kíván érvelni, hogy a terhelő felvétel manipulált vagy hamis.[190] Herke Csongor „A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra" című tanulmányában átfogó elemzést nyújt a jelenségről, rámutatva arra, hogy a deepfake többféleképpen kerülhet alkalmazásra a bizonyítás során. Nem zárható ki az, hogy a bizonyítékot előterjesztő szándékosan, más esetben anélkül, hogy annak hamis voltáról tudomással bírna, nyújt be hamis digitális felvételt. A szerző

[188]European Parliamentary Research Service (Európai Parlament Képviselőinek Kutatási Szolgálata): Deepfakes: challenges and regulatory responses. EPRS BRI (2025)775855, 2025. Elérhető: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf (letöltés dátuma: 2025. 08. 11.)

[189]Országgyűlés, Képviselői Információs Szolgálat: Deepfake technológia és jog. *Infojegyzet* 2024/20. Elérhető:https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog (Letöltés: 2024. 08. 11.)

[190]Herke Csongor: A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra. *Magyar Jog*, 71. évfolyam, 6. szám (2024) 321–332

érvelése szerint az ilyen „mélyhamis” bizonyítékok komoly veszélyeket hordoznak, mivel téves ítéletekhez vezethetnek, alááshatják a tanúvallomások hitelességét, és jelentősen csökkenthetik a vizuális és audio alapú bizonyítékok megbízhatóságát.[191]A tanulmány külön érdeme, hogy nem pusztán a problémát azonosítja, hanem konkrét megoldási irányokat is kijelöl amelynél hangsúlyozza a bíróságok számára az új autentikációs módszerek és mesterséges intelligencia-alapú detektálási technológiák alkalmazásának szükségességét, továbbá kiemeli a jogi keretek megerősítésének, a hatóságok tagjai és a védők célzott képzésének fontosságát valamint a szakértők fokozott bevonásának elengedhetetlenségét. Ezen megállapításokat szemléletesen támasztja alá egy 2025. szeptember 30-át követően utótűzként terjedő, bolti CCTV-stílusú „lopást” bemutató AI-videó. Több internetes bejegyzés az OpenAI által frissen bejelentett Sora 2-höz (egy szövegből és rövid felvételekből videót generáló rendszerhez és iOS-alkalmazáshoz) kapcsolta azt a videótartalmat avagy klipet, amelyben egyes posztok szerint Sam Altman, az OpenAI ismert vezetője „szerepelt”, amint GPU-kat (nagy számítási teljesítményű grafikus processzorokat, amelyeket többek között mesterségesintelligencia-modellek tanítására és futtatására használnak) „lop” egy Target áruházból.[192]A felvételt egy X-felhasználó kifejezetten demonstrációs és figyelemfelkeltő céllal készítette, annak érdekében, hogy bemutassa a Sora 2 és az új közösségi videóalkalmazás lehetőségeit ugyanakkor nyíltan jelezte is, hogy a klip AI-generált, nem pedig egy valós bűncselekmény dokumentuma.[193] Mindezek ellenére az alacsony felbontás, a szemcsézettség és az „akciókamera”-nézőpont együttesen olyan erős valósághatást keltett, hogy sok nézőt megtévesztett, és a videó rövid idő alatt intenzív online terjedésnek indult. Ez jól példázza, hogy a szintetikus tartalmak esetében az esztétika és vizualitás milyen meggyőzővé teheti a valószerű illúziót. A bemutatott jelenség kifejezetten indokolja, hogy a bizonyítási rendszer felkészülten kezelje a deepfake-kockázatokat. Az Egyesült Államok jogirodalmában Delfino javaslata által már megfogalmazódott az igény a szövetségi bizonyítási szabályok (Federal Rules of Evidence) felülvizsgálatára, különösen a 901. szabály kiegészítésére, annak érdekében,

[191]Herke Csongor: A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra. *Magyar Jog*, 71. évfolyam, 6. szám (2024) 321–332
[192]Indiatimes: Fact check: Is that really Sam Altman in viral GPU theft video? Clip sparks debate among netizens. Elérhető: https://www.indiatimes.com/trending/fact-check-is-that-really-sam-altman-in-viral-gpu-theft-video-sora-2-clip-sparks-debate-among-netizens/articleshow/124257170.html (letöltés dátuma: 2025. 09. 30.)
[193]OpenAI: *Sora 2* Elérhető: https://openai.com/index/sora-2/ (letöltés dátuma: 2025. 09. 30.)

hogy a bírák a deepfake gyanúját nagyobb súllyal, fokozott figyelemmel értékeljék.[194][195] Az Európai Unió az AI-rendelet (2024/1689) révén elsőként alkotott átfogó jogi keretet az MI-rendszerekre.[196] A rendelet differenciált kockázati kategóriákat állapít meg, és a magas kockázatú rendszerekre szigorúbb megfelelési és nyilvántartási kötelezettségeket ír elő. A deepfake-szolgáltatókra vonatkozóan átláthatósági és címkézési kötelezettséget vezet be, a jogsértések esetén a bírság akár 35 millió euró is lehet.[197] Az Európai Unió 2022-ben megerősítette a Code of Practice on Disinformation nevű kódexet, amely önmagában nem jár bírsággal. A legfeljebb az előző évi világméretű árbevétel 6%-áig terjedő pénzbírság kiszabására a Digitális Szolgáltatásokról szóló rendelet (DSA) ad lehetőséget, amennyiben a platformok megszegik a DSA-ban előírt kötelezettségeiket (nem pedig közvetlenül azért, mert elmulasztják a deepfake-tartalmak eltávolítását).[198]

Magyarországon a Büntető Törvénykönyv több tényállása is irányadó lehet a manipulált tartalmak készítése vagy terjesztése esetén, ugyanakkor kifejezetten a deepfake jelenséget önálló bűncselekményként szabályozó rendelkezés jelenleg nem található a jogrendszerben. A szakirodalom és a jogszabályok alapján ide sorolható a személyes adattal visszaélés, amelyet a Btk. 219. § (1) a) pontja szabályoz, hiszen a mélyhamisításhoz felhasznált portrék biometrikus adatnak minősülnek, így azok engedély nélküli felhasználása a különleges személyes adatokkal való visszaélés bűncselekményét valósíthatja meg.[199] A Nemzeti Média- és Hírközlési Hatóság, valamint több elemzés is a 219. § alkalmazását javasolja a non-konzenzuális intim tartalmak elleni

[194]Rebecca Delfino: Deepfakes on Trial 2.0: A Revised Proposal for a New Federal Rule of Evidence to Mitigate Deepfake Deceptions in Court. Loyola Law School Legal Studies Research Paper No. 2025-10 2-17. p.
[195]United States House of Representatives.Committe on the Judiciary: Federal Rules of Evidence. Rule 901 Authenticating or Identifying Evidence. 1 December 2024. Committee Print No. 11, 118th Congress, 2nd Session. U.S. Government Publishing Office, Washington 2025.
[196]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Document 32024R1689. Official Journal of the European Union, L 2024/1689, 12 July 2024.
[197]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Document 32024R1689. Official Journal of the European Union, L 2024/1689, 12 July 2024.
[198]Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27.10.2022, Art. 52(3).
[199]Btk. 219. § (1) a)

fellépésre.[200] Ugyancsak releváns lehet a rágalmazás továbbá a valótlan képfelvétel tényállása a Btk. 226. és 226/A–B. § alapján, amennyiben a deepfake tartalom a sértett becsületének csorbítására szolgál.[201][202] Ebben az esetben a rágalmazás mellett a becsület csorbítására alkalmas hamis kép- vagy hangfelvétel készítése és annak nyilvánosságra hozatala is szóba jöhet. A Btk. 226/B. § kifejezetten kimondja, hogy „aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt hozzáférhetővé tesz, vétség miatt két évig terjedő szabadságvesztéssel büntetendő."[203] A zaklatás tényállása is felmerülhet a Btk. 222. § alapján, ha a deepfake tartalmat a sértett megfélemlítése vagy gyötrése céljából ismételten elküldik vagy közzéteszik.[204]A Nemzeti Kibervédelmi Intézet kiadványai külön kiemelik, hogy a deepfake-alapú bosszúpornó esetében ez a rendelkezés alkalmazható.[205] A zsarolás tényállása a Btk. 367. § szerint akkor valósul meg, ha a hamisított felvétellel a sértettet pénz vagy szolgáltatás átadására kényszerítik.[206] Súlyosabb esetben a szemérem elleni erőszakos bűncselekmények is felmerülhetnek a Btk. 195–196. § rendelkezései alapján, ha a deepfake felvételt kényszerítő eszközként használják szexuális cselekmény elkövetésére.[207] A gyermekpornográfia tényállását a Btk. 204. § szabályozza, amely alapján amennyiben a deepfake felvételen kiskorú vagy fiatalkorú személy jelenik meg, a kép vagy hang hamis voltától függetlenül gyermekpornográfia bűncselekményéről beszélhetünk.[208] Ezt a megközelítést az NMHH is kiemeli.[209] Végül a hamis magánokirat felhasználása is releváns lehet a Btk. 345. § alapján, mivel a deepfake technológiával előállított hang- vagy képfelvételek bizonyos esetekben okiratszerűen is felhasználhatók. A tényállás értelmében büntetendő az is, aki hamis vagy meghamisított magánokiratot használ fel jog vagy kötelezettség igazolására. Az erre vonatkozó tanulmányok rámutatnak arra is, hogy a mesterséges intelligencia által támogatott

[200]NMHH: Hozzájárulás nélkül közzétett tartalom (cikk). Elérhető: https://nmhh.hu/cikk/190112/Hozzajarulas_nelkul_kozzetett_tartalom (letöltés dátuma: 2024. 11. 12.)
[201]Btk. 226. §
[202]Btk. 226/A–B. §
[203]Btk. 226/B. §
[204]Btk. 222. §
[205]NMHH: Online zaklatás (cikk). Elérhető: https://nmhh.hu/cikk/190113/Online_zaklatás (letöltés dátuma: 2024. 11. 12.)
[206]Btk. 367. §
[207]Btk. 195–196. §
[208]Btk. 204. §
[209]NMHH: Gyermekkel szembeni online szexuális bántalmazás, gyermekpornográfia (cikk). Elérhető: https://nmhh.hu/cikk/19011/ Gyermekkel_szembeni_online_szexuális_bántalmazás_gyermekpornográfia (letöltés dátuma: 2024. 11. 12.)

dokumentumhamisítás szorosan összefügghet ezen rendelkezéssel, és új kihívásokat vet fel a büntetőjogi értékelés során.[210] A jelenség komplexitása rámutat arra, hogy szükséges a nemzetközi és összehasonlító szabályozási gyakorlatok vizsgálata, mivel ezek értékes támpontokat adhatnak a magyar jogrendszer fejlődési irányainak kijelöléséhez.

Az Egyesült Államokban jelenleg mozaikos a szabályozás. 2019-ben elsőként Kaliforniában és Texasban tiltották meg a választási kampányokhoz kapcsolódó a hamis politikai deepfake-ek közzétételét, valamint a pornográf deepfake-ek terjesztését, míg pl.: Virginia 2019-ben bővítette a „revenge porn" törvényt, hogy kiterjedjen a szintetikus tartalmakra.[211][212][213]2024-ben Minnesota és Kalifornia már külön törvényekkel védték az választási integritást.[214] 2025 májusában pedig szövetségi szinten elfogadták a „Take Down" törvényt, amely bűncselekménnyé nyilvánítja a nem konszenzuális szexuális deepfake-ek közzétételét, és előírja a platformoknak, hogy 48 órán belül távolítsák el a bejelentett tartalmakat.[215]A törvény továbbá pénzbírságot és akár három évig terjedő szabadságvesztést helyez kilátásba. A Kongresszus előtt további tervezetek (defiance-, no fakes-,protect elections act) is szerepelnek.[216][217][218] Ehhez szorosan kapcsolódik a már említett Rebecca Delfino 2025-ben megfogalmazott javaslata, amely a Federal Rule of Evidence 901 új (c) bekezdésének beiktatását szorgalmazza. Ennek célja, hogy a bírák fokozott ellenőrzést gyakorolhassanak a digitális bizonyítékok felett, és hatékonyabban vizsgálhassák felül a deepfake gyanúját.[219] Kanadában a hatályos jogszabályok tiltják az intim képek hozzájárulás nélküli terjesztését, továbbá a Canada Elections Act

[210]Citron, Danielle K. – Franks, Mary Anne: *Criminalizing Revenge Porn*. = Wake Forest Law Review, 49. köt., 2014 nyár, 345–391. o. Elérhető: https://scholarship.law.bu.edu/faculty_scholarship/643 (letöltés dátuma: 2022. 08. 12.)
[211]Va. Code § 18.2-386.2. (*revenge porn kiterjesztése „images … created by any means whatsoever*)
[212]California Civil Code § 1708.86. (AB 602, 2019, non-consensual deepfake pornography)
[213]Texas Penal Code § 21.165. (Unlawful Production or Distribution of Certain Sexually Explicit Media)
[214]Minn. Stat. § 609.771. (Use of Deep Fake Technology to Influence an Election)
[215]Public Law 119-12 (2025. máj. 19.) „TAKE IT DOWN Act
[216]U.S. Congress: S. 1837 (119th Congress) Defiance Act (bill text). https://www.congress.gov/bill/119th-congress/senate-bill/1837/text (letöltés: 2025. 07. 02.)
[217]U.S. Congress: S. 1367 / H.R. 2794 (119th Congress) No Fakes Act (bill text). https://www.congress.gov/bill/119th-congress/senate-bill/1367 (letöltés: 2025. 07. 02.)
[218]U.S. Congress: S. 1213 (119th Congress) Protect Elections from Deceptive AI Act (summary/text). https://www.congress.gov/bill/119th-congress/senate-bill/1213
[219]Rebecca Delfino: Deepfakes on Trial 2.0: A Revised Proposal for a New Federal Rule of Evidence to Mitigate Deepfake Deceptions in Court. Loyola Law School Legal Studies Research Paper No. 2025-10 2-17. p.

rendelkezései is alkalmazhatóak a deepfake tartalmakra.[220][221] Kína 2025 márciusában vezette be az AI által generált tartalmak kötelező címkézéséről szóló szabályozást, amely előírja a mesterségesen létrehozott vagy módosított tartalmak látható és láthatatlan megjelölését, valamint tiltja a vízjelek eltávolítását.[222][223]A rendelkezések elsősorban a szolgáltatókat célozzák, nem pedig a felhasználókat, céljuk pedig a tartalmak nyomon követhetőségének és az elszámoltathatóság biztosítása. Dél-Korea 2020-ban fogadott el olyan törvényt, amely a közérdeket sértő deepfake-ek terjesztését akár öt évig terjedő szabadságvesztéssel és 50 millió wonig terjedő pénzbírsággal rendeli büntetni.[224] 2024 szeptemberében a parlament újabb módosítást fogadott el, amely már a pornográf deepfake-ek megtekintését és birtoklását is kriminalizálja, a terjesztés büntetési tételét pedig hét évig terjedő szabadságvesztésre emeli.[225] A Reuters beszámolója szerint 2024-ben több mint nyolcszáz ilyen bűncselekményt regisztráltak.[226]Ausztrália 2021-ben módosította a nemi képmásokkal kapcsolatos törvényét, hogy a mesterségesen létrehozott tartalmakra is kiterjedjen és 2025-ben az Online Safety Act végrehajtása során az online platformok fokozott korhatár-ellenőrzést vezettek be.[227] Dánia 2025 nyarán javaslatot terjesztett elő a szerzői jogi törvény módosítására, amely értelmében mindenki jogot kapna saját teste, arcvonásai és hangja felett. A tervezet szerint a személyhez fűződő jogok (így különösen a hang és az arcképmás) megsértése esetén lehetőség nyílna a jogsértő felvétel eltávolításának követelésére, valamint kártérítés igénylésére. A javaslat a paródia és a szatíra körébe tartozó felhasználás kivételével büntetendővé tenné a

[220]1985 R.S.C., c. C-46 Criminal Code of Canada, s. 162.1 (Publication of an intimate image without consent).
[221]2000 S.C., c. 9 Canada Elections Act, s. 91 (Publishing false statement to affect election results).
[222]InsidePrivacy: China releases new labeling requirements for AI-generated content. Elérhető: https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/ (letöltés dátuma: 2025. 04. 12.)
[223]Kínai Internetinformációs Hivatal: 关于印发《人工智能生成合成内容标识办法》的通知 Tájékoztatás a „Mesterséges intelligencia által generált szintetikus tartalom azonosítására vonatkozó intézkedések” kiadásáról. 2025. március 14. Elérhető: https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm (letöltés dátuma: 2025. 08. 12.)
[224]FoundationRA: Rest of World Deep Fake AI Laws. Elérhető: https://foundationra.com/rest-of-world-deep-fake-ai-laws/ (letöltés dátuma: 2025. 08. 12.)
[225]Reuters: South Korea to criminalise watching or possessing sexually explicit deepfakes (2024. 09. 26.) (letöltés: 2024. 10. 02.)
[226]Reuters: Why South Korea is high alert over deepfake sex crimes. 2024. augusztus 30. Elérhető: https://www.reuters.com/world/asia-pacific/why-south-korea-is-high-alert-over-deepfake-sex-crimes-2024-08-30/ (letöltés dátuma: 2024. 09. 12.)
[227]eSafety: What’s on, Online Safety Act. Elérhető: https://www.esafety.gov.au/newsroom/whats-on/online-safety-act (letöltés dátuma: 2025. 09. 01.)

hozzájárulás nélküli digitális imitációt.[228] Franciaország 2024-ben a francia Büntető Törvénykönyv 226-8-1. cikkének beiktatásával kriminalizálta a nem konszenzuális szexuális deepfake-eket, amelyek elkövetőit két évig terjedő szabadságvesztéssel és 60 000 eurós pénzbüntetéssel fenyegeti.[229][230]2025-ben a Nemzetgyűlés napirendre tűzte a közösségi médiatartalmak kötelező címkézéséről szóló javaslatot is, amely pénzbírságot írna elő a címkézési kötelezettség elmulasztása esetére.[231] [232]Az Egyesült Királyságban a 2023-as Online Safety Act már tiltja az intim deepfake-ek megosztását, a 2025-ös módosítás pedig a tartalmak készítőinek büntetőjogi felelősségre vonását is javasolja, legfeljebb két évig terjedő szabadságvesztés kilátásba helyezésével.[233] 2025 júliusától emellett szigorúbb korhatár-ellenőrzési kötelezettséget vezettek be a pornográf tartalmakat kínáló weboldalakon.[234]

Az eddigiekből kirajzolódik, hogy a deepfake nem elszigetelt technikai jelenség, hanem egyszerre érinti a büntetőeljárás működését, az alapjogok érvényesülését és a gyakorlati végrehajtáshoz szükséges technológiai-infrastrukturális hátteret. Ennek megfelelően a továbbiakban célszerű egy olyan, egymásra reflektáló elemzési keretet alkalmazni, amely a bizonyítás és eljárásjog kérdéseit, a szólásszabadság és személyiségi jogok közötti egyensúly dilemmáit, valamint a detekció és intézményi-technológiai megoldások lehetőségeit és korlátait összekapcsolva tárgyalja. A deepfake-ek megkérdőjelezik az úgynevezett „vizuális igazság” paradigmáját, vagyis azt a feltételezést, hogy a vizuális felvételek önmagukban hiteles bizonyítékok. A szakirodalom egyrész rámutat arra, hogy a manipulált felvételek elterjedése nyomán több joghatóság kiterjesztette a hozzájárulás nélküli intim tartalmakat szankcionáló szabályokat, és megjelentek olyan normák is,

---

[228]Thomas Kong J. D.: To thine own self be true’ – Denmark considers extending copyright to physical likenesses. Wolters Klwer. Vital Briefing.2025.18. July. 1-2. p. https://business.cch.com/ipld/VB_Denmark-bill-copyright-physical-likenesses_07-18-2025.pdf (Letöltés: 2025. 08. 13.)

[229]Code pénal, art. 226-8. Franciaország.https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049571542?

[230] Code pénal, art. 226-8-1. Franciaország https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049571542?

[231]Assemblée nationale: Proposition de loi n° 675 (17e législature). Elérhető: https://www.assemblee-nationale.fr/dyn/17/textes/l17b0675_proposition-loi (Letöltés: 2025. 08. 13.)

[232]Hogan Lovells: France prohibits non-consensual deep fakes. Elérhető: https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes (letöltés dátuma: 2025. 08. 13.)

[233]UK Government: Online Safety Act explainer. Elérhető: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (letöltés dátuma: 2025. 08. 13.)

[234]Online Safety Act 2023. Egyesült Királyság. (https://www.legislation.gov.uk/ukpga/2023/50?utm)

amelyek gyors eltávolítási kötelezettséget írnak elő a bejelentett tartalmakra. Ugyanakkor a nemzeti szabályozási megoldások összességükben továbbra is töredezett rendszert alkotnak, ezért elengedhetetlen a nemzetek feletti együttműködés erősítése és a követelmények összehangolása. A deepfake-technológia könnyen konfliktusba kerülhet a szólásszabadság gyakorlásával. A szolgáltató központú szabályozási modell eltér az egyén és tartalomszabadság központú megközelítésektől, és bizonyos esetekben fokozott felhasználóvédelmet biztosíthat. Célszerű annak biztosítására is törekedni, hogy a paródia és a szatíra érvényesüléséhez szükséges garanciák fennmaradjanak, mivel ezek hiányában fennáll annak kockázata, hogy az intézkedések a szólásszabadság mozgásterét a kelleténél szűkebbre korlátozzák. A szakirodalom másrészt mindinkább a technológiai, jogi és társadalmi eszközök kombinációját javasolja. Kiemelt hangsúly esik a generatív tartalmak felismerését segítő megoldások fejlesztésére és a mesterségesintelligencia-műveltség erősítésére. Ugyanakkor jelenleg nem létezik teljes bizonyossággal működő felismerő rendszer, ezért a szabályozási megoldások nem alapozhatók kizárólag technikai szűrőkre. Ez a hármas fókusz közvetlen válasz a feltárt kockázatokra (ideértve a védekezési stratégiák manipulációs potenciálját, a politikai illetőleg a közéleti torzításokat, valamint a bosszúpornó és hasonló visszaélések terjedését), és egyben keretet ad annak bemutatására, hogy elvi szinten és gyakorlati eszköztárral miként kezelhetők ezek a kihívások.

3.3. Darknet és illegális kereskedelem

A darknet az internet azon rejtett, anonimizált része, amelyet az erre kifejlesztett kifejezetten speciális böngészőkkel (pl. Tor) lehet elérni, és ahol a felhasználók nehezen visszakövethető módon folytathatnak tevékenységeket vagy éppen kommunikálhatnak.[235] Eredeti célja és rendeltetése szerint ezen internetes felület a privátszféra védelmét, nemzetbiztonságot kívánta szolgálni, azonban az ebben rejlő potenciált a bűnelkövetők kihasználták és ezzel az illegális kereskedelemi tevékenységek

[235] Omar, Zakariye Mohamud; Ibrahim, Jamaluddin: An Overview of Darknet, Rise and Challenges and Its Assumptions. International Journal of Computer Science and Information Technology Research, Vol. 8, Issue 3, 2020, 110–116. Elérhető: https://www.researchgate.net/publication/343282387_An_Overview_of_Darknet_Rise_and_Challenges_and_Its_Assumptions (letöltés dátuma: 2021. 09. 14.)

lefolytatására alkalmas közeggé vált. Ilyen online piactérként működött a nemzetközileg hírhedt Silk Road, amelyet 2011-ben alapítottak és többek között kábítószerek, fegyverek és egyéb tiltott áruk titkos adásvételének adott teret. Az oldalt 2013-ban zárták le az amerikai hatóságok amikor az oldal üzemeltetőjét Ross Ulbrich-ot letartóztatták.[236] 2015-ben Ulbrich-ot életfogytiglani börtönbüntetésre ítélték az Egyesült Államokban.[237] Azóta számtalan hasonló, gyakran rövid életű vagy éppen sokkal nagyobb fekete piacok (lásd: Alphabay) bukkannak fel és tűnnek el a dark weben. Az illegális termékek, szolgáltatások palettája igen széleskörű. A már említett kábítószerek, lőfegyverek, egyéb tiltott áruk, mellett hamis vagy lopott személyes adatok, hamis okmányok, hackerek által ellopott adatbázisok, gyermekpornográf felvételek, de még bérhackelés vagy épp bérgyilkosság is kínálható anonim módon.[238] A fizetés jellemzően kriptovalutákkal (Bitcoin, Monero stb.) történik, amelyek további anonimitást biztosítanak a feleknek. [239] A darkneten folytatott ügyletek vonatkozásában, az ezen a felületen elkövetett és megvalósuló bűncselekményeket a hatályos tényállások szerint kell elbírálni ideértve például a kábítószer-kereskedelemet, a lőfegyverrel vagy lőszerrel visszaélést, a gyermekpornográf tartalmak terjesztését vagy az orgazdaságot stb. Azonban a felület sajátosságai miatt a bűncselekmények felderítése és bizonyítása rendkívül nehéz. A nyomozó hatóságok gyakran fedett módszereket alkalmaznak (pl. beépülnek a piacterek felhasználói közé, álvevőként próbálnak információt szerezni vagy számítógépes csapdákat (ún. honeypotokat) állítanak fel).[240] A nemzetközi illegális és veszélyes piacterek leállítása és mindenkori megszüntetésére a nemzetközi összefogás és együttműködés véleményem szerint elengedhetetlen. Az Europol és az FBI együttműködése révén mára számtalan hatékony akciót tudtak végig vinni a darknet piacainak a felszámolására. E körben

---

[236] Egyesült Államok Igazságügyi Minisztériuma: United States v. Ross Ulbricht – Indictment. United States District Court, Southern District of New York, 2014. február 4. Elérhető: https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf (letöltés dátuma: 2022. 09. 14.)

[237]2025-ben, Donald Trump amerikai elnök feltétel nélküli elnöki kegyelemben részesítette Ross Ulbrichtet.

[238] Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. Büntetőjogi Szemle, 2020/1. szám, 91–107. o. Elérhető: https://ujbtk.hu/wp-content/uploads/lapszam/BJSz_202001_91-107o_SerbakovMarton.pdf (letöltés dátuma: 2021. 05. 14.)

[239] Mezrich, Ben: Az első bitcoinmilliárdosok. Ford. Marczali Tamás. Alexandra Kiadó, Budapest, 2022.

[240]Országgyűlés Hivatala: A sötét web. Képviselői Információs Szolgálat, Infojegyzet 2021/14. Elérhető: https://www.parlament.hu/documents/10181/39233854/Infojegyzet_2021_14_sotet_web.pdf (letöltés dátuma: 2021. 04. 17.)

kiemelhető a 2021-ben lefolytatott nemzetközi művelet, amely az „Operation Dark HunTOR" fedőnevet viselte.[241] Az akció során kilenc ország együttműködése (Ausztrália, Bulgária, Franciaország, Németország, Olaszország, Hollandia, Svájc, Egyesült Királyság és Egyesült Államok), több tucatnyi darkweb-kereskedő letartóztatását és jelentős mennyiségű kábítószer lefoglalását eredményezte. A nemzetközi színtér mellett a hazai színtéren is volt példa a darknettel összefüggésbe került vagy azon zajló bűncselekményre. A Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) Kiberbűnözés Elleni Főosztály Felderítő Osztálya több évvel ezelőtt nyomozást indított egy magyar állampolgár ellen, amelynek során az Amerikai Egyesült Államok Budapesti Nagykövetségének Jogi Attasé Hivatalán keresztül a Szövetségi Nyomozó Irodától (FBI) jelzést kaptak arról, hogy egy általuk azonosított magyar állampolgár a dark web különböző piacain jelentős mennyiségben kábítószert értékesít. Az NNI (az FBI-val szoros együttműködésben) fejlett kiberfelderítési eszközöket alkalmazott a dark web releváns felületeinek monitorozására. A nyomozás során feltárt adatok alapján megállapítást nyert, hogy a férfi 2021 és 2023 között legalább 16 országba irányuló, több kontinensre kiterjedő online drogkereskedelmi tevékenységet folytatott. A megrendelések és szállítások olyan országokat érintettek, mint az Egyesült Államok, Kanada, Ausztrália, Szerbia, Belgium, Svédország, Olaszország, Németország, Franciaország, Anglia, Írország, Spanyolország és más európai államok. A férfi üzleti modellje közvetítői szerepen alapult tehát a beszállítóktól kriptovalutával megvásárolt kábítószert magasabb áron értékesítette tovább a végfelhasználóknak.[242] Az ilyen ügyekben a hagyományos nyomozati munka (pl. csomagok nyomon követése, gyanús pénzügyi tranzakciók figyelése) ötvöződik a kibertechnológiák ismeretével. A nyomozás során lefoglalt informatikai eszközök és adattárolók, valamint az FBI által nyújtott technikai támogatás egyértelműen alátámasztották, hogy a gyanúsított személyesen nem került kapcsolatba a kábítószerekkel, tevékenysége kizárólag a digitális térben zajlott. A forgalmazott szerek között szintetikus drogok, kokain és heroin is szerepelt. Az elkövető három év alatt mintegy 100 millió forint értékű forgalmat bonyolított le, bevételeinek egy

[241]Europol: 150 arrested in dark web drug bust as police seize €26 million. Elérhető: https://www.europol.europa.eu/media-press/newsroom/news/150-arrested-in-dark-web-drug-bust-police-seize-%E2%82%AC26-million (letöltés dátuma: 2025. 05. 14.)

[242] Magyar Rendőrség: Dark weben bonyolította le a drogbizniszt. 2024. június 20. Elérhető: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/dark-weben-bonyolitotta-le-a-drogbizniszt (letöltés dátuma: 2024. 06. 22.)

részéből ingatlant vásárolt.[243] A férfit 2023. június 11-én tartóztatták le vértesszőlősi tartózkodási helyén. Kábítószer-kereskedelem megalapozott gyanúja miatt bűnügyi őrizetbe vették, jelenleg bűnügyi felügyelet alatt áll. Az eljárás keretében vagyonvisszaszerzési intézkedések is folyamatban vannak. A darknet és az azon keresztül folytatott tevékenységek elleni fellépés összetett kihívásokat vet fel mind a bűnüldözés, mind a technológiai megvalósíthatóság, valamint a jogalkotási és szabályozási keretek szempontjából (különös tekintettel a szükségesség és arányosság elvére). Felmerül például a titkosítás szándékos gyengítésének vagy hátsó kapuk (backdoor) beépítésének gondolata, amely ugyan elősegíthetné a hatóságok információhoz jutását, ugyanakkor súlyos adatbiztonsági és alapjogi aggályokat vet fel.[244] A jelenlegi nemzetközi gyakorlat elsősorban az államok közötti együttműködés erősítésére, valamint specializált nyomozócsoportok létrehozására helyezi a hangsúlyt. Emellett a megelőzés is fontos szerepet kap, például a kriptovaluta-tőzsdéken alkalmazott pénzmosás elleni intézkedések révén.

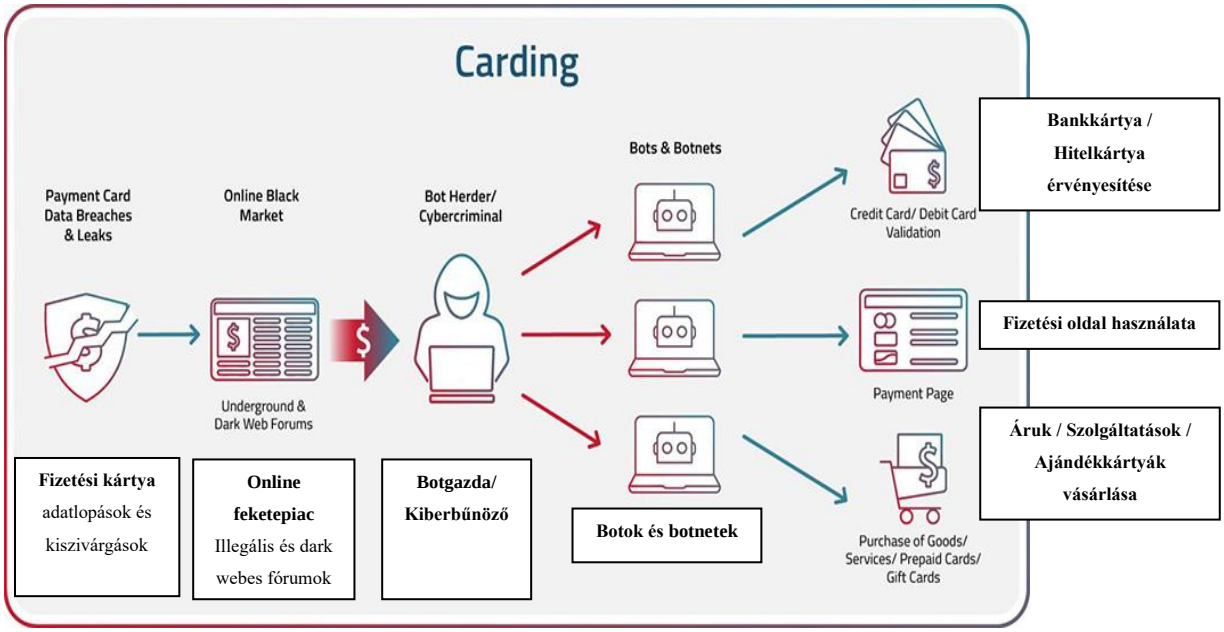
3.4. Digitális pénzügyi bűncselekmények és kriptoeszközök

Az informatika és a digitális technológiák térhódításával a vagyon elleni bűncselekmények is új, kifejezetten a 21. századra jellemző formákat öltöttek. Ide sorolhatjuk mindazon csalásokat, lopásokat, amelyek különféle elektronikus pénzügyi rendszereket céloznak. Gyakori példák között sorolandó az online banki fiókok feltörése, e-bank azonosítók megszerzése a már részletezett adathalász támadás révén, vishing azaz hamis banki hívások, smishing azaz hamis banki emailek, meghamisított banki oldalak, nem banki szolgáltatók nevével történő visszaélés, wangiri azaz visszahívásos telefoncsalás, hamis tranzakciók jóváhagyása, hamis befektetési lehetőségek, hamis online ajánlatok, személyesadat-lopás a közösségi médiában , evil twin phishing azaz hamis WiFi-hálózat létrehozása, rosszindulatú kód telepítése a készülékre, hívószám spoofing azaz hívószám-hamisítás, QR-kódos csalás, angler phishing: hamis szolgáltatói

[243]Police Hungary: Dark weben bonyolította le a drogbizniszt. 2024. június 20. YouTube. Elérhető: https://www.youtube.com/watch?v=GVxHK4D6ezc

[244]Imperva Inc.: Backdoor Shell Attack What is it and how to prevent it? Elérhető: https://www.imperva.com/learn/application-security/backdoor-shell-attack/ (letöltés dátuma: 2022. 05. 14.)

ügyintézés a közösségi médiában illetve az e-kereskedelemben elkövetett visszaélések, mint például a valótlan illetőleg a nem létező termékek hirdetése vagy a fizetés után elérhetetlenné váló webáruházak.[245] Kifejezetten ide tartoznak a bankkártya-adatokkal való visszaélések is. A bűnözők gyakran lopott kártyaadatokat használnak online vásárlásra vagy pénzfelvételre. Az ún. "carding" fórumokon nemzetközi szinten kereskednek az ellopott kártyaszámokkal és a PIN kódokkal. Magyarországon az ilyen jellegű cselekményeket a Btk. 375. §-a az információs rendszer felhasználásával elkövetett csalás vagy a 393. § készpénz-helyettesítő fizetési eszközzel visszaélés alapján rendeli büntetni a törvény.[246][247][248] A kárérték függvényében emelkednek a büntetési tételek, és a szervezett, az üzletszerű elkövetés esetén igen súlyosak is lehetnek a bűntettek (akár 5-10 év szabadságvesztés).



6. ábra

Radware: Carding: What Is Carding Attack and How Does It Work? Elérhető: https://www.radware.com/cyberpedia/bot-management/carding/

[245]Magyar Nemzeti Bank: Az adathalász csalások legjellemzőbb típusai. Elérhető: https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai (letöltés dátuma: 2025. 05. 16.)

[246]Radware: Carding: What Is Carding Attack and How Does It Work? Elérhető: https://www.radware.com/cyberpedia/bot-management/carding/

[247] Btk. 375. §

[248] Btk. 393. §

A kriptovaluták megjelenése a gazdasági bűnelkövetés terén is új fejezetet nyitott. Egyrészt új bűncselekménytípusok jelentek meg, mint például a kriptotőzsdék feltörése, valamint a virtuális vagyon eltulajdonítása, vagy az ún. "crypto-jacking", amikor a támadó észrevétlenül más számítógépét használja kriptopénz bányászására.[249] Másrészt ezek a kriptoeszközök, a Magyar Nemzeti Bank (MNB) meghatározása szerint a „kriptoeszköz" (angolul: crypto-asset) olyan érték vagy jog digitális megtestesítője, amely osztott főkönyvi technológia (distributed ledger technology, DLT) vagy hasonló technológia alkalmazásával elektronikusan átruházható és tárolható, egyúttal olyan eszközként szolgálhatnak, amelyek a bűnözői tevékenységek során alkalmasak lehetnek a pénzmozgások elrejtésére és a pénzmosás megvalósítására.[250] A következő eset kiváló példája annak, hogy a kriptoeszközök piacán működő technológiai rendszerek sebezhetősége milyen súlyos következményekkel járhat a virtuális vagyon biztonságára nézve. Az eset bemutatásának a célja, hogy rávilágítson arra, hogy a technikai hibák és az elégtelen biztonsági protokollok kihasználásával az elkövetők képesek akár százmillió dollár értékű virtuális vagyont eltulajdonítani. A Nomad Bridge célja, hogy különböző blokkláncok között biztosítson eszközátvitelt, viszont a sebezhetőség lehetővé tette azt, hogy a támadók jogosulatlan pénzmozgásokat hajtsanak végre.[251] A Nomad decentralizált pénzügyi (DeFi) protokollból közel 190 millió dollárnyi kriptovalutát loptak el az incidens során, miután egy kritikus biztonsági hibát kihasználva a rendszer védtelenné vált. A hatóságok szerint Alexander Gurevich volt az első, aki a hibát kihasználta, mintegy 2,89 millió dollár értékű tokent emelt el a platformról. A hiba gyorsan ismertté vált, így több mint 88 másik támadó is csatlakozott, és az összesített veszteség elérte a 190 millió dollárt. A támadás után Gurevich kapcsolatba lépett a Nomad technológiai igazgatójával, James Prestwich-csel, és elismerte, hogy ő volt a támadás elsődleges végrehajtója. Elnézést kért a kellemetlenségekért, és visszautalt 162 000 dollárt a cég által létrehozott visszatérítési címre. Emellett 500 000 dolláros „bug bounty"-t követelt, vagyis

---

[249] Eszteri Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és Jog, 2017/1. szám, 25–31. o. Elérhető: https://infojog.hu/eszteri-daniel-egy-bitcoinnal-elkovetett-vagyon-elleni-buncselekmeny-es-az-ahhoz-kapcsolodo-egyes-jogi-kerdesek-20171-68-25-31-o/ (letöltés dátuma: 2021. 05. 15.)

[250] Magyar Nemzeti Bank: Kriptoeszközök és szolgáltatók – kérdések és válaszok. 2024. május 7. Elérhető: https://www.mnb.hu/letoltes/24-05-07-kriptoeszkozok-es-szolgaltatok-kerdesek-valaszok-final.pdf (letöltés dátuma: 2024. 05. 8.)

[251] Google Cloud: Dissecting the Nomad Bridge Hack and Following the Trail of Stolen Funds. Elérhető: https://cloud.google.com/blog/topics/threat-intelligence/dissecting-nomad-bridge-hack (letöltés dátuma: 2022. 11. 29.)

jutalmat a sebezhetőség felfedezéséért. Miután a cég csupán 10%-os jutalékot ajánlott fel, Gurevich megszakította a kapcsolatot. 2025 áprilisában Gurevich visszatért Izraelbe, majd április 29-én hivatalosan megváltoztatta nevét „Alexander Block”-ra, és új útlevelet is kiváltott ezen a néven. Május 1-jén megpróbálta elhagyni az országot egy Oroszországba tartó járattal, de a Ben-Gurion repülőtéren őrizetbe vették az izraeli hatóságok és letartóztatták a 47 éves izraeli–orosz kettős állampolgárt, akit a 2022-ben történt Nomad Bridge hack fő elkövetőjének tartanak. Az Egyesült Államok már korábban hivatalos kiadatási kérelmet nyújtott be, és többek között pénzmosás, számítógépes bűncselekmények, valamint lopott vagyon nemzetközi átvitele miatt emeltek vádat ellene. Az egyes vádpontok akár 20 évig terjedő szabadságvesztéssel is sújthatók. [252] Az ügy nemcsak a DeFi protokollok sebezhetőségére világít rá, hanem arra is, milyen nehézségekkel jár a határokon átnyúló digitális bűnözés felderítése és szankcionálása. Gurevich esete egyúttal példát szolgáltat arra, hogyan próbálják a bűnelkövetők kihasználni a decentralizált technológiák és a nemzetközi jogi különbségek nyújtotta „kiskapukat”, joghézagokat. Mindez alátámasztja, hogy a kriptoeszközök és azokhoz kapcsolódó platformok feltörése, valamint a digitális javak eltulajdonítása a 21. századi vagyon elleni bűnözés egyik legjelentősebb új formájává vált. Ezen túlmenően a támadás lebonyolítása, az elkövető nemzetközi mozgása és a kiadatási eljárás komplexitása is jól mutatja, milyen kihívásokkal szembesülnek a hatóságok a bűncselekmények nyomozása során. A zsarolóvírusok (ransomware) elterjedése tipikusan együtt járt a Bitcoin népszerűségével, hiszen a zsarolók kizárólag kriptopénzben kérik a váltságdíjat, ezzel is biztosítva anonimitásukat. 2023 első felében világszerte robbanásszerűen nőtt a zsarolóvírus-támadások száma, melyek célpontjai között kormányzati szervek, kórházak és nagyvállalatok egyaránt szerepeltek.[253] Nem áll rendelkezésre minden kétséget kizáró bizonyíték, azonban feltételezhető, hogy magyarországi intézmények is érintettek lehettek olyan incidensekben, ahol adatállományokat titkosítottak, majd váltságdíjat követeltek.[254] A disszertáció

[252] FinanceFeeds: Russian-Israeli Accused In $190M Nomad Bridge Hack Faces US Extradition. Elérhető: https://financefeeds.com/russian-israeli-accused-in-190m-nomad-bridge-hack-faces-us-extradition/ (letöltés dátuma: 2025. 05. 15.)

[253] Nemzeti Kibervédelmi Intézet: Zsarolóvírusok – Intézkedések a támadás megelőzéséhez, a kockázatok csökkentéséhez, valamint a sikeres helyreállításhoz. Elérhető: https://nki.gov.hu/wp-content/uploads/2020/07/Zsarol%C3%B3v%C3%ADrusok-1.pdf (letöltés dátuma: 2021. 03. 15.)

[254]Védelmi Beszerzési Ügynökség: Tájékoztatás hacker támadásról. Védelmi Beszerzési Ügynökség. honlapja, 2024. november 14. Elérhető: https://www.vbuzrt.hu/ext-hirek/update?ID_HIR=265748617591249 (letöltés dátuma: 2024. 11. 15.)

készítésének kezdetekor a kriptoeszközök jogi szabályozása még kialakulóban volt, azonban azóta számos előrelépés történt ezen a területen. Az Európai Unió, Európai Parlament és Tanács (EU) 2023/1114 számú rendelete MiCA (Markets in Cryptoassets Regulation) alapján Magyarország elfogadta a kriptoeszközök piacáról szóló 2024. évi VII. törvényt, amely 2024. június 30-án lépett hatályba.[255][256][257]E törvény célja a kriptoeszközök kibocsátására és a kapcsolódó szolgáltatásokra vonatkozó jogi keretek egységesítése az EU területén. A szabályozás gyakorlati alkalmazása fokozatosan történik, és 2025. július 1-jétől minden Magyarországon működő kriptoeszköz-szolgáltatónak kötelező lesz megfelelni a MiCA által előírt követelményeknek, beleértve az engedélyezési eljárások lefolytatását és a szükséges technológiai és biztonsági feltételek biztosítását.[258] Kiemelendő, hogy ezen szabályozási fejlődés főként pénzügyi felügyeleti szempontból jelent előrelépést, nem közvetlenül a büntetőjogi oldalról. A büntetőjogi dogmatika mindazonáltal még keresi a helyét a kriptoeszközöknek. Egy kriptotőzsdéről ellopott virtuális valutát ma lopásként (Btk. 370. §) vagy információs rendszer felhasználásával elkövetett csalásként (Btk. 375. §) bírálják el, a későbbi tranzakciók pedig pénzmosásként jelenhetnek meg a Btk. 399. §-a alapján.[259][260][261] A digitális pénzügyi bűncselekmények elleni harcban kulcsfontosságú a pénzügyi szektor és a hatóságok együttműködése. Magyarországon a Magyar Bankszövetség és az Magyar Nemzeti Bank (MNB) is több programot indított és együttműködésben vesz rész (pl. KiberPajzs), amelyek célja a csalások megelőzése és a lakosság tájékoztatása.

