PÉCSI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK DOKTORI ISKOLA

RÉGI ÉS ÚJ TENDENCIÁK A KIBERBŰNÖZÉSBEN, KÜLÖNÖS TEKINTETTEL A KRIPTOVALUTÁKKAL TÖRTÉNŐ BŰNELKÖVETÉSRE

- doktori értekezés -

GÁSPÁR ZSOLT
PÉCS, 2024

TÉMAVEZETŐK:
PROF. DR. HABIL. KŐHALMI LÁSZLÓ
DR. TÓTH DÁVID PHD.

VAKÁT OLDAL

Köszönetnyilvánítás

Ezúton szeretném tisztelettel kifejezni mérhetetlen hálámat témavezetőimnek, Kőhalmi Lacinak és Tóth Dávidnak a doktori képzésem során nyújtott szakmai és baráti támogatásért, az önfeledt és lélekemelő beszélgetésekért, a sok nevetésért és természetesen Lacinak külön a hasznos életvezetési tanácsokért is.

Köszönettel tartozom a feleségemnek és Mirkó fiamnak, amiért a kutatással járó stresszt és a rengeteg munkával, tanulmányírással töltött éjszakát kibírták.

Hálával tartozom barátaimnak, Ákosnak, Palinak, Alexnek és Zsoltnak, akiknek a biztatására és támogatására mindenben számíthattam.

Szeretném megköszönni kedves kollégáimnak és barátaimnak, hogy életem egyik legszebb időszakává tették számomra a doktori képzést.

Hálás vagyok továbbá drága szüleimnek és nagyszüleimnek, amiért egész életemben mellettem álltak és támogattak.

„A nagy dolgok megkövetelik, hogy az ember vagy hallgasson róluk, vagy fennkölt hangnemben szóljon róluk: fennkölten, vagyis ártatlanul – cinikusan.”

- Friedrich Nietzsche -

Tartalomjegyzék

1. A kutatás tárgya, célja, módszere

1.1. A témaválasztás indoklása

A radikális mértékű technológiai fejlődés és globalizáció[1] hatására a 2020-as évekre a társadalom szignifikáns változásokon esett át, melynek hatására az egyének jelentős részénél kialakult egyfajta konstans függés az online tér és az internetes jelenlét irányába. E folyamatra egyfajta katalizátorként hatottak az olyan egyéb tényezők, mint a koronavírus-járvány és az ún. energiaválság, ezek ugyanis az otthoni munkavégzés és az online tanulás felértékelődését eredményezték. A fentiek mind hozzájárultak ahhoz, hogy az egyébként is növekvő tendenciát mutató kiberbűnözés egyes válfajai eddig soha nem látott mértéket öltsenek. Ennek egyik oka, hogy a fentebb említett körülmények miatt olyan társadalmi rétegek is rákényszerültek arra, hogy a mindennapokban számítástechnikai eszközöket használjanak, akik meglehetősen szegényes informatikai tudással rendelkeznek, így könnyen a csalók áldozataivá válnak. Az előzőek mellett általános problémaként elmondható, hogy a kiberbűnözés nyomozása rengeteg szakértelmet és forrást követel, így az ilyen bűncselekmények felderítése sok esetben akadályokba ütközhet, melyet tovább nehezítenek az olyan technológiai megoldások használata, mint a VPN, a proxy szerverek vagy éppen az egyes kriptovaluták (pl.: Monero). Az ilyen típusú bűncselekményeknek – az említett aktuális trendeket leszámítva is – az egyik legjellegzetesebb tulajdonsága az anonimitás, a nagyfokú látencia, illetve a több, különböző joghatóságon átívelő cselekmények.

Következtetésként leszűrhető, hogy a kiberbűnözés egy igen szofisztikált bűnözési ág, melynek elkövetői általában nehezen felderíthetők, s melynek változatos, sokszor pontosan be nem határolható számú sértettje lehet. A kibertérben észlelt bűncselekmények egyre bonyolultabb és egyre biztonságosabb módokon is elkövethetőek, hála a technológiai fejlődés vívmányainak. E tény már önmagában is megalapozza az igényt, hogy az új kiberbűncselekmények folyamatosan bővülő halmaza tudományos kutatás tárgyát képezze.

A kriptovaluták és a technológiai alapját képező blokklánc megjelenésével és elterjedésével meglehetősen kibővültek az online tér színterei. E technológiai áttörés nem csupán forradalmi változást hozott a fizetési tranzakciós lehetőségek és a tőzsdei élet terén, de olyan új gazdasági és jogi megoldások tömkelegét is előrevetítette, mint például a blokklánc-alapú, ún. okosszerződések (smart contracts).

[1] Lásd: Zsigovits László: Globalizációból fakadó rendészeti kihívások a korszerű információtechnológia tükrében. In: Pécsi Határőr Tudományos Közlemények Vol. 15, 2014. pp. 61-66.

A kriptovaluták számtalan előnyén túlmenően sajnos számos hátránnyal is számolnunk kell, hiszen meglehetősen gyakran kerülnek kapcsolatba a kiberbűnözéssel. Ennek több formája is lehet: egyrészről, amikor a kriptovalutát bűncselekmény elkövetésének megkönnyítésére vagy annak elfedésére használják; másrészről, amikor maga az adott kriptovaluta a bűncselekmény elkövetési tárgya.

1.2. A kutatás hipotézisei

A kutatás célját alapul véve a következő hipotézisek vizsgálatát tartottam indokoltnak, annak érdekében, hogy de lege ferenda javaslatokat fogalmazhassak meg a jogalkotás számára, illetve a kiberbűnözéssel foglalkozó szakemberek (rendvédelmi szervek alkalmazottai, ügyészségi és bírósági alkalmazottak) számára is hasznos, gyakorlati tapasztalatokat szem előtt tartó konklúziókat vonhassak le:

1. *A hazai büntető jogszabályok meglehetősen nehezen követik a technológiai vívmányok által támasztott új jogi kihívásokat, melynek okán a joghézagot a gyakorlati szakemberek – az analógia tilalmának okán – gyakran nem tudják betölteni.*
2. *A kriptovaluták és a technológiai alapjukat nyújtó blokkláncok – mint a 21. század egyik legjelentősebb technológiai újítása a hazai jogrendszerben – nincsen kellő mértékben szabályozva, mely meglehetősen sok kérdést vet fel, többek között a büntetőjog területén is.*
3. *A kriptovaluták megjelenésével párhuzamosan új típusú bűncselekmények evolválódnak, az ún. „hagyományos" bűncselekmények egy bizonyos része pedig átalakul, melyet a hatályos büntető jogszabályokkal összhangba kell hozni.*
4. *Léteznek olyan új, absztrakt jogesetek, új technológiai megoldásokon alapuló bűncselekmények, melyeket a Büntető Törvénykönyvről szóló 2012. évi C. törvény tényállásai nem fednek le. A Btk. bizonyos mértékű módosítására van szükség.*

1.3. A kutatási anyagok feldolgozásának módszerei

Az értekezés első része egyfajta történeti áttekintést tartalmaz. Ennek során a technológiai fejlődés – mint egyfajta katalizátor – hatására a jogszabályi és az intézményi rendszer egyaránt hatalmas változásokon ment keresztül. E jogfejlődés áttekintését követi a hatályos nemzetközi szerződések és uniós jogforrások, majd pedig a hazai jogszabályi környezet áttekintése. A

jogszabályi környezet tanulmányozását követően az intézményi rendszert kívánom áttekinteni, melynek során az egyes szerveknek (például az ügyészség, a nyomozó hatóságok, stb.) kiberbűnözés vonatkozásában fennálló esetleges hiányosságait kívánom feltárni.

A fentieket követően az egyes hagyományos bűncselekményeket veszem górcső alá, melyek újabb formákat ölthetnek a kibertérben. Az értekezésben kiemelt részt szenteltem a kriptovalutáknak és azok kiberbűnözésben betöltött szerepének. A kriptovaluták vonatkozásában vizsgálom mind az ún. hagyományos bűncselekményeket, mind pedig a megjelenésük óta felmerült új bűncselekmény-típusokat. A kriptovaluták országonként eltérő szabályozásából rendkívül széleskörű problémák eredhetnek. Ennek okán vizsgálatomat érintőlegesen kiterjesztettem egyes országok tanulmányozására, ahol a kriptovaluták jogi szabályozása kirívó tendenciát mutatott. Végül az értekezés záró részében a kutatás összefoglalását követően kiértékelésre kerülnek a feltett hipotézisek.

A kutatási anyagok feldolgozása során az összegyűjtött szakirodalom elemzése és értékelése kulcsfontosságú. Álláspontom szerint érdemes megismerni a releváns hazai és nemzetközi, elméleti és gyakorlati szakemberek látásmódját és gondolatmenetét. Az így kapott adatokat – amennyiben szükséges – aktualizálni kell, majd pedig összevetni a jelenleg is hatályos nemzetközi, uniós és hazai jogszabályokkal. A tisztán elméleti jellegű kutatás helyett az egyes fejezetekben – ahol lehet – releváns jogesetek elemzésével, továbbá – ha az adott kérdés vonatkozásában létezik, akkor – a jogalkalmazó szervek gyakorlatának analizálása mellett döntöttem, így adva egy ún. experimentális, gyakorlatban is hasznosítható karaktert az értekezésnek. Véleményem szerint a gyakorlati hasznosíthatóság ugyanis kiemelt jelentőséggel bír a doktori kutatás során. Célom az egyes joghézagok feltérképezésével és a gyakorlat hiányosságainak feltárásával de lege ferenda javaslatok megfogalmazása a jogalkotás számára, a gyakorlati szakemberek munkájának elősegítése, illetőleg a tudományos diskurzus elmélyítése a kriptovaluták büntetőjogi vonatkozásainak kapcsán.

2. Alapvetések a kiberbűnözés vonatkozásában

2.1. A kiberbűnözés fogalma, típusai

A kiberbűnözés fogalmára gondolva rögtön szinonimák tömkelege juthat az ember eszébe. Az elmúlt évtizedek során – a technológiai fejlődéssel párhuzamosan – fokozatosan alakult át a számítástechnikai bűncselekmények fogalma. A szakirodalomban ennek okán számos fogalommal találkozhatunk, a teljesség igénye nélkül:

- számítástechnikai bűnözés,

- számítógépes bűnözés,
- informatikai bűnözés,
- internetes bűnözés[2],
- digitális bűnözés,
- stb.

Az egyes „rokon- vagy társfogalmaknak" egyenként is több tucat különböző definíciós kísérlete található meg a szakirodalomban, így ezen fogalmak áttekintését terjedelmi okokból az értekezésben mellőzöm, kizárólag a kiberbűnözés, mint komplex fenomén definíciós törekvéseivel kívánok foglalkozni.

A kiberbűnözés egységes fogalmának meghatározására számos szerző tett javaslatot.

Grund Borbála tanulmányában a kiberbűnözés fogalmának evolválódását részletekbe menően áttekintette, melynek eredményeként egy „tipizáló jellegű" definíció mellett érvel. E szerint a kiberbűncselekmények:

- *„az olyan bűncselekmények, amelyekben a számítógép vagy a számítógépes hálózat biztonságát fenyegeti a kriminális tevékenység, ezek az IKT létrejövetelével karöltve alakultak ki (szűk értelemben vett kiberbűnözés), továbbá*
- *az olyan hagyományos bűncselekmények, amelyekhez a számítógépet az elkövetés eszközeként használják fel, ezek léteztek az IKT előtt is, de új életre keltek a kibertérbe való bizonyos fokú integrálódással (számítógép segítségével megvalósuló bűnözés), valamint*
- *a számítógépes tartalommal kapcsolatos bűncselekmények, amelyeknél az eszköz tartalma az elkövetés bizonyítékául szolgálhat (számítógépen tárolt adatok tartalmával kapcsolatos bűnözés)."*[3]

Oscar Morales a következőképpen definiálta a kiberbűnözést: *„bármilyen illegális tevékenység, melyet számítógépen keresztül követnek el."*[4]

Gema Sánchez Medero szerint *„a kiberbűnözés alatt azon büntetendő tevékenységeket értjük, melyek megvalósítását kommunikációs hálózatok és elektronikus információs rendszerek vagy hasonló hálózatok és rendszerek segítségével követik el."*[5]

---

[2] Az internetes bűnözés kapcsán megjegyzendő, hogy a többihez képest sokkal szűkebb kategóriáról van szó, hiszen nem foglalja magába a hálózaton kívüli bűncselekmények, sem pedig az intranetes vagy egyéb magánhálózatokon történő elkövetést.

[3] Grund Anna Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. MTA Law Working Papers No. 21, 2021. pp. 1-37.

[4] Reina Barroso Toledo: Los Delitos en Internet: Un enfoque desde la pornografía infantil en la red. In: Revista F@ro No. 13, 2011. p. 60.

[5] Gema Sánchez Medero: Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI. In: Revista Enfoques: Ciencia Política y Administración Pública Vol. 10, No. 16, 2012. p. 73.

Varga Árpád tanulmányában Weulen Kranenbarg fogalmi elhatárolásával ért egyet, mely megkülönbözteti a kibertér által elősegített bűnözést a kibertérfüggő bűncselekményektől. Ezutóbbi alatt azon bűncselekményeket érti, amelyeket magát az infokommunikációs technológiát célozzák és amelyeknek az informatika kulcsszerepet játszik a végrehajtásában.[6]
Egyes szakértők (például Michael MCGuire) véleménye szerint egyenesen be kell fejezni a definícióalkotást a kiberbűnözéssel kapcsolatban és a gyakorlati magyarázatokra kellene fókuszálni. Mások (például Peter Grabosky) ezzel szemben a folyamatos fogalomalkotás és fogalomfejlesztés mellett voksolnak.[7]
Álláspontom szerint a kiberbűnözés definiálásának során a teljesen közömbös, hogy az adott informatikai rendszer vagy eszköz a bűncselekmény eszköze vagy tárgya. A kiberbűnözés véleményem szerint minden olyan bűnelkövetési módot magába kell foglaljon, melynek során a kibertér bármilyen szinten is érintett, legyen az tisztán számítástechnikai bűncselekmény, vagy csak járulékos informatikai bűncselekmény. Ez alapján tehát kiberbűncselekménynek minősül minden olyan hagyományos vagy új típusú bűncselekmény, melyet részben vagy egészben a kibertérben követnek el, vagy ott fejti ki hatását.
A kiberbűncselekmények csoportosítása szintén többféleképpen, illetőleg több séma mentén történhet. A kategorizálás egyik lehetséges módja a sértetti kör szerinti elhatárolás, mely szerint a kiberbűncselekmények lehetnek:

- egyén ellen irányulóak,
- vagyon ellen irányulóak,
- szervezetek, vállalatok ellen irányulóak, vagy
- a társadalom ellen irányulóak.[8]

A fenti csoportosítás kapcsán megjegyzendő, hogy Parti és Kiss az előbbi kategóriákat az informatikai bűncselekmények vonatkozásában szabták meg, ugyanakkor – véleményem szerint – az a kiberbűncselekmények kapcsán is megfelelően használható.
A Budapest Egyezmény az előbbivel szemben egy másik megközelítést használ a csoportosításra. Az egyezmény a következő bűncselekményeket különbözteti meg:

[6] Varga Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In: In Medias Res Vol. 8, No. 1, 2019. p. 152. cit.:
Maleen Waulen Kranenbarg: Cyber-offenders versus traditional offenders: An Empirical Comparison. Vrije Universiteit. Doktori értekezés, 2018.,
http://dare.ubvu.vu.nl/bitstream/handle/1871/55530/complete_dissertation.pdf?sequence=6&isAllowed=y
[7] Parti Katalin: Cyberbullying, Bitcoin, Silk Road, Darknet, TOR: Az internetes bűnözés tárgyában tartott nemzetközi konferenciák kurrens témái 2014-ben. In: Ügyészek Lapja Vol. 22, No. 1, 2015. p. 84.
[8] Parti Katalin; Kiss Tibor: Informatikai bűnözés. In: Borbíró Andrea; Gönczöl Katalin; Kerezsi Klára; Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., Budapest, 2016. pp. 495-496.

- a számítástechnikai rendszer és adat hozzáférhetősége, titkossága és sértetlensége elleni bűncselekmények,
- a számítógéppel kapcsolatos bűncselekmények,
- a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények, valamint
- a szerzői jogok megsértésével kapcsolatos bűncselekmények.[9]

Álláspontom szerint az egyezmény által alkalmazott csoportosítás ugyanakkor már elavultnak számít, a technológiai fejlődés szintje már meghaladta azt, melynek eredménye, hogy bizonyos bűncselekményeket nem, vagy csak meglehetősen nehezen lehet besorolni a fenti kategóriákba. További kritikaként fogalmaznám meg, hogy az egyezmény még a számítástechnikai bűncselekmények kategóriáját használja, mely azóta már ugyancsak „elhasználódott" fogalom.

2.2. A kiberbűncselekmények elkövetői köre

A kiberbűnözők profiljának általános megalkotása és a motivációjuk behatárolása meglehetősen nehéz feladat. Álláspontom szerint a hagyományos bűnelkövetőkhöz hasonlatosan egy-egy különböző bűncselekmény-kategóriának az elkövetőit más és más jellemzi, más motivációkkal és okokkal (haszonszerzés, agresszió levezetése, személyiségzavarok, helytelen szocializációs folyamatok, stb.) válnak bűnelkövetőkké. Ennek okán a téma egyes szerzői többféleképpen próbálták meg kategorizálni a kiberbűncselekmények elkövetői köreit.

Chawki és szerzőtársai a következőképpen csoportosítják a kiberbűncselekmények elkövetőit:

- 6 és 18 év közötti gyermekek és tinédzserek,
- szervezett hackerek,
- professzionális hackerek vagy ún. crackerek,
- elégedetlen alkalmazottak.[10]

A fenti csoportosítással kapcsolatban számos kritika fogalmazható meg. Álláspontom szerint ezen felsorolásból hiányoznak egyrészről az élvezeti motiváción alapuló bűnözés elkövetői (például a pedofilok, illetőleg az online gyermekpornográfia vonatkozásában). Ezen csoportok nem feltétlenül működnek szervezetten, az elkövetők pedig nem feltétlenül rendelkeznek professzionális szaktudással.

[9] Uo.
[10] Mohamed Chawki; Ashraf Darwish; Mohammad Ayoub Khan; Sapna Tyagi: Cybercrime, Digital Forensics and Jurisdiction. Studies in Computational Intelligence Vol. 593, Springer, 2015. p. 17.

Arroyo számos szerző munkáját alapul véve a kiberbűnözők egy másféle tipizálását alkotta meg azok szakképzettségi szintjét alapul véve:

- specializálódott kiberbűnözők:
    - hackerek,
    - „cracker-ek”[11], „phreaker-ek”[12] és „cyberpunk-ok”,
    - „virucker-ek”[13],
    - malware programok (vírusok, spyware-ek és egyéb kártékony szoftverek) kereskedői,
    - a pénzintézetekre specializálódott elkövetők,
    - az ún. „szerződéses hackerek”, akik bárki által felbérelhetőek,
    - különleges ügynökök,
    - „kibernindzsák”[14],
    - „kiberkatonák”,
    - „spammer-ek”,
    - „domainer-ek”,
    - informatikai kémek,
    - „sniffer-ek”,
    - kiberterroristák,
    - adathalászok (ún. „phiser-ek”),
    - csalók (ún. „hoaxer-ek”),
    - „hacktivisták”,
- nem specializálódott kiberbűnözők:
    - „emugger-ek”[15],
    - „wannebe-k”[16],
    - „poseur-ök”[17],
    - „lamer-ek”[18],
    - „script kiddie-k”[19].[20]

[11] Szoftverek feltörésére specializálódott elkövetők.
[12] A távközlési rendszereket célzó elkövetők.
[13] Számítógépes vírusok készítői.
[14] Nagyvállalatok adatainak ellopására és értékesítésére specializálódott elkövetők.
[15] A bagatell bűnözőkkel egyenértékű fogalom a kibertérben.
[16] Olyan elkövetők, akik hackerekké szeretnének válni.
[17] Olyan elkövetők, akik hacker-nek akarnak látszani.
[18] Olyan elkövetők, akik nem igazán vannak tisztában azzal, hogy mit is csinálnak a kibertérben.
[19] Olyan (általában fiatalkorú) elkövetők, akik mások által kifejlesztett scripteket használnak fel az elkövetéshez.
[20] Sergio Cámara Arroyo: Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. In: Derecho y Cambio Social No. 60, 2020. pp. 492-502.

Arroyo a fenti csoportosítás mellett egy motiváció alapú tipizálást is felvázol. Ez alapján a kiberbűnözők motivációja lehet:

- gazdasági,
- politikai, vagy
- szociális.[21]

Álláspontom szerint az Arroyo által használt kettős jellegű – a szakértelem és a motiváció ötvözésével megvalósuló – kategorizálás megfelelően lefedheti a kibertér bűnelkövetőinek köreit. Ezzel kapcsolatban kritikaként ugyanakkor megjegyezném, hogy a szakképzettséget alapul vevő tipizálás álláspontom szerint túlságosan szűk körökre bontja le az elkövetők csoportjait, egyes alcsoportok között igen vékony a határvonal (például a kiberharcosok, a kiberkatonák és a kiberterroristák vagy a különleges ügynökök és az informatikai kémek között).

3. A kiberbűnözés előzményei és kialakulása

A számítógépes bűnözés, mint új jelenség Magyarországon a 80-as évek végén, illetve a 90-es évek elején kezdte el bontogatni a szárnyait. Ekkor még pusztán egy meglehetősen szűk réteg rendelkezett saját személyi számítógéppel, ez zömében inkább az ipari, illetőleg a statisztikai[22] célú felhasználásra korlátozódott, főleg nagyobb gyárakban kezdték el hasznosítani ennek a technológiai vívmánynak az előnyeit. Ebből adódóan azon bűncselekmények köre, melyek kapcsolódhattak a számítástechnikához szintén meglehetősen behatárolt volt. Később a számítástechnika fejlődésével ezek az eszközök egyre kompaktabb formát öltöttek, áruk a tömeggyártás miatt lecsökkent, így fokozatosan elérhetővé váltak az egyéni felhasználók és a kisebb vállalkozások számára is. Ez a folyamat természetesen magába foglalta a számítástechnikai bűncselekmények számának növekedését, illetve az új bűncselekmények megjelenését, új elkövetési módok alkalmazását. Az 1990-es évek elején Magyarországon is megjelent az internet, ami katalizátorként hatott az imént említett folyamatra. A 2000-es évek elején már hazánkban is tömegek kapcsolódtak az internethez (2005-re már több, mint egymillió internet előfizetés volt hazánkban a KSH adatai szerint).

Az első számítógépek megjelenése óta eltelt idő alatt hatalmas technológiai változásnak

[21] Op.Cit. pp. 502-504.

[22] Lásd például: Dávid Gábor: Számítástechnika és kriminálstatisztika. In: Jogtudományi Közlöny Vol. 30, No. 1, 1975. pp. 32-35., továbbá
Halász Kálmán: A polgári ügyek statisztikájának fejlődési távlatai a számítógépre figyelemmel. In: Jogtudományi Közlöny Vol. 30, No. 1, 1975. pp. 35-44.

lehettünk szemtanúi, melynek során a hatalmas méretű, néha egész helyiségeket elfoglaló gépmonstrumokat szépen lassan felváltották a kisebb, kompaktabb kivitelű számítógépek, majd az ezek tudását akár több ezerszeresen is meghaladó mikro-processzorokkal, illetve később már többmagos processzorokkal rendelkező számítógépek.

Hazánkban a számítógépes rendszerek vonatkozásában alkotott első jogszabály *a belügyminiszter 1/1981. (I. 27.) BM számú rendelete a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről*, mely 1981. július 1-jén lépett hatályba. A rendelet megjelenésének idejében Magyarországon még csak néhány helyen, elvétve lehetett találkozni számítástechnikai rendszerekkel. Bár az 1950-es, 1960-as évektől[23] bizonyos – javarészt állami – intézetekben már voltak kutatócsoportok, melyek a számítástechnika, illetve a kibernetika területén végeztek fejlesztéseket, kutatásokat, ezek még zömében meglehetősen kezdetleges, lyukkártyás vagy lyukszalagos módszerrel[24] működő eszközök voltak, melyek csak egy igen szűk réteg számára voltak hozzáférhetőek, emellett a bűncselekményekre történő felhasználásuk sem volt jellemző. Jóllehet a rendelet sokkal inkább adatvédelmi szempontból viszonyul a számítógépes rendszerekhez, ugyanakkor a jogalkotási folyamat bemutatásának teljessége végett mégis adekvátnak tartom a rövid áttekintését.

A rendelet 3.§-a tartalmazza a taxatív felsorolását a jogi védelem alá vont tárgyakról, melyek a következők:

- az adatok és az adathordozók a végleges megsemmisítésükig, illetve a közlésre szánt adatok a felhasználásukig,
- a személyhez fűződő és a vagyoni jogok,
- a számítástechnikai berendezések, azok környezete, működésük biztonsága és a dokumentációik,
- a számítástechnikai berendezésekhez tartozó okmányok, programok és azok dokumentációi, és
- az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.[25]

[23] 1960-ban például két URAL-1-es modell beszerzését sikerült eszközölni, melyek egyike a Központi Statisztikai Hivatalba (KSH), a másik pedig a Központi Fizikai Kutatóintézetbe került. Az 1980-as éveket megelőző hazai számítástechnikai eszközbeszerzésekről, illetve a Magyarországon alkalmazott számítástechnika-történeti vívmányokról lásd részletesebben: Raffai Mária (2000): A hazai számítástechnika története. http://www.sze.hu/~raffai/org/raffai-infotort.pdf (2021.01.22.)

[24] A lyukkártyák és lyukszalagok által történő adatrögzítés és adatbevitel folyamatáról, illetve működési elvéről lásd részletesebben: Hámori Miklós: Ismerkedés a komputerrel. Budapest, Tankönyvkiadó, 1973.

[25] 1/1981. (I. 27.) BM számú rendelet a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről 3.§

A rendeletben szabályozásra került többek között az államtitok, a szolgálati titok és a személyhez fűződő jogok kezelése, illetve számítógépes rendszer általi feldolgozása, az ilyen minősített adatok továbbítása és törlése. Ahogyan fentebb említésre került, a rendelet megjelenésekor még meglehetősen kevés helyen lehetett hozzáférni számítástechnikai eszközökhöz, így az 1980-as évek közepéig főként az adatfeldolgozás szabályozását érintő kérdésekre sikerült reagálnia a jogalkotónak. Így került megalkotásra az *1/1983. (X. 13.) KSH rendelkezés a statisztikai adatok számítástechnikai eszközök útján végzett rögzítéséről, feldolgozásáról, tárolásáról, továbbításáról*; illetve a *25/1986. (VIII. 8.) MT rendelet az állami népességnyilvántartásról szóló 1986. évi 10. tvr. végrehajtására*.

A számítástechnika Magyarországon történő megjelenése természetesen a bűnügyi tudományok területén kutatók érdeklődését is felkeltette, hiszen a számítógépes bűnözéssel kapcsolatban már akkoriban is jelentek meg tanulmányok a nemzetközi irodalomban. Az említett szabályozások (a fenti három rendelet) rendelkezéseiből Nagy Zoltán a számítógéppel elkövethető bűncselekmények vonatkozásában *társadalomra veszélyességüket*[26] az elektronikus adatfeldolgozási tevékenységek jogilag szabályozott rendjének veszélyeztetésében, illetve megsértésében összegezte.[27]

Egy 1983-ban megjelent tanulmányban Polt Péter a számítógéppel kapcsolatos bűncselekményekkel kapcsolatban már megjegyezte, hogy dacára annak, hogy akkoriban ezen típusú bűnözés csak a legfejlettebb ipari államokban fordult elő, az elkövetkező évtizedben Magyarországon is jelentkezni fog. Meglátásai szerint, illetve az akkori helyzet áttekintése után arra a következtetésre jutott, hogy hazánkban vélhetően a szolgáltatáslopás és a társadalmi tulajdon elleni bűncselekmények terén fog kibontakozni a számítógépes bűnözés.[28] Egy, az International Criminal Police Review című folyóiratban ugyanabban az évben megjelent tanulmányban egy több országra kiterjedő felmérés alapján közzétett becslések szerint a számítógépes bűnözés az Amerikai Egyesült Államokban éves szinten 100 millió és 3 milliárd dollár közötti kárt okozott. Ezt a számot Franciaországban 5 milliárd frankot is meghaladó összegre becsülték, az NSZK-ban pedig 15 milliárd márkára.[29] Megjegyzendő, hogy a fenti becslések csak a rendőrségnek bejelentett bűncselekményeket vették alapul, ugyanakkor a

[26] A bűncselekmények társadalomra veszélyességéről lásd bővebben: Kőhalmi László: A büntetőjog alapproblémái. Pécs, PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, 2012.
[27] Nagy Zoltán: Az informatika és a büntetőjog. In: Magyar Jog Vol. 38, No. 1, 1991. p. 24.
[28] Polt Péter: A számítógépes bűnözés. In: Belügyi szemle Vol. 31, No. 6, 1983. pp. 60-64.
[29] Castorál Zdenek; Bimová Alena: A számítástechnikával kapcsolatos bűnözés. In: Belügyi Szemle Vol. 38, No. 1, 1990. p. 117.

látenciában[30] maradt bűnelkövetések száma a számítógépes közegben elkövetett bűncselekmények tekintetében igen magas, így pontos becslés – véleményem szerint – nem volt végezhető.

A fentiek tükrében megállapítható, hogy a számítástechnikával kapcsolatos bűnözés 1983-ban már nemzetközi és hazai szinten is foglalkoztatta a kutatókat, hiszen jelentős károkban nyilvánult meg – már akkor is – az ilyen bűnelkövetők tevékenysége.

Az első vonatkozó hazai jogesetre négy évet kellett várnunk. 1987-ben egy pénzintézeti alkalmazott hamis összeget írt jóvá egy külföldi állampolgár betétszámláján, amiért az ügyben eljáró bíróság csalás bűncselekményét állapította meg.[31]

Az elkövetkező években egyre inkább felértékelődtek a számítástechnikai bűnözés jelentette problémák, így világszerte egyre több fórumon vált témává és egyre több kutató kezdett el foglalkozni a büntetőjog ezen új irányvonalával.

Az Európa Tanács szakértői bizottságot állított fel a számítógépes bűncselekményekre vonatkozó ismeretek összegzésére. E folyamat eredményeképpen a bizottság 1989. szeptember 13. napján egy ajánlást bocsátott ki a tagállamok számára, melyben meghatározott egy ún. minimum-listát (kötelező) és egy fakultatív listát az egyes bűncselekmények büntetendővé tételével kapcsolatban. A minimum-lista a következő bűncselekménytípusokat tartalmazta:

- számítógépes csalás,
- számítógépes hamisítás,
- számítógépes programban vagy adatban történő károkozás,
- számítógépes szabotázs,
- jogosulatlan belépés (behatolás),
- jogosulatlan titokszerzés,
- védett számítógépes program jogellenes reprodukciója,
- félvezető tipográfiák jogellenes reprodukciója.[32]

A fentiek mellett az ún. fakultatív listán szerepel továbbá a számítógépes adat vagy program megváltoztatása, a számítógépes kémkedés, a számítógép jogosulatlan használata, illetőleg a védett számítógépes program jogosulatlan használata.[33]

[30] Lásd bővebben a látenciáról: Korinek László: Rejtett bűnözés. Közgazdasági és Jogi Könyvkiadó, Budapest, 1988.
[31] Nagy, 1991, Op.Cit. p. 26.
[32] Molnár Gábor: Gazdasági bűncselekmények. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2009. 277. o.
[33] Ibid.

Castorál és Bimová 1990-es Belügyi Szemlében megjelent tanulmányukban összegyűjtötték és felsorolták a számítógépes bűncselekmények – akkoriban – leggyakoribbnak számító elkövetési módjait, ezek az általuk kiemelt megjelenési formák a következők:

- vagyon elleni bűncselekmények (pl.: hamis megrendelések a cég nevében),
- pénzügyi manipulációk (pl.: fiktív kifizetések),
- számítógépes szolgáltatások eltulajdonítása (pl.: a számítógép jogtalan – munkaidőn vagy műszakon kívüli – használata, az ún. gépidő-lopás),
- információhordozók eltulajdonítása (pl.: adatok ellopásának céljával),
- szoftver eltulajdonítása,
- oktatóprogramok eltulajdonítása,
- ipari kémkedés (általában alkalmazottak körében volt – és ma is – gyakori),
- szabotázs, vandalizmus, terrorizmus (pl.: mágnesszalagokon tárolt adatok erős mágnessel vagy egyéb módon történő megsemmisítése),
- egészségügyi visszaélések (pl.: a betegek orvosi és egyéb személyes adataival visszaélés).[34]

A folyamatosan növekvő tendenciát mutató számítógépes bűnözés, illetve az egyre változatosabb előfordulási formák és elkövetési módok miatt az 1990-es évek elejére több aggasztó probléma is felmerült a számítógépes rendszerek biztonságát illetően (például adatvédelmi kérdések[35]), illetve fontos mérföldkőnek tekinthető, hogy az új évtized elejére bűnüldözői oldalon is elkezdték keresni a lehetőségeket a számítógépes rendszerek előnyös kihasználására, amely folyamat részeként – ha csak lassan, lépésről lépésre is – fokozatosan elkezdték a rendvédelmi szervek adatbázisait digitalizálni, hiszen a tetemes mennyiségű papírmunka és az átláthatóság hiánya ekkorra már – a magas ügyszámok miatt – nagy mértékben megnehezítette a nyomozó hatóságok munkáját.[36]

1992. október 5-8. között a Nemzetközi Büntetőjogi Társaság (Association Internationale de Droit Penal, vagy röviden AIDP) által Würzburgban megrendezésre került „Számítógépes bűnözés és az információtechnika területének egyéb deliktumai” című nemzetközi konferencia, mely jeles eseményen hazánkat Pusztai László és Kertész Imre professzor képviselte. A konferencia eredményeként elfogadásra kerültek az AIDP ajánlásai, mely magába foglalták a büntetőjogi szabályozás körébe vonandó jogellenes magatartások minimum listáját, melyen

[34] Castorál; Bimová, Op.Cit. pp. 117-120.
[35] Lásd bővebben: Károlyi László: A személyi számítógépes rendszerek adatvédelmi problémái. In: Belügyi Szemle Vol. 38, No. 4, 1990. p. 46-51.
[36] Lásd részletesebben a témáról: Jasenszky Nándor: A számítógépek felhasználási lehetőségei elsőfokú rendőri szerveknél. In: Belügyi Szemle Vol. 38, No. 6, 1990. pp. 22-26.

szándékos elkövetés esetén a következő – az Európa Tanács szakértői bizottsága által hozott 1989-es ajánlásától csekély mértékben eltérő – magatartások:

- számítógépes csalás,
- számítógépes hamisítás,
- számítógépes adatokban, programokban történő károkozás,
- számítógépes szabotázs,
- számítógép jogtalan használata,
- számítógép jogtalan lehallgatása,
- védett számítógépes programok jogtalan másolása,
- félrevezető topográfiák jogtalan másolása.[37]

Az 1990-es évek számítástechnikai bűnözésének egyik „legdivatosabb" formája a hitelkártyákkal, illetőleg bankkártyákkal történő visszaélések[38] voltak. Természetesen ebben az időszakban a különböző típusú kártyákkal történő visszaélések még nem olyan sémák szerint zajlottak, mint napjainkban, noha találhatóak bizonyos átfedések. Dulin Tamás és Kó József az egyes kártyatípusokkal való bűncselekményeket a következőképpen csoportosította:

- az előre fizetett kártyákkal kapcsolatos visszaélések,
- kártyahamisítások:
    - hamisított kártya,
    - hamis kártya,
- a kibocsátókhoz kapcsolódó bűncselekmények:
    - scoring csalás,
    - fülesadás,
    - rendszerhibák kihasználása,
    - bevont kártyák újrahasznosítása,
- a bankkártyák felhasználásához kapcsolódó bűncselekmények:
    - illegálisan megszerzett kártyával történő vásárlás,
    - hamis adatokkal való kártyaigénylés,
- az elfogadókhoz kapcsolódó bűncselekmények:
    - hamis adatokkal való szerződéskötés,
    - összejátszás,
    - többszöri kártyalehúzás,

[37] Nagy Zoltán: Konferencia az információtechnikai bűnözésről. In: Magyar Jog Vol. 40, No. 2, 1993. 102-104. o.
[38] Lásd továbbá: Kunos Imre: A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. In: Belügyi Szemle Vol. 37, No. 11, 1999. pp. 35-38.