---

[255] Európai Parlament és Tanács: Az (EU) 2023/1114 rendelet a kriptoeszközök piacáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A32023R1114 (letöltés dátuma: 2024. 07. 16.)

[256] 2024. évi VII. törvény a kriptoeszközök piacáról. Magyar Országgyűlés.

[257] Magyar Nemzeti Bank: Kriptoeszköz-szolgáltatók tevékenységének engedélyezése – Útmutató. Elérhető: https://www.mnb.hu/letoltes/casp-tevekenysegi-engedelyezesi-utmutato.pdf (letöltés dátuma: 2025. 05. 16.)

[258] Magyar Nemzeti Bank: Segédlet a belső szabályzat elkészítéséhez a 2025. január elsejét követően a MiCA rendeletben foglaltaknak megfelelő működési engedélyt kérő kriptoeszköz-szolgáltatók részére. Elérhető: https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/szabalyzatok-segedletek/segedlet-a-belso-szabalyzat-elkeszitesehez-a-2025-januar-elsejet-kovetoen-a-mica-rendeletben-foglaltaknak-megfelelo-mukodesi-engedelyt-kero-kriptoeszkoz-szolgaltatok-reszere (letöltés dátuma: 2025. 02. 16.)

[259] Btk. 370. §

[260] Btk. 375. §

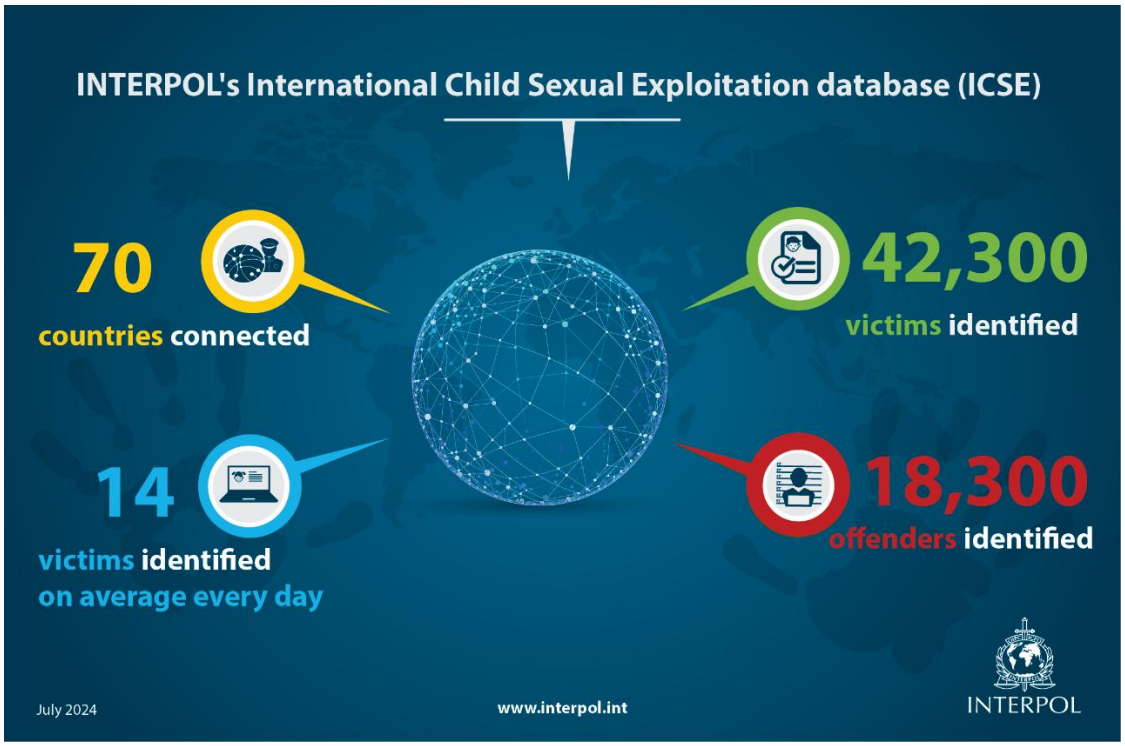
[261] Btk. 399. §

3.5. Szexuális kizsákmányolás és emberkereskedelem az online térben

Az internet elterjedése nemkívánatos módon a szexuális jellegű bűncselekmények új hullámát is magával hozta. Az online térben különösen aggasztó jelenség a gyermekek szexuális kizsákmányolása, amelynek egyik megnyilvánulása a gyermekpornográfia terjesztése.[262] Amíg korábban az ilyen anyagok terjesztése fizikai adathordozókon (mint például videókazetták, DVD-k) zajlott, addig napjainkban már zárt internetes fórumokon, fájlmegosztó hálózatokon vagy épp a weben különösen a darkweb felületeken cserélnek gazdát a felvételek. Magyarország a gyermekpornográfia ellen zéró toleranciát hirdetett. A Btk. 204. § értelmében már a tiltott pornográf felvétel megszerzése vagy tartása is bűntett, amely miatt 1-5 évig terjedő szabadságvesztéssel, valamint a kínál, átad vagy hozzáférhetővé tételével, bűntett miatt 2-8 évig, ugyanakkor készítése és forgalmazása vagy ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tétele esetén ennél is súlyosabban bűntett miatt 5 - 10 évig terjedő szabadságvesztéssel büntetendő.[263] A jelenség globális jellege miatt világszerte azonosítanak gyermekpornográf felvételeken szereplő áldozatokat így e körben kiemelten fontos a nemzetközi együttműködés, hangsúlyozva a gyermekek jogainak védelmét és előmozdítását az online térben.[264] Az elkövetők felderítését és elfogását az Europol illetőleg az Interpol ICSE (International Child Sexual Exploitation) adatbázisa is jelentősen segíti, ugyanis az adatbázis 4,9 millió képet és videót tartalmaz, amelyhez jelenleg 70 ország csatlakozott, és eddig világszerte 42 300 áldozatot, valamint 18 300 elkövetőt sikerült azonosítani, naponta átlagosan 14 áldozat felismerésével. [265] Ez a globális nyomozati és hírszerzési eszköz lehetővé teszi a gyermekek szexuális kizsákmányolásával kapcsolatos képek és videók szakértői elemzését és összehasonlítását. A rendszerhez hitelesített szakértők férhetnek hozzá, amely elősegíti az áldozatok és az elkövetők azonosítását, valamint támogatja az információmegosztást a párhuzamos nyomozások között.

---

[262] Btk. 204. §
[263] Btk. 204. §
[264] ENSZ Gyermekjogi Bizottság: 25. számú általános kommentár (2021) a gyermekek jogairól a digitális környezetben. CRC/C/GC/25. Elérhető: https://documents.un.org/doc/undoc/gen/g21/053/43/pdf/g2105343.pdf?OpenElement (letöltés dátuma: 2022. 05. 18.)
[265] INTERPOL: International Child Sexual Exploitation database. Elérhető: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (letöltés dátuma: 2024. 08. 18.)



7. ábra

INTERPOL: International Child Sexual Exploitation database. Elérhető: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Továbbá e tekintetben külön figyelmet érdemel az Európai Bizottság a gyermekek szexuális bántalmazása elleni hatékonyabb fellépést célzó uniós stratégia, amelyet 2020. július 24-én elfogadtak el. A stratégia átfogó válaszlépéseket fogalmaz meg a gyermekekkel szembeni online és offline szexuális visszaélések fokozódó kockázatára, amely alapot nyújtott a 2022-es Európai Parlament és a Tanács rendeletére a gyermekek szexuális bántalmazásának megelőzésére és leküzdésére vonatkozó szabályok megállapításáról (COM (2022) 209 final) szóló javaslathoz.[266] A javaslatban foglaltak kötelezné az online szolgáltatókat a platformjaikon megjelenő gyermekkel szembeni szexuális visszaélést ábrázoló anyagok automatikus felismerésére és bejelentésére ez által lehetőség adódna arra is, hogy az online szolgáltatók bevonódjanak a gyermekvédelembe, amely a nyomozó hatóságok számára proaktív fellépést tesz lehetővé. Ez alapján

[266] A gyermekek szexuális bántalmazása elleni hatékonyabb küzdelmet célzó uniós stratégia, 2020. július 24., COM(2020) 607, 2. o. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52020DC0607 (letöltés dátuma: 2020. 09. 16.)

kötelesek észlelni és bejelenteni a már ismert gyermekpornográf tartalmakat, felismerni az újonnan felbukkanó tartalmakat és egyúttal kiszűrni a gyermekek csábításra („grooming”) utaló kommunikációt, amely egyértelműen előrelépést jelenthetne 21. századi nyomozás szempontjából. A gyermekek elleni bűncselekmények (különösen a szexuális kizsákmányolás) korunkban már döntően a digitális térben történnek, így azok hatékony megelőzése és a felderítése is csak korszerű, technológiai alapokra épülő eszközökkel valósítható meg, melyet a javaslat is elismer. Mindemellett a rendelet uniós szinten létrehozna egy úgynevezett EU Centre-t, amely koordináló központként funkcionálna és elősegítené az információáramlást, az adatok elemzését és a tagállamok közötti együttműködést. Ez által kiküszöbölhetővé válna a nemzeti szabályozások közötti különbségekből fakadó joghézag mindamellett, hogy a határon túli nyomozások hatékonyságát is növelhetné és azonnali védelmet nyújthatna az áldozatok számára. Jóllehet, hogy a rendeletjavaslat korszerű, digitálisan támogatott, áldozatközpontú és nemzetközileg összehangolt nyomozási gyakorlatot alapozhatna meg, amely világosan tükrözi a 21. századi bűnfelderítési szemléletet, azonban jelentős adatvédelmi aggályt vet fel, különösen az adatvédelem, a titkosított kommunikáció esetében ahol a végpontok közötti titkosítással védett adatokat is ellenőrzés alá vetnék ezáltal több alapvető emberi joggal is ellentétbe kerülhet, különösképp az Európai Unió Alapjogi Charta a magánélethez (Európai Unió Alapjogi Charta, II. Szabadságok, 7. cikk A magán- és családi élet tiszteletben tartása), személyes adatok védelméhez (Európai Unió Alapjogi Charta, II. Szabadságok, 8. cikk A személyes adatok védelme) és a véleménynyilvánítás és a tájékozódás szabadságához való joggal (Európai Unió Alapjogi Charta , II. Szabadságok, 11. cikk A véleménynyilvánítás és a tájékozódás szabadsága) valamint Az Európai Jogok Európai Egyezménye (EJEE) 8. cikk (Az Emberi Jogok Európai Egyezménye 8. cikk A magán- és családi élet tiszteletben tartásához való jog) és 10. cikk (Az Emberi Jogok Európai Egyezménye 10. cikk A véleménynyilvánítás szabadsága) esetében is összeütközésbe kerülhet. [267][268]

[267] Európai Unió: Az Európai Unió Alapjogi Chartája. HL C 326., HU 2012.10.26., 391–407. o. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A12012P%2FTXT (letöltés dátuma: 2022. 05. 19.)

[268] Európa Tanács: Európai Emberi Jogi Egyezmény (European Convention on Human Rights). Elérhető: https://www.echr.coe.int/documents/d/echr/convention_ENG (letöltés dátuma: 2022. 05. 19.)

Kiemelten fontos cél a megelőzés illetőleg a hatékony fellépés az online szexuális visszaélések esetében azonban az ilyen célú intézkedéseknek is meg kell felelniük az uniós jog által garantált alapvető jogoknak, amelyhez kapcsolódóan érdemes áttekinteni a La Quadrature du Net ügyet. A tényállás szerint a La Quadrature du Net nevű francia digitális jogvédő szervezet, valamint több más szervezet és magánszemély azzal a keresettel fordult a francia államhoz, hogy a nemzeti jog alapján előírt, általános és válogatás nélküli adatmegőrzési kötelezettségek sértik az Európai Unió Alapjogi Chartájában biztosított jogokat.[269] Az érintett francia szabályozás kötelezte az elektronikus hírközlési szolgáltatókat arra, hogy nagymennyiségű metaadatot (pl. helymeghatározási, forgalmi adatokat) gyűjtsenek és tároljanak, különös tekintettel a nemzetbiztonságra, bűnmegelőzésre és bűnüldözésre hivatkozva a hatóságok számára. A francia Államtanács az ügy elbírálása során előzetes döntéshozatal iránti kérelmet terjesztett az Európai Unió Bírósága (továbbiakban: EUB) elé, hogy megítélje, hogy az ilyen adatmegőrzési gyakorlat összhangban áll-e az uniós joggal. Az uniós jog nem teszi lehetővé az általános és válogatás nélküli adatmegőrzést, amelyet az EUB 2020. október 6-án meghozott ítéletében is megállapított, továbbá hangsúlyozta, hogy az ilyen intézkedések súlyosan sértik az Európai Unió Alapjogi Charta 7. és 8. cikkében biztosított jogokat. A Bíróság ugyanakkor elismerte, hogy a célzott, időben korlátozott adatmegőrzés megengedhető lehet, ha a közbiztonságra vagy a nemzetbiztonságra konkrét, valós és súlyos fenyegetés áll fenn, az intézkedés arányos és azt független hatóság felügyeli továbbá a megfelelő jogorvoslati lehetőség biztosított. Az ítélet kiemelte, hogy az általános adatmegőrzés sem a bűnmegelőzés, sem a bűnüldözés céljából nem igazolható (kivéve, ha nemzetbiztonsági szükséghelyzet indokolja). A Bíróság szerint, az uniós tagállamoknak kötelességük olyan szabályozást kialakítani, amely biztosítja a személyes adatok védelmét az arányosság és szükségesség elveinek megfelelően. A La Quadrature du Net ügy relevanciája tehát ebben a kontextusban az, hogy a Bíróság az ítéletben világosan kimondta, hogy az általános és válogatás nélküli adatgyűjtés és tartalomellenőrzés összeegyeztethetetlen az uniós joggal, kivéve, ha az a nemzetbiztonság védelmét szolgálja és szigorúan korlátozott, ellenőrzött módon történik.

[269] Európai Unió Bírósága: C-511/18, C-512/18 és C-520/18. sz. egyesített ügyek – La Quadrature du Net és társai kontra Premier ministre és mások, ECLI:EU:C:2020:791, ítélet, 2020. október 6. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A62018CJ0511 (letöltés dátuma:2021.11.16)

Mivel a COM (2022) 209 final javaslat gyermekvédelmi célra hivatkozva vezetne be kvázi általános ellenőrzési mechanizmusokat, a Bíróság értelmezése szerint ez túllépheti az arányosság és a szükségesség határait. Továbbá, ha a javaslat előírja a titkosított kommunikációba való beavatkozást, az egyes értelmezések szerint, de facto, a titkosítás feltörését vagy megkerülését eredményezheti, amelyet az EUB az ítéletében elutasítandónak minősített. Az online tér nemcsak a gyermekek, hanem a felnőttek szexuális kizsákmányolásában, illetve az emberkereskedelemben is szerepet játszik. A bűnszervezetek (különösen a szexuális célú kizsákmányolást végző emberkereskedők) egyre gyakrabban használják a digitális platformokat áldozataik toborzására.[270] Számos esetben a fiatal nőket hamis álláshirdetésekkel, például modell- vagy hoszteszmunkának álcázott ajánlatokkal csábítják külföldre, majd prostitúcióra kényszerítik őket. Az alábbiakban öt különböző esettanulmány keretében mutatjuk be az ilyen típusú bűncselekmények konkrét példáit.

1.eset: El Salvador, 2009 (UNODC Eset 36)

2009 szeptemberében két 15 éves guatemalai lányt toboroztak modellmunkára hivatkozva Guatemalában. Az elkövetők (egy férfi (I. rendű terhelt), egy nő (II. rendű terhelt) és egy másik férfi (III. rendű terhelt)) azt ígérték nekik, hogy heti 1.000 dolláros fizetésért farmernadrágokat fognak bemutatni egy El Salvadorban működő, állítólagosan I. rendű vádlott tulajdonában lévő cégnél. A lányokat hamis okmányokkal vitték át a határon El Salvadorba, ahol egy házban tartották fogva őket. A szabad mozgásukban korlátozott áldozatokat fenyegetésekkel, fizikai és verbális bántalmazással próbálták prostitúcióra kényszeríteni. Az ügyben 2011. január 31-én tartott nyilvános tárgyaláson a San Salvador-i „A" jelű Speciális Büntetőbíróság bűnösnek mondta ki a három terheltet emberkereskedelem bűntettében. Az I. rendű vádlott kilenc év, II. rendű vádlott nyolc év

[270] Európa Tanács: Online és technológia által elősegített emberkereskedelem Összefoglaló és ajánlások. Készült: Dr. Paolo Campana, Cambridge-i Egyetem. Strasbourg, 2022. március. Elérhető: https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c (letöltés dátuma: 2022. 05. 23.)

és egy hónap, míg III. rendű vádlott négy év és hat hónap szabadságvesztést kapott az El Salvador-i Büntető Törvénykönyv 367-B és 367-C szakaszai alapján.[271]

2.eset: Amerikai Egyesült Államok, 2012 (UNODC Eset 71)

Az Egyesült Államok kontra I. rendű vádlott és társai ügyben, amelyet Florida állam középső kerületének szövetségi bírósága tárgyalt, az I. rendű terheltet 2013 márciusában életfogytiglani szabadságvesztésre ítélték. Az ítéletet azt követően hozták meg, hogy az esküdtszék 2012 novemberében bűnösnek mondta ki három kiskorú és két felnőtt személy szexuális kizsákmányolásában, amely során erőszakot, csalást és kényszert alkalmazott, valamint fegyveres bűncselekményeket is elkövetett. A társai, II. rendű vádlott és a III. rendű terhelt, is bűnösnek vallotta magát a bűnszövetségben való részvétel kiskorúak szexuális kizsákmányolása céljából, valamint erőszak, csalás és kényszer alkalmazásával I. rendbeli vádpontban. A II. rendű vádlott esetében 2012 decemberében 46 hónap szabadságvesztés büntetés börtön végrehajtási fokozatát szabták ki, míg a III. rendű vádlott 2013 februárjában a már letöltött szabadságvesztési idő eltelte alapján szabadlábra helyezték. A bíróságon tanúként vallomást tett a II. és III. rendű vádlott, valamint öt áldozat is. Vallomásukból kiderült, hogy az I. rendű vádlott egy „GMB" nevű prostitúciós hálózatot működtetett („GMB" teljes néven: Get Money Bitch). A hálózat különféle módszerekkel, például modellmunkák ígéretével hálózta be áldozatait többek között kiskorúakat illetőleg fiatal felnőtt személyeket, akiket az interneten, többek között a Backpage.com oldalon hirdetett, továbbá az utcára is kényszerítette őket, hogy „vendégeket" szerezzenek. A lányoknak szigorú szabályokat kellett követniük, és minden bevételt az I. rendű terheltnek kellett átadniuk, aki Floridából Észak-Karolinába (Tampa–Charlotte útvonalon) utaztatott prostitúciós célból, több alkalommal is. A terheltek fegyverrel fenyegették és súlyosan bántalmazták azokat, akik megpróbáltak a hálózatból kilépni.[272]

---

[271] UNODC: Collection of Court Case Summaries – Global Report on Trafficking in Persons 2022. 62.o. Elérhető: https://www.unodc.org/documents/data-and-analysis/glotip/2022/Court_Cases_Summaries_GLOTIP_2022_web.pdf (letöltés dátuma: 2023. 05. 21.)

[272] UNODC: Collection of Court Case Summaries – Global Report on Trafficking in Persons 2022. 108.o. Elérhető: https://www.unodc.org/documents/data-and-analysis/glotip/2022/Court_Cases_Summaries_GLOTIP_2022_web.pdf (letöltés dátuma: 2023. 05. 21.)

3.eset: Fehéroroszország (UNODC Eset 230)

2017 február 24-én a minszki Pervomajszkij kerületi bíróság ítéletet hozott két nő (1992-ben született I. rendű vádlott és az 1969-ben született II. rendű terhelt) ügyében, akiket nemzetközi államhatárt átlépő szexuális célú emberkereskedelem miatt vontak felelősségre. A terheltek olyan bűnszervezet tagjai voltak, amely modellalkatú fiatal lányokat toborzott Fehéroroszországból, Ukrajnából, Oroszországból és Kazahsztánból, akiket aztán Törökországba irányítottak prostitúció céljából. Az ügyben közel 100 áldozatról van szó. A bűnszervezet tagjai (köztük ukrán, orosz és török állampolgárok) az interneten keresztül, személyes találkozás nélkül szervezték meg a bűncselekményt. A lányokat az úgynevezett „VKontakte" nevű közösségi oldalon hirdetett „modellmunkák" ígéretével, kiemelkedő fizetéssel és luxusutakat ígérve, bírták rá az áldozatokat a jelentkezésre anélkül, hogy prostitúciót említettek volna. A jelentkezők fürdőruhás, félmeztelen vagy meztelen fotókat küldtek magukról, amelyeket az ukrán „toborzók" a Viber-en (amely egy üzenetküldő alkalmazás) keresztül továbbítottak a minszki bűnszervezet tagjainak jóváhagyásra. A kiválasztott jelentkezőknek ezután felfedték, hogy valójában szexuális szolgáltatások nyújtására szerződtetik őket. Aki visszakozni próbált, azt a korábban elküldött kompromittáló fényképekkel zsarolták. A kiválasztott lányokért fejenként 500 amerikai dollárt fizettek a „toborzóknak" a Western Unionon vagy MoneyGramon keresztül így a terheltek, a lányokat gyakorlatilag eladták anélkül, hogy valaha is személyesen találkoztak volna a bűnszervezet további tagjaival. A minszki terheltek megszerezték az áldozatok útlevél adatait, portré fotóit, valamint egy írásos nyilatkozatot is, amely igazolta, hogy a fényképek valóban őket ábrázolják. A török bűntársaikkal együtt megszervezték a repülőjegyek megvásárlását, a szállások lefoglalását és a „munka" feltételeit. A lányokat isztambuli hotelekben helyezték el egy-két hétre, akik kötelesek voltak megtéríteni a szállás és a repülőjegy költségének felét, valamint jövedelmük 50%-át, amit hetente kétszer kellett befizetniük. Ezenfelül „büntetéseket" is kiszabtak, amelyeket nemfizetés esetén azzal toroltak meg, hogy a lányok nem kaptak klienseket, vagy kizárták őket a szállásról. A fehéroroszországi terheltek távolról, az interneten keresztül irányították a működést, maguk soha nem utaztak Törökországba. A szolgáltatásokat escortügynökségnek álcázott weboldalakon keresztül hirdették, ahol félmeztelen képek, szolgáltatási típusok és árak is szerepeltek (30 perc 400 lírától egy éjszaka 3.000 líráig, azaz körülbelül 140–1050 amerikai dollárig terjedően). A kliensekkel való kommunikáció további azonnali üzenetküldő

alkalmazáson keresztül történt Viberen, WhatsAppon és Telegramon és a lányok a kliensekkel nem tarthattak közvetlen kapcsolatot. A bevételt a terhelteknek kellett átutalniuk Western Unionon keresztül. A bűncselekményből származó teljes bevétel mintegy 360.000 USD volt, amelyből 220.000 dollárt lakásokon tartott házkutatás során, további 140.000 dollárt bankszámlákon foglaltak le. A bíróság a két terheltet bűnösnek találta a kerítés, prostitúció elősegítésére és kihasználására vonatkozó büntető törvénycikk alapján. Az I rendű terheltet három év szabadságvesztésre ítélték, amelyet két évre felfüggesztettek, valamint 3.730 USD-nek megfelelő pénzbírságot is kiszabtak rá. A II rendű terheltet két év hat hónap szabadságvesztésre ítélték, egy évre felfüggesztették, és 2.485 USD-nek megfelelő pénzbírságot kellett fizetnie. Emellett mindkettőjük vagyonát, összesen 399.470 USD értékben, az állam javára elkobozták.

4.eset: Csehország (UNODC Eset 252)

2016 március 3-án a csehországi Hradec Králové Regionális Bíróság négy személyt ítélt el gyermekpornográfiával kapcsolatos bűncselekmények miatt. Az egyikük, az I rendű terhelt, a Cseh Büntető Törvénykönyv 168. § (1) bekezdés a) pontja alapján emberkereskedelem miatt kapott három év szabadságvesztést. A bíróság megállapította, hogy a nő saját hétéves lányát és azonos korú fiát kínálta fel „modell munkára" gyermekpornográf tartalmak előállításához. A másik három terheltet gyermekpornográf anyagok készítésében való közreműködésért ítélték el. Az ítélet szerint mindhárman olyan bűncselekményeket követtek el, amelyek kiskorúak sérelmére irányultak, és céljuk a gyermekek szexuális kizsákmányolásán alapuló tartalmak készítése volt. A bíróság az esetet különösen súlyosnak minősítette mivel a sértettek nagyon fiatal, mindössze hétéves gyermekek voltak, akiket saját anyjuk kínált fel szexuális jellegű tartalmak készítésére. A gyermekek kiszolgáltatottságát az elkövetők tudatosan kihasználták, a cselekmények pedig kizárólag gyermekpornográf tartalmak előállítására irányultak. A három további terheltet (akik nem közvetlen hozzátartozói voltak a gyerekeknek) szintén felelősségre vonták gyermekpornográfia előállítása és terjesztése miatt, büntetésük mértékét azonban az ítélet kivonata nem részletezi. [273]

[273]UNODC: Collection of Court Case Summaries – Global Report on Trafficking in Persons 2022. 376.o. Elérhető: https://www.unodc.org/documents/data-and-analysis/glotip/2022/Court_Cases_Summaries_GLOTIP_2022_web.pdf (letöltés dátuma: 2023. 05. 21.)

5.eset: Magyarország (Ügy száma: B.210/2014/127)

2015-ben a Balassagyarmati Törvényszék jogerősen elítélte azt a vádlotti kört, amely egy szervezett, üzletszerűen működő internetes rendszeren keresztül gyermekpornográf tartalmak terjesztésében vett részt. Az ügy II. rendű vádlottját a Btk. 204. § (1) bekezdés c) pontja alapján gyermekpornográfia bűntettében találta bűnösnek, amiért 2 év 4 hónap szabadságvesztésre, pénzbüntetésre és közügyektől való eltiltásra ítélte. A bizonyítás során megállapítást nyert, hogy a vádlott legalább három, 18 év alatti gyermeket ábrázoló pornográf képet helyezett el egy internetes szerveren, amelyhez a felhasználók emelt díjas SMS-szolgáltatáson keresztül férhettek hozzá. A képek között voltak olyanok is, amelyeken a gyermekeket egyértelműen szexuális tartalmú pózokban ábrázolták, a bíróság szerint „a szexuális vágy felkeltésére egyértelműen alkalmas módon". A rendszer üzleti modellje a hozzáférés fizetősségére épült: a látogatók SMS-ben fizettek, a befolyó összegek egy részét a vádlott és társai különféle cégek és hamis számlák révén legalizálták, ami pénzmosásként is értékelésre került. Az ítélet szerint a vádlottak a gyermekek életkorát és kiszolgáltatottságát kihasználva tudatosan hoztak létre és tettek közzé az interneten olyan képi tartalmakat, amelyek a gyermekek szexuális kizsákmányolását szolgálták. Az internetes platform ezen esetben nem csupán az elkövetés eszközeként, hanem a bűncselekmény üzleti hátttereként is funkcionált, a technológia lehetőségeit maximálisan kihasználva.[274]

Ez az utóbbi eset súlyos példái annak, amikor a gyermekeket éri a szexuális kizsákmányolás, amely nemcsak büntetőjogi szempontból jelent kiemelt súlyosan minősített cselekményt, hanem gyermekvédelmi szempontból is rendkívüli társadalmi veszélyességgel bír. A fenti esettanulmányok és azok magatartásainak büntetőjogi jelentősége illetőleg nemzetközi dimenziói jól szemléltetik, hogy az internet, mint platform, milyen hatékony eszközzé vált a bűncselekmények elkövetésében.

A közösségi média is a jelentős mértékben hozzájárult ahhoz, hogy könnyebben fel tudják venni a kiszemelt áldozatokkal a kapcsolatot az elkövetők.[275] Közkedvelt módszer a bűnelkövetők anonimitásának megőrzésére a hamis profil létrehozás, amely által nehezen

[274]Balassagyarmati Törvényszék: B.210/2014/127. számú ítélet. Balassagyarmat, 2014. 13-BJ-2020-4 Bírósági Határozatok Gyűűjteménye

[275]Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. Büntetőjogi Szemle, 2020/1. szám, 91–107. o. Elérhető: https://ujbtk.hu/wp-content/uploads/lapszam/BJSz_202001_91-107o_SerbakovMarton.pdf (letöltés dátuma: 2021. 05. 14.)

azonosítható módon tudják felvenni a kapcsolatot az áldozataikkal vagy éppen ez által lehetőségük nyílik arra, hogy célzott módon azonosítsák azokat a személyeket, akik a „prostitúcióra alkalmasnak ítélhetők", illetve az emberkereskedelem céljaira különösen kiszolgáltatott helyzetük révén potenciálisan kihasználhatók. Az emberkereskedelem (Btk. 192. §) súlyos bűntettét ilyen esetekben is megállapítják, de a bizonyítás során az online kommunikáció (pl. Facebook, Tiktok vagy Intagram stb. üzenetek, e-mail nyomok) rögzítése és elemzése létfontosságú.[276] Az emberkereskedelemmel kapcsolatos esetek jelentős részében kimutatható volt valamilyen online tevékenység az elkövetők részéről, legyen szó toborzásról, reklámozásról vagy épp az áldozatok kontrollálásáról internetes eszközökkel, amelyet az Európai Parlament „Az emberkereskedelem megelőzéséről és az ellene folytatott küzdelemről című jelentése is alátámasztott."[277] [278] A másik ide sorolható jelenség az ún. bosszúpornó ("revenge porn") valamint a szexuális tartalmakkal való visszaélés, amely során az elkövető a sértett szexuális jellegű, intim képeit vagy videóit az interneten teszi közzé bosszúból vagy zsarolási céllal.[279] A következő esettanulmány precedensértékű és kiemeli, hogy a digitális visszaélések elleni fellépés nem csupán bűnüldözési, hanem alapjogi kötelezettség is.

Az M.Ș.D. kontra Románia ügyben az Emberi Jogok Európai Bírósága (EJEB) 2024. december 3-án kimondta, hogy Románia megsértette az Emberi Jogok Európai Egyezményének 8. cikkét, amely a magánélethez való jogot garantálja. Az ügy középpontjában az állt, hogy a kérelmező egy román nő, volt partnere bosszúból közzétett róla készült intim fényképeket az interneten, köztük prostitúciós hirdetésekben is, megadva a nő nevét, lakcímét és telefonszámát is. Fontos kiemelni, azt, hogy ezeket a képeket a nő korábban a férfival folytatott kapcsolata idején, beleegyezéssel küldte el. Azonban a kapcsolat megszakítása után, a férfi kifejezetten lejáró és zaklató céllal a nyilvánosság részére közzé, többek között a nő családtagjainak is elküldte a képeket. A kérelmező 2016 októberében tett feljelentést, de a román hatóságok, a bukaresti 8-as

[276] Btk. 192. §
[277] Btk. 219. §
[278] Európai Parlament: Jelentés az emberkereskedelem megelőzéséről és az ellene folytatott küzdelemről, valamint az áldozatok védelméről szóló 2011/36/EU irányelv végrehajtásáról. A9-0011/2021. Elérhető: https://www.europarl.europa.eu/doceo/document/A-9-2021-0011_HU.html (letöltés dátuma: 2022. 05. 21.)
[279]Herke Csongor: A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra. In: *Magyar Jog*, 2024/6., 321–332. o. Elérhető: https://szakcikkadatbazis.hu/doc/7075790?ts=2024-06-01#ss80 (letöltés dátuma: 2025. 01. 23.)

számú rendőrkapitányság és az ügyészség éveken át tétlenek maradtak. Bár a nő USB-n bizonyítékokat, köztük hangfelvételeket is benyújtott, a rendőrség csak másfél évvel később hallgatta ki először az elkövetőt, aki beismerte tettét. A hatóságok ezt követően sem kezdeményeztek eljárást és megszüntették a nyomozást, arra hivatkozva, hogy a fényképeket a nő önként adta át, és a férfi fiatal korára, valamint a „kapcsolat szexuális jellegére" tekintettel a társadalomra veszélyességre csekély fokára hivatkoztak. A kérelmezőt, aki a történtek hatására pszichológiai kezelésre szorult, az ügyészség részéről szexista, megalázó hangnemben kezelték. Egyik indoklásuk szerint a nő maga is hozzájárult az eseményekhez, mivel „indecens pózokban" szereplő képeket küldött, és így „túlzottan szexualizált kapcsolatot alakított ki". A nyomozás folyamatosan elhúzódott, az eljárás több ponton elévüléssel zárult, és az ügyet csak akkor vették ismét komolyabban, amikor sajtónyilvánosságot kapott, és tüntetések szerveződtek a nő védelmében. Ennek ellenére az ügyészség végül elutasította a vádemelést, arra hivatkozva, hogy a vádlott már bocsánatot kért és közösségi munkát végzett, az ügy folytatása pedig az áldozat számára is fájdalmas lehetne. Az EJEB ítéletében megállapította, hogy Románia nem biztosított hatékony büntetőjogi védelmet az áldozat számára, továbbá nem folytatott gyors, pártatlan és alapos nyomozást. Kiemelte, hogy a nemi alapú erőszak (akkor is ha online) (így pl.: a bosszúpornó) olyan súlyos jogsérelem, amely büntetőjogi beavatkozást igényel. A Bíróság hangsúlyozta, hogy a hatóságok előítéletes és áldozathibáztató hozzáállása különösen az ügyészség által használt kifejezések nemcsak a konkrét ügyben, hanem általánosságban is visszatartó erővel hathat más áldozatok jogérvényesítésére. Az EJEB 700 euró vagyoni, 7500 euró nem vagyoni kártérítést, valamint 125 euró költségtérítést ítélt meg a kérelmezőnek. Magyarországon nevezetesen erre nincs külön törvényi tényállás, de a gyakorlatban ilyen esetekben alkalmazható a zaklatás (Btk. 227. §) (ha tartós és megfélemlítő jellegű) vagy a becsületsértés (Btk. 227. §) vagy rágalmazás (Btk. 226. §), illetve személyes adattal visszaélés vétsége is. (Btk. 219. §).[280][281][282]Ezen bűncselekmények online vetülete ellen a büntetőjogi fellépés csak több szint egységével valósulhat meg mind szigorú anyagi jogi tényállások, specializált rendőri egységek (pl. magyar rendőrségen belül a Kiberbűnözés

[280] Btk. 227. §
[281] Btk. 226. §
[282] Btk. 219. §

Elleni Főosztály foglalkozik internetes gyermekvédelmi ügyekkel is), valamint nemzetközi összefogás (Interpol, Europol) révén.

3.6. Online bántalmazás és zaklatás

Az online tér a kommunikáció megkönnyítése mellett sajnos teret adott az online bántalmazás különböző formáinak.[283] Ide tartozik a „cyberbullying" (azaz online zaklatás, főként fiatalok között), a „cyberstalking" (azaz elektronikus eszközökkel történő követés), valamint az online térben megvalósuló fenyegetés, zsarolás, rágalmazás.[284] Különösen az információs rendszerekkel való zaklatás vált jelentős problémává, ugyanis az internet nagy hatósugara megkönnyíti a zaklatók számára, hogy azonnali és szinte következmények nélkül célba vegyék az egyéneket.[285] A kibernetikai zaklatás az interneten keresztül tanúsított szándékos, hosszan tartó és káros viselkedésre utal. A zaklató célja lehet az áldozat megalázása, fenyegetése, nevetségessé tétele, kiközösítése, rágalmazása vagy bármely negatív ábrázolása. Az internetes zaklatás gyakori formái közé tartozik a lángolás (flaming), a becsmérlés, a kirekesztés, a megszemélyesítés, az úgynevezett „outing" és a „sexting".[286] Az úgynevezett „flaming" „tüzelő" jellegű és ellenséges üzenetek online közzétételét jelenti, hogy érzelmi reakciót váltson ki az áldozatból, amelynek formái gyakran a komment szekciókban, fórumokon és a közösségi médiaplatformokon látható. A becsmérlés magában foglalja az áldozatról valótlan és káros információk terjesztését, hogy rontsák a hírnevét. Ez magában foglalhatja pletykák, hamisított képek vagy rágalmazó kijelentések közzétételét is. A megszemélyesítés, a hamis profilok létrehozását vagy az áldozat fiókjának feltörését jelenti, oly módon, hogy nem megfelelő, ártó tartalmakat tegyen közzé, rosszindulatú üzeneteket küldjön, vagy

[283]Szabó Barbara: Cyber Harassment and the Law. In: Kovács Bettina – Glázer-Kniesz Adrienn – Tislér Ádám (szerk.), XII. Interdiszciplináris Doktorandusz Konferencia – konferenciakötet = 12th Interdisciplinary Doctoral Conference – Conference Proceedings. Pécs: PTE Doktorandusz Önkormányzat, 2024. pp. 56–69. 14 p. ISBN: 978-963-626-282-2

[284]Szabó Barbara: Mobbing im XXI. Jahrhundert. Bartkó, Róbert (szerk.) Doktori Műhelytanulmányok 2024 - Doctoral Working Papers 2024 Győr, Magyarország : Universitas-Győr Nonprofit Kft. (2024) pp. 451-461. , 11 p. ISSN 2064-1788

[285]Kraut Andrea – Kőhalmi László – Tóth Dávid: Az okostelefonok digitális veszélyei. = Journal of Eastern-European Criminal Law, 7. évf., 36–49. o.

[286]Olweus, Dan: Iskolai zaklatás. = Educatio, 1999/4, 717–739. o. Elérhető: http://www.hier.iif.hu/hu/educatio_reszletes.php?id=26 (letöltés dátuma: 2020. 02.11.)

megtévesztő tevékenységet folytasson.[287] Ezek a cselekmények súlyosan befolyásolhatják az áldozat személyes, szakmai életét és pszichológiai jóllétét.[288] Az „outing" azt a cselekményt jelenti, amikor valaki magánjellegű, érzékeny vagy kínos információit a beleegyezése nélkül nyilvánosságra hozzák. Ez magában foglalhatja a szexuális irányultság, személyes titkok vagy magánbeszélgetések nyilvánosságra hozatalát. A „sexting", amely szexuális tartamú üzenetek vagy képek küldését jelenti, akkor válik internetes zaklatássá, amikor ezeket a magánjellegű üzenetváltásokat hozzájárulás nélkül megosztják, ami megalázáshoz és érzelmi traumához vezet az áldozat számára. A kirekesztés pedig az a szándékos cselekedet, amikor valakit szándékosan kiközösítenek a digitális tereken egy online csoportból, chatből vagy közösségi hálózatból.[289] Különösen az információs rendszerekkel való zaklatás vált jelentős problémává, ugyanis az internet nagy hatósugara megkönnyíti a zaklatók számára, hogy azonnali és szinte következmények nélkül célba vegyék az egyéneket.[290] A magyar büntetőjog a zaklatás (Btk. 222. §) tényállásával fedi le a tartós vagy rendszeres háborgató magatartásokat, beleértve az elektronikus úton történő zaklatást is. A jogszabály szerint, aki abból a célból, hogy mást megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen vagy tartósan háborgatja (technológiai viszonylatban például telefonon, e-mailben, közösségi médián üzenetekkel eláraszt), ha súlyosabb bűncselekmény nem valósul meg, vétséget követ el, minősített esetben (házastársa, volt házastársa, élettársa vagy volt élettársa sérelmére, nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére, hatalmi vagy befolyási helyzetével visszaélve, illetve hivatalos személy sérelmére, hivatali tevékenységével össze nem egyeztethető helyen vagy időben) bűntettet.[291] Míg az előző rész az online zaklatás különböző formáit, azok társadalmi és pszichológiai

[287] Wachs, Sebastian – Wright, Michelle F. – Vazsonyi, Alexander T. – Gámez-Guadix, Manuel: To intervene or not to intervene: Young adults' views on when and how to intervene in online harassment situations. = Journal of Computer-Mediated Communication, 2023, 28(5), zmad027. Elérhető: https://academic.oup.com/jcmc/article/28/5/zmad027/7237464 (letöltés dátuma: 2023. 10. 27.)
[288]Szabó Barbara: Abuses in Virtual Space and Aiding Suicide. Essays of Faculty of Law University of Pécs Yearbook 2021–2022, Pécs: PTE ÁJK, 2023. pp. 183–190. (2023) DOI: 10.15170/studia.2023.01.11 ISSN:2939-8606, ISSN:2061-8824
[289] Wachs, Sebastian – Wright, Michelle F. – Vazsonyi, Alexander T. – Gámez-Guadix, Manuel: To intervene or not to intervene: Young adults' views on when and how to intervene in online harassment situations. = Journal of Computer-Mediated Communication, 2023, 28(5), zmad027. Elérhető: https://academic.oup.com/jcmc/article/28/5/zmad027/7237464 (letöltés dátuma: 2023. 10. 27.)
[290] Kraut Andrea – Kőhalmi László – Tóth Dávid: Az okostelefonok digitális veszélyei. = Journal of Eastern-European Criminal Law, 7. évf., 36–49. o.
[291] Btk. 222. §

hatásait, valamint büntetőjogi minősítését mutatta be, addig a következő eset már egy szorosan kapcsolódó aspektusra irányítja a figyelmet. A kiberzaklatás és a személyes adatokkal való visszaélés ugyanis gyakran ugyanazon magatartásokban fonódik össze ugyanis az elkövető célja mindkét esetben az áldozat megalázása, megszégyenítése vagy társadalmi lejáratása, ám míg a zaklatás a háborgató, ismétlődő magatartás büntetőjogi kategóriájába tartozik, addig az intim vagy magánjellegű adatok engedély nélküli közzététele már az információs önrendelkezés sérelmének körébe esik. E kettősséget jól érzékelteti a következő, jogerős bírósági ítélet.

A Bhar.I.677/2021/6. számú ítélet az információs önrendelkezéshez való jog büntetőjogi védelmének egyik meghatározó példája, különös tekintettel a személyes adattal való visszaélésre vonatkozó Btk. 219. § (1) bekezdés a) pontjának értelmezésére. A döntés középpontjában a vádlott (Terhelt I.) azon cselekménye állt, amely során korábbi élettársáról intim fényképfelvételt osztott meg a Facebook közösségi platformon, ahol a sértett felismerhető módon látható volt. A vádlott célja a posztolással a sértett társadalmi lejáratása, erkölcsi megítélésének rombolása volt, különösen a kis lélekszámú (kb. 3000 fős) Nyírbélteki közösségen belül. Az elsőfokú bíróság a vádlottat bűnösnek mondta ki többek között személyes adattal visszaélés vétségében, és 2 év felfüggesztett szabadságvesztést szabott ki. A másodfokú bíróság azonban felmentette a vádlottat e vádpont alól, mivel nem látta bizonyítottnak a „jelentős érdeksérelem” tényállási elemének megvalósulását. Ezzel szemben az ügyészség kifejtette, hogy a közzététel súlyosan sértette a sértett magánszféráját, és objektív, jól körülhatárolható személyes hátrányt eredményezett. A Debreceni Ítélőtábla ezzel az állásponttal egyetértett, és megállapította, hogy a közösségi médiában történő intimkép-megosztás (különösen a helyi társadalmi kontextusban) kétségkívül jelentős érdeksérelmet okozott. Az Ítélőtábla hangsúlyozta, hogy az ilyen típusú képek jogellenes közzététele (még ha nem is kifejezetten a szexuális tartalomra utalnak) alappal minősülhet személyes adattal visszaélésnek, és nem csupán erkölcsi, hanem büntetőjogi relevanciával is bír. Az ítélőtábla a másodfokú ítéletet ebben a részben megváltoztatta, és kimondta a vádlott bűnösségét a személyes adattal visszaélés vétségében. A szabadságvesztést 1 év 8 hónapra súlyosította, azonban annak végrehajtását figyelemmel a vádlott teljes körű

beismerésére, az eljárás gyorsítására, valamint az életvitel rendeződésére 5 év próbaidőre felfüggesztette.[292]

A digitális térben elkövetett jogsértések kiemelten indokolják a büntetőjogi beavatkozást, amelynek álláspontját a Debreceni Ítélőtábla döntése is egyértelműen tükrözi és megerősíti, hogy az információs önrendelkezés sérthetetlensége a büntetőjog védelme alatt áll. Ezen szabályozási struktúrába szervesen illeszkedik a Budapesti IV. és XV. Kerületi Bíróság B.737/2020/39. számú ügye is, amely alkalmas arra, hogy bemutassa miként valósulhat meg a zaklatás és annak minősített esete a különféle digitális technológiák közvetítésével.[293] Az elkövetési magatartások döntő többsége elektronikus eszközökön keresztül történt, a bűncselekmények elkövetésének módja pedig világosan mutatja, hogy a digitális és a fizikai tér közötti elhatárolás fokozatosan elmosódik, ami új típusú társadalmi és jogi kihívásokat eredményez. Az ügyben elítélt férfi azután kezdte digitálisan zaklatni volt élettársát, hogy kapcsolatuk végleg megszakadt. A sértettet folyamatosan kereste telefonhívásokkal, SMS- és Viber-üzenetekkel, melyek száma és tartalma az idő múlásával egyre sértőbbé és fenyegetőbbé vált, ezen túlmenően magánnyomozót fogadott, akivel a sértettet és új partnerét figyeltette, ez által alkalma adódott arra, hogy az új partner részére a sértettről intim fényképeket mutathasson és küldjön, amelyek között szexuális aktust rögzítő felvétel is volt. A bíróság szerint ezek a felvételek a sértett szexuális életére vonatkozó különleges személyes adatoknak minősülnek, amelyek kezelése csak az érintett kifejezett hozzájárulásával történhetne meg. A vádlott ezzel a Btk. 219. § (1) és (3) bekezdése szerinti különleges személyes adattal visszaélés vétségét is elkövette, mivel az adatokat nemcsak jogellenesen, hanem jelentős érdeksérelmet okozva kezelte ugyanis a sértett új párkapcsolata a vádlott digitális beavatkozásának következményeként megszakadt, és a nő kénytelen volt lakóhelyet változtatni. A zaklatás minősített esete a vádlott volt élettársa sérelmére valósult meg. A vádlott magatartása a sértett mindennapi életvitelébe önkényesen beavatkozva, tartósan háborgatva tette, nemcsak az online térben tanúsított folyamatos jelenlétével és a megalázó tartalmak küldésével, hanem a valós élet színtérre, személyes környezetére is kiterjedő, megfélemlítő jellegű megfigyeléseivel. A digitális térben megvalósuló bántalmazás tehát nem állt meg a technikai eszközök dimenziójában, hanem közvetlen

[292] Debreceni Ítélőtábla: Bhar.677/2021/6. számú ítélet.
[293] Budapesti IV. és XV. Kerületi Bíróság: 10.B.737/2020/39. számú ítélet.

hatással volt a sértett magánéletére, lakhatására, munkavállalási lehetőségeire, valamint társas kapcsolataira is. Az ítélet egyik lényeges megállapítása, hogy a digitálisan közvetített zaklatás és adatkezelési visszaélés büntetőjogi szankció alá esik, és a bíróság e cselekményeket nem csupán erkölcsi, hanem büntetőjogi értelemben is súlyos megítélés alá vonja. Az ítélet indokolásából világosan kiolvasható a társadalmi üzenet közvetítésének szándéka, miszerint a technológia nem legitimálhatja az emberi méltóság megsértését, sem a magánélet megsértésén alapuló önkényes beavatkozást. Ez az ügy tehát jól illusztrálja, hogy a modern bántalmazás egyik fő tere az online világ, amelynél az új bűnelkövetési mintázatokra (hasonlóan a Bhar.I.677/2021/6. ügyhöz) a bírósági ítélkezési gyakorlat válasza az, hogy a digitális technológia nemcsak eszköz, hanem potenciális fegyver is lehet, amely sérti az áldozat autonómiáját, emberi méltóságát és információs önrendelkezését.

A 2025. január 1-jétől hatályos Btk. 332/A. § bevezetésével a jogalkotó az „internetes agresszió" külön tényállásban való nevesítésével kívánta kezelni az online térben terjedő, beazonosítható személyekkel szembeni erőszakos cselekményekre buzdító, gyűlöletkeltő tartalmak problémáját.[294] Ezen szabályozás különösen releváns a közösségi média és a digitális kommunikáció térnyerésének tekintetében, ahol a sértegetés, fenyegetés és a megalázás egyre gyakrabban zajlik nyilvánosan, tömegek előtt. E körben különös figyelmet érdemel a zaklatás online formája, azaz a cyberbullying, amelyet a magyar Büntető Törvénykönyv külön nem nevesít, azonban a joggyakorlat rendszerint zaklatásként (Btk. 222. §) vagy becsületsértésként (Btk. 227. §) kezeli, és számos esetben a problémák kezelésére gyermekvédelmi eljárás keretében kerül sor. A 332/A. § alkalmazása ugyan nem általános még az ilyen esetekre, de bizonyos súlyosabb megnyilvánulások (például, ha az elkövető halált vagy különös kegyetlenséggel elkövetett erőszakot kíván vagy erre irányuló szándékot fejez ki az áldozatnak) már kimeríthetik a vétség tényállását, különösen, ha az online tartalom vagy a poszt széles körben, nagy nyilvánosság előtt elektronikus hírközlő hálózat útján történt. A törvény ugyanakkor kivételt biztosít azon esetekre, amikor az adott közlés ismeretterjesztő, tudományos, oktatási vagy művészeti célt szolgál, és nem alkalmas félelemkeltésre (332/A. § (2) bek.). Ez különösen fontos a szólásszabadság védelme szempontjából, amely az online térben is alapvető érték, ám nem élvez abszolút védelmet, különösen, ha

[294] Btk. 332/A. §

mások emberi méltóságát vagy testi-lelki épségét veszélyezteti. A közösségi média platformon elérhető tartalmak és azok algoritmikus terjesztése e büntetőjogi tényállás kontextusában különös figyelmet érdemel mindamellett, nem elhanyagolható e tekintetben az UNICEF azon felmérése, amelyből kiderült, hogy a gyermekek egyharmadát zaklatták már online platformokon, és világszerte a gyermekek 72%-a tapasztalta már a cyberbullying valamilyen formáját.[295] A „Blackout Challenge" néven ismert online kihívás keretében felhasználókat buzdítanak arra, hogy a légzésük korlátozásával (például övvel, zsinórral vagy más tárggyal) eszméletvesztést idézzenek elő. Ezen kihívás az internetes tartalmak „virálissá" válásának mechanizmusát kihasználva terjed, gyakran éppen a TikTok „For You Page" algoritmusán keresztül felajánlott tartalomként az arra legfogékonyabb és legkiszolgáltatottabb fiatal felhasználók számára. Az Egyesült Államokban több tragikus eset is napvilágra került, amelyek során gyermekek vesztették életüket a kihívás végrehajtása közben. A szülők több esetben jogi lépéseket tettek, így például 2022-ben Christina Arlington Smith, Heriberto Arroyo és Christal Arroyo keresetet nyújtottak be a TikTok Inc. és a ByteDance Inc. ellen, mivel a 8 éves Lalani Walton és a 9 éves Arriani Jaileen Arroyo az alkalmazás hatására végre hajtották az életveszélyes kihívást, amely halálukat okozta.[296] Hasonló esetek történtek Pennsylvaniában, Oklahomában és Olaszországban is ahol a sértettek életkora 10 és 12 év között mozgott, és minden esetben az alkalmazás algoritmusa tölthetett be szerepet abban, hogy a gyermekek szembesültek a halálos kimenetelű tartalmakkal.[297][298][299] Ezek az esetek nem csupán a platform üzemeltetőinek felelősségét veti fel, hanem jogértelmezési kérdéseket is generálnak a 332/A. § vonatkozásában.[300] A

---

[295] UNICEF: UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying., 2019. szeptember 4. Elérhető: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying (letöltés dátuma: 2020. 05. 27.)

[296] Anderson kontra TikTok Inc., 2:22-cv-01930 (E.D. Pa. 2022. május 12.). Elérhető: https://www.smbb.com/wp-content/uploads/2022/05/Timestamped-Complaint-1.pdf (letöltés dátuma: 2022. 05. 27.)

[297] Leggo.it: Antonella, morta per una sfida su TikTok: la cintura era del padre. 2021. január 23. Elérhető: https://www.leggo.it/italia/cronache/antonella_morta_tik_tok_cintura_padre_palermo_oggi_23_gennaio_2021-5719864.html (letöltés dátuma: 2021. 02. 27.)

[298] The Sun: Boy, 12, dies after TikTok 'Blackout Challenge' left him on life support. 2021. április 14. Elérhető: https://www.the-sun.com/news/2701439/boy-dies-tiktok-blackout-challenge-joshua-haileyesus/ (letöltés dátuma: 2021. 05. 27.)

[299] USA Today: 12-year-old Oklahoma boy found dead after participating in TikTok 'blackout challenge,' reports say. 2021. július 22. Elérhető: https://eu.usatoday.com/story/news/nation/2021/07/22/oklahoma-12-year-old-tiktok-blackout-challenge-social-media/8065926002/ (letöltés dátuma: 2021. 07. 27.)

[300] Btk. 332/A. §

kérdés az, hogy amennyiben egy nyilvánosan közzétett tartalom (mint például egy „kihívásvideó”) olyan pszichológiai nyomást gyakorol a nézőkre, amely az önkárosítás vagy halál kockázatával jár, és a közlés alkalmas a súlyos félelem kiváltására, úgy e tényállás alkalmazható-e a tartalom előállítóival vagy terjesztőivel szemben. További nehézséget jelent, hogy az alkalmazás algoritmusa sem semleges közvetítő. Több esetben a tartalom ajánlás mögött üzleti és viselkedéselemzési logika húzódik meg, amely nem célzottan vagy éppen célzottan ajánlhat fokozottan veszélyes videókat, így felvethető a közvetett szándék vagy legalábbis a gondatlan közrehatás. A fentiek tükrében indokolt megvizsgálni, hogy a gyermekek védelme érdekében milyen módon alkalmazható a büntetőjog preventív és represszív funkciója, különös tekintettel a 332/A. § és a digitális platformok működésének viszonyára. Az online tér nem lehet szabályozatlan helye az olyan tartalmaknak, amelyek fiatalok ezreit sodorják veszélybe, akár közvetett módon, algoritmikus révén.[301] Prevenciós oldalon kiemelten fontos a társadalmi tudatosság növelése. A fiatalok számára elengedhetetlen, hogy tisztában legyenek az online magatartásuk jogi és erkölcsi következményeivel, ahogy az is, hogy tudják, hová fordulhatnak segítségért, ha zaklatás áldozatává válnak. A Nemzeti Média- és Hírközlési Hatóság (NMHH) által 2018-ban létrehozott Internet Hotline szolgáltatás egyike ezeknek az eszközöknek, amely lehetőséget biztosít többek között gyűlöletkeltő vagy zaklató tartalmak bejelentésére, és közreműködik azok eltávolításában ezen túlmenően az állam jogi eszközökkel kötelezheti a szolgáltatót arra, hogy folyamatosan szűrje az internetes tartalmakat, valamint tegye elérhetetlenné a jogsértő tartalmakat, illetve távolítsa el azokat.[302] Mivel az online bántalmazási magatartások jellemzően nemzetközi platformokon (például a már említett TikTok, a Facebook vagy az Instagram felületein) zajlik, különösen fontos annak feltérképezése, hogy más országok jogalkotói és igazságszolgáltatási szervei miként kezelik ezt a problémát. Ennek megfelelően az alábbiakban Németország és az Egyesült Államok példáin keresztül mutatom be az online zaklatás elleni jogi fellépés különböző modelljeit.[303] Németországban specifikus

[301] Macenaite, Milda: Protecting children's privacy online: a critical look to four European self-regulatory initiatives. = European Journal of Law and Technology, 2016, 7(2). Elérhető: https://ejlt.org/index.php/ejlt/article/view/473 (letöltés dátuma: 2021. 05. 27.)
[302] Parti Katalin – Marin, Luisa: *Foltvarrással az on-line illegális tartalom ellen: a tartalomblokkolás, a közvetítő szolgáltató felelőssége és az értesítési-levételi eljárás*. Infokommunikáció és Jog, 2012/49, 58–65. o.
[303]Szabó Barbara: Digitális Zaklatás Elleni Küzdelem: Németország és az USA Megközelítései. Gaál Gyula – Hautzinger Zoltán (szerk.): A rendészet tudománya és gyakorlata. Tudományos Közlemények XXVI.

törvények foglalkoznak az online zaklatás különböző formáival. Az online zaklatás áldozatai több csatornán keresztül is bejelenthetik az eseteket. A legtöbb német tartomány (Bundesländer) „online rendőrségi állomásokat" (Onlinewache) működtet, ahol az emberek digitálisan nyújthatják be panaszukat. Ez a folyamat egy űrlap kitöltését foglalja magában, amelyben részletezik az esetet, majd a panaszt áttekintik és a megfelelő osztályhoz rendelik további intézkedésekre.[304] Ezek az online platformok könnyen hozzáférhető módot biztosítanak az áldozatok számára, hogy segítséget kérjenek anélkül, hogy személyesen kellene meglátogatniuk egy rendőrkapitányságot, amely gyors reagálási lehetőséget is biztosít, hiszen az áldozatok nem kötődnek nyilvántartási időhöz vagy földrajzi korláthoz ezáltal könnyedén bejelenthetik az eseteket. A Bundeskriminalamt (BKA) és speciális kiberbűnözési egységei nyomoznak az online zaklatási ügyekben. Ezek az egységek fejlett technológiákat használnak és nemzetközi együttműködésben dolgoznak, hogy felkutassák az elkövetőket. A BKA CC részlege például a kiberbűnözés nyomozásával, az információk gyűjtésével és elemzésével, valamint az elkövetők büntetőeljárás alá vonásával foglalkozik.[305]A bűncselekményekkel szembeni hatékony fellépés érdekében Németországban együttműködnek a bűnüldöző szervek, más szektorok, és szervezetek. Ezen együttműködés egyik kiváló példáját a Német Kompetencia Központ a Kiberbűnözés Ellen (G4C) statuálja. Ezen kívül kötelezik a közösségi hálózatokat, hogy mihamarabb eltávolításra kerüljenek az illegális tartalmak, a biztonságosabb online környezet kialakítása végett.[306]A német büntető törvénykönyv, közismert nevén Strafgesetzbuch (StGB), számos rendelkezést tartalmaz, amelyek az online zaklatás különböző formáival foglalkoznak. A zaklatás (§ 238 StGB) rendelkezése kriminalizálja a tartós zaklatást mind fizikai, mind digitális úton.[307] Ez magában foglalja a távközlési eszközökön keresztüli tartós kommunikációt és a személyes adatokkal való visszaélést, így elismerve a digitális korszakban ilyen módon történő zaklatás elleni fellépés iránti szükségességét. A súlyos bűncselekmény elkövetésével való fenyegetés (§ 241 StGB) rendelkezése az online fenyegetésekre is vonatkozik, büntetőjogi szankciókat

---

Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja – Magyar Rendészettudományi Társaság, (2024.) 137-141o. ISSN:1589-1674

304 Bundesministerium der Justiz. Onlinewache. Bundesministerium der Justiz. Németország, n.d. https://justizonline.gv.at/jop/web/formulare/gruppe/6/17 (letöltési idő: 2024.05.05.)

305 Bundeskriminalamt. Cybercrime. Bundeskriminalamt. Németország, n.d. https://www.bka.de (letöltési idő: 2024.05.05.)

306 Bundeskriminalamt. Cybercrime. Bundeskriminalamt. Németország, n.d. https://www.bka.de (letöltési idő: 2024.05.05.)

307 Büntető Törvénykönyv. Strafgesetzbuch (StGB). Stalking (§ 238 StGB). Németország

kiszabva azok számára, akik komoly bűncselekmények elkövetésével fenyegetnek.[308] Az online fenyegetések ezen rendelkezés alá vonása tükrözi a digitális megfélemlítés növekvő aggodalmát. A rágalmazás és becsületsértés (§ 185, 186, 187 StGB) rendelkezései átfogó keretet biztosítanak az online rágalmazás és becsületsértés kezelésére.[309][310][311]Ezek védelmet nyújtanak az egyének számára a hamis állításokkal szemben, amelyek ronthatják hírnevüket, így kiterjesztve a védelmet azokra a digitális platformokra, ahol ezek a bűncselekmények egyre inkább előfordulnak. A magánélet megsértése (§ 201 StGB) rendelkezése az engedély nélküli beszélgetésrögzítést és terjesztést kezeli.[312]Az ilyen cselekmények kriminalizálásával védelmet nyújt az egyének magánéletének mind fizikai, mind a digitális interakciók során. Az intim magánélet megsértése fényképezéssel (§ 201a StGB) rendelkezése specifikusan célozza az intim fényképek engedély nélküli készítését és terjesztését.[313] Kiemeli ezen cselekmények büntethetőségét, különösen a digitális terjesztés vonatkozásában. A Netzwerkdurchsetzungsgesetz (NetzDG), vagyis a közösségi hálózatokban történő törvény végrehajtásának javításáról szóló törvény előírja, a közösségi média platformok számára azt, hogy meghatározott időn belül távolítsák el az illegális tartalmakat.[314] Ez különösen a gyűlöletbeszéd, a rágalmazás és a fenyegetések kezelésére vonatkozik, amelyek el nem távolítása esetén jelentős bírságokat szabnak ki azokra a platformokra, amelyek nem tartják be az előírásokat. A NetzDG értelmében a közösségi hálózatoknak megfelelőségi kötelezettségeik vannak az illegális tartalmak eltávolítására. Ezek a platformok kötelesek a felhasználói adatokat is kiadni a bűnüldöző hatóságoknak kérésre, megkönnyítve az elkövetők azonosítását és büntetőeljárás alá vonását. A NetzDG célja ezzel az, hogy lehetőséget biztosítson az áldozatok számára, hogy minél gyorsabban és hatékonyabban tudjanak fellépni az atrocitások ellen. Az általános adatvédelmi rendelet (GDPR), bár elsősorban az adatvédelemre összpontosít, olyan rendelkezéseket is tartalmaz, amelyek segíthetnek az online zaklatás kezelésében.[315] A GDPR úgynevezett

308 Büntető Törvénykönyv. Strafgesetzbuch (StGB). Androhung der Begehung eines Verbrechens (§ 241 StGB). Németország
309 Büntető Törvénykönyv. Strafgesetzbuch (StGB). Beleidigung. (§ 185 StGB). Németország
310 Büntető Törvénykönyv. Strafgesetzbuch (StGB). Üble Nachrede. (§ 186 StGB). Németország
311 Büntető Törvénykönyv Strafgesetzbuch (StGB). Verleumdung. (§ 187 StGB). Németország
312 Büntető Törvénykönyv Strafgesetzbuch (StGB). Verletzung der Vertraulichkeit des Wortes (§ 201 StGB). Németország
313 Büntető Törvénykönyv Strafgesetzbuch (StGB). Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB). Németország
314 Hálózatok Végrehajtási Törvénye. Netzwerkdurchsetzungsgesetz (NetzDG). Németország
315 Általános Adatvédelmi Rendelet. Datenschutz-Grundverordnung (GDPR). Európai Unió, 2016.

"elfeledtetési joga" lehetővé teszi az egyének számára, hogy kérjék személyes adataik eltávolítását az online platformokról. Ez a mechanizmus különösen fontos az online zaklatás eseteiben, ahol a személyes adatokkal való visszaélés súlyos következményekkel járhat az áldozatok számára. A kiberbűnözés határokon átívelő bűncselekmények esetében pedig a Bundeskriminalamt (BKA), a rendőri erők speciális kiberbűnözési egységei mindamellett, hogy végrehajtják ezeket a törvényeket, vizsgálatokat folytatnak, bizonyítékokat gyűjtenek és együttműködnek az Europol és Interpol nemzetközi szervezetekkel.[316] Az online zaklatás kérdésére adott esetleges választ Amerikában különböző perspektívákból vizsgálták, kiemelve a kihívásokat, a bűnüldözés és más érintettek részéről. Lawler és Boxall (2023) szerint az áldozatok nagyobb valószínűséggel jelentenek személyes szexuális erőszakot a rendőrségnek, mint online zaklatást, és a marginalizált csoportok jelentős akadályokkal és negatív tapasztalatokkal szembesülnek, amikor bejelentést tesznek, ami befolyásolja későbbi segítségkérési hajlandóságukat.[317]Broll (2014) azt vizsgálta, hogy a különböző entitások, beleértve a szülőket, oktatókat, hogyan reagálnak a cyberbullyingra, megjegyezve az együttműködő, mégis gyakran széttagolt megközelítést.[318]Weinstein (2019) hangsúlyozta a kiberzaklatás kezelésének jogi összetettségét az Első Alkotmánykiegészítés védelme miatt, azzal érvelve, hogy a jelenlegi módszerek gyakran nem megfelelően kezelik az online megnyilvánulások sajátosságait.[319]Deo (2016) és Griffiths (1999) is kiemelte az úgynevezett „kiberstalking" fejlődő természetét, hangsúlyozva a bűnüldözés szükségességét az új jelenséghez való felkészültséget.[320] Az Egyesült Államok különféle jogi kereteket alkalmaz az online zaklatás kezelésére, mind hagyományos, mind digitális specifikus törvények felhasználásával. Az állami törvények az Egyesült Államokban az online zaklatás kezelésére jelentős eltéréseket mutatnak a terjedelem és a végrehajtási mechanizmusok tekintetében. Vines (2015) rámutatott arra, hogy az állami „anti-

316 Bundeskriminalamt. Cybercrime. Bundeskriminalamt. Németország, n.d. https://www.bka.de (letöltési idő: 2024.05.05.)
317 Siobhan Lawler – Hayley Boxall: Reporting of Dating App Facilitated Sexual Violence to the Police. Victim-Survivor Experiences and Outcomes. Australian Institute of Criminology. Canberra, 2023. 1-18. o.
318 Ryan Broll: Policing Cyber Bullying. How Parents, Educators, and Law Enforcement Respond to Digital Harassment. Electronic Thesis and Dissertation Repository. 2014. 1-350. o.
319 James Weinstein: Cyber Harassment and Free Speech. Drawing the Line Online. In Free Speech in the Digital Age, In.: Susan J. Brison – Katharine Gelber (szerk.): Oxford University Press. Oxford, UK, 2019. 123-145. o.
320 Mona E. Deo: The Evolution of Cyberstalking. A Comparative Analysis of Legal Responses. International Journal of Cyber Criminology. Centre for Cyber Victim Counselling. India, 2016. 147-161. o.

bullying" törvények jelentősen különböznek meghatározásaikban és protokolljaikban mivel egyes államok részletes iránymutatásokat nyújtanak az elektronikus kommunikáció és a zaklatás tekintetében, míg mások az egyes iskolai körzetekre bízzák a szabályzatok kidolgozását, ami következetlen megközelítéseket eredményez az államok különböző részein.[321] Ezen elgondolást Postal (2015) is hangsúlyozta, miként az állami törvények különböznek a diákok beszédjogai és azok fegyelmi intézkedéseinek tekintetében ugyanis, egyes államok széles hatáskört biztosítanak az oktatási intézményeknek az intézményen kívüli kiberbullying kezelésére, míg máshol csak az intézmény területén belül történő incidenseket szabályozzák, ami bonyolítja a végrehajtást, főként, ha az az interneten történik.[322] McNeal (2020) az állami és helyi törvények fejlődését vagy éppen nem fejlődésében absztrahálja a diverz felfogást, miként az egyes államok elmaradnak a technológiai fejlődéssel, ezért elmaradnak a technológiával lépést tartó jogszabályok elfogadásában egyaránt.[323]Fukuchi (2011) azzal érvelt, hogy a kiberzaklatási törvények teheráthelyező eszközként növelhetik az ügyészségi eljárások hatékonyságát és méltányosságát.[324]Goodno (2007) a kiberstalking különböző természetét és hiányosságait vizsgálta az offline zaklatáshoz képest, és javasolta, hogy mind az állami, mind a szövetségi törvényeket frissíteni kell, hogy hatékonyan kezeljék az online zaklatás sajátosságait, mivel a meglévő törvények gyakran nem megfelelően kezelik a kiberstalking egyedi aspektusait, ami következetlen ügyészi eljárást és védelmet eredményez az áldozatok számára.[325] Chang (2020) több kihívást is azonosított, amelyekkel a bűnüldözés szembesül a nyomozás során, beleértve az ismerethiányt, a joghatósági korlátokat és az elkövetők adatainak megszerzésének nehézségeit, amelyek államonként különböznek és befolyásolják a végrehajtás hatékonyságát.[326] Smith (2009)

---

321 James Vines: Inconsistencies across the States. An Examination of Anti-Bullying Laws. In Legal Frontiers in Education. Complex Law Issues for Leaders, Policymakers and Policy Implementers. In.: Advances in Educational Administration. Vol. 24. Emerald Group Publishing Limited. Leeds, 2015. 1-18. o.

322Andrew Postal: Where the Schoolhouse Gates End. An Analysis of State Cyberbullying Laws. Georgetown University. 2015. 1-82. o.

323 Ramona Sue McNeal – Susan M. Kunkle – Lisa Dotterweich Bryan: State-Level Cyberbullying Policy. Variations in Containing a Digital Problem. In: Gordon A. Crews (szerk.): Critical Examinations of School Violence and Disturbance in K-12 Education. IGI Global. Hershey, PA, 2016. 62-82. o.

324 Aimee Fukuchi: A Balance of Convenience. Burden-Shifting Devices in Criminal Cyberharassment Law. Boston College Law Review. USA, 52 (1). 2011. 289. o.

325 Naomi Harlin Goodno: Cyberstalking, a New Crime. Evaluating the Effectiveness of Current State and Federal Laws. Missouri Law Review. University of Missouri, Missouri, 2007. 127-188. o.

326 Wei-Jung Chang: Cyberstalking and Law Enforcement. Procedia Computer Science Vol. 176. 2020. 1188-1194. o.

az internetes zaklatás meghatározásának és büntetőjogi eljárásának tágabb kihívásait tárgyalta, hangsúlyozva a világos és átfogó törvények szükségességét, hogy célzottan irányítsák a végrehajtási erőfeszítéseket a különböző államokban.[327]Az online zaklatás kezelésének megközelítései Németországban és az Egyesült Államokban eltérőek, de mindkét ország jogi rendszere különös figyelmet fordít ezen probléma kezelésére.[328] Németországban a szabályozási keretrendszer részletesen foglalkozik az online zaklatás különböző formáival és a német büntető törvénykönyv, a Strafgesetzbuch (StGB), egyértelműen kriminalizálja. Az online zaklatásra adott választ a kiberbűnözési egységek, mint a Bundeskriminalamt (BKA) koordinálják, amelyek nemzetközi együttműködésben is részt vesznek a nemzetközi szervezetekkel egyaránt. Továbbá, a hálózatok végrehajtásáról szóló törvény (NetzDG) előírja a közösségi hálózatok számára, hogy gyorsan eltávolítsák az illegális tartalmakat, és biztosítja, hogy a felhasználói adatokat a bűnüldöző hatóságok rendelkezésére bocsássák. Az Egyesült Államokban az online zaklatás kezelése szövetségi és állami szinten egyaránt történik, de a jogi keretek eltérnek az egyes államok között. Míg egyes államok részletes iránymutatásokat dolgoztak ki az elektronikus kommunikáció és zaklatás kezelésére, mások az egyes iskolai körzetekre bízzák a szabályzatok kidolgozását. Az Első Alkotmánykiegészítés szabad véleménynyilvánításra vonatkozó védelme bonyolítja az online megnyilvánulások szabályozását, ezért a jelenlegi módszerek gyakran nem megfelelően kezelik az online beszéd árnyalatait.[329] Az online zaklatás elleni küzdelem hatékonysága érdekében az Egyesült Államok különféle jogi kereteket alkalmaz, beleértve a hagyományos és digitális specifikus törvényeket is, amelyek alapvető jogi keretet biztosítanak, de az állami törvények jelentős eltéréseket mutatnak terjedelmük és végrehajtási mechanizmusaik tekintetében. Mindkét esetben azonban megállapítható, hogy ezen jogi keretek és a speciális szabályozások bevezetése hozzájárulhat az online zaklatás hatékonyabb kezeléséhez.

327Alison M. Smith: Protection of Children Online. Federal and State Laws Addressing Cyberstalking, Cyberharassment, and Cyberbullying. Congressional Research Service. Washington D.C., USA, 2008. 1-40. o.

[328] Szabó Barbara: *Rechtliche Maßnahmen und Schutzstrategien gegen Online-Belästigung*. KRE-DIT: A KRE-DOK Online Tudományos Folyóirat, VII/2. szám (2024) (megjelenés 2025). 121 ISSN 2630-8711

329Kathleen Conn: From Student Armbands to Cyberbullying. The First Amendment in Public Schools. Legal Frontiers in Education: Complex Law Issues for Leaders, Policymakers and Policy Implementers In : Advances in Educational Administration, Vol. 24. Emerald Group Publishing Limited. Leeds, 2015. 35-58. o.

4. Bűncselekmények a virtuális valóságban és azok nyomozása

Az informatika fejlődése illetőleg a metaverzum jelenség megteremtette a valósághű virtuális világokat, ahol a felhasználók avatárokon keresztül élnek, játszanak és akár dolgoznak. A virtuális valóság (VR) és a metaverzum már nem pusztán játék ugyanis bennük saját gazdaságok, társas kapcsolatok és digitális vagyontárgyak is megjelennek. A tudományos diskurzus ugyanakkor egyre inkább felismeri, hogy ezek a digitális terek nem tekinthetők jogmentes zónának, mivel a felhasználói magatartást nemcsak a társadalmi normák, hanem a jogi szabályozás is alakítja.[330] A különböző platformokon történő bűncselekmények, az avatárok sérelmére elkövetett zaklatásoktól a digitális vagyon ellopásáig valós és gyakran jelentős károkat is okozhatnak. A jelenségre a jogi szabályozás nehezen ad koherens választ, mivel a virtuális javak tulajdonjogának meghatározása, a személyes adatok védelme és az illetékesség kérdése egyaránt számos bizonytalanságot vet fel.[331] Jelen fejezet célja a VR–térben elkövetett bűncselekmények fogalmának, típusainak és nyomozásának áttekintése. A vizsgálat kiterjed a magyar és nemzetközi szakirodalomra, a releváns jogszabályokra, valamint a bűnüldöző szervek gyakorlatára. Külön figyelmet fordítunk arra, hogy a játékokban vásárolt virtuális javakért valódi pénzzel fizetnek, ugyanakkor a játékon belüli lopások esetében a tett „virtuálisan" valósul meg, ezen dichotómia jelentős kihívást jelent a jogalkalmazók számára. Egyúttal arra is rámutat ezen fejezet, hogy amennyiben egy online metaverzum-jellegű játékkörnyezetbe például a felhasználó virtuális vagyonát a 10. szint elérése után tulajdonítják el, a nyomozás lefolytatásához a hatóság képviselője kénytelen lehet a játék teljes folyamatát végig játszani. Ilyen esetben a munkáltatónak el kell fogadnia, hogy a nyomozó munkaidőben a játékfelületen tevékenykedik, mivel csak így férhet hozzá a releváns digitális bizonyítékokhoz. Már létrejöttek olyan speciális rendőri és igazságügyi

[330]Qin, Hua Xuan – Wang, Yuyang – Hui, Pan: Identity, crimes, and law enforcement in the Metaverse. = Humanities and Social Sciences Communications 2025/12, Art. 194. https://www.nature.com/articles/s41599-024-04266-w (letöltés dátuma: 2025. szeptember 13.)
[331]Falus Orsolya – Józwiak Piotr – Kővári Attila: „Gólyakalifa" a 21. században Joghézag és analógia a virtuális valóság jogában. = *Jogelméleti Szemle* 2022/2, 20–33. o.

egységek, amelyek kifejezetten a metaverzumon belül elkövetett bűncselekmények vizsgálatára szakosodtak.[332]

4.1. Fogalmi alapok (VR, metaverzum, virtuális vagyontárgyak, „metabűn")

Virtuális valóság

Virtuális valóság alatt olyan háromdimenziós, számítógéppel generált környezetet értünk, amelybe a felhasználók speciális eszközök (például VR-szemüveg, fejhallgató vagy mozgásérzékelő kontrollerek stb.) segítségével lépnek be, és amelyben a valósághoz hasonló módon képesek mozogni és cselekedni. A metaverzum ezen technológia tágabb értelmezését adja, mivel több, egymással összekapcsolt digitális világot foglal magában, ahol a felhasználók az adott avatárokon keresztül vesznek részt a társas interakciókban, a vásárlásban, a munkavégzésben és a szórakozásban.[333] A metaverzum térnyerésével a társadalmi és gazdasági folyamatok egyre nagyobb része áttevődik a digitális dimenzióba, ennek következtében pedig a bűnözés is természetes módon követi a felhasználók tevékenységét ugyanebben a közegben.[334]

Virtuális vagyontárgyak

A virtuális vagyontárgyak olyan digitális eszközök vagy jogok, mint a játékbeli tárgyak, földparcellák, avatár-kiegészítők vagy nem helyettesíthető tokenek (NFT), amelyeket a felhasználók a platform szabályai szerint szerezhetnek meg, birtokolhatnak és értékesíthetnek. Ezen javak megszerzése gyakran valós pénzbeli befizetéshez kötődik, ugyanakkor az online fizetős játékok piacán nem létezik egységes árképzés, így előfordul,

---

[332]Fraud Conference News: How the IRS investigates and combats Metaverse fraud. https://www.fraudconferencenews.com/home/2024/6/26/how-the-irs-investigates-and-combats-metaverse-fraudnbspnbsp (letöltés dátuma: 2024. október 13.)

[333]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)

[334]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)

hogy egyes elemekért bármilyen összeget kérnek. Ez a sajátosság pénzmosási kockázatokat is felvet, mivel a bűncselekményből származó források a virtuális gazdaságon keresztül legális bevételként jelenhetnek meg.[335]

Virtuális bűncselekmény (metabűn)

A szakirodalom szerint virtuális bűncselekményről (angolul: metacrime) akkor beszélhetünk, ha a cselekmény elkövetése, okozati folyamata és következményei a virtuális térben vagy a kibertérben valósulnak meg.[336] Ezen kategória magában foglalja az olyan személy elleni bűncselekményeket, mint például a zaklatás vagy a szexuális erőszak vagy a vagyon elleni deliktumokat, példaként említhető a csalás, lopás és zsarolás valamint a pénzügyi bűncselekményeket, ideértve a pénzmosást és a költségvetési csalást is. A „metacrime" (azaz metabűn) kifejezést az Interpol alkalmazza a metaverzumon belül elkövetett különféle jogsértések összefoglalására.[337] A szervezet hangsúlyozza, hogy ezek a cselekmények, bár virtuális környezetben zajlanak, valós gazdasági illetőleg pszichológiai károkat okozhatnak.[338]

4.2. A VR-térben előforduló bűncselekmény-típusok

4.2.1. Személy elleni bűncselekmények

A metaverzum platformjai számos esetben váltak szexuális zaklatás vagy erőszak virtuális színterévé, amely az avatárok elleni nem kívánt abúzusokban mind fizikai

[335]Kovács Zoltán (szerk.): A kibernyomozói munka büntetőjogi sajátosságai. Budapest, Nemzeti Közszolgálati Egyetem, 2023. 115 o. DOI:10.37372/mrttvpt.2023.4 (letöltés dátuma: 2024. október 14.)
[336]Eszteri Dániel: A számítógépes bűnözés legújabb tendenciái, különös tekintettel az online közösségi tereken elkövetett visszaélésekre. = *Magyar Rendészet* 2013/1, 55–69. o.
[337]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)
[338]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)

interakciókban vagy verbális bántalmazásban nyilvánul meg.[339] A Humanities and Social Sciences Communications egyik tanulmánya rámutat arra, hogy az ilyen tapasztalatok a felhasználók számára valós pszichológiai traumát idézhetnek elő.[340] A Major Cities Chiefs Association (MCCA) jelentése szerint a metaverzumban elkövetett szexuális zaklatások már a béta, azaz tesztidőszakban is súlyos problémát jelentettek, ezért a szervezet különösen fontosnak tartja a kriminális magatartásformák korai felismerését és a platformüzemeltetők felelősségének megerősítését.[341] Az Egyesült Királyságban jelenleg is folyik egy olyan ügy vizsgálata, amelyben egy 16 év alatti lányt felnőtt férfiakból álló csoport támadott meg a metaverzum egyik immerzív videojátékában. A beszámolók szerint az eset súlyos pszichés megterhelést okozott, amely a fizikai támadásokkal járó traumához hasonlítható.[342] Az ügy jól rávilágít arra, hogy az valósághű jelenlétélményt nyújtó technológia a digitális élményeket rendkívül valóságossá teszi, ezért az ilyen környezetben átélt erőszak vagy sokk pszichológiai hatása korántsem elhanyagolható. Nem ez az első hasonló bejelentés a metaverzumban történt szexuális visszaélésekről. 2021 novemberében, a Meta Horizon Worlds bétaidőszakában egy felhasználó virtuális tapogatásról számolt be. 2021 decemberében egy kutató avatárját több férfi avatár körülvette, zaklatta, lefényképezte, majd virtuális nemi erőszakot követett el rajta.[343] 2022 májusában a SumOfUs szervezet egyik munkatársa arról számolt be, hogy egy privát szobában, egy parti közben avatárját egy másik felhasználó megerőszakolta, miközben több jelenlévő végignézte az eseményt.[344] Ezek az esetek komoly kérdéseket vetnek fel a felhasználók védelmét, valamint a virtuális valóság

---

[339]Szabó Barbara: Online Crime of Violence on Virtual Platforms. In: IRC 2022 – XVI. International Research Conference Proceedings. Pulau Bali, Indonézia: WASET, 2022. pp. 122–125. 4 p.IRC 2022 XVI. International Research Conference Proceedings open science index 16 2022 October 20-21, 2022 Bali Indonesia International Scholarly and Scientific research & innovation ISSN:1307-6892

[340]Qin, Hua Xuan – Wang, Yuyang – Hui, Pan: Identity, crimes, and law enforcement in the Metaverse. = *Humanities and Social Sciences Communications (Nature Portfolio)* 2025/12(1), Art. 194**.** https://doi.org/10.1057/s41599-024-04266-w,https://www.nature.com/articles/s41599-024-04266-w (letöltés dátuma: 2025. március 17.)

[341]Major Cities Chiefs Association (MCCA): *Metaverse Reference Guide.* https://majorcitieschiefs.com/wp-content/uploads/2025/06/MCCA_Metaverse-Reference-Guide_Oct-2024.pdf (letöltés dátuma: 2024. december 16.)

[342]Major Cities Chiefs Association (MCCA): *Metaverse Reference Guide.* https://majorcitieschiefs.com/wp-content/uploads/2025/06/MCCA_Metaverse-Reference-Guide_Oct-2024.pdf (letöltés dátuma: 2024. december 16.)

[343]Major Cities Chiefs Association (MCCA): *Metaverse Reference Guide.* https://majorcitieschiefs.com/wp-content/uploads/2025/06/MCCA_Metaverse-Reference-Guide_Oct-2024.pdf (letöltés dátuma: 2024. december 16.)

[344]Major Cities Chiefs Association (MCCA): *Metaverse Reference Guide.* https://majorcitieschiefs.com/wp-content/uploads/2025/06/MCCA_Metaverse-Reference-Guide_Oct-2024.pdf (letöltés dátuma: 2024. december 16.)

platformjain alkalmazott biztonsági illetőleg moderálási megoldások hatékonyságát illetően. Az online játékok és közösségi platformok olyan közeget teremtenek, ahol felnőttek hamis identitás mögé rejtőzve férkőzhetnek a gyermekek bizalmába, és ezt követően könnyen manipulálhatják a védelemre szoruló korosztály tagjait, akik erről mit sem sejtve kerülhetnek kiszolgáltatott, akár online visszaéléseknek való kiszolgáltatottságot eredményező vagy zaklatásnak minősülő szituációkba.

4.2.2. Vagyon elleni bűncselekmények

A virtuális javak elleni támadások lényege, hogy az elkövető a digitális tárgy feletti rendelkezést a jogos használótól erőszakkal, fenyegetéssel vagy megtévesztéssel elvonja, illetve a hozzáférést megszünteti vagy eltéríti. A külföldi gyakorlat már jelezte, hogy a játékbeli vagy metaverzum-beli erőforrások és hozzáférések büntetőjogi védelme levezethető, amely szerint a digitális tárgyak értékkel bírnak, megszerezhetők és átruházhatók, míg a fiókok és avatarok feletti kontroll elvesztése a hozzáférési jogosultság sérelmét jelenti.[345][346]Ebből következően a metaverzumban tipikusan két dogmatikai tengely mentén jelennek meg a deliktumok. A vagyon elleni jogsértések (a birtok/rendelkezés elvonása, lopás), valamint az információs rendszerekhez való jogellenes hozzáférést, adatmódosítást vagy szolgáltatás-megbénítást megvalósító cselekmények. A metaidentitás (avatar, profil, hitelesítési adatok) elleni támadások sajátos kockázati csoportot alkotnak. A fiókátvételek, az avatar-klónozás és a deepfake-alapú megszemélyesítés, személyiséglopás-jellegű sérelmeket és tovagyűrűző vagyoni károkat eredményezhetnek.[347]A bűnözői motivációk között a virtuális tárgyak és kriptoeszközök „átjárhatósága” is kiemelt szerepet játszik. A platformok nem transzparens árazása és a tokenizált javak másodpiaca megkönnyíti a jogtalan eredet leplezését (pénzmosási kockázat), az adóelkerülést, valamint a piramis- és „rug pull”

[345]Wildman, N. – McDonnell, N.: The puzzle of virtual theft. = *Analysis* 2020/80(3), 493–499. o. http://eprints.gla.ac.uk/210232/ (letöltés dátuma: 2025. szeptember 16.)
[346]Gibbons, Llewellyn J.: Law and the Emotive Avatar. = *Vanderbilt Journal of Entertainment & Technology Law* 2009/11(4), 899–920. o.
[347]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)

jellegű sémák lefuttatását. [348][349] A virtuális gazdaságban elterjedt „scam" magatartások (hamis ígéretek, manipulált tranzakciók, színlelt projektek) jogilag jellemzően beilleszthetők a meglévő kategóriákba.[350] A hazai dogmatika szempontjából ilyennek minősülhet többek között a csalás, sikkasztás, hűtlen kezelés, vagyon elleni bűncselekmények illetve (a technikai végrehajtástól függően) az információs rendszer felhasználásával elkövetett bűncselekmények köre.[351] A gyakorlat nem igényel feltétlenül új, kizárólag digitális környezetre szabott tényállásokat inkább a meglévő normák következetes, értékalapú alkalmazása, valamint a bizonyítási eszköztár (log- és metaadat-rögzítés, platform-auditnyomok, blokklánc-elemzés) megerősítése szükséges.