    - hamis autorizálás,
- egyéb, a bankkártyákhoz kapcsolódó bűncselekmények:
    - postai tolvajlás,
    - hamis ATM telepítése,
    - számítástechnikai rendszerbe való behatolás,
    - nem jogosult kártyahasználat,
    - erőszakos cselekmények.[39]

A fentieket hangsúlyozta Edwin Kube is, aki a 90-es évek végén megjelent tanulmányában arról számolt be, hogy nemzetközi viszonylatban megnövekedett azon esetek száma, amelyek során ún. szoftverkalózok kártyakibocsátó cégek adatbázisait törték fel, így megszerezve a tökéletes hamisításhoz szükséges adatokat (pl.: biztonsági kódokat).[40] Mindazonáltal, a hitelkártya-visszaélések mellett az internet terjedésével nagyobb mértéket öltött a bűnelkövetők általi pénzmosás, illetőleg más bűncselekmények is, továbbá fokozódott a felhasználók kiszolgáltatottsága is.[41]

A fentiekkel összhangban Nagy Zoltán a számítógéppel elkövethető hamisítások vonatkozásában a hitel- és bankkártyahamisítások mellett kiemelte továbbá a telefonkártyák hamisítását, illetőleg a bankjegyhamisítást és a közokiratok hamisítását, melyekhez a korszakban elegendő volt számítógéppel, szkennerrel és nyomtatóval rendelkezni.[42] Bardócz Csaba a pénzmosási technikák vizsgálata során szintén kiemelte az internet és a számítástechnika veszélyeit. Álláspontja szerint az elektronikus átutalások tömkelege – a távolság, a gyorsaság és a nagyfokú anonimitás miatt – kivételesen kedvező lehetőségként állt a bűnelkövetők rendelkezésére, melynek részét képezhette továbbá külföldi bankok bevonása. Ez akkoriban meglehetősen nehezen követhető és bonyolult folyamatnak számított.[43] Ennek oka egyrészről a határokon átnyúló bűnügyi együttműködés kezdetleges mivolta, a gyakorlat (az ún. good practice) deficitje, másrészről pedig a joghatóság hiánya. Különösen jellemző bűnelkövetési magatartás volt a múlt évezred végén az illegális szoftverfelhasználás, az ún. szoftverkalózkodás, mely a szerzői jog által védett szoftvereknek a szerzői jog birtokosának a hozzájárulása nélküli másolása, illetve terjesztése.[44] Jekyné Wohlfarth Zsuzsanna – a már kiemelt szerzőkkel egyetértésben – az illegális szoftvermásolás és terjesztés, az

[39] Dulin Tamás; Kó József: A hitelkártya-visszaélésekről. In: Belügyi Szemle Vol. 34, No. 11, 1996. pp. 50-60.
[40] Edwin Kube: Technikai fejlődés és a bűnözés formái. In: Belügyi Szemle Vol. 36, No. 9, 1998. p. 46.
[41] Kube, Op.Cit. pp. 49-52.
[42] Nagy Zoltán: A számítógéppel elkövethető hamisításokról. In: Belügyi Szemle Vol. 35, No. 3, 1997. pp. 29-34.
[43] Bardócz Csaba: Pénzmosási technikák. In: Belügyi Szemle Vol. 35, No. 3, 1997. pp. 74-76.
[44] Schukkert András: A magyarországi számítógépes bűnözés helyzete, a szoftverek illegális használata. In: Belügyi Szemle Vol. 33, No. 13, 1995. p. 120.

okirathamisítások, illetőleg a mobiltelefonnal és a telefonkártyákkal elkövethető bűncselekményeket emeli ki, ugyanakkor az előbbiek mellett kiemeli az internetes bűncselekmények jelentette veszélyeket is.[45]

A 90-es évek folyamán a technológia vívmányai és az általuk biztosított lehetőségek számtalan módon lettek a bűnelkövetők segítségére, mely újításokra a bűnüldözésnek és a biztonságtechnikának is reagálni kellett. A 2000-es évek beköszönte már égető igényeket hozott a számítástechnikai bűnözéssel szembeni harc terén. A millenniumfordulón az Országos Rendőr-főkapitányság Kommunikációs Igazgatóságának feladatköre bővült, melyhez immár hozzátartozott az internet figyelése, illetőleg az ott felderített bűncselekményekre történő reakció, továbbá az ezzel kapcsolatos új és egységes joggyakorlat kialakítása. Ezeket a feladatokat az ún. internetfigyelő csoport látta el 2000 februárjától. A csoport munkájához hozzátartozott az egyes weboldalakon fellelhető törvénysértésekkel kapcsolatos bejelentések kezelése, ellenőrzése és vizsgálata. Ezen vizsgálatok tárgya lehetett – a teljesség igénye nélkül – pedofil tartalmak, kábítószer, robbanószer vagy egyéb törvénybe ütköző áru készítését bemutató honlap, de akár személyiségi vagy szerzői jogokkal történő visszaélés is.[46] Ekkorra általánossá kezdett válni azon felismerés, hogy a technológiai fejlődés és az internet nem csak a bűnelkövetők, de a nyomozó hatóságok, illetőleg a tudományos igényű kutatás, közvetetten pedig ezáltal a jogalkotás számára is rengeteg lehetőséget rejtenek[47] és ezek a lehetőségek sorra kezdtek megmutatkozni a gyakorlatban is.

A következő nagy mérföldkövet az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye jelentette, mely dokumentumnak kiemelkedő szerepe volt a nemzetközi joggyakorlat kialakításában a kiberbűnözés megfelelő szankcionálása érdekében. A Budapesti Egyezmény részletesebben a következő fejezetben kerül kifejtésre.

A számítástechnikával kapcsolatos bűncselekmények hazai szabályozásának kapcsán megfigyelhető, hogy az 1990-es és 2000-es évek során büntetőjogi szabályozások sorát alkotta meg a jogalkotó[48], mely nélkülözött mindennemű stabilitást, egyúttal felvetette az igényét a

[45] Jekyné Wohlfarth Zsuzsanna: Számítógép segítségével elkövetett bűncselekmények. In: Belügyi Szemle Vol. 37, No. 11, 1999. pp. 43-50.
[46] Peszleg Tibor: Internet és bűnözés. In: Belügyi Szemle Vol. 38, No. 12, 2000. p. 30.
[47] Werner Rüther: Az internet és az „informatikai bűnözés" a kriminológia számára is kihívás. In: Belügyi Szemle Vol. 51, No. 2-3. 2003. p. 262.
[48] Lásd bővebben:
1994. évi IX. törvény a büntető jogszabályok módosításáról
1996. évi LII. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról
1998. évi LXXXVII. törvény a büntető jogszabályok módosításáról
1999. évi CXX. törvény a büntető jogszabályok módosításáról
2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról

terület kodifikációjának, mellyel kapcsolatos törekvések a fenti időszak alatt megjelent tanulmányok tömkelegében felmerültek.[49] Fázsi László és Fázsi László Milán a 2000-es évek végén elsőszámú javaslatként a szabályozás stabilitását emelték ki, melyet azzal indokoltak, hogy a számítástechnika nem fejlődik annyira rohamosan, ami indokolhatná a szabályozás sűrű módosítását.[50] Másfél évtizeddel a tanulmány megjelenését követően nyilvánvaló, hogy a technológiai fejlődés sosem tapasztalt sebességű ütemet vett fel, mely egyértelműen megcáfolta a szerzőpáros tézisét a 2009-2023 közötti időszakra vonatkozóan, ugyanakkor a javaslat azon részét mindenféleképpen el kell fogadni, hogy egy stabil, időtálló szabályozásra volt (és lesz is mindig) szükség, melyet az absztrakt jogesetek extrémitásai sem tudnak kikezdeni. A szerzők azon javaslata szintúgy helytálló volt, hogy a számítástechnikai bűncselekményeket a Büntető Törvénykönyv egy önálló fejezete alatt kell kezelni, hiszen a törvényi tényállások tekintetében a jogalkotó által védeni rendelt jogi tárgya ezen bűncselekményeknek nem illett bele a Btk. korabeli rendszerezési struktúrájába.[51]

A 2000-es évek végére, dacára a büntetőjogi jogszabályok folyamatos módosításának, még mindig nem sikerült egy koherens, minden igényt kielégítő szabályozást létrehozni. A gyakorlati jogalkalmazásban ugyanis felmerültek olyan problémás esetkörök, melyeket az adott jogszabályi környezetben rendkívül nehézkes volt megoldani.[52] A fentieket követően – a sürgető kodifikációs igényeknek hála – megszületett a Büntető Törvénykönyvről szóló 2012. évi C. törvény, mely új alapokra helyezte a számítógépes bűncselekmények büntetőjogi megítélését.

2003. évi II. törvény a büntető jogszabályok és a hozzájuk kapcsolódó egyes törvények módosításáról
2005. évi XCI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény és más törvények módosításáról
2007. évi XXVII. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény és más büntetőjogi tárgyú törvények módosításáról

[49] Lásd: Nagy Zoltán: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda. In: Belügyi Szemle Vol. 37, No. 11, 1999. pp. 16-27.

[50] Fázsi László; Fázsi László Milán: Megjegyzések a számítógépes bűncselekmények hatályos szabályozásához. In: Rendészeti Szemle Vol. 57, No. 5, 2009. pp. 8-9.

[51] Ibid.

[52] Az egyik jellemzően ilyen bűncselekmény-kategória a mobiltelefon-feltöltéses csalás volt, melynek lényege, hogy az elkövetők egy telefonhívás során – hamis nyeremény lehetőségével kecsegtetve – mobiltelefon feltöltőkártya vásárlására bírták rá a sértetteket, akiknek a feltöltőkártya aktiválókódját be kellett diktálniuk az elkövetőknek, hogy „ellenőrizzék" a számokat. Ezt követően az elkövetők – nyilvánvalóan – nem „írták jóvá" az egyenleget, ahogy ígérték, hanem a saját telefonjaikat töltötték fel a kóddal. A probléma büntetőjogi vetülete az volt az ilyen csalásoknál, hogy a kár jellemzően 20.000,- forint alatti volt, így kizárólag szabálysértési ügyként kezelték ezeket a tényállásokat, ugyanakkor a szabálysértési hatóságok – jogkör hiányában – nem tudtak sikeresen adatkéréseket foganatosítani a szolgáltatóknál.
Lásd erről bővebben: Kökényesi-Bartos Attila: Számítástechnikai rendszerek használatával elkövetett bűncselekmények jogi megítélése. In: Ügyészek Lapja Vol. 16, Különszám, 2009. pp. 62-63.

4. A kiberbűnözés elleni fellépés jogszabályi dimenziói

4.1. Nemzetközi szintű egyezmények a kiberbűnözés körében

4.1.1. Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (Budapest Convention 2001)

A számítástechnikai bűnözés elleni küzdelem nemzetközi perspektíváit tekintve a 2001. év november hó 23. napján kelt Számítástechnikai Bűnözésről szóló Egyezmény (a továbbiakban: Egyezmény) tekinthető az első és legnagyobb mérföldkőnek. Az egyezmény célja, hogy uniformizálja az aláíró tagállamok belső jogát a számítástechnikai bűnözéssel kapcsolatban, melynek keretében előír bizonyos nemzeti szinten meghozandó intézkedéseket. Ezen rendelkezések egyrészről a tagállamok anyagi büntetőjogi szabályai közé épülnek be, így teljesítve azt a célt, hogy az aláíró tagállamokban – ha csak minimális szinten is – de egységes legyen azon tényállások köre, melyeket a jogalkotó szankcionál az számítástechnikai bűnözéssel összefüggésben. Ezen tényállásokat az egyezmény a következő csoportosítás szerint tartalmazza:

- *Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények:*
    - Jogosulatlan belépés,
    - Jogosulatlan kifürkészés,
    - Számítástechnikai adat megsértése,
    - Számítástechnikai rendszer megsértése,
    - Eszközökkel való visszaélés.
- *Számítógéppel kapcsolatos bűncselekmények:*
    - Számítógéppel kapcsolatos hamisítás,
    - Számítógéppel kapcsolatos csalás.
- *Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények:*
    - Gyermekpornográfiával kapcsolatos bűncselekmények.
- *Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények:*
    - Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.
- *Egyéb felelősségi és büntetési formák:*
    - Kísérlet és bűnsegély vagy felbujtás,

- Jogi személyek felelőssége.[53]

Kritikaként megfogalmazható, hogy az egyezmény által használt csoportosítási mód nem megfelelő, a kategorizálás revízióra szorul, hiszen a kategóriák egy része a védelem tárgya alapján csoportosít, míg a „számítógéppel kapcsolatos bűncselekmények" kategória az elkövetés módjára utal.[54]

Az anyagi büntetőjogi tényállások mellett az egyezmény büntető eljárásjogi rendelkezéseket is tartalmaz, melyeket az egyezmény II. fejezete foglal össze. Az általános jogalkotói kötelezettségvállalást (jogkörök és eljárások megteremtése, bevezetése és alkalmazása) követően konkrét eljárásjogi szabályanyagokat tartalmaz, melyek a következő területeket érintik:

- tárolt számítástechnikai adat gyors megőrzése,
- forgalmi adat gyors megőrzése és részbeni átadása,
- közlésre kötelezés,
- tárolt számítástechnikai adat átvizsgálása és lefoglalása,
- forgalmi adatok valós idejű összegyűjtése,
- tartalomra vonatkozó adatok kifürkészése.[55]

Az Egyezmény a már említett nemzeti szabályozási kötelezések mellett iránymutatásokat tartalmaz a joghatósági kérdésekkel kapcsolatban, megalapozva az érintett tagországok joghatóságát amennyiben a bűncselekményeket:

a) a területén; vagy

b) a Fél lobogóját viselő hajó fedélzetén; vagy

c) a Félnél lajstromozott repülőgép fedélzetén követték el; vagy

d) amelyet állampolgára követett el, ha a bűncselekmény az elkövetés helyének joga szerint büntetendő, vagy ha a bűncselekmény nem tartozik egyetlen állam joghatósága alá sem.

A pozitív joghatósági összeütközés kapcsán továbbá az Egyezmény lehetőséget biztosít az érintett tagországok számára, hogy – amennyiben az célszerű – tárgyalást folytassanak le annak érdekében, hogy eldöntsék, melyik tagország tudja a legmegfelelőbb módon lefolytatni az eljárást. [56]

[53] Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (Budapest Convention 2001) 1-12. cikkei

[54] Krasznay Csaba: Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése. In: Külügyi Szemle Vol. 20, Különszám. 2021. pp. 209-210.

[55] Egyezmény 14-21. cikkei

[56] Egyezmény 22. cikke

Az Egyezmény részletes szabályozást tartalmaz a számítógépes bűncselekmények kapcsán a nemzetközi bűnügyi együttműködés vonatkozásában is. E körben a dokumentum a kiadatás és az egyes jogsegélyek részletszabályait rögzíti. A jogsegélyeket az Egyezmény két csoportba sorolja. Az ideiglenes intézkedésekkel kapcsolatos jogsegélyek körében a tárolt számítástechnikai adat gyors megőrzését, illetőleg a megőrzött forgalmi adat gyors átadását szabályozza az Egyezmény.[57] A másik egy tágabb kategória, mely a nyomozati jogkörökkel kapcsolatos, egyes jogsegély-típusokat sorolja fel taxatíve, melyek a következők:

- a tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély,
- a tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén,
- a forgalmi adat valós idejű összegyűjtésével kapcsolatos jogsegély, továbbá
- a tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély.[58]

1. ábra: A Budapesti Egyezmény tagországai 2023-ban. Forrás: https://www.coe.int/en/web/cybercrime/parties-observers (Letöltés dátuma: 2023.11.25.)

[57] Egyezmény 29-30. cikkei
[58] Egyezmény 31-34. cikkei

A Budapesti Egyezményt mérföldkőnek tekinthetjük a számítástechnikai bűnözés elleni harcban. Az Egyezmény létrejötte előtt a nyomozó hatóságok hiányos kollaborációja és a joghatósági kollíziók miatt meglehetősen nehéz és időigényes volt a határokon átívelő bűncselekmények nyomozása és a bűnelkövetők felelősségre vonása. Az Egyezmény által kialakított rendszer megteremtette a nemzetközi együttműködés alapjait, ugyanakkor az elmúlt húsz év távlatából megállapítható, hogy az Egyezmény rendelkezései elavulttá váltak, több kérdést, problémát tisztázatlanul hagynak.

Az egyezmény kapcsán számos kritika megfogalmazható. Krasznay többek között felveti a fogalommeghatározás hiányának problémáját, melynek jelentőségét a részes államok jogalkotásának közelítésében látja[59], továbbá az egyezmény által használt csoportosítás is vitatható.

Egy másik jelentős problémakört jelent a joghatósági elvek közötti prioritási sorrend kialakítása[60], a joghatósági problémák kiküszöbölése.[61] Ezen hiányosságok egyrészt annak a ténynek tudhatóak be, hogy az egyezmény a minimumszabályozásra törekszik, másrészről a technológiai fejlődés is jelentősnek bizonyult az egyezmény létrejötte óta. Maillart tanulmányában felhívja a figyelmet például arra, hogy az elkövetők zöme már meg sem próbálkozik a saját IP-címével elkövetni bűncselekményeket. Egyes programok segítségével – akár több szerver igénybevételével – akár visszakövethetetlen módon is képesek megváltoztatni az IP-címüket és technikailag más államokból indítani egy-egy támadást, jelentős adminisztratív problémákat okozva ezzel a nyomozó hatóságok számára.[62]

4.1.1.1. Az egyezmény intézményrendszere

Az egyezmény rendelkezései megvalósításának elősegítésére létrejött egy bizottság az aláíró államok delegáltjaiból. A *Kiberbűnözés Elleni Egyezmény Bizottság* vagy *Budapesti Egyezmény Bizottság* (Cybercrime Convention Committee, röviden T-CY) tevékenységének fontossága a tagállamok közötti kommunikáció megkönnyítésében és felgyorsításában

[59] Krasznay, Op.Cit. p. 208.

[60] A pozitív joghatósági összeütközések esetére ugyanis a Budapesti Egyezmény mindössze konzultációt javasol az érintett államok között, ugyanakkor ez kötelező erővel nem bír, illetőleg az egyezmény nem határoz meg ilyen esetekre prioritási sorrendet. Lásd bővebben: Brenner, Susan W.; Koops, Bert-Jaap: Approaches to Cybercrime Jurisdiction. In: Journal of High Technology Law Vol. 4, No. 1, 2004. p. 42.

[61] A kiberbűnözés vonatkozásában fennálló joghatósági problémákról és kérdésekről lásd részletesebben: Tóth Dávid; Gáspár Zsolt: Jurisdictional Challenges of Cybercrime. In: JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW Vol. 7, No. 2, 2020. pp. 101-118.

[62] Maillart, Jean-Baptiste: The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime. In: ERA Forum Vol. 19, No. 3, 2019. p 379.

keresendő. E konzultatív szervezet célja továbbá az egyezmény hatékony végrehajtásának biztosítása, illetőleg a jövőbeni módosítások mérlegelésének és megvitatásának az elősegítése.[63]

A *Kiberbűnözési Programiroda* (Cybercrime Programme Office of the Council of Europe, röviden C-PROC) az Európa Tanács alatt működő, bukaresti székhelyű szervezet, melynek célja, hogy segítséget nyújtson a világ országainak a jogrendszereik megerősítésében. E tevékenységének gyakorlása során a C-PROC a Budapesti Egyezmény szabályanyagát veszi alapul. A programiroda segítséget nyújt az egyes országoknak a kiberbűnözés és az elektronikus bizonyítékok körébe tartozó jogszabályok fejlesztésében, az ügynökségek közötti együttműködés megerősítésében, a nemzetközi együttműködés hatékonyságának növelésében és a bírók, az ügyészek és a nyomozó hatóságok tagjainak képzésében.[64]

4.1.1.2. Az egyezmény kiegészítő jegyzőkönyvei

A Budapesti Egyezmény első kiegészítésére viszonylag korán, már 2003-ban sor került. Az egyezmény első kiegészítő jegyzőkönyvének célja a kibertérben elkövetett rasszista és idegengyűlölő jellegű cselekmények kriminalizálása volt, melyre az aláíró államok elkötelezték magukat. A jegyzőkönyv 3. cikke a megkülönböztetésről, a 4. cikke a félelemkeltésről, az 5. cikke pedig az inzultálásról tartalmaz rendelkezéseket. A 6. cikk a népírtás és az emberiesség elleni bűncselekmények (például a Holokauszt) tagadásáról, kétségbe vonásáról, jelentéktelen színben való feltüntetéséről vagy azok igazolására törekvésről rendelkezik. A 7. cikkben a felbujtókra és a bűnsegédekre vonatkozó szankcionálás jelenik meg.[65]

A Kiberbűnözés Elleni Egyezmény Bizottsága 2021. május 28. napján elfogadta a második kiegészítő jegyzőkönyv tervezetét, melyet továbbított az Európa Tanács Miniszteri Bizottságának, amely 2021. november 17. napján úgyszintén elfogadta a kiegészítést.

A második kiegészítés szükségességét indokolja többek között a kiberbűnözés áldozatainak folyamatosan növekvő száma, az elektronikus bizonyítékokkal kapcsolatos joghatósági összeütközések, illetve ezek megszerzése érdekében a hatékony büntető igazságszolgáltatási lépések lehetővé tétele és a fokozottabb államközi együttműködés szükségessége.

[63] https://www.coe.int/en/web/cybercrime/tcy (2023.12.03.)
[64] https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc- (2023.12.03.)
[65] A Budapesti Egyezmény 2003. január 28. napján, Strasbourg-ban kelt ETS. no. 189. számú, a számítástechnikai rendszereken keresztül elkövetett rasszista és idegengyűlölő cselekmények kriminalizálásáról szóló kiegészítő jegyzőkönyvének 3-7. cikkei

A jegyzőkönyv 6. cikke a domainnév-bejegyzésre vonatkozó tájékoztatáskérésről rendelkezik. E körben a 2. pont konkrét jogalkotási kötelezettséget ró a tagországokra, melynek keretében biztosítaniuk szükséges, hogy a területükön lévő egyes jogalanyok a domainnévvel kapcsolatos tájékoztatás iránti kérelemre válaszolhassanak, információt adhassanak át.
A 7. cikk hasonló kötelezettségvállalást takar az előfizetői adatok átadásával kapcsolatban, melynek során az igénylő hatóságok szintén közvetlenül élhetnek felhívással a szolgáltató felé.
A 9. cikk – a hét napján, napi 24 órában működő kapcsolattartási pontok kialakítása révén – lehetővé teszi, hogy veszélyhelyzetben[66] a felek azonnali segítséget kérjenek egymástól, gyorsított adatátadás útján. A veszélyhelyzetben alkalmazható kölcsönös segítségnyújtási eljárás a jegyzőkönyv 10. cikkében kerül részletesen kifejtésre.
A 11. cikk lehetőséget biztosít arra, hogy hogy egy tanú vagy egy szakértő videokonferencia útján nyilatkozzon és tegyen tanúvallomást. E körben a megkereső tagállam által meghatározott eljárási normákat kell követni, kivéve, ha a megkeresett fél belső jogával ez nem összeegyeztethető. Ebben az esetben a megkeresett fél saját belső joga szerinti eljárást szükséges alkalmazni, ugyanakkor ettől a felek kölcsönösen eltérhetnek.
Az egyezmény kiegészítő jegyzőkönyvének 12. cikke alapján a tagállamok – közös megállapodással – közös nyomozócsoportokat hozhatnak létre és működtethetnek, amennyiben a fokozott koordináció különösen hasznosnak bizonyul. A működésüket, eljárásaikat szabadon határozhatják meg a megállapodásban, illetőleg a hatóságok közötti közvetlen kommunikáció is lehetséges. A jegyzőkönyv részletekbe nyúló, a személyes adatok védelmére irányuló intézkedéseket is tartalmaz, melynek ismertetését terjedelmi okokból a szerző jelen tanulmányban mellőzi.

4.1.2. Egyéb jelentősebb nemzetközi egyezmények

A legjelentősebb Budapesti Egyezményen kívül léteznek más, a kiberbűnözés elleni nemzetközi együttműködésre irányuló egyezmények. Ezek közül érdemes kiemelni a következőket:

- az Arab Liga (korábban Arab Államok Ligája) egyezménye az információs technológiai bűnözés elleni küzdelemről (Kairó, 2010. december 21.),
- a Független Államok Közösségének egyezménye a számítógépes információhoz kapcsolódó bűncselekmények elleni küzdelemről (2001),

[66] A második jegyzőkönyv 3. cikkében szereplő fogalommeghatározás szerint a veszélyhelyzet *„olyan helyzet, amelyben valamely természetes személy életét vagy biztonságát jelentős és közvetlen veszély fenyegeti.”*

- a Sanghaji Együttműködési Szervezet egyezménye a nemzetközi információbiztonság terén folytatott együttműködésről (2010),
- az Afrikai Unió egyezménytervezete az afrikai kiberbiztonságot elősegítő jogi keretek meghatározásáról (2012),
- az Afrikai Unió egyezménye a kiberbiztonságról és a személyes adatok védelméről (Malabo, 2014. június 27.).

4.2. Uniós szintű jogforrások

4.2.1. Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

A fenti, röviden AAIS vagy 2013-as irányelvként hivatkozott direktíva célja az információs rendszereke elleni támadások vonatkozásában a minimumszabályok meghatározása révén a tagállami jogalkotás közelítése, illetőleg az egyes nyomozó hatóságok egymással és az Európai Unió intézményeivel (pl.: ENISA, EUROPOL, EUROJUST) történő büntetőjogi együttműködés javítása, megerősítése.[67] A jogalkotó – felismerve a kiberbűnözés jelentette növekvő veszélyt, illetőleg az ilyen támadások által okozott jelentős gazdasági károkat – az egységes, közös fogalommeghatározásokra is hangsúlyt fektetett, mely körben az irányelvben meghatározásra került az információs rendszer, a számítógépes adatok, a jogi személy, illetve a jogosulatlan jelző.[68] A büntetőjogi tényállások közül az irányelv az információs rendszerekhez való jogellenes hozzáférést, a rendszert érintő jogellenes beavatkozást, az adatot érintő jogellenes beavatkozást, illetve a jogellenes adatszerzést nevesíti, továbbá ezen tényállások vonatkozásában fogalmaz meg kötelezettséget a tagállamok számára, továbbá kötelezettségvállalást tartalmaz arra nézve, hogy az előbbi bűncselekmények vonatkozásában a tagállamok büntetni rendelik a felbujtást, a kísérletet és a bűnsegélyt. [69] Az irányelv 9. cikke a szankciókra nézve tartalmaz rendelkezéseket. E körben szorgalmazza, hogy a fenti bűncselekmények szabadságvesztéssel legyenek büntetendők, egyúttal meghatározza, hogy az egyes bűncselekmények esetén mennyi legyen a büntetési tétel felső határának minimuma. Az irányelv 10-11. cikke a jogi személyek felelősségének kérdésével, illetve a velük szemben alkalmazandó szankciókkal foglalkozik. E körben az irányelv törekedve arra, hogy a szankció

[67] 2013/40/EU irányelv (1) bekezdése
[68] 2. cikk a)-d) pontjai
[69] 3-8. cikkek

hatékony, arányos és kellő visszatartó erejű legyen, a jogi személy felelősségének megállapításán túlmenően a következő szankciókat kínálja fel exemplifikatív módon:

- az állami kedvezményekből és támogatásokból való kizárás,
- a kereskedelmi tevékenység folytatásától való átmeneti vagy végleges eltiltás,
- a bírósági felügyelet alá helyezés,
- a bíróság által elrendelt felszámolás, vagy
- a bűncselekmény elkövetésére használt létesítmények ideig lenes vagy végleges bezárása.[70]

A direktíva a fentieken túlmenően elköteleződést tartalmaz az információcsere vonatkozásában is. E tekintetben a tagállamoknak gondoskodniuk kell egy saját, operatív, nemzeti kapcsolattartó pont létrehozásáról, melynek 0-24-ben rendelkezésre kell állnia. E kapcsolattartó pont sürgős esetben 8 órán belül vissza tud jelezni, hogy teljesíti-e a segítségkérést, illetőleg – amennyiben igen, úgy – milyen formában és várhatóan mennyi időn belül teszi ezt meg.[71]

4.2.2. Európai Parlament és a Tanács (EU) 2023/1543 rendelete 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

A rendelet célja egy olyan szabályrendszer megalkotása, mely révén egy tagállami hatóság a büntetőeljárásában közlésre kötelező európai határozatot vagy megőrzésre kötelező európai határozatot bocsáthat ki. Ez alapján az Európai Unióban szolgáltatást kínáló szolgáltatók kötelesek az adatok helyétől függetlenül elektronikus bizonyítékokat (adatokat) közölni vagy megőrizni.[72] A rendelet az egyes fogalmak (például a közlésre kötelező európai határozat, a megőrzésre kötelező európai határozat) meghatározását követően részletezi az egyes határozatok korlátait, illetve feltételeit. E követelmények betartása mellett a közlésre kötelező európai határozatról az ún. KKEHT tanúsítványt, míg a megőrzésre kötelező európai határozatról az ún. MKEHT tanúsítványt szükséges kitölteni, illetőleg a címzett részére továbbítani.[73] A címzett a KKEHT esetében haladéktalanul[74], míg az MKEHT esetében indokolatlan késedelem nélkül köteles intézkedni a kért adatok megőrzése iránt.[75] A KKEHT

[70] 10-11. cikkek
[71] 13. cikk
[72] Európai Parlament és a Tanács (EU) 2023/1543 rendeletének 1. cikke
[73] 9. cikk
[74] 10. cikk (1) bekezdése
[75] 11. cikk (1) bekezdése

tanúsítványok teljesítésére – amennyiben a végrehajtó hatóságot értesíteni kell – a hatóság értesítését követően, ha a hatóság 10 napon belül nem hivatkozott egyetlen megtagadási okra sem, úgy az időköz leteltével az adatok továbbíthatóak. Amennyiben a hatóság a megtagadási okok hiányában előbb megerősíti, hogy az adat továbbítható, úgy a lehető leghamarabb, de legkésőbb az időköz leteltével intézkedni kell a közlés iránt.[76] Az MKEHT esetében a megőrzésre kötelezés 60 napig tart, mely időszak letelte után a kötelezettség megszűnik, kivéve, ha az adatok vonatkozásában KKEHT kibocsátására kerül sor. A 60 napos időszak további 30 nappal meghosszabbítható.[77]

A rendelet meghatároz bizonyos megtagadási okokat is a közlésre kötelező európai határozat kibocsátásával kapcsolatban, melyek a következők:

- a kért adatokat a végrehajtó állam joga alapján biztosított olyan mentességek vagy kiváltságok védik, amelyek megakadályozzák a határozat teljesítését vagy végrehajtását, vagy a kért adatokra a sajtószabadság vagy az egyéb médiában való véleménynyilvánítás szabadsága tekintetében a büntetőjogi felelősség megállapítására vagy korlátozására vonatkozó szabályok vonatkoznak, amelyek megakadályozzák a határozat teljesítését vagy végrehajtását,
- olyan kivételes helyzet áll fenn, amikor konkrét és objektív bizonyítékok alapján alapos okkal feltételezhető, hogy a határozat teljesítése az ügy sajátos körülményei között az EUSZ 6. cikkében és a Chartában meghatározott valamely vonatkozó alapvető jog nyilvánvaló megsértésével járna,
- a határozat teljesítése ellentétes lenne a kétszeres eljárás alá vonás és a kétszeres büntetés tilalmának elvével,
- az a magatartás, amely miatt a határozatot kibocsátották, a végrehajtó állam joga szerint nem minősül bűncselekménynek, kivéve, ha a IV. mellékletben foglalt bűncselekmény-kategóriák egyikébe tartozó, a kibocsátó hatóság által a KKEHT-ban megjelölt bűncselekményről van szó, feltéve, hogy e bűncselekmény a kibocsátó állam joga szerint legalább három évig terjedő szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel büntetendő.[78]

A megőrzésre kötelező európai határozat végrehajtásával kapcsolatban a rendelet szintén megfogalmaz bizonyos megtagadási okokat, melyek a következők:

[76] 10. cikk (2) bekezdése
[77] 11. cikk (1) bekezdése
[78] 12. cikk (1) bekezdése

- a megőrzésre kötelező európai határozatot nem a rendelet 4. cikke szerinti kibocsátó hatóság bocsátotta ki vagy hitelesítette,
- a címzett nem tud eleget tenni az MKEHT-nak a címzettnek nem felróható körülményekből eredő, de facto kivitelezhetetlenség miatt, vagy pedig azért, mert az MKEHT nyilvánvaló hibákat tartalmaz,
- a megőrzésre kötelező európai határozat nem a szolgáltató által vagy nevében az MKEHT kézhezvételének időpontjában tárolt adatokra vonatkozik,
- a szolgáltatás nem tartozik a rendelet hatálya alá,
- a kért adatokat a végrehajtó állam joga alapján biztosított mentességek vagy kiváltságok védik, vagy a kért adatokra a sajtószabadság vagy az egyéb médiában való véleménynyilvánítás szabadsága tekintetében a büntetőjogi felelősség megállapítására vagy korlátozására vonatkozó szabályok vonatkoznak, amelyek megakadályozzák a megőrzésre kötelező európai határozat teljesítését vagy végrehajtását,
- olyan kivételes helyzet áll fenn, amikor pusztán az MKEHT-ban található információkból kiindulva, konkrét és objektív bizonyítékok alapján alapos okkal feltételezhető, hogy a megőrzésre kötelező európai határozat teljesítése az ügy sajátos körülményei között az EUSZ 6. cikkében és a Chartában meghatározott valamely vonatkozó alapvető jog nyilvánvaló megsértésével járna.[79]

A rendelet 15. cikke lehetőséget biztosít a tanúsítványokat végre nem hajtó szolgáltatókkal szemben szankciók kiszabására. Ezt a jogalkotó a szolgáltató előző pénzügyi évre vonatkozó, világszintű éves összforgalma 2%-ának megfelelő pénzösszegben maximalizálja. Amennyiben a szolgáltató nem működik együtt, illetőleg a kibocsátó hatóság által elfogadott indokolást sem szolgáltat, úgy a rendelet lehetőséget biztosít arra, hogy a végrehajtó hatóság végrehajtási eljárás keretében juttassa érvényre a határozatot.[80]

A rendelet 17. cikke taglalja a kötelezettségek pozitív kollíziója esetén alkalmazandó procedúrát. E körben a teljesítés megtagadását a kötelezett fél a KKEHT kézhezvételétől számított 10 napon belül indokolással ellátott kifogással tájékoztatja a kibocsátó és a végrehajtó hatóságokat. E kifogás ugyanakkor nem alapulhat pusztán azon a tényen, hogy a közlésre kötelező határozat kibocsátásának feltételeivel, alaki követelményeivel és az arra vonatkozó eljárással kapcsolatos hasonló rendelkezések nem léteznek a harmadik ország alkalmazandó jogában vagy azon, hogy az adatokat harmadik országban tárolják. A kibocsátó hatóság a kifogásban szereplő információ alapján felülvizsgálja a határozatot, melynek során vizsgálja,

[79] 16. cikk (5) bekezdésének a)-f) pontjai
[80] 16. cikk (1) bekezdése

hogy ténylegesen fennáll-e a kötelezettségek közötti ütközés. Amennyiben fennáll, úgy több egyéb szempontot figyelembe véve kell döntésre jutnia (pl.: a határozatnak való megfelelés esetén a kötelezettre vagy a szolgáltatóra nézve milyen következményei lehetnek a teljesítésnek, sérti-e a harmadik ország nemzetbiztonsági érdekeit, stb.). A vizsgálat eredményeképpen a határozatot fenntarthatja, mely esetben a végrehajtó állam illetékes bíróságától kell felülvizsgálatot kérelmezni, de dönthet úgy is, hogy megszünteti a határozatot.[81]

A rendelet bizonyos kibervédelmi intézkedéseket is előirányoz, melyek egyik követelménye, hogy az illetékes hatóságok és a kijelölt telephelyek vagy jogi képviselők közötti írásbeli kommunikációt – beleértve a formanyomtatványokat, valamint a közlésre kötelező európai határozat vagy a megőrzésre kötelező európai határozat alapján kért adatcserét – biztonságos és megbízható decentralizált informatikai rendszeren keresztül kell végrehajtani. Az egyes tagállamoknak további kötelezettsége, hogy hozzáférést biztosítsanak a szolgáltatóknak e rendszerhez. A szolgáltatók szintén kötelezettséget vállalnak, hogy megfelelően használják a rendszert, lehetővé teszik a telephelyeik, jogi képviselőik számára, hogy a rendszert alkalmazzák, továbbá rendelkezniük szükséges valamilyen alternatívával is, arra az esetre, ha a rendszer meghibásodik vagy annak alkalmazása valami okból kifolyólag akadályoztatott. Amennyiben az utóbbi eshetőségre bekövetkezne, a szolgáltatóknak indokolatlan késedelem nélkül kell a decentralizált rendszerben rögzíteni a továbbítást.[82]

A rendelet által létrehozott rendszert viszonylag gyorsan szükséges kialakítania a tagállamoknak, a rendeletet ugyanis 2026. augusztus 18. napjától kell alkalmazni. Rövidtávon ez kihívást jelenthet a tagországoknak, ugyanakkor az új rendszer rengeteg előnnyel járhat, illetőleg jelentősen megkönnyítheti a nyomozó hatóságok napi munkáját.