4.2.3. Jogszabályi háttér és kihívások

Az előző alfejezetekben feltártuk, hogyan működik a VR és a metaverzum, milyen társas-gazdasági folyamatok települnek át ezekbe a terekbe, és milyen személy-, illetve vagyon elleni cselekménytípusok jelennek meg bennük. Ezen a ponton indokolt az elméleti-kriminológiai leírásról a magyar büntetőjog normatív talajára átlépni. Azt kell megvizsgálnunk, hogy a hatályos Btk. tényállásai miként fogják meg a virtuális térben zajló magatartásokat, és hol mutatkoznak dogmatikai bizonytalanságok. A cél kettős: egyrészt iránymutatást adni a minősítéshez a jelenlegi jog keretei között (de lege lata), másrészt jelezni a lehetséges jogfejlesztési irányokat (de lege ferenda). A magyar Büntető Törvénykönyv alapján lopást követ el az, aki idegen dolgot mástól azért vesz el, hogy azt jogtalanul eltulajdonítsa.[352]A tényállás „dolog" fogalma klasszikusan kézzelfogható, fizikai tárgyat jelent. A virtuális tárgyak sajátossága, hogy nem rendelkeznek fizikai formával, ami bizonyos esetekben kérdéseket vethet fel a hagyományos lopás

[348]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)
[349]Kovács Zoltán (szerk.): A kibernyomozói munka büntetőjogi sajátosságai. Budapest, Nemzeti Közszolgálati Egyetem, 2023. 115 o. DOI:10.37372/mrttvpt.2023.4 (letöltés dátuma: 2024. október 14.)
[350]Eszteri Dániel: A számítógépes bűnözés legújabb tendenciái, különös tekintettel az online közösségi tereken elkövetett visszaélésekre. = *Magyar Rendészet* 2013/1, 55–69. o.
[351]Eszteri Dániel: A számítógépes bűnözés legújabb tendenciái, különös tekintettel az online közösségi tereken elkövetett visszaélésekre. = *Magyar Rendészet* 2013/1, 55–69. o.
[352]Btk. 370. §

tényállásának alkalmazhatóságával kapcsolatban. A jogirodalomban ezen kérdés megítélése jelenleg is különböző álláspontokat tükröz, és a magyar jogban egyelőre nem körvonalazódtak egyértelmű irányelvek a virtuális vagyontárgyak jogi megítélésére vonatkozóan. Egyes álláspontok szerint analógia útján alkalmazható a lopás tényállása, ha a virtuális javak mögött pénzben kifejezhető érték áll.[353] A kriptoeszközökről szóló büntetőjogi tanulmány ugyancsak rámutat arra, hogy az új típusú digitális javakra a hagyományos bűncselekményi kategóriák csak korlátozottan alkalmazhatók, ezért indokolt lenne a fogalmi keretek korszerűsítése és új jogi kategóriák bevezetése.[354]

A VR-környezetben gyakran előforduló támadások (például felhasználói fiókok feltörése, jogosulatlan belépés vagy hozzáférési jogosultságok megkerülése, valamint szolgáltatások megbénítása), nem önálló „virtuális bűncselekmények", hanem a Büntető Törvénykönyvben (Btk.) már régóta szabályozott informatikai bűncselekmények digitális megnyilvánulásai**.** A Btk. 423. § az információs rendszer vagy adat megsértése bűncselekményt írja le, amely „Aki az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép információs rendszerbe, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bennmarad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. Aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza (például túlterheléses DDoS támadással), vagy az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztatja, törli vagy hozzáférhetetlenné teszi, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. A büntetés egy évtől öt évig terjed, ha a cselekmény jelentős számú információs rendszert érint vagy jelentős érdeksérelmet okoz, és két évtől nyolc évig terjed, ha a bűncselekményt közérdekű üzem ellen követik el."[355] Amennyiben a támadó titokban adatokat szerez, így például felhasználói jelszavakat vagy pénzügyi információkat gyűjt be, a Btk. 422. § szerinti tiltott adatszerzés is megvalósulhat.[356]Ha a VR-játékok vagy metaverzum platformok felületén a támadó úgy manipulálja a rendszer

[353]Falus Orsolya – Józwiak Piotr – Kővári Attila: „Gólyakalifa" a 21. században Joghézag és analógia a virtuális valóság jogában. = *Jogelméleti Szemle* 2022/2, 20–33. o.
[354]Bácskai Máté: A kriptovaluták büntetőjogi értelmezése a pénzmosás és a lopás tükrében. = Ügyészek Lapja 2024/1–2 (XXXIV. évfolyam), 103–111. o. https://ugyeszeklapja.hu/?p=4534 (letöltés dátuma: 2025. szeptember 16.)
[355]Btk. 423. §
[356]Btk. 422. §

adatkezelését, hogy ezzel vagyoni hátrányt okoz (például csalárd tranzakciókkal virtuális javakat von el) a Btk. 375. § szerinti információs rendszer felhasználásával elkövetett csalás is alkalmazható. Ez a szakasz bünteti azt, aki jogtalan haszonszerzés céljából adatot bevisz, módosít, töröl vagy tesz hozzáférhetetlenné, és ezzel kárt okoz.[357] A gyakorlati nyomozás szempontjából ez gyors digitális nyombiztosítást, logfájlok és metaadatok rögzítését, valamint platformokkal és hatóságokkal folytatott nemzetközi együttműködést igényel. [358]

4.2.4. Nemzetközi jog és ajánlások

A fenti, de lege lata kerethez jól illeszkednek a nemzetközi példák, amelyek azt mutatják, hogy a virtuális javak és metaverzum-események valós joghatásokkal járnak. A holland Runescape-ítéletben a Legfelsőbb Bíróság 2012-ben helybenhagyta annak megállapítását, hogy a játékbeli amulett és maszk „dolognak" minősül, időráfordítással megszerezhető, értéket hordoz, ezért a fizikai kényszerrel kikényszerített átadás lopás (konkrétan erőszakos vagyon elleni bűncselekmény) megállapítására alkalmas volt. A döntés a virtuális javak büntetőjogi védhetőségét példaszerűen elismerte, és azóta is kiindulópont a „dolog" fogalmának digitális kiterjesztéséhez.[359] A japán MapleStory-ügy ezzel párhuzamosan arra világít rá, hogy a platform-hozzáférések és elektronikus adatok manipulálása önmagában is büntetőjogi relevanciát hordoz. A 2008-as esetben a hatóságok jogosulatlan hozzáféréssel és adathamisítással gyanúsították azt a nőt, aki volt partnere avatarját törölte. A sajtóban is megjelent, hogy az ügy akár öt év szabadságvesztéssel is járhatott. Bár nem ismert a jogerős ítéleti anyag, az eljárás ténye és minősítése megerősíti, hogy az elektronikus adatok a büntetőjog által védett jogi tárgyak körébe eshetnek.[360] A nemzetközi bűnüldöző szervek állásfoglalásai a hazai minősítési dilemmákhoz további támpontot adnak. Az INTERPOL metaverzumról szóló fehér könyve a „metacrime" kategóriáit többek között NFT-csalásokra, identitáslopásra,

---

[357]Btk. 375. §
[358]Kovács Zoltán (szerk.): A kibernyomozói munka büntetőjogi sajátosságai. Budapest, Nemzeti Közszolgálati Egyetem, 2023. 115 o. DOI:10.37372/mrttvpt.2023.4 (letöltés dátuma: 2024. október 14.)
[359]Wildman, N. – McDonnell, N.: The puzzle of virtual theft. = Analysis 2020/80(3), 493–499. o. http://eprints.gla.ac.uk/210232/ (letöltés dátuma: 2025. szeptember 16.)
[360]Gibbons, Llewellyn J.: Law and the Emotive Avatar. = *Vanderbilt Journal of Entertainment & Technology Law* 2009/11(4), 899–920. o.

3D-modellek eltulajdonítására és virtuális szexuális zaklatásra bontja, és kiemeli a joghatóság, bizonyítékgyűjtés és avatár-anonimitás gyakorlati nehézségeit.[361] Az EUROPOL 2022/2023-as anyagai pedig arra figyelmeztetnek, hogy a metaverzum új terepe a megszemélyesítésnek (avatar-klónozás, impersonation), és a rendvédelemnek ehhez új módszertant kell fejlesztenie.[362] Az USA-ban a pénzügyi-adózási vetületre jó példa, hogy az Egyesült Államok Adóhatósága (IRS: Criminal Investigation) és a Egyesült Államok Igazságügyi Minisztériuma (DOJ: Department of Justice) több NFT „rug pull"-ügyben lépett fel, („rug pull": azaz olyan kriptós csalás, amikor a projekt készítői hirtelen kivonják a pénzt és eltűnnek) a Frosties-ügyben 2022 márciusában vádat emeltek egy hozzávetőlegesen 1–1,1 millió USD körüli károsszegű csalási sémával összefüggésben, az eljárásokban pedig blokklánc-elemzés, webes adatgyűjtés és informátorhálózat is megjelent, ami a metaverzumhoz kapcsolódó pénzmozgások nyomozhatóságát illusztrálja.[363] Végül a Dán Rendőrség Online Járőrszolgálatának (Politiets Online Patrulje) gyakorlata megmutatja, hogy a prevenció és a felderítés a platformokra belépve lehet igazán hatékony. A 2022-ben létrehozott egység stream- és játékkörnyezetekben (Twitch, TikTok, Counter-Strike, Minecraft) épít bizalmat, célzottan kezeli a fiatalokat érő zaklatást és csalásokat és hivatalos beszámolók szerint már a működés első szakaszában is jelentős számú ügyet nyitottak. A megközelítés lényege, hogy a rendőrség a célcsoport nyelvén és terepén kommunikál, amely legitimálhatja a „játékkal végzett munkát" bizonyos szolgálati feladatok keretében.[364] Ezen példák a magyar, de lege lata kerethez visszacsatolva két gyakorlati tanulságot erősítenek. Egyrészt a lopás tágabb értelmezése a „dolog" digitális megfelelőire is kiterjeszthető lehet (de esetről esetre, óvatos dogmatikával), miközben az információs

---

[361]Interpol: Metaverse: a law enforcement perspective use cases, crime, forensics, investigation, and governance. White Paper. 3-26. p. January 2024. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf (letöltés dátuma: 2025. január 13.)

[362]Europol: Policing in the Metaverse What Law Enforcement Needs to Know. An Observatory Report from the Europol Innovation Lab. Luxembourg, Publications Office of the European Union, 2022. PDF | ISBN 978-92-95220-47-8 | ISSN 2600-5182 | DOI: 10.2813/81062 | QL-AS-22-002-EN-N, 4–28. o. https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf (letöltés dátuma: 2024. október 16.)

[363]United States Attorney's Office, Southern District of New York: Two Defendants Charged in Non-Fungible Token (NFT) Fraud and Money Laundering Scheme. https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0 (letöltés dátuma: 2024. október 16.)

[364]Politi (Dánia): *Politiets Online Patrulje*. https://politi.dk/om-politiet/virksomheden/politiets-online-patrulje (letöltés dátuma: 2024. október 16.)

rendszer elleni bűncselekmények (jogosulatlan belépés, rendszer-/adat-manipuláció, szolgáltatás-megbénítás) a metaverzumos ügyek elsődleges „kapaszkodói”. A bizonyításban a nemzetközi gyakorlat szerint a kulcs a log- és metaadat-rögzítés, a blokklánc-nyomkövetés, a platform-auditnyomok és a határokon átnyúló együttműködés.

4.3. Bűnüldözési kihívások és módszerek a VR-környezetben

A virtuális bűncselekmények felderítésekor a hatóságoknak egyszerre kell kezelniük az azonosítás és joghatóság problémáit, a gyorsan „illékony” digitális nyomok rögzítésének kihívását, valamint a platform-ökoszisztémák sajátosságait.[365] Mivel az elkövetők gyakran álneveket használnak, és a kapcsolódó szerverek több joghatóság alatt helyezkednek el, a valódi személyazonosság feltárása tipikusan szolgáltatói adatszolgáltatáson, nemzetközi jogsegélyen és (kriptoeszközök esetén) blokklánc-analitikán alapul.[366][367][368]A bizonyítási lánc fenntartása megköveteli, hogy a platformi eseményeket (például avatárok közt lezajló interakciók, tranzakciók, hozzáférési kísérletek) a lehető legkorábban és forenzikailag hiteles módon rögzítsék, amelynél képernyőfelvételek, rendszerszintű naplók, hálózati forgalmi adatok, valamint a szolgáltatótól beszerzett nyomok egyaránt szükségesek lehetnek.[369] A gyakorlatban külön nehézséget jelent, hogy egyes üzemeltetők rövid megőrzési időt alkalmaznak, ezért a

[365] Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)

[366] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, pp. 118–179. (EU) 2023/1543 rendelet (e-Evidence rendelet)

[367]Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról, HL L 191, 2023.7.28., 118–180. o.; alkalmazandó: 2026. aug. 18

[368]Europol: Europol Spotlight, Cryptocurrencies: Tracing the evolution of criminal finances. Luxembourg, Publications Office of the European Union, 2021. PDF | ISBN 978-92-95220-37-9 | ISSN 2600-2760 | DOI: 10.2813/75468 | QL-AN-21-004-EN-N, 1–37. o.https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf (letöltés dátuma: 2024. október 17.)

[369]ISO/IEC: Information technology, Security techniques, Guidelines for identification, collection, acquisition, and preservation of digital evidence. ISO/IEC 27037:2012. Geneva, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2012. 38 o.

nyomozás korai szakaszában kiemelten fontos a megőrzési kérelmek kibocsátása, majd a formális adatigénylések és jogsegélylépések időbeni megtétele.[370] Speciális eset, amikor a bizonyíték megszerzése csak „játékon belül" lehetséges ugyanis több szerepjáték vagy metaverzum-színtér a releváns helyszínt és interakciókat kizárólag adott szint vagy küldetés teljesítése után teszi hozzáférhetővé. Ilyenkor a nyomozó, fedett avatárként, belép a világba, és a játékmenet során szerzi meg a szükséges tapasztalati bizonyítékot.

Ezt a módszert a gyakorlatban több valós eset is szemlélteti. A Second Life virtuális világában 2007-ben egy német tényfeltáró újságíró beépült egy pedofil hálózatba, amely zárt helyszíneken gyermekpornográf tartalmak kereskedelmével, sőt „virtuális pedofil szex" szolgáltatásokkal is foglalkozott. A riporter avatárként vett részt a közösség tevékenységében, és sikerült bejutnia egy kizárólag meghívásos alapon működő vetítésre is, ahol értékes információkat gyűjtött a résztvevőkről és terjesztőkről. Az akció eredményeként a német rendőrség vizsgálatot indított, amelyben a platform üzemeltetője, a Linden Lab, együttműködött a hatóságokkal, és kiadta a releváns felhasználói adatokat. Ez az eset jól mutatja, hogy a bűnüldöző szerveknek olykor maguknak is avatárként kell jelen lenniük, ha a bűncselekmények kizárólag virtuális térben, „játékon belüli" módon valósulnak meg.[371][372] Ugyanebben az évben az FBI avatárjai is megjelentek a Second Life kaszinóiban, mivel a platformon elterjedt szerencsejáték-tevékenységek jogi megítélése kétségessé vált. A hatóság vizsgálta, hogy a Linden-dollárban zajló fogadások sértik-e az amerikai szerencsejáték-törvényeket. Az ügynökök avatárként „körülnéztek" a kaszinókban, hogy a gyakorlatban is megértsék a rendszer működését. Bár ez az akció inkább elővigyázatossági jellegű volt, mint konkrét büntetőeljárás, azonban rávilágított arra, hogy a metaverzumban zajló gazdasági tevékenységek és virtuális valuták valós pénzügyi és jogi következményekkel járhatnak, így a nyomozóknak a digitális gazdaság

[370]Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)
[371]Connolly, Kate: Germany investigates Second Life child pornography. https://www.theguardian.com/technology/2007/may/08/secondlife.web20 (letöltés dátuma: 2024. október)
[372]Szabó Barbara: Virtual pandemonium. In Kajos, L F; Bali, Cintia; Puskás, T; Szabó, R (szerk.) XI. Interdiszciplináris Doktorandusz Konferencia 2022 Tanulmánykötet : 11th Interdisciplinary Doctoral Conference 2022 Conference Book Pécs, Magyarország : Pécsi Tudományegyetem Doktorandusz Önkormányzat (2023) 692 p. pp. 526-533. , 8 p. ISBN:9789636260705

világát is be kell építeniük vizsgálati módszereik közé.[373] A 2008-as év új szintet hozott a virtuális nyomozásokban. Edward Snowden későbbi kiszivárogtatásai alapján kiderült, hogy az NSA, a CIA és a brit GCHQ ügynökei is tömegesen jelentek meg fedett avatárként olyan játékokban, mint a World of Warcraft vagy a Second Life. A hírszerzés attól tartott, hogy ezek a platformok rejtett kommunikációs csatornaként szolgálnak terroristák és bűnszervezetek számára. A titkos ügynökök a játékbeli beszélgetéseket és interakciókat monitorozták, sőt, külön koordinációs egységet kellett létrehozni, nehogy véletlenül egymást figyeljék meg. Bár közvetlen terrorcselekményt nem sikerült leleplezniük, a brit hatóságok egy online bankkártya-adatokkal kereskedő bűnszervezetet így buktattak le, miután annak tagjai a Second Life-ban folytatták tevékenységüket.[374]Az ilyen típusú nyomozásokban a fedett avatárok szerepe kulcsfontosságú. A nyomozóknak sok esetben szintet kell lépniük, küldetéseket teljesíteniük, sőt, a közösség tagjaivá válniuk ahhoz, hogy hozzáférjenek a zárt csoportokhoz vagy privát helyszínekhez. Ez nem csupán technikai, hanem szociális kihívás is: a tapasztalt játékosok gyorsan kiszúrják, ha valaki „nem odavaló”, így a nyomozónak hitelesen kell beépülnie. Gyakran gamer-szakértők segítségére is szükség van, akik tanácsot adnak a játékon belüli viselkedéshez, szóhasználathoz vagy karakterfejlesztéshez. Munkáltatói szempontból a „játékon belüli” nyomozás első pillantásra nehezen magyarázható ugyanis kívülről nézve úgy tűnhet, mintha a rendőr munkaidőben játszana. Valójában azonban ez speciális, engedéllyel végzett fedett művelet, amely célzott bizonyítékszerzést szolgál. Az időráfordítás igazolható hivatalos feladatkijelöléssel, részletes jelentéssel és adatgyűjtési protokollal. A nyomozó nem szórakozik, hanem információt gyűjt, kapcsolatot épít, és a virtuális tér saját szabályai szerint „helyszínel”. A munkáltató feladata, hogy ezt megfelelő keretek közé helyezze, azaz pontosan meghatározza a célokat, a kockázatokat, a megengedett interakciókat és a pszichológiai támogatás módját. Ez a megközelítés ma már elfogadott eleme lehet az operatív munkának, feltéve, hogy a titkos információgyűjtésre és bizonyíték-rögzítésre vonatkozó jogi garanciák maradéktalanul

[373]Reuters: FBI checks gambling in Second Life virtual world. https://www.reuters.com/article/technology/fbi-checks-gambling-in-second-life-virtual-world-idUSN03278658/ (letöltés dátuma: 2024. október 18.)
[374]ProPublica: World of Spycraft: Intelligence Agencies Spied in Online Games.https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games (letöltés dátuma: 2024. október 18.)

érvényesülnek.[375] Mindezekből arra lehet következtetni, hogy a hatékony felderítés egyik alapvető előfeltétele a célzott készség- és kompetenciafejlesztés, amely biztosítja, hogy a nyomozóhatóságok a technológiai eszközöket tudatosan, jogszerűen és eredményesen alkalmazzák. A bűnüldözőknek érteniük kell a VR/XR-környezetek működését, a platformszabályok sajátos „tulajdon"- és hozzáférési logikáját, a digitális lánc- és hash-alapú hitelesítés eljárásait, valamint a blokklánc-nyomkövetés módszertanát. Ennek megfelelően világszerte megjelentek metaverzum-alapú tréningek és laborhelyzetek, ahol a résztvevők VR-eszközökkel, szimulált tömegjelenetek és incidensek mellett gyakorolják a bizonyítékok rögzítését és az eseménykezelést. A speciális nyomozói kapacitások bővítésére jó gyakorlat, hogy egyes országok dedikált, multidiszciplináris csoportokat állítanak fel ilyenek a fintech- és kriptoelemzők, OSINT-szakértők, digitális forenzikusok és a jogászok, akik közös csapatban dolgoznak ezeken ügyeken.[376] Másutt (különösen a fiatalkorúak védelme terén) online járőröző egységek jelennek meg a streaming- és játékközösségekben, a célcsoport nyelvén és felületein bizalmat építve és korai bejelentési csatornákat.[377] Magyarországon ugyan jelenleg nem működik önálló „metaverzum-egység", azonban a kiberbűnözés elleni szervezeti egységek tevékenységi köre egyre inkább kiterjed az ilyen jellegű feladatokra is. Számukra kiemelt jelentőséggel bír a célzott továbbképzés, a gyakorlati protokollok fejlesztése, valamint az eszközpark folyamatos korszerűsítése. Kiemelendő az is, hogy a nagy, globális szolgáltatók (például Meta, Roblox, Epic Games) együttműködése nélkül a hatóságok nem jutnak hozzá a szükséges IP-, napló-, tranzakciós illetőleg profiladatokhoz.[378][379]A rendvédelmi szervek nemzetközi tapasztalata szerint két irány szükséges egyszerre. Egyrészt „bizonyítás-

[375]Council of Europe GLACY: Law Enforcement Training Strategy. Project area specific strategies. Kézirat, Draft version, 2014. augusztus 5. Strasbourg, Council of Europe, 5–74. o.

[376]Europol: Europol Spotlight, Cryptocurrencies: Tracing the evolution of criminal finances. Luxembourg, Publications Office of the European Union, 2021. PDF | ISBN 978-92-95220-37-9 | ISSN 2600-2760 | DOI: 10.2813/75468 | QL-AN-21-004-EN-N, 1–37. o.https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf (letöltés dátuma: 2024. október 17.)

[377]Politi (Dánia): Politiets Online Patrulje.https://politi.dk/om-politiet/virksomheden/politiets-online-patrulje (letöltés dátuma: 2024. október 16.)

[378] Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27.10.2022, Art. 52(3).

[379] Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)

barát” platform-funkciók (könnyített jelentés és jelzőrendszer, incidens-naplók egységes szerkezete, célzott adatmegőrzés és adatigénylésre visszakereshetőség), másrészt a jogalkotói keretek pontosítása szükséges.[380] Utóbbi körben a virtuális vagyontárgyak jogi természetének tisztázása (különösen a „dolog”-fogalomhoz, a birtokláshoz és a rendelkezési jogosultsághoz való viszonyuk) elengedhetetlen ahhoz, hogy a büntetőjogi tényállások egyértelműen és kiszámíthatóan alkalmazhatók legyenek.[381] A bizonyíthatóság erősítése érdekében indokolt minimumkövetelményeket meghatározni a naplózási és adatmegőrzési gyakorlatra, különösen a magas kockázatú, tranzakciót vagy értékcserét támogató platformok esetében. E standardokhoz célszerűen illeszthetők az egységesített hatósági adatigénylési űrlapok, a standardizált időbélyeg- és hash-követelmények, valamint azok az eljárási mechanizmusok, amelyek a határokon átnyúló ügyekben elősegítik és felgyorsítják az adathozzáférést.[382] A platformtól származó adatok átvételekor és kezelésekor végig biztosítani kell a bizonyítás integritását és hitelességét. A hash-értékek rögzítése, időbélyegzés, a gyűjtés és tárolás részletes jegyzőkönyvezése, valamint a láncolat dokumentálása nélkülözhetetlen. A képernyőfelvételek önmagukban ritkán elégségesek. Értékük akkor erős, ha alátámasztják őket rendszer- és hálózati logok, szerveroldali audit-nyomok, szerződéses feltételek és (kriptós ügyekben) a blokklánc-tranzakciók visszaigazolásai. Az eljárási garanciák oldalán a szükségesség-arányosság mércéje, a célhoz kötött adatkezelés és a személyes adatok védelme (különösen a fiatalkorúaké) végig érvényesítendő, az aránytalanul széles vagy differenciálatlan adatigénylések a bírósági bizonyíthatóságot is veszélyeztethetik.[383] De lege ferenda érdemes megfontolni egy önálló ‘digitális vagyon’ dogmatikai kategória vagy értelmező klauzula bevezetését, amely egyértelműen rendezné a nem anyagi, de gazdasági értékkel bíró virtuális javak büntetőjogi védelmét. Indokolt továbbá a platformszintű naplózási és adatmegőrzési minimumkövetelmények jogszabályi rögzítése a bizonyítás hatékonyságának növelése érdekében, valamint a gyorsított, standardizált hatósági

---

[380] Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)

[381] Wildman, N. – McDonnell, N.: The puzzle of virtual theft. = Analysis 2020/80(3), 493–499. o. http://eprints.gla.ac.uk/210232/ (letöltés dátuma: 2025. szeptember 16.)

[382] Council of Europe: Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), opened for signature: 12 May 2022 (Strasbourg); hivatalos szöveg és jegyzék: CoE Treaty Office. (HU rövidítés: „Budapesti Egyezmény, Második kiegészítő jegyzőkönyv (CETS 224).)

[383] Be. alapelvek és személyesadat-kezelési garanciák releváns részei

adatigénylési csatornák kialakítása a jelentős szolgáltatókkal (ideértve a központi kapcsolattartó pontok, egységes formátumok és határidők meghatározását.) A kiberforenzikus képzések és a metaverzum-szimulációk rendszeresítése az igazságügyi és rendvédelmi képzésben tovább erősítené a szakmai kompetenciákat, míg a nyílt együttműködési protokollok kiterjesztése (összhangban a Budapesti Egyezmény második kiegészítő jegyzőkönyvével) elősegítené a határokon átnyúló ügyek gyorsabb és hatékonyabb kezelését.).[384][385] Ezen lépések együttesen teremthetik meg azt a kiszámítható és bizonyítás-barát jogi környezetet, amelyben a VR- és metaverzum-eredetű cselekmények a hatályos Büntető Törvénykönyv keretei között is hatékonyan feltárhatók és szankcionálhatók, miközben a jogbiztonság és az alapvető jogok védelme maradéktalanul érvényesül.

5. A nyomozási cselekmények az elektronikus adatok körében

5.1. Az elektronikus adatokkal kapcsolatos nyomozási cselekmények és jelentősége

Az elektronikus adatokkal kapcsolatos nyomozási cselekmények a bűncselekmények felderítésének és vizsgálatának azon területét képezik, amely az információs rendszerekből származó adatok hatósági felhasználására és az azokhoz való hozzáférésre irányul. Ide tartozik minden olyan eljárási cselekmény, amelynek során az elektronikus úton rögzített adatokat, azaz elektronikus adatokat gyűjtenek, kezelnek, elemeznek és értékelnek a hatóságok a büntetőeljárás megindításának, vádemelés céljából.[386]. Az online térben fellelhető információk képviselik az új dimenzióját az úgynevezett második generációs bizonyítékoknak, amelyek új szemléletű, informatikai eszközöket igénylő módszereket követelnek a cselekmény rekonstrukciójához és az elkövető

[384] Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024.
https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)
[385]Council of Europe: Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), opened for signature: 12 May 2022 (Strasbourg); hivatalos szöveg és jegyzék: CoE Treaty Office. (HU rövidítés: „Budapesti Egyezmény, Második kiegészítő jegyzőkönyv (CETS 224).)
[386] Be. 158. §, Be. 315. §, Be. 316–318. §, Be. 343–345. §

azonosításához.[387][388] Ennek oka főként ahogy, Eoghan Casey találó megfogalmazása is állítja „a mai modern világban nehéz elképzelni olyan bűncselekményt, amelynek nincs digitális dimenziója”.[389] Ezen állítással egyet lehet érteni, ugyanis a XXI. században az emberi tevékenység szinte minden mozzanata valamilyen formában nyomot hagy maga után, legyen az fizikai, (mint például ujj- vagy lábnyom) vagy elektronikus (mint az elektronikus kommunikáció, online jelenlét vagy közösségi médiahasználat). A technológia áthatja a mindennapjainkat oly módon, hogy az emberek jelentős része online végzi kommunikációját, személyes és hivatalos ügyeit mindamellett okostelefont vagy okos eszközöket hord magánál, amely folyamatosan adatokat generál vagy rögzít az egyén tevékenységeiről, vagy éppen a tartózkodási helyéről. Ennek következtében a bűncselekmények kapcsán keletkezhetnek olyan elektronikus adatok, amelyek releváns bizonyítékokká válhatnak, akár magából az elkövetésből fakadóan, akár a körülményekből adódóan. [390] Ennél fogva amennyiben a nyomkutatási terv elektronikus, informatikai, technológiai, internetalapú vagy ezzel kapcsolatos elemeket érint úgy, két fő szegmensre tagolható az eljárás.[391] Egyrészt a kiberbűnözéssel (azaz a számítógépes bűnözéssel) kapcsolatos bűncselekmények felderítését, másrészt a „hagyományos” (nem feltétlenül technológiai) bűncselekmények során keletkező elektronikus adatok kezelését is magába foglalhatja a nyomozás.[392] E körben fontos megjegyezni azt, hogy a szakirodalom megkülönbözteti a számítógépes bűnözés különböző típusait az alkalmazott technológia szerepe alapján.[393] Egyfelől megkülönbözteti a számítógép-központú bűncselekményeket (computer centered crime), amikor maga a számítógépes

[387] Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. = Magyar Jog, 2014/7–8., 433–443. o. Elérhető: https://szakcikkadatbazis.hu/doc/3072353 (letöltés dátuma: 2022. 05. 27.)

[388]Gácsi Anett Erzsébet: Az elektronikus bizonyítás alapvető dogmatikai kérdései. = Magyar Rendészet, 2018/2., 77–89. o. Elérhető: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1360 (letöltés dátuma: 2022. 05. 27.)

[389]Casey, Eoghan: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3. kiadás, Academic Press, London, 2011.

[390]Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. = Belügyi Szemle, 64. évf. 11. sz. (2016), 81–96. o. Elérhető: https://epa.oszk.hu/05200/05238/00023/pdf/EPA05238_bsz_2016_11_081-096.pdf, (letöltés dátuma: 2022. 05. 27.)

[391] Fenyvesi Csaba – Herke Csongor – Tremmel Flórián (szerk.): Kriminalisztika. 4. kiadás, Dialóg Campus Kiadó, Budapest–Pécs, 2022.

[392] Gácsi Anett Erzsébet: Az elektronikus bizonyítás alapvető dogmatikai kérdései. = Magyar Rendészet, 18(2), 2018, 77–89. o. Elérhető: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1360 (Letöltés: 2022. 05. 27.)

[393]Bodnár András Péter: A digitális bizonyítékok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. = Büntetőjogi Szemle, XI. évf. 1. sz. (2022), 19–29. o. Elérhető: https://ujbtk.hu/dr-bodnar-andras-peter-a-digitalis-bizonyitekok-megjelenese-a-buntetoeljarasban-kulonos-tekintettel-a-szakerto-igenybevetelere/, (letöltés dátuma: 2023. 05. 27.)

rendszer, hálózat vagy digitális eszköz a támadás közvetlen célpontja.[394] Ilyen eset például a már előző fejezetekben részletezett számítógépes rendszerek feltörése, vírusok terjesztése, vagy egy kereskedelmi weboldal tartalmának jogosulatlan módosítása, amelyek felderítéséhez különleges informatikai szakértelem szükséges.[395] Másfelől léteznek számítógéppel segített bűncselekmények (computer assisted crime), amikor az informatikai eszköz megkönnyíti a bűncselekmény elkövetési módját, elkövetését, (viszont nem feltétlenül nélkülözhetetlen hozzá.) Ilyen például a gyermekpornográf felvételek forgalomba hozatala az interneten amely esetében a számítógép vagy az adott okoseszköz az elkövetés eszköze, mely gyorsabbá, kiterjedtebbé teheti a nagy nyilvánosság számára a bűncselekményt, bár maga a bűncselekmény (pl: a tizennyolcadik életévét be nem töltött személyt ábrázoló pornográf felvételt kínálása stb.) elvben technológia nélkül is megvalósítható lenne.[396] Harmadrészt beszélhetünk járulékos számítógépes bűnözésről (incidental computer crime), amikor egy alapvetően „klasszikus" bűncselekménynek is megjelenik egy digitális vetülete. Ebben az esetben a számítógépes rendszer vagy elektronikus adat csupán mellékkörülmény, például az elkövető a bűncselekmény tervét e-mailben beszéli meg (tehát elektronikus adat és információs nyom marad utána), vagy a bűncselekményhez köthető adatokat (pl. a számvitelről szóló törvényben vagy a felhatalmazásán alapuló jogszabályokban előírt bizonylati rendet megsérti vagy könyvvezetési, beszámoló készítési kötelezettségének megszegéséből) nem papíron, hanem számítógépen tárolja.[397] Ezen utóbbi kategória jelentősége folyamatosan növekszik, hiszen manapság egyre több konvencionális bűncselekmény során merül fel az „elektronikus bizonyíték" vagyis megállapítható, hogy

[394] Phillips, Kirsty – Davidson, Julia C. – Farr, Ruby R. – Burkhardt, Christine – Caneppele, Stefano – Aiken, Mary P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. = Forensic Sciences, 2022/2(2), 379–398. o. DOI: 10.3390/forensicsci2020028

[395] Gácsi Anett Erzsébet: Az elektronikus bizonyítás alapvető dogmatikai kérdései. = Magyar Rendészet, 18(2), 2018, 77–89. o. Elérhető: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1360 (Letöltés: 2022. 05. 27.)

[396] Bodnár András Péter: A digitális bizonyítékok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. = Büntetőjogi Szemle, XI. évf. 1. sz. (2022), 19–29. o. Elérhető: https://ujbtk.hu/dr-bodnar-andras-peter-a-digitalis-bizonyitekok-megjelenese-a-buntetoeljarasban-kulonos-tekintettel-a-szakerto-igenybevetelere/, (letöltés dátuma: 2023. 05. 27.)

[397] Gácsi Anett Erzsébet: Az elektronikus bizonyítás alapvető dogmatikai kérdései. = Magyar Rendészet, 18(2), 2018, 77–89. o. Elérhető: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1360 (Letöltés: 2022. 05. 27.)

a technológia fejlődésével a klasszikus bűncselekmények digitális oldala is egyre fontosabbá vált.[398][399]

Az elektronikus adatok nyomozási jelentőségét tehát két fő tényező adja: egyrészt a tisztán kiber-(cyber) jellegű bűncselekmények terjedése, másrészt az elektronikus adat bizonyítás eszközeként való általánossá válása a mindennapi bűnüldözésben.[400][401]Az elmúlt években exponenciálisan növekedett az információs rendszerek elleni bűncselekmények és az internet felhasználásával megvalósuló csalások, visszaélések száma.[402] Az információs rendszerek elleni bűncselekmények száma Magyarországon is az elmúlt években jelentős növekedést mutatott. A Legfőbb Ügyészség éves statisztikai jelentései alapján az információs rendszer felhasználásával elkövetett csalások száma az alábbiak szerint alakult:[403]

Év	Esetek száma
2018	3 073
2019	2 634
2020	3 401
2021	2 700

[398] Szabó Imre: A számítástechnikai adat, mint elektronikus bizonyíték, A magyar szabályozás elemzése az Európai Tanács számítástechnikai bűnözéséről szóló egyezménye alapján Kriminológiai Tanulmányok 48., Országos Kriminológiai Intézet., Budapest (2011) Elérhető: https://www.okri.hu/images/stories/KT/KT_48_2011/003_1_szabo_13-28.pdf (letöltés dátuma: 2023. 05. 27.)

[399] Gácsi Anett Erzsébet: Az elektronikus bizonyítás alapvető dogmatikai kérdései. = Magyar Rendészet, 18(2), 2018, 77–89. o. Elérhető: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1360 (Letöltés: 2022. 05. 27.)
Bodnár András Péter: A digitális bizonyítékok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. = Büntetőjogi Szemle, XI. évf. 1. sz. (2022), 19–29. o. Elérhető: https://ujbtk.hu/dr-bodnar-andras-peter-a-digitalis-bizonyitekok-megjelenese-a-buntetoeljarasban-kulonos-tekintettel-a-szakerto-igenybevetelere/, (letöltés dátuma: 2023. 05. 27.)

[400] Be. 165. §

[401] Phillips, Kirsty – Davidson, Julia C. – Farr, Ruby R. – Burkhardt, Christine – Caneppele, Stefano – Aiken, Mary P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. = Forensic Sciences, 2022/2(2), 379–398. o. DOI: 10.3390/forensicsci2020028

[402] INTERPOL: Cybercrime. Elérhető: https://www.interpol.int/en/Crimes/Cybercrime (Letöltés dátuma: 2023. május 29.)

[403]Legfőbb Ügyészség: Tájékoztató a bűnözés 2022. évi adatairól. Budapest, 2023. Elérhető: https://ugyeszseg.hu/repository/mkudok34379.pdf (Letöltés dátuma: 2024. május 29.)

Év	Esetek száma
2022	4 084

8. ábra: A Legfőbb Ügyészség éves statisztikai jelentései alapján az információs rendszer felhasználásával elkövetett csalások száma

Ezen táblázatból egyértelmű következtetésként levonható, az, hogy a 2022-as évben az esetek száma több mint kétszeresére nőtt az előző évhez képest, amely betudható a kiberbűnözés fokozódásának. Emellett a bűncselekmények felderítésében ma már szinte elengedhetetlen az elektronikus bizonyítékok gyűjtése hiszen legyen szó egy lopásról, rablásról vagy csalásról, nagy eséllyel lesznek a nyomozásban felhasználható elektronikus nyomok (pl. térfigyelő kamera felvétele, mobiltelefon cellainformáció, e-mail kommunikáció stb.). [404][405] E körben a nyomozás lényege éppen az, hogy ezeket a bizonyítási eszközöket a hatóságok felderítsék, összegyűjtsék, biztosítsák, majd a hagyományos bizonyítékokkal együtt, értékelve tárják az ügyészség rendelkezésére amely dönt a nyomozás befejezésének kérdésében.[406][407][408] Koncepcionálisan tehát a nyomozás (felderítés és vizsgálat) során összegyűjtött elektronikus adatok és információk ugyanolyan értékű bizonyítékok (mint bármely más, egy tanúvallomás, egy okirat vagy egy tárgyi bizonyítási eszköz) hiszen mindegyik célja az, hogy a megtörtént cselekményt rekonstruáljuk és az elkövetőt azonosítsuk.[409][410] Ugyanakkor az elektronikus adatok sajátos jellemzői (immateriális jelleg, módosíthatóság, másolhatóság stb.) miatt a hatóságoknak különös figyelmet kell fordítaniuk az ilyen adatok szakszerű kezelésére és hitelesítésére (erre a későbbiekben, az elektronikus bizonyítékokról szóló fejezetben

[404]Bodnár András Péter: Digitization in criminal proceedings – issues related to electronic data. = Büntetőjogi Szemle, XI. évf. 1. sz. (2021), 19–29. o. Elérhető: https://ujbtk.hu/andras-peter-bodnar-digitization-in-criminal-proceedings-issues-related-to-eletronic-data/, letöltés dátuma: 2025. 03. 13.
[405] Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. = Belügyi Szemle, 64. évf. 11. sz. (2016), 81–96. o. Elérhető: https://epa.oszk.hu/05200/05238/00023/pdf/EPA05238_bsz_2016_11_081-096.pdf, letöltés dátuma:
[406]Gyaraki Réka Eszter: A számítógépes bűnözés nyomozásának problémái. PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2018, 71. o.
[407]Casey, Eoghan*:* Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3. kiadás, Academic Press, London, 2011.
[408] Be. 166. §
[409]Gyaraki Réka Eszter: A számítógépes bűnözés nyomozásának problémái. PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2018, 71. o.
[410] Be. 165. §

térünk ki.) Emellett áttekintjük, miként változtak meg a bűncselekmények elkövetési módszerei a technológia hatására.

5.2. A bűncselekmények elkövetési módjának változása

A XXI. században a bűnelkövetők egyre gyakrabban használnak elektronikus eszközöket és különféle hálózatokat, alkalmazásokat a bűncselekmények megtervezéséhez, elkövetéséhez vagy leplezéséhez. A bűncselekmények elkövetési módja így alapvetően megváltozott a korábban fizikai jelenlétet vagy személyes érintkezést igénylő cselekmények sokszor átkerültek az online térbe, vagy legalábbis az internet nyújtotta lehetőségek tovább bővítették azt, új technológiai eszköztárakkal és ezáltal új bűncselekménytípusok jelentek meg amelyeket kifejezetten a digitális környezet teremtett meg. Ilyenek a már részletezett kiberbűncselekmények, például a hackertámadások, túlterheléses támadások (DDoS), zsarolóvírusok (ransomware) alkalmazása, adathalászat (phishing) vagy a személyes adatokkal való visszaélések. Ezen cselekmények közös jellemzője, hogy az elkövetésük elképzelhetetlen lenne a korszerű informatikai hálózatok hiányában ugyanis az elkövető az informatikai eszköz révén, sokszor földrajzilag távolról követi el a bűntettet, valós károkat okozva. A magyar büntető jogszabályok is reagáltak ezen jelenségre, a Büntető Törvénykönyvben (Btk.) külön fejezetek foglalkoznak az információs rendszerek elleni és az azokat felhasználó bűncselekményekkel többek között ilyen a tiltott adatszerzés (Btk. 422. §), az információs rendszer vagy adat megsértése (Btk. 423. §), információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424. §), készpénz-helyettesítő fizetési eszköz hamisítása (Btk. 392. §), a készpénz-helyettesítő fizetési eszközzel való visszaélés (Btk. 393 §), levéltitok megsértése (Btk. 224. § (1)(b)), Információs rendszer felhasználásával elkövetett csalás (Btk. 375. §), (valamint adathalászat amely gyakran a Btk. 375. § szerinti csalás tényállása szerint kerül minősítésre). Ezen tényállások sajátossága, hogy az elkövetési magatartás teljes mértékben a virtuális térben valósul meg, nem hagyományos fizikai jelenléttel, hanem informatikai eszközök segítségével, globálisan, földrajzi korlátok nélkül, ezért az ilyen ügyek nyomozása során a nemzetközi együttműködésre

(pl. közös nyomozócsoportok, Budapesti Egyezmény) is szükség lehet.[411]Az új bűncselekmények megjelenése mellett a hagyományos bűnözés módszerei is átalakultak. Ennek egyik jellegzetes példája és egyúttal ennek prezentálására is alkalmas az ún. utazó bűnözés és a sorozatbűncselekmények keretében elkövetett esetek. Ezen bűncselekmények elkövetői sokszor szervezetten, lakóhelyüktől távoli településeken követnek el sorozatjelleggel lopásokat, kihasználva azt, hogy a hatóságok között illetékességi határok vannak (Be. 21. § az illetékesség alapvetően a bűncselekmény helye szerint alakul, de a 21. § (2) bekezdése rendelkezik a több helyszínes elkövetés esetére alkalmazandó szabályról.).[412][413] A technológia fejlődése ezt a módszert még könnyebbé tette az elkövetők számára ugyanis általánosabb esetben gépjárművel nagy sebességgel haladnak, így nagy területen tudnak rövid időn belül bűncselekményeket elkövetni, és telekommunikációs eszközök segítségével tartják a kapcsolatot egymással úgynevezett "munkatelefon" -t használva (egy olyan előre beszerzett mobilkészülék és SIM-kártya, amelyet kizárólag a bűncselekmény idején, az elkövetés koordinálására használnak, majd utána kikapcsolnak vagy eldobnak).[414] Ennél fogva a telefon lehallgatása vagy annak cellaadatainak elemzése megnehezül, hiszen az eszköz anonim és csak rövid ideig volt aktív.[415]A modern utazó bűnözők emellett titkosított üzenetküldő alkalmazásokat vesznek igénybe (például Viber, WhatsApp, Signal), hogy kommunikációjukat ne lehessen egyszerűen lehallgatni.[416] A terepi felderítésben is támaszkodnak digitális eszközökre akként, hogy az elkövetés előtt a nyilvános online térképszolgáltatásokat (pl. Google Maps) használják a leendő célpontok (épületek, útvonalak) feltérképezésére, és

---

[411]Tanácsi kerethatározat (2002/465/IB) a közös nyomozócsoportokról, 2002. június 13. Elérhető: https://www.eurojust.europa.eu/sites/default/files/Partners/JITs/CFDonJITs-2002-06-13-EN.pdf (Letöltés dátuma: 2022. 05.29.)

[412]Boi László: Az utazó bűnözés és a sorozatbűncselekmények összefüggései. In: Pécsi Határőr Tudományos Közlemények, 16. kötet, 2015, 149–156. o. Elérhető: https://epa.oszk.hu/04500/04581/00016/pdf/EPA04581_pecsi_hataror_2015_149-156.pdf (Letöltés dátuma: 2022. 05. 29.

[413]Be. 21. § (2)

[414]Boi László: Az utazó bűnözés és a sorozatbűncselekmények összefüggései. In: Pécsi Határőr Tudományos Közlemények, 16. kötet, 2015, 149–156. o. Elérhető: https://epa.oszk.hu/04500/04581/00016/pdf/EPA04581_pecsi_hataror_2015_149-156.pdf (Letöltés dátuma: 2022. 05. 29.

[415]Blueforce Learning: What is Mobile Data, and How is it Used in Criminal Investigations?. Elérhető: https://www.blueforcelearning.com/blog/what-is-mobile-data-and-how-is-it-used-in-criminal-investigations (Letöltés dátuma: 2025. 01. 29.)

[416]Bodnár András Péter: Digitization in criminal proceedings – issues related to electronic data. = Büntetőjogi Szemle, XI. évf. 1. sz. (2021), 19–29. o. Elérhető: https://ujbtk.hu/andras-peter-bodnar-digitization-in-criminal-proceedings-issues-related-to-eletronic-data/, letöltés dátuma: 2023. 03. 13.

GPS alapú navigációt a helyszín megközelítéséhez. Mindezen módszerek azt eredményezik, hogy a bűnelkövetők tevékenységeiket eredményesebben egyben kevésbé kockázatosan tudják végrehajtani a cselekményeiket, és igyekeznek minimálisra csökkenteni a konvencionális nyomok (ujjlenyomat, DNS, stb.) hátrahagyását. Ugyanakkor ezen technológia használata elkerülhetetlenül elektronikus nyomok keletkezésével jár, ami végső soron a nyomozó hatóságok munkáját is segítheti. A fenti példában említett sorozatbűncselekmények nyomozásában például releváns elektronikus bizonyíték lehet a biztonsági kamerák felvétele (ha a tettesek mozgását rögzítette valahol kamera), a mobiltelefonok cellainformációi (amelyek igazolhatják, hogy az elkövetők telefonjai a bűncselekmény helyszíne közelében voltak az adott időben), az elfogásuk esetén lefoglalt telefonok híváslistái és üzenetei, vagy a GPS eszközük útvonalelőzményei.[417] Az elektronikus nyomok kettős szerepet töltenek be. Míg a bűnelkövetők számára a technológia a cselekmények megvalósítását segítő eszközként jelenik meg, addig a hatóságok számára bizonyítási lehetőséget kínál. Megállapítható, hogy a bűncselekmények elkövetési módja az utóbbi évtizedekben a digitalizáció hatására jelentősen megváltozott. A technológia egyrészt új bűnözési formákat hozott létre (kiberbűnözés), másrészt a klasszikus bűncselekményekhez is integrálódott (pl: digitális kommunikáció, adatkezelés formájában). A bűnüldöző szerveknek lépést kellett tartaniuk ezen változásokkal, és fejleszteniük kellett módszereiket és eszköztárukat. A következőkben áttekintjük az ehhez kapcsolódó nyomozás módszereit, amelyekkel a hatóságok reagáltak ezekre a kihívásokra, különös tekintettel a megfigyelésre, lehallgatásra és adatszerzésre.

5.3. Az elektronikus nyomozás módszerei: megfigyelés, lehallgatás, adat szerző tevékenység

A nyomozás során a hatóságok számos módszert alkalmazhatnak a szükséges információk titkos vagy nyílt megszerzésére. E módszerek jogi kereteit Magyarországon

[417]Mohammed Okmi – Lip Yee Por – Tan Fong Ang – Ward Al-Hussein – Chin Soon Ku: A Systematic Review of Mobile Phone Data in Crime Applications: A Coherent Taxonomy Based on Data Types and Analysis Perspectives, Challenges, and Future Research Directions. = Sensors, 2023, 23(9), 4350. DOI: 10.3390/s23094350. Elérhető: https://www.mdpi.com/1424-8220/23/9/4350 (Letöltés dátuma: 2024. 05. 30.

elsősorban a Büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.), (továbbá: az ügyészségről, a rendőrségről, a Nemzeti Adó- és Vámhivatalról vagy a nemzetbiztonsági szolgálatokról szóló törvény alapján rendelik el), határozza meg. A leplezett eszközök alkalmazása alapvető jogok korlátozásával járó, a büntetőeljárásban végzett különleges tevékenység, amelyet az erre feljogosított szervek az érintett tudta nélkül végeznek, azaz, bírói vagy ügyészi engedély alapján avatkozik be a hatóság a magánszférába a bizonyíték megszerzése érdekében.[418][419] E körben kiemelten fontos leplezett eszközök közé tartozik a megfigyelés, a lehallgatás és az adatszerzés különböző formái, amelyeket az alábbiakban részletezük.

5.3.1. Megfigyelés

A megfigyelés a nyomozó hatóság, az ügyészség vagy a speciális egységek (terrorizmust elhárító szerv, bűnügyi felderítő szolgálatok, Nemzeti Adó-és Vámhivatal illetve nemzetbiztonsági szolgálatok) által folytatott rendszeres és célzott információgyűjtés, amelynek során az elkövető (vagy más érintett) tevékenységét, kapcsolatait, mozgását figyelik meg és rögzítik.[420] Hagyományos értelemben a megfigyelés történhet fizikai rejtett fizikai megfigyeléssel (az ügyészség engedélyével a fedett nyomozó vagy titkosan együttműködő személy alkalmazható, aki fizikai jelenléttel követheti az elkövetőt, információt gyűjthet), hely titkos megfigyelésével (bírói engedéllyel nem nyilvános hely (pl. lakás, jármű) titkos technikai megfigyelése engedélyezhető) vagy technikai eszközök például kamerák, hangrögzítők, (információs rendszer titkos megfigyelése során a leplezett eszközök alkalmazására feljogosított szerv bírói engedéllyel információs rendszerben kezelt adatokat titokban megismerhet, az észlelteket technikai eszközzel rögzítheti) helymeghatározó, rögzítő eszköz, (technikai eszköz titkos elhelyezése lakásban, járműben, tárgyban bírói engedéllyel) fizetési műveletek megfigyelése (ügyészi engedéllyel rendelhető el, max. 3+3 hónapra) alkalmazásával.[421][422][423] A XXI. században a megfigyelés kiterjedhet az információs terekre is, ideértve az érintett személy

[418]Be. 214–260. §
[419]Herke Csongor: Büntető eljárásjog., Első kiadás., Pécs (2018)
[420]Be. 216–227. §, Be. 231–232. §, Be. 231–232. §, Be. 235.- 236. §, Be. 241. §
[421]Be. 222–225. §, Be. 232. § (3)
[422]Be. 231. § e), 232. § (5), Be. 232. § (1), (3)
[423]Be. 216–218. §

információs rendszerének titkos megfigyelését (számítógépen vagy más információs rendszeren végzett tevékenység titkos megfigyelése, adat rögzítése, eszköz telepítése), valamint a kommunikációs tartalom megismerését (elektronikus hírközlő hálózaton vagy eszközön folytatott kommunikáció lehallgatása) vagy elektronikus adat hozzáférését, másolását, vizsgálatát (nyomozási szakaszban, elektronikus adatok zárolása, másolása, vizsgálata bírói engedéllyel).[424][425][426] Ezen megfigyelések alkalmazása rendszerint bírói vagy ügyészi engedélyhez kötött, és csak szigorú törvényi feltételek fennállása esetén megengedett. A Be. a leplezett eszközök között nevesíti az információs rendszer titkos megfigyelését, amely új jogintézményként került bevezetésre 2018-ban.[427] Ennek lényege, hogy a lehallgatás során a leplezett eszközök alkalmazására feljogosított szerv (bírói engedély birtokában) jogosult titokban megismerni és rögzíteni a személyek közötti elektronikus hírközlési szolgáltatás keretében, például telefonhívás, internetes kommunikáció vagy más információs rendszeren keresztül zajló beszélgetések tartalmát, annak érdekében, hogy a büntetőeljárásban bizonyítékot szerezzen a bűncselekmény elkövetéséről. Elméletileg elképzelhető, hogy az adott hatóság a megfelelő jogi engedély birtokában akár olyan technikai eszközt is alkalmazhat, amely képes egy gyanúsított számítógépének megfigyelésére, például a leütött billentyűk, megnyitott fájlok, vagy akár a webkamera és az eszközhöz tartozó mikrofon használatának rögzítésére és továbbítására.[428] Ilyen esetekben például egy chatszolgáltatáson keresztül küldött üzenetek a küldő számítógépén még olvasható formában rögzíthetők lehetnek. Az ilyen típusú megfigyelés azonban a magánszférába való súlyos beavatkozásnak minősülhetne, ezért általában csak szigorú bírói engedélyhez kötött, és jellemzően kizárólag különösen súlyos bűncselekmények esetén engedélyezhető. A fizikai megfigyelések körében alkalmazhatók bizonyos rejtett kamerák vagy GPS-alapú nyomkövető eszközök, különösen akkor, ha a hatóság célja egy gyanúsított mozgásának, találkozóinak dokumentálása. A technológiai fejlődés eredményeként ma már az sem zárható ki, hogy a nyomozó hatóságok a jogszabályi keretek között, akár valós időben is hozzáférjenek

[424]Be. 232. § (1)
[425]Be. 232. § (5)
[426]Be. 315–316. §
[427]Be. 232. § (5) – (vonatkozó szabályok az 1998. évi XIX. törvényben régi Be. esetében nem szerepeltek).
[428]Gyaraki Réka: A számítógépes bűnözés nyomozásának problémái. PhD értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2018. Elérhető: https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf, letöltés dátuma: 2023. 03. 13

egyes térfigyelő kamerarendszerek felvételeihez, lehetővé téve ezzel egy adott személy mozgásának követését a közterületeken. A megfigyelés tágabb értelmezésében ide sorolható az online térben történő adatszerzés is, különösen a nyilvánosan elérhető közösségi média profilok, bejegyzések, illetőleg a hozzászólások figyelemmel kísérése. Ez a tevékenység egyes esetekben nyílt információgyűjtésnek is tekinthető, hiszen a közösségi média felületeken létrehozott nyilvános profilok tartalma bárki számára hozzáférhető. Módszertanilag azonban, bizonyos körülmények között közel állhat a klasszikus megfigyeléshez, különösen, ha az rendszeres, célzott vagy rejtett módon zajlik. Példának okán az adott körözött személy felkutatásának során előfordulhat, hogy a hatóság figyelemmel kíséri az ismerőseinek közösségi oldalait, vagy egy terrorcselekménnyel összefüggésbe hozott személy internetes aktivitását elemzi abból a célból, hogy szélsőséges nézetekre vagy kapcsolati hálóra utaló jeleket azonosítson. A megfigyelés jogi keretei Magyarországon több szintűek. Ha a megfigyelés nem jár magánszféra korlátozásával (például közterületen követ egy nyomozó egy gyanúsítottat, vagy nyilvános adatokat figyel meg), akkor akár külön engedély nélkül is végezhető a nyomozati cselekmény. Amennyiben azonban magánlakásba való bejutással vagy magántitok megismerésével jár (pl. rejtett kamera elhelyezése magánterületen, informatikai rendszer titkos megfigyelése stb.), akkor már bírói engedélyhez kötött leplezett eszköznek minősül. Ilyen esetekben a bíróság határozott időre (tipikusan 90 napra, meghosszabbíthatóan) engedélyezheti a megfigyelést, ha azt a nyomozás érdekei indokolják és más módon az információ nem szerezhető meg. A megfigyelés során keletkező felvételek, információk és adatok a büntetőeljárásban, mint bizonyítási eszközök felhasználhatók, feltéve, hogy a beszerzésük törvényes volt és a keletkezett adatok eredetét, sértetlenségét igazolni tudják.[429] Ezen különböző megfigyelési formák mind fizikai, technikai, elektronikus vagy online, egy közös ugyanakkor alapvető követelményrendszerhez kötődnek, amely által kimondható, hogy a magyar jogrend nem teszi lehetővé az általános, válogatás nélküli („tömeges") megfigyelést, még akkor sem, ha az eszköz technikailag alkalmas lenne ilyen mértékű adatrögzítésre. Ezt a megközelítést támasztja alá a Nemzeti Adatvédelmi és Információszabadság Hatóság 2014. decemberében készített vizsgálati jelentése, amely kifejezetten azt vizsgálta, hogy a magyar nemzetbiztonsági szolgálatok kémprogramokat alkalmaznak-e a tömeges

[429]Be. 259-260. §.

megfigyelés eszközeként.[430] A jelentés megállapította, hogy a kémprogramok alkalmazása noha technikailag képes lenne akár tömeges adatgyűjtésre is csak célhoz kötötten, szigorúan szabályozott eljárásrend alapján, külső (jellemzően bírói) engedély birtokában jogszerű.[431]A jelentés rávilágított arra is, hogy a nemzetbiztonsági szolgálatok által alkalmazott technikai eszközök használata személyhez, időtartamhoz és konkrét nemzetbiztonsági célhoz kötött, és kizárólag akkor engedélyezhető, ha az adott információ más módon nem szerezhető be.[432] A törvényes működés alapfeltétele az is, hogy az információs önrendelkezési jogot, valamint a magánélethez való jogot csak a feltétlenül szükséges mértékben és időtartamban korlátozzák, az arányosság és célhoz kötöttség elvei alapján. Mindezek alapján kijelenthető, hogy a megfigyelés és adatgyűjtés jelenlegi jogi keretei Magyarországon nemcsak az alkotmányos jogokkal, hanem a nemzetközi emberi jogi elvárásokkal is összhangban állnak.[433][434] A titkos információgyűjtés során keletkező beavatkozásokat nemcsak előzetes bírói engedély, hanem folyamatos, többszintű kontrollmechanizmusok is szabályozzák (pl. az adatkezelés időtartama, célhoz kötöttsége, visszamenőleges ellenőrizhetősége). Ennek eredményeképp sem a rendőrségi, sem a nemzetbiztonsági célú megfigyelés nem minősülhet tömeges, válogatás nélküli lehallgatásnak vagy adatgyűjtésnek, mivel az ellentétes lenne az Alaptörvény I. és VI. cikkeiben rögzített alapvető jogokkal, továbbá az Infotv. és az Nbtv. rendelkezéseivel is.[435] Ezek a magyar jogi garanciák szoros párhuzamban állnak az Európai Unió Bíróságának (EUB) és az Emberi Jogok Európai Bíróságának (EJEB) ítélkezési gyakorlatával. Az EUB például a Schrems I. és Schrems II. ítéleteiben kimondta, hogy a tömeges, cél nélküli adatgyűjtés összeegyeztethetetlen az

[430]Bíró János o. v.: *Jelentés a kémprogramok alkalmazásáról a nemzetbiztonsági szolgálatok titkos információgyűjtése körében*. Ügyszám: NAIH-1904-6/2014/T. Nemzeti Adatvédelmi és Információszabadság Hatóság, Budapest, 2015. Elérhető: https://naih.hu/files/adatved-jelentes-1904-6-2014-T_kemprogram.pdf (letöltés dátuma: 2021. 05. 30.)
[431]1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (Nbtv.)56–58. §
[432]1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (Nbtv.)53. § (2) bek.
[433]Infotv. 4–7. §; Emberi Jogok Európai Egyezménye 8. cikk
[434]Herke Csongor - Szabó Barbara: Limits of Freedom of Public Authorities with Respect to Obtaining Evidence at the Stage of Investigation: Hungarian Report. In: Maria Rogacka-Rzewnicka (szerk.), Limits of Freedom of Public Authorities with Respect to Obtaining Evidence at the Stage of Investigation: A Comparative Legal Study. Leiden, Hollandia: Brill/Nijhoff, 2024. pp. 129–144. ISBN-10 9004710310, ISBN-13 978-9004710313
[435]Alaptörvény I. cikk (3), VI. cikk (1)–(2); Infotv. 4–7. §

EU Alapjogi Chartájában rögzített magánélethez és adatvédelemhez való joggal.[436][437]A bíróság elvárja, hogy minden tagállami vagy nemzetközi adatkezelés során érvényesüljenek a célhoz kötöttség, a szükségesség és az arányosság követelményei, továbbá biztosítva legyenek a hatékony jogorvoslat és a független felügyeleti mechanizmusok. Hasonló követelményeket fogalmaz meg az EJEB is a Big Brother Watch v. Egyesült Királyság ügyben is, amelyben kifejezetten hangsúlyozta, hogy a titkos tömeges megfigyelés csak akkor egyeztethető össze az Emberi Jogok Európai Egyezménye 8. cikkével, ha szigorú jogállami garanciák és kontrollmechanizmusok korlátozzák. Ezt a magyar szabályozás a NAIH-jelentésben is hangsúlyozta, azaz a háromfokozatú ellenőrzés (engedélyezés, alkalmazás, utóellenőrzés), valamint a bírói engedély és célhoz kötöttség összhangban áll az EJEB elvárásaival. [438]Mindezek vonatkozásában megállapítható tehát, hogy a megfigyelés, legyen az fizikai, digitális vagy informatikai alapú, mindig konkrét személyre, cselekményre és jogszabályi feltételekre épül, és a technológiai fejlődésre reagáló jogalkalmazás mellett nem lehet eszköze általános társadalmi kontrollnak. A digitális eszközök kapcsán különösen fontos, hogy a jogalkalmazó szervek a rendelkezésükre álló technológiát csak a jogszabályozás keretei között, a szükségesség és arányosság követelményeit szem előtt tartva alkalmazzák.

5.3.2. Lehallgatás

A lehallgatás a kommunikáció tartalmának titkos megismerését jelenti. Elsősorban a telefonbeszélgetések lehallgatását értjük alatta, de a fogalom ma már kiterjed minden fajta elektronikus kommunikációra ideértve a mobiltelefonok közötti beszélgetéseket,

[436]C-362/14. sz. ügy (Maximillian Schrems kontra Data Protection Commissioner). Az Európai Unió Bíróságának ítélete, 2015. október 6. Elérhető: https://curia.europa.eu/juris/liste.jsf?num=C-362/14 (letöltés dátuma: 2023. 05. 30.)

[437] C-311/18. sz. ügy (Data Protection Commissioner kontra Facebook Ireland Ltd és Maximillian Schrems. Az Európai Unió Bíróságának ítélete, 2020. július 16. Elérhető: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=HU (letöltés dátuma: 2023. 05. 30.)

[438] Big Brother Watch és társai kontra Egyesült Királyság, 58170/13, 62322/14 és 24960/15. számú ügyek. Emberi Jogok Európai Bírósága. 2018. augusztus–szeptember. Elérhető: https://hudoc.echr.coe.int/eng?i=002-12080 (letöltés dátuma: 2023. 06. 02.)

vezetékes telefonokat, az internetes hanghívásokat (*VoIP*[439]*), sőt a szöveges üzenetváltásokat, e-maileket is.[440] A lehallgatás rendszerint titkos adatszerzési módszer, amelyet a büntetőeljárásban csak szigorú garanciák mellett lehet alkalmazni. A Be. értelmében a telekommunikációs eszközökön folytatott kommunikáció lehallgatása azaz elektronikus hírközlési szolgáltatás keretében elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban megismerheti és rögzítheti, kizárólag bírói engedéllyel, meghatározott súlyos bűncselekmények esetén lehetséges, és ennek alkalmazásával a bűncselekménnyel összefüggő információ, illetve bizonyíték megszerzése valószínűsíthető.[441][442]Az engedélyt az ügyészség indítványára a bíró adja meg, általában legfeljebb 90 napos időtartamra, amely indokolt esetben meghosszabbítható.[443][444]A lehallgatás során a szolgáltatók együttműködnek a hatóságokkal, amelynél a telefontársaságok kötelesek biztosítani azt, hogy a kijelölt vonal forgalma rögzíthető legyen a hatóság által.[445] Technikailag összetettebb feladat az internetes kommunikáció lehallgatása (például az e-mail forgalom, az internetalapú csevegőprogramok (chat) üzeneteinek titkos megismerése) amelyet a hatóság a hálózati szolgáltató közreműködésével végez (pl. a szolgáltató szerverén átmenő adatforgalom másolásával), vagy az előzőekben említett információs rendszer titkos megfigyelése módszerével (amikor az érintett információs rendszerében (annak felhasználói oldalán) elhelyezett technikai eszközzel a kommunikáció tartalmát még a titkosítás előtt vagy után rögzítik) azonban mindkét esetben bírói engedély kell, a magántitokhoz tartozó adat titokban való megszerzése miatt.[446] A Nemzetbiztonsági Szakszolgálat (NBSZ) keretében (különösen a Technikai Felderítő Igazgatóság révén) mindkét fenti módszer alkalmazható, azaz a szolgáltató

**A VoIP jelentése: Voice over Internet Protocol, Ez azt jelenti, hogy a hagyományos telefonvonalak helyett az internetkapcsolatot használják a hanghívások lebonyolítására. Ilyenek például a WhatsApp hívások, Skype, Viber, Messenger hanghívások, Microsoft Teams, Zoom hívások stb.*

[440] Be. 231. § e).

[441] Be. 232. § (5) bek.

[442] Parti Katalin: Az elektronikus kommunikáció titkos megismerésével kapcsolatos jogszabályi garanciák Magyarországon. = Miskolci Jogi Szemle, 14. évf. 2. különszám 2. kötet (2019), 303–314. 304. o. Elérhető: https://www.mjsz.uni-miskolc.hu/files/6601/29_partikatalin_t%C3%B6rdelt.pdf, letöltés dátuma: 2022. 03. 13.

[443] Parti Katalin: Az elektronikus kommunikáció titkos megismerésével kapcsolatos jogszabályi garanciák Magyarországon. = Miskolci Jogi Szemle, 14. évf. 2. különszám 2. kötet (2019), 303–314. 304. o. Elérhető: https://www.mjsz.uni-miskolc.hu/files/6601/29_partikatalin_t%C3%B6rdelt.pdf, letöltés dátuma: 2022. 03. 13.

[444] Be. 239. § (1) bek.

[445] 2003. évi C. törvény az elektronikus hírközlésről 157. §

[446] Be. 231, 232. § (1) bek.

közreműködésével végzett adatmásolás vagy az információs rendszer felhasználói oldalán elhelyezett műszeres megfigyelés is lehetséges, ugyanakkor ezek a beavatkozások kizárólag megrendelés alapján történhetnek és szigorú bírói engedélyhez kötöttek, az alapjogi védelem és a magántitok védelmének biztosítása érdekében.[447][448] A lehallgatott kommunikáció tartalma a nyomozás szempontjából rendkívül értékes lehet. Gyakran közvetlen bizonyítékként is szolgálhat egy-egy tervezett vagy elkövetett bűncselekményre (ilyen például, ha a gyanúsított telefonon utasítást ad a bűntársának egy bűncselekményre, vagy utólag beszélnek a tett részleteiről, esetleg beismerő jellegű kijelentést tesznek). A lehallgatás vagy más leplezett eszköz alkalmazása esetén a hatóság jegyzőkönyvet vagy feljegyzést készít.[449] A jegyzőkönyvet, valamint a technikai eszközzel rögzített adatokat, továbbá a bírói engedélyt, az eljárás iratanyagába kell csatolni, ezek hivatalos bizonyítási eszközként szolgálnak.[450] A tárgyaláson a bíróság a lehallgatásból származó iratok lényegét ismerteti, indítványra a releváns részeket felolvassa, a hang- vagy képhang-felvételeket pedig bemutathatja.[451] [452]A védelem bizonyíték kirekesztése iránti indítvánnyal élhet, a bíróság pedig a bizonyítékokat szabadon értékeli, de nem értékelhet olyan bizonyítékot, amely tiltott módon, bűncselekménnyel vagy a felek eljárási jogainak lényeges sérelmével keletkezett.[453][454] Az elektronikus kommunikáció eredménye (mint irat/okirat vagy elektronikus adat) bizonyítási eszköz lehet.[455] Ezen bizonyítékok elfogadhatóságának megítélésénél nemcsak a magyar büntetőeljárási jogszabályok irányadók, hanem az Emberi Jogok Európai Bíróságának (EJEB) gyakorlata is, amely meghatározza az ilyen típusú elektronikus bizonyítékok felhasználásának nemzetközi mércéjét. Az EJEB szerint az elektronikusan rögzített kommunikáció bizonyítékként felhasználható a büntetőeljárásban, azonban önmagában a beszerzés jogellenessége nem vezet automatikusan a kizárásához. A döntő az, hogy az eljárás egésze megfelelt-e az Emberi Jogok Európai Egyezménye 6. cikkében rögzített tisztességes eljárás követelményeinek

[447] Nbtv. 53. § (1) bek.
[448] Nemzetbiztonsági Szakszolgálat: Szervezeti felépítés. Elérhető: https://nbsz.gov.hu/rolunk/szervezeti-felepites
[449] Be. 243. § (1)
[450] Be. 249. § (1)
[451] Be. 531. §
[452] Be. 532. §
[453] Be. 167. § (5)
[454] Be. 505. §
[455] Be. 165. §

(lásd.:*Schenk v. Switzerland, 1988*; *Khan v. United Kingdom, 2000)*.[456][457] A Bíróság minden esetben vizsgálja a jogszerűséget, hogy a bizonyíték beszerzése megfelelt-e a nemzeti jogszabályoknak, az eredetet, hogy hitelt érdemlően igazolható-e, hogy a rögzített tartalom az adott személytől származik, és a sértetlenséget, hogy a rögzítés óta a tartalom sértetlen maradt-e, továbbá, hogy ezekre a pontokra a nemzeti bíróságok érdemben reagáltak-e.[458][459] (lásd.:*Dragojević v. Croatia*, *2015*; *Roman Zakharov v. Russia, 2015*). Ezen nemzetközi mércék a magyar jogalkalmazásban is irányadók, mivel a Büntetőeljárási törvény 167. § (5) bekezdése tiltja a tiltott módon, bűncselekménnyel vagy a résztvevők eljárási jogainak lényeges sérelmével beszerzett bizonyítékok értékelését.[460] Napjainkban a lehallgatás hatékonyságát csökkenti a felek között fennálló kommunikáció titkosítása. A modern üzenetküldő alkalmazások többsége (például a Signal, a WhatsApp vagy a Viber stb.) végponttól végpontig terjedő titkosítást alkalmaz, amelynek következtében a hálózaton lehallgatott adatfolyam a tartalom ismerete nélkül értelmezhetetlen.[461] Emiatt a bűnüldöző hatóságok világszerte keresik a jogszerű és technikailag megvalósítható módszereket az ilyen kommunikációkhoz való hozzáférésre. Indokolt arra a következtetésre jutni, hogy a lehallgatás továbbra is nélkülözhetetlen eszköze a XXI. századi bűncselekmények nyomozásának, azonban a titkosítás és más technológiai akadályok miatt egyre inkább szükség van a különböző eszközök és módszerek kombinációjára.

5.3.3. Adatszerző tevékenység

[456]Európai Emberi Jogi Bíróság: *Schenk kontra Svájc* (10862/84), ítélet, 1988. július 12.). Elérhető: https://hudoc.echr.coe.int/tur?i=001-57572 (letöltés dátuma: 2023. 08. 11.)
[457]Európai Emberi Jogi Bíróság*: Khan kontra Egyesült Királyság* (35394/97), ítélet, 2000. május 12. Elérhető: https://hudoc.echr.coe.int/eng?i=001-58841 (letöltés dátuma: 2023. 08. 11.)
[458]Európai Emberi Jogi Bíróság: *Dragojević kontra Horvátország* (68955/11) ítélet, 2015. január 15. Elérhető: https://hudoc.echr.coe.int/fre?i=002-10328 (letöltés dátuma: 2023. 08. 11.)
[459]Európai Emberi Jogi Bíróság: *Roman Zakharov kontra Oroszország* (47143/06), ítélet, Nagykamara, 2015. december 4. Elérhető: https://hudoc.echr.coe.int/fre?i=001-159324 (letöltés dátuma: 2023. 08. 11.)
[460] Be. 167. § (5)
[461]Afreen, Afreen – Ivaturi, Shalini: *A Systematic Literature Review on End-to-End Cryptographic Protocols in Secure Messaging Applications*. 2025. július 13. SSRN. Elérhető: http://dx.doi.org/10.2139/ssrn.5357785 (letöltés dátuma: 2025. 07. 18.)

Nyeste Péter és Szendrei Ferenc: A bűnügyi hírszerzés kézikönyvében az adatgyűjtés fogalmát a rendőrség bűnüldözési célú, titokban folytatott információszerző tevékenységeként határozza meg.[462] Hangsúlyozandó, hogy az ilyen jellegű tevékenység legitimációját elsősorban az arányosság és a szükségesség elve biztosítja továbbá az információs önrendelkezési jogról szóló 2011. évi CXII. törvény (Infotv.) bűnüldözési adatkezelésre vonatkozó és a Be. -vel összhangban alkalmazandó szabályai.[463] E körben külön figyelemmel kell lenni arra, hogy a bűnüldözési célú adatkezelésre nem az általános adatvédelmi rendelet (GDPR) alkalmazandó (GDPR 2. cikk (2) bekezdés d) pont), hanem a 2016/680/EU irányelv végrehajtásaként az Infotv. kifejezetten bűnüldözési fejezete, amely az érintettek jogainak érvényesülését is garantálják, mindenekelőtt a célhoz kötöttség és a törléshez való jog (mint személyhez fűződő jog) biztosítása révén, amelyeket a Be. kifejezetten is rögzít.[464][465][466]Az ilyen módon megszerzett adatoknak nem csupán a beszerzése, hanem a bizalmassága is egyaránt fontos, amelyet a kézikönyv is kiemel, akként, hogy a végrehajtás és az adatok felhasználása során gondoskodni kell arról, hogy az adatok ne váljanak jogosulatlan személyek számára elérhetővé, az adatszolgáltatás kapcsán pedig a Be. külön titoktartási klauzulát ír elő.[467][468] A Be. az adatszerző tevékenységet (VII. fejezet) több elemre bontja: adatkérés (Be. 261–265. §), feltételes adatkérés (Be. 266. §), adatgyűjtés (Be. 267. §) és egyéb adatszerző tevékenység (Be. 268-270.§).[469][470][471][472] Az adatkérés keretében a hatóság a törvényi felhatalmazás alapján kérhet adatokat állami nyilvántartó szervektől, hivataloktól vagy

[462]Nyeste Péter – Szendrei Ferenc: *A bűnügyi hírszerzés kézikönyve*. Budapest, Dialóg Campus Kiadó, 2019.
[463]Az információs önrendelkezési jogról szóló 2011. évi CXII. törvény (Infotv.)
[464]Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR), HL L 119, 2016.5.4., 1–88. o., 2. cikk (2) bekezdés d) pont.
[465] a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről. HL L 119, 2016.5.4., 89–131. o.
[466] Be. 264. § (4) – (6).
[467]Nyeste Péter – Szendrei Ferenc: *A bűnügyi hírszerzés kézikönyve*. Budapest, Dialóg Campus Kiadó, 2019.
[468]Be. 264. § (7) – (8)
[469]Be. 261–265.§
[470]Be. 266. §
[471]Be. 267. §
[472]Be. 268.-270 §

magánszolgáltatóktól.[473][474] A kérelem kötelező tartalmi elemeit a Be. 261. § (5) bekezdése sorolja fel, minthogy a cél, a jogalap, az azonosító adatok, a kért adatkör, a teljesítés módja és a határideje.[475] A különösen érzékeny adatforrásoknál ügyészi engedély szükséges, így különösen az elektronikus hírközlési szolgáltató, postai szolgáltató és közreműködő, bank-, fizetési-, értékpapír-, pénztár- vagy biztosítási titkot kezelő szervezet (ilyen adatra), egészségügyi és kapcsolódó személyes adatot kezelő szervezet tartozik e körbe.[476] Sürgős esetben előzetes engedély nélkül is kérhető az adatszolgáltatás, de az ügyészi engedélyt utólag haladéktalanul be kell szerezni és jogkövetkezményként az így megszerzett adat törlését kötelező elrendelni, ha az ügyészség a sürgősségi megkeresést utóbb nem engedélyezi, vagy az adatszerzés a meghatározott ügyészi engedély kereteit túllépve valósult meg, az ilyen adatok bizonyítékként nem használhatók fel.[477][478][479]A súlyos bűncselekményeknél az ügyész keretengedélyt is adhat, amely alatt a nyomozó hatóság egyedileg külön ügyészi engedély nélkül kérhet adatot ilyen esetben az ügyész utólagos felülvizsgálata előfeltétele a bizonyítékként felhasználásnak.[480] Kiemelendő, hogy azon esetekben, amikor az adatszerzés a meghatározott ügyészi engedélyben foglaltak kereteit meghaladva valósult meg, akkor az így jogszerűtlenül megszerzett adat törlését a jogszabály kötelezően előírja.[481]Az adatszolgáltatás határideje elektronikus kérelemnél legalább 1, legfeljebb 30 nap, egyéb úton legalább 8, legfeljebb 30 nap.[482]A megkeresett szervezet köteles teljesíteni, ugyanakkor csak az elengedhetetlenül szükséges személyes adat kérhető, és a célhoz nem kapcsolódó személyes adatot haladéktalanul törölni kell, az eredeti iratot legkésőbb az eljárás befejezésekor vissza kell küldeni.[483][484][485][486] A nemteljesítés, alaptalan megtagadás vagy a titoktartási kötelezettség megsértése rendbírsággal

---

[473]Nyeste Péter – Szendrei Ferenc: *A bűnügyi hírszerzés kézikönyve*. Budapest, Dialóg Campus Kiadó, 2019.
[474] Be. 261. § (1), (4)
[475] Be. 261. § (5)
[476] Be. 262. § (1)
[477] Be. 262. § (4) a)
[478] Be. 262. § (4) b)
[479] Be. 262. § (4) c), (5)
[480] Be. 262/A. §
[481] Be. 262/A. § (3) – (4)
[482] Be.263. § (2)
[483]Be. 264. § (1) –(3)
[484]Be. 264. § (4)
[485]Be. 264. § (5)
[486]Be. 264. § (6)

szankcionálható, ha a törvény kizárja a teljesítést, további kényszerintézkedés nem végezhető az adott szervezetnél az adat megszerzésére.[487][488]A Be. továbbá lehetővé teszi önkéntes teljesítésre felhívás alkalmazását is szankció kilátásba helyezése nélkül.[489] A feltételes adatkérés esetén a meghatározott feltétel bekövetkezésére előre beállított, időben korlátozott (max. 1 év) adatszolgáltatás állami vagy közfeladatot ellátó szervektől, a feltétel beálltával a megkeresett szerv haladéktalanul teljesít, ennek hiányában a megjelölt adatokat törli.[490] Az adatgyűjtés a bűncselekmény gyanújának megállapítására, illetve a bizonyítási eszközök létének és helyének tisztázására szolgál, amelynek eszközei a hatósági nyilvántartásokból, a nyilvános forrásokból való adatok gyűjtése, személy illetőleg tárgy kiválasztatása-azonosítása kép- vagy hangfelvétellel, a helyszín megvizsgálása továbbá bárkitől felvilágosítás kérése.[491] Az eljárásról feljegyzés készül, amely közlés vallomásként csak fenntartás esetén használható.[492] Vádemelés után az ügyész is végezhet adatgyűjtést, a vagyonelkobzás alá eső dolog vagy vagyon felderítése és biztosítása elősegítésére is.[493] Az egyéb adatszerző tevékenység körében a Be. elrendeli többek között a tárgy (dolog) vagy személy, vagy holttest körözését és annak rendjét, továbbá lehetővé teszi a biometrikus nyilvántartásokból történő adattovábbítást, arcképelemzési tevékenység igénybevételét, illetve a Schengeni Információs Rendszerben (SIS) figyelmeztető jelzés elhelyezését.[494][495] Vádemelés után ezek közül bizonyosakat az ügyész a bizonyítás érdekében maga is kérhet.[496] E szabályok gyakorlati érvényesülését a szaktanácsadó közreműködése is előmozdítja, amikor a bizonyítás szakszerű lefolytatásához nélkülözhetetlen ismereteket biztosít. Igénybevétele a bizonyítási eszközök felderítéséhez, felkutatásához, megszerzéséhez rögzítéséhez szükséges különleges szakismeret biztosítására szolgál továbbá közreműködésének ténye és tartalma jegyzőkönyvben, feljegyzésben rögzítendő, és tanúként kihallgatható.[497]

[487]Be. 265. § (1)
[488]Be. 265. § (2)
[489]Be. 265/A. §
[490]Be. 266. §
[491]Be. 267. §
[492]Be. 267. § (4) – (5)
[493]Be. 267. § (2)
[494]Be. 268. §
[495]Be. 269. §
[496]Be.269. § (2)
[497]Be. 270. §

Az adatszerző tevékenység szabályozása a hatályos Be. -ben csak a korábbi rendelkezésekkel összevetve érthető meg teljeskörűen. A korábbi büntetőeljárási törvény (1998. évi XIX. törvény) a nyomozó hatóság egyéb adatszerző tevékenységeként ezt „megkeresésnek" nevezte és lehetőséget nyújtott például telefonszolgáltatók, bankok, utazási irodák adataihoz való hozzáférésre.[498] A szabályozás szerint „a bíróság, az ügyészség és a nyomozó hatóság állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és egyesületet kereshet meg a tájékoztatás adása, az adatok közlése, átadása, illetőleg az iratok rendelkezésre bocsátása végett, és ennek a teljesítésére legalább nyolc, legfeljebb harminc napos határidőt állapíthat meg".[499] A jogszabály rögzítette továbbá azt, hogy a megkeresés a személyes adatok közlésére csak olyan körben terjedhet ki, amely „a megkeresés céljának megvalósításához elengedhetetlenül szükséges" és a kért adatok körét, valamint az adatkezelés pontos célját meg kellett jelölni.[500] Amennyiben a megkeresés során olyan személyes adat jutott a hatóság tudomására, amely a megkeresés céljával nem függött össze, azt törölni kellett.[501] Ezzel szakított a jelenleg hatályos 2017. évi XC. törvény (az új Büntetőeljárási törvény, „Be.") ugyanis ezt a jogintézményt új koncepció mentén vezette be adatkérés néven. Ez alapján a nyomozó hatóság ügyészi engedéllyel kérhet adatokat olyan szervezetektől, amelyek vélhetően rendelkeznek a nyomozás szempontjából releváns információval (pl. banki tranzakciók, híváslisták, cellainformációk, utazási adatok, internetes szolgáltatói fiók információk).[502] Az adatkérésnek arányosnak kell lennie (csak a szükséges információkat kérhetik el, figyelembe véve az adatvédelmi szempontokat) és az így kapott adatok a nyomozati iratok részeként bizonyítékként használhatók fel. A bűnüldözés eszköztára kettős. Egyrészt a Be. VII. Fejezetben szabályozott adatszerző tevékenység révén, másrészt a Be. VIII. Fejezetben meghatározott, bírói engedélyhez kötött leplezett eszközök útján szerezhetők be az adatok, ha a bizonyítás érdeke ezt indokolja. Az adatszerző tevékenység rendszerint nyílt, illetve ügyészi engedélyhez kötött forma, amelynek keretében a hatóság a különböző nyilvántartásokból, adatbázisokból vagy szolgáltatóktól kérhet adatot, illetve végezhet adatgyűjtést. Ezzel szemben a leplezett eszközök a titkos információszerzés

[498]1998. évi XIX. törvény a büntetőeljárásról. (régi Be.) 178. § (1), (2) bek.
[499]1998. évi XIX. törvény a büntetőeljárásról. (régi Be.) 71. § (1) bek.
[500]1998. évi XIX. törvény a büntetőeljárásról. (régi Be.) 71. § (3) bek.
[501]1998. évi XIX. törvény a büntetőeljárásról. (régi Be.) 71. § (4) bek.
[502]Be. 341. §

körébe tartoznak. Az alkalmazásuk minden esetben bírói engedélyhez kötött, és olyan jelentős beavatkozást testesítenek meg az érintettek alapjogaiba, amelyet kizárólag a legsúlyosabb bűncselekmények felderítése és bizonyítása érdekében lehet elrendelni. A két jogintézmény közötti határvonal tehát egyúttal garanciális funkciót is betölt, hiszen világosan elválasztja a nyílt adatkezelési módokat a titkos megfigyelési eszközöktől. E különbségtételt követően a vizsgálat az alkalmazási módok belső tagolására irányul. A bírói engedélyhez kötött leplezett eszközök bizonyos pontokon összefonódhatnak a lehallgatás és a megfigyelés eseteivel, és ide tartozik minden olyan (többek között technikailag online) információszerzés, amikor a hatóság rejtett módon szerez meg adatot anélkül, hogy feltétlenül élő kommunikációt hallgatna le. Ilyen lehet például a felhőszolgáltatónál tárolt adatok titkos megismerése vagy egy felhasználói fiók (pl. e-mail) tartalmának a bírói engedéllyel, leplezett eszköz alkalmazása keretében történő megismerése. A módszertani spektrum másik végpontját azonban az eszköz tényleges hozzáférhetősége jelöli, amelyre eltérő eljárási rend vonatkozik. Amennyiben az informatikai eszköz a hatóság közvetlen tényleges rendelkezésére kerül (fizikai birtokbavétel), az érintett helyen vagy személynél végzett kutatás és a lefoglalás szabályai irányadók, különös tekintettel az elektronikus adatra vonatkozó rendelkezésekre. [503][504] Az elektronikus adat önálló bizonyítási eszköz, amely lefoglalható többek között másolat készítésével is, valamint a Be. külön jogintézménye az elektronikus adat megőrzésére kötelezés.[505] Ezzel szemben a távoli (online) hozzáférés a leplezett eszközök körébe tartozó információs rendszer titkos megfigyelése.[506] Ilyen megfigyelés esetén a leplezett eszköz alkalmazására feljogosított szerv bírói engedéllyel az információs rendszerben kezelt adatokat titokban megismerheti, az észlelteket technikai eszközzel rögzítheti. Tekintettel arra a célra, hogy az ehhez szükséges elektronikus adat az információs rendszerben elhelyezhető, a szükséges technikai eszköz (a nyilvános vagy a közönség részére nyitva álló hely kivételével) lakásban, egyéb helyiségben, bekerített helyen, valamint (a közösségi közlekedési eszköz kivételével) járműben, továbbá az érintett személy használatában lévő tárgyban elhelyezhető. Ennek alkalmazása nem azonos a fizikai birtokbavétellel járó kutatás vagy lefoglalás eseteivel, tekintettel arra, hogy a

[503]Be. 231–236. §
[504]Be. 315–316. §
[505]Be. 315–316. §
[506]Be. 231–234. §

távoli, titkos hozzáférés kizárólag a leplezett eszközökre vonatkozó garanciák (bírói engedély, időbeli és tárgyi korlátok, arányosság) mellett engedélyezhető. [507][508] Az elektronikus adat lefoglalása több módon végrehajtható, az elektronikus adatról másolat készítésével, az elektronikus adat áthelyezésével, az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével, az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy a jogszabályban meghatározott más módon.[509] Fizetésre használt elektronikus adat esetén a lefoglalás végrehajtható úgy is, hogy az érintett rendelkezési lehetőségét akadályozzák meg.[510] Ha az elektronikus adat iratnak minősül, a 313–314. § szabályai megfelelően alkalmazandók.[511] A lefoglalást úgy kell végrehajtani, hogy lehetőleg ne terjedjen ki a büntetőeljárás céljából szükségtelen elektronikus adatra, illetve az ilyen adatot a lefoglalás a legrövidebb ideig érintse.[512] Információs rendszer vagy adathordozó lefoglalása akkor alkalmazható, ha az elkobozható vagy vagyonelkobzás alá esik, vagy tárgyi bizonyítási eszközként bír jelentőséggel, vagy a bizonyítás érdekében a benne tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálása szükséges.[513] Ha ez az eljárás érdekét nem veszélyezteti, a lefoglalás esetén az elektronikus adatra jogosult kérelmére a megjelölt elektronikus adatról másolatot kell készíteni.[514] A megőrzésre kötelezés önálló eszköz a bűncselekmény felderítése, bizonyítási eszköz felderítése vagy biztosítása, illetve a gyanúsított kilétének vagy tényleges tartózkodási helyének megállapítása érdekében rendelhető el. Ezen határozat korlátozza a megőrzésre kötelezett (birtokos, feldolgozó, kezelő) rendelkezési jogát az érintett elektronikus adat felett.[515] A megőrzésre kötelezést a bíróság, ügyészség vagy nyomozó hatóság rendelheti el.[516]A megőrzésre kötelezett a közléstől köteles az érintett elektronikus adatot változatlanul megőrizni, szükség esetén elkülönítve, biztonságos tárolásról gondoskodni, és megakadályozni a megváltoztatást, törlést, megsemmisülést, továbbítást, jogosulatlan másolatkészítést vagy jogosulatlan hozzáférést.[517] Az elrendelő

[507]Be. 231-236.§
[508]Be.232.§ (1)
[509]Be. 315. § (1)
[510]Be. 315. § (2)
[511]Be. 315. § (3)
[512]Be. 315. § (4)
[513]Be. 315. § (5)
[514]Be. 315. § (6)
[515]Be. 316. § (1) – (3)
[516]Be. 316. § (2)
[517]Be. 316. § (4)

a megőrzéssel érintett adatot minősített vagy a minősített tanúsítványon alapuló fokozott biztonságú e-aláírással illetőleg bélyegzővel elláthatja.[518] Ha az eredeti helyen való megőrzés az érintett tevékenységét jelentősen akadályozná, az elrendelő engedélyével az adat más rendszerre vagy adathordozóra másolható, és ezt követően az eredetire vonatkozó korlátozások részben vagy teljesen feloldhatók.[519] A megőrzéssel érintett adathoz a kényszerintézkedés tartama alatt kizárólag a bíróság, az ügyészség, a nyomozó hatóság, valamint az elrendelő engedélyével a megőrzésre kötelezett férhet hozzá amely esetében a tájékoztatás is csak az elrendelő engedélyével adható.[520] Haladéktalanul tájékoztatni kell az elrendelőt, ha jogosulatlan változtatás, törlés, megsemmisítés, továbbítás, másolás, megismerés történt vagy annak kísérlete észlelhető.[521] A megőrzést elrendelő haladéktalanul megkezdi az adatok átvizsgálását, amelynek eredményeként dönt a lefoglalás más módjának elrendeléséről vagy a megőrzés megszüntetéséről.[522] A megőrzés legfeljebb három hónapig tart amely megszűnik a büntetőeljárás befejezésével és amelyről az érintettet tájékoztatni kell.[523] A Büntetőeljárási törvény az elektronikus adat ideiglenes hozzáférhetetlenné tételét két módon szabályozza.[524]Az elektronikus adat ideiglenes eltávolításával és az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával (úgynevezett ‘blokkolással’) amely mindkettő esetben határozattal rendelhető el. [525][526] A ‘blokkolás’ végrehajtását a bíróság haladéktalanul közli a Nemzeti Média- és Hírközlési Hatósággal (NMHH), amely a végrehajtást szervezi és ellenőrzi, bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába, és értesíti az elektronikus hírközlési szolgáltatókat, akik egy munkanapon belül kötelesek a hozzáférést megakadályozni, illetve a megszűnéskor visszaállítani.[527]