4.2.3. A NIS irányelv[83]

Az első kifejezetten kiberbiztonsági célzatú uniós irányelv 2016-ban lépett hatályba. A tagállamok – felismerve a hálózati és információs rendszerek társadalomban betöltött szerepét és a biztonsági események egyre növekvő számát – arra az elhatározásra jutottak, hogy megalkotják az uniós szintű minimumszabályozást a kibervédelem területén.[84] Az irányelv

[81] 17. cikk (1)-(6) bekezdései
[82] 19. cikk (1)-(6) bekezdései
[83] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (a továbbiakban röviden: NIS1 irányelv)
[84] NIS 1 irányelv (1)-(3) bekezdései

célja egy európai szintű együttműködés közös intézményi és jogszabályi alapjainak megteremtése.[85] Annak érdekében, hogy az említett törekvéseknek a tagállamok eleget tudjanak tenni, az irányelv kötelezettségvállalást tartalmaz a következőkre vonatkozóan:

- a tagállamok a hálózati és információs rendszerek biztonsága érdekében nemzeti stratégiát fogadnak el,
- létrehoznak egy együttműködési csoportot, melynek célja a stratégiai kooperáció és az információcsere elősegítése,
- létrehoznak egy számítástechnikai biztonsági eseményekre reagáló csoportot (Computer Security Incident Response Team, röviden CSIRT) a gyors és hatékony operatív együttműködés végett,
- biztonsági és bejelentési követelményeket állapítanak meg a digitális szolgáltatók[86] és az alapvető szolgáltatásokat nyújtó szereplők[87] számára,
- a hálózati és információs rendszerek biztonságával kapcsolatos feladatok ellátására kijelölnek egy illetékes nemzeti hatóságot, egyedüli kapcsolattartó pontokat és CSIRT-eket.[88]

Az irányelv a nemzeti kibervédelmi stratégiával kapcsolatban az alábbi tartalmi követelményeket rögzíti:

- a cél és a prioritások meghatározása,
- az irányítási keretrendszer és egyéb érintett szervek szerepkörének, felelősségének lehatárolása,
- a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítása, ideértve a köz- és a magánszféra közötti együttműködést is,
- a stratégiához kapcsolódó oktatási, tájékoztató és képzési programok megjelölése,
- a stratégiához kapcsolódó kutatási és fejlesztési (K+F) tervek meghatározása,
- a kockázatok feltárására szolgáló kockázatértékelési terv,
- a stratégia végrehajtásába bevont egyes szereplők jegyzéke.[89]

A nemzeti kibervédelmi stratégia kidolgozásához a tagállamok segítséget kérhetnek az ENISA-tól. További követelményként jelenik meg a rendeletben, hogy a stratégia elfogadását követően

[85] https://nki.gov.hu/figyelmeztetesek/archivum/megjelent-a-halozati-es-informacios-rendszerek-biztonsagarol-szolo-eu-s-iranyelv/ (2024.02.21.)
[86] Az irányelv III. mellékletének alkalmazásában a digitális szolgáltatások típusai közé tartoznak az online piacterek, az online keresőprogramok, illetőleg a felhőalapú számítástechnikai szolgáltatások.
[87] Az alapvető szolgáltatást nyújtó szervezetek típusait az irányelv II. melléklete tartalmazza. Ezek az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvíz-ellátás és elosztás, valamint a digitális infrastruktúra.
[88] NIS 1 irányelv 1. cikke (2) bekezdésének a)-e) pontjai
[89] NIS 1 irányelv 7. cikke (1) bekezdésének a)-g) pontjai

azt (a nemzetbiztonsággal kapcsolatos elemek kivételével) három hónapos határidőn belül meg kell küldeni a Bizottság részére.[90]

Az irányelv 12. cikke rendelkezik a CSIRT-ek hálózatáról, mely a tagállamok CSIRT-jeiből és a CERT-EU képviselőikből áll. A hálózathoz az ENISA biztosítja a titkárságot, illetőleg támogatja a tagok közötti együttműködést. A hálózat feladatköre sokrétű, egyrészről információcsere platformjaként szolgál, másrészről aktívan részt vesz az egyes biztonsági incidensek analízisében, amennyiben kell, úgy pedig koordinált választ ad az adott problémára.[91] A CSIRT-ek kötelezettségeit és feladatkörét az irányelv I. számú melléklete tartalmazza. Ez alapján a CSIRT-ek ellátják a következő feladatokat:

- a biztonsági események nemzeti szintű monitoringja,
- a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára,
- reagálás a biztonsági eseményekre,
- dinamikus kockázat- és eseményelemzés, valamint helyzetkép nyújtása,
- a CSIRT-ek hálózatában való részvétel.[92]

A fenti feladatok ellátása mellett a CSIRT-ek kötelezettsége, hogy a kritikus hibapontok kiküszöbölése révén biztosítsák a hírközlési szolgáltatásaik magas szintű elérhetőségét, illetve az üzletmenet folytonosságát.[93]

4.2.4. A NIS 2 irányelv[94]

Az első NIS irányelv (2016/1148/EU) felülvizsgálata feltárta az irányelv hiányosságait, illetőleg elegendő indokot biztosított arra, hogy az EU továbbfejlessze ezt a területet. A felülvizsgálat egyrészről jelentős eltéréseket mutatott az irányelv tagállamok általi végrehajtása terén, beleértve a hatály tekintetében, amelynek lehatárolása nagyrészt a tagállamok mérlegelési jogkörében maradt. Az irányelv másrészről igen tág mérlegelési jogkört biztosított a tagállamoknak az egyes biztonság események jelentéstételi kötelezettségeinek végrehajtása terén. A fentiek mellett továbbá jelentős eltérések vannak a felügyeletre és végrehajtásra

[90] NIS 1 irányelv 7. cikkének (2)-(3) bekezdései
[91] NIS 1 irányelv 12. cikke
[92] NIS 1 irányelv I. mellékletének (2) bekezdése
[93] [93] NIS 1 irányelv I. mellékletének (1) bekezdése
[94] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (a továbbiakban röviden: NIS2 irányelv)

vonatkozó rendelkezések végrehajtásában is.[95] Tekintve, hogy a NIS 1 irányelv célja a kiberbiztonság egységesen magas szintjének elérése a tagállamokban, a fenti eltérések okozta problémák végső soron az irányelv célját veszélyeztetik. A fentiekre tekintettel tehát az előző irányelv hiányosságainak kiküszöbölése érdekében szükség volt annak revíziójára, ennek okán pedig létrejött a NIS 2 irányelv. Az új rendelet szakít az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók közötti megkülönböztetéssel, mivel az elavultnak bizonyult.[96]

Az irányelv személyi hatályát tekintve kiterjed az irányelv I. és II. mellékletében körülírt olyan állami vagy magánszervezetekre, amelyek a 2003/361/EK ajánlás mellékletének 2. cikke szerint középvállalkozásoknak minősülnek vagy meghaladják az említett cikkben a középvállalkozásokra vonatkozóan előírt küszöbértékeket, és amelyek az Unión belül nyújtják szolgáltatásaikat vagy végzik tevékenységeiket. Az ilyen szervezetek esetén akkor lehet alkalmazni az irányelvet, ha

- a szervezet
    - nyilvános elektronikus hírközlő hálózatok szolgáltatójának vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatónak minősül,
    - bizalmi szolgáltató,
    - legfelső szintű doménnév-nyilvántartó és doménnévrendszer-szolgáltató,
- a szervezet egy tagállamban az egyetlen szolgáltató egy olyan szolgáltatás tekintetében, amely elengedhetetlen a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához,
- a szervezet által nyújtott szolgáltatás zavara jelentős hatással lehet a közvédelemre, a közbiztonságra vagy a közegészségre,
- a szervezet által nyújtott szolgáltatás zavara jelentős rendszerszintű kockázatot idézhet elő, különösen, ha ennek határokon átnyúló hatása lehet,
- a szervezet kritikus, mivel nemzeti vagy regionális szinten különös jelentőséggel bír az adott ágazat vagy szolgáltatás típusa, vagy a tagállam más, kölcsönösen függő ágazatai szempontjából,
- a szervezet:
    - valamely tagállam által annak nemzeti jogával összhangban meghatározott, központi kormányzathoz tartozó közigazgatási szerv, vagy

[95] NIS 2 irányelv (4) bekezdése
[96] NIS 2 irányelv (6) bekezdése

- valamely tagállam által annak nemzeti jogával összhangban meghatározott, regionális szintű közigazgatási szerv, amely kockázatalapú értékelés alapján olyan szolgáltatásokat nyújt, amelyek zavara jelentős hatást gyakorolhat kritikus fontosságú társadalmi vagy gazdasági tevékenységekre.[97]

A fentiek mellett az irányelv továbbá alkalmazandó a 2022/2557/EU irányelv szerint kritikus szervezetként azonosított szervezetekre, valamint a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetekre is,[98] továbbá a tagállamok mérlegelési joga szerint a helyi szintű közigazgatási szervekre és az oktatási intézményekre, különösen, ha kritikus fontosságú kutatási tevékenységeket végeznek.[99]

A nemzeti kiberbiztonsági stratégia kapcsán az irányelv az aktív tevékenységeket részesíti előnyben a passzív reakcióval szemben. Ennek kapcsán – többek között – a következő szakpolitikák fontosságát emeli ki:

- IKT termékek és szolgáltatások kiberbiztonsága,
- sérülékenységek kezelése,
- kis- és középvállalkozások alapszintű kibervédelmének megerősítése,
- aktív kiberbiztonság előmozdítása,
- a tudományos és kutatóintézetek támogatása a kiberbiztonsági eszközök és a biztonságos hálózati infrastruktúra fejlesztésére, megerősítésére és bevezetésének előmozdítására,
- a legkorszerűbb kiberbiztonsági kockázatkezelési intézkedések végrehajtását célzó megfelelően fejlett technológiák fejlesztésének és integrációjának előmozdítása,
- oktatás és képzések a kiberbiztonság terén.[100]

Az irányelv bizonyos intézményi és szervezeti követelményeket is meghatároz a tagállamok számára. Ennek fényében a tagállamoknak ki kell jelölniük vagy létre kell hozniuk egy (vagy több) a kiberbiztonságért és a felügyeleti és végrehajtási feladatokért illetékes hatóságo(ka)t,[101] továbbá egy (vagy több), a nagyszabású kiberbiztonsági események és válságok kezeléséért felelős hatóságo(ka)t.[102] Az irányelv 10. cikke rendelkezik a CSIRT-ek létrehozásáról és azok körülményeiről, míg a CSIRT-ekre vonatkozó konkrét követelményeket, illetőleg azok feladatkörét az irányelv 11. cikke, a CSIRT-hálózat részleteit pedig a 15. cikke rögzíti.

[97] NIS 2 irányelv 2. cikkének (1)-(2) bekezdései
[98] NIS 2 irányelv 2. cikkének (3)-(4) bekezdései
[99] NIS 2 irányelv 2. cikkének (5) bekezdése
[100] NIS 2 irányelv 7. cikkének (2) bekezdése
[101] NIS 2 irányelv 8. cikkének (1) bekezdése
[102] NIS 2 irányelv 9. cikkének (1) bekezdése

Az irányelv egyik legnagyobb újítása, hogy hivatalosan is létrehozta az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (European Cyber Crisis Liaison Organisation Network, röviden EU-CyCLONe) a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelésének támogatása, továbbá a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása végett.[103] A hálózat tagjai a tagállami kiberválságok kezelésével foglalkozó hatóságok képviselőiből állnak, akikhez egyes esetekben a Bizottság képviselői csatlakoznak.[104] Feladatkörét tekintve a következők emelendők ki:

- a nagyszabású kiberbiztonsági események és válságok kezelésére való felkészültségi szint növelése,
- a nagyszabású kiberbiztonsági eseményekkel és válságokkal kapcsolatos közös helyzetismeret kialakítása,
- a nagyszabású kiberbiztonsági események és válságok hatásértékelése, valamint azok mérséklését szolgáló intézkedésekre történő javaslattétel,
- a nagyszabású kiberbiztonsági események és válságok kezelésének összehangolása és az ezekkel kapcsolatos politikai döntéshozatal támogatása,
- valamely érintett tagállam kérésére a nagyszabású nemzeti kiberbiztonsági eseményekre és válságokra való reagálási tervek megvitatása.[105]

Az irányelv IV. fejezete meghatározza a kiberbiztonsági kockázatkezelési intézkedések és jelentéstételi kötelezettségek alapvetéseit. A kiberbiztonsági kockázatkezelési intézkedések körében az irányelv rögzíti, hogy minden veszélyre kiterjedő megközelítésen kell alapulniuk. Ebből a célból pedig a következő területekre kell fókuszálni:

- kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok,
- eseménykezelés,
- üzletmenet-folytonosság,
    - tartalékrendszerek kezelése,
    - katasztrófa utáni helyreállítás és válságkezelés,
- az ellátási lánc biztonsága,
- biztonság a hálózati és információs rendszerek beszerzésében, fejlesztésében és karbantartásában, sérülékenység-kezelés és közzététel,

[103] NIS 2 irányelv 16. cikkének (1) bekezdése
[104] NIS 2 irányelv 16. cikkének (2) bekezdése
[105] NIS 2 irányelv 16. cikkének (3) bekezdése

- kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelését szolgáló szabályzatok és eljárások,
- alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzés,
- szabályzatok és eljárások a kriptográfia és a titkosítás használatára,
- humánerőforrás-biztonság, hozzáférés-ellenőrzési szabályzatok és eszközgazdálkodás,
- többtényezős vagy folyamatos hitelesítési megoldások, biztonságos hang-, video- és szöveges kommunikáció, valamint biztonságos vészhelyzeti kommunikációs rendszerek használata.[106]

A jelentéstételi kötelezettségek terén az irányelv a korábbi NIS 1 irányelv rendelkezéseivel összevetve sokkal konkrétabb szabályanyagot tartalmaz, melynek keretében pontosan meghatározza, hogy mikor tekinthető jelentősnek egy esemény, ezzel kiküszöbölve a tagállamok közötti eltéréseket.[107]

Az irányelv VII. fejezete taglalja a felügyelet és végrehajtás szabályait, követelményeit. E körben az irányelv 34. cikke rendelkezik a közigazgatási bírság, mint szankció részleteiről, illetőleg mértékéről is, melyet a 32-34. cikkekben foglaltak alapján kell meghatározni. Ennek során kiemelt jelentőséget kell fordítani a 32. cikk (7) bekezdésében foglalt körülményekre, melyek:

- a jogsértés súlya, a megsértett rendelkezés jelentősége,
- a jogsértés időtartama,
- az érintett szervezet által korábban elkövetett releváns jogsértések,
- az okozott bármely vagyoni vagy nem vagyoni kár,
- a bűnösség foka (szándékosság vagy gondatlanság),
- a szervezet által a kár megelőzésére vagy mérséklésére tett intézkedések,
- a jóváhagyott magatartási kódexek vagy tanúsítási mechanizmusok betartása,
- az illetékes hatóságokkal való együttműködésének szintje.

A tagállamok e körben kötelezettséget vállalnak arra, hogy az alapvető szervezetek jogsértése esetén minimum 10.000.000,- euró vagy ha az magasabb, legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 2%-a, amelyhez az alapvető szervezet tartozik. Ez az összeg a fontos szervezetek vonatkozásában legalább 7.000.000,- euró vagy ha az magasabb, akkor legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 1,4%-a, amelyhez tartozik.[108]

[106] NIS 2 irányelv 21. cikke (2) bekezdésének a)-j) pontjai
[107] NIS 2 irányelv 23. cikkének (3) bekezdése
[108] NIS 2 irányelv 34. cikkének (3)-(5) bekezdései

4.2.5. További uniós részletszabályok

A fentiekben részletesen kifejtett jogforrásokon kívül más aktusokban is találhatóak további részletszabályok, melyek említést érdemelnek.

A *2011/93/EU irányelv*[109] létrejöttének oka, hogy a gyermekek szexuális bántalmazását ábrázoló képek, továbbá a gyermekek szexuális bántalmazásának és szexuális kizsákmányolásának más különösen súlyos formái az új technológiák és az internet használata révén egyre növekvő méreteket öltenek, terjedésük egyre gyorsabb.[110] További fenyegetést rejt magában az a tény, hogy az internet eddig még nem látott mértékű névtelenséget biztosít a felhasználók számára, akik könnyedén elrejthetik valós személyazonosságukat és életkorukat.[111]

Az irányelv 25. cikke rendelkezik a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedésekről. E körben az (1) bekezdés szerint a tagállamok kötelezettséget vállalnak arra, hogy a területükön üzemeltett ilyen jellegű weboldalakat azonnali hatállyal eltávolítják, valamint törekednek a területükön kívül üzemeltetett ilyen weboldalak eltávolítására is. A (2) bekezdés felhatalmazza a tagállamokat arra, hogy intézkedéseket tegyenek a gyermekpornográfiát tartalmazó vagy azt terjesztő, a területükön található internetfelhasználókat célzó weboldalakhoz való hozzáférés meggátolására. Ezen intézkedéseket kellően transzparens, megfelelő garanciákat tartalmazó eljárások során kell meghozni, melyek során kiemelt figyelmet kell szentelni a szükségesség-arányosság követelményének, további biztosítani kell a bírósági jogorvoslati lehetőséget is. Az előbbiek mellett az irányelv minimumszabályozást tartalmaz arra vonatkozóan is, hogy a gyermekeket érintő szexuális bűncselekmények megfelelően és egységesen legyenek kriminalizálva a tagországokban. Ezek között található továbbá számos olyan bűncselekmény, melyet internetes közegben is el lehet követni, így a direktíva e szempontból is releváns lehet.

Az uniós jogi aktusok közül mindenképpen szükséges kiemelni az ún. *DORA-rendeletet*[112] is, mely az Európai Unió pénzügyi szektorának a kibertámadásokkal szembeni ellenállóságát

[109] Az Európai Parlament és a Tanács 2011/93/EU irá nyelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról

[110] (3) bekezdés

[111] (19) bekezdés

[112] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (a továbbiakban: DORA-rendelet)

hivatott biztosítani. A rendelet legjelentősebb újítása, hogy bevezeti és harmonizálja a digitális működési követelményeket az Európai Unió pénzügyi szolgáltatási szektorában, egyúttal pedig kötelezi a vállalatokat, hogy bizonyosodjanak meg arról, hogy képesek ellenállni a IKT-val kapcsolatos zavaroknak és fenyegetéseknek, képesek azokra kellően reagálni.[113] A rendelet egyik érdekessége, hogy a személyi hatálya kiterjed a pénzügyi szektor klasszikus szereplőin kívül az elektronikuspénz-kibocsátó intézményekre, illetőleg a kriptoeszközök piacairól szóló rendelet alapján engedélyezett kriptoeszköz-szolgáltatókra, valamint az eszközalapú tokenek kibocsátóira is.[114] A rendelet megjelenését követően a három európai felügyeleti hatóság (az Európai Bankhatóság, az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság és az Európai Értékpapír-piaci Hatóság) közzétette a DORA-rendelet szerinti végleges technikai standardtervezetek első csoportját. Ez magába foglalja a szabályozástechnikai standardokat az IKT kockázatkezelési keretrendszerre vonatkozásában, az IKT-vonatkozású események osztályozási kritériumaival kapcsolatban és a kritikus vagy fontos funkciókat támogató IKT szolgáltatókra vonatkozóan, illetőleg a végrehajtás-technikai standardokat az információ-nyilvántartás mintadokumentumainak meghatározása érdekében.[115]

Kiemelendő továbbá a *2019/713/EU irányelv*[116], mely a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és az ilyen eszközök hamisítása ellen kíván fellépni. Az irányelv (8) bekezdése szerint *„a fogalommeghatározásoknak ki kell terjedniük a készpénz-helyettesítő fizetési eszközök olyan új típusaira is, amelyek lehetővé teszik az elektronikus pénz és a virtuális fizetési eszközök átutalását."* A virtuális fizetőeszköz fogalmát az irányelv az 5. pénzmosás elleni uniós irányelv fogalomtárából vette át. Az irányelv (10) bekezdése rögzíti, hogy a virtuális fizetőeszközök átutalását lehetővé tevő digitális pénztárcák (tehát a kriptovaluta-tárcák is) az irányelv hatálya alá tartoznak, mint a készpénz-helyettesítő fizetési eszközök. Polt Péter tanulmányában rögzíti, hogy a Btk. 76. §-a alapján – a vagyonelkobzás vonatkozásában – *a kriptovaluták, mint pénzben kifejezhető értékkel bíró előnyök, büntetőjogi értelemben*

[113] https://www.europarl.europa.eu/topics/hu/article/20221103STO48002/harc-a-kiberbunozes-ellen-az-uj-unios-kiberbiztonsagi-torvenyek-magyarazata (2024.03.04.)
[114] DORA-rendelet 2. cikke (1) bekezdésének d) és f) pontjai
[115] „Az európai felügyeleti hatóságok közzétették a DORA rendelet első csomagjába tartozó, az IKT- és harmadik fél kockázatkezelésre és az incidensek osztályozására vonatkozó részletszabályokat" https://www.mnb.hu/felugyelet/felugyeleti-keretrendszer/felugyeleti-hirek/hirek-ujdonsagok/az-europai-felugyeleti-hatosagok-kozzetettek-a-dora-rendelet-elso-csomagjaba-tartozo-az-ikt-es-harmadik-fel-kockazatkezelesre-es-az-incidensek-osztalyozasara-vonatkozo-reszletszabalyokat (2024.03.05.)
[116] Az Európai Parlament és a Tanács (EU) 2019/713 irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról

vagyonelemnek minősülnek.[117] Polt szerint a hivatkozott irányelv vagyoni fogalmának megfelel a Btk. megoldása. Álláspontom szerint az irányelvet a kriptovaluta-tárcák vonatkozásában lehet alkalmazni, tehát konkrétan a kriptovaluták fogalmát nem érinti. Ahogyan az irányelv preambulumának (10) bekezdéséből is kiderül, a jogalkotó nem mondja ki expressis verbis, hogy a kriptovaluták (vagy ahogyan az irányelv fogalmaz, virtuális fizetési eszközök) készpénz-helyettesítő fizetési eszközöknek minősülnek, mindössze rögzíti, hogy a virtuális fizetési eszközök átutalását lehetővé tevő digitális pénztárcákra is kiterjed az irányelv tárgyi hatálya. Ugyanakkor a jogi aktus elnevezéséből és fogalomhasználatából egyértelműen nem tűnik ki az, hogy az irányelv élesen külön kezelné a fenti kategóriákat, véleményem szerint ez a fogalmi ellentmondás pedig alkalmas arra, hogy az egyes definíciókat összemossa, fogalmi zavart idézzen elő.

A már említett uniós jogforrásokon kívül érdemes megemlíteni, hogy – magától értetődően – a jogalkotás folyamatos tevékenység, így jelen kézirat lezárásakor is léteznek bizonyos „tervezet" vagy ún. „draft" fázisban lévő uniós jogi aktusok. Ezek közül pedig kiemelendő kezdeményezés az ún. *kiberreziliencia törvény-tervezet*, mely a digitális termékek biztonságát hivatott növelni.[118]

4.3. Hazai jogszabályok

A hazai büntetőjogi és büntető eljárásjogi jogszabályi környezet vizsgálata során leszögezhető, hogy a legnagyobb jelentőségű normák, melyekből ki kell indulni, az anyagi jog tekintetében a Büntető Törvénykönyv, az eljárásjogi szabályok vonatkozásában pedig a Be. Rögzítendő ugyanakkor, hogy e két kódex koránt sem tartalmaz minden szabályanyagot a kiberbűnözés által megvalósítható tényállások megítéléséhez. Bizonyos részletszabályokat a jogalkotó – különböző elgondolásokból – nem tett részévé sem a Btk.-nak, sem pedig a Be.-nek, így néhány esetben más jogforrásokat (például a Pmt.-t, Hpt.-t) is szem előtt kell tartani. A Büntető Törvénykönyv és az eljárásjogi kódex vonatkozó rendelkezései az értekezés további részeiben, az egyes bűncselekménytípusok áttekintésénél, valamint a büntetőeljárásnak a kriptovaluták vonatkozásában releváns fejezetében kerülnek kifejtésre.

[117] Polt Péter: A 21. század kihívásainak hatása a büntetőeljárásra: Kriptovaluták, azaz az új vagyoni értékek büntetőjogi kérdései. In: Barabás Andrea Tünde; Christián László (szerk.): Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est. Budapest, Ludovika Egyetemi Kiadó, 2021. pp. 422-423.

[118] https://www.europarl.europa.eu/news/hu/press-room/20230717IPR03029/cyber-resilience-act-meps-back-plan-to-boost-digital-products-security (2024.03.04.)

5. Az Európai Unió eszköztára a kiberbűnözés elleni harcban

5.1. A kiberbűnözésre szakosodott uniós intézmények rendszere

5.1.1. Az Europol

A rendőrségi és bírósági együttműködések a gazdasági kötelékek megerősödésével párhuzamosan fejlődtek az Európai Unió tagállamai között. Az ellenőrzések eltörlése a határokon átnyúló bűnözés megerősödését eredményezte, így sürgető volt a tagállomok együttműködésének intézményesítése ezeken a területeken.[119] A tagállamok közötti büntetőjogi kooperáció és az European Police Office (röviden: Europol) megalapítása már az 1992-es Maastrichti Szerződésben is kitűzött cél volt, azzal az elképzeléssel, hogy egy tagállamok közötti rendőrségi együttműködést hozzanak létre a terrorizmus, kábítószer-kereskedelem és a nemzetközi bűnözés más formái elleni küzdelem megerősítése érdekében, melynek alapját az Europol képezné az információ-áramlás biztosításának révén.[120] Az Europol Drugs Unit (röviden EDU) hágai központtal 1994-ben kezdte meg működését, ekkor még korlátozott formában, nevéből is kitűnik, hogy legfontosabb feladata ekkor a kábítószer-kereskedelem és a pénzmosás megfékezése volt, a következő évben a Miniszterek Tanácsa ugyanakkor kibővítette a hatáskörét és az Europol általánosan elfogadottá vált a tagállamok között.[121] Az Europol fő célja a tagállami nyomozó hatóságok munkájának megkönnyítése, hatékonyságuk növelése a terrorizmus és a nemzetközi bűnözés elleni küzdelem során. A legfontosabb feladatai többek között:

- az információ áramlásának megkönnyítése a tagállamok között,
- támogatás nyújtása a tagállami nyomozó hatóságok operációi során,
- bűnözéssel kapcsolatos információk összegyűjtése, rendszerezése és vizsgálata,
- az adatok vizsgálatára szolgáló számítógépes informatikai rendszer fejlesztése és karbantartása,
- gyakorlati és technikai segítség nyújtása a tagállami nyomozó hatóságok nyomozásaihoz.[122]

2013-ban az Europol felállította az Európai Kiberbűnözési Központot (European Cybercrime Centre, röviden EC3), a kiberbűnözéssel kapcsolatos megerősített uniós jogi szabályozások

[119] Nikač, Željko: The European Arrest Warrant-Europol. In: International Journal of Economics and Law 2014/4, pp. 91-92.
[120] Lásd: Európai Unióról szóló szerződés (Maastrichti Szerződés) VI. cím, K1 cikk
[121] https://www.policija.si/eng/areas-of-work/other-areas/international-cooperation/europol (2020.09.24.)
[122] Nikač, Op.Cit. 2014, p. 92.

támogatása, illetőleg az uniós polgárok, kormányok és vállalkozások védelme végett. Az EC3 a következő feladatkörökkel rendelkezik:

- a kiberbűnözéssel kapcsolatos adatgyűjtés, az összegyűjtött adatok feldolgozása, továbbá helpdesk üzemeltetése a tagállami nyomozó hatóságok számára,
- az uniós tagállamok területén történő nyomozás támogatása, közös nyomozócsoportok támogatása, az EU-n kívüli partnerekkel történő együttműködés elősegítése, komplex nemzetközi ügyek koordinálása az Eurojust-tal és az Interpol-lal,
- a kiberfenyegetések értékelése, az elkövetési trendek elemzése, új fejlemények előrejelzése,
- a CEPOL-lal történő szoros együttműködés, illetőleg képzések szervezése a tagállami nyomozó hatóságok és igazságügyi alkalmazottak számára,
- a privát szféra szereplőivel, valamint a CERT-ekkel történő együttműködés.[123]

Az EC3 keretein belül három ún. fókuszpont található:

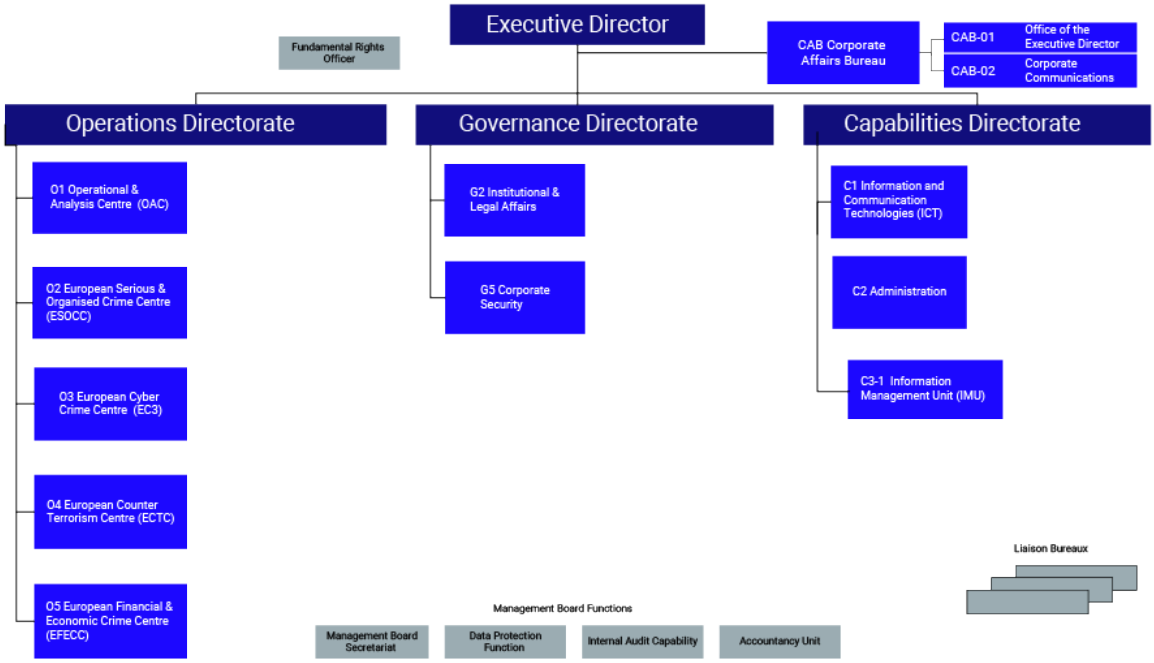
- a kiberbűncselekmények (FP Cyborg),
- a gyermekek szexuális kizsákmányolása (FP Twins), illetve
- a bankkártyás csalások (FP Terminal).[124]

A Központ évente kiadja jelentését az internetes szervezett bűnözés veszélyeiről (Internet Organised Crime Threat Assessment, röviden IOCTA), melyben a terület jogi szabályozásának megerősítésére is tesz javaslatokat, emellett kulcsfontosságú információval szolgál a tagállamok kormányai, illetve az uniós polgárok és vállalkozások számára. 2014 óta a Központhoz tartozik egy kiberbűnözéssel foglalkozó különítmény is,[125] melynek feladata akciócsoportként többek között a kiberbűnözéssel kapcsolatos határokon átívelő nyomozások és műveletek koordinálása. Az említett intézmények kiépítése számos sikert eredményezett, többek között:

- egy egyesített művelet koordinálása egy botnet, a Ramnit ellen, mely számítógépek millióit fertőzte meg az egész világon,
- egy, az Eurojust-tal közös művelet koordinálása, melynek eredményeként számos Ukrajnából induló malware támadást sikerült felderíteni, mely művelet során több ügynökség is részt vett a nyomozásban és így több elkövetőt is sikerült beazonosítani és letartóztatni,

[123] Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. In: THEMIS: Az ELTE Állam- és Jogtudományi Doktori Iskola Elektronikus Folyóirata Vol. 13, No. 1, 2015. p. 371.
[124] Ibid.
[125] Joint Cybercrime Action Taskforce (J-CAT)

- egy művelet egy nagyobb, kiberbűnözésre szakosodott fórum, az ún. Zero Day Exploits ellen, mely hackeléssel, malware és botnet programokkal kereskedett.[126]



2. ábra: Az Europol szervezeti felépítése. Forrás: https://www.europol.europa.eu/about-europol:hu (Letöltés dátuma: 2024.02.03.)