5.4. A technológiai alapú bizonyítékok nyomozati felhasználhatóságának kérdései

[518]Be. 316. § (5)
[519]Be. 316. § (6)
[520]Be. 316. § (7)
[521]Be. 316. § (8)
[522]Be. 316. § (9)
[523]Be. 316. § (10)
[524]Be. 335–338. §
[525]Be 336. §
[526]Be.337. §,
[527]Be. 337. § (3) – (4), (8), (11)

A technológián alapuló bizonyítékok nyomozati felhasználhatósága alatt azt értjük, hogy az így megszerzett információk mennyiben illetőleg hogyan használhatók fel a büntetőeljárás során a tényállás megállapítására. E kérdéskör több aspektust foglal magában, mint a jogszerűség, megbízhatóság, értékelhetőség és gyakorlati kezelhetőség. Bármilyen bizonyíték csak akkor használható fel, ha törvényes módon jutott a hatóság tudomására. A bizonyítás törvényességének elve szerint a bizonyítási eszközök felderítése, összegyűjtése, biztosítása és felhasználása a törvény rendelkezései szerint történik, és nem értékelhető olyan bizonyíték, amelyet bűncselekmény útján, más tiltott módon vagy a büntetőeljárási jogok lényeges sérelmével szereztek meg.[528][529] Emellett a bizonyítás alapvetéseihez tartozik a nemo tenetur és az in dubio pro reo is.[530] Az online környezetben ez azt jelenti, hogy például engedély nélküli információs rendszeren belüli beavatkozással (a már említett Be. szerinti bírói engedélyes „információs rendszer titkos megfigyelése" nélkül) beszerzett adatok felhasználhatósága kizárt.[531][532] Ha például a nyomozó hatóság egy számítógépet jogosulatlanul hackel meg, vagy egy okoseszköz tartalmát illegális módon szerzi meg, az így nyert adatok felhasználhatósága erősen korlátozott. A magyar bírói gyakorlat az elmúlt években egyre szigorúbbá vált az illegálisan beszerzett bizonyítékok kizárása terén, amely összeegyeztethető a bizonyítási eszközök szabad mérlegelésének elvével, amennyiben a bíróság a tisztességes eljáráshoz fűződő jogot magasabb rendűnek tekinti a bizonyítás szabadságánál.[533] A nyomozati felhasználhatóság másik kulcsa a hitelesség. Ahogy azt az előző fejezetekben is tárgyaltuk, biztosítani kell az adatok integritását (változatlanságát) és azt, hogy egyértelmű legyen az eredetük. Tegyük fel, hogy egy lefoglalt számítógépen találnak egy gyanús dokumentumot, de nem lehet teljesmértékben kizárni azt, hogy azt feltehetően utólag másolta oda egy adott személy (tekintettel arra, hogy a lefoglalás után nem zárták le megfelelően a gépet), akkor ez az információ a nyomozásban csak korlátozottan értékelhető. A Be. önálló bizonyítási eszközként nevesíti az elektronikus adatot és kimondja, hogy ahol a törvény tárgyi bizonyítási eszközt említ, azon (eltérő rendelkezés

[528]Be. 166. §
[529]Be. 167. § (5)
[530]Be. 7. § (3) – (4)
[531]vö. Be. 231–234. §, 232. §
[532]Be. 232. §
[533]Bérces Viktor: *Chapters from the Scope of Hungarian Criminal Law and Criminal Procedure Law*. Forum Iuris, Cluj-Napoca, 2024. 97–101.p

hiányában) az elektronikus adatot is érteni kell.[534][535][536] A szemle- és rögzítési szabályok a digitális bizonyítékok felkutatásának, rögzítésének és megőrzésének ellenőrizhetőségét szolgálják, ezáltal biztosítva a digitális integritást. Ennek technikai garanciája a hash-érték („digitális ujjlenyomat”), vagyis az adott adatállományból képzett egyedi kivonat, amely a bizonyíték eredetiségének és változatlanságának igazolására szolgál. Ez egy adatból készített rövid, fix hosszúságú kód. Amennyiben az adaton akár egy bitet is változtatnak úgy, teljesen más lesz a hash, hash láncolat (hash láncolat: „egymáshoz fűzött ujjlenyomatok sorozata”). Minden elem tartalmazza az előző elem hashét, ezért, (ha valaki egy korábbi elemet átír, a lánc „elszakad”, és az azonnal észrevehető) dokumentálását is megköveteli a hitelesség alátámasztására.[537][538] A már említett feltevésünkhöz visszatérve a hitelesség alátámasztásából kifolyólag fontos, hogy már a nyomozati szakban felmérésre kerüljön, hogy az adat integritása, hogy sértetlen és eredeti ugyanis, ha az integritás vagy eredet tisztázatlan, a bizonyító erő sérül. Az ilyen esetekre a hash értékek és egyéb ellenőrző mechanizmusok alkalmazása zsinórmértékül szolgálhat ugyanis egy e-mail fejlécét elemezve a szakértő megállapítja, hogy azt valóban a gyanúsított postafiókjából küldték, adott időben, akkor ez erős hitelességi bizonyíték, amelyre a nyomozó hatóság építhet.[539] Amennyiben viszont kétség marad fenn e körben (pl. mert lehetett manipulálni a fejlécet), akkor óvatosabban kell kezelni az így nyert adatot, és további bizonyítékokkal alátámasztani.[540][541] Az elektronikai vonatkozású esetleges bizonyítékok számos esetben további értelmezést tehetnek szükségessé ahhoz, hogy a nyomozásban felhasználhatók legyenek. A Be. 183. § (1) bekezdése szerint a bíróság, az ügyészség és a nyomozó hatóság szakértőt rendel ki, ha a bizonyítandó tény megítéléséhez különleges szakértelem szükséges.[542]Egy titkosított fájl, egy bonyolult logfájl részlet vagy az ilyen jellegű adatok vizsgálata interdiszciplináris feladat, amely a

[534]Be. 165. § f)
[535]Be. 205. §
[536]Be. 205. § (2)
[537]Be. 207. § (2)
[538]Ayers, Rick – Brothers, Sam – Jansen, Wayne: *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101, Rev. 1, National Institute of Standards and Technology, Gaithersburg, 2014. DOI: 10.6028/NIST.SP.800-101r1. (letölthető: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf)
[539]Herédi István: *A nyílt forrású adatgyűjtés szerepe a kiberbűncselekmények felderítésében*, Rendőrségi Tanulmányok 2022/3., 30–69. o.
[540]Be. 165.-166. §
[541]Be. 7 §
[542]Be. 183. § (1)

nyomozói munka és az informatikai szakértés összehangolt alkalmazását követeli meg. A szakértői vélemény ugyanakkor jellemzően a nyomozás vége felé készül el, így a nyomozati cselekmények során előzetes informális konzultációkra, technikai tanácsokra is szükség lehet. A bizonyítékok felhasználhatóságát érdemben növeli, ha a nyomozói munkát megfelelő digitális kompetenciák és/vagy informatikai szakértői támogatás kíséri ennek okán a rendelkezésre álló adatok jelentősége pontosan azonosítható és az ügy összefüggéseibe illeszthető. Ezért is indokolt, hogy a nyomozók legalább alapvető ismeretekkel rendelkezzenek az elektronikus adatokra vonatkozó bizonyítékok természetéről amint erre Peszleg Tibor is rámutat.[543] Az ügy sajátosságától függően gyakori az együttműködés a nyomozó és az igazságügyi informatikus szakértő között. A nyomozó gyakorlati kérdéseket tesz fel (például: „Mit jelez az adott időbélyeg?"; „Felmerül-e a távoli törlés lehetősége?"), a szakértő pedig (még a formális szakvélemény előtt) segít a válaszok megalapozásában. Ez az együttműködés érdemben növeli annak esélyét, hogy az elektronikus adattal kapcsolatos bizonyítékokat helyesen értékeljék és a nyomozásban megfelelően használják fel.

A bizonyítékok felhasználhatóságát számos gyakorlati tényező is befolyásolja. Ide tartozik többek között az adatok mennyisége (a modern bűnügyekben sokszor „terabyte" -nyi (TB.) adatot foglalnak le), amelynek átvizsgálása időigényes, és a nyomozás határidőjének szűkösségét is fokozhatja. Ezen probléma rendszerszinten is tetten érhető amelyet a HMICFRS (His Majesty's Inspectorate of Constabulary and Fire & Rescue Services) országos ellenőrző jelentése is szemléltet, amely szerint 2022 augusztusára több mint 25 000 eszköz várt kivizsgálásra az angol–walesi rendőri erőknél, ami két év alatt 32%-os növekedést mutatott.[544] A bemutatott tendencia nem sajátosan brit jelenség, hanem az európai gyakorlatban is megjelenő probléma, amely releváns összehasonlítási alapot kínál a jelenség nagyságrendjének érzékeltetésére. A hazai rendészeti szakirodalom (különösen a Belügyi Szemle) szintén ezt rögzíti, amely szerint a digitális bizonyítékok mennyisége és relevanciája bővül, miközben az országos, eszközszintű

[543]Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek Lapja, 2010/2.
[544]HMICFRS: *An inspection into how well the police and other agencies use digital forensics in their investigations* (2022). Elérhető: https://hmicfrs.justiceinspectorates.gov.uk/publication-html/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/ (letöltés dátuma: 2024. 08. 11.)

statisztikák csak szórványosan hozzáférhetők.[545]Az érdemi információk kiszűrésére a hatóságok egyre gyakrabban alkalmaznak automatizált keresőeszközöket (pl. kulcsszavas keresés, adatbányászat), ennek ellenére nem zárható ki, hogy a bizonyítékok relevanciája csak utóbb kerül felszínre.[546]Szemléltető példaként szolgál az, ha egy gyanúsított telefonján több ezer chatüzenet lelhető fel, és ezek közül kizárólag a szakértői vizsgálat deríti ki, hogy egy korai üzenet alapvető alibit támaszt alá, avagy a bűnösségre utal.[547] Mindez szükségessé teszi, hogy a nyomozás folyamán a bizonyítékokat a változó tényállási képhez igazodva ismételten értékeljék.[548][549]További kihívást hordozhat a titkosítás különösen, ha egy merevlemez teljes (lemezes és végpontok közötti, E2EE) egészében titkosítva van, ugyanis a lefoglalás önmagában nem garantálja, hogy a nyomozó hatóság ténylegesen hozzáfér az adatokhoz. Ezt a gyakorlati tapasztalatot az EU Innovációs Hub Encryption Reportja is megerősíti, rámutatva, hogy az e-Evidence-reform nem kezeli érdemben az ebből fakadó korlátot. [550] Ilyenkor vagy a gyanúsított együttműködésére (pl: jelszó kiadására) van szükség, vagy speciális támadási módszerekre, amelyek azonban idő- és erőforrás-igényesek, és nem garantált a sikerük. A titkosított, hozzáférhetetlen adat olyan, mintha ott se lenne, így a nyomozati felhasználhatóság szempontjából ez komoly akadály.[551] Ide kapcsolódik a szolgáltatói együttműködés kérdése is ugyanis egyre több adat van külföldi szolgáltatók (Google, Facebook stb.) szerverein, amelyek kiadásához nemzetközi jogsegély kell. Ezt a

---

[545]Gaál, Tibor (2018): A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban. Belügyi Szemle, 2018/7–8., 22–35. DOI: 10.38146/BSZ.2018.7-8.2.

[546]NIST: *NISTIR 8354: The Emergence of Locally Available Anti-Forensic Capabilities: A State of the Art Survey*. Elérhető: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf (letöltés dátuma: 2024. 08. 11.)

[547]Be. 188. § (1)

[548]ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence. Genf, ISO, 2015.

[549]Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek Lapja, 2010/2.

[550]EU Innovation Hub: First Report on Encryption (Europol, Eurojust, European Commission's Directorate-General for Migration and Home Affairs (DG HOME), European Commission's Joint Research Center (JRC), European Council's Counter-Terrorism Coordinator, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA). 2024. Elérhető: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf (letöltés dátuma: 2025. 01. 11.)

[551]EU Innovation Hub: First Report on Encryption (Europol, Eurojust, European Commission's Directorate-General for Migration and Home Affairs (DG HOME), European Commission's Joint Research Center (JRC), European Council's Counter-Terrorism Coordinator, European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA). 2024. Elérhető: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf (letöltés dátuma: 2025. 01. 11.)

problémát felismerve az EU 2018-ban előterjesztette az e-bizonyíték rendelet és irányelv javaslatát, amely lehetővé tenné, hogy a tagállamok hatóságai közvetlenül, gyorsított eljárásban kérhessenek adatkiadást a szolgáltatóktól ezzel forradalmasítva a határokon átnyúló elektronikus bizonyítékgyűjtést.[552] Az említett problémakör kezelésére az Európai Unió 2023-ban elfogadta az ún. e-Evidence csomagot. Ennek központi eleme a 2023/1543/EU rendelet, amely bevezeti az európai adatkiadási és adatmegőrzési határozatok (European Production and Preservation Orders: EPOC/EPOC-PR) intézményét.[553] A rendelet rendelkezései 2026. augusztus 18-tól alkalmazandók, a szolgáltatók számára pedig főszabály szerint tíznapos, sürgős esetekben nyolcórás válaszhatáridőt írnak elő illetőleg ezen részletszabályokat és határidőket az Európai Bizottság hivatalos összefoglalója is megerősíti.[554] A csomag kiegészítő elemeként a 2023/1544/EU irányelv kötelezi a szolgáltatókat arra, hogy uniós jogi képviselőt vagy kijelölt telephelyet létesítsenek, ezzel biztosítva az intézkedések átvételének és teljesítésének hatékony gyakorlati megvalósítását.[555] Nemzetközi kitekintésben e szabályozási törekvésekhez illeszkedik az Európa Tanács keretében elfogadott Budapesti Egyezmény második kiegészítő jegyzőkönyve (2022), amely a szolgáltatókkal való közvetlen együttműködési csatornákat erősíti a határokon átnyúló ügyekben.[556] A hagyományos jogsegély gyakran lassú (hónapokig eltarthat), miközben az eljárás határideje szoríthat így, ezek fő célja, hogy az elektronikus adatokkal kapcsolatos bizonyítékok a nyomozás során időben hozzáférhetővé váljanak, hiszen mit sem ér egy adat, ha azt csak a nyomozás befejezése után kapja meg a hatóság.

---

[552]Dornfeld László: A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az EU-ban. *Infokommunikáció és Jog*, 2019/2., 37–42. o.

[553]Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról, HL L 191, 2023.7.28., 118–180. o.; alkalmazandó: 2026. aug. 18

[554]Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról, HL L 191, 2023.7.28., 118–180. o.; alkalmazandó: 2026. aug. 18

[555]Az Európai Parlament és a Tanács (EU) 2023/1544 irányelve (2023. július 12.) a kijelölt telephelyek kijelölésére és a jogi képviselők kinevezésére vonatkozó összehangolt szabályok megállapításáról az elektronikus bizonyítékok beszerzése céljából a büntetőeljárásokban, HL L 191, 2023.7.28., 181–190. o.

[556] Európa Tanács: Budapesti Egyezmény 2. kiegészítő jegyzőkönyv (2022)
Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), elfogadva: 2022. máj. 12., Strasbourg

6. Nyomozó hatóságok és technológiai fejlődés

A modern technológiai fejlődés olyan ütemű és mértékű, hogy annak hatása alól a bűnüldözés sem vonhatja ki magát. A nyomozó hatóságok munkájában egyre nagyobb szerepet kapnak az elektronikus eszközök, adatok és nyomok, amelyek megfelelő felhasználásával a felderítés hatékonysága növelhető. Ugyanakkor a technológiai innováció a nyomozó hatóságok számára is új kihívásokat teremt hiszen folyamatosan bővülő kompetenciák elsajátítását igényli. Mindemellett kiemelt jelentőségű annak biztosítása, hogy az elektronikus bizonyítékok hitelessége és integritása a büntetőeljárás teljes folyamata során sértetlen maradjon. Ezen fejezetben áttekintjük a nyomozó hatóságok és a technológiai fejlődés kapcsolatát, különös tekintettel a technológiai kompetenciák esetleges hiányosságaira és azok következményeire, a digitalizáció nyújtotta eszközökre és alkalmazásukra, szükséges szakértelemre a elektronikus bizonyítékok integritásának garantálására, valamint hazai és nemzetközi példákra a nyomozási technológiák alkalmazásában.

6.1. Technológiai kompetenciák hiányosságai és ezek következményei

A bűnüldözés területén a XXI. században alapvető elvárássá vált, hogy a nyomozó hatóságok lépést tartsanak a technológiai fejlődéssel. Napjainkban szinte nincs olyan bűncselekmény, amelynek ne lenne digitális dimenziója ahogyan Eoghan Casey találóan megjegyezte: „*a mai modern világban nehéz elképzelni olyan bűncselekményt, amelynek nincs digitális dimenziója*” idézi Casey szavait Sorbán Kinga egy tanulmányában.[557][558] Ez azt jelenti, hogy a bűncselekmények elkövetői gyakran hagynak maguk után elektronikus nyomokat, és az információs technológia a bűncselekmények eszközeként vagy a bizonyítékok hordozójaként jelenik meg. A nyomozó hatóságoknak fel kell ismerniük és fel kell dolgozniuk ezeket a nyomokat annak érdekében, hogy a bűncselekményeket sikeresen felderítsék. Mindazonáltal a technológiai robbanás

[557]Sorbán Kinga: „A digitális bizonyíték a büntetőeljárásban.” *Belügyi Szemle*, 2016/11, 81–96 DOI: 10.38146/BSZ.2016.11.5

[558]Eoghan Casey: Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet (3. kiadás), Academic Press/Elsevier, 2011, 3. o

tempóját nem mindig könnyű követni a nyomozati gyakorlatban. A technológiai kompetenciák kérdésköre arra mutat rá, hogy a nyomozó hatóságok tagjai (ideértve a nyomozókat, bűnügyi technikusokat és igazságügyi szakértőket) számára kiemelten fontos a digitális szaktudás és készségek folyamatos fejlesztése és naprakészen tartása. Ennek több oka is lehet. Egyrészt figyelembe veendő, hogy a rendőri állomány egy része olyan időszakban szerezte alapvető képzését, amikor a digitális technológia még nem bírt kiemelt jelentőséggel, másrészt a technológia folyamatos fejlődése szükségessé teszi a rendszeres továbbképzést, mivel ennek hiányában a meglévő ismeretek rövid időn belül elavulhatnak. A szakirodalom is rámutat arra, hogy a nyomozók akkor járhatnak sikerrel az elektronikus nyomok felhasználásával egy ügy megoldásában, ha új ismereteket, készségeket és képességeket sajátítanak el, továbbá újszerű eljárásokat alkalmaznak.[559] Gaál Tibor szerint a digitális bizonyítékok hatékony felhasználása megköveteli a nyomozó hatóságok tagjaitól az informatikai jártasságot és újfajta szemléletmódot is.[560] Mindez azt jelenti, hogy a sikeres felderítés érdekében a hagyományos nyomozói tudást ki kell egészíteni például hálózati ismeretekkel, adatkezelési és adat-elemzési képességekkel, valamint kiberbiztonsági alapismeretekkel. Amennyiben a nyomozók technológiai felkészültsége nem teljes körű, annak a bűnüldözés eredményességére nézve kedvezőtlen következményei lehetnek. Ilyen kockázatot jelenthet például a bűncselekmények felderítési arányának csökkenése, hiszen az elektronikus nyomok felismerésének vagy megfelelő értelmezésének hiányában előfordulhat, hogy bizonyos bizonyítékok begyűjtése vagy szakszerű felhasználása elmarad. Ennek szemléletes példája lehet, ha egy nyomozó nem ismeri fel, hogy a gyanúsított okostelefonján található alkalmazások adatai relevánsak lehetnek, illetve nem rendelkezik azok kinyeréséhez szükséges ismeretekkel vagy eszközökkel, mindez értékes bizonyítékok elvesztéséhez vezethet. Ugyanígy, ha a hatóságok nem férnek hozzá időben a szükséges elektronikus adatokhoz, fennáll annak veszélye, hogy azok megsemmisülnek vagy elvesznek. Az is közismert probléma, ahogy az előző fejezetekben is hangsúlyoztuk, hogy az elektronikus adatok könnyen törölhetők vagy titkosíthatók ezért különösen fontos, hogy a nyomozók rendelkezzenek a megfelelő eszközökkel és tudással ezen adatok gyors rögzítésére, mert

[559]Gaál Tibor: „A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban”, *Belügyi Szemle*, 2018/7–8., 22–35. DOI: 10.38146/BSZ.2018.7-8.2

[560]Gaál Tibor: „A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban”, *Belügyi Szemle*, 2018/7–8., 22–35. DOI: 10.38146/BSZ.2018.7-8.2

ennek hiányában fokozódik a bizonyíték megsemmisítésének kockázata.[561][562] Amint azt fentebb (*lásd: A technológiai alapú bizonyítékok nyomozati felhasználhatóságának kérdései fejezetben*) jeleztük egy másik következmény a nyomozások elhúzódása és a szakértői függőség. Amennyiben a nyomozó hatóság saját berkein belül nem rendelkezik a szükséges kompetenciával egy bonyolult digitális bizonyíték elemzéséhez, kénytelen igazságügyi szakértőt kirendelni. A Büntetőeljárásról szóló törvény szerint, ha a bizonyítandó tény megállapításához különleges szakértelem szükséges, szakértőt kell alkalmazni.[563] Ez természetesen biztosítja a szakszerűséget, de időigényes és költséges lehet, ráadásul a hatóság ilyenkor kiszolgáltatott a külső szakértő kapacitásának. Gaál elemzéséből kiderül, hogy bár az utóbbi években történt előrelépés (a rendőrségen dolgoznak már informatikus végzettségű elemzők, és bizonyos fejlett eszközök is rendelkezésre állnak) ez nem mondható el minden szervezeti egységről. Ahol a belső erőforrások (szakember, eszköz) hiányoznak, ott továbbra is csak a külső szakértők bevonása jelent megoldást.[564] Ez pedig azzal jár, hogy az eljárás meghosszabbodhat (a szakértő bevonása és vizsgálata időigényes), és a nyomozó hatóság kevésbé önállóan, kisebb kontrollal halad a bizonyítékok feltárásában. A hiányos technológiai felkészültség további következménye lehet a bűnüldözési lemaradás a jól felszerelt és képzett bűnözői csoportokkal szemben. A kiberbűnözők gyakran magas szintű technikai tudással rendelkeznek, vagy könnyen hozzáférnek fejlett eszközökhöz (pl. anonimáló szoftverekhez, erős titkosításhoz). Ha a rendőrség nem tart lépést, akkor kialakulhat egy "technológiai szakadék" a bűnözők javára. Például a bűnelkövetők használhatnak egyszer használatos, eldobható e-mail címeket vagy titkosított kommunikációs csatornákat, amelyek megnehezítik a nyomozást. Erre utalt Bor Olivér kiberbiztonsági szakértő is egy eseti elemzés kapcsán miként manapság az online térben nagyon nehéz kideríteni, ki van a másik oldalon, hiszen a digitális "ujjlenyomatok" ügyesen elrejthetők, például egyszer használatos email-címek vagy úgynevezett "eldobható, feltöltős mobiltelefonok" alkalmazásával, amelyek beazonosítása rendkívül nehéz.[565] Ha a nyomozó hatóság nincs

[561] Be. 207. § (2)
[562] Be. 315–316. §
[563]Be. 188. § (1)
[564]Gaál, Tibor: „A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban." = Belügyi Szemle 66. évf. 7–8. sz. (2018) 22–? o. [Online] DOI: 10.38146/BSZ.2018.7-8.2
[565]Kalapos Mihály: „Kiberszakértő: teljesen elrejthető a digitális ujjlenyomat, nehéz lesz a nyomozás a bombariadók ügyében." InfoStart.hu, 2025. január 25. Elérhető: https://infostart.hu/belfold/2025/01/25/kiberszakerto-teljesen-elrejtheto-a-digitalis-ujjlenyomat-nehez-lesz-a-nyomozas-a-bombariadok-ugyeben. Letöltés dátuma: 2025. február 7.

felkészülve az ilyen módszerek kezelésére, akkor egyes ügyekben tehetetlen maradhat. A nemzetközi tapasztalatok is alátámasztják, hogy a rendvédelmi szerveknek komoly kihívást okoz a digitális készség- illetve eszközhiány. Egy amerikai kutatóintézet (RAND Corporation) jelentése rámutatott arra, hogy az igazságszolgáltatási rendszer nincs teljesen felkészülve az olyan ügyek kezelésére, mint a kibertérben elkövetett zaklatások (*lásd: Online bántalmazás és zaklatás fejezetben)* mivel hiányzik a megfelelő képzés a nyomozók számára az ilyen ügyek lefolytatásához.[566]Az ilyen hiányosságok a bűnüldözés hatékonyságát csökkentik, és végső soron a büntető igazságszolgáltatásban a törvényes rend érvényesítését gyengíthetik. Ekképp megállapítható, hogy a nyomozó hatóságok technológiai kompetenciáinak hiányosságai valós veszélyt jelentenek a hatékony bűnüldözésre.[567] A következmények között említhető a bizonyítékok elvesztése vagy fel nem ismerése, a nyomozások elhúzódása és a külső szakértőktől való függés, valamint a bűnözői technológiai fölényből fakadó felderítési nehézségek. E negatív hatások ellensúlyozása érdekében elengedhetetlen a folyamatos képzés és a technológiai felkészültség fejlesztése a rendőrségen belül, amire a következő alfejezetekben is kitérünk (összhangban a Be. 166–167. § által megkövetelt törvényes bizonyítási renddel és a 183. § (1) szerinti szakértői közreműködéssel).[568][569]

6.2. A digitalizáció nyújtotta eszközök és azok hatékony alkalmazása

A digitalizáció számos új eszközt és módszert biztosít a nyomozó hatóságok számára, melyek megfelelő alkalmazásával a bűncselekmények felderítése gyorsabbá és eredményesebbé tehető. Fontos azonban, hogy ezen technológiai eszközöket hatékonyan és szakszerűen használják, különben a bennük rejlő potenciál kihasználatlan marad. Ebben az alfejezetben áttekintjük a legfontosabb digitális eszközöket, amelyeket a nyomozó hatóságok a gyakorlatban alkalmaznak, valamint ezek hatékony

---

[566]RAND Corporation**:** *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, CA: RAND Corporation, 2015. 298 p. Elérhető: https://www.rand.org/pubs/research_reports/RR890.html (letöltés: 2024. október 6.)
[567]Gaál, Tibor: „A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban.” = Belügyi Szemle 66. évf. 7–8. sz. (2018) 22-35 o. DOI: 10.38146/BSZ.2018.7-8.2
[568]Be. 166–167. §
[569]Be. 183. § (1)

felhasználásának feltételeit. A bűnügyi technikusok és informatikus szakértők ma már speciális szoftverek és hardverek segítségével tudják rögzíteni és elemezni a digitális bizonyítékokat. Ilyenek például a forenzikus képalkotó programok (mint az EnCase vagy FTK), amelyek lehetővé teszik egy számítógép merevlemezének bitpontos (bit-by-bit) lemásolását. A bitazonos, ún. tükörmásolat azért lényeges, mert ez biztosítja, hogy a vizsgálat egy, az eredetivel minden bitjében megegyező másolaton történjen, megóvva az eredeti adathordozót a változástól. Az EnCase és az FTK (Forensic Toolkit) olyan szoftvercsaládok, amelyek nemzetközileg is elterjedtnek számítanak, és kiemelkedő szerepet töltenek be az elektronikus bizonyítékok feltárásában és értékelésében.[570] Mindkettő integrált, moduláris környezetet kínál a bizonyítékok forenzikusan helyes megszerzésére, feldolgozására, elemzésére és a jelentéskészítésre, miközben a láncolatbiztonság, az ellenőrizhetőség és a megismételhetőség követelményeit intézményi szinten támogatja. Ezek az eszközök a már említett bitpontos rögzítést tesznek lehetővé (fizikai vagy logikai képfelvétel), a keletkező bizonyítékkonténereket kriptográfiai ellenőrzőösszegekkel (tipikusan MD5/SHA-256) látják el, és a feldolgozás során automatizált indexeléssel, fájlrendszer-rekonstrukcióval, valamint rendszer- és alkalmazás-artefaktok (például Prefetch, LNK, böngészési és e-mail naplók) célzott kibontásával segítik a bizonyítéktárgy releváns részterületeinek gyors azonosítását.[571] Az EnCase erőssége hagyományosan a mély fájlrendszer-szintű rekonstrukció és az EnScript-alapú, reprodukálható munkafolyamatok, míg az FTK indexelés-első megközelítése nagy adattömegen (különösen e-mail- és dokumentumkorpuszon) biztosít gyors, átfogó kereshetőséget és vizsgálói kollaborációt.[572] A Nemzeti Nyomozó Iroda (NNI) szakemberei a gyakorlatban minden lefoglalt informatikai rendszerről teljes bitazonos másolatot készítenek, és ezt hash-értékkel látják el annak igazolására, hogy a másolat megegyezik az eredeti tartalommal[573] Ezt a másolatot vizsgálják át a nyomozás során, miközben az eredeti eszközt biztonságosan elkülönítik. Ez a módszer nem csak az

---

[570]OpenText Corporation: *OpenText EnCase Forensic, Product Overview.* https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-po-encase-forensic-en.pdf (letöltés dátuma: 2024. október 7.)

[571]OpenText Corporation: *OpenText EnCase Forensic Overview.* https://static.carahsoft.com/concrete/files/8117/3807/7578/OpenText_EnCase_Forensic_Overview_PDF.pdf (letöltés dátuma: 2024. október 7.)

[572]dtSearch Corporation: *Case Study, AccessData Forensic Toolkit.* https://www.dtsearch.com/CS_ForensicToolkit.html (letöltés dátuma: 2024. október 7.)

[573]Sorbán Kinga: *A digitális bizonyíték a büntetőeljárásban. = Belügyi Szemle* 2016/11, 81–96. o. https://real.mtak.hu/120115/1/SorbanBelugyiSzemle2016.evi11.szam81-96.pdf (letöltés dátuma: 2025. október 7.)

integritást védi, hanem korlátozza is azok körét, akik a nyers adatokhoz hozzáférhetnek, így csökkenti az illetéktelen módosítás kockázatát.[574] Ugyanakkor tudni kell, hogy a teljes adattartalom tükörmásolata nagy adatmennyiségek esetén erőforrás-igényes, amely hatékonyan inkább a kisebb adathalmazoknál alkalmazható, míg nagyon nagy rendszerek esetén más megoldások (pl. célzott másolatkészítés) is szóba jöhetnek. A digitalizáció következtében a nyomozó hatóságok (megfelelő törvényi felhatalmazás birtokában) ma már az elektronikus kommunikáció szinte minden formájához hozzáférhetnek. Ez magában foglalja a telefonos kommunikáció lehallgatását és a hálózati metaadatok (például híváslisták, cellainformációk) gyűjtését, valamint az internetes forgalom megfigyelését is. A Büntetőeljárási törvény kifejezetten nevesíti az elektronikus adatok lefoglalását, mint kényszerintézkedést, és különféle módozatokat határoz meg ennek végrehajtására, amelyekről az előző fejezetekben részletesen kitértünk (pl. adatok másolása, áthelyezése, adathordozó lefoglalása).[575] A nyomozók ma már hozzáférhetnek olyan speciális eszközökhöz, mint az IMSI-vadászok (IMSI-catcherek), amelyek (hamis cellatornak álcázva) képesek a környezetükben lévő mobilkészülékek IMSI/IMEI-azonosítóját kinyerni és a készülékek helyzetét bemérni. Egyes készülékeknél ezek az eszközök lehetővé tehetik a forgalom részleges lehallgatását, valamint a kapcsolódó kommunikáció biztonsági protokolljainak mesterséges csökkentését, érvénytelenítését vagy egyszerűsítését is azaz olyan beavatkozást, amely gyengíti a kapcsolat védelmét. Emellett léteznek olyan hálózati forgalom-figyelő rendszerek (például csomagszintű mélyvizsgálat, DPI: „Deep Packet Inspection", szolgáltatói jogszerű lehallgatási megoldások), amelyekkel az internetes kommunikáció metaadatai és megfelelő jogosultság esetén a csomagszintű tartalmi információk is nyomon követhetők.[576][577] Ezen eszközök akkor tekinthetők jogszerűnek és hatékonynak, ha a hatóságok a törvényben meghatározott garanciális szabályokat szigorúan betartják. A titkos információgyűjtéshez

---

[574]Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. = Belügyi Szemle 2016/11, 81–96. o. https://real.mtak.hu/120115/1/SorbanBelugyiSzemle2016.evi11.szam81-96.pdf (letöltés dátuma: 2024. október 7.)

[575]Róth Erika: Az elektronikus adat megszerzését, megőrzését szolgáló büntetőeljárási kényszerintézkedések. = Infokommunikáció és Jog 2020/2. (75.), 10–15. o. https://szakcikkadatbazis.hu/doc/2147096 (letöltés dátuma: 2024. október 7.)

[576] Threat Lab / Electronic Frontier Foundation: Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (White Paper, 2019). https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf (letöltés dátuma: 2024. október 7.)

[577]Electronic Privacy Information Center (EPIC): *Deep Packet Inspection and Privacy.* https://archive.epic.org/privacy/dpi/?utm_ (letöltés dátuma: 2024. október 7.)

általában előzetes bírói engedély szükséges, továbbá elengedhetetlen a részletes jogszabályi előírásoknak megfelelő relevancia-, arányosság- és célhoz kötöttségvizsgálat, valamint a láncolatbiztonság és az adatkezelés átlátható dokumentálása.[578] Ugyanakkor az IMSI-catcherek és a hálózati forgalomfigyelés rendkívüli jelentőséggel bírnak a felderítés során, hiszen az adott gyanúsított tartózkodási helye meghatározható a mobiltelefon cellainformációi alapján, egy bűnszervezet belső kapcsolatrendszere feltérképezhető az online üzenetváltások és metaadatok elemzésével, továbbá az ilyen adatok gyakran kulcsfontosságú bizonyítékokként szolgálnak, mint ahogyan igazolva, hogy a gyanúsítottak kapcsolatban álltak egymással a bűncselekmény elkövetését megelőzően.[579][580] Mindezek következtében a technikai, technológiai megoldások alkalmazása nem csupán műszaki, hanem alapjogi kérdés is, hiszen a hatékony nyomozás és a személyes adatok védelme közötti egyensúly megőrzése érdekében a gyakorlatot jogi és emberi jogi garanciákkal, független felügyelettel, valamint átlátható elszámoltathatósági mechanizmusokkal szükséges kísérni. Emellett indokolt, hogy a konkrét eljárási döntések meghozatalakor a műszaki és jogi szempontokat egyaránt mérlegeljék.[581] A digitalizáció a bűnüldözés számára új információs és elemzési dimenziót teremtett, mivel az internet nyilvános szférája (a közösségi médiától a különböző online adatbázisokig) a nyomozati munka szerves részévé vált. A nyílt forrású hírszerzés (Open Source Intelligence: OSINT) lényege ugyanis az, hogy a nyomozó hatóságok nyilvánosan elérhető adatokból gyűjtenek információt.[582] Ez magában foglalhatja a gyanúsított(ak) közösségi média felhasználói profiljainak áttekintését, nyilvános posztok, fényképek illetőleg kapcsolati hálók elemzését. Továbbá kereshetnek

---

[578]Bąkowski, Piotr: Access to data for law enforcement: Lawful interception. = EPRS Briefing 2025 (PE 775.881).https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775881/EPRS_BRI%282025%29775881_EN.pdf (letöltés dátuma: 2025. augusztus 7.)

[579]Borgaonkar, Ravishankar – Martin, Andrew – Park, Shinjo – Shaik, Altaf – Seifert, Jean-Pierre: White-Stingray: Evaluating IMSI Catchers Detection Applications. In: 11th USENIX Workshop on Offensive Technologies (WOOT '17) – Proceedings. Berkeley, USENIX Association, 2017. 1–12. o. https://www.usenix.org/system/files/conference/woot17/woot17-paper-park.pdf (letöltés dátuma: 2024. október 7.)

[580]Nyeste Péter – Szendrei Ferenc: Nyílt forrású információszerzés a bűnüldözésben: OSINT in Law Enforcement. = Nemzetbiztonsági Szemle (online) 2019/2, 50–67. o. https://folyoirat.ludovika.hu/nbsz/article/download/1436/760/5500

[581]Privacy International: IMSI Catchers: Legal Analysis. 202. 1-25.o. https://privacyinternational.org/sites/default/files/2020-06/IMSI%20catchers%20legal%20analysis.pdf (letöltés dátuma: 2024. október 7.)

[582]Nyeste Péter – Szendrei Ferenc: Nyílt forrású információszerzés a bűnüldözésben: OSINT in Law Enforcement. = Nemzetbiztonsági Szemle (online) 2019/2, 50–67. o. https://folyoirat.ludovika.hu/nbsz/article/download/1436/760/5500 (letöltés dátuma: 2025. október 9.)

a nyomozók a nyilvános, hozzáférhető, nyílt adatbázisokban (például céginformációs rendszerekben, domain-regisztrációs adatok között stb.). A digitalizáció a bűnüldözésben is új lehetőségeket teremtett, többek között a nagyszabású bűnügyi nyilvántartó rendszerek kiépítésével. Magyarországon a rendőrség hosszú ideje alkalmazza a Robotzsaru Neo integrált ügyfeldolgozó rendszert, amely a nyomozati iratkezelés teljes körű digitalizációját valósítja meg. A digitalizációs infrastruktúra gerincét ezen rendszer adja, amely egységes szervezeti és technológiai keretbe rendezi a nyomozati és az igazgatásrendészeti folyamatok során keletkező adatokat és iratokat.[583] A kliens szerver architektúrára épülő megoldás differenciált jogosultságkezelést biztosít a rendőri feladatkörök szerint, a folyamatos (24/7) rendelkezésre állás mellett, valamint támogatja az offline üzemmódot is, így a terepi munkavégzésből visszaszinkronizált adatok ellenőrizhető módon integrálódnak a központi adatbázisba.[584] A rendszerbe épített dokumentumtár az ügyek elektronikus példányait az ügy selejtezéséig kezeli, míg a Netzsaru felület statisztikai, keresési és kutatási funkciókat tesz elérhetővé. A NOVA alrendszerek (például KGIR, TIR, OFRA) a pénzügyi, tevékenységirányítási és objektív felelősségi funkciókat integrálják egy egységes, interoperábilis ügyviteli ökoszisztémába. A kötelező, egységes használat és a naplózott folyamatok a láncolatbiztonságot szolgálják, a SZEÜSZ-kapcsolatok (például a Központi Érkeztető Rendszer és a Központi Hivatali Kapu) pedig a közigazgatási infrastruktúrával való átjárhatóságot garantálják. [585] Az iratkezelés rendjét és a digitális munkafolyamatok minőségbiztosítását a szervezeti szabályzatok és a jogszabályi előírások határozzák meg. Az elektronikus iktatás, a beérkező iratok digitalizálása és a verziókövetés egységes protokoll szerinti megvalósítása a bizonyítékok hitelességét és megismételhetőségét rendszerszinten garantálja, ezáltal a digitális eljárásrend egyik legfontosabb garanciális elemévé válik. Ugyanez a szemlélet érvényesül az adatvédelem és az információbiztonság terén is hiszen a hozzáférések szerepkörökhöz kötötten, naplózott módon történnek, az adattovábbítás pedig a központi szolgáltatásokhoz illeszkedő, szabályozott interfészeken keresztül

[583]35/2017. (XII. 13.) ORFK utasítás a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól 18/2011. (IX. 23.) ORFK utasítás módosításáról.

[584]Országos Rendőr-főkapitányság: Műszaki leírás a KÖFOP-1.0.0 – VEKOP-15 „inNOVA" projekt „Rendszertervezési és minőségbiztosítási szolgáltatások" moduljához. Műszaki dokumentáció (belső kézirat, Verzió 3.4.). Budapest, 2016. december 20., Országos Rendőr-főkapitányság.17-19.o.

[585]Országos Rendőr-főkapitányság: Műszaki leírás a KÖFOP-1.0.0 – VEKOP-15 „inNOVA" projekt „Rendszertervezési és minőségbiztosítási szolgáltatások" moduljához. Műszaki dokumentáció (belső kézirat, Verzió 3.4.). Budapest, 2016. december 20., Országos Rendőr-főkapitányság.17-19.o.

valósul meg. Ezen szabályozottság egyrészt lehetővé teszi, hogy a nyomozók a napi munkavégzés részeként, standardizált módon használják a digitális eszközöket, másrészt biztosítja, hogy a keletkező digitális adatok (a későbbi eljárási felhasználás szempontjából) igazolható forrásból, ellenőrzött folyamatok eredményeként álljanak rendelkezésre.[586][587][588]Emellett léteznek specializált adatbázisok, például ujjnyomat-nyilvántartó (AFIS: Automated Fingerprint Identification System), DNS-adatbázis, lőfegyver-ballisztikai nyilvántartás stb., amelyek mind digitális platformon működnek.[589][590][591][592] Az automatikus ujjnyomat-azonosító rendszer (AFIS) a digitális daktiloszkópiai adatbázis alapját képezi. A bűnügyi nyilvántartásokra vonatkozó 2009. évi XLVII. törvény értelmében a bűnügyi és rendészeti biometrikus adatok nyilvántartása két részből áll: a daktiloszkópiai nyilvántartásból és a DNS-profil-nyilvántartásból.[593]A daktiloszkópiai nyilvántartás célja, hogy a bűncselekmény helyszínén rögzített ujj- vagy tenyérnyomat alapján azonosítsa a bűncselekmény elkövetőjét, a rendkívüli halálesetek ismeretlen áldozatait, illetve a fogvatartottak személyazonosságát.[594] A nyilvántartás három alrendszerből épül fel, amely tartalmazza

---

[586]Uo. 18–19. o.

[587]35/2017. (XII. 13.) ORFK utasítás a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól 18/2011. (IX. 23.) ORFK utasítás módosításáról.

[588]Országos Rendőr-főkapitányság: Műszaki leírás a KÖFOP-1.0.0 – VEKOP-15 „inNOVA" projekt „Rendszertervezési és minőségbiztosítási szolgáltatások" moduljához. Műszaki dokumentáció (belső kézirat, Verzió 3.4.). Budapest, 2016. december 20., Országos Rendőr-főkapitányság.17-19.o.

[589]Demeter Gabriella: Daktiloszkópiai nyilvántartás Magyarországon – Az ujj- és tenyérlenyomatok bűnügyi célú kezelése. https://www.jogiforum.hu/files/publikaciok/demeter_gabriella__daktiloszkopiai_nyilvantartas_magyarorszagon%5Bjogi_forum%5D.pdf (letöltés dátuma: 2024. október 9.)

[590] 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, 37–51. §.

[591]2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, 52–66. §.

[592]12/2016. (V. 4.) BM rendelet az arcképmás, az ujj- és tenyérnyomat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérnyomat és a szájnyálkahártya-törlet levételének részletes technikai szabályairól; a DNS-profil meghatározásának szakmai-módszertani követelményeiről; továbbá a nyilvántartás technikai vezetésének részletes szabályairól.

[593]2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, IV. Fejezet. A bűnügyi és rendészeti biometrikus adatok nyilvántartása.

[594]2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, IV. Fejezet. A bűnügyi és rendészeti biometrikus adatok nyilvántartása. A daktiloszkópiai nyilvántartás 37-51. §

a helyszíni ujj- és tenyérnyomokat, a büntetőeljárás alatt állók nyomatait, valamint a jogerősen elítéltek nyomatait.[595] A 12/2016. (V. 4.) BM rendelet rögzíti a daktiloszkópiai mintavétel technikai szabályait, és lehetővé teszi az ujj- és tenyérnyomatok digitális rögzítését. A mintavétel történhet hagyományos, festékes eljárással, illetve „a szakértői nyilvántartó szerv által jóváhagyott digitális nyomatfelvételi berendezéssel".[596]A digitális berendezéssel készült nyomatokat kizárólag elektronikus formában továbbítják a szakértői nyilvántartó szervhez, ahol belső azonosító kóddal látják el.[597] A digitalizáció ezen formája nemcsak az adatfelvétel pontosságát növeli, hanem az elektronikus adatcsere gyorsaságát illetőleg a megbízhatóságát is javítja. A szakirodalom rámutat arra is, hogy az AFIS 1993 óta működik Magyarországon, és az ujjnyomat-adatbázis digitalizálása alapvetően átalakította a bűnügyi azonosítás gyakorlatát.[598]A rendszer digitálisan rögzíti és tárolja az ujjlenyomatokat, majd automatikus összehasonlítást végez a bűncselekmény helyszínén talált nyomtöredékek és a nyilvántartásban szereplő minták között.[599] A digitális adatkezelésnek köszönhetően számos korábban lezárt ügyben is sikerült azonosítani az elkövetőt.[600] A számítógépes AFIS-rendszerek ma már kizárólagos eszközként szolgálnak a daktiloszkópiai összehasonlításban. Az adatbázisaik tízujjas

[595]12/2016. (V. 4.) BM rendelet az arcképmás, az ujj- és tenyérnyomat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérnyomat és a szájnyálkahártya-törlet levételének részletes technikai szabályairól, a DNS-profil meghatározásának szakmai-módszertani követelményeiről, továbbá a nyilvántartás technikai vezetésének részletes szabályairól.