5.1.2. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA)

Az Európai Parlament és a Tanács 460/2004/EK számú rendeletével 2004-ben megalakult az athéni székhelyű Európai Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, röviden ENISA), melynek célja a kiberbiztonság egységesen magas szintjének megteremtése az Európai Unióban. A szervezet mandátuma 2008-2013-ig folyamatosan bővült, majd az elnevezése 2019-ben[127] Európai Uniós Kiberbiztonsági Ügynökségre változott.[128]

Az ügynökség szervezete a következőképpen épül fel:

- Igazgatótanács: biztosítja az alapító rendelettel összhangban történő szervezeti működés feltételeit,

[126] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime (2020.09.21.)
[127] Az ügynökség működésének jogszabályi kereteit jelenleg az Európai Parlament és a Tanács 2019/881/EU irányelve határozza meg.
[128] https://www.enisa.europa.eu/about-enisa/regulatory-framework (2024.02.24.)

- Felügyelőtestület: előkészíti az Igazgatótanács részére az elfogadandó határozatokat,
- Ügyvezető igazgató: az ügynökség irányításáért felelős független tisztség,
- Nemzeti kapcsolattartó tisztviselők hálózata: az ügynökség és a tagállamok közötti információcserét hivatott biztosítani,
- Tanácsadó csoport: az érdekképviseleti tevékenység,
- Eseti munkacsoportok: szakértőkből álló csoportok, melyek konkrét tudományos- és/vagy műszaki kérdésekkel foglalkoznak.[129]

Az ENISA célkitűzései és feladatai közé tartozik egy ágazatokon átívelő együttműködési keret létrehozása, egy egységes kiberbiztonsági szakpolitika kialakítása, az uniós szintű operatív együttműködés támogatása, a képzések fejlesztése, a kapacitásépítés.[130]

5.1.3. Az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (Eurojust)

Az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége (European Union Agency for Criminal Justice Cooperation avagy Eurojust) 2002-ben alakult meg, majd 2003-tól hágai székhellyel működik. 2002-es létrehozása óta az Eurojust jogi kereteit két ízben érte nagyobb módosítás, 2003-ban és 2009-ben.[131] A szervezet célja az egyes nemzeti hatóságok közötti koordináció javítása a két vagy több tagállamot érintő büntetőeljárások esetében. Ennek legfőbb eszközei a kölcsönös nemzetközi (vagy európai) jogsegélyek és az európai elfogatóparancs.[132] Működését tekintve a főbb feladat- és hatáskörébe tartoznak a következők:

- a nyomozás vagy büntetőeljárás megindításának szempontjából annak megállapítása, hogy több tagállam közül melyik van kedvezőbb helyzetben,
- az illetékes hatóságok munkájának összehangolása,
- közös nyomozócsoportok létrehozása,
- a tagállami hatóságok felkérése, hogy egy konkrét ügyben rendeljenek el nyomozást vagy büntetőeljárást,
- információ bekérése a tagállami hatóságoktól,
- a hatóságok közötti információcsere biztosítása.[133]

Az Eurojust felépítését tekintve három szervezeti egységre bontható: a testületre, az igazgatótanácsra és a hivatalra. A testület tagjai a résztvevő uniós tagállamok egy-egy nemzeti

[129] https://www.enisa.europa.eu/about-enisa/about/hu (2024.02.24.)
[130] Ibid.
[131] A kézirat lezártakor az Eurojust hatályos jogi kereteit az Európai Parlament és a Tanács 2018/1727/EU rendelete rögzíti.
[132] https://e-justice.europa.eu/23/HU/eurojust (2024.03.04.)
[133] Ibid.

tagja és – ha a testület nem operatív jellegű ügyben jár el, akkor – az Európai Bizottság egy képviselője. Az igazgatótanács tagjai az elnök, két alelnök és az Európai Bizottság egy képviselője, illetőleg a testület két tagja.[134]

Az Eurojust szervezete prioritásként kezeli a súlyos és összetett bonyolultságú, határokon átnyúló bűnügyeket, melyek típusai a teljesség igénye nélkül a következők:

- terrorizmus,
- pénzmosás,
- kiberbűnözés,
- kábítószer-kereskedelem,
- PIF-bűncselekmények,
- migránsok csempészése,
- környezeti bűnözés,
- csalás.[135]

A kiberbűnözés elleni szerepét tekintve az Eurojust több projektben is részt vesz, melyek közül kiemelendő a SIRIUS-projekt. Ez egy, az Europol, az Eurojust és az Európai Igazságügyi Hálózat együttműködésében létrejött olyan projekt, melynek célja egy olyan platform létrehozása volt, ami kellően képes segíteni a tagállami nyomozó hatóságokat azzal, hogy számukra információt biztosít, iránymutatásokat és tapasztalatokat oszt meg. Egy másik említést érdemlő iniciatíva a GLACY+ projekt, melyet az Európai Unió és az Európa Tanács közös kezdeményezésére hoztak létre. Célja 12 kiemelt (afrikai, ázsiai, csendes-óceáni, latin-amerikai és karibi) ország kiberkapacitásának növelése volt.[136]

5.1.4. Az Európai Unió Kiberbűnözés Elleni Akciócsoportja (EUCTF)

Az akciócsoport egy bizalmi alapú együttműködés, mely évente kétszer ülésezik és mintegy informatív fórumként szolgál az uniós tagállamok és a társult országok (Egyesült Királyság, Svájc, Norvégia, Izland és Dánia), valamint az EUROPOL, az EUROJUST és a CEPOL szakértői számára. Célkitűzései között szerepelnek többek között az alábbiak:

- a kiberbűnözés és a számítógépes bűnözés megelőzése, felderítése,
- az internet hatékony irányításának előmozdítása,
- a bűnügyi infrastruktúra eltörlése,

[134] https://www.eurojust.europa.eu/sites/default/files/2020-12/2020-08_Generic-factsheet_public_Final4_HU.pdf (2024.03.04.)
[135] Ibid.
[136] https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime (2024.03.04.)

- az interneten megvalósuló feketepiac felszámolása,
- együttműködés az információbiztonság terén,
- képzések fejlesztése,
- nemzetközi jó gyakorlat népszerűsítése.[137]

5.1.5. Az Európai Kiberbiztonsági Kompetenciahálózat és Központ (ECCC)

Az Európai Kiberbiztonsági Kompetenciahálózat és Központ (European Cybersecurity Network and Cybersecurity Competence Centre, röviden ECCC) megalapítására az Európai Parlament és a Tanács (EU) 2021/887 rendeletével[138] került sor. A bukaresti székhelyű kompetenciaközpont létrehozásának célja, hogy az Európai Unió fő eszköze legyen arra, hogy összefogja a kiberbiztonsággal összefüggő K+F beruházásokat, valamint a hálózattal együttműködve végrehajtsa a releváns projekteket és iniciatívákat.[139] Szervezeti felépítését tekintve a kompetenciaközpont három egységre osztható: az igazgatótanácsra, az ügyvezető igazgatóra és a stratégiai tanácsadó csoportra. Az igazgatótanács kiberbiztonsági ismeretekkel rendelkező tagállami vezető képviselőkből és a Bizottság két képviselőjéből áll, feladata a stratégiai irányítás biztosítása és a központ tevékenysége feletti felügyelet ellátása. Az ügyvezető igazgató a központ jogi képviselője, felelőssége a napi ügyvezetésre terjed ki. A stratégiai tanácsadó csoport az igazgatótanács által kinevezett 20 tagból áll, feladata a hálózat és a központ közötti párbeszéd biztosítása.[140]

A központ feladatköre meglehetősen sokrétű, ezek részben stratégiai, részben pedig végrehajtási jellegűek. A stratégiai feladatok közé tartozik a kiberbiztonsági program kidolgozása és a végrehajtásának nyomon követése, szinergiák létesítése a Horizont Európa és a Digitális Európa program kiberbiztonsági és egyéb részei között. Emellett más uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel is együttműködik, biztosítja az információcserét a hálózaton keresztül, tagállami kérésre szakmai tanácsadást nyújt. A végrehajtási jellegű feladatai körében – többek között – koordinálja és igazgatja a hálózat és a közösség munkáját, elkészíti éves munkaprogramját a kiberbiztonsági programmal és a

[137] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf (2024.02.24.)
[138] Az Európai Parlament és a Tanács (EU) 2021/887 rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról (a továbbiakban: ECCC-rendelet).
[139] ECCC-rendelet (14) bekezdése
[140] https://eur-lex.europa.eu/HU/legal-content/summary/european-cybersecurity-network-and-competence-centre.html (2024.03.05.)

többéves munkaprogrammal összhangban, szakmai tanácsadást nyújt kiberbiztonsági ipari, technológiai és kutatási kérdésekben a Bizottság részére.[141]

5.2. Az európai elfogatóparancs jelentősége

Ahogyan az már korábban rögzítésre került, a kiberbűncselekmények egyik legfontosabb ismérve, hogy általában határokon átívelő, több joghatóságot is érintő bűncselekményekről beszélhetünk. Az ilyen büntetőeljárások során nagy segítséget jelenthet az európai elfogatóparancs intézménye. Az európai elfogatóparancs elsődleges célja a büntetőeljárás lefolytatása, ezen kívül a szabadságelvonással járó intézkedés és a szabadságvesztés-büntetés végrehajtása végett a keresett személy elfogása és átadása.[142] Hazánkban a 2012. évi CLXXX. törvény (az Európai Unió tagállamaival folytatott bűnügyi együttműködésről) rögzíti a hatályos szabályozást.

Az európai elfogatóparancs alkalmazási köre a minimum tizenkét hónap szabadságvesztéssel fenyegetett bűncselekményekre, illetve a legalább négy hónap szabadságelvonással járó büntetésekre terjed ki. A kettős inkriminációtól csak a katalogizált bűncselekmények esetében tekint el az elfogatóparancs, melyek esetén is kizárólag akkor, ha a kibocsátó állam joga szerinti büntetési tétel felső határa eléri legalább a három évi szabadságvesztést.[143] Katalogizált bűncselekmények csoportjai a teljesség igénye nélkül: bűnszervezetben való részvétel, terrorizmus, emberkereskedelem, gyermekek szexuális kizsákmányolása és a gyermekpornográfia, fegyverek, lőszerek és robbanóanyagok tiltott kereskedelme, kábítószerek és pszichotróp anyagok tiltott kereskedelme, korrupció, pénzmosás, pénzhamisítás, szándékos emberölés, illetve a számítógépes bűnözés, azzal, hogy a bűncselekmények körét a Tanács[144] bővítheti.[145] A fentebb felsoroltak között az értekezés témaköre szempontjából látható, hogy több releváns bűncselekménytípus is kiemelésre került.

Az átadással kapcsolatban az európai elfogatóparancs szabályai alóli kivételt jelentenek bizonyos okok, amelyek alapján a Fővárosi Törvényszék az átadást megtagadja (kötelező okok esetén), illetve megtagadhatja (fakultatív okok esetén).

A kötelező megtagadási okok a 2012. évi CLXXX. törvény 3. alfejezetében kerültek rögzítésre, melyek a következők:

---

[141] ECCC-rendelet 5. cikkének (1)-(3) bekezdései

[142] Bárd Petra: Az európai elfogatóparancs Magyarországon. Országos Kriminológiai Intézet, Budapest, 2015. p. 26.

[143] Az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény 3.§ (3)

[144] Európai Unió Tanácsa

[145] Bárd, 2015, Op.Cit. pp. 25-27.

„a) a keresett személy gyermekkor miatt büntetőjogilag nem vonható felelősségre,

b) a kibocsátó állam joga szerint a büntetési tétel felső határa a 3 év szabadságvesztést nem éri el és magyar törvény szerint nem számít bűncselekménynek,

c) a magyar törvény szerint a büntethetőség vagy a büntetés elévült, feltéve, hogy az európai elfogatóparancs alapjául szolgáló bűncselekmény magyar joghatóság alá tartozik,

d) egy tagállamban a keresett személy ellen az európai elfogatóparancs kibocsátásának alapjául szolgáló cselekmény miatt már olyan határozatot hoztak, amely a büntetőeljárás megindításának akadályát képezi, vagy amely alapján a büntetést már végrehajtották, annak végrehajtása folyamatban van, vagy a jogerős ítéletet hozó tagállam joga szerint az nem hajtható végre,

e) a keresett személyt egy harmadik államban ugyanazon cselekmény miatt jogerősen felmentették vagy jogerősen elítélték, feltéve, hogy a büntetést már végrehajtották, annak végrehajtása folyamatban van, vagy a jogerős ítéletet hozó állam joga szerint az nem hajtható végre,

f) az európai elfogatóparancs kibocsátásának alapjául szolgáló cselekmény miatt a keresett személy ellen Magyarország területén büntetőeljárás van folyamatban,

g) a magyar igazságügyi hatóság (bíróság, ügyész) vagy nyomozó hatóság az európai elfogatóparancs alapjául szolgáló bűncselekmény miatt a feljelentést elutasította, vagy a nyomozást, illetve az eljárást megszüntette,

h) az európai elfogatóparancs alapjául szolgáló bűncselekmény magyar joghatóság alá tartozik, és a bűncselekményre a magyar törvény szerint közkegyelem terjed ki.”[146]

Meg kell tagadni továbbá az átadást, amennyiben azt olyan határozat végrehajtása céljából bocsátották ki, amelyet a keresett személy távollétében hoztak, kivéve, ha:

- a keresett személy megfelelően lett értesítve,
- meghatalmazott vagy kirendelt védő a keresett személy érdekében a tárgyaláson eljárt,
- a határozat kézbesítése megtörtént, a jogorvoslati lehetőségekről megfelelő tájékoztatást kapott, de azzal nem élt vagy a határozatot nem kézbesítették a keresett személynek, de az átadását követően haladéktalanul kézbesítik számára, tájékoztatják a rendes, illetve a rendkívüli jogorvoslati lehetőségekről, és az erre rendelkezésre álló határidőről.[147]

Ezen felül ugyancsak meg kell tagadni az átadást, ha az európai elfogatóparancsot szabadságvesztés büntetés vagy szabadságelvonással járó intézkedés végrehajtása céljából bocsátották ki, és a keresett személy olyan magyar állampolgár, aki Magyarország területén

[146] 2012. évi CLXXX. törvény 5.§
[147] 2012. évi CLXXX. törvény 6.§

lakóhellyel rendelkezik, ebben az esetben az igazságügyminiszter kezdeményezi a tagállamnál az elítélt szabadságvesztés büntetése vagy szabadságelvonással járó intézkedése végrehajtásának átvételét.[148]

A hivatkozott törvény ugyanezen alfejezetben foglalja össze a fakultatív megtagadási okokat is, amelyek fennállása esetén a Fővárosi Törvényszék hatáskörébe utalja a döntást az európai elfogatóparancs végrehajtásáról, illetve annak megtagadásáról:

- ha az elfogatóparancs olyan bűncselekményre vonatkozik, amelyet egészben vagy részben Magyarország területén követtek el,[149] vagy
- ha ugyanazon személy ellen két vagy több tagállam bocsátott ki európai elfogatóparancsot, a Fővárosi Törvényszék az összes körülmény mérlegelésével dönt arról, hogy melyik európai elfogatóparancs alapján kerüljön a keresett személy először átadásra.[150]

Amennyiben egyáltalán nem állnak fent megtagadási okok, abban az esetben kérvényezhető az európai elfogatóparancs. Ebben az esetben a kérvénynek tartalmaznia kell a következőket:

- az alanyául szolgáló személy személyes adatait és nemzetiségét,
- a kérvényező hatóság nevét, címét, telefonszámát, e-mail címét,
- elfogatóparancsot, az érvényesíteni kívánt eljárás bizonyítékait vagy bármi más bírósági döntést, melyet érvényre kívánnak juttatni,
- az elkövetett cselekmény természetét, illetve jogi megítélését,
- az elkövetés körülményeinek leírását, beleértve az időt, helyet, illetve a bűnösség fokát, és
- a kiszabott büntetést, amennyiben már van jogerős döntés az ügyben, illetve amennyiben nincs, úgy a tagállamban kiszabható büntetési tételt.[151]

Számos ok alapján felmerülhet az európai elfogatóparancs igénylésének a lehetősége, különösen egy bűncselekmény nyomozásának okán, egy jogerős ítélet végrehajtása végett, illetve előzetes őrizetbe vétel céljából, lehetőséget biztosítva egy sokkal hatékonyabb küzdelemre a nemzetközi bűncselekmények és a bűnözés más formái ellen.[152]

[148] 2012. évi CLXXX. törvény 8.§ (1) bekezdése
[149] 2012. évi CLXXX. törvény 7.§
[150] 2012. évi CLXXX. törvény 9.§ (1) bekezdése
[151] Nikač, Op.Cit. p. 96.
[152] Tóth Dávid; Gáspár Zsolt: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. In: Büntetőjogi Szemle Vol. 9, No. 2, 2020. pp. 140-150.

6. A kiberbűnözés elleni fellépés intézményi rendszere hazánkban

6.1. Az ügyészség szerepe a kiberbűnözés elleni harcban

6.1.1. Általános áttekintés – az ügyészség felkészültsége a kiberbűnözésre

Az ügyészi szervezetnek a kiberbűnözés kapcsán betöltött kardinális szerepe vitathatatlan. Köztudomású tény, hogy az ügyész a bűnügy „ura", mely viszonylag nagy mozgástérrel és döntésekkel jár együtt. Ebből következik, hogy az adott büntetőügy nyomozásának iránya többféle irányba tud elmenni, attól függően, hogy a nyomozás felügyeletét végző ügyész milyen nyomozati cselekmények elvégzését tartja indokoltnak, mikor és milyen összefüggéseket, ellentmondásokat fedez fel.

A kiberbűncselekmények rendkívül speciális, több komponensű háttértudást igényelnek. Egyrészről magától értetődően szükséges a megfelelő irányú jogi szaktudás, melynek során az eljáró ügyésznek részletekbe nyúlóan ismernie kell a rendelkezésére álló lehetőségeket. Ezek között nem kifejezetten csak a Btk. és a Be. vonatkozó rendelkezéseit kell érteni. Álláspontom szerint szükséges kellően ismerni a társszervek munkáit is, az európai jogsegélykérelmek rendszerét, az egyes (akár kriptovaluta-)szolgáltatók megkeresésére vonatkozó szabályokat, lehetőségeket, illetőleg az Europol és más szervek által közzétett használható szakanyagokat is. Megjegyzendő, hogy az effektív és gyors munkavégzés, mely az ilyen típusú ügyeknél kardinális jelentőséggel bír, feltételezi az erős idegennyelv-tudást is, leginkább angol, de sok esetben akár francia, spanyol, német, orosz nyelvek tekintetében. Ennek jelentősége abban áll, hogy a hivatalos fordítások rengeteg időt vesznek igénybe, mely az adott ügy szempontjából szintén az elkövetőknek kedvez. A speciális szakmai tudás mellett másrészről egy sokkal több problémát jelentő szaktudással is rendelkezni szükséges az ilyen ügyek megoldásához. Ez a terület az informatika. A modern technológia nyújtotta lehetőségek kiaknázásával az elkövetők akár VPN, akár proxy-szerverek segítségét vehetik igénybe, melyet ötvözhetnek akár több zombigép felhasználásával is, ezzel pedig számos joghatóságon átívelő feladatot tudnak okozni. Emellett a kriptovaluták is bonyolító tényezőként jelennek meg a kiberbűnözésben. Az ilyen és hasonló technológiai újításoknak az informatikai hátterét (legalább a minimum szinten) a kollégáknak meg kell ismerniük ahhoz, hogy hatékonyan tudjanak részt venni a nyomozás felügyeletében, illetőleg fellépni a vádképviselet során.

A fenti hiányosságok kiküszöbölése végett alakult meg 2015 decemberében a Számítógépes Bűnözéssel Foglalkozó Ügyészi Hálózat, melynek célja, hogy az ügyészek – informatikusok

bevonásával, képzéseken történő részvételekkel és egy közös adatbázis létrehozásával – megfelelő informatikai támogatást kapjanak a munkájukhoz. A hálózatban helyet kap valamennyi főügyészség egy-egy informatikusa, egy-egy ügyész a vármegyei főügyészségekről és a Fővárosi Főügyészségről, egy ügyész tagot delegál továbbá a Legfőbb Ügyészség Terrorizmus, Pénzmosás és Katonai Ügyek Főosztálya, a Legfőbb Ügyészség Büntetőbírósági Ügyek Főosztálya, a Legfőbb Ügyészség Gyermek- és Fiatalkorúak Bűnügyeinek Önálló Osztálya, valamint a Legfőbb Ügyészség Kiemelt, Korrupciós és Szervezett Bűnözés Elleni Ügyek Főosztálya.[153]

6.1.2. Nemzetközi együttműködések rendszere

A magyar ügyészi szervezet kiterjedt kooperációs rendszerrel rendelkezik, mely megnyilvánul mind a nemzetközi szervezetek és európai uniós intézmények rendszerében történő részvételben, mind a bi- és multilaterális egyezmények és munkakapcsolatok megerősítését célzó diplomáciai és szakmai fórumokban. Az alábbi kooperatív törekvések szinte mindegyike érinti a kiberbűnözés területét, ezért nagyban hozzájárulnak az ilyen bűncselekmények nyomozásához.

6.1.2.1. Együttműködés az Európai Ügyészséggel

Az Európai Ügyészség (European Public Prosecutor's Office vagy röviden EPPO) gondolata már viszonylag régen megfogalmazódott. Az 1990-es és 2000-es évek alatt lassan kikristályosodott és javaslat formát öltött az elképzelése egy európai szintű ügyészi szervezet létrehozásának. A Lisszaboni Szerződés végül megteremtette a kezdeményezés jogi alapját.[154] E hosszú folyamat végül 2017-ben vezetett eredményre, amikor a Tanács elfogadta az Európai Ügyészség létrehozására irányuló rendeletet.[155] A szervezet élére 2019-ben nevezték ki Laura Codruța Kövesi európai főügyészt, aki korábban Románia legfőbb ügyészi, majd a román Országos Korrupcióellenes Ügyészség (Direcția Națională Anticorupție, röviden DNA) vezető ügyészi tisztségét töltötte be. A szervezet a tényleges működését 2021. június 1. napján kezdte meg.

---

[153] Kökényesi-Bartos Attila: A Számítógépes Bűnözéssel Foglalkozó Ügyészi Hálózat. In: Bencsik Balázs; Sabjanics István: Digitális környezetünk fenyegetettsége a mindennapokban. Budapest, Dialóg Campus Kiadó, 2018. pp. 105-106.

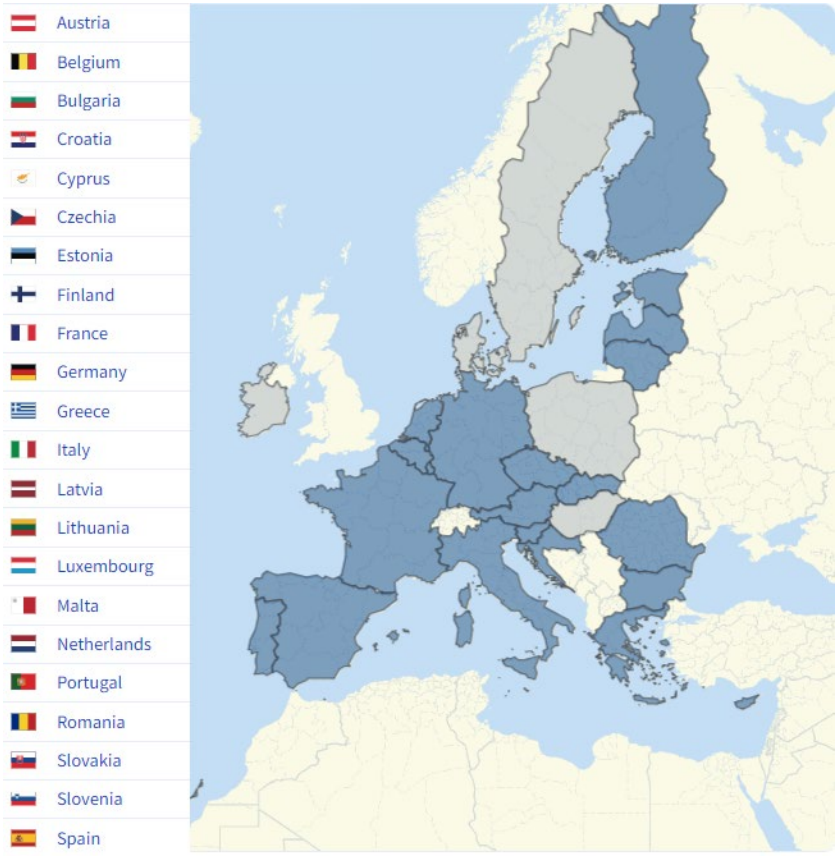
[154] https://www.eppo.europa.eu/en/background (2024.02.19.)

[155] A Tanács (EU) 2017/1939 rendelete az Európai Ügyészség létrehozására vonatkozó megerősített együttműködés bevezetéséről

Az EPPO-hoz 2024-ig összesen 22 uniós tagállam csatlakozott. Magyarország nem tagja ugyan az Európai Ügyészségnek, azonban szorosan együttműködik vele. Az együttműködés alapját a 2021. március 26. napján, Luxemburgban kelt munkamegállapodás[156] képezi, melyben kiemelt célként szerepel a stratégiai és információcsere, valamint az operatív és intézményi együttműködés.[157] Az együttműködés egyes személyi – kvázi diplomáciai – jellegű rendelkezéseket tartalmaz, melyek egyike, hogy a felek az EPPO-val történő kapcsolattartásra a Legfőbb Ügyészség Kiemelt, Korrupciós és Szervezett Bűnözés Elleni Ügyek Főosztályának vezetőjét jelölték ki.[158] A másik oldalról pedig – az 5. cikk alapján – a Legfőbb Ügyészség az EPPO székhelyére delegálhat egy fő összekötő munkatársat.

Az Európai Ügyészség feladatköre az Európai Unió pénzügyi érdekeit sértő bűncselekményekkel kapcsolatos nyomozásokra és az ilyen ügyekben történő vádképviseletre terjed ki. E bűncselekmények közé tartoznak különösen a csalások, a korrupciós bűncselekmények, a pénzmosás, illetőleg a határokon átívelő héacsalások.[159] Ezen bűncselekmények kivétel nélkül megjelenhetnek a kibertérben (különösen a pénzmosás és a csalások), így álláspontom szerint az EPPO-val történő szoros együttműködés a kiberbűnözés terén is pozitívumként értékelendő.

[156] Magyarország Legfőbb Ügyészsége és az Európai Ügyészség (EPPO) közötti együttműködésről szóló munkamegállapodás
[157] Munkamegállapodás 1. cikke
[158] Munkamegállapodás 4. cikke
[159] https://www.consilium.europa.eu/hu/policies/eppo/#eppo (2024.02.20.)



3. ábra: Az Európai Ügyészség tagállamai 2024-ben. Forrás: https://www.eppo.europa.eu/en/members (2024.02.19.)

6.1.2.2. A Visegrádi Csoport legfőbb ügyészeinek találkozói

A Visegrádi Csoport (V4) tagállamainak legfőbb ügyészeinek találkozóinak többször is képezte már tárgyát a kiberbűnözés elleni fellépés megerősítése a régió államaiban. A 2018. szeptember 3-5. között Visegrádon megrendezésre kerülő legfőbb ügyészi találkozón Pavel Zeman cseh legfőbb ügyész, Jaromir Ciznár szlovák legfőbb ügyész és Polt Péter magyar legfőbb ügyész, továbbá Bogdan Swieczkowski lengyel legfőbb ügyész helyettes vettek részt, illetőleg jelen volt Ladislav Hamran, az Eurojust elnöke is.[160] A tanácskozás eredményeként a felek egy közös szándéknyilatkozatot fogadtak el arra vonatkozóan, hogy kiemelt, fokozott és közös figyelmet szentelnek az információs rendszerek elleni támadásokkal szembeni védekezésnek. Emellett elköteleződést jelentett az egyezmény a szellemi tulajdon elleni internetes bűnözés és az internetes gyermekpornográfia visszaszorítására. Bogdan Święczkowski lengyel legfőbb

[160] https://www.jogiforum.hu/hir/2018/09/06/egyuttmukodo-ugyeszek-europaert-a-visegradi-csoport-legfobb-ugyeszei-alairtak-a-visegradi-nyilatkozatot/ (2023.12.03.)

ügyész helyettes kiemelte, hogy a lengyel ügyészségi szervezeten belül külön osztályok foglalkoznak a korrupciós és kiberbűnözéssel.[161]

A modern magyar ügyészség 150 éves évfordulójának apropóján 2021-ben Budapestre érkezett Franz Plöchl osztrák legfőbb ügyész, Maroš Žilinka szlovák legfőbb ügyész, Bogdan Święczkowski lengyel legfőbb ügyész helyettes, Pavel Zeman cseh legfőbb ügyész, valamint Ladislav Hamran, az Eurojust elnöke egy nemzetközi konferencia erejéig, melynek kiemelt témája a kiberbűnözésnek a pandémia idején leginkább jellemzővé vált formái (gyermekpornográfia, online csalások, kritikus infrastruktúrák elleni támadások) elleni védekezés volt.[162] A konferencia eredményeként újabb szándéknyilatkozat született az előbbi bűncselekménytípusok elleni küzdelem elleni nemzetközi együttműködés megerősítésének céljából.[163]

A legfőbb ügyészségi delegációk 2023. május 23-24. között Csehországban, Brno-ban tartották meg a találkozót, melyen Maroš Žilinka szlovák legfőbb ügyész, Igor Stříž cseh legfőbb ügyész, Dariusz Barski lengyel főállamügyész, továbbá Polt Péter magyar legfőbb ügyész vettek részt. E megbeszélés témáját – többek között – újfent a kiberbűnözés elleni küzdelem aktuális kihívásai adták. A felek ezúttal is szándéknyilatkozatot fogadtak el arra vonatkozóan, melyben kiemelték, hogy törekedni fognak a megfelelő jogi és technikai intézkedések nyújtására a kiberbűnözés elleni küzdelemben, illetőleg hangsúlyozták az ilyen ügyekben folytatott nemzetközi igazságügyi együttműködés szerepét, melynek továbbfejlesztésének szükségességét szorgalmazták.[164]

6.1.2.3. Egyéb nemzetközi és európai uniós hálózati tagságok

A magyar ügyészi szervezet a korábban említett és kifejtett európai uniós és nemzetközi csoportosulásokon kívül az alábbi fórumok és hálózatok tagja:

- Európai Ügyészek Konzultatív Tanácsa (Consultative Council of European Prosecutors, röviden CCPE),

[161] Lajtár István: A kiberbűnözésről. In: Ügyészek Lapja Vol. 26, No. 1, 2019. pp. 47-52.
[162] https://ugyeszseg.hu/nemzetkozi-konferencia-az-ugyeszseg-150-eves-evfordulojan-a-visegradi-negyek-es-ausztria-legfobb-ugyeszei-valamint-az-eurojust-elnoke-reszvetelevel/ (2023.12.03.)
[163] https://ugyeszseg.hu/szandeknyilatkozat-a-visegradi-negyek-es-ausztria-legfobb-ugyeszei-kozott/ (2023.12.03.)
[164] https://ugyeszseg.hu/kozos-nyilatkozatot-fogadtak-el-a-visegradi-negyek-legfobb-ugyeszei-fotoval-a-legfobb-ugyeszseg-sajtokozlemenye/ (2023.12.03.)