[596]12/2016. (V. 4.) BM rendelet az arcképmás, az ujj- és tenyérnyomat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérnyomat és a szájnyálkahártya-törlet levételének részletes technikai szabályairól, a DNS-profil meghatározásának szakmai-módszertani követelményeiről, továbbá a nyilvántartás technikai vezetésének részletes szabályairól. 4. melléklet a 12/2016. (V. 4.) BM rendelethez. Az ujj- és tenyérnyomatvétel módja

[597]12/2016. (V. 4.) BM rendelet az arcképmás, az ujj- és tenyérnyomat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérnyomat és a szájnyálkahártya-törlet levételének részletes technikai szabályairól, a DNS-profil meghatározásának szakmai-módszertani követelményeiről, továbbá a nyilvántartás technikai vezetésének részletes szabályairól. 4. melléklet a 12/2016. (V. 4.) BM rendelethez. Az ujj- és tenyérnyomatvétel módja. 5. pont

[598]Demeter Gabriella: Daktiloszkópiai nyilvántartás Magyarországon: Az ujj- és tenyérlenyomatok bűnügyi célú kezelése. https://www.jogiforum.hu/files/publikaciok/demeter_gabriella__daktiloszkopiai_nyilvantartas_magyarorszagon%5Bjogi_forum%5D.pdf (letöltés dátuma: 2024. október 11.)

[599]Demeter Gabriella: Daktiloszkópiai nyilvántartás Magyarországon: Az ujj- és tenyérlenyomatok bűnügyi célú kezelése. https://www.jogiforum.hu/files/publikaciok/demeter_gabriella__daktiloszkopiai_nyilvantartas_magyarorszagon%5Bjogi_forum%5D.pdf (letöltés dátuma: 2024. október 11.)

[600]Demeter Gabriella: Daktiloszkópiai nyilvántartás Magyarországon: Az ujj- és tenyérlenyomatok bűnügyi célú kezelése. https://www.jogiforum.hu/files/publikaciok/demeter_gabriella__daktiloszkopiai_nyilvantartas_magyarorszagon%5Bjogi_forum%5D.pdf (letöltés dátuma: 2024. október 11.)

nyomatokat, tenyérnyomatokat és bűncselekményi nyomtöredékeket tartalmaznak, melyek alapján a rendszer automatikusan kizárja a nem egyező mintákat, a végső azonosítást pedig a szakértő manuálisan erősíti meg.[601][602] A DNS-profil-nyilvántartás szintén megjelenik a 2009. évi XLVII. törvényben, amely a bűncselekmények helyszínén rögzített DNS-profilok, a büntetőeljárás alá vont személyek, valamint a jogerősen elítéltek DNS-profiljainak kezelését szabályozza.[603] A szakértői nyilvántartó szerv köteles a részére megküldött mintákat haladéktalanul nyilvántartásba venni, kezelni, összehasonlítani, és minden egyes mintához belső azonosító kódot rendelni.[604] A 12/2016. (V. 4.) BM rendelet kiegészítő jelleggel meghatározza a DNS-mintavétel technikai szabályait, valamint a minták rögzítésének és továbbításának követelményeit.[605] A magyar bűnügyi DNS-adatbázist jelenleg a CODIS (Combined DNA Index System: Kombinált DNS-indexrendszer) szoftver működteti. Füredi Sándor tanulmánya rámutat arra, hogy a rendszer a DNS-profil-alkotó allélok számszerű egyezését vizsgálja, ezért a rossz minőségű vagy több személytől származó (kevert) minták automatikus keresése korlátozott.[606]A szerző valószínűségi alapú keresési algoritmus bevezetését javasolja, amely az egyező allélok populációs gyakoriságát és intenzitását is figyelembe veszi, ezáltal jelentősen növelhető a CODIS-találatok

[601]Demeter Gabriella: Daktiloszkópiai nyilvántartás Magyarországon: Az ujj- és tenyérlenyomatok bűnügyi célú kezelése. https://www.jogiforum.hu/files/publikaciok/demeter_gabriella__daktiloszkopiai_nyilvantartas_magyarorszagon%5Bjogi_forum%5D.pdf (letöltés dátuma: 2024. október 11.)

[602]Fenyvesi Csaba – Herke Csongor – Tremmel Flórián (szerk.): Kriminalisztika. Budapest, Nemzeti Közszolgálati Egyetem. Ludovika Egyetemi Kiadó, 2022. 624 o.

[603]2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, IV. Fejezet. A bűnügyi és rendészeti biometrikus adatok nyilvántartása. 2. §

[604]2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról, IV. Fejezet. A bűnügyi és rendészeti biometrikus adatok nyilvántartása. 35. §

[605]12/2016. (V. 4.) BM rendelet az arcképmás, az ujj- és tenyérnyomat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérnyomat és a szájnyálkahártya-törlet levételének részletes technikai szabályairól; a DNS-profil meghatározásának szakmai-módszertani követelményeiről; továbbá a nyilvántartás technikai vezetésének részletes szabályairól.

[606]Füredi Sándor: A magyarországi bűnügyi DNS-profil nyilvántartás találatkeresési módszerének fejlesztése. = Rendőrségi Tanulmányok 2024/különszám, 3–77. o. https://epa.oszk.hu/04000/04093/00026/pdf/EPA04093_rendorsegi_tanulmanyok_2024_ksz_003-077.pdf (letöltés dátuma: 2025. január 11.)

pontossága és száma.[607]A digitális adatkezelés fejlesztése így nemcsak a minták rögzítésének gyorsaságában, hanem a keresési algoritmusok hatékonyságában is megmutatkozik. Az uniós szintű adatcsere jogi keretét a Prüm-határozatok és a 2024/982/EU (Prüm II) rendelet biztosítják.[608] A rendelet előírja, hogy a tagállamok a bűnügyi adatbázisaikban tárolt DNS-profilokat és ujjnyomat-adatokat olyan módon tegyék automatikus keresésre elérhetővé más tagállamok és az Europol számára, amely elősegíti a határokon átnyúló bűnügyi együttműködést és a személyazonosítás gyorsabb, standardizált eljárásait.[609] Az automatikus keresések kizárólag egyedi ügyekben végezhetők, és a potenciális találatokat szakértői megerősítésnek kell követnie.[610] A rendelet külön hangsúlyt fektet a titkosság, az adatintegritás, a titkosított kommunikáció és a minőségbiztosítás követelményeire, ezzel erősítve az európai szintű adatcsere biztonsági és garanciális kereteit.[611] Az Európai Unióban a Prüm rendszer kapcsolja össze a tagállamok ujjnyomat és DNS nyilvántartásait, így a nyomozók gyorsan ellenőrizhetik, hogy egy ismeretlen minta szerepel e bármely más ország adatbázisában. Hasonlóan az Interpol globális adatbázisai (pl. ellopott útlevelek nyilvántartása vagy a körözési információk) is digitalizáltan érhetők el, ami tovább erősíti az információáramlás hatékonyságát. Ezen eszközök hatékony alkalmazása azt jelenti, hogy a nyomozó valós időben fér hozzá hatalmas mennyiségű adathoz, és ezekből másodpercek alatt releváns információhoz juthat. Természetesen mindezt csak a hozzáférés szabályozottsága és a személyes adatok védelme mellett lehet biztosítani, hiszen a lekérdezést kizárólag jogosultsággal rendelkező személyek végezhetik, és minden művelet naplózásra kerül. Hatékony alkalmazásnak tekinthető például, ha egy bűncselekmény helyszínén rögzített

[607]Füredi Sándor: A magyarországi bűnügyi DNS-profil nyilvántartás találatkeresési módszerének fejlesztése. = Rendőrségi Tanulmányok 2024/különszám, 3–77. o. https://epa.oszk.hu/04000/04093/00026/pdf/EPA04093_rendorsegi_tanulmanyok_2024_ksz_003-077.pdf (letöltés dátuma: 2025. január 11.)

[608]Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 (the Prüm II Regulation). HL L 2024/982, 2024. 04. 05.

[609]Európai Unió EUR-Lex: Police cooperation: automated search and exchange of data. https://eur-lex.europa.eu/EN/legal-content/summary/police-cooperation-automated-search-and-exchange-of-data.html (letöltés dátuma: 2024. október 11.)

[610] Európai Unió EUR-Lex: Police cooperation: automated search and exchange of data. https://eur-lex.europa.eu/EN/legal-content/summary/police-cooperation-automated-search-and-exchange-of-data.html (letöltés dátuma: 2024. október 11.)

[611]Európai Unió EUR-Lex: Police cooperation: automated search and exchange of data. https://eur-lex.europa.eu/EN/legal-content/summary/police-cooperation-automated-search-and-exchange-of-data.html (letöltés dátuma: 2024. október 11.)

ujjnyomot perceken belül összevetnek az AFIS rendszerrel, és így sikerül egy korábban regisztrált személyt azonosítani, ezzel értékes nyomot adva a nyomozásnak. A lőfegyver-azonosítás területén a digitalizáció hasonlóan jelentős áttörést hozott, mint a daktiloszkópiai és DNS-adatbázisok esetében. Az INTERPOL által működtetett Ballisztikai információs hálózat (Ballistic Information Network (IBIN)) több mint 1,8 millió rekordot tartalmaz, és globális platformként szolgál a ballisztikai adatok központosított gyűjtésére, tárolására és összehasonlító elemzésére.[612]A lőfegyver elsütésekor a töltényhüvelyen és a lövedéken mikroszkopikus jellegzetességek keletkeznek, amelyek egyedi „digitális ujjlenyomatként" azonosíthatók. Az IBIN ezeket a jelöléseket nagyfelbontású digitális képekké alakítja, majd azokat elektronikus azonosítóvá (digitális aláírássá) konvertálja, és a meglévő adatbázissal összeveti.[613]A rendszer potenciális találatokat (hits) generál, amelyek több, egymással összefüggésbe hozható bűncselekményt azonosíthatnak, illetve egy konkrét fegyvert kapcsolhatnak korábbi bűnesetekhez.[614] Az ilyen digitális megoldások hiányában a ballisztikai azonosítás manuális mikroszkópos összehasonlításra korlátozódna, ami időigényes és kevésbé hatékony eljárás. A digitalizáció ezzel szemben lehetővé teszi a nagyméretű adatbázisok automatizált vizsgálatát, a nemzetközi adatcsere gyorsítását, valamint az azonosítás pontosságának növelését. Bár még fejlődőben lévő terület, meg kell említeni a mesterséges intelligencia (MI) és a nagy adathalmazok elemzésének lehetőségét a bűnüldözésben.[615] Néhány ország rendőrsége már kísérletezik prediktív rendészeti rendszerekkel, amelyek hatalmas mennyiségű adat (korábbi bűnesetek helye, ideje, körülményei, térfigyelő kamerák adatai stb.) elemzésével próbálják megjósolni, hol várható újabb bűncselekmény.[616][617] Továbbá az MI segíthet az arcfelismerésben (pl.

---

[612]INTERPOL: INTERPOL Ballistic Information Network (IBIN). https://www.interpol.int/en/Crimes/Firearms-trafficking/INTERPOL-Ballistic-Information-Network (letöltés dátuma: 2024. október 11.)

[613]INTERPOL: INTERPOL Ballistic Information Network (IBIN). https://www.interpol.int/en/Crimes/Firearms-trafficking/INTERPOL-Ballistic-Information-Network (letöltés dátuma: 2024. október 11.)

[614] INTERPOL: INTERPOL Ballistic Information Network (IBIN). https://www.interpol.int/en/Crimes/Firearms-trafficking/INTERPOL-Ballistic-Information-Network (letöltés dátuma: 2024. október 11.)

[615]Fantoly Zsanett: Mesterséges intelligencia a büntetőeljárás nyomozási szakaszában. *In: Acta Universitatis Szegediensis: Forum: acta juridica et politica*, 12. évf., 1. szám, Szeged, 2022. 49–61. o. ISSN 2063-2525 https://acta.bibl.u-szeged.hu/82201/

[616]Európai Parlament: Jelentés „Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters" (A9-0232/2021).

[617] Fantoly Zsanett – Herke Csongor – Szabó Barbara: The role of AI-based systems in negotiated proceedings. eRevue internationale de droit pénal 7 Paper: 18 , 8 p. (2023) ISSN: 2522-2945

térfigyelő kamerák felvételein gyanúsítottak beazonosítása), a darknet forgalmának elemzésében, vagy akár a rengeteg lefoglalt digitális fájl közötti gyors keresésben (pl. gyermekpornográf felvételek automatikus felismerése képfelismerő algoritmusokkal).[618][619][620]Az ilyen eszközök hatékony alkalmazásához nem csak technológiai, hanem jogi és etikai felkészültség is szükséges. Például az automatikus arcfelismerő rendszerek használata felveti a személyiségi jogok kérdését, ezért alkalmazásuk csak törvényes keretek között, illetve garanciák mellett történhet.[621]Ugyanakkor megfelelő használat mellett jelentősen felgyorsíthatják a nyomozást. Vegyünk egy példát, egy városi kamerahálózat több napnyi felvételéből kell kiszűrni egy menekülő gyanúsítottat. Emberi munkaerő bevonásával a keresés érdemben nehezen, hosszú idő alatt valósítható meg. Ezzel szemben egy célzottan betanított MI-algoritmus a mintafelismerés révén órákon belül képes lesz azonosítani a releváns képsorokat. Fontos azonban megjegyezni, hogy az ilyen technológiák alkalmazása során különös figyelmet kell fordítani a pontosságra, az adatvédelemre és a jogi garanciákra, hogy a gyorsaság ne menjen a jogszerű eljárás és az alapjogok sérelme rovására. Ahhoz, hogy a digitalizáció nyújtotta eszközök a bűnüldözésben valóban hatékonyan alkalmazhatók legyenek, elengedhetetlen a megfelelő személyi, szervezeti és technikai feltételek biztosítása. Egyrészt szükséges a nyomozók, technikusok és szakértők folyamatos képzése, illetve továbbképzése az új technológiai eszközök és módszerek szakszerű használatára (ld. előző alfejezet). Másrészt ki kell alakítani azokat a belső eljárásrendeket és protokollokat, amelyek egyértelműen meghatározzák az eszközök alkalmazásának módját, ezzel garantálva, hogy a gyűjtött digitális adatok a büntetőeljárásban bizonyítékként is felhasználhatók legyenek.[622]Harmadrészt nélkülözhetetlen a technikai infrastruktúra folyamatos fejlesztése, mivel a szakmai kompetenciák önmagukban nem elegendők, ha a rendelkezésre álló hardver vagy szoftver elavult, illetve nem felel meg a licencelési és biztonsági követelményeknek.

---

[618]Guia, Maria João – Mihai, Ioan-Cosmin: *Mesterséges intelligencia innovációk a bűnüldözési képzésben: CEPOL stratégia 23–27. = Belügyi Szemle* 2025/9, 1879–1896. o.

[619]Fantoly Zsanett: Mesterséges intelligencia a büntetőeljárás nyomozási szakaszában. *In: Acta Universitatis Szegediensis: Forum: acta juridica et politica*, 12. évf., 1. szám, Szeged, 2022. 49–61. o. ISSN 2063-2525 https://acta.bibl.u-szeged.hu/82201/

[620]INHOPE: What is child sexual abuse material detection? https://inhope.org/EN/articles/what-is-child-sexual-abuse-material-detection (letöltés dátuma: 2025. október 11.)

[621]2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről.

[622]Európai Parlament jelentés (A9-0232/2021), 23. pont: a rendészeti és bírósági dolgozók számára kötelező speciális képzést sürget az AI etikai, jogi és technikai vonatkozásainak megismerésére, hogy felismerjék az algoritmusok torzításait és korlátait.

Magyarországon kedvező irányú fejleményként értékelhető, hogy az elmúlt években számottevő előrelépés történt a rendőrség informatikai rendszereinek és technikai eszközparkjának fejlesztésében. Ennek részeként megvalósult a számítógépes hálózatok korszerűsítése, valamint a speciális nyomrögzítő eszközök beszerzése is.[623] A fejlesztések hatékony hasznosítása ugyanakkor a szervezeti integrációtól is függ, hiszen a modern technológiai megoldások akkor tudják leginkább kifejteni hatásukat, ha alkalmazásuk a mindennapi nyomozati gyakorlatba is fokozatosan beépül. Ennek megfelelően célszerű, hogy a jelentősebb bűnügyek nyomozási tervei a gyakorlatban is következetesen tartalmazzák az elektronikus bizonyítékok feltárásának és elemzésének lépéseit, beleértve a már bevett gyakorlatnak megfelelően a mobilkészülékek adatainak vizsgálatát, a kamerafelvételek rendszerezett begyűjtését, valamint a közösségi médiában fellelhető releváns információk szakszerű értékelését is. Végezetül megállapítható, hogy a digitalizáció számos korszerű és hatékony eszközt biztosít a nyomozó hatóságok számára, az igazságügyi adatmentéstől kezdve a kommunikáció megfigyelésén át egészen a nyílt forrású információgyűjtés és a mesterséges intelligencia alkalmazásáig. E technológiák eredményes használata azonban megköveteli a megfelelően képzett személyi állományt, a korszerű technikai hátteret, valamint a jogszerűségi és garanciális keretek következetes érvényesítését.[624]

6.3. A nyomozás jövője: fotogrammetria, digitális ikrek és VR-technológiák integrációja

A bűnügyi és baleseti helyszínelések folyamatát a filmekben gyakran futurisztikus eszközök segítségével mutatják be, miközben a valóságban a dokumentáció sokszor a múlt század technológiáira épül. A következőkben bemutatott projekt azonban új irányt mutat. Az IdomSoft Innovációs és Kutatási Csapata olyan rendszert fejleszt, amely olcsóbb vagy akár ingyenesen elérhető eszközöket (például a Cinema 4D, Blender, Unreal Engine grafikus motor, valamint a Meta Quest 2 VR-szemüveg) alkalmaz a

[623]Belügyminisztérium (BM): Megkezdődött a Rendőrség elektronikus rendszereinek korszerűsítése a közép-magyarországi régióban. https://bmprojektek.kormany.hu/megkezdodott-a-rendorseg-elektronikus-rendszereinek-korszerusitese-a-kozep-magyarorszagi-regioban1 (letöltés dátuma: 2024. október 11.)
[624]Európai Parlament jelentés (A9-0232/2021), 23. pont: a rendészeti és bírósági dolgozók számára kötelező speciális képzést sürget az AI etikai, jogi és technikai vonatkozásainak megismerésére, hogy felismerjék az algoritmusok torzításait és korlátait.

helyszínek gyors digitalizálására.[625] A rendszer fő erőssége, hogy a helyszínelők egy átlagos okostelefonnal 80–100 fényképet készítenek az objektum körül, és ezekből fotogrammetriai módszerrel háromdimenziós modellt állítanak elő. A VR-modell bármikor előhívható, a részletek újra vizsgálhatók, sőt a napszak és az időjárás is szimulálható.[626][627] A témával egy 2024-ben megrendezett szakmai rendezvényen „*A metaverzum és a mesterséges intelligencia lehetőségei és veszélyei*" NBT és vármegyei bűnmegelőzési tanácsülésén találkoztam, ahol Kellessy Tibor, az IdomSoft munkatársa mutatta be a rendszert. A demonstráció során VR-szemüveget viselve egy fiktív bűnügyi helyszínt jártunk be „Kovács nyomozó" szimulált esete alapján, amelyet az Országos Rendőr-főkapitányság épületében alakítottak ki. A 3D-s rekonstrukció minősége elsősorban a felhasznált fényképek számától és a kijelzők felbontásától függött, a virtuális térben apró tárgyak, nyomok és részletgazdag struktúrák is jól kivehetők voltak. Kellessy Tibor hangsúlyozta, hogy a technológia nemcsak bűncselekmények helyszínelésénél, hanem közlekedési balesetek esetében is hatékonyan alkalmazható, mivel céljuk egy olyan rendszer kialakítása, amely lehetővé teszi, hogy a helyszínelés 4–6 percen belül befejezhető legyen, ezáltal a forgalom mielőbbi helyreállítása is biztosítható.[628] A prezentációhoz két rövid videó is kapcsolódott. Az egyik a helyszínmodell AR- és VR-feldolgozását mutatta be, a másik pedig az úgynevezett „áldozat modellezést", amelyben egy női torzó, valamint a kezére kötött csomó részletei voltak vizsgálhatók. Kellessy Tibor kifejtette, hogy a csomó kötési technikája sajátos mintázatot követ, amely az ujjlenyomathoz hasonlóan egyedi azonosítóként értelmezhető. A harmadik modell egy sáros Merrell bakancs talpmintáját ábrázolta, amely a VR-környezetben minden apró barázdájában és szennyeződésében részletgazdagon megfigyelhető volt. [629] Az ilyen

---

[625]HWSW: Helyszínelés 3D-ben és VR-ban – ORFK/BRFK fotó- és 3D-dokumentációs bemutató (Unreal Engine, Meta Quest, Lightroom). https://www.hwsw.hu/hirek/66106/helyszineles-orfk-brfk-foto-3d-ar-vr-unreal-engine-meta-quest-lightroom-idomsoft-rendorseg.html (letöltés dátuma: 2024. október 13.)

[626]HWSW: Helyszínelés 3D-ben és VR-ban – ORFK/BRFK fotó- és 3D-dokumentációs bemutató (Unreal Engine, Meta Quest, Lightroom). https://www.hwsw.hu/hirek/66106/helyszineles-orfk-brfk-foto-3d-ar-vr-unreal-engine-meta-quest-lightroom-idomsoft-rendorseg.html (letöltés dátuma: 2024. október 13.)

[627] Kellessy Tibor: *Digital twin és AI a rendvédelemben.* Előadás. Budapest, 2024. szeptember 10. Nemzeti Bűnmegelőzési Tanács (NBT) és vármegyei bűnmegelőzési tanácsok ülése: „A metaverzum és a mesterséges intelligencia lehetőségei és veszélyei".

[628] Kellessy Tibor: *Digital twin és AI a rendvédelemben.* Előadás. Budapest, 2024. szeptember 10. Nemzeti Bűnmegelőzési Tanács (NBT) és vármegyei bűnmegelőzési tanácsok ülése: „A metaverzum és a mesterséges intelligencia lehetőségei és veszélyei".

[629] Kellessy Tibor: *Digital twin és AI a rendvédelemben.* Előadás. Budapest, 2024. szeptember 10. Nemzeti Bűnmegelőzési Tanács (NBT) és vármegyei bűnmegelőzési tanácsok ülése: „A metaverzum és a mesterséges intelligencia lehetőségei és veszélyei".

típusú 3D-s modellezés alapját a fotogrammetria képezi, amely a különböző szögből készített felvételek alapján teszi lehetővé a valóság pontos digitális rekonstrukcióját. A fotogrammetria, mint a kriminalisztikai gyakorlatban régóta alkalmazott módszer, a különböző szögből készített fényképek alapján háromdimenziós modellt hoz létre, amelyen pontos mérések végezhetők. A Cseh Műszaki Egyetem kutatása szerint a mobil fotogrammetria, a Pix4Dcatch és RTK eszközök együttes használatával 30 és 1300 közötti felvételből is képes nagy pontosságú 3D rekonstrukció előállítására, miközben gyorsabb és költséghatékonyabb alternatívát kínál a lézerszkennerekhez képest.[630] A Pix4Dcatch egy olyan mobil alapú fotogrammetriai alkalmazás, amely a digitális térbeli adatgyűjtést és háromdimenziós (3D) rekonstrukciót teszi lehetővé okoseszközök (elsősorban iPadek és okostelefonok) segítségével. A program működési elve a képalapú térmodellezés. A felhasználó a vizsgált objektum vagy terület körbejárása során nagyszámú, egymással átfedő képet készít, miközben a szoftver a beépített szenzorok (kamera, giroszkóp, gyorsulásmérő, LiDAR, ARKit) és a GPS-adatok integrálásával rögzíti az egyes felvételek térbeli pozícióját.[631] Az így gyűjtött adatokat a Pix4D ökoszisztémába tartozó szoftverek (például Pix4Dmapper, Pix4Dcloud) dolgozzák fel, amelyek algoritmikus úton háromdimenziós pontfelhőt, térbeli hálót (mesh) és ortofotót hoznak létre.[632] A technológia különösen hasznos az építészeti felmérések, ipari dokumentálás, valamint a bűnügyi és baleseti helyszínek digitális rögzítése területén, mivel a valós környezetet fotorealisztikus pontossággal, mérethelyesen és visszamérhetően rekonstruálja.[633]A Real Time Kinematic (RTK) technológia ezzel szemben egy nagy pontosságú helymeghatározási eljárás, amely a globális műholdas navigációs rendszerek (GNSS) jeleit valós időben korrigálja.[634] A módszer lényege, hogy egy fix bázisállomás és egy mozgó vevő közötti folyamatos adatátvitel révén kiszámítja a GPS-jelek fáziseltérését, és ennek alapján akár centiméteres pontosságú pozíciót határoz meg. Míg a hagyományos, beépített GPS-rendszerek tipikusan 3–5 méteres

[630]Pix4D: Crash scene analysis: testing Pix4D's solution for forensics. https://www.pix4d.com/blog/crash-scene-analysis-pix4d-forensic (letöltés dátuma: 2025. április 13.)
[631] Pix4D: App Overview – PIX4Dcatch. https://support.pix4d.com/hc/en-us/articles/7636967841437 (letöltés dátuma: 2025. április 13.)
[632]Pix4D: Support (Help Center). https://support.pix4d.com
[633]Gini, R. – Passoni, D. – Suriano, M. – Tamburini, A. – Travaglio, M.: Accuracy and Usability of 3D Models Generated by Smartphone Photogrammetry and LiDAR Scanners. = Sensors 2023/23(2), Art. 728. https://doi.org/10.3390/s23020728
(letöltés dátuma: 2024. október 13.)
[634]Leick, Alfred – Rapoport, Lev – Tatarnikov, Dmitry: *GPS Satellite Surveying.* Hoboken, John Wiley & Sons, 2015. 840 o.**,** 564–568. o. ISBN: 978-1-119-01826-1

eltéréssel dolgoznak, az RTK-korrekció alkalmazásával a helymeghatározás hibahatára 1–2 centiméterre csökkenthető. A Pix4Dcatch és RTK-eszközök kombinált alkalmazása a digitális helyszínelés és kriminalisztikai térmodellezés területén különösen jelentős technológiai előrelépést képvisel. Az RTK-alapú GNSS-vevő (például Emlid Reach RX, Leica GS18, Trimble Catalyst stb.) Bluetooth-kapcsolaton keresztül csatlakoztatható a Pix4Dcatch alkalmazáshoz, amely így nem csupán a vizuális adatokat, hanem a valós világ koordinátarendszeréhez illesztett, georeferált pozíciókat is rögzíti.[635] Ennek eredményeként a 3D-s modell nemcsak vizuálisan hiteles, hanem mérhető és bizonyító erejű digitális dokumentumként is funkcionálhat a bűnügyi helyszíni szemle során. A technológia alkalmazása tehát egyszerre növeli az adatgyűjtés objektivitását, reprodukálhatóságát és bizonyítási értékét, miközben csökkenti a manuális helyszínrögzítés hibalehetőségeit és időigényét. Egy másik tanulmány, amely kifejezetten okostelefonok kameráit vizsgálta, arra az eredményre jutott, hogy ezek is alkalmasak 3D modellek készítésére, bár a kamera előzetes kalibrációja tovább növeli a pontosságot. [636] Az a tény, hogy a háromdimenziós rekonstrukciók mérhető, megismételhető és bizonyító erejű digitális dokumentummá válhatnak, természetes módon vezet el a digitális iker fogalmához, amelynél a modell már nem csupán a helyszínrögzítés eszköze, hanem orvosszakértői és bírói értékelés alapjául is szolgálhat. A digitális iker definiciója (vagyis a valós tárgy, személy vagy környezet digitális másának létrehozása) egyre hangsúlyosabban jelenik meg a kriminalisztikai gyakorlatban. Ezt jól példázza a „*The Role of a Digital Twin in Supporting Criminal Investigations: A Case Report About a Possible Abuse”* című, a Forensic Science, Medicine and Pathology folyóiratban megjelent gyermekbántalmazásról szóló 2024-es esettanulmány amelyben a szerzők egy alacsony felbontású mobilvideó alapján rekonstruáltak egy háromdimenziós jelenetet.[637]A modell lehetővé tette a gyermek fejkerületének pontos mérését, ami bizonyítékként szolgált az esetleges bántalmazás időpontjának megállapításához. Ezen

[635]Pix4D: PIX4D ecosystem: new updates. https://www.pix4d.com/blog/pix4d-ecosystem-new-updates (letöltés dátuma: 2024. október 14.)
[636]Jasińska, Aleksandra – Pyka, Krystian – Pastucha, Elżbieta – Midtiby, Henrik Skov: A Simple Way to Reduce 3D Model Deformation in Smartphone Photogrammetry. = Sensors 2023/23(2), Art. 728. https://www.mdpi.com/1424-8220/23/2/728, https://doi.org/10.3390/s23020728 (letöltés dátuma: 2024. október 13.)
[637]Becker, Sven – Fritzsch, Tim Hanjo – Labudde, Dirk: The role of a digital twin in supporting criminal investigations – a case report about a possible abuse. = Forensic Science, Medicine and Pathology 2025/21, 245–254. o. https://link.springer.com/article/10.1007/s12024-024-00857-w (letöltés dátuma: 2025. október 14.)

esettanulmány rámutat arra, hogy a digitális ikrek nem csupán helyszínrekonstrukcióra, hanem orvosszakértői és jogi bizonyítékként is alkalmazhatók.[638] Mindez nem csupán ígéretes, hanem kifejezetten szükségszerű fejlődési irány a bizonyítás és a szakértői értékelés modernizálásában. Ezt támasztja alá a VR- és AR-technológiák kriminalisztikai alkalmazásáról készült 2025-ös áttekintés is, amely megállapítja, hogy az XR-eszközök javítják a bizonyítékok gyűjtésének pontosságát, növelik a hatékonyságot és elősegítik a csapatmunkát.[639] Ugyanakkor a kutatás rámutat arra is, hogy ezen technológiák használata etikai és technológiai kihívásokkal, valamint szabványosítási hiányosságokkal jár. A tanulmány kiemeli továbbá, hogy a virtuális helyszínek értelmezése kognitív torzításokat eredményezhet, és hangsúlyozza a megfelelő jogi és eljárásjogi keretek kialakításának szükségességét.[640] Amint azt az előző fejezetekben már részletesen áttekintettem, a Be. 205. § (1) bekezdése az „elektronikus adatot" úgy határozza meg, mint minden olyan tényt, információt vagy fogalmat, amely információs rendszerben feldolgozható, a (2) bekezdés pedig kifejezetten kimondja, hogy a tárgyi bizonyítási eszköz fogalma az elektronikus adatot is magában foglalja.[641][642] Mégis, a gyakorlatban a bíróságok jellemzően optikai adathordozón (CD-R, DVD-R) fogadják a digitális bizonyítékokat, és bizonyos esetekben méretkorlátot is alkalmaznak kompatibilitási és archiválási megfontolásokhoz igazodva.[643][644][645]Ez súlyosan korlátozza a nagyfelbontású fotogrammetriai modellek vagy VR-felvételek felhasználását. Az EU-ban az elektronikus bizonyítékok határokon átnyúló cseréjét a 2024-es SIRIUS Electronic Evidence Situation Report (Elektronikus bizonyítékokról szóló helyzetjelentés) szerint jelenleg több jogszabály és jogforrás (az EU Digital Services Act, az elektronikus bizonyítékokra vonatkozó jogalkotási csomag és a Budapesti Egyezmény második kiegészítő

[638]Becker, Sven – Fritzsch, Tim Hanjo – Labudde, Dirk: The role of a digital twin in supporting criminal investigations – a case report about a possible abuse. = Forensic Science, Medicine and Pathology 2025/21, 245–254. o. https://link.springer.com/article/10.1007/s12024-024-00857-w (letöltés dátuma: 2025. október 14.)
[639]Chango, Xavier – Flor-Unda, Omar – Bustos-Estrella, Angélica – Gil-Jiménez, Pedro – Gómez-Moreno, Hilario: Extended Reality Technologies: Transforming the Future of Crime Scene Investigation. https://www.preprints.org/manuscript/202506.1628/v1 (letöltés dátuma: 2025. október 14.)
[640]Chango, Xavier – Flor-Unda, Omar – Bustos-Estrella, Angélica – Gil-Jiménez, Pedro – Gómez-Moreno, Hilario: Extended Reality Technologies: Transforming the Future of Crime Scene Investigation. https://www.preprints.org/manuscript/202506.1628/v1 (letöltés dátuma: 2025. október 14.)
[641]Be. 205. § (1)
[642]Be. 205. § (2)
[643]Be. 155–159. §
[644]17/2014. (XII. 23.) OBH utasítás 3.pont
[645]17/2014. (XII. 23.) OBH utasítás 61. §

jegyzőkönyve) szabályoz, ugyanakkor a gyakorlati megvalósítás továbbra is összetett és lassú folyamat.[646][647][648][649] Ugyanakkor a jelentés is megerősíti azt, hogy az egyes tagállamokban dolgozó Egységes kapcsolattartó pont (Single Point of Contact (SPoC)) rendszerek és a nyomozók képzése kulcsfontosságú a gyors adatcseréhez.[650] A magyar joggyakorlat számára célszerűnek tűnik, hogy a nemzetközi tendenciákhoz igazodva fokozatosan kialakítsa a digitális ikrek és a virtuális valóság alapú modellek bírósági elfogadásának megfelelő, szakmailag és jogilag is megalapozott keretrendszerét. A konferencián szerzett élményeim alapján meggyőződtem arról, hogy a digitális helyszínelés valós alternatívát kínál a hagyományos módszerekkel szemben. A VR-alapú rendszer gyors, költséghatékony és könnyen használható eszközökre épül, és lehetővé teszi a bizonyítékok részletes újraelemzését. A technológia széles körű elterjedéséhez több egymást erősítő feltételnek kell teljesülnie. Mindenekelőtt jogszabályi modernizációra van szükség. A gyakorlatban méretkorlátot is alkalmaznak kompatibilitási és archiválási megfontolásokhoz igazodva, ami akadályozhatja a nagy állományú digitális ikrek bírósági bevitelét. Ennek feloldásához az elektronikus bizonyítékok online benyújtásának és a nagyobb adatméret kezelésének kifejezett jogi elfogadása szükséges. Ezzel párhuzamosan elengedhetetlenek a standardizált protokollok. Nemzetközi és hazai iránymutatások kellenek a fotogrammetriai felvételek készítésére, a 3D modellek hitelesítésére és a VR bemutatók bizonyító erejének meghatározására. A technológia bevezetésének hatékonyságát elsősorban a célzott képzés és a tudásmegosztás biztosíthatja. Célszerűnek látszik, hogy a helyszínelők,

---

[646]Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)

[647] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA), OJ L 277, 27.10.2022, pp. 1–102. (EU 2022/2065 rendelet DSA.)

[648]Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, pp. 118–179. (EU) 2023/1543 rendelet (e-Evidence rendelet)

[649]Council of Europe: Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), opened for signature: 12 May 2022 (Strasbourg); hivatalos szöveg és jegyzék: CoE Treaty Office. (HU rövidítés: „Budapesti Egyezmény, Második kiegészítő jegyzőkönyv (CETS 224).)

[650]Europol, Eurojust, European Judicial Network (EJN): SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1-73p. 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)

ügyészek és bírák számára olyan, gyakorlati szemléletű képzési modulok is elérhetők legyenek, amelyek a fotogrammetria, az adatbiztonság és a virtuális valóság technológiáinak alkalmazásával kapcsolatos alapvető ismereteket közvetítik. Mindemellett elengedhetetlen a világos etikai és adatvédelmi keretek kialakítása. A kiterjesztett valóság (XR: összefoglaló gyűjtőfogalom a VR/AR/MR technológiákra) alapú vizsgálatok esetében külön figyelmet kell fordítani a személyes adatok védelmére, a kognitív torzítások kockázatának csökkentésére, valamint a virtuális jelenetek manipulációs lehetőségeinek megfelelő szabályozására. „Kovács nyomozó esete" jól szemlélteti, hogy a játékipari technológiák és a fotogrammetriai módszerek integrálása új dimenziókat nyithat meg a kriminalisztikai gyakorlatban. A jövőben nem kizárt, hogy a bíróságok virtuális valóság-eszközök, például VR-szemüvegek segítségével vizsgálják a bizonyítékokat, ezáltal közvetlenebb és szemléletesebb módon értékelve a helyszíni rekonstrukciókat. Mindez azonban feltételezi a jogi, technológiai és oktatási keretek összehangolt, fokozatos fejlesztését, hogy a digitális megoldások bevezetése a jogbiztonság és a bizonyítási garanciák teljes körű érvényesülése mellett valósulhasson meg.

Hipotézisek vizsgálata

1. Az elkövetési szándék önmagában nem elegendő a büntethetőséghez: Feltételezem, hogy a bűncselekmény elkövetésére irányuló szándék puszta kinyilvánítása önmagában nem minősül büntetendő cselekménynek, amennyiben nem kapcsolódik konkrét cselekményekhez vagy előkészületi magatartáshoz. Ez különösen releváns a digitális térben megvalósuló fenyegetések és szándéknyilatkozatok értékelésekor.
2. Az internetes anonimitás és jogi felelősség hiánya elősegíti az online zaklatás és más személy elleni bűncselekmények terjedését: Hipotézisem szerint az online térben uralkodó anonimitás és a határokon átnyúló kommunikáció lehetősége növeli az ilyen típusú bűncselekmények elkövetésének gyakoriságát, továbbá jelentősen nehezíti a felelősségre vonást és a bizonyítást.

3. A digitális bűncselekmények számának növekedése összefügg az információbiztonsági tudatosság hiányosságaival: Feltételezem, hogy a személyes adatok fokozott sérülékenysége, valamint az online tranzakciókhoz kapcsolódó biztonsági rések növelik a digitális csalások, identitáslopások és adathalász támadások előfordulását.
4. A nemzetközi szabályozási keretek hatékonysága korlátozott: A Budapesti Egyezmény és hasonló nemzetközi jogi szabályozások bár szükségesek, önmagukban nem elégségesek a XXI. századi digitális bűncselekmények hatékony visszaszorításához. Feltételezem, hogy a jogharmonizáció nehézségei és a nemzetközi jogérvényesítés hiányosságai továbbra is jelentős kihívást jelentenek a bűnüldözés számára.

Az első hipotézis értékelése

Feltételezésem szerint a büntetőjogi felelősség megállapításához nem elegendő a szándék puszta kinyilvánítása, hanem konkrét, külsőleg is megnyilvánuló cselekményre van szükség. A kutatás során arra a következtetésre jutottam, hogy a digitális térben tett fenyegetések, online üzenetek vagy szándéknyilatkozatok önmagukban nem alapozzák meg a büntetőjogi felelősséget, amennyiben azok nem járnak együtt előkészületi vagy kísérleti magatartással. A digitális térben tett kijelentések, fenyegetések vagy virtuális megnyilvánulások önmagukban nem elegendőek a bűncselekmény tényállási elemeinek megvalósításához. A Be. bizonyítási szabályainak elemzése is megerősítette számomra, hogy a szándék bizonyítása csak akkor vezethet jogkövetkezményhez, ha az tényleges, az elkövető tudatos magatartásában is megnyilvánul. Következtetésem szerint az első hipotézisem megerősítést nyert. A digitális térben is kizárólag a tényleges, bizonyítható elkövetési magatartás tekinthető büntetendőnek, ezzel a büntetőjog ultima ratio jellegét kívántam hangsúlyozni.

A második hipotézis értékelése

A második hipotézisem szintén megerősítést nyert, mivel a kutatás során feltárt esetek és jogi elemzések alapján az internetes anonimitás és a jogi felelősség korlátozott érvényesülése egyértelműen elősegíti az online zaklatás és más személy elleni bűncselekmények terjedését. Feltételezésem, hogy a névtelenség, a határokon átnyúló kommunikáció, valamint a platformszolgáltatók részleges felelőssége hozzájárul a büntetlenség érzetéhez és az áldozatok védelmének hiányosságaihoz, beigazolódott. A DSA és a Budapesti Egyezmény rendelkezéseinek elemzése során arra a következtetésre jutottam, hogy bár ezek a szabályozások előremutatók, végrehajtásuk még nem biztosít kellő védelmet. Álláspontom szerint az online zaklatás visszaszorítása csak akkor lehet eredményes, ha az anonimitás korlátozása, az adatkiadási mechanizmusok hatékonyabbá tétele és a szolgáltatói felelősség erősítése egyensúlyba kerül a szólásszabadság védelmével. A vizsgálat kimutatta, továbbá, hogy a hatósági fellépést akadályozza a platformok közötti joghatósági széttagoltság és az adatigénylés nem egységes rendje. Következtetésem szerint a második hipotézisem megerősítést nyert. A digitális térben az anonimitás, a decentralizált adatáramlás és a határokon átnyúló kommunikáció valóban elősegíti a személy elleni online bűncselekmények terjedését és jelentős kihívást jelent a bizonyítás és a jogérvényesítés számára.

A harmadik hipotézis értékelése

A harmadik hipotézisem teljes mértékben igazolást nyert, mivel a vizsgálat eredményei szerint a digitális bűncselekmények számának növekedése szoros összefüggésben áll az információbiztonsági tudatosság hiányával. Feltételezésem szerint az alacsony szintű kiberbiztonsági ismeretek és a felhasználói tudatosság hiánya közvetlenül növeli a digitális csalások, adathalász-támadások és zsarolóvírusok előfordulását. Az Eurostat, az Europol SIRIUS és a Legfőbb Ügyészség statisztikai adatai alátámasztották a hipotézis helytállóságát és ez alapján arra a következtetésre jutottam, hogy a technológiai ismeretek hiánya nemcsak a civil felhasználók, hanem a nyomozó hatóságok körében is kockázati tényezőt jelent. Megítélésem szerint a bűnmegelőzés kulcsa a digitális

kompetenciák fejlesztésében, az oktatási programok megerősítésében és a tudatos felhasználói magatartás kialakításában rejlik, mivel a technológiai fejlődés üteme messze meghaladja a jogi adaptáció sebességét.

A negyedik hipotézis értékelése

A negyedik hipotézisem megerősítést nyert, ugyanis a kutatás során arra a következtetésre jutottam, hogy a nemzetközi szabályozási keretek hatékonysága valóban korlátozott a kiberbűnözés komplex, határokon átnyúló jellege miatt. A disszertáció jogösszehasonlító elemzése megerősítette a hipotézis helytállóságát. Az adatátvitelre, megőrzésre és átadásra vonatkozó hatásköri szabályok még mindig széttagoltak, ami késlelteti a nemzetközi együttműködést és akadályozza a valós idejű adat-hozzáférést. Feltételezésem szerint a Budapesti Egyezmény, a Digital Services Act és az e-Evidence Rendelet bár fontos mérföldkövek, önmagukban nem biztosítanak megfelelő választ a gyorsan fejlődő technológiai és bűnözési trendekre. Megítélésem szerint a legnagyobb problémát a joghatósági konfliktusok, az eltérő adatkiadási eljárások és az együttműködés hiányosságai okozzák, amelyek a bizonyítékok kezelését és felhasználását is jelentősen megnehezítik. A kutatás eredményei alapján úgy vélem, hogy a hatékony fellépéshez nem csupán jogharmonizációra, hanem az intézményi és technológiai szintek integrációjára is szükség van. Következtetésem szerint a jelenlegi nemzetközi jogi keretek alapvető fontosságúak, azonban nem biztosítanak kellően hatékony, egységes és gyors reagálási mechanizmust. A XXI. századi digitális bűnözés elleni fellépéshez koordinált, technológiailag egységesített és valós idejű adatáramlást biztosító nemzetközi jogérvényesítési modell kialakítása szükséges.