- Az Európa Tanács Igazságszolgáltatás Hatékonyságáért Küzdő Európai Bizottsága (Council of Europe European Commission for the Efficiency of Justice, röviden CEPEJ),
- Pénzmosás és a Terrorizmus Finanszírozása Elleni Intézkedéseket Vizsgáló Szakértői Csoport (Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, röviden MONEYVAL),
- Korrupció Elleni Államok Csoportja (Group of States against Corruption, röviden GRECO).[165]

6.2. A küzdelem frontvonala, a nyomozó hatóságok

6.2.1. A képzési rendszer kapcsán felmerült kritikák

A rendőrség állományának informatikai tudásával kapcsolatban meglehetősen kevés releváns információval rendelkezünk, ugyanakkor a gyakorlati tapasztalatok az elmúlt évekből arra engednek következtetni, hogy országos szinten igencsak nagy volt a differencia két vármegye (vagy pontosabban inkább két rendőrkapitányság) tudása, felkészültsége és gyakorlata között. Simon Béla 2018-as kutatása arra engedett következtetni, hogy a rendőrség aktív állományában szolgálatot teljesítő személyek általánosságban nem a belső, rendőrségi képzési rendszerből szerezték meg a kiberbűncselekmények elleni fellépéshez szükséges (informatikai) ismereteket, háttértudást. Emellett kiemelte továbbá, hogy hazánkban nem voltak kellően fejlettek a kiberbűnözés elleni fellépést segítő továbbképzési lehetőségek. Úgy vélte, hogy a Belügyminisztérium által szervezett képzések csak egy bizonyos szűk réteg részére nyújtanak ismereteket, továbbá problémaként vetette fel, hogy jellemzően ad hoc jellegű, nem pedig rendszeres és tervezett képzéseket szerveztek.[166]

6.2.2. A Mátrix Projekt, a rendőrség kiberbűnözésre szakosodott egysége

Simon rögzítette, hogy országos szinten még nem alakult ki olyan rendszer, amelyben valamennyi kapitányságon vagy kirendeltségen dolgozó rendőrök a hatáskörükbe tartozó bűncselekmények vonatkozásában szakképzett segítséget kaphatnának a digitális bizonyítékok

[165] https://ugyeszseg.hu/az-ugyeszsegrol/nemzetkozi-kapcsolatok/magas-szintu-nemzetkozi-kapcsolatok/ (2024.02.19.)
[166] Simon Béla: A rendőrség állományának felkészültsége a kiberbűnözésre. In: Hadtudományi Szemle Vol. 11, No. 1, 2018. p. 389.

rögzítéséhez, analíziséhez, illetőleg a nyomozások lefolytatásához szükséges háttértudást a rendelkezésükre bocsátanák, azonban már tervben voltak egy ilyen hálózat megvalósítása az ORFK részéről.[167] A 2023-as év során ugyanakkor az elképzelés megvalósult a *Mátrix Projekt* névre keresztelt új, önálló rendőrségi szervezeti egység keretein belül. Az egység közel 300 magasan képzett, megfelelő tudással rendelkező munkatárs bevonásával alakult meg, akik a vármegyei rendőrkapitányságok, a Budapesti Rendőr-főkapitányság és a Készenléti Rendőrség Nemzeti Nyomozó Iroda munkáját segítik. Az egység munkáját az ORFK szintén újonnan megalakult Kiberstratégiai Osztálya koordinálja. Ezen osztály felel továbbá a rendőri szervezetrendszer kibervédelmi tevékenységének összehangolásáért és a nemzetközi kapcsolattartásért egyaránt.[168]

6.2.3. Bűnüldözési szemléletváltás

Egy másik tanulmányában Simon kiemeli, hogy a magyar rendészeti szervek egy másik nagy problémája a tettes alapú bűnüldözési szemlélet. Ennek keretében kifejti, hogy egy-egy bűnügy során, amennyiben a vagyonbiztosítás, vagyonvisszaszerzés nem lehetséges (például azért, mert a gyanúsítottnak nincsen végrehajtás alá vonható vagyona), akkor álláspontja szerint az összes további nyomozati cselekmény improduktív, ami más ügyek nyomozásától vonja el a nyomozó hatóság erőforrásait.[169] Véleményem szerint egyrészről igazként kell elfogadni az a tényt, miszerint a nyomozó hatóságok bűnüldözési szemléletét modernizálni szükséges. Nem feltétlenül kielégítő, ha a bűnügy pusztán az elkövető kiléte körül forog, más faktorokat is figyelembe szükséges venni (mint például a sértetti reparáció vagy bűncselekménnyel okozott kár megtérülése, a kár minimalizálása). Könnyelmű kijelentésnek tűnik azonban az a megállapítás, mely szerint minden további nyomozati cselekmény improduktív lenne, ha egy bűnügyben a nyomozó hatóság olyan helyzettel találkozik, hogy a gyanúsítottnak nincsen végrehajtható vagyona. Igaz, hogy az adott ügyben érdemben a sértett helyzetét nem feltétlenül mozdítja elő, ha további kihallgatásokat, szakértői kirendeléseket és egyéb nyomozati cselekményeket végeznek a rendészeti szervek, ugyanakkor egy eljárásnak annak integritásában történő továbbvitele, majd befejezése kriminológiai szempontból jelentőséggel bírhat. További információkkal szolgálhat például a metodikát vagy a viktimizációt illetően,

[167] Simon, 2018: A rendőrség állományának felkészültsége a kiberbűnözésre, Op.Cit. p. 394.
[168] Trencsényi Zoltán: Mátrix Projekt a kiberbiztonságért.
https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/matrix-projekt-a-kiberbiztonsagert (2024.01.30.)
[169] Simon Béla: A bűnüldözés előtt álló digitális kihívások. In: Magyar Rendészet Vol. 17, No. 5, 2017. p. 98.

melyek a generális prevenció szempontjából lehetnek relevánsak. Statisztikai szempontból is sokkal tisztább képet kapunk így, mintha „félbehagynánk” az adott eljárást. Végső soron nem kizárható az sem, hogy a gyanúsított vagy más, az eljárásban résztvevő személy olyan információval szolgál, mely alapján mégis végrehajtás alá vonható vagyon vagy arra utaló tény birtokába juthat a nyomozó hatóság.

Általánosságban megállapítható, hogy a rendőrségi szervezetben az elmúlt évek során kifejezetten előremutató szemléletváltás történt, melynek a fentiekben említett Mátrix Projekt is egy eredménye. Önmagában az a tény, miszerint a nyomozó hatóság felismerte szakmai hiányosságait az adott szakterületen és ennek kiküszöbölésére ilyen méretű – főként a személyi állományt illető – változtatások mellett döntött, értékelendő novum. Mindazonáltal nincs vége a feladatnak, hiszen a kiberbűnözés frontvonalában küzdő rendészeti alkalmazottaknak folyamatosan naprakésznek kell lenniük az új bűnözési trendekkel, elkövetési módokkal, továbbá az új állományt „meg is kell tartani”, tehát célul kell tűzni, hogy az ilyen jellegű pozíciók (kifejezetten, de nem kizárólag az informatikus végzettséghez kötöttek) vonzóak legyenek a fiatalok számára. E terület jellemzője ugyanis, hogy rengeteg munkalehetőség van a piacon, egyre jobban és jobban fizető, nagyfokú rugalmasságot nyújtó állásokról van szó, melyek mellett a rendészeti szférának is versenyképesnek kell lennie. Ahogyan Simon is kiemeli, a rendőrségen kívül a többi rendészeti szerv (és nemzetbiztonsági szerv – *a szerző*) is azzal a problémával küzd, hogy a szakemberek sok esetben csak a gyakorlatuk megszerzésének helyéül választják ezeket a szervezeteket, így azt annak megszerzése után nagy arányban is hagyják el.[170] Ennek okai álláspontom szerint a fentebb kifejtett, a magánszektorban tapasztalható, álláskínálatok jelentősen megnövekedett száma és a fizetések emelkedése.

6.2.4. Etikus hackerek a rendészeti és nemzetbiztonsági szervek alkalmazásában

Simon tanulmányában rögzítette, miszerint a rendészeti informatikai állomány számára jelentős igény merült fel az informatikai rendszerüzemeltető képzésre és az etikus hacker képzésekre.[171] Az *etikus hackerek* kiberbiztonsági ismeretekkel ötvözött kreatív gondolkodásmóddal tesztelik az egyes szervezetek informatikai rendszereinek és alkalmazásainak sérülékenységét. Ennek keretében a rosszindulatú hackelési stratégiákat reprodukálják és megkísérlik a rendszerbe történő behatolást.[172] A metodológiáját tekintve az etikus hackelés öt főbb fázisra bontható le:

[170] Simon Béla: Kiberbűnözés elleni képzésfejlesztés. In: Magyar Rendészet Vol. 18, No. 3, 2018. p. 203.
[171] Simon, 2018: Kiberbűnözés elleni képzésfejlesztés. Op.Cit. p. 202.
[172] https://www.purdue.edu/science/careers/what_can_i_do_with_a_major/Career%20Pages/ethical_hacker.html (2024.03.05.)

- *felderítés:* az etikus hacker információt gyűjt a célrendszerről, melynek során megkísérli azonosítani a lehetséges sebezhetőségeket,
- *szkennelés / keresés:* különféle eszközök használata abból a célból, hogy az adott célrendszer vagy hálózat gyenge pontjait azonosítsa,
- *hozzáférés megszerzése:* sikeres azonosítás esetén a sérülékenységet a hacker megkísérli kihasználni, hogy hozzáférést nyerhessen a rendszerhez,
- *hozzáférés fenntartása:* a hozzáférés megszerzését követően a hacker fenntartja azt, hogy felmérhesse a lehetséges kár mértékét, melyet az adott sérülékenység lehetővé tesz,
- *nyomok elfedése:* az utolsó fázis során a hacker eltakarítja a nyomait, hogy a rendszergazdák ne (vagy csak megkésve) észleljék a jelenlétét.[173]

Rendészeti alkalmazásukkal kapcsolatban érdemes kiemelni, hogy Nagy Zoltán 2001-ben – magát naivnak bélyegezve ugyan, de már – eljátszott a gondolattal, hogy az ún. „jó hackerek" akár a társadalom javára is végezhetnének munkát honorárium ellenében.[174] E gondolat az elmúlt húsz év során másokban is felmerült, ugyanakkor nem egyszerű kérdés annak meghatározása, hogy a két járható út közül melyik a célravezetőbb:

- a saját állomány bizonyos tagjainak (tovább)képzése, illetőleg az etikus hacker képzésen történő részvételi lehetőség biztosítása számukra, vagy
- már etikus hacker végzettséggel (vagy pusztán adekvát szaktudással és gyakorlattal) rendelkező külső, civilek állományba vétele, alkalmazása.

Mindkét típusú toborzásnak meg vannak az előnyei és hátrányai egyaránt, melyeket az adott szervezet vezetőinek kell mérlegelnie. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete például a második lehetőség szerint járt el, melynek során a saját internetes felületén, nyíltan[175] hirdet állásokat „Sérülékenységvizsgálati szakértő / Ethical Hacker" pozíciókra. Ennek keretében olyan legalább középfokú végzettséggel rendelkező, az IT-ban jártas szakembereket keresnek, akik állami-, önkormányzati és nemzetbiztonsági védelem alá eső rendszerek sérülékenységvizsgálatát végeznék, majd a feltárt sérülékenységeket dokumentálják.[176] Az előbbi nem egyedi eset, 2022-ben a Nemzeti Adó- és Vámhivatal is hirdetett kifejezetten „Etikus hacker" állásajánlatot. A sikeres pályázók feladata

[173] https://www.itgovernance.co.uk/ethical-hacking (2024.03.05.)
[174] Nagy Zoltán: Informatikai bűncselekmények. In: Magyar Tudomány Vol. 48 (108), No. 8, 2001. p. 951.
[175] Nagy Zoltán 2009-ben megjelent monográfiájában szintén felveti az ún. „jó hackerek" alkalmazását, mint a kibertérben zajló terrorizmus elleni lehetséges fegyver használatát, ugyanakkor – nyilvánvaló tényként – hozzáteszi, hogy ez nem lesz publikus. Lásd: Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Budapest, Ad Librum, 2009. p. 228.
[176] https://nki.gov.hu/intezet/tartalom/karrier-lehetosegek/#whitehat (2023.12.23.)

– a felhívás szerint – a NAV elektronikus információs rendszereinek rendszeres IT biztonsági tesztelése, a sérülékenységek és más hibák feltárása, a kiberbiztonsági incidensek feltárása és vizsgálata volt.[177]

6.3. Egyéb (társ)szervek, intézményi lehetőségek a kiberbűnözéssel szembeni fellépésre

6.3.1. A Pénzügyi Információs Egység (FIU)

Hazánkban a Pénzügyi Információs Egység (Financial Intelligence Unit vagy röviden FIU) a 2003-as Pmt.[178] hatálya alatt az Országos Rendőr-főkapitánysághoz tartozott, majd a 2007-es Pmt.[179] e feladatokat a Vám- és Pénzügyőrség hatáskörébe utalta. A pénzügyi információs egység feladatainak ellátásáért 2012 óta a Nemzeti Adó- és Vámhivatal (NAV) Pénzmosás és Terrorizmusfinanszírozás Elleni Irodája felelős. E feladatkörében fogadja a szolgáltatók által küldött bejelentéseket, elemző-értékelő tevékenységet folytat, továbbá kiemelt feladata az információtovábbítás és a más államokban működő szervek közötti nemzetközi információcsere.[180] A szerv a feladatait a NAV szervezetén belül, mégis függetlenül végzi.[181] A pénzügyi információs egység feladata – ahogyan a fentiek alapján következik – inkább a háttérmunkában, információgyűjtésben és információcserében nyilvánul meg, ugyanakkor működése mégis jelentőséggel bír. Amellett, hogy az ügyletek és szolgáltatók monitorozása közben kiszűrhet bizonyos bűncselekményre utaló tranzakciókat, hatáskörrel rendelkezik az egyes ügyek során konkrét ügyleteket, tranzakciókat felfüggeszteni, mely a későbbi (eshetőleges) büntetőeljárás során az eszközök biztosításában is segítséget nyújthat (akár egy későbbi zár alá vételhez, lefoglaláshoz) a nyomozó hatóságok számára.[182]

6.3.2. A Magyar Nemzeti Bank (MNB)

Az MNB pénzügyi felügyeleti szerepének ellátása során ellenőrzi a pénzügyi intézményeknek a pénzmosás és a terrorizmus finanszírozásának megelőzésével és azok megakadályozásával

[177] https://nav.gov.hu/navit/tartalmak/allaspalyazatok/informaciobiztonsag/etikus-hacker-informatikai-biztonsagi-osztaly-20221121 (2024.03.05.)
[178] 2003. évi XV. törvény a pénzmosás megelőzéséről és megakadályozásáról
[179] 2007. évi CXXXVI. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
[180] Simonka Gábor; Tóth András: A magyar FIU tevékenysége és szerepe a pénzmosás elleni küzdelemben. In: Farkas Ákos; Dannecker Gerhard; Jacsó Judit (szerk.): Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre. Budapest, Wolters Kluwer Kft. 2019. pp. 360-361.
[181] Op.Cit. p. 362.
[182] Op.Cit. p. 366.

kapcsolatos tevékenységét, illetőleg informatikai felügyeletet is végez. Amennyiben azonnali intézkedés szükséges, cél- és témavizsgálatokat folytat le.[183] Jegybanki funkciójából következik, hogy az MNB a jogalkotásban is jelentős szerepet tölt be. Ennek során a felügyelete alá tartozó szolgáltatókra nézve kötelező erővel bíró rendeleteket[184], illetőleg ajánlásokat[185] is kibocsát, felügyeleti ügyekben pedig határozatot hoz.

7. A kiberbűnözés különböző irányai az egyes országok gyakorlatában

Jelen fejezet egy nemzetközi jogösszehasonlító kitekintésként kíván szolgálni abból a célból, hogy az egyes államoknak a kiberbűnözés ellen rendelkezésre álló intézményi és jogszabályi kereteinek összevetésével a jó gyakorlat összegyűjthető lehessen. Az országok kiválasztásánál egyrészről szempont volt a nyelvhasználat, ennek okán olyan országok áttekintését tűztem célul, melyek hivatalos nyelve a spanyol. Egy másik lényeges szempont volt a kiválasztásnál, hogy a vizsgálandó országok a Budapesti Egyezmény részes tagállamai legyenek, mely a szabályozás és az intézményi rendszer kapcsán meghatározza azon minimumkövetelményeket, melyekkel a kiberbűnözés elleni harc effektív lehet. A fejezetben szereplő rövid országtanulmányok elemzését a gyakorlati tapasztalatok összegzése és kiértékelése követi.

7.1. Kolumbia

7.1.1. A kiberbűnözés helyzete Kolumbiában

Ricardo Franco Mahecha által 2016-ban készített kutatás szerint Kolumbiában a kibertámadások fajsúlyos része, egészen pontosan 75,29%-a a pénzügyi / bankszektor ellen irányul, ezt követik a kormányellenes támadások 10,56%-al, továbbá a távközlési szolgáltatók elleni támadások 8,41%-al. Ezzel szemben az energiaszektort csak a támadások 3,71%-a, az ipari szférát a támadások 1,98%-a, míg a kereskedelmi szektort csupán a támadások 0,05%-a

[183] https://www.mnb.hu/web/felugyelet (2024.03.05.)
[184] A pénzmosás és a terrorizmus finanszírozásának szempontjából kiemelt jelentőséggel bír a 26/2020. (VIII. 25.) MNB rendelet, mely a Pmt.-re végrehajtása kapcsán fogalmaz meg minimumkövetelményeket. A rendelet meghatározza többek között az auditált elektronikus hírközlő eszköz útján végzett ügyfél-átvilágítás, a kockázatbesorolás szabályait is.
[185] E körben kiemelendő a Magyar Nemzeti Bank 15/2022. (IX.15.) számú ajánlása a pénzmosási és terrorizmus finanszírozási kockázatok értékeléséről és a kapcsolódó intézkedések meghatározásáról. Az ajánlás rögzíti a kockázatértékelés és kezelés elveit, az ügyfélátvilágítással kapcsolatos intézkedésekre vonatkozó elvárásokat, illetőleg ágazatspecifikus iránymutatásokat is tartalmaz (többek között az elektronikuspénz-kibocsátási szolgáltatást nyújtó intézmények részére), illetőleg kiemeli a MICA-rendelettervezetet is.

érinti. A becslések szerint a támadások a 2015-ös évben csak Kolumbiában mintegy 600 millió amerikai dollár kárt okoztak.[186] Az ESET 2015-ben felmérést készített a latin-amerikai országok kibertámadások általi érintettségével kapcsolatban, mely szintén ijesztő számokat mutatott. A kutatási adatok szerint a felmérésben résztvevő kolumbiai vállalkozások több, mint 57%-a észlelt malware fertőzéseket.[187]

7.1.2. Kolumbia kiberbűnözés elleni intézményrendszere

7.1.2.1. ColCERT

Kolumbia számítógépes vészhelyzeti reagálási csoportja, a COLCERT célja a kritikus infrastruktúrák azonosítása, kiberbiztonsági kockázataik kiküszöbölése, a köz- és privátszektor gazdasági szereplőinek megelőző jelleggel történő tájékoztatása az esetleges kiberfenyegetésekről és sérülékenységekről, továbbá tanácsadás a kiberbiztonsági események kezeléséhez, melyek biztosítják a létfontosságú szolgáltatások folyamatosságát a kolumbiai állampolgárok számára.[188]

A ColCERT széles feladatkörrel rendelkezik, ezek a következők:

- együttműködés a digitális biztonságért felelős szervekkel, többek között a CSIRT-ekkel és a köz- és magánszektorral, valamint a Nemzeti Digitális Biztonság fenyegetéseinek és incidenseinek kezelésére szolgáló információ-megosztás,
- egyetlen kapcsolattartó pontként és koordinációs szervként fejti ki tevékenységét, annak érdekében, hogy hatékonyan és gyorsan reagálhasson a Nemzeti Digitális Biztonságot fenyegető vagy veszélyeztető digitális biztonsági eseményekre,
- Kolumbia közigazgatási alkotóegységeit érintő digitális biztonsági incidensekre történő válaszlépések koordinálása az 1998. évi 489. sz. törvény 39. cikkének (és az azt módosító vagy felváltó rendelkezéseknek) megfelelően,
- Kolumbia közigazgatási alkotóegységeit képező entitások támogatása a digitális biztonsági incidensek kezelésének javítása érdekében, valamint a technológiai infrastruktúra biztonsági folyamataiban,

[186] Ricardo Franco Mahecha: Ciberseguros, la mejor forma de transferir riesgos de ataques informáticos. Diplomamunka. Universidad Piloto de Colombia, 2016. p. 3.
[187] Op.Cit. p. 2.
[188] Acerca de colCERT.
Elérhető: https://www.colcert.gov.co/800/w3-article-198657.html (2024.03.13.)

- a helyi és ágazati kapacitások fejlesztésének, valamint az ágazati CSIRT-ek létrehozásának elősegítése a magánszektorban és a civil társadalomban,
- digitális biztonsági protokollok, eljárások, útmutatók és ajánlások kidolgozása, terjesztése, valamint végrehajtásuk nyomon követese,
- a digitális biztonsági kockázatoknak kitett kritikus infrastruktúrák azonosítási tevékenységének koordinálása, megelőzési és védekezési mechanizmusok létrehozása a kapcsolódó funkcionális, szabályozási és felelősségi szabálykeretek betartásával, összhangban a hatályos jogszabályokkal és az egyéni szabadságjogokkal,
- nemzeti és nemzetközi együttműködések megszilárdítása az információmegosztás terén,
- az incidenskezelési rendszer naprakészen tartása (módszerek, ellenőrzések, eljárások, kézikönyvek, útmutatók, digitális nyilvántartások, bizonyítékok) a felelőssége alá tartozó tervezési, végrehajtási, ellenőrzési, mérési, kockázatcsökkentési és fejlesztési szakaszok vonatkozásában,
- az állampolgárok és a szabályozó szervek igényeinek (bejelentéseinek) eredményes figyelembevételéhez szükséges tevékenységek elvégzése, illetőleg a feladatkörébe tartozó dokumentációnak a Minisztérium által meghatározott iránymutatások és eljárások szerinti kezelése,
- információbiztonsági és adatvédelmi irányelvek betartása,
- integrált tervezési és irányítási modell megvalósítása és fenntarthatósága érdekében a belső és külső auditok eredményeiből levont következtetések alkalmazása.[189]

7.1.2.2. A Kolumbiai Informatikai és Telekommunikációs Kamara (CSIRT-CCIT)

A Kolumbiai Informatikai és Telekommunikációs Kamara (Cámara Colombiana de Informática y Telecommunicaciones) egy olyan szakszervezeti egység, mely a távközlési és informatikai szektor legfontosabb kolumbiai vállalatait fogja össze 1993-as megalakulása óta. Célkitűzései közé tartozik, hogy elősegítse és ösztönözze az információs és kommunikációs technológiai szektor rendezett növekedését, illetőleg ellássá a szektor érdekképviseletét.
Feladatköre kiterjed a következőkre:

- a kamarához tartozó vállalkozások érdekeinek biztosítása, védelme, előmozdítása, fejlesztése és népszerűsítése,

[189] Ibid.

- az ágazati, országos és regionális önkormányzatoknak a szektor érdekkörébe tartozó szabályozásainak figyelemmel kísérése,
- tanácsadás és tájékoztatás nyújtása a kamarához tartozó vállalkozások számára,
- kapcsolattartás a szektort érintő ügyekben az illetékes hatóságokkal,
- előmozdítja a szektor fejlődését, jogi stabilitását,
- stratégiai terveket készít, figyelemmel a külső és belső kapcsolatépítés fontosságára,
- egyfajta általános tanácsadó testületként szolgál a kormány számára a szektort érintő jogalkotás során.[190]

7.1.2.3. A Kolumbiai Rendőrség Kiberközpontja (CSIRT PONAL)

A Kolumbiai Rendőrség Kiberközpontja (Centro Cibernético Policial) jelenlegi formájában 2018 óta működik, ugyanakkor annak előzményei egészen 2001-ig nyúlnak vissza, amikor megalakult az ország első informatikai bűncselekményekkel foglalkozó nyomozócsoportja.
A Kiberközpont a Bűnügyi Nyomozó Igazgatóság és az INTERPOL alá tartozik. Az osztály felelőssége a kiberbiztonságra, a kibervédelemre, továbbá az ország kiberterében keringő információ és adatok védelmére vonatkozó stratégiák és projektet kidolgozására terjed ki. Feladatkörében eljárva kivizsgálja és elintézi a „kiberpolgárok" által tett kiberbiztonsági incidenseket, alkalmazva a digitális bizonyítékok feldolgozására és kezelésére vonatkozó protokollokat az illetékes hatóság előtt, továbbá fejleszti az felderítési, a megelőzési, a nyomozási és az elemzési kapacitásokat, illetőleg a konkrét készenléti terveket az informatikai krízishelyzetekkel szemben, valamint elősegíti az igazságszolgáltatást a nemzeti szintű kiberbiztonságot érintő fenyegetések terén. Munkája során együttműködik a Nemzeti Kiberbűnözés Megfigyelőközponttal. Ez az egység elemzéseket folytat a kiberbűncselekmények elkövetési módjaival kapcsolatban, azonosítja az új tendenciákat.[191]

7.1.3. Az ország büntetőjogi szabályanyaga a kiberbűnözés szankcionálására

A vonatkozó kolumbiai jogforrások áttekintését követően megállapítható, hogy a jogrendszer erőteljesen kazuisztikus beállítottságú, kodifikációs törekvések a büntetőjog terén nem

[190] LA CCIT
Elérhető: https://www.ccit.org.co/la-ccit/ (2024.03.13.)
[191] Funciones del CeCiP
Elérhető: https://caivirtual.policia.gov.co/conocenos/funciones (2024.03.13.)

történtek, a jogszabályanyag átláthatatlan, továbbá meglehetősen nehezen felkutatható az interneten. A hatályos kolumbiai büntető törvénykönyv, a 2000. évi 599. törvény (Código Penal de Colombia)[192] az információs rendszerek és adatok védelmében az alábbi rendelkezéseket tartalmazza:

7.1.3.1. Információs rendszer megsértése (Acceso abusivo a un sistema informático)

A tényállást a 269 A. cikk tartalmazza:

„Aki jogosulatlanul vagy a jogosultságának kereteit túllépve részben vagy egészben hozzáfér egy biztonsági intézkedéssel védett vagy nem védett információs rendszerhez, vagy azon belül annak akarata ellenére tartózkodik, akinek törvényes joga van őt a rendszerből kizárni, negyvennyolc (48) hónaptól kilencvenhat (96) hónapig terjedő szabadságvesztésre ítélhető és a mindenkori havi minimálbérrel számolt 100 havi tételtől 1.000 havi tételig terjedő pénzbírsággal sújtható."

A tényállás meglehetősen hasonló a magyar Btk. 423. § (1) bekezdésében szereplő Információs rendszer vagy adat megsértésének alapesetével. A cselekmény elkövetési tárgyát mindkét szabályozás esetében az információs rendszer képezi. E tényállások közötti hasonlóság a Budapesti Egyezmény 2. cikke alatt szabályozott jogosulatlan belépés átültetésével magyarázható. A kettő közötti különbséget alapvetően az információs rendszer védelmét biztosító technikai intézkedéssel lehet megfogni, melynek kijátszása vagy megsértése a hazai szabályozásban szükségszerű tényállási elem, míg a kolumbiai büntető törvénykönyvben csak eshetőleges, mindazonáltal a cselekmény a védelmi intézkedés megsértésének hiányában is büntetendő. Jelentős a különbség a szankció vonatkozásában is, ugyanis a magyar szabályozás három évig terjedő szabadságvesztéssel, míg a kolumbiai két évtől nyolc évig terjedő szabadságvesztéssel, valamint viszonylag magas pénzbüntetéssel szankcionálja. Lényeges különbség továbbá a fokozatosság hiánya, mivel a tényállás összesen egy fordulatból, egy alapesetből áll, sem privilegizált, sem pedig minősített esete nincsen, szemben a magyar szabályozással.

[192] Megjegyzendő, hogy a kolumbiai büntető törvénykönyvet az informatikai bűncselekmények vonatkozásában jelentősen módosította a 2018. évi 1928. törvény, mellyel az ország végül 2020-ban elérte, hogy megfeleljen a Budapesti Egyezmény rendelkezéseinek.

7.1.3.2. Információs rendszer vagy távközlési hálózat illegális akadályozása (Obstaculización ilegítima de sistema informático o red de telecomunicación)

A tényállást a törvény 269 B. cikke tartalmazza:

„Aki erre felhatalmazás nélkül megakadályozza vagy meggátolja az információs rendszer, az abban foglalt adatok, illetve a távközlési hálózat normál működését vagy az azokhoz való hozzáférést, negyvennyolc (48) hónaptól kilencvenhat (96) hónapig terjedő szabadságvesztésre ítélhető és a mindenkori havi minimálbérrel számolt 100 havi tételtől 1.000 havi tételig terjedő pénzbírsággal sújtható.”

A tényállást a hazai Btk. rendszerében nagyjából a 423. § (2) bekezdésének a) pontjában szereplő, az információs rendszer vagy adat megsértésének minősített esetével lehet megfeleltetni, ugyanakkor a jogalkotó úgy ítélte meg, hogy különállóan szabályozza a cselekményt. A tényállások a Budapesti Egyezmény 5. cikke szerinti „Számítástechnikai rendszer megsértése” cím implementációi. Elkövetési tárgyuk az információs rendszer. Az elkövetési magatartást nem konkretizálta a jogalkotó, így a hozzáférés megakadályozásának bármilyen módjával megvalósulhat a bűncselekmény. Lényeges különbség itt is a szankciók mértékével kapcsolatban állapítható meg. Míg a magyar Btk. három évig terjedő szabadságvesztést helyez kilátásba, úgy a kolumbiai tényállás két évtől nyolc évig terjedő szabadságvesztéssel és magas pénzbírsággal sújtja a cselekmény elkövetőjét. A hazai tényállás tartalmaz két minősített esetet is, szemben a vizsgálat tárgyát képező rendelkezéssel. Ha a cselekmény jelentős számú információs rendszert érint vagy jelentős érdeksérelmet okoz, a szankció egy évtől öt évig terjedő, ha pedig közérdekű üzem ellen irányul, akkor két évtől nyolc évig terjedő szabadságvesztés. A kolumbiai szabályozás itt is mellőzi a minősített esetek alkalmazását.

7.1.3.3. Információs adat kifürkészése (Interceptación de datos informáticos)

A tényállást a 269 C. cikk tartalmazza:

„Aki előzetes bírósági végzés nélkül információs adatokat vagy az információs rendszerből származó elektromágneses sugárzást azok származási helyén, rendeltetési helyén vagy

információs rendszeren belül kifürkészi, harminchat (36) hónaptól hetvenkét (72) hónapig terjedő szabadságvesztéssel sújtandó.”

A tényállás a hazai szabályozásban a Btk. 422. § (1) bekezdésének e) pontjával állítható párba, ugyanakkor lényeges különbségek rögzíthetőek a kettő között. A magyar szabályozás szerint ugyanis kizárólag akkor valósul meg bűncselekmény, ha a kifürkészett adatokat az elkövető technikai eszközzel rögzíti is. A Btk. kommentárja ezt a kritériumot azzal indokolja, hogy a kifürkészett adatok rögzítése jelentős mértékben emeli a cselekmény társadalomra veszélyességét. A kolumbiai szabályozás többleteleme a bírósági végzés hiánya, mely a hazai szabályozásból hiányzik. A magyar tényállás ugyanakkor célzatos bűncselekményt takar, célzatként pedig a személyes adat, a magántitok, a gazdasági titok vagy az üzleti titok jogosulatlan megismerését rögzíti.

7.1.3.4. Informatikai károkozás (Daño informático)

A törvény 269 D. cikke tartalmazza a tényállást:

„Aki erre való felhatalmazás nélkül megsemmisít, megkárosít, megrongál, hozzáférhetetlenné tesz, megváltoztat vagy töröl információs adatokat, információt feldolgozó rendszert, annak részeit vagy logikai összetevőit, negyvennyolc (48) hónaptól kilencvenhat (96) hónapig terjedő szabadságvesztésre ítélhető és a mindenkori havi minimálbérrel számolt 100 havi tételtől 1.000 havi tételig terjedő pénzbírsággal sújtható.”

A bűncselekmény jogi tárgya az információs adat, az információs rendszer, illetőleg annak részeinek védelme. Az elkövetési magatartás sokféle lehet: megsemmisítés, megkárosítás, megrongálás, hozzáférhetetlenné tétel, megváltoztatás vagy törlés. Az első alapvető kritika, mely megfogalmazható a fenti tényállással kapcsolatban, hogy – dacára annak, hogy a tényállás elnevezésében is szerepel a károkozás – maga a kár, mint eredmény a tényállás szövegében csak, mint egy elkövetési magatartás jelenik meg. Ennél fogva a bűncselekmény a kár tényleges bekövetkezése nélkül, pusztán az adat modifikációjával is elkövethető. Ez alapján pedig kevésbé lenne félrevezető egy olyan elnevezés használata, mely nem szükségszerűen tartalmazza a kár és a károkozás fogalmakat.

A tényállás a hazai büntetőjogi szabályozással összevetve az információs rendszer felhasználásával elkövetett csalás alapesete és az információs rendszer vagy adat megsértése alapesetének a második fordulata szerinti rendelkezései között képez egyfajta átmenetet.
Újabb kritikaként rögzíthető a szankció eltúlzott mértéke. A bűncselekmény elkövetése esetén ugyanis – a rendkívül magas pénzbüntetés mellett – négytől nyolc év szabadságvesztéssel büntetendő az elkövető. A hazai tényállásokat vizsgálva szembetűnő különbség állapítható meg, az információs rendszer vagy adat megsértésének alapesete ugyanis csak vétségnek minősül, mely két évig terjedő szabadságvesztés büntetendő, míg az információs rendszer felhasználásával elkövetett csalás esetében – ahol a kár bekövetkezése szükségszerű – bűntett miatt három évig terjedő szabadságvesztés szabható ki. Álláspontom szerint a kolumbiai tényállás nem következetes, hiszen a büntetőjogi szankció alsó határa eltúlzott mértékű, mely nem enged lehetőséget arra, hogy egy adott esetben meglehetősen csekély társadalomra veszélyességű magatartást például pénzbüntetéssel szankcionáljon a bíróság. Ennél fogva előállhatnak olyan absztrakt helyzetek, melyben egy büntetlen előéletű elkövető információs rendszer megsértését követi el, tényleges kár bekövetkezése nélkül, a bíróság pedig – a törvényi keretek hiánya és ezáltal a mérlegelési jogkörének erős korlátjai miatt – kénytelen szabadságvesztés büntetést kiszabni, nem beszélve a rendkívül magas pénzbüntetést.

7.1.3.5. Rosszindulatú szoftver felhasználása (Uso de software malicioso)

A tényállást a törvény 269 E. cikke tartalmazza:

„Aki erre felhatalmazás nélkül rosszindulatú szoftvert vagy más, kártékony hatású számítógépes programot előállít, forgalmaz, megszerez, terjeszt, elad, elküld, az ország területére behoz vagy onnan kivisz, negyvennyolc (48) hónaptól kilencvenhat (96) hónapig terjedő szabadságvesztéssel, továbbá a mindenkori havi minimálbérrel számolt 100 havi tételtől 1.000 havi tételig terjedő pénzbírsággal sújtható.”

Az ún. malware programok felhasználása meglehetősen sokféleképpen történhet a gyakorlatban, illetőleg az általuk okozott károk is igen széles skálán mozoghatnak. A jogalkotó döntése e tényállás tekintetében az volt, hogy a károkozást, mint tényállási elemet mellőzi, csakúgy, mint a minősített eseteket, értékhatárok szerinti fokozatosságot. A bűncselekmény elkövetéséhez nem szükségszerű a program felhasználása, annak előállítása, megszerzése, az

ország területére behozatala, illetőleg az onnan történő kivitele, tehát az előkészületi tevékenységek már megvalósítják a bűncselekmény. Ezen elkövetési magatartások mellett büntetni rendeli a jogalkotó továbbá a terjesztést, a forgalomba hozatalt, az értékesítést és az elküldést.

7.1.3.6. Személyes adatok megsértése (Violación de datos personales)

A tényállást a törvény 269 F. cikke tartalmazza:

„Aki felhatalmazás nélkül saját maga vagy harmadik fél részére aktákban, archívumokban, adatbázisokban vagy más hasonló adathordozókban található személyes kódokat vagy személyes adatokat megszerez, összeállít, kivonatol, felajánl, elad, elcserél, elküld, megvesz, kifürkész, nyilvánosságra hoz, módosít vagy felhasznál, negyvennyolc (48) hónaptól kilencvenhat (96) hónapig terjedő szabadságvesztéssel, továbbá a mindenkori havi minimálbérrel számolt 100 havi tételtől 1.000 havi tételig terjedő pénzbírsággal sújtható."

A tényállás, bár elnevezésében közel áll a Btk. 219. §-a szerinti személyes adattal visszaéléshez, a két tényállás között meglehetősen sok a különbség. A magyar szabályozás utalást tartalmaz az Infotv. és az Európai Unió jogi aktusaira. A tényállás első fordulata célzatos (haszonszerzésre törekvés). Ezen felül mind az első, mind a második fordulat eredménybűncselekmény, ahol az eredmény a jelentős érdeksérelem. A kolumbiai szabályozás ezzel szemben konkrétan megjelöli az elkövetések tárgyát (akták, archívumok, adatbázisok, adathordozók) és az elkövetés modus-ait is.

7.1.3.7. Weboldalakkal történő visszaélés személyes adatok megszerzésének céljából (Suplantación de sitios web para capturar datos personales)

A tényállást a törvény 269 G. cikke tartalmazza:

„Aki tiltott célból vagy arra való felhatalmazás nélkül elektronikus oldalakat, linkeket vagy felugró ablakokat tervez, fejleszt, forgalmaz, értékesít, végrehajt, programoz vagy elküld, ha súlyosabb bűncselekmény nem valósul meg, negyvennyolc (48) hónaptól kilencvenhat (96)

hónapig terjedő szabadságvesztéssel, továbbá a mindenkori havi minimálbérrel számolt 100 havi tételtől 1.000 havi tételig terjedő pénzbírsággal sújtható.
Ha súlyosabb bűncselekmény nem valósul meg, az első bekezdés szerint büntetendő, aki a domain név rendszert oly módon módosítja, hogy a felhasználót egy másik IP címre irányítja abban a tévhitben, hogy azzal hozzáfér a bankjához vagy más személyes vagy bizalmas weboldalhoz.
Az előző két bekezdésben megjelölt büntetési tételek egyharmad részétől annak fele részéig súlyosbítandóak, amennyiben az elkövető áldozatokat toborzott a tevékenységéhez."

Az egyes pénzügyi intézetek, biztosítók, állami szereplők internetes honlapjainak „hamisítása" meglehetősen elterjedt és hatékony módja az adathalász („phising") tevékenységnek. Az így megszerzett személyes adatok, belépési kódok, felhasználónevek, banki adatok további bűncselekményekhez történő felhasználása miatt kétségtelen, hogy e cselekmények társadalomra veszélyessége magas. A jogalkotó e megfontolásból döntött a cselekmény önálló szankcionálása mellett. A hazai szabályozás a tevékenységet egyszerűen a csalással azonosítja, nem alkot különálló büntetőjogi tényállást. Álláspontom szerint a kolumbiai megoldás – a rosszindulatú szoftverek felhasználásának önálló szankcionálásához hasonlóan – eredményesebb is lehet, hiszen a jogalkotó konkrét álláspontját, egyfajta hangsúlyos „helytelenítését" fejezi ki az adott magatartással szemben, mely nagyobb visszatartó erőt is jelenthet. Figyelmet kell fordítani azonban arra is, hogy a törvényhozó ne kreáljon túlságosan sok, túl speciális tényállást. Úgy vélem, hogy ebben az esetben a jogalkotó az arany középutat választotta, helyesen ismerte fel, hogy a jelenség kiemelt figyelmet érdemel.

7.1.3.8. Informatikai és más hasonló eszközökkel történő lopás (Hurto por medios informáticos y semejantes)

A tényállást a törvény 269 I. cikke tartalmazza:

„Aki a számítógépes biztonsági intézkedéseket leküzdve a 239. cikkben[193] megjelölt magatartást számítógépes rendszer, elektronikus, telematikai rendszerhálózat vagy más hasonló eszköz manipulálásával, illetve a kialakított hitelesítési és engedélyezési rendszerek előtt felhasználónak kiadva hajtja végre, a 240. cikke szerint büntetendő."

[193] A kolumbiai büntető törvénykönyv 239. §-a tartalmazza a lopás tényállását.

A szankció vonatkozásában a tényállás utal a törvény 240. cikkére, mely a lopás minősített eseteit tartalmazza. E körben – amennyiben a lopást telefonos, távíró, informatikai, telematikai vagy műholdas távközlési rendszeren, illetve villamosenergia és háztartási gáz előállítására, továbbítására vagy elosztására szolgáló, illetve vízvezeték- és szennyvízszolgáltatás biztosítására szolgáló rendszerelemeken keresztül követik el – a törvény öt évtől tizenkét évig terjedő szabadságvesztést helyez kilátásba.

7.1.3.9. Vagyonelemek beleegyezés nélküli átruházása (Transferencia no consentida de activos)

A tényállást a törvény 269 J. cikke tartalmazza:

„Aki haszonszerzés céljából bármilyen informatikai manipuláció segítségével vagy hasonló módon eléri bármely vagyon beleegyezés nélküli átadását és ezzel harmadik fél részére kárt okoz, ha súlyosabb bűncselekmény nem valósul meg, negyvennyolc (48) hónaptól százhúsz (120) hónapig terjedő szabadságvesztéssel, továbbá a mindenkori havi minimálbérrel számolt 200 havi tételtől 1.500 havi tételig terjedő pénzbírsággal sújtható.
Az első bekezdés szerint büntetendő, aki az ott szereplő bűncselekmény elkövetéséhez számítógépes programot gyárt, bevezet, birtokol vagy rendelkezésre bocsát.
Ha az előző bekezdésekben szereplő bűncselekmények pénzbüntetése meghaladja a 200 havi tételt, az ott jelölt szankció a felével emelkedik.”

Álláspontom szerint ezen cselekményt a lopás tényállása kellőképpen lefedhetné, így annak külön, önálló tényállásban történő szankcionálására nincsen szükség. Emellett a tényállás második fordulatában szereplő magatartást pedig a törvénykönyv 269 E. cikkében szereplő rosszindulatú szoftver felhasználása fedhetné le, így önmagában a szabályozás véleményem szerint felesleges.

7.1.4. Összegző gondolatok

Kolumbia kiberbűnözés elleni intézményi és jogszabályi kereteinek vizsgálata nyomán – a fentieket összegezve – több megállapítás is rögzíthető. Egyrészről vitathatatlan, hogy Kolumbia intézményi rendszere fejlődő tendenciát mutat az utóbbi években, mely szépen megnyilvánul a kiberbűnözéssel foglalkozó szervezetek eredményességében. A kiberközpont éves

összefoglalói alapján megállapítható, hogy a 2022. év során 286 sikeres felderítést hajtott végre a hatóság, melyből 236 informatikai bűncselekmény, míg 50 gyermekek interneten történő szexuális kizsákmányolása volt. Ebben az évben összesen 65.794 bejelentés érkezett a központhoz, mely a 2021. évhez képest 21,6 % növekedést mutat.[194] A 2023. év folyamán a kiberközponthoz 59.033 bejelentés érkezett, mely 10% csökkenést jelent az előző évhez képest, ugyanakkor a központ 352 sikeres felderítést tudhatott magáénak, melyből 277 informatikai bűncselekmény és 75 gyermekek interneten történő szexuális kizsákmányolása volt.[195] Ennek egyik lehetséges oka, hogy a kolumbiai rendőrség kiberközpontja szorosan együttműködik az Interpollal.

A jogszabályi oldal vizsgálata során megállapítható, hogy a kolumbiai törvénykönyv a következő tényállásokat tartalmazza az információs rendszer vagy adat védelmében:

- információs rendszer megsértése,
- információs rendszer vagy távközlési hálózat illegális akadályozása,
- információs adat kifürkészése,
- informatikai károkozás,
- rosszindulatú szoftver felhasználása,
- személyes adatok megsértése,
- weboldalakkal történő visszaélés személyes adatok megszerzésének céljából,
- informatikai és más hasonló eszközökkel történő lopás,
- vagyonelemek beleegyezés nélküli átruházása.

Az egyes tényállások szövegezésében meglehetősen sok párhuzam vonható a hazai büntetőjogi rendelkezések között. Ennek oka, hogy Kolumbia 2020 óta már tagja a Budapesti Egyezmény rendszerének is, ezért az egyezményben szereplő követelményeket implementálta. A két szabályozás között azonban lényeges különbségek is megállapíthatóak. A hazai büntetőjogi szabályanyag álláspontom szerint sokkal következetesebb a szankciók fokozatosságát tekintve. A kolumbiai büntető törvénykönyv legtöbb releváns tényállása meglehetősen szigorú következményeket állapít meg az elkövetőkre nézve. A szankciók alsó határa gyakran meglehetősen magas, nem enged más, csekélyebb büntetést (például közérdekű munkát vagy pénzbüntetést) kiszabni, még a társadalomra kevésbé veszélyes elkövetési módokra nézve sem. A fentiek alapján álláspontom szerint Kolumbia intézményi oldala hatékonyan képes felvenni a harcot a kiberbűnözőkkel, ugyanakkor a jogszabályi oldal jelentős problémákat vet fel.

[194] https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf (2024.03.20.)
[195] https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf (2024.03.20.)

Egyrészről mellőzi a fokozatosság, arányosság-szükségesség elvét a szankciók terén, másrészről a privilegizált és minősített esetek hiányából fakadóan az egyes elkövetési módok elhatárolására sem tart igényt. Ez egyrészről eltúlzott mértékű szankciókat, másrészről a büntetés-végrehajtási rendszer jelentős leterheltségét is eredményezi, mellyel a latin-amerikai börtönök zöme küzd napjainkban is.
A weboldalakkal személyes adatok megszerzésének céljából való visszaélés önálló büntetőjogi tényállásként történő szankcionálása álláspontom szerint egy működőképes megoldás lehet a gyakorlatban. A cselekmény egyrészről kellőképpen speciális ahhoz, hogy külön tényállásként szabályozza a jogalkotó, másrészről esetlegesen nagyobb visszatartó erőt válthat ki az állampolgárokból, hogy az állam egyértelműen konkretizálja az álláspontját az adathalász tevékenységekkel kapcsolatban.

7.2. Argentína

7.2.1. Argentína kiberbűnözés elleni intézményrendszere

7.2.1.1. Az Argentin Legfőbb Ügyészség Kiberbűnözésre Szakosodott Egysége (Ministerio Público Fiscal. Unidad Fiscal Especializada en Ciberdelincuencia, röviden UFECI)

Az ügyészség Kiberbűnözésre Szakosodott Egységét 2015-ben hozták létre[196] azzal a céllal, hogy megerősítsék a szervezet reagálási képességét a szervezett bűnözéssel és az állampolgárok biztonságát legjobban veszélyeztető bűncselekményekkel szemben. Azon esetekben jár el, mikor az elkövetés fő vagy járulékos eszköze az információs rendszerek használata, különös tekintettel a szervezett bűnözés területére, illetőleg olyan esetekben, mikor információs rendszer nem volt érintett a bűncselekmény során, de azok használata a nyomozás során szükséges. Az egység fő feladatai közé a teljesség igénye nélkül a következők tartoznak:

- beavatkozás a hatáskörükbe tartozó ügyekbe, az ügyészek munkájának segítése,
- panaszok fogadása, előzetes és általános vizsgálatok lefolytatása,
- a különböző argentin és nemzetközi szereplőkkel, intézményekkel történő kapcsolattartás,
- együttműködés a Legfőbb Ügyészség egységeivel a kiberbűnözés elleni hatékony stratégiák kidolgozása és megvalósítása érdekében,

[196] Resolución PGN No. 3743/15

- tanácsadás az ügyészek számára az országban rendelkezésre álló technológiai erőforrásokkal, eszközökkel, laboratóriumokkal, kutatási módszerekkel kapcsolatban,
- tanulmányok kidolgozása a jogalkotás számára a jogfejlesztés érdekében,
- jelentések készítése.[197]

7.2.1.2. A Buenos Aires-i Ügyészség Informatikai Bűncselekményekre és Szabálysértésekre Szakosodott Egysége (Ministerio Público Fiscal de CABA. Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas, röviden UFEDyCI)

Az UFEDyCI a Legfőbb Ügyészség fentebb bemutatott egységéhez hasonlóan informatikai bűncselekményekkel foglalkozik. Illetékességét tekintve Buenos Aires autonóm városában fejti ki tevékenységét. Az UFEDyCI feladatköre meglehetősen széleskörű, a teljesség igénye nélkül a következő tevékenységeket fedi le:

- az igazságszolgáltatási rendszer üzemeltetőinek kiképzése, részükre megfelelő eszközök biztosítása a digitális úton elkövetett bűncselekmények és szabálysértések kivizsgálására, melyek nem tartoznak a kizárólagos hatáskörébe,
- a gyermek- és serdülőkorúak, szüleik és tanáraik tájékoztatása az internetes bűncselekmények elkerülésének és megelőzésének lehetőségeiről,
- kérelemre tanácsot ad az ügyészségeknek a nyomozásaik során a digitális bizonyítékok összegyűjtéséhez, megőrzéséhez és elemzéséhez, kapcsolattartóként működik a külföldi szolgáltatókkal, amennyiben a bizonyíték másik országban található,
- segíti a nemzetközi együttműködés mechanizmusainak elmélyítését, a kapcsolatok megerősítését,
- koordinációs tevékenységet folytat a szakosodott szervek, társszervek nyomozásaiban, városi, szövetségi és nemzeti szinten egyaránt,
- képzési terveket hoz létre az ügyészek, technikusok és informatikusok közötti tapasztalatcsere érdekében,
- kézikönyvek megalkotása, melyek a felderítési szaktól a tárgyalási szakig bemutatják a nyomozás egyes cselekményeit,
- a mesterséges intelligencia használata a nyomozás és a bizonyítékok feldolgozásának sikere érdekében.[198]

[197] „Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)”
Elérhető: https://www.mpf.gob.ar/ufeci/ (2024.03.22.)
[198] „DELITOS INFORMÁTICOS”

7.2.1.3. Az Argentin Szövetségi Rendőrség Technológiai Bűncselekmények Részlege (División Delitos Tecnológicos de la Policía Federal Argentina), valamint a Gyermekeket és Serdülőkorúakat ért Kiberbűncselekmények Részlege (División Delitos Ciberneticos contra la Niñez y Adolescencia)

Az argentin rendőrség említett részlegeiről meglehetősen csekély információ lelhető fel, így források hiányában azok részletes bemutatását mellőztem.

7.2.2. A kiberbűnözés jogszabályi dimenziói Argentínában

A hatályos argentin büntető törvénykönyv, a 1921. évi 11.179. törvény (Código Penal de la Nación) meglehetősen régre nyúlik vissza, felépítését tekintve a jogalkotó maradt a módosításoknál és nem tartotta szükségesnek új kodifikációs folyamatok elindítását. A kódex sémáját tekintve megállapítható, hogy nem tartalmazza az egyes bűncselekmények elnevezését, kizárólag számozással és a nagyobb bűncselekménykategóriák (fejezetcímekben történő) megjelölésével különíti el egymástól az egyes cselekményeket.
A törvénykönyvet a 2008. évi 26.388. törvény egészítette ki az informatikai bűncselekményekkel, melyek a következők:

- az tiltott adatszerzés,
- az információs rendszer vagy adat megsértése,
- a levéltitok megsértése,
- az információs rendszer felhasználásával elkövetett csalás, valamint az
- az informatikai károkozás.

A módosítás a fentiek mellett több, a korrupció leküzdését szolgálni hivatott rendelkezést is beemelt a törvénykönyvbe, ugyanakkor ezek részletes vizsgálatát terjedelmi okokból mellőztem.

7.2.2.1. Tiltott adatszerzés

Az argentin büntető törvénykönyv 153. cikke rendeli büntetni a tiltott adatszerzést:

„Tizenöt naptól hat hónapig terjedő szabadságvesztéssel büntetendő, aki nem neki címzett elektronikus közleményt, levelet, zárt iratot, távirati, telefonos vagy egyéb küldeményt engedély

Elérhető: https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos (2024.03.22.)

nélkül nyit meg, vagy engedély nélkül elektronikus kommunikációt, levelet, iratot, hivatalos vagy magánlevelet átvesz, vagy a nem neki címzett levelezést vagy elektronikus kommunikációt engedély nélkül törli vagy célhelyéről áthelyezi.
Az első bekezdés szerint büntetendő, aki bármely magán vagy korlátozott hozzáférésű rendszerből engedély nélkül elektronikus kommunikációt vagy távközlést lehallgat vagy rögzít.
A büntetés egy hónaptól egy évig terjedő szabadságvesztés, ha az elkövető a levél, az írás, a feladott küldemény vagy az elektronikus közlés tartalmát mással is közli vagy azt közzéteszi.
Ha a cselekményt a tisztségével visszaélő köztisztviselő követi el, a büntetés kétszeresével megegyező idejű foglalkozástól eltiltással büntetendő."

A hazai szabályozással párhuzamba állítva rögzíthető, hogy az argentin szankciók sokkal enyhébbek a tiltott adatszerzés tekintetében. A magyar tényállás ugyanakkor csak a kifürkészett információ rögzítését szankcionálja, míg az argentin magát a kifürkészést is. A minősített esetek vonatkozásában a magyar szabályozás a hivatalos eljárás színlelését, míg az argentin a köztisztviselő általi elkövetést szankcionálja.

7.2.2.2. Információs rendszer vagy adat megsértése

A tényállást a 153 bis cikk rögzíti:

„Aki tudatosan, bármilyen módon, megfelelő felhatalmazás nélkül vagy a jogosultsága kereteit túllépve hozzáfér egy korlátozott hozzáférésű információs rendszerhez vagy adathoz, amennyiben súlyosabb bűncselekmény nem valósul meg, tizenöt naptól hat hónapig terjedő szabadságvesztéssel büntetendő.
A büntetés egy hónaptól egy évig terjedő szabadságvesztés, ha a hozzáférés közfeladatot ellátó állami szerv, közszolgáltató vagy pénzügyi szolgáltató rendszeréhez vagy adataihoz történik."

A magyar tényállással összehasonlítva megfigyelhető az egyik leglényegesebb különbség, az információs rendszer védelmét biztosító intézkedés megsértésének vagy kijátszásának a hiánya. Az argentin jogalkotó megoldása e tekintetben az információs rendszer korlátozott hozzáférésű voltának tényállási elemek közé történő beemelése volt. A szankciókat tekintve az argentin rendelkezés szerinti büntetési tétel felső határa a magyarban megszabott két évhez képest csak hat hónap, míg a minősített esetnél csak egy év.

7.2.2.3. Levéltitok megsértése

A levéltitok megsértésének tényállását a kódex 155. cikke tartalmazza:

„Aki levelezés, elektronikus hírközlés, zárt irat, távirati, telefonos vagy egyéb, nem publikusnak szánt küldemény birtokában azok engedély nélküli közzétételét idézi elő, ha az harmadik személynek kárt okoz vagy okozhat, ezerötszáz pesótól százezer pesóig terjedő pénzbírsággal büntetendő.
Mentesül a büntetőjogi felelősség alól, aki a közérdek védelmének egyértelmű céljával járt el.”

7.2.2.4. Információs rendszer felhasználásával elkövetett csalás

A csalás alapesetét az argentin kódex a 172. cikkben rögzíti:

„Egy hónaptól hat évig terjedő szabadságvesztéssel büntetendő, aki felvett névvel, színlelt minőséggel, hamis címekkel, hazug befolyással, bizalommal való visszaéléssel vagy vagyon, hitel, jutalék, vállalkozás vagy üzlet színlelésével vagy más csellel vagy megtévesztéssel mást tévedésbe ejt.”

Az információs rendszer felhasználásával elkövetett csalás a 173. cikk 16. pontjában, a csalás minősített, különleges formáinak felsorolásában található meg:

„Az előző (172.) cikk általános rendelkezéseinek sérelme nélkül, az ott meghatározott szankcióval büntetendők a csalás különleges esetei.
…
16. Aki olyan informatikai manipulációs technikával ejt mást tévedésbe, amely megváltoztatja egy információs rendszer működését vagy az adatátvitelt.”

Az információs rendszer felhasználásával elkövetett csalás tényállása a magyar szabályozáshoz képest meglehetősen tág, melyhez a kiszabható szankció mértéke is alkalmazkodik. A tényállás mellőzi a minősítés terén az károkozás mértéke szerinti fokozatosságot, az alapeset már önmagában egy hónaptól hat évig terjedő szabadságvesztéssel büntetendő, mely szűk mérlegelési teret biztosít a jogalkalmazás számára.

7.2.2.5. Informatikai károkozás

Az argentin kódex az informatikai károkozást a rongálás tényállásának egyik fordulataként rögzíti és az ott meghatározott tizenöt naptól egy évig terjedő szabadságvesztéssel sújtja a 183. cikkének második bekezdésében:

„A fenti bekezdés szerint büntetendő, aki adatokat, dokumentumokat, informatikai programokat vagy rendszereket megváltoztat, megsemmisít vagy hozzáférhetetlenné tesz, vagy bármilyen kártékony hatású programot értékesít, terjeszt, forgalomba hoz vagy információs rendszerbe bevisz.”

A kódex a rongálás minősített eseteit is tartalmazza, melyet a 184. cikk rögzít. E cikk a büntetési tételeket bizonyos modus operandi-k esetén három hónaptól négy évig terjedő szabadságvesztésre emeli. Jelen tanulmány szempontjából a cikk 5. és 6. pontjai relevánsak.
Az 5. pont az információs rendszerek vonatkozásában minősített esetté nyilvánítja a közszféra információs rendszerei vagy programjai elleni elkövetést, míg a 6. pont az egészségügyi, a távközlési, az energia, a közlekedés és más közszolgáltatások szektorainak szolgáltatóit helyezi kiemelt védelem alá.

7.2.2.6. Gyermekpornográfia

A szexuális integritás ellen a kibertérben elkövethető bűncselekmények a büntető törvénykönyv további módosításai által kerültek beemelésre a kódexbe. A gyermekpornográfia tényállását a 2018. évi 27.436. törvény emelte be a büntető törvénykönyv 128. cikkébe:

„Háromtól hat évig terjedő szabadságvesztéssel büntetendő, aki bármilyen módon előállítja, finanszírozza, felajánlja, kereskedelmi forgalomba hozza, közzéteszi, elősegíti, közvetíti vagy terjeszti tizennyolc éven aluli kiskorú személy kifejezetten szexuális tevékenység folytatása közbeni ábrázolását vagy a nemi szerveinek bármilyen ábrázolását túlnyomórészt szexuális célból, valamint aki olyan szexuális megjelenítést bemutató élő közvetítésű műsort szervez, melyben kiskorú személy részt vesz.
A büntetés négy hónaptól egy évig terjedő szabadságvesztéssel büntetendő, aki az első bekezdésben foglalt anyagokat tudatosan birtokolja.

Hat hónaptól két évig terjedő szabadságvesztéssel büntetendő, aki az első bekezdésben foglalt anyagokat egyértelműen terjesztés vagy kereskedelmi forgalomba hozatal céljából birtokol.
Egy hónaptól három évig terjedő szabadságvesztéssel büntetendő, aki tizennégy éven aluli kiskorúak pornográf műsorokhoz való hozzáférését elősegíti vagy részükre pornográf anyagot juttat el.
A fenti bekezdésekben szereplő magatartások szankcióinak alsó és felső határa egyharmad résszel emelkedik, amennyiben a sértett tizenhárom évesnél fiatalabb."

A minősítések a magyar szabályozáshoz képest e tényállás vonatkozásában is eltérőek. Az argentin szabályozás nem minősíti a hivatalos személyként történő elkövetést, ugyanakkor a korhatárok tekintetében szigorúbban jár el, mint a magyar tényállás.

7.2.2.7. Szexuális behálózás

A szexuális behálózás vagy más szóval az ún. grooming szankcionálását a 2013. évi 26.904. törvény emelte be a büntető törvénykönyvbe. A tényállást a kódex 131. cikke tartalmazza:

„Hat hónaptól négy évig terjedő szabadságvesztéssel büntetendő, aki elektronikus hírközlési, távközlési vagy egyéb adatátviteli technológiával kiskorú személlyel kapcsolatba lép azzal a céllal, hogy vele szemben a szexuális integritása elleni bűncselekményt kövessen el."

A grooming tényállása a magyar Btk. rendelkezéseiben önálló tényállásként nem szerepel, ugyanakkor álláspontom szerint a jogalkotó helyesen értékelte úgy, hogy a cselekmény társadalomra veszélyessége és a következmények lehetősége miatt a tényállásban szereplő magatartást különállóan rendeli büntetni. A hazai megoldás a behálózást a Btk. 198. § (2) bekezdésében, a szexuális visszaélés körében rendeli büntetni. A magyar tényállás ugyanakkor nem szorítkozik az online térre, a rábírni törekvés bármely módját egy helyen szankcionálja.

7.2.3. Összegző gondolatok

Az ország kiberbűnözés elleni eszközrendszerének áttekintése azzal a céllal történt, hogy az ún. good practice jegyében olyan intézményi vagy jogszabályi megoldásokat találjak, melyet a hazai jogrendszerben eredményesen lehetne hasznosítani, egyfajta példaként szolgálhatna. Álláspontom szerint a hazai jogszabályi és intézményi rendszer minden téren fejlettebb, mint

az argentin, így megfelelően hasznosítható, jó gyakorlatot kiemelni nem sikerült. Ennek ellenére ugyanakkor mindenképpen szükséges megjegyezni, hogy az ország statisztikai adatai az utóbbi években javuló tendenciát mutatnak, így pusztán azért, mert a szabályozás más jellegű vagy más rendszert követ, még nem degradálandó. Argentínában a 2022. év folyamán 335 informatikai incidenst regisztráltak, mely a 2021. évi 591 bejelentett incidenshez képest 46%-os visszaesést jelent. A 2022-ben regisztrált bűncselekmények 72%-át tették ki az adathalász tevékenységek (phising).[199] Az eredményben közrehathat, hogy Argentína 2018-tól már a Budapesti Egyezmény tagjává vált, melynek kapcsán eleget kellett tennie a vonatkozó jogalkotási kötelezettségeknek.

7.3. Spanyolország

7.3.1. Az ország helyzete a statisztika fényében

A spanyol kiberbűnözési statisztika 2018-2022 periódusának áttekintése után megállapítható, hogy a kiberbűncselekmények száma folyamatosan növekedett, ugyanakkor nem teljesen egyenlő eloszlásban. A leginkább kiugró növekedést az információs rendszer felhasználásával elkövetett csalás mutatja, mely 2018-ban 136.656 incidenst jelentett, míg 2022-ben már 335.995 esetet regisztráltak a hatóságok, ez az összes kiberbűnözés 89,7%-át teszi ki az országban. Az egyetlen csökkenő tendenciát az intellektuális tulajdon ellen elkövetett bűncselekmények vonatkozásában állapíthatjuk meg, mely a 2018-tól 2022-ig terjedő időszakban 232 esetről 114-re csökkent.[200]

7.3.2. Az ország kiberbűnözésre szakosodott intézményeinek rendszere

7.3.2.1. A Polgárőrség Telematikai Bűncselekményekkel Foglalkozó Csoportja (El Grupo de Delitos Telemáticos de la Guardia Civil, röviden GDT)

A csoport 1996-ban azzal a céllal jött létre, hogy a Polgárőrség Központi Műveleti Osztályán kivizsgáljon minden, az interneten keresztül elkövetett bűncselekményt, majd 2003 óta a

[199] „Informe de Gestión CERT.ar 2022"
Elérhető: https://www.argentina.gob.ar/noticias/informe-de-gestion-certar-2022 (2024.03.22.)
[200] „INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA 2022"
Elérhető: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf (2024.03.22.)

jelenlegi elnevezést használja. Feladatkörében a távközlési szektorban előforduló számítógépes bűnözéssel és csalásokkal kapcsolatos vizsgálatokat végezhet hivatalból vagy az igazságügyi hatóságok megkeresésére vagy állampolgári bejelentés alapján, továbbá nyomozást folytat a számítógépes bűncselekmények esetén.[201]

7.3.2.2. A Rendőrség Technológiai Bűnözés Elleni Egysége (Unidad de Investigación Tecnológica, röviden C.G.P.J.)

Az egység alá tartozik a Központi Technológiai Nyomozó Brigád (La Brigada Central de Investigación Tecnológica, röviden B.C.I.T.), mely a bűnözés új formái által jelentett fenyegetésekre reagál. A brigád hatáskörébe tartozik a gyermekpornográfia, az internetes csalások, a számítástechnikai támadások és más hasonló bűncselekmények nyomozása. Az egység és a brigád célja a digitális bizonyítékok összegyűjtése, az elkövetők felderítése és bíróság elé állítása. E végett képzéseket szervez a rendészeti szervek számára, együttműködik a magánszektor és az állam intézményeivel, továbbá a nemzetközi együttműködés platformjain képviselteti magát.[202]

7.3.2.3. A Legfőbb Ügyészség Informatikai Bűnözés Elleni Főosztálya (Sala de Criminalidad Fiscal del Ministerio Fiscal)

Az Informatikai Bűnözés Elleni Főosztály akár az alárendelt ügyészség utasításával, akár közvetlen eljárási cselekménnyel beavatkozhat a kiemelt jelentőségű, informatikai bűnözéssel összefüggő büntetőeljárásokba, felügyeli és koordinálja a Számítógépes Bűnözés Elleni Osztályok tevékenységét, azokról jelentéseket gyűjt. Emellett összehangolja és kialakítja az informatikai bűncselekmények elleni fellépés gyakorlatát az alárendelt ügyészségek vonatkozásában, melynek kapcsán javaslatot tehet a legfőbb ügyész számára a megfelelő utasítások kiadására. Éves jelentést készít az ügyészség informatikai bűnözéssel kapcsolatos eljárásairól és intézkedéseiről. Azon ügyekben, amelyekben több tartomány érintett, koordinációs tevékenységet lát el az ügyészségek felett. A gyakorlati funkció mellett a főosztály szakmai képzések szervezésével segíti elő a ügyészek munkáját, felkészültségét.[203]

---

[201] „Delincuencia informática”
Elérhető: https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/gdt/index.html (2024.03.22.)
[202] „BRIGADA CENTRAL DE INVESTIGACIÓN TECNOLÓGICA (B.C.I.T.)”
Elérhető:
https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php (2024.03.22.)
[203] „Criminalidad informática”
Elérhető: https://www.fiscal.es/web/fiscal/-/criminalidad-informatica?assetCategoryIds=36767 (2024.03.22.)

7.3.2.4. Nemzeti Kiberbiztonsági Intézet (Instituto Nacional de Ciberseguridad, röviden INCIBE)

A Nemzeti Kiberbiztonsági Intézet a Digitális Átalakulásért felelős és Közszolgálati Minisztérium (Ministerio para la Transformación Digital y de la Función Publica) alá tartozó és a Digitalizációért és Mesterséges Intelligenciáért felelős Államtitkárság irányítása alatt álló intézmény, melynek célja a kiberbiztonság és az állampolgárok digitális bizalmának fejlesztése, az állampolgárok, a kiskorúak és a magánszektor védelme, a kiberbiztonsági ágazat megerősítése, a kutatás-fejlesztés támogatása, illetőleg a szektor szakembereinek képzése, továbbképzése. Az intézet (a minisztérium és az államtitkárság segítségével) üzemelteti az INCIBE-CERT névre hallgató gyors reagálási incidensközpontját is.[204]

7.3.3. A kiberbűnözés büntetőjogi szabályozása

A spanyol büntető törvénykönyv, az 1995. évi 10. organikus törvény (Ley Orgánica 10/1995 del Código Penal) a következő informatikai bűncselekményeket tartalmazza:

- titkok felfedése (Descubrimiento y revelación de secretos)[205],
- információs rendszer megsértése (Acceso ilícito a sistemas informáticos)[206],
- üzleti titkok megsértése (Descubrimiento y revelación de secretos de empresa)[207],
- informatikai károkozás (Daños informáticos)[208],
- informatikai hamisítás (Falsedades informáticas)[209],
- információs rendszer felhasználásával elkövetett csalás (Estafa informática)[210],
- telekommunikációs csalás (Defraudación de telecomunicaciones)[211],
- szexuális jellegű kiberbűncselekmények (Ciberdelitos sexuales)[212],

[204] „Qué es INCIBE”
Elérhető: https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe (2024.03.22.)
[205] 197. cikk 1., 2. és 7. bekezdései
[206] 197 bis. cikk 1-2. bekezdései és a 197 ter. cikk
[207] 278-279. cikkek
[208] 264. cikk, 264 bis. cikk, 264 ter. cikk, 400. cikk
[209] Az informatikai hamisítás megnyilvánulhat többféleképpen, ezért az egyes elkövetési tárgyak szerint rendszerezi a kódex a tényállásokat is. A pénzhamisítással kapcsolatos rendelkezéseket a kódex 386-389. cikkei, a közokirat-hamisítást a 390-394. cikkei, a magánokirat-hamisítást a 395-396. cikkei, a bizonyítvány-hamisítást a 397-399. cikkei, a készpénz-helyettesítő fizetési eszközök hamisítását a 399 bis. cikke, míg az eszközök vonatkozásában a 400. cikke tartalmazza.
[210] 248-258 bis. cikkek
[211] 255-256. cikkek
[212] 181-189. cikkek

- intellektuális tulajdon elleni bűncselekmények (Delitos contra la propiedad intelectual)[213],
- becsületsértő bűncselekmények (Delitos contra el honor)[214],
- kényszer és fenyegetés (Amenazas y coacciones)[215],
- gyűlöletbeszéd és bocsánatkérés a terrorizmusért (Odio y apología del terrorismo)[216].

Mivel az európai uniós jogi normák által kifejtett jogközelítés miatt a spanyol és a magyar szabályozás között lényegesen kevesebb eltérés figyelhető meg, ezért jelen fejezetben az egyes büntető anyagi jogi tényállások részletes elemzését terjedelmi okokból mellőztem.

8. Régi bűncselekmények új köntösben: egyes „hagyományos" bűncselekmények megjelenése a kibertérben

A kibertér új lehetőségeket nyitott meg a bűnelkövetők előtt, melynek eredményeként bizonyos bűncselekmények részben vagy egészben megjelentek ebben a dimenzióban. E folyamat nem egyik napról a másikra történt, az egyes bűncselekmények elkövetési magatartásai a technológiai fejlődéssel párhuzamosan, annak új vívmányait fokozatosan kihasználva helyeződtek át. E fejezet célja ezen folyamatok áttekintése a leggyakoribb, illetőleg a társadalomra leginkább veszélyes bűncselekmények vonatkozásában. Ennek során részletesen elemzem az egyes bűncselekmények olyan elkövetési magatartásait, melyeknél részben vagy egészben a kibertér is érintett.