Összegzés

A kutatás a XXI. századi bűncselekmények vizsgálatán keresztül arra törekedett, hogy feltárja, miként formálja át a digitalizáció a büntetőjog, a büntetőeljárás hagyományos kereteit. A dolgozat célja nem pusztán a meglévő ismeretek rendszerezése volt, hanem a jogtudományi gondolkodás olyan új, innovatív irányainak kijelölése is, amelyek a

digitális bűnözés és a technológiai alapú bizonyítás területén nyújthatnak elméleti és gyakorlati kapaszkodót. Az értekezés központi tétele szerint a jogrendszernek szükségszerűen reagálnia kell a technológiai fejlődésre, ugyanakkor úgy, hogy közben megőrizze a büntetőjog ultima ratio jellegét és garantálja az eljárásjogi garanciák érvényesülését a digitális térben is. A kutatás egyik legfontosabb tudományos hozzájárulása abban áll, hogy új értelmezési keretet kínál a bizonyítékok és az online térben megvalósuló bűncselekmények dogmatikai megközelítéséhez. Az értekezés a jogrendszert nem statikus normatív struktúraként, hanem adaptív, technológiaérzékeny rendszerként mutatja be, amelynek képesnek kell lennie a mesterséges intelligencia, a kriptoeszközök, a deepfake-technológia, online bántalmazás és a metaverzum-jelenségek által teremtett új valóságok befogadására. A dolgozat innovatív módon veti fel a „digitális vagyon", a „virtuális jogtárgy" és a „digitális bűnügyi tér" kategóriáinak bevezetését, amelyek a jelenlegi büntetőjogi fogalomrendszert új dogmatikai dimenzióba helyezhetik. Az empirikus és dogmatikai elemzések alapján megállapítható, hogy a nemzetközi együttműködés (különösen a Budapesti Egyezmény, az Európai Unió Digital Services Act-je (2022/2065) és az e-Evidence Rendelet (2023/1543)) bár átfogó keretet biztosít, a gyakorlatban továbbra is lassú. A kutatás arra kívánt rámutatni, hogy a XXI. századi bűnüldözéshez elengedhetetlenek a gyorsabb, egységesített adat-hozzáférési és megőrzési protokollok, valamint a nemzeti hatóságok közötti állandó digitális kommunikációs csatornák kialakítása. Ennek érdekében a dolgozat javaslatot tesz egy központi elektronikus bizonyítékkezelő platform létrehozására, amely elősegítheti a hatóságok, a szolgáltatók és az igazságügyi szereplők közötti valós idejű, biztonságos adatáramlást. A disszertáció újdonságértéke elsősorban abban ragadható meg, hogy kísérletet tesz a kriminalisztikai innováció és a jogdogmatika összekapcsolására. A dolgozat bemutatja, hogy a fotogrammetria, a mesterséges intelligencia-alapú elemzések, valamint a VR- és XR-technológiák alkalmazása miként járulhat hozzá a bizonyítás korszerűsítéséhez, a tisztességes eljárás elvének tiszteletben tartása mellett.[651] A vizsgálat eredményei egyértelműen azt jelzik, hogy a jövő nyomozása egyre inkább adatvezérelt, technológiai alapú rekonstrukción fog nyugodni, nem kizárólag az emberi megfigyelésen. A dolgozat ennek megfelelően javasolja a nyomozó hatóságok képzési rendszerének

[651]Herke Csongor - Szabó Barbara: False confession as a possible cause of wrongful convictions. JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 10 : 2 pp. 9-21. , 13 p. (2023) ISSN:2360-4964

modernizálását, a mesterséges intelligencia és a kiberbiztonsági ismeretek kötelező integrálását, valamint a jogász–informatikus szakértői együttműködés intézményesítését. A kutatás tudományos újdonságát elsősorban abban a törekvésben látom, hogy ne csupán tartalmi, hanem módszertani szinten is új megközelítést képviseljen: a klasszikus jogi elemzést igyekeztem technológiai és kriminológiai dimenzióval kiegészíteni, ezáltal előmozdítva egy interdiszciplináris szemléletű tudásmodell kialakítását. Célom az volt, hogy a digitális korszak bűncselekményeit ne pusztán új elkövetési formákként, hanem a büntetőjogi gondolkodás átalakulásának lehetséges katalizátoraként mutassam be, ezzel is gazdagítva a témáról folyó tudományos diskurzust.

Summary

The research, through the examination of twenty-first-century crimes, sought to reveal how digitalization is reshaping the traditional framework of criminal law and criminal procedure. The purpose of the dissertation was not merely to systematize existing knowledge but also to outline new, innovative directions of legal scholarship that can provide both theoretical and practical guidance in the fields of digital crime and technology-based evidence. The central thesis of the study is that the legal system must inevitably respond to technological progress, while preserving the ultima ratio nature of criminal law and ensuring the effectiveness of procedural safeguards within the digital sphere. One of the most significant scientific contributions of the research lies in offering a new interpretative framework for the dogmatic understanding of evidence and crimes committed in the online space. The dissertation presents the legal system not as a static normative structure but as an adaptive, technology-sensitive system that must be capable of accommodating new realities created by artificial intelligence, crypto-assets, deepfake technology, online abuse, and metaverse phenomena. Innovatively, the study introduces the potential legal categories of “digital property,” “virtual legal object,” and “digital crime scene,” which may place the current conceptual framework of criminal law into a new dogmatic dimension. Based on empirical and dogmatic analyses, it can be concluded that while international cooperation (particularly the Budapest Convention, the European Union’s Digital Services Act (2022/2065), and the e-Evidence Regulation (2023/1543)) provides a comprehensive framework, its implementation in practice remains slow. The research aimed to demonstrate that twenty-first-century law enforcement requires faster

and more standardized data-access and data-preservation protocols, along with the establishment of permanent digital communication channels among national authorities. To this end, the dissertation proposes the creation of a centralized electronic evidence management platform to enable real-time, secure data exchange between authorities, service providers, and judicial actors. The novelty of the dissertation lies primarily in its attempt to bridge the gap between forensic innovation and legal dogmatics. It demonstrates how photogrammetry, AI-based analytical tools, and VR/XR technologies can modernize the process of evidence gathering while respecting the principles of a fair trial. The findings clearly indicate that the future of investigation will increasingly rely on data-driven, technology-based reconstruction rather than solely on human observation. Accordingly, the dissertation recommends the modernization of investigator training systems, the mandatory integration of artificial intelligence and cybersecurity knowledge, and the institutionalization of legal–IT expert cooperation. The scientific originality of the research is found above all in its methodological ambition to represent not only a substantive but also a procedural innovation: the classical legal analysis is complemented by technological and criminological dimensions, thereby advancing the development of an interdisciplinary model of knowledge. My aim was to present crimes of the digital age not merely as new forms of offending but as potential catalysts for the transformation of criminal law thinking thus enriching the ongoing scientific discourse on the subject.

Irodalomjegyzék

Aczél, Petra – Veszelszki, Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Gondolat Kiadó, 2023.

Ahmad, R. – Shah, M. A. – Wahid, A. – Khan, M. A.: Botnets Unveiled: A Comprehensive Survey on Evolving Threats, Detection Techniques, and Future Directions. = International Journal of Communication Systems 2024/3, e5056. o. DOI: 10.1002/ett.5056.

Alston, Philip – Goodman, Ryan (szerk.): International Human Rights. Oxford, Oxford University Press, 2013. 1580 o.

Anderson, Ross – Barton, Chris – Böhme, Rainer – Clayton, Richard – van Eeten, Michel J. G. – Levi, Michael – Moore, Tyler – Savage, Stefan: Measuring the Cost of Cybercrime. In: Böhme, Rainer (szerk.): The Economics of Information Security and Privacy. Berlin–Heidelberg, Springer, 2013. 265–300. o. Elérhető: https://doi.org/10.1007/978-3-642-39498-0_12 (letöltés dátuma: 2025. 03. 13.)

Axon, Louise – Erola, Arnau – Agrafiotis, Ioannis – Uuganbayar, Ganbayar – Goldsmith, Michael – Creese, Sadie: Ransomware as a Predator: Modelling the Systemic Risk to Prey. = Digital Threats: Research and Practice 2023/4, 1–38. o.

Bácskai Máté: A kriptovaluták büntetőjogi értelmezése a pénzmosás és a lopás tükrében. = Ügyészek Lapja 2024/1–2 (XXXIV. évfolyam), 103–111. o. Elérhető: https://ugyeszeklapja.hu/?p=4534 (letöltés dátuma: 2025. 09. 16.)

Becker, Sven – Fritzsch, Tim Hanjo – Labudde, Dirk: The role of a digital twin in supporting criminal investigations – a case report about a possible abuse. = Forensic Science, Medicine and Pathology 2025/21, 245–254. o. Elérhető: https://link.springer.com/article/10.1007/s12024-024-00857-w (letöltés dátuma: 2025. 10. 14.)

Bende-Szabó Gábor: Az Európai Közösség joga. = Európai Tükör 2000/6, 27–40. o.

Bodnár András Péter: A digitális bizonyítékok megjelenése a büntetőeljárásban – különös tekintettel a szakértő igénybevételére. = Büntetőjogi Szemle XI. évf. 1. sz. (2022), 19–29. o. Elérhető: https://ujbtk.hu/dr-bodnar-andras-peter-a-digitalis-bizonyitekok-

megjelenese-a-buntetoeljarasban-kulonos-tekintettel-a-szakerto-igenybevetelere/ (letöltés dátuma: 2023. 05. 27.)

Bodnár András Péter: Digitization in criminal proceedings – issues related to electronic data. = Büntetőjogi Szemle XI. évf. 1. sz. (2021), 19–29. o. Elérhető: https://ujbtk.hu/andras-peter-bodnar-digitization-in-criminal-proceedings-issues-related-to-eletronic-data/ (letöltés dátuma: 2025. 03. 13.)

Casey, Eoghan: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3. kiadás. London, Academic Press/Elsevier, 2011.

Citron, Danielle K. – Franks, Mary Anne: Criminalizing Revenge Porn. = Wake Forest Law Review 49. köt., 2014 nyár, 345–391. o. Elérhető: https://scholarship.law.bu.edu/faculty_scholarship/643 (letöltés dátuma: 2022. 08. 12.)

Clough, Jonathan: Principles of Cybercrime. Cambridge, Cambridge University Press, 2015. 10–11. o.

Dornfeld László: Az elektronikus bizonyítékszerzés aktuális kérdései. In: Kriminológiai Tanulmányok 56., 2019, 215–232. o.

Dornfeld László: Fájlmegosztás: a szellemi tulajdonjog legújabb kihívása. = Diskurzus 2014/1., 4. évf., 54–61. o. Elérhető: http://blszk.sze.hu/iv-evfolyam-2014 (letöltés ideje: 2023. 07. 07.)

Douligeris, C. – Mitrokotsa, A.: DDoS attacks and defense mechanisms: classification and state-of-the-art. = Computer Networks 2004/5, 643–666. o. DOI: 10.1016/j.comnet.2003.10.003.

Eoghan Casey: Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet (3. kiadás). Academic Press/Elsevier, 2011, 3. o.

Eszteri Dániel: A számítógépes bűnözés legújabb tendenciái, különös tekintettel az online közösségi tereken elkövetett visszaélésekre. = Magyar Rendészet 2013/1, 55–69. o.

Eszteri Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. = Infokommunikáció és Jog 2017/1, 25–31. o. Elérhető: https://infojog.hu/eszteri-daniel-egy-bitcoinnal-elkovetett-vagyon-elleni-buncselekmeny-es-az-ahhoz-kapcsolodo-egyes-jogi-kerdesek-20171-68-25-31-o/ (letöltés dátuma: 2021. 05. 15.)

Fantoly Zsanett – Herke Csongor – Szabó Barbara: *The role of AI-based systems in negotiated proceedings.* eRevue internationale de droit pénal 7 Paper: 18 , 8 p. (2023) ISSN: 2522-2945

Falus Orsolya – Józwiak Piotr – Kővári Attila: „Gólyakalifa" a 21. században – Joghézag és analógia a virtuális valóság jogában. = Jogelméleti Szemle 2022/2, 20–33. o.

Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. = Magyar Jog 2014/7–8., 433–443. o. Elérhető: https://szakcikkadatbazis.hu/doc/3072353 (letöltés dátuma: 2022. 05. 27.)

Fenyvesi Csaba – Herke Csongor – Tremmel Flórián (szerk.): Kriminalisztika. 4. kiadás. Budapest–Pécs, Dialóg Campus Kiadó, 2022.

Gácsi Anett Erzsébet: A digitális bizonyíték és a kriminalisztika fejlődése a XXI. században. = Magyar Rendészet 2022/3., 45–55. o.

Gácsi Anett Erzsébet: Az elektronikus bizonyítás alapvető dogmatikai kérdései. = Magyar Rendészet 18(2), 2018, 77–89. o. Elérhető: https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1360 (letöltés: 2022. 05. 27.)

Gaál Tibor: A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban. = Belügyi Szemle 66. évf. 7–8. sz. (2018) 22–35. o. DOI: 10.38146/BSZ.2018.7-8.2

Gelgi, Metehan – Guan, Yueting – Arunachala, Sanjay – Rao, Maddi Samba Siva – Dragoni, Nicola: Systematic Literature Review of IoT Botnet DDoS Attacks and Evaluation of Detection Techniques. = Sensors (Basel) 2024/11, 3571. o.

Gibbons, Llewellyn J.: Law and the Emotive Avatar. = Vanderbilt Journal of Entertainment & Technology Law 2009/11(4), 899–920. o.

Greenberg, Andy: Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York, Doubleday, 2019.

Herke Csongor: A digitalizáció szerepe a büntetőeljárásban. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécs, PTE ÁJK, 2019, 104–113. o.

Herke Csongor: A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra. = Magyar Jog 71. évf., 6. sz. (2024), 321–332. o.

Herke Csongor: Büntető eljárásjog. Budapest, Ludovika Egyetemi Kiadó, 2022. 327 o.

Herke Csongor: Büntető eljárásjog. Egyetemi jegyzet. Pécs, Baufirma Kiadó, 2021. 327 o.

Herke Csongor: Deepfake: áldás vagy átok? Jogi szabályozási szempontok. = Pro Futuro 13(1), 2023, 157–178. o. DOI: 10.26521/profuturo/2023/1/13334

Herke Csongor: Mesterséges intelligencia a büntetőjogi döntéshozatalban. = Jogtudományi Közlöny 2023/4., 165–176. o. Elérhető: https://szakcikkadatbazis.hu/doc/1207285 (letöltés dátuma: 2024. 01. 05.)

Herke Csongor – Szabó Barbara: *False confession as a possible cause of wrongful convictions.* JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW 10 : 2 pp. 9-21. , 13 p. (2023) ISSN:2360-4964

Herke Csongor – Szabó Barbara: *Limits of Freedom of Public Authorities with Respect to Obtaining Evidence at the Stage of Investigation: Hungarian Report.* In: Maria Rogacka-Rzewnicka (szerk.), *Limits of Freedom of Public Authorities with Respect to Obtaining Evidence at the Stage of Investigation: A Comparative Legal Study.* Leiden, Hollandia: Brill/Nijhoff, 2024. pp. 129–144. ISBN-10 9004710310, ISBN-13 978-9004710313

Kiss Károly: A környezetvédelmi adóreformok jóléti hatásai az EU-ban. In: Inotai András (szerk.): EUtanulmányok. Budapest, Nemzeti Fejlesztési Hivatal, 2004. 1067–1088. o.

Kovács Zoltán (szerk.): A kibernyomozói munka büntetőjogi sajátosságai. Budapest, Nemzeti Közszolgálati Egyetem, 2023. 115 o. DOI: 10.37372/mrttvpt.2023.4

Leick, Alfred – Rapoport, Lev – Tatarnikov, Dmitry: GPS Satellite Surveying. Hoboken, John Wiley & Sons, 2015. 840 o., 564–568. o. ISBN: 978-1-119-01826-1

Letsas, George: A Theory of Interpretation of the European Convention on Human Rights. Oxford, Oxford University Press, 2007. 15–48. o.

Manfred Nowak – William A. Schabas (szerk.): U.N. Covenant on Civil and Political Rights: CCPR Commentary. 3. kiadás. Kehl, N.P. Engel Verlag, 2019.

Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. = Pro Futuro 2018/1, 66–83. o.

Mezei Kitti: Ügyészek Lapja 2020/3., 54–55. o.

Mezei Géza: Helyreállított Európa. Budapest, Osiris Kiadó, 2001. 343 o.

Mezrich, Ben: Az első bitcoinmilliárdosok. Ford. Marczali Tamás. Budapest, Alexandra Kiadó, 2022.

Olweus, Dan: Iskolai zaklatás. = Educatio 1999/4, 717–739. o. Elérhető: http://www.hier.iif.hu/hu/educatio_reszletes.php?id=26 (letöltés dátuma: 2020. 02. 11.)

Phillips, Kirsty – Davidson, Julia C. – Farr, Ruby R. – Burkhardt, Christine – Caneppele, Stefano – Aiken, Mary P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. = Forensic Sciences 2022/2(2), 379–398. o. DOI: 10.3390/forensicsci2020028

Qin, Hua Xuan – Wang, Yuyang – Hui, Pan: Identity, crimes, and law enforcement in the Metaverse. = Humanities and Social Sciences Communications 2025/12, Art. 194. https://doi.org/10.1057/s41599-024-04266-w (letöltés: 2025. 03. 17.)

Rainey, Bernadette – McCormick, Pamela – Ovey, Clare (szerk.): Jacobs, White and Ovey: The European Convention on Human Rights. Oxford, Oxford University Press, 2021. 792 o.

Schneier, Bruce: Secrets and Lies: Digital Security in a Networked World. Wiley, 2000. ISBN: 978-0471253112

Szabó Barbara: *Abuses in Virtual Space and Aiding Suicide. Essays of Faculty of Law University of Pécs Yearbook 2021–2022*, Pécs: PTE ÁJK, 2023. pp. 183–190. (2023) DOI: 10.15170/studia.2023.01.11 ISSN:2939-8606, ISSN:2061-8824

Szabó Barbara: *Crimes Committed on Online Surfaces.* In: Tóth Dávid (szerk.), *Az internet és a közösségi média jogi kihívásai – Konferenciakötet.* Pécs: PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, 2022. pp. 80–87. *8 p. ISBN: 9789634299929*

Szabó Barbara: *Cyber Harassment and the Law.* In: Kovács Bettina – Glázer-Kniesz Adrienn – Tislér Ádám (szerk.), *XII. Interdiszciplináris Doktorandusz Konferencia – konferenciakötet = 12th Interdisciplinary Doctoral Conference – Conference Proceedings.* Pécs: PTE Doktorandusz Önkormányzat, 2024. pp. 56–69. *14 p. ISBN: 978-963-626-282-2*

Szabó Barbara: *Digital Crime: New Challenges for Criminal Justice Systems.* Tomita, Mihaela – Ungureanu, Roxana (szerk.): Designing the Future of Criminal Justice System Under the Lens of Technology. International Conference "Multidisciplinary Perspectives in the Quasi-Coercive Treatment of Offenders" (SPECTO – 8th Edition), 16–17 May 2024, Timișoara, Romania. Bologna, Filodiritto Editore, 2024. ISBN 979-12-80225-72-6, DOI: 10.26352/I516-SPECTO-2024. 122-132. p.

Szabó Barbara: *Digitális Zaklatás Elleni Küzdelem: Németország és az USA Megközelítései.* Gaál Gyula – Hautzinger Zoltán (szerk.): A rendészet tudománya és gyakorlata. Tudományos Közlemények XXVI. Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja – Magyar Rendészettudományi Társaság, (2024.) 137-141o. ISSN:1589-1674

Szabó Barbara: *Mobbing im XXI. Jahrhundert.* Bartkó, Róbert (szerk.) Doktori Műhelytanulmányok 2024 - Doctoral Working Papers 2024 Győr, Magyarország : Universitas-Győr Nonprofit Kft. (2024) pp. 451-461. , 11 p. ISSN 2064-1788

Szabó Barbara: *Online Crime of Violence on Virtual Platforms.* In: *IRC 2022 – XVI. International Research Conference Proceedings.* Pulau Bali, Indonézia: WASET, 2022. pp. 122–125. 4 p.IRC 2022 XVI. International Research Conference Proceedings open science index 16 2022 October 20-21, 2022 Bali Indonesia International Scholarly and Scientific research & innovation ISSN:1307-6892

Szabó Barbara: *Problematic internet use, endangering children and minors.* In Jámborné, Róth Erika (szerk.) Doktoranduszok fóruma, 2022 Miskolc-Egyetemváros, Magyarország : Miskolci Egyetem, Állam- és Jogtudományi Kar (2023) 232 p. pp. 185-189. , 7 p. ISBN: 9789633583272

Szabó Barbara: *Rechtliche Maßnahmen und Schutzstrategien gegen Online-Belästigung.* KRE-DIT: A KRE-DOK Online Tudományos Folyóirat, VII/2. szám (2024) (megjelenés 2025.) *121 ISSN 2630-8711*

Szabó Barbara: *Virtual pandemonium.* In Kajos, L F; Bali, Cintia; Puskás, T; Szabó, R (szerk.) XI. Interdiszciplináris Doktorandusz Konferencia 2022 Tanulmánykötet : 11th Interdisciplinary Doctoral Conference 2022 Conference Book Pécs, Magyarország : Pécsi Tudományegyetem Doktorandusz Önkormányzat (2023) 692 p. pp. 526-533. , 8 p. ISBN:9789636260705

Stallings, S.: Hash Functions and Their Applications. = International Journal of Computer Applications, 2011. Elérhető: https://www.researchgate.net/publication/325090921_Hash_Functions_and_Their_Applications (letöltés dátuma: 2022. 04. 29.)

Taylor, Paul J. – Dargahi, Tooska – Dehghantanha, Ali – Parizi, Reza M. – Choo, Kim-Kwang Raymond: Blockchain for Cybersecurity: Systematic Literature Review and Directions for Future Research. = Journal of Computer Information Systems, 2021. DOI: 10.1080/08874417.2021.1995914.

Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: Kriminalisztika – Tankönyv és atlasz. Budapest–Pécs, Dialóg Campus, 2005.

Varga Árpád: Az adathalászat általános jellemzői, trendjei és észlelési kérdései napjainkban. = Infokommunikáció és Jog, 2020/1. (74.), 14–20. o. Elérhető: https://szakcikkadatbazis.hu/doc/1134438 (letöltés dátuma: 2021. 01. 14.)

Wildman, N. – McDonnell, N.: The puzzle of virtual theft. = Analysis 2020/80(3), 493–499. o. Elérhető: http://eprints.gla.ac.uk/210232/ (letöltés dátuma: 2025. 09. 16.)

Wright, Michelle F. – Wachs, Sebastian – Vazsonyi, Alexander T. – Gámez-Guadix, Manuel: To intervene or not to intervene: Young adults' views on when and how to intervene in online harassment situations. = Journal of Computer-Mediated Communication 2023/28(5), zmad027. Elérhető: https://academic.oup.com/jcmc/article/28/5/zmad027/7237464 (letöltés dátuma: 2023. 10. 27.)

Internetes forrásjegyzék

ATF: National Integrated Ballistic Information Network (NIBIN). Elérhető: https://www.atf.gov/firearms/national-integrated-ballistic-information-network-nibin (letöltés dátuma: 2024. 10. 11.)

Belügyminisztérium Statisztikai Rendszere: Regisztrált bűncselekmények. Elérhető: https://bsr-sp.bm.hu/SitePages/ExcelMegtekinto.aspx (letöltés dátuma: 2024. 01. 10.)

Bende-Szabó Gábor: Az Európai Közösség joga. = Európai Tükör 2000/6, 27–40. o. (online megjelenés)

BH 1989.184.; BH 2009.264. I.; EBH 2009.2033. I. (Bírósági Határozatok Gyűjteménye)

Big Brother Watch és társai kontra Egyesült Királyság (EJEB). Elérhető: https://hudoc.echr.coe.int/eng?i=002-12080 (letöltés dátuma: 2023. 06. 02.)

Blueforce Learning: What is Mobile Data, and How is it Used in Criminal Investigations? Elérhető: https://www.blueforcelearning.com/blog/what-is-mobile-data-and-how-is-it-used-in-criminal-investigations (letöltés dátuma: 2025. 01. 29.)

Borgaonkar, Ravishankar – Martin, Andrew – Park, Shinjo – Shaik, Altaf – Seifert, Jean-Pierre: White-Stingray: Evaluating IMSI Catchers Detection Applications. WOOT '17. Elérhető: https://www.usenix.org/system/files/conference/woot17/woot17-paper-park.pdf (letöltés dátuma: 2024. 10. 07.)

Büntető Törvénykönyv. Strafgesetzbuch (StGB) – §185, §186, §187, §201, §201a, §238, §241. Németország.

Bundeskriminalamt: Cybercrime. Elérhető: https://www.bka.de (letöltés dátuma: 2024. 05. 05.)

Bundesministerium der Justiz: Onlinewache. Elérhető: https://justizonline.gv.at/jop/web/formulare/gruppe/6/17 (letöltés dátuma: 2024. 05. 05.)

CASEY Eoghan – számos hivatkozás, lásd Felhasznált irodalom.

CCPR Centre: Simple Guide on the ICCPR. Elérhető: https://ccprcentre.org/files/media/ICCPR_easy_to_read_commentary_WEB.pdf (letöltés dátuma: 2022. 04. 28.)

CERT Advisory CA-2000-04: Love Letter Worm. US-CERT, 2000. Elérhető: https://www.cert.org/advisories/CA-2000-04.html

Chango, Xavier – Flor-Unda, Omar – Bustos-Estrella, Angélica – Gil-Jiménez, Pedro – Gómez-Moreno, Hilario: Extended Reality Technologies… Preprints.org. Elérhető: https://www.preprints.org/manuscript/202506.1628/v1 (letöltés dátuma: 2025. 10. 14.)

Christidis, Konstantinos – Devetsikiotis, Michael: Blockchains and smart contracts for the IoT. = IEEE Access 4 (2016), 2292–2303. o. Elérhető:

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408 (letöltés dátuma: 2022. 04. 07.) DOI: 10.1109/ACCESS.2016.2566339

Connolly, Kate: Germany investigates Second Life child pornography. https://www.theguardian.com/technology/2007/may/08/secondlife.web20 (letöltés dátuma: 2024. október)

Council of Europe: ECHR – hivatalos magyar fordítás. Elérhető: https://www.echr.coe.int/documents/d/echr/convention_hun (letöltés dátuma: 2022. 04. 28.)

Council of Europe: Online és technológia által elősegített emberkereskedelem – összefoglaló. Elérhető: https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c (letöltés dátuma: 2022. 05. 23.)

Data Retention and Investigatory Powers Act 2014 (UK). Elérhető: https://www.legislation.gov.uk/ukpga/2014/27/contents (letöltés dátuma: 2023. 04. 18.)

Demeter Gabriella: Daktiloszkópiai nyilvántartás Magyarországon – Az ujj- és tenyérlenyomatok bűnügyi célú kezelése. Elérhető: https://www.jogiforum.hu/files/publikaciok/demeter_gabriella__daktiloszkopiai_nyilvantartas_magyarorszagon%5Bjogi_forum%5D.pdf (letöltés dátuma: 2024. 10. 11.)

Digital Watch Observatory: Encryption. Elérhető: https://dig.watch/topics/encryption (letöltés dátuma: 2024. 05. 06.)

Dornfeld László: A határokon átnyúló elektronikus bizonyítékgyűjtés szabályozása az EU-ban. = Infokommunikáció és Jog 2019/2., 37–42. o.

ECHR ítéletek: Schenk v. Switzerland (1988); Khan v. UK (2000); Dragojević v. Croatia (2015); Roman Zakharov v. Russia (2015). HUDOC (letöltés dátuma: 2023. 08. 11.)

Electronic Privacy Information Center (EPIC): Deep Packet Inspection and Privacy. Elérhető: https://archive.epic.org/privacy/dpi/ (letöltés dátuma: 2024. 10. 07.)

ENISA: Threat Landscape 2022. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (letöltés dátuma: 2022. 04. 16.)

Europol: IOCTA 2020; IOCTA 2024. Elérhető: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (letöltés dátuma: 2024. 08. 06.)

Europol: 150 arrested in dark web drug bust… Elérhető: https://www.europol.europa.eu/media-press/newsroom/news/150-arrested-in-dark-web-drug-bust-police-seize-%E2%82%AC26-million (letöltés dátuma: 2025. 05. 14.)

Europol – Eurojust – EJN: SIRIUS EU Electronic Evidence Situation Report 2024. The Hague, 1–73. o. Elérhető: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. 12. 14.)

Europol, Eurojust, European Judicial Network (EJN): *SIRIUS EU Electronic Evidence Situation Report 2024.* The Hague, 1–73. o., 2024. Elérhető: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (letöltés dátuma: 2024. december 14.)

EU Innovation Hub: First Report on Encryption, 2024. Elérhető: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf (letöltés dátuma: 2025. 01. 11.)

Európai Bizottság: A Biztonsági Unió Stratégiája (COM(2020) 605); EU Cybersecurity Strategy (JOIN(2020) 18); e-Evidence javaslat (COM(2018) 225). (letöltések: 2022. 05. 01–06.)

Európai Parlament: AI in criminal law – A9-0232/2021. (23. pont) (letöltés dátuma: 2024. 10. 11.)

FBI/US DOJ: United States v. Ross Ulbricht – Indictment. Elérhető: https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf (letöltés dátuma: 2022. 09. 14.)

FinanceFeeds: Russian-Israeli Accused In $190M Nomad Bridge Hack Faces US Extradition. Elérhető: https://financefeeds.com/russian-israeli-accused-in-190m-nomad-bridge-hack-faces-us-extradition/ (letöltés dátuma: 2025. 05. 15.)

FoundationRA: Rest of World Deep Fake AI Laws. Elérhető: https://foundationra.com/rest-of-world-deep-fake-ai-laws/ (letöltés dátuma: 2025. 08. 12.)

Gaál Tibor: Belügyi Szemle 2018/7–8., 22–35. o. DOI: 10.38146/BSZ.2018.7-8.2 (online elérhetőség)

Gácsi Anett Erzsébet – több hivatkozás, lásd Felhasznált irodalom.

Gerő Péter – Endersz Péter: Biztonságosan és magabiztosan II. (openSUSE, GNOME). Elérhető: https://mek.oszk.hu/09300/09321/pdf/biztonsagosan2gnome.pdf (letöltés dátuma: 2021. 04. 14.)

Gini, R. – Passoni, D. – Suriano, M. – Tamburini, A. – Travaglio, M.: Accuracy and Usability of 3D Models… = Sensors 2023/23(2), 728. DOI: 10.3390/s23020728 (letöltés: 2024. 10. 13.)

Google Cloud: Dissecting the Nomad Bridge Hack… Elérhető: https://cloud.google.com/blog/topics/threat-intelligence/dissecting-nomad-bridge-hack (letöltés dátuma: 2022. 11. 29.)

Hogan Lovells: France prohibits non-consensual deep fakes. Elérhető: https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes (letöltés dátuma: 2025. 08. 13.)

Hollósi Gábor: Levelező jogászhallgatók rétegződése és pályaképe. Elérhető: http://www.jogiforum.hu/files/publikaciok/hollosi_gabor-levpalya.doc (letöltés dátuma: 2004. 03. 16.)

HWSW: Helyszínelés 3D-ben és VR-ban – ORFK/BRFK bemutató. Elérhető: https://www.hwsw.hu/hirek/66106/helyszineles-orfk-brfk-foto-3d-ar-vr-unreal-engine-meta-quest-lightroom-idomsoft-rendorseg.html (letöltés dátuma: 2024. 10. 13.)

Indiatimes: Fact check – Sam Altman GPU theft video? Elérhető: https://www.indiatimes.com/trending/fact-check-is-that-really-sam-altman-in-viral-gpu-theft-video-sora-2-clip-sparks-debate-among-netizens/articleshow/124257170.html (letöltés dátuma: 2025. 09. 30.)

INHOPE: What is child sexual abuse material detection? Elérhető: https://inhope.org/EN/articles/what-is-child-sexual-abuse-material-detection (letöltés dátuma: 2025. 10. 11.)

Interpol: Cybercrime Directorate; Metaverse white paper (2024); Databases; SLTD; IBIN. Elérhető: https://www.interpol.int/ (letöltés dátuma: 2024–2025.)

Jasińska, A. – Pyka, K. – Pastucha, E. – Midtiby, H. S.: A Simple Way to Reduce 3D Model Deformation… = Sensors 2023/23(2), 728. Elérhető: https://www.mdpi.com/1424-8220/23/2/728 (letöltés dátuma: 2024. 10. 13.)

Kaspersky: Ransomware: What is it and how to protect yourself. Elérhető: https://www.kaspersky.com/resource-center/threats/ransomware (letöltés dátuma: 2024. 03. 13.)

Kellessy Tibor: Digital twin és AI a rendvédelemben. Előadás (NBT), 2024. 09. 10.

KiberPajzs: Csalástípusok. Elérhető: https://kiberpajzs.hu/csalastipusok (letöltés dátuma: 2023. 05. 30.)

KiberPajzs (Mastercard kutatás, 2025): 2024-es kár – tízmilliárdos nagyságrend, tízezres számú áldozat. (Sajtóközlés, 2025. 02. 20.)

Kriptomat: Mi az a blokklánc technológia és hogyan működik? Elérhető: https://kriptomat.io/hu/blockchain/mi-az-a-blockchain-technologia/ (letöltés dátuma: 2022. 05. 06.)

Legfőbb Ügyészség: Tájékoztató a bűnözés 2022. évi adatairól. Elérhető: https://ugyeszseg.hu/repository/mkudok34379.pdf (letöltés dátuma: 2024. 05. 29.)

Magyar Nemzeti Bank: Az adathalász csalások legjellemzőbb típusai. Elérhető: https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai (letöltés dátuma: 2025. 05. 16.)

Magyar Posta Zrt.: Figyelem! Adathalász levelek és SMS-ek. Elérhető: https://www.posta.hu/aktualitasok/adathalasz_levelet_es_smst_kuldenek_a_magyar_posta_neveben_20230628 (letöltés dátuma: 2023. 09. 29.)

Magyar Rendőrség: Dark weben bonyolította le a drogbizniszt. Elérhető: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/dark-weben-bonyolitotta-le-a-drogbizniszt (letöltés dátuma: 2024. 06. 22.)

Manapság (összefoglaló állítás): 2025-ben 30,9 milliárd IoT-eszköz – lásd Statista tétel.

Mándi Veronika: A személyes adatok kezelése a büntetőeljárásban és a nyilvánosság kapcsolata. = Büntetőjogi Szemle 2023/1., 54–63. o. Elérhető: https://ujbtk.hu/mandi-veronika-a-szemelyes-adatok-kezelese-a-buntetoeljarasban-es-a-nyilvanossag-kapcsolata/ (letöltés dátuma: 2023. 05. 19.)

Major Cities Chiefs Association (MCCA): Metaverse Reference Guide (2024). Elérhető: https://majorcitieschiefs.com/wp-content/uploads/2025/06/MCCA_Metaverse-Reference-Guide_Oct-2024.pdf (letöltés dátuma: 2024. 12. 16.)

Magyar Nemzeti Bank: Kriptoeszközök és szolgáltatók – kérdések és válaszok. (2024. 05. 07.) Elérhető: https://www.mnb.hu/letoltes/24-05-07-kriptoeszkozok-es-szolgaltatok-kerdesek-valaszok-final.pdf (letöltés dátuma: 2024. 05. 08.)

Magyar Nemzeti Bank: Kriptoeszköz-szolgáltatók engedélyezése – Útmutató. Elérhető: https://www.mnb.hu/letoltes/casp-tevekenysegi-engedelyezesi-utmutato.pdf (letöltés dátuma: 2025. 05. 16.)

NKI: Éves kiberbiztonsági jelentés (2023; 2024). Elérhető: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf (letöltés dátuma: 2024. 04. 16.)

NMHH: Hozzájárulás nélkül közzétett tartalom; Online zaklatás; Gyermekkel szembeni online szexuális bántalmazás. Elérhető: https://nmhh.hu/ (letöltés dátuma: 2024. 11. 12.)

NIST: SP 800-101r1 (2014) – Mobile Device Forensics; NISTIR 8354 (2022) – Anti-Forensics. (letöltés dátuma: 2024. 08. 11.)

OECD Guidelines for the Security of Information Systems and Networks (1992).

OpenAI: Sora 2. Elérhető: https://openai.com/index/sora-2/ (letöltés dátuma: 2025. 09. 30.)

OpenText: EnCase Forensic – Product Overview. Elérhető: https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-po-encase-forensic-en.pdf (letöltés dátuma: 2024. 10. 07.)

Országgyűlés, Képviselői Információs Szolgálat: Deepfake technológia és jog. Infojegyzet 2024/20. Elérhető: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_20_deepfake_technologia_es_jog (letöltés dátuma: 2024. 08. 11.)

Parliament UK – UK Government: Online Safety Act explainer; Online Safety Act 2023. (letöltés dátuma: 2025. 08. 13.)

Pix4D: PIX4D ecosystem: new updates; Crash scene analysis; App Overview – PIX4Dcatch; Support. Elérhető: https://www.pix4d.com/ és https://support.pix4d.com (letöltések: 2024–2025.)

Police Hungary (YouTube): Dark weben bonyolította le a drogbizniszt. Elérhető: https://www.youtube.com/watch?v=GVxHK4D6ezc (letöltés: 2024. 06. 22.)

Privacy International: IMSI-catchers – Legal Analysis (2020). Elérhető: https://privacyinternational.org/sites/default/files/2020-06/IMSI%20catchers%20legal%20analysis.pdf (letöltés dátuma: 2024. 10. 07.)

Radware: Carding – What Is It and How Does It Work? Elérhető: https://www.radware.com/cyberpedia/bot-management/carding/ (letöltés dátuma: 2025. 05. 16.)

RAND Corporation: Digital Evidence and the U.S. Criminal Justice System (2015). Elérhető: https://www.rand.org/pubs/research_reports/RR890.html (letöltés dátuma: 2024. 10. 06.)

Reuters: South Korea to criminalise watching or possessing sexually explicit deepfakes (2024. 09. 26.); Why South Korea is on high alert… (2024. 08. 30.).

Róth Erika: Az elektronikus adat megszerzését, megőrzését szolgáló kényszerintézkedések. = Infokommunikáció és Jog 2020/2., 10–15. o. Elérhető: https://szakcikkadatbazis.hu/doc/2147096 (letöltés dátuma: 2024. 10. 07.)

Reuters: FBI checks gambling in Second Life virtual world. https://www.reuters.com/article/technology/fbi-checks-gambling-in-second-life-virtual-world-idUSN03278658/ (letöltés dátuma: 2024. október 18.)

Schrems-ügyek: C-362/14; C-311/18 – EUB ítéletek. Elérhető: https://curia.europa.eu (letöltés dátuma: 2023. 05. 30.)

SecurityWeek (Ionut Arghire): PayPal Phishing Campaign Employs Genuine Links… (2025. 01. 10.) Elérhető: https://www.securityweek.com/paypal-phishing-campaign-employs-genuine-links-to-take-over-accounts/ (letöltés dátuma: 2025. 01. 13.)

Statista: Number of IoT connected devices worldwide (2022–2033). Elérhető: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (letöltés dátuma: 2022. 05. 06.)

Threat Lab / EFF: Gotta Catch 'Em All – IMSI-Catchers (2019). Elérhető: https://www.eff.org/files/2019/07/09/whitepaper_imsicatchers_eff_0.pdf (letöltés dátuma: 2024. 10. 07.)

UNICEF: Poll on online bullying (2019. 09. 04.). Elérhető: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying (letöltés dátuma: 2020. 05. 27.)

United States Attorney's Office, SDNY: Two Defendants Charged in NFT Fraud… Elérhető: https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0 (letöltés dátuma: 2024. 10. 16.)

UNODC: Court Case Summaries – GLOTIP 2022. Elérhető: https://www.unodc.org/documents/data-and-analysis/glotip/2022/Court_Cases_Summaries_GLOTIP_2022_web.pdf (letöltés dátuma: 2023. 05. 21.)

USA Today; The Sun; Leggo.it: TikTok „Blackout challenge" esetei (2021) – online cikkek (letöltések: 2021. 02–07.)

U.S. Congress: S. 1213 (Protect Elections from Deceptive AI Act); S. 1367 / H.R. 2794 (No Fakes Act); S. 1837 (Defiance Act) – 119th Congress. Elérhető: https://www.congress.gov/ (letöltés: 2025. 07. 02.)

Va. Code; California Civil Code; Texas Penal Code; Minnesota Statutes – lásd Jogszabályjegyzék.

VBÜ Zrt.: Tájékoztatás hacker támadásról (2024. 11. 14.). Elérhető: https://www.vbuzrt.hu/ext-hirek/update?ID_HIR=265748617591249 (letöltés dátuma: 2024. 11. 15.)

24.hu; HVG: Figyelmeztetések banki adathalász SMS-ekről (2022. 12.).

Jogszabály jegyzék

1993.évi XXXI. törvény az emberi jogok és az alapvető szabadságok védelméről szóló Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99300031.tv (letöltés dátuma: 2022. 04. 28.)

1993. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (Nbtv.) 53. §, 56–58. §

1993. évi XIX. törvény a büntetőeljárásról (régi Be.) 71. § (1)–(4), 178. § (1)–(2).

2000 S.C., c. 9 Canada Elections Act, s. 91.

2003. évi C. törvény az elektronikus hírközlésről 157. §

2008/616/IB tanácsi határozat (2008. június 23.) a 2008/615/IB határozat végrehajtásáról. HL L 210/12, 2008. 08. 06.

2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről… IV. Fejezet; 2. §; 35. §; 37–66. §

2010. évi CXII. törvény az információs önrendelkezési jogról (Infotv.)

2009 évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről.

2009.évi (EU) 2016/679 rendelet (GDPR). HL L 119, 2016. 5. 4., 1–88. o., 2. cikk (2) d).

12/2016. (V. 4.) BM rendelet az arcképmás, ujj- és tenyérnyomat, DNS-profil rögzítésének technikai szabályairól; 4. melléklet, 5. pont.

2013/40/EU irányelv az információs rendszerek elleni támadások elleni büntetőjogi intézkedésekről. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32013L0040 (letöltés dátuma: 2022. 04. 06.)

2019/713/EU irányelv (2019. április 17.) a készpénz-helyettesítő fizetési eszközzel elkövetett csalás elleni küzdelemről. HL L 123, 2019.5.10., 18–29. o. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32019L0713 (letöltés dátuma: 2022. 05. 01.)

2022/2065/EU rendelet (Digital Services Act – DSA). HL L 277, 2022.10.27., 1–102. o., 52. cikk (3).

2023/1114/EU rendelet a kriptoeszközök piacáról (MiCA). Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32023R1114 (letöltés dátuma: 2024. 07. 16.)

2023/1543/EU rendelet az elektronikus bizonyítékokról (e-Evidence). HL L 191, 2023.7.28., 118–180. o.; alkalmazandó: 2026. 08. 18.

2023/1544/EU irányelv a kijelölt telephelyekről és jogi képviselőkről (e-Evidence kísérő irányelv). HL L 191, 2023.7.28., 181–190. o.

2024/1689/EU rendelet (Artificial Intelligence Act). HL L 2024/1689, 2024. 07. 12.

2024/982/EU rendelet (Prüm II). HL L 2024/982, 2024. 04. 05.

Büntető Törvénykönyv (Btk.): 176–177. §; 192. §; 195–196. §; 204. §; 219. §; 222. §; 226. §; 226/A–B. §; 227. §; 256–260. §; 370. §; 373. §; 375. §; 393. §; 399. §; 413. §; 422. §; 423. §; 424. §

Büntetőeljárásról szóló törvény (Be.): 7. §; 21. § (2); 155–159. §; 165–167. §; 165. § f); 166–167. §; 167. § (5); 183. § (1); 188. § (1); 205. §; 205. § (2); 207. § (2); 214–260. §; 216–227. §; 231–236. §; 231. § e); 232. § (1), (3), (5); 232/A. §; 239. § (1); 241. §; 259–260. §; 261–270. §; 262. § (1), (4) a)–c), (5); 262/A. § (3)–(4); 263. § (2); 264. § (1)–(6); 265. § (1)–(2); 265/A. §; 266–270. §; 315–316. §; 335–338. §; 341. §; 505. §; 531–532. §

Council of Europe: Convention on Cybercrime (Budapesti Egyezmény), ETS 185; I. 2–12. cikk; II. 15–17. cikk; III. 18. cikk; IV. 19–20. cikk. Elérhető: https://rm.coe.int/16802fa405 (letöltés dátuma: 2022. 04. 29.)

Council of Europe: Second Additional Protocol to the Convention on Cybercrime (CETS 224) – 2022. máj. 12.

Európai Unió Alapjogi Chartája, 7–8. cikk. HL C 326., 2012.10.26., 391–407. o.

Európai Unió Bírósága: C-293/12. Digital Rights Ireland; C-203/15. és C-698/15. Tele2

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA). OJ L 277, 27.10.2022, 1–102. o. *(EU 2022/2065 rendelet – Digital Services Act, DSA)*

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. OJ L 191, 28.7.2023, 118–179. o. *(EU 2023/1543 rendelet – e-Evidence rendelet)*

Sverige / Watson; C-511/18., C-512/18., C-520/18. La Quadrature du Net – ítéletek.

United States House of Representatives, Committee on the Judiciary: Federal Rules of Evidence – Rule 901 (Committee Print No. 11), 2024. 12. 01., 118th Congress, 2nd Session. U.S. Government Publishing Office, Washington, 2025.

Va. Code § 18.2-386.2.; California Civil Code § 1708.86.; Texas Penal Code § 21.165.; Minn. Stat. § 609.771.