8.1. A kiberterrorizmus, avagy a 21. század egyik legnagyobb fenyegetése

A technológiai fejlődés hatására – más bűncselekményekhez hasonlóan – a terrorizmus különböző, új megjelenési formái is felütötték a fejüket az internetes környezetben. Kiemelendő azonban, hogy a terrorista szervezetek internethasználata korántsem újkeletű fenomén. Az 1990-es évek második felében már jelentek meg dzsihádista tartalmú weboldalak. Az egyik legnagyobb hatással bíró weboldal, mely a témába illő tartalommal működött, a www.azzam.com volt, melyet 1996-ban létesítettek és angol nyelven publikálták rajta a

[213] 270. cikk
[214] 205., 208. és 211. cikkek
[215] 169-172. cikkek és a 271. cikk
[216] 510. és 578. cikkek

tartalmakat. Szintén érdemes kiemelni a www.alneda.com nevű weboldalt, mely 1998-től kezdte meg a működését.[217]

A 2001. szeptember 11. napján történt események hatására megállapíthatjuk, hogy az addig hagyományos módon folytatott háborúk kiléptek a földrajzilag megha tározott fizikai térből. Ennek eredményeként általánossá vált azon felfogás, miszerint az addig alkalmazott hagyományos hadviselési módszerek mellett jobban szükséges koncentrálni a kibertérre, mely a 2020-as évekre a terrorizmus egyik legalkalmasabb eszközévé vált a politikai és katonai célok eléréséhez.[218] Ez a platform ugyanis rendkívül jól hasznosítható illegális célokra. Az internet hatékony és gyors forrása lehet a félelemkeltésnek, illetőleg a terrorcselekmények elkövetéséhez való toborzásnak és az ideológia, propaganda terjesztésének. A különféle terrorszervezetek használhatják továbbá az egymás közötti rejtett kommunikáció és információ-megosztás folytatásához, illegális fegyverkereskedelemhez, az egyes támadási technikák oktatásához, népszerűsítéséhez.[219]

8.1.1. A kiberterrorizmus fogalma

A kiberterrorizmus mibenlétének definiálásához elsőkörben szükséges volna a terrorizmus nemzetközileg elfogadott fogalmi meghatározása, ugyanakkor e körben sincsen teljes egyetértés a kutatók között. A terrorizmus fogalmát, illetőleg az egyes szerzőknek a definíciókkal kapcsolatos álláspontját – mivel már megannyi cikk[220] foglalkozott e témával – jelen tanulmány mellőzi.

A kiberterrorizmus fogalmára ugorva – általánosan elfogadott definíció hiányában – megállapítható, hogy igencsak különféle irányokból kerül megközelítésre a vonatkozó szakirodalomban.[221] Az egyik uralkodó álláspont szerint a kiberterrorizmus alatt azon kiberbűncselekményeket értjük, melyekhez terrorista célzat társul. Az ezen perspektívát vallók úgy vélik, hogy az ilyen cselekményektől el kell határolni a terrorista csoportok egyéb internetes tevékenységeit (mint például a toborzás, a hírszerzés, a finanszírozás megoldása, az egyes propagandaanyagok népszerűsítése, etc.). Egy másik nézet szerint ez utóbbi

[217] Cano Paños, Miguel Ángel: Odio e incitación a la violencia en el contexto del terrorismo islamista. Internet como elemento ambiental. In: Indret No. 4, 2016. p. 6.
[218] Simon László; Magyar Sándor: A terrorizmus és indirekt hatása a kibertérben. In: Nemzetbiztonsági Szemle Vol. 5, No. 3, pp. 90-91.
[219] Simon; Magyar, Op.Cit. pp. 94-95.
[220] Lásd például: Tóth Dávid: The history and types of terrorism. In: LAW OF UKRAINE: LEGAL JOURNAL: SCIENTIFIC-PRACTICAL PROFESSIONAL JOURNAL Vol. 11, No. 1, 2015. (UDC 343.326)
[221] Lásd például: Nagy Melánia, Tóth Dávid: The types of terrorism - with special attention to cyber and religious terrorism. In: JURA Vol. 25, No. 1, 2019. p. 418.

tevékenységeket is magába kell foglalnia a fogalomnak.[222] Eszerint az elhatárolás szerint létezik a kiberterrorizmusnak egy tágabb és egy szűkebb fogalma. Alapvető különbség a kiberterrorizmus és más, a kibertérben elkövetett bűncselekmények között a célzat és az eredmény viszonya. Míg a vagyon elleni kiberbűncselekmények túlnyomó részénél az elkövető célja az egyszeri vagy rendszeres haszonszerzés, addig a kiberterroristák számára az elsődleges cél a politikai vagy ideológiai eszme kifejtése, a megfélemlítés. A bűncselekménnyel esetlegesen szerzett vagyoni előnyök csupán másod- vagy harmadlagos indokok.[223]

Subijana Zunzunegui a kiberterrorizmus fogalmát két megközelítés szerint vizsgálja, egy ún. köztes vagy közvetítő, illetve egy végső perspektívából. A köztes perspektíva az infokommunikációs technológiák által kínált lehetőségek kihasználása a céljaik elérése érdekében. Ez két fogalmi elemet feltételez: a terrorista szervezet jelenlétét és egy technológiai infrastruktúra felhasználását annak működéséhez. Ebben az értelemben a kiberterrorizmus a terrorizmus azon formájaként fogható fel, mely az információs technológiákat egyes társadalmi csoportok megfélemlítésére, kényszerítésére vagy károkozásra használja fel politikai és/vagy vallási okokból. A végső perspektíva pedig a kritikus infrastruktúrák (közszolgáltatások, bank- és tőzsderendszer, ipari termelés, honvédelem), az érzékeny információ megsemmisítését veszi alapul. A végső perspektíva fogalmi elemei közé tartoznak a számítógépes rendszerek és a bennük található információ elleni támadások azzal a céllal, hogy egy kormányt vagy a lakosságot rákényszerítsék valamire, politikai és/vagy társadalmi célok elérésének érdekében. A két megközelítés keresztmetszete és azok elemeinek ötvözete a Subijana Zunzunegui által használt kiberterrorizmus fogalom. Eszerint a kiberterrorizmus minden olyan információtechnológiával végrehajtott cselekmény, amely közvetlenül vagy közvetve terrort válthat ki vagy jelentős károkat okozhat egy politikai és/vagy társadalmi csoportnak, azok bármely alapvető infrastruktúrájának a technológia segítségével történő megsemmisítésével.[224]

Simon László és Magyar Sándor a kiberterrorizmus vonatkozásában kiemelik, hogy a jelenséget nem kizárólag bűnügyi, hanem katonai szempontból is, tehát kiterjesztetten kell értelmezni. E körben a terroristák harcosokként, katonákként definiálhatóak[225], a hadszíntér

[222] Bőczné Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. In: Ügyészek Lapja Vol. 27, No. 1, 2020. p. 79.
[223] Tóth Dávid: How the Cyberspace Changes Terrorism. In: JURA Vol. 28, No. 3, 2022. p. 99. Cit.: MacKinnon, Lachlan; Bacon, Liz; Gan, Diane; Loukas, Georgios; Chadwick, David; Frangiskatos, Dimitrios: Cyber Security Countermeasures to Combat Cyber Terrorism. Strategic intelligence management. Butterworth-Heinemann, 2013. p. 236.
[224] Subijana Zunzunegui, Ignacio José: El ciberterrorismo: una perspectiva legal y judicial. In: Eguzkilore: cuaderno del Instituto Vasco de Criminología No. 22, 2008. pp. 172-173.
[225] Simon; Magyar Op.Cit. p. 95.

fogalma pedig a kiberteret is magába foglalja.[226] A terrorista szervezetek által elkövetett kiberbűncselekmények kapcsán tehát katonai, politikai, stratégiai, regionális és helyi szinten egyeztetett, komplex és katonailag koherens lépéseket szükséges tenni.[227]

A kiberterrorizmus jelenségét szükséges továbbá elhatárolni a többi kibertérben elkövetett bűncselekménytől. Sánchez Medero a kiberterrorizmus alatt azon elkövetési módokat érti, melyekben a terroristák információs technológiákat alkalmaznak azért, hogy bizonyos társadalmi csoportokat megfélemlítsenek, valamire rákényszerítsenek vagy azoknak kárt okozzanak vallási vagy politikai célokból. Álláspontja szerint a fenomént az különbözteti meg más kiberbűncselekményektől, hogy a kiberterrorizmus motivációja, hogy politikai és/vagy vallási célok elérése érdekében a lehető legnagyobb kárt okozzák az elkövetők, míg más kiberbűncselekmények esetében az elkövetők inkább vagyonszerzésre törekednek.[228]

Felmerül a kérdés, hogy egyáltalán szükséges-e a kiberterrorizmus önálló definiálása, hiszen a terrorizmus kategóriája is lefedhetné a kibertérben zajló terrorista célzatú tevékenységeket, mint annak egyfajta alkategóriáját. Ezzel szemben egyes szerzők kifejezetten szorgalmazzák a fogalmak elhatárolását,[229] mások tovább gondolva ezt, egy önálló büntetőjogi kategória megalkotását is, ugyanis a kiberterrorizmus tényállásával sokkal pontosabban lehetne szankcionálni a terrorista célzatú internethasználatot, mely magába foglalhatná a kiberterrorizmus tágabb vonatkozását.[230]

8.1.2. A kiberterrorizmus eszközrendszere

A jelenség eszközrendszerét tekintve számos lehetőség áll rendelkezésére a terrorista szervezeteknek. A szakirodalomban a kiberterrorizmus kategorizálásakor a leggyakrabban az információtechnológia *„soft”* és *„hard”* típusú alkalmazásai közötti elhatárolás szerepel. A kettő közötti különbséget a direkt és indirekt megnyilvánulásban kell keresni. A *„soft”* kategóriába tartoznak a terroristák által indirekt módon kifejtett magatartások, melyek jellemzően nem kibertámadások, hanem a szervezet működéséhez és fenntartásához szükséges tevékenységeket takarnak (pl.: az ideológia terjesztése, toborzás, felhívások, finanszírozás megoldása). A „hard” kategóriába az előbbivel szemben pedig a konkrét kibertámadások

[226] Op.Cit. p. 92.
[227] Op.Cit. p. 95.
[228] Sánchez Medero Op.Cit. p. 74.
[229] Bőczné, Op.Cit. p. 83.
[230] Saul, Ben; Heath, Kathleen: Cyber Terrorism. In: Sydney Law School Legal Studies Research Paper No.14/11. 2014.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2387206 (2023.12.04.)

tartoznak (pl.: informatikai rendszerbe történő jogellenes belépés, az egyes informatikai rendszerek működésének korlátozása vagy meghiúsítása, terheléses támadások, vírusok és/vagy férgek felhasználása, adathalászat, stb.[231]

Álláspontom szerint a fentiek mellett az információtechnológia „hard" típusú alkalmazásának eszközrendszere a következő specifikus, fizikai hatáson alapuló eszközöket, támadásokat is magába foglalhatja:

- Az *elektronikai zavarás (electronic jamming)* az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti azzal a céllal, hogy ezáltal megakadályozzuk a támadás célpontjául szolgáló infrastruktúra elektronikai eszközeinek vagy rendszereinek hatékony működését. E körbe tartozik minden olyan jelenség, amely egy adott elektronikai vevőeszközöknél a hasznos jel vételét akadályozza vagy meggátolja. [232]
- Az *elektronikai megtévesztés (electronic deception)* hamis jelek szándékos kisugárzását, átalakítását, elnyelését, visszasugárzását vagy visszaverését jelenti, amely megtéveszti, félrevezeti, összezavarja vagy eltéríti az információs rendszer működését.[233]
- Az *elektronikai pusztítás (electronic neutralization)* az elektronikai pusztítás az elektromágneses és egyéb irányított energiák, vagy az önrávezetésű fegyverek alkalmazását jelenti, az ellenség elektronikai eszközeiben és az élőerőben tartós vagy ideiglenes károkozás céljából.[234]

8.1.3. Az információtechnológia terrorista célú felhasználásának „soft" típusai

Alapvetően igaz Dornfeld László megállapítása, miszerint a kiberterrorizmusról szóló publikációkban kevesebb figyelmet kap a terroristák egyéb internetes tevékenységének vizsgálata, mint a konkrét kibertámadások elemzése[235], ugyanakkor az utóbbi időben úgy tűnik, hogy az ún. „soft" típusú internetes terrorista aktivitások is elkezdtek bekerülni a kutatók látóterébe.[236] A kiberterrorizmus soft eszközrendszere – ahogyan fentebb már említésre került

[231] Tóth Dávid: A terrorizmus típusai és a kiberterrorizmus. In: Rab Virág (szerk.): XII. Országos Grastyán Konferencia előadásai. Pécs, Pécsi Tudományegyetem Grastyán Endre Szakkollégium, 2014. p. 292.
[232] Horváth József: Az elektronikai zavarás napjainkban. In: Hadmérnök Vol. 10, No. 1, 2015. pp. 184-185.
[233] Papp Zoltán István: A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái. Doktori értekezés. Budapest, 2018, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola
[234] Horváth, Op.Cit. p. 184.
[235] Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécs, Budapest, Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK), MTA Társadalomtudományi Kutatóközpont, 2019. p. 61.
[236] Lásd például: Serbakov Márton Tibor: Legújabb tendenciák a terroristák internethasználatát illetően. In: Büntetőjogi Szemle Vol. 9, No. 2, 2020. p. 122-139., továbbá

– magába foglalja a terroristák internethasználatának azon típusait is, melyek nem kibertámadásokat valósítanak meg. E körben érdemes kiemelni a következő aktivitási pontokat:

- a terrorszervezetek finanszírozásának megoldása,
- toborzás,
- propaganda-anyagok közzététele,
- félelemkeltés,[237]
- etc.

A kriptovalutáknak a terrorizmus finanszírozásában betöltött szerepe, alkalmassága és az abban rejlő veszélyek a következő fejezetben kerülnek kifejtésre.

8.1.4. Az információtechnológia terrorista célú felhasználásának „hard" típusai, különös tekintettel a kritikus infrastruktúrákra jelentett kiemelt veszélyforrásokra

A konkrét kibertámadások tipizálása rengeteg szempont szerint történhet, melyben közre játszhat az elkövetők motivációja, célja, a bűncselekmény jellege, illetőleg a sértettek köre is. Nagy Zoltán tanulmányában különbséget tesz az egyéni felhasználók elleni tipikus támadások és a kritikus infrastruktúrák, más gazdasági – pénzügyi – igazgatási vállalkozások, politikai pártok elleni támadások között.[238]

Álláspontom szerint a terroristák kibertámadásainak potenciális célpontjainak mérlegelésekor kiemelt jelentőségű veszélyforrásként kell értékelni a kritikus infrastruktúrák[239], a

---

Serbakov Márton Tibor: Az utóbbi évek jelentős nemzetközi szélsőjobboldali terrorcselekmények elkövetőinek internethasználata és globális összefüggései. In: Jogelméleti szemle, Vol. 21, No. 3, 2020. pp. 60-69.

[237] Igen gyakori, hogy egyes terrorista csoportok audiovizuális felületeket használnák a propaganda és a félelemkeltés vagy éppen bizonyos társadalmi csoportok zsarolásának céljából. Ennek lehetséges megnyilvánulási formái között szerepel a kínzásokról, lefejezésekről, öngyilkos merényletekről vagy más terrorcselekményekről készült videófelvételek interneten történő közzététele is. Lásd részletesebben a témáról: Cano Paños, Op.Cit. pp. 14-16.

Az audiovizuális felületek szabályozásának egyes kérdéseiről lásd bővebben: Sorbán Kinga: A videomegosztó platformok európai szabályozásának aktuális kérdései. In: MÉDIAKUTATÓ: MÉDIAELMÉLETI FOLYÓIRAT Vol. 19, No. 1, 2018. pp. 9-20.

[238] Nagy Zoltán: Kiberbűncselekmények, kiberháború, kiberterrorizmus - avagy ébresztő Magyarország! In: Magyar Jog Vol. 63, No. 1, 2016. p. 20.

[239] A TANÁCS 2008/114/EK IRÁNYELVE (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről 2. cikk a)-b) pontjai rögzítik a kritikus infrastruktúra, illetőleg az európai kritikus infrastruktúra fogalmait. Ez alapján a kritikus infrastruktúra fogalma alá tartoznak *„a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban."* A fentitől szükséges elhatárolni az európai kritikus infrastruktúra (ECI) fogalmát, mely *„a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra. A hatás jelentőségét a horizontális kritériumok alapján kell értékelni. Ide tartoznak azok a hatások is, amelyek az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló kölcsönös függőségből erednek."*

létfontosságú rendszerelemeket, melyek védelmi szintjének megerősítése sürgető feladat, melynek során szükséges számolni az esetleges – akár terrorista szervezetek általi – kibertámadások bekövetkezésével. Természetesen előfordulhat, hogy a kiberterroristák egyéni felhasználókat is célba vesznek, ugyanakkor ezek szerepe a kiberterrorizmus szempontjából elenyésző, sokkal inkább a kibertérben elkövetett terrorizmus-finanszírozás körében fordul elő, mely az előző fejezetben került kifejtésre. Az előbbiek okán jelen fejezetben a kritikus infrastruktúrák védelmének vizsgálatára szorítkozik a szerző.

A 2012. évi CLXVI. törvény értelmében a létfontosságú rendszerelemek közé tartoznak az alábbi ágazatok valamelyikébe tartozó szolgáltatások, eszközök, létesítmények vagy rendszerek olyan rendszerelemei, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna:

- energia,
- közlekedés,
- agrárgazdaság,
- egészségügy,
- társadalombiztosítás,
- pénzügy,
- infokommunikációs technológiák,
- víz,
- honvédelem,
- közbiztonság-védelem.[240]

Ezek a rendszerelemek kiváltképpen vonzó célpontoknak minősülnek az egyes terrorista szervezetek számára, hiszen egy ilyen intézmény elleni kibertámadás sokkal jelentősebb károkat tud okozni egy állam szervezetében, illetőleg akár több áldozattal is járhat egy-egy ilyen rendszerelem kiiktatása vagy ideiglenes megbénítása.

8.1.4.1. Egészségügyi ágazat

[240] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény – 1. § j) pontjára figyelemmel a törvény – 1. melléklete

A kritikus infrastruktúrák közül a terrorszervezetek számára az egyik leginkább sebezhető rendszer az egészségügyi szektor, mely mind hazai, mind nemzetközi szinten potenciális veszélyforrás lehet. A kockázat valós, melyre példaként szolgálhat a wyoming-i Campbell County Health esete, mely 2019. szeptemberében egy zsarolóvírus-támadás áldozata lett. Ennek eredményeként a kórház nagyjából 8 órán keresztül egy több, mint 100 kilométerre található másik intézménybe kényszerült küldeni a betegeit, mivel a diagnosztikai rendszerek nagy része nem működött. A rendszer teljes helyreállítása 17 napot vett igénybe.[241] Egy másik hasonló eset történt Nagy-Britanniában is, ahol a National Health Service egészségügyi szolgáltató rendszerét érte támadás a WannaCry vírus által. Az incidens során nem csupán számítógépek, de MRI szkennerek, robotsebészeti rendszerek is érintettek voltak, egyes kórházakban pedig teljes szárnyakat kellett lezárni, műtéteket elnapolni.[242] Palicz et al. tanulmányukban kiemelik, hogy az egészségügyi szektort ért támadások által elszenvedett károk túlmutatnak a pénzügyi károkon (helyreállítási díj, reputációcsökkenés, stb.), a probléma másik részét az egészségügyi károk jelentik, melyek keretében számolni kell azzal, hogy a sürgősségi ellátásokat átmenetileg fel kell függeszteni. Emellett elképzelhető, hogy a betegek egészségügyi rekordjai átmenetileg vagy tartósan nem lesznek elérhetőek, a tervezett szolgáltatásokat (például műtéteket) el kell halasztani, a kórházi felvételeket fel kell függeszteni.[243] Az előbbi kimenetelek mind emberéletekbe kerülhetnek, így álláspontom szerint az egészségügyi intézmények informatikai (védelmi) rendszerének megerősítése elengedhetetlen.

8.1.4.2. Pénzügyi ágazat

Az egyes országok bank- és tőzsderendszerei, illetőleg a pénzügyi ágazat egésze egyike a leginkább védett infrastruktúráknak. Ennek egyik oka, hogy ezen szektor szereplőit érik a leggyakrabban támadások[244], hiszen a pénzügyi rendszer megbénításán, esetleges megsemmisítésén keresztül lenne a legkönnyebb egy állam padlóra kényszerítése, továbbá a támadások sokszor nem is feltétlenül terrorista célzatúak, egyszerűen csak vagyonszerzésre irányulnak. Ettől függetlenül azonban a terrorszervezetek által elkövetetett kibertámadásokkal

[241] Palicz Tamás; Sas Tibor; Tisóczki József; Bencsik Balázs; Joó Tamás: „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben. In: Orvosi Hetilap Vol. 161, No. 36, 2020. p. 1499.
[242] Déri Attila: Napjaink informatikai kihívásai - gondolatok a kritikus infrastruktúrák informatikai sérülékenységéről és védelméről. In: Rendvédelem Vol. 7, No. 1, 2018. p. 284.
[243] Palicz et al. Op.Cit. p. 1504.
[244] Jelen alfejezetben terjedelmi okokból csak a kiberterrorizmus szempontjából leginkább releváns jogesetek lettek kiemelve. A pénzügyi intézeteket ért jelentős kibertámadásokról lásd bővebben: Gulyás Olivér: A kiberbiztonság és a banki kibervédelem fejlődése napjainkig. In: Biztonságtudományi Szemle Vol. 4, No. 2, 2022. pp. 10-11.

ebben a szektorban is kell. Példaként szolgálhat az „orosz-észt kiberháborúként” emlegetett incidens. 2007 áprilisától májusáig egy orosz szervezet észt közintézményeket és bankokat célzott meg túlterheléses támadásokkal. A 128 regisztrált eset során 178 országból másodpercenként 100 megabyte-os forgalmat generáló támadásokat hajtottak végre az észt intézmények ellen. Az incidens eredményeként az állami intézmények internetes felületeinek nagy része megbénult, több állami intézményt le kellett kapcsolni a hálózatról, továbbá jelentős fennakadásokat tapasztaltak az online átutalások és fizetések rendszerében. A támadásokat 2009-ben vállalta magára egy, a Kreml által finanszírozott ifjúsági mozgalom.[245]

8.1.4.3. Energiaágazat

A létfontosságú rendszerelemek között kiemelt szerepe van az energiaellátást biztosító létesítményeknek. Az ágazaton legkritikusabb alrendszere az atomenergia, melynek vonatkozásában elegendő történelmi tapasztalattal rendelkezünk (például Csernobil-Pripjaty, Fukusima, stb.) ahhoz, hogy tudjuk, emberi ésszel felfoghatatlan károkat és pusztítást képes okozni, ha ezen rendszerek működését valami megzavarja, legyen az akaratlagos vagy véletlen. Ennek okán ebben az ágazatban erre az alszektorra fektetem a hangsúlyt.

Az atomerőművek szabályozása és a nukleáris energia nem tartozik a 2012. évi CLXVI. törvény hatálya alá, annak sokkal komplexebb biztonsági követelményeknek kell megfelelnie. Ezek közül az egyik legfontosabb jogforrás a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről szóló 1/2022. (IV. 29.) OAH rendelet. A rendelet rögzíti, hogy *„meg kell határozni az atomerőművi blokk irányítástechnikájával összefüggésben a mereven huzalozott - a félvezető alapú áramkörökkel gyártott logikákat beleértve - és a programozott eszközök megkülönböztetésével az informatikai és irányítástechnikai biztonság szempontjából kockázatot jelentő hozzáférések, valamint a funkció, a programok és az adatok módosításának fizikai lehetőségeit. Ezeket a lehetőségeket a megvalósíthatóság, valamint a módosítás eléréséhez szükséges szakértelem szintjének szempontjából sorrendbe kell állítani és ennek megfelelően kell a beavatkozásokat megtervezni.”*[246]

A rendelet III. fejezete tartalmazza az informatikai és irányítástechnikai biztonság tervezés követelményeit. Ennek 3a.4.5.5500. pontja alapján a fenti lehetőségeket mind az Előzetes

[245] Bányász Péter; Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. In: HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA Vol. 23, No. 1 (E-szám), 2013. pp. 191-192.

[246] 1/2022. (IV. 29.) OAH rendelet 3.4.5.3500. pontja, továbbá 3a.4.5.5500. pontja

Biztonsági Jelentésben, mind a Végleges Biztonsági Jelentésben meg kell határozni. Emellett detektálni kell a programozható eszközök rendellenességeit is. A rendelet előírja, hogy biztosítani kell azt, hogy a program és a konstans adatfájlok át nem írható adathordozóról beolvasott, installálás kor képzett megbízható adatok szerint ellenőrizhetőek legyenek. Ahol észszerűen megvalósítható, szükséges a technológiából beolvasott adatok vizsgálata.[247] További követelmény, hogy a védelmi és biztonsági rendszerekhez tartozó végrehajtó szerveket működtető, továbbá a nukleáris biztonság szempontjából fontos, az üzemeltető személyzet döntéseit befolyásoló adatokat gyűjtő és megjelenítő funkciókat ellátó rendszereket és eszközöket meg kell védeni a biztonsági funkció megváltoztatását vagy ellehetetlenítését elvileg lehetővé tévő külső informatikai befolyásolás ellen.[248] További biztonsági kritériumként jelenik meg a rendeletben az adminisztratív rendszer, a belső eljárások és a hozzáférések biztonsági protokolljának kidolgozása, mely magába foglalja a karbantartásokat, a digitális rendszerek módosításait, a feltárt program- és adathibák kijavítását, valamint az adathordozók ellenőrzését, ki- és beszállítását.[249] Az előbbiek mellett a konfigurációkezelésnek le kell fednie a rendszer és a rendszerelemek dokumentációját, a hardver dokumentációt, a szoftver dokumentáció és kód minden formáját, a fejlesztő rendszereket, a teszt-eseteket és eredményeket, a módosításokat és az azokhoz kapcsolódó elemzéseket, valamint az oktatási anyagokat is.[250]

A fokozott biztonsági intézkedések meghozatalában – a nukleáris katasztrófák történelmi tapasztalatai mellett – nagy szerepe volt az olyan eseteknek is, mint a 2010-ben, az iráni Natanz mellett kialakított urándúsító telepet ért kibertámadás. Az incidenst a Stuxnet nevezetű számítógépes vírus[251] okozta, mely – dacára a magas biztonsági óvintézkedéseknek – képes volt bejutni a vezérlő informatikai rendszerbe és átvenni felette az irányítást. A vírus nagyjából 1000 gázcentrifugát tett tönkre, mellyel évekre visszavetette Irán atomprogramját.[252] A program képes volt megváltoztatni a gázcentrifugák áramellátásának frekvenciáját, melynek eredményeként azok felváltva magas és alacsony sebességen kezdtek el működni, mely nagyban eltér a rendeltetésüktől, mivel nem erre lettek tervezve, így könnyen tönkrementek.[253]

---

[247] 3a.4.5.5600. pont
[248] 3.4.5.3700. pont, továbbá a 3a.4.5.5700. pont
[249] 3a.4.5.5900. pont
[250] 3a.4.5.6000. pont
[251] Ralph Langner a Stuxnet vírus és az iráni incidens körülményeinek beható elemzését készítette el, melyről lásd részletesebben: Langner, Ralph: To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. München, The Langner Group, 2013. Elérhető: https://www.cs.yale.edu/homes/jf/Langner.pdf (2023.12.17.)
[252] Bányász; Orbók, Op.Cit. pp. 203-204.
[253] Farwell, James P.; Rohozinski, Rafal: Stuxnet and the Future of Cyber War, Survival Vol 53, No. 1, 2011. pp. 24-25.

Szerencsére az incidens során nem történt nukleáris robbanás, illetőleg radioaktív anyagok sem kerültek a környezetbe, ugyanakkor könnyen lehetett volna az esetnek tragikus kimenetele, mely intő jelként szolgál a jövőre nézve.[254] A lehetséges pusztító hatás mellett továbbá mindenképpen számolni kell egy ilyen támadás politikai vetületeivel a nemzetközi közéletben. Egy, az iránihoz hasonló támadás beláthatatlan következményekkel járhat, akár egy nagyobb horderejű háború kitöréséhez is vezethet.[255]

Egy Szaúd-Arábiában történt eset szintén példaként szolgálhat az energiaszektort ért kibertámadások terén. A Saudi Aramco nemcsak a térség, de az egész világ egyik legnagyobb olajvállalata. 2012-ben a cég malware-támadást szenvedett. Ennek eredményeként a „Shamoon" névre keresztelt malware a vállalat mintegy 30.000 számítógépének a merevlemezét törölte le teljes mértékben. Ez az Aramco számítástechnikai eszközeinek mintegy ¾-ed részét tette ki. A vállalat rendszerének helyreállítása az incidenst követően nagyjából két hétbe telt és rendkívüli anyagi károkat okozott. Az esemény mégis „szerencsésnek" mondható, mivel a malware nem érte el a termelést irányító SCADA-rendszert, mely még nagyobb károkat okozhatott volna, illetőleg adott esetben akár emberéletekbe is kerülhetett volna.[256]

Az előbbi példák mellett kiemelendő továbbá egy Magyarországhoz sokkal közelebb álló eset. A NotPetya névre hallgató vírust 2017-ben észlelték először. Lényege, hogy a WannaCry vírushoz hasonlóan az EthernalBlue sérülékenységet használja ki. A vírus elsősorban Ukrajna, Oroszország és Lengyelország területét érintette. Veszélyességét jelzi, hogy a vírus által megfertőződött például az ukrán miniszterelnök-helyettes számítógépe, több pénzintézet (köztük az Ukrán Nemzeti Bank és az ukrán OTP-lányvállalat) rendszere, továbbá – ami a leginkább letaglózó, – a csernobili atomerőmű állapotát felügyelő rendszer is.[257]

8.1.4.4. Közlekedési ágazat

[254] Jogosan veti fel a kérdést Bányász és Orbók, hogy – figyelemmel a Stuxnet azóta detektált, továbbfejlesztett változataira, – milyen következményekkel jár a fenomén a kiberbiztonságra nézve. Ennek fényében a kritikus infrastruktúrák kiberfenyegetettségének a szerzőpáros is kiemelt jelentőséget tulajdonít. Lásd: Bányász; Orbók, Op.Cit. p. 205.

[255] A fenti álláspontot több szerző is osztja, kiváltképpen az iráni Stuxnet-támadás fényében. Lásd például: Collins, Sean; McCombie, Stephen: Stuxnet: the emergence of a new cyber weapon and its implications, Journal of Policing, Intelligence and Counter Terrorism, Vol 7, No. 1, 2012. p. 88.

[256] Cath Senker: Cybercrime and the Darknet. Revealing the hidden underworld of the internet. Arcturus Holdings Ltd., London, 2017. p. 102.

[257] Déri, Op.Cit. p. 288.

A közlekedés szektora a fentiek közül talán a leggyakrabban érintett a terroristatámadások során, hiszen e szektor biztonsági protokolljait a legnehezebb a külső behatások által immunissá tenni. A történelem során mindig is célpontot jelentettek a közlekedési eszközök, legyen szó egy postakocsi kifosztásáról vagy egy gőzvonat eltérítéséről, de akár a Közel-Keleten egy-egy autó vagy busz felrobbantása is gyakori. A repülés mindennapossá válásával a támadások a légi járműveket is megkörnyékezték, melynek eddigi legjelentősebb megnyilvánulása a 2001. szeptember 11. napján történt terrorcselekmények voltak, mely a repülésbiztonság teljes átértelmezését vonzotta maga után, talán nem túlzás kijelenteni, hogy az egész világon. A technológiai fejlődés azonban e téren is újkeletű veszélyforrásokat rejt magában, ugyanis a 2020-as évekre elértük azt a fejlettségi szintet, hogy a járművek nagy csoportja (repülőgépek[258], gépkocsik, drónok, stb.) fejlett számítógépes rendszerrel rendelkeznek. Ezek további célpontokként szolgálhatnak a terrorista csoportok kibertámadásai számára.

A fentiek mellett további kockázatokat rejthet magában az egyes (GPS-alapú) alkalmazások használata is. Bányász Péter tanulmányában kiemeli, hogy a katonai műveletek (közúti szállítások) vonatkozásában az ilyen alkalmazások (például Google Maps vagy a Street View) komoly biztonsági kockázatokat jelenthet.[259] Álláspontom szerint hasonlóképpen szükséges értékelni ezeket az alkalmazásokat a kritikus infrastruktúrák körébe tartozó intézmények tekintetében is, így a személyi állomány okostelefon-használatát – amennyiben egyes intézmények még nem írnak elő erre vonatozó szabályozást – olyan szinten kell korlátozni, hogy az a lehető legkevesebb veszélyforrással járjon a kiemelt védelmet igénylő létfontosságú rendszerelem vonatkozásában.

8.1.5. Megállapítások

Az elmúlt nagyjából húsz évben megjelent tanulmányok áttekintését követően levonható azon következtetés, miszerint az egyes szerzők meglehetősen különböző álláspontón vannak a kiberterrorizmus jelenségének a létezésével kapcsolatban, annak büntetőjogi megítélése pedig még megosztóbb a tudományos közösségben. Ez a megosztottság jellemzi a kiberterrorizmus elkövetési módjainak, a valószínűsíthető célpontjainak, illetve további körülményeinek megítélését is.

[258] A légi közlekedés kapcsán felmerülő informatikai támadások kockázatáról lásd bővebben: Balogh Regina: A légiközlekedés biztonsági kihívásai és kockázatai, a velük szembeni terrortámadások elleni védelem követelményei és módszerei. In: Hadtudományi Szemle Vol. 10, No. 3, 2017. pp. 468-469.

[259] Bányász Péter: A közlekedést támogató alkalmazások biztonsági aspektusai. In: Horváth Attila; Bányász Péter; Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. Budapest, Nemzeti Közszolgálati Egyetem (NKE), 2014. p. 57.

Sánchez Medero úgy vélekedik, hogy a kiberterrorizmus és a kiberbűnözés a 21. század legnagyobb fenyegetései közé tartoznak, melyekkel meg kell küzdenünk.[260]
Bányász szerint leggyakrabban a védelmi ipari cégek, különösen a kis- és középvállalkozások a kibertámadások célpontjai, melynek okaként ezen vállalkozások vélhetően kevesebb költségvetéséből fakadó informatikai biztonsági protokoll hiányát jelöli meg. Ezt követően, a kisebb védelmi ipari szereplőkön keresztül az elkövetők eljuthatnak a nagyobb cégekhez is.[261]
Ez a faktor mindenféleképpen közrejátszik a kritikus infrastruktúrák közé tartozó létesítmények ellen elkövetett támadások vonatkozásában is, hiszen bizonyos intézmények – anyagi források hiányában – nem rendelkeznek megfelelő biztonsági szintű informatikai védelmi rendszerrel, az egyes adatbázisok, számítástechnikai rendszerek sokszor elavultak, így könnyebben „találnak rést a pajzson" az elkövetők. Le kell szögezni azonban, hogy nem csupán a kis- és középvállalkozások vannak kitéve a közvetlen fenyegetettségnek, a kritikus infrastruktúra intézményei, a magasabb biztonsági szintű intézmények és a nagyvállalatok ugyanúgy ki vannak téve a közvetlen támadásoknak. Ezt kellően alátámasztják a fentebb felsorolt példák is, melyeket a kritikus infrastruktúrák összes elemét veszélyeztetik, így álláspontom szerint szükségszerű a létfontosságú rendszerelemek kiberbiztonságának megerősítése, egyes esetekben a biztonsági rendszerek és protokollok teljes újragondolása.

8.2. A csalások új elkövetési formái

8.2.1. Áttekintés

Az online csalások rendkívül változatos és kreatív formákat ölthetnek. Ezek közül a leggyakoribbak – a teljesség igénye nélkül – az alábbiak:

- szerelmi csalások,
- hamis aukciós felületek,
- malware-csalások,
- kártékony spam üzenetek,
- hamis vagy nem létező áruk adásvétele,
- hamis állásajánlatok,
- befektetési csalások,

[260] Sánchez Medero Op.Cit. p. 85.
[261] Bányász Péter: A közösségi médiahasználat biztonsági kérdései a védelmi iparban. In: HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA Vol. 24, No. 1, 2014. p. 64.

- személyiséglopás bizonyos formái,
- felhasználói fiókok feltörése.[262]

A fentiek szükséges megemlíteni bizonyos offline jellegű csalásokat, melyek szintén kötődhetnek a kibertérhez (pl.: a bankkártya csalások egyes esetei).

A csalások sikerességének viktimológiai jellegű vizsgálatakor több faktort és ezáltal többféle magyarázatot kell figyelembe venni. Egyrészről szerepet játszik a „nagy számok törvénye", főként a kártékony spam üzenetek (például Facebook Marketplace-n, e-mailen vagy más platformokon) történő terjesztése. Minél nagyobb közegből merítenek az elkövetők, annál valószínűbb, hogy egyesek áldozatául fognak válni a csalásnak. Kiemelt sértetti kör lehet az idősebb, kevesebb informatikai ismerettel rendelkező korosztály is.

Egy másik körülmény, amit érdemes figyelembe venni viktimológiai szempontból a szégyen és a félelemérzet. Bizonyos típusú csalások (tipikusan ilyenek a szerelmi csalások, szexuális jellegű csalások) meglehetősen nagy szégyenérzetet keltenek az áldozatokban, mely sokszor – a félelem miatt, hogy lebuknak (például egy házasságtörő kapcsolat miatt vagy egy fel nem vállalt szexuális kapcsolat miatt,) hajlamosak mindent megtenni, hogy elkerüljék a számukra szerencsétlen végkimenetelt.[263] Ezen bűncselekmények tekintetében – érthető okokból – magasabb látenciáról is beszélünk, hiszen a nyomozó hatóságok tudtára sem szívesen hozzák az áldozatok ezeket a kényes információkat.

Statisztikai szempontból vizsgálva a csalások hazánkban meglehetősen számottevő bűncselekménytípusnak számítanak. A csalással okozott károk igencsak jelentős mértékűek, továbbá folyamatosan növekvő tendenciát mutatnak. Ezt támasztja alá, hogy míg 2012-ben az összes bűncselekménnyel okozott kár 18,4%-át tették ki a csalások, úgy 2017-re már ez az érték elérte a 27,9%-ot.[264]

Szintén kiemelendő, hogy az elkövetők rendkívül gyorsan és hatékonyan tudják lekövetni az egyes társadalmi és környezeti változásokat, ezzel új köntösbe burkolva a csalások régi, már jól bevált válfajait. Kiváló példa erre a jelenségre a COVID-19 járvány okozta helyzet, melynek során a csalók számtalan új forgatókönyv szerint tudták átírni a „régi recepteket".[265]

---

[262] Mark Button; Carol McNaughton Nicholls; Jane Kerr; Rachael Owen: Online Frauds: Learning from Victims Why They Fall for These Scams. In: Australian and New Zealand Journal of Criminology Vol. 47, No. 3, 2014. pp. 397-399.

[263] Op.Cit. p. 402.

[264] Krasznay Csaba; Simon Béla: Kiberbűncselekmények az online kereskedelemben. In: Hadmérnök Vol. 12, No. 2 „KÖFOP-különszám", 2017. p. 125.

[265] A koronavírus-világjárvánnyal kapcsolatos online csalásokról lásd bővebben: Mostafa Saidur Rahim Khan; Yoshihiko Kadoya: Who Became Victims of Financial Frauds during the COVID-19 Pandemic in Japan? In: Sustainability Vol. 15, No. 4, 2023. pp. 1-17.

8.2.2. Bankkártya-csalások

A leggyakrabban elkövetett bankkártyával kapcsolatos csalások a következők:

- bankkártya-hamisítás,
- elveszett vagy lopott bankkártyák használata,
- hamis weboldalak vagy alkalmazások által megszerzett bankkártya-adatok felhasználása,
- felhasználói fiókok feltörése,
- kereskedői oldalról elkövetett csalások.[266]

A büntető törvénykönyvünk rendszerében a különböző bankkártyákat – utalva a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvényre (röviden Hpt.-re)[267] – a készpénz-helyettesítő fizetési eszköz, mint gyűjtőfogalom tartalmazza. A Btk. fogalommeghatározása szerint *„készpénz-helyettesítő fizetési eszköz a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett”*.[268] Ehhez társul a Btk. 459. § (1) bekezdésének 20. pontjában rögzített elektronikus készpénz-helyettesítő fizetési eszköz, mely az előbbi fogalmat kiterjeszti továbbá a kincstári kártyára és a személyi jövedelemadóról szóló törvény felhatalmazása alapján kiadott elektronikus utalványra, feltéve, hogy ezek információs rendszer útján kerülnek felhasználásra.

A Btk. az alábbi tényállásokat tartalmazza a készpénz-helyettesítő fizetési eszközök vonatkozásában:

- készpénz-helyettesítő fizetési eszköz hamisítása,[269]
- készpénz-helyettesítő fizetési eszközzel visszaélés,[270] illetve a
- készpénz-helyettesítő fizetési eszköz hamisításának elősegítése.[271]

---

[266] Adrian Cristian Moise: Types of Bank Cards Related Frauds. In: Journal of Law and Public Administration Vol. 2, No. 4, 2016. pp. 115-119.

[267] A Hpt. 6. § (1) bekezdésének 55. pontja alapján készpénz-helyettesítő fizetési eszköz a csekk, az elektronikus pénz, a pénzforgalmi szolgáltató és az ügyfél közötti keretszerződésben meghatározott olyan személyre szabott dolog vagy eljárás, amely lehetővé teszi az ügyfél számára a fizetési megbízás megtételét.

[268] Btk. 459. § (1) bekezdésének 19. pontja

[269] Btk. 392. §

[270] Btk. 393. §

[271] Btk. 394. §

A fentiek mellett a kódex a lopás tényállásának minősített esetként rögzíti a készpénz-helyettesítő fizetési eszköz egyidejű elvételével történő elkövetést.[272]

A kibertérben elkövetett bankkártyás visszaélésekkel kapcsolatosan hazai jogeset is a rendelkezésünkre áll. A KR NNI Kiberbűnözés Elleni Főosztály az Europol segítségével beazonosított egy magyar állampolgárt, aki korábban az Alphabay nevű dark webes kereskedelmi felületen hozzávetőlegesen 390 darab bankkártya-adatot vásárolt meg. A nyomozó hatóság és az Europol munkájának eredményeként sikerült beazonosítani az elkövető egy másodlagosan használt e-mail címét, melyet egy magyar középiskolában regisztráltak. A nyomozás során sikerült továbbá meghatározni az elkövető lakóhelyét is, így lehetőség nyílt arra, hogy a nyomozó hatóság kutatást foganatosítson. Ennek keretében összesen 7454 darab, nagyrészben külföldön kibocsátott VISA és MasterCard kártyákat sikerült beazonosítani. Végeredményben a terheltet 7844 rendbeli elektronikus készpénz-helyettesítő fizetési eszközön tárolt adat jogosulatlan megszerzésével elkövetett készpénz-helyettesítő fizetési eszközzel visszaélés vétségével sikerült meggyanúsítani.[273]

8.2.3. Távoli hozzáférést biztosító programokkal (alkalmazásokkal) elkövetett csalások

A távoli hozzáférést lehetővé tévő programok fokozatos elterjedésével – melyhez nagymértékben hozzájárult a koronavírus-járvány és az egyre általánosabb otthoni munkavégzés (az ún. home office) – igencsak megszaporodott az ilyen programok kriminális felhasználása. Az ilyen jellegű csalásoknak számtalan formája létezik, jelen tanulmányban a gyakorlatban leggyakrabban előforduló módozatok áttekintése a cél. Ennek érdekében mindenekelőtt adekvátnak tartom e programok működésének általános áttekintését.

Az úgynevezett távoli asztal alkalmazások (szoftverek) – ahogy a nevükből is következtethetünk rá – lehetővé teszik, hogy egy számítógép asztali környezetét lássuk viszont egy másik számítógépen (okostelefonon, szerveren, stb.). Az alkalmazás hozzáférést biztosít az első számítógépen tárolt adatokhoz, továbbá lehetővé teszi ezen eszköz irányítását is. Ehhez a folyamathoz azonban elengedhetetlen egy ilyen szoftver telepítése mind a két (az irányító és az irányított) eszközre is, továbbá mindkét számítógép esetében szükséges az internetkapcsolat biztosítása is.[274] A leggyakrabban használt távoli asztal alkalmazások a TeamViewer[275], illetve

[272] Btk. 370. § (2) bekezdésének be) pontja

[273] Hertelendi Lajos: Egy dark weben elkövetett bűncselekmény felderítésének tanulságai, a nemzetközi összefogás jelentősége. In: Belügyi Szemle Vol. 70, No. 3, 2022. pp. 615-616.

[274] Margaret Rouse: Remote Desktop Software.
Elérhető: https://www.techopedia.com/definition/29710/remote-desktop-software (2022.09.19.)

[275] https://www.teamviewer.com/en (2022.09.19.)

az AnyDesk[276], ugyanakkor számos hasonló ingyenes és fizetős szoftver elérhető a piacon, melyek funkciói kisebb eltérésekkel ugyan, de tulajdonképpen azonosak.
Az ilyen alkalmazásoknak ugyanakkor léteznek maliciózus változatai is, melyet a felhasználók nem önszántukból telepítenek az eszközeikre, hanem egy ún. trójai vírus *(Remote Access Trojan, röviden RAT)* segítségével, a felhasználók tudtán kívül kerülnek a számítógépekre, emellett gyakran megpróbálnak elrejtőzni a sértettek elől. Ezek a rosszindulatú alkalmazás egyfajta „hátsó ajtót" biztosítanak a sértett eszközén, így az a támadónak szinte teljeskörű adminisztratív hozzáférést biztosít az adott eszközhöz. Az elkövető számára a RAT programok használata a lehetőségek tárházát nyitja meg, melynek keretében megvalósulhat a teljesség igénye nélkül:

- a felhasználó tevékenységeinek nyomon követése különböző kémprogramok, billentyűnaplózó alkalmazások által,
- adathalászat, információlopás,
- csatlakoztatott vagy beépített webkamera elindítása és azon keresztül mozgó- és állóképek rögzítése,
- képernyőfotók készítése,
- fájlokkal történő műveletek végzése (törlés, módosítás, telepítés, stb.).[277]

8.2.3.1. A távoli asztal alkalmazások bűncselekményekre történő felhasználása

Ennél az esetkörnél az elkövetők olyan számítógépes szoftvereket, illetve alkalmazásokat használnak fel a bűncselekmény elkövetéséhez, melyek ab origine nem kriminális felhasználásra készültek (pl.: AnyDesk, TeamViewer, stb.). Az ilyen alkalmazásoknak rengeteg felhasználási módja lehet, akár ügyeleti jellegű vagy egyéb irodai munkaköröknél. A bevezetőben taglaltakhoz visszanyúlva tehát, az ilyen alkalmazások lényege voltaképpen az, hogy távoli hozzáférést biztosítson a felhasználók számára az egyik eszközről a másikhoz. A gyakorlatban, az esetek túlnyomó részében az elkövetők – általában előzetes adathalászat (phishing) útján begyűjtött adatok alapján – telefonhívások útján veszik fel a kapcsolatot a csalások sértettjeivel. Az elkövetők ilyenkor gyakran valamelyik közismert bank (OTP, Raiffeisen, K&H Bank, stb.) munkatársaként mutatkoznak be a sértetteknek, akiket alkalmanként akár név szerint keresnek fel, ezzel is tovább növelve a sértett bizalmát a vélt

[276] https://anydesk.com/en (2022.09.19.)
[277] Kinza Yasar: RAT (Remote Access Trojan).
Elérhető: https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan (2022.09.19.)

ügyintéző személyazonosságával kapcsolatban. A csaló által előadott történet lényege, hogy a sértett folyószámlájáról gyanús átutalás(oka)t fedeztek fel, mivel a kedvezményezetthez több állítólagos bűncselekmény is köthető. A tranzakciókat ugyanakkor meg tudják szüntetni, de ehhez azonnali intézkedésre van szükség, melynek keretében a sértettet ráveszik egy távoli hozzáférést biztosító szoftver letöltésére és telepítésére. A felhasználót rábírják, hogy az alkalmazásban egy kód megadásával csatlakozzanak és ezáltal engedélyezzék számukra a hozzáférést. Ezt követően utasításokat adnak a sértettnek, hogy lépjen be az adott bank internetes (netbank) felületére, melyet az alkalmazáson keresztül nyomon követnek és a megfelelő pillanatban elvégzik az általuk tervezett tranzakciókat. Általában nem csak a számítógép, hanem az okostelefon vonatkozásában is kérik, hogy a sértett telepítse az egyik távoli elérést lehetővé tévő alkalmazást, így amennyiben az érintett felhasználónak be van állítva az SMS jóváhagyó (ún. aláíró) funkció a tranzakciókhoz, az elkövetők már az SMS érkezésének pillanatában látják a kapott kódot. A csalás utóbbi változatánál, illetve a műveletsor ezen része általában akképpen valósul meg, hogy az alkalmazásnak a sértett mobilkészülékére történő telepítését követően az elkövető – a sértett alapvető személyes adatainak birtokában – kezdeményezi a sértett szolgáltatójánál az adott készülékhez tartozó SIM kártya cseréjét. Az ilyen csalásokat nevezik többek között ún. „SIM SWAP" – csalásoknak is.[278]

Az ilyen bűncselekmények vonatkozásában szükségszerű a felhasználók széleskörű tájékoztatása. Ennek során különös figyelmet kell fordítani azokra a csoportokra, melyek az ilyen jellegű csalások leginkább potenciális áldozatai lehetnek (tehát jellemzően a legidősebb és a legfiatalabb korosztályok). Érdemes az egyes csalások különböző elkövetési módjainak mellett felhívni a figyelmüket a feljelentés relevanciájára is. Fontos megjegyezni, hogy sokszor nem csak külföldi, de magyar hívóazonosítójú telefonszámokról is próbálkoznak az elkövetők, így ezek bejelentése érdemi segítséget nyújthat a nyomozó hatóságok számára más, hasonló cselekmények miatt folyamatban lévő büntetőeljárások felderítésének előmozdítására.

8.2.3.2. A távoli hozzáférést biztosító trójai vírusok (RATs)

A távoli elérést lehetővé tévő trójai vírusok olyan rosszindulatú szoftverek, melyek különféle mértékű hozzáférést tesznek lehetővé az elkövetők számára a sértettek eszközeihez. A fentebb részletezett – exemplifikatív jelleggel felsorolt – felhasználási módjaik meglehetősen nagy

[278] Póczik Szilveszter; Sárik Eszter; Vass Péter; Bolyky Orsolya: A COVID-19 pandémia egyes kriminológiai aspektusai. In: Belügyi Szemle Vol. 69, No. 3, 2021, p. 385.

veszélyt jelentenek, számos különféle bűncselekmény részcselekményét képezhetik. Az ilyen programokat a legtöbb esetben e-mail üzenetekben vagy a közösségi média különböző platformjain küldött üzenetekben terjesztik az elkövetők. Az üzeneteket a jóhiszemű felhasználók megnyitják, melynek során az adott fájl letöltése és telepítése is végbe mehet. A terjesztésük egy másik lehetséges módja a Java Downloader-en keresztül történik. Ezekben az esetekben a felhasználó által látogatott bizonyos weboldalak megnyitásakor a Java kódokat a felhasználó eszköze letölti, majd a kódok az eszközön – a sértett tudta nélkül – aktiválódnak.[279]

8.2.4. Az online apróhirdetési felületeken elkövetett csalások egy elkövetési módjáról

Krasznay és Simon tanulmányukban felhívják a figyelmet egy, az online apróhirdetési portálokon felmerült, egyre gyakrabban használt elkövetési módra, melynek lényege, hogy az elkövető lényegében kifizetteti az általa kiszemelt árucikkek értékét a sértettel. Ennek során az elkövető a kiszemelt árucikk eladójával üzenetben veszi fel a kapcsolatot, majd megállapodik az áruval kapcsolatban abban, hogy előre utalással fizeti ki a terméket. Ehhez az elkövető elkéri az eladó bankszámlaszámát és telefonszámát. Közben az elkövető felveszi a kapcsolatot egy vevővel is, akivel szintén előre utalásos fizetésben állapodnak meg, melyhez az elkövető megadja a tényleges eladó banki adatait. Amint a vevő elküldi az elkövetőnek az átutalási megbízásról készült képernyőfotót, az elkövető azt sajátjaként továbbítja a tényleges eladó felé, majd közli vele, hogy intézte a futárt, aki sokszor ő maga vagy valamely ismerőse. Mire a felháborodott vevő felveszi a kapcsolatot a tényleges eladóval – aki természetesen jogosan állítja, hogy a terméket átadta a futárnak, – a termék már régen az elkövetőhöz került. A szerzőpáros kiemeli, dacára annak, hogy túlságosan körülményes egy ilyen jellegű csalást megszervezni, meglehetősen nagy potenciál van ebben az elkövetési módban, ugyanis igen nehéz a felderítése ezeknek a bűncselekményeknek, továbbá a módszer még tovább csiszolható, tökéletesíthető, így a jövőben várható, hogy e modus operandi gyakrabban elő fog fordulni a gyakorlatban.[280]

8.2.5. Szerelmi csalások az online térben

[279] Ilker Kara; Murat Aydos: The Ghost in the System: Technical Analysis of Remote Access Trojan. In: International Journal on Information Technologies & Security Vol. 11, No. 1, 2019, p. 75.
[280] Krasznay; Simon, 2017, Op.Cit. pp. 133-134.

A felgyorsult, globalizált világ egyik nagy hozománya, hogy a romantikus céllal történő ismerkedés – sok más tevékenységgel együtt – átkerült a kibertérbe. Ennek a pszichológiai oldala meglehetősen komplex. Az online randialkalmazások népszerűségében számos tényező játszik szerepet:

- *kényelem:* az emberek az otthonuk kényelméből tudnak társas kapcsolatokat kezdeményezni, kiépíteni, akár adott esetben olyan emberekkel is, akik lakóhelyük földrajzi elhelyezkedése, munkájuk, illetőleg egyéb elfoglaltságaik miatt nem tudnának a személyes párkeresésben effektíven részt venni,
- *kevesebb visszautasítás:* alapvetően megállapítható, hogy a randialkalmazások különböző szűrőinek használatával az érdeklődési köreinknek, egyéb társadalmi és személyi preferenciáinknak megfelelően, célirányosan tudjuk szűrni a lehetséges partner-jelölteket, így – a nagy számok törvénye alapján – kevesebb negatív élményben, visszautasításban, kudarcban lehetne részünk (legalábbis az elképzelés szerint),
- *pozitív visszacsatolás – önigazolás – önmegerősítés:* az ilyen alkalmazások zöme arra az alapra épül, hogy valamilyen mechanizmussal tetszésünket tudjuk kifejezni egy másik személy profilja iránt. Legyen szó szívekről, like-okról vagy csillagozásról, esetleg valami hasonló „jutalmazó" metódusról, ezek mind egy séma mentén működnek, veszélyességük pedig abban jelentkezik, hogy meglehetősen könnyen függőséget okoznak.

Az online társkereső oldalak népszerűségével a csalók is észlelték a terület nyújtotta potenciált és egyre jobban elterjedtek az ún. szerelmi csalások (romance frauds). A csalás ezen formájának a lényege, hogy az elkövető egy online randialkalmazáson kreált álprofillal felveszi a kapcsolatot a kiszemelt (általában elkeseredett, sebezhető) áldozatával. A kommunikáció során meglehetősen gyorsan megpróbálja elhitetni az áldozattal, hogy mély érzéseket táplál iránta, szerelmes az áldozatba. E szerelem ugyanakkor csak plátói lehet, hiszen valamilyen (pénzügyi) oknál fogva sajnos a csaló nem tud személyesen találkozni az áldozattal. Az indokokat tekintve számtalan verzió létezik, az egészen egyszerűektől (például az elkövetőnek nincsen pénze utazni) a már hihetetlen történetekig (például az elkövetőnek másik országba kell költöznie, egészségügyi problémái vannak).

A romantikus átverésekkel kapcsolatban az Amerikai Egyesült Államok Magyarországi Nagykövetsége honlapján közzétett egy felhívást, melyben óvatosságra int az online társkeresés kapcsán. E honlapon közzétette a gyanúsnak számító körülményeket, melyek szerelmi csalás gyanújára adhatnak okot. Ezek a teljesség igénye nélkül az alábbiak:

- az adott személy túl hamar szerelmet vall, gyengéd megszólítással illeti a másik felet, pedig még sohasem találkoztak egymással,
- azt állítja, hogy békefenntartóként dolgozik, szülei, felesége már nem élnek, gyermekére pedig más vigyáz,
- biztonsági okokra hivatkozva kerüli, hogy telefonon vagy videóhívásban beszéljenek,
- azt ígéri, hogy egy diplomatával küld valamit (például ékszert, pénzt, stb.),
- valamiért soha nem sikerül telefonon vagy videóhívásban beszélniük, azt állítja, hogy nincsen postai vagy email címe,
- nyelvtani és helyesírási hibákkal vannak tele az üzenetei,
- azt kéri, hogy küldjenek neki vagy valamilyen harmadik személynek pénzt.[281]

8.2.6. Adathalászat / Phising

A 21. század legnagyobb értéke az adat, legyen az személyes adat, pénzügyi adat, egészségügyi adat vagy más, az elkövetők ezért számtalan módot találnak rá, hogy kicsikarják azt az áldozatokból. Az adathalászat, vagyis az ún. phising során az elkövetők hivatalos szervek, pénzügyi intézmények, ismert szervezetek weboldalait másolják le azzal a céllal, hogy felhasználói azonosítókat és jelszavakat, valamint bankkártya-adatokat szerezzenek meg. Az elkövetők sokszor emailen vagy a közösségi oldalak felületein küldik szét a hamis weboldalak linkjeit, sokszorosítva ezzel a sértettek körét.[282]

9. A kriptovaluták, avagy a büntető anyagi és eljárásjog Achilles-sarka

9.1. A kriptovaluták körében előforduló fogalmak

A kriptovaluták technológiai és jogi aspektusból történő megértéséhez az egyes fogalmak tisztázása nyújthat segítséget.

A kriptovaluták fogalmát tekintve több hasonló megoldást is találhatunk. *Glavanits és Király (2018)* a következő definíciót emelte ki: *„a kriptovaluták olyan decentralizált digitális valuták, melyek nem minősülnek törvényes fizetőeszköznek, de csereeszközként vagy fizetőeszközként általánosan elfogadnak és használnak, és amelyet nem egy központi bank, állami hatóság,*

[281] U.S. Embassy Budapest: Vigyázat! Romantikus átverések.
Elérhető: https://hu.usembassy.gov/hu/vigyazat-romantikus-atveresek/ (2024.03.10.)
[282] Simon Béla; Gyaraki Réka: Kiberbűnözés. In: Kiss Tibor (szerk.): Kibervédelem a bűnügyi tudományokban. Budapest, Dialóg Campus Kiadó, 2020. p. 107.

hanem egy fejlesztő/fejlesztői csapat bocsát ki, szabályoz és kontrollál, valamint kriptográfiát használ az új kriptovaluta egységek kibocsátására, tárolására és a tranzakciók rögzítésére."[283]
Az egyes országok részéről egyre nagyobb az igény a kriptovaluták szabályozására, mely egyfajta szabályozási hullámot indított el a 2010-es évek végétől, a 2020-as évek elejétől. Olyannyira, hogy a fenti definíció már módosításra szorul, hiszen akadnak olyan országok, ahol bizonyos kriptovaluták (például El Salvadorban a Bitcoin) a jog által elismert, törvényes fizetőeszközzé vált.[284] *A kriptovaluta tehát a valuták bármely olyan formája, amely digitálisan vagy virtuálisan létezik, és kriptográfiai titkosítást használ a tranzakciók biztonságára.* A kriptovaluták nincsenek központi kibocsátó, szabályozó hatóság vagy központi bank alá rendelve, ehelyett decentralizált rendszert használnak a tranzakciók rögzítésére és az új egységek kibocsátására.[285] A kriptovaluták alapvetően két csoportra oszthatóak: a saját blokklánccal rendelkező ún. „coin"-okra, illetve a már meglévő blokkláncra épülő ún. „token"-ekre. Az előbbit ugyancsak tovább lehet bontani a Bitcoin-ra és az alternatív kriptovalutákra, azaz „altcoin"-okra. A nyílt forráskódú kriptovaluták, mint a Bitcoin, azzal az előnyös tulajdonsággal járnak, hogy a szofver kódjának megváltoztatására is bárkinek meg van a lehetősége. Ennél fogva az így létrehozott egyes kriptovaluták újabb tulajdonságokkal ruházhatóak fel. [286] A másik nagy csoport, vagyis az ún. tokenek nem rendelkeznek saját blokklánccal, hanem más kriptovaluták (coin-ok) blokkláncát használják fel. Ennek forgalomba hozatalához meghirdetik a kezdeti érmekibocsátást (Initial Coin Offering, röviden ICO)[287] egy ún. fehér könyv (white paper) formájában. Ez a közösségi finanszírozás egy új formájaként fogható fel a kriptovaluták világában.[288]
A kriptovaluták vonatkozásában továbbá érdemes tisztázni az alábbi meghatározó jelentőséggel bíró fogalmakat:

[283] Glavanits Judit; Király Péter Bálint: A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége. In: JOG ÁLLAM POLITIKA: JOG- ÉS POLITIKATUDOMÁNYI FOLYÓIRAT Vol. 10, No. 3, 2018, p. 179.
[284] Decreto nº 57.
Lásd bővebben: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2020-2029/2021/06/E75F3.PDF (2021.06.08.)
[285] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency (2023.06.20.)
[286] Bugár Gyöngyi; Somogyvári Márta: Bitcoin: digitális szemfényvesztés, vagy a jövő valutája? In: Hitelintézeti Szemle Vol. 19, No. 1, 2020. pp. 137-138.
[287] A fogalmat egyes szerzők gyakran az IPO-hoz (Initial Public Offering) hasonlítják, ugyanakkor lényeges különbség, hogy míg az IPO esetében a tőke előteremtéséhez eladják az adott vállalkozás tulajdonjogát (részvényeit), addig az ICO esetében a befektetők nem vásárolják meg a kriptovaluta részvényeit, tulajdonjogát, az ICO-t pusztán tőketeremtő mechanizmusként használják a projekt korai szakaszában. Lásd bővebben: Germán Péter: A kriptopiac legveszélyesebb befektetése - Mi is az az ICO? Elérhető: https://cryptofalka.hu/blokklanc/mi-az-ico (2024.03.08.)
[288] Ibid.

- *bitcoin:* kriptovaluta, mely olyan peer-to-peer technológiát használ, mely folyamatban a közvetítő szerepet a központi bank helyett a felhasználók egy csoportja látja el, általuk kerülnek kibocsátásra új bitcoinok és ők hitelesítik a tranzakciókat. A konstrukció nyilvános, nyílt forráskódú, bárki által szabadon használható és/vagy módosítható.[289]
- *blokklánc (blockchain):* megosztott nyilvántartási könyv, a tranzakciókat tartalmazó decentralizált adatbázis, amely többszáz, többezer számítógépen nyilván van tartva. Az adatok blokkokra vannak tagolva, amelyek egyedi azonosítóval (időbélyegzővel és digitális aláírással) vannak ellátva. Az újabb blokkok úgy jönnek létre, hogy a megelező blokkhoz kriptografikus eljárással egy új blokkot kapcsolnak, amelyet a rendszert használó többi szereplő hitelesít. A validációt követően a láncban résztvevők adatbázisai megmásíthatatlan és visszavonhatatlan módon frissülnek.[290] Az egyes adatok hitelesítése tehát peer-to-peer módon történik, magyarán bármilyen közvetítő intézmény vagy személy nélkül.[291]
- *központi banki digitális valuta (central bank-issued digital currency, röviden CBDC):* olyan centralizált digitális valuták, melyek törvényes fizetőeszköznek minősülnek és csereeszközként vagy fizetőeszközként általánosan elfogadnak és használnak, és amelyeket egy központi bank bocsát ki, szabályoz és kontrollál.[292]
- *kriptovaluta-bányászat:* a kriptobányászat biztosítja az olyan kriptovaluták biztonságát és decentralizációját, mint a Bitcoin, amelyek Proof-of-Work (PoW) konszenzusmechanizmuson alapulnak. A bányászat egy kritikus elem, amely lehetővé teszi, hogy a rendszer központi hatóság nélkül tudjon működni. E folyamat során az ún. bányászok a felhasználók tranzakcióit hitelesítik és hozzáadják a blokklánc nyilvános főkönyvéhez. Ehhez a bányászoknak összetett matematikai problémákat kell megoldania, amelyek sok számítási erőforrást igényelnek. Minden sikeresen kibányászott blokkért a bányászok újonnan létrehozott kriptovalutákból és tranzakciós díjakból álló blokkjutalmat kapnak kompenzáció gyanánt.[293]
- *kriptovaluta-tárcák (wallet-ek):* a kriptovaluták tárolására használatos módszerek összefoglaló neve. A kriptovaluta-tárcák alábbi típusai ismertek:
    - *mobiltárcák,*

[289] https://bitcoin.org/hu/ (2023.06.20.)
[290] Gábor Tamás; Kiss Gábor Dávid: Bevezetés a kriptovaluták világába. In: Gazdaság és Pénzügy Vol. 5, No. 1, 2018. 38. o.
[291] Glavanits; Király, 2018, Op.Cit. p. 174.
[292] Glavanits; Király, 2018. Op.Cit. p. 178.
[293] https://academy.binance.com/hu/articles/what-is-crypto-mining-and-how-does-it-work (2023.06.20.)

    - *asztali tárcák,*
    - *online tárcák,*
    - *hardveres tárcák,*
        - *Ledger USB tárca.*
        - *Trezor tárca,*
    - *papíralapú tárca.*[294]
- *stablecoin: olyan kriptovaluta, melynek értéke egy adott valutához, áruhoz vagy pénzügyi eszközhöz van kötve, s melynek célja, hogy alternatívát nyújtsanak a nagy volatilitású kriptovaluták mellett.*[295]

9.2. A kriptovaluták megjelenési formái a „hagyományos" bűncselekmények esetében

Az elmúlt két évtizedben egy hihetetlen mértékű globalizációs folyamat és egy minden eddigi elképzelést felülmúló technológiai fejlődés tanúi lehettünk, melynek eredményeként számottevő változások következtek be – többek között – a szervezett bűnözés[296] megjelenési formáiban is. A Bitcoin 2008/2009-es megjelenésével a kriptovaluták terén keletkezett vacuum iuris, dacára az azóta eltelt 13 hosszú évnek, a mai napig kitöltetlenül maradt, szabályozásuk tekintetében sokszor még a fogalmi meghatározások szintjén sem sikerül megegyezésre jutnia a terület kutatóinak. A megosztottságon és a szakmai ellentéteken alapuló szabályozatlanság – sajnálatosan – a bűnelkövetőknek kedvez, hiszen a kriptovaluták használata által nyújtott bizonyos fokú anonimitást kihasználva jelentősen megkönnyítik bizonyos bűncselekmények, kiváltképp a kiberbűncselekmények[297] elkövetését. Ahogyan a gyakorlati tapasztalat is mutatja, a kriptovalutákat számottevő mértékben használják fel illegális ügyletek[298] (fegyverkereskedelem, kábítószerkereskedelem) megkötésére a dark web-en, emellett egyéb –

[294] https://www.bitcoinbazis.hu/utmutato/hogyan-taroljuk-bitcoint/ (2024.03.06.)
[295] Adam Hayes: Stablecoins: Definition, How They Work, and Types.
Elérhető: https://www.investopedia.com/terms/s/stablecoin.asp (2024.03.08.)
[296] A szervezett bűnözésről lásd bővebben: Kőhalmi László: Szervezett bűnözés. In: Barabás A. Tünde: Alkalmazott kriminológia. Budapest, Ludovika Egyetemi Kiadó, 2020, pp. 461-474., továbbá
Tóth Mihály; Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea; Gönczöl Katalin; Kerezsi Klára; Lévay Miklós (szerk.): Kriminológia. Budapest, Wolters Kluwer Kft., 2016. pp. 603-625., illetve
Tóth Dávid; Gál István László; Kőhalmi László: Organized Crime in Hungary. In: Journal of Eastern-European Criminal Law Vol. 2, No. 1, 2015, pp. 22-27.
[297] Lásd bővebben: Torma Adrienne; Bendes Ákos: Cybercrime, a jelen és a jövő kihívásai. In: Szabó Csaba (szerk.): Tavaszi Szél 2018 (Spring Wind 2018), Budapest, Doktoranduszok Országos Szövetsége (DOSZ), 2018. pp. 256-268.
[298] Példaként említhető a Ross Ulbricht által működtetett Silk Road nevezetű weboldalon évekig folytatott illegális kábítószer-kereskedelem, melynek keretein belül tipikusan kriptovalutákban foganatosították a tranzakciókat. A Silk Road-dal kapcsolatban lásd bővebben: https://www.investopedia.com/terms/s/silk-road.asp, (2021.01.18.)

a társadalomra veszélyes[299] - illegális szolgáltatások ellenértékeként is felhasználásra kerülnek (gyermekpornográfia[300], bérgyilkosságok). A kriptovaluta-ökoszisztéma[301] fejlődésével mára már az informatika terén a felhasználói szintű tudást minimálisan meghaladó képességek birtokában bárki bevásárolhat ezekből a valutákból, értékük jelentős növekedést mutat és egyre nagyobb stabilitással bírnak, jelenlétük akár a pénzügyi kultúra[302] szervezés részévé is válhat a jövőben, mely jelenség felvetette a pénzmosásra, illetve a terrorizmus finanszírozására történő felhasználásuk kockázatát, melyet az Európai Unió intézményei is felismertek.

9.2.1. A kriptovaluták pénzmosásra történő felhasználása

Az Európai Unió hatodik pénzmosás elleni irányelve előtt állva, az eddigi tapasztalatok pedig azt mutatják – a kriptovaluták szemszögéből – hogy az uniós minimumszabályozás nem minden téren tud kielégítő választ nyújtani a pénzmosással kapcsolatos aggályokra, emellett a nemzeti szinten történő szabályozásra sem mutatkozott hajlandóság az elmúlt évtized folyamán. A kriptovaluták szabályozatlan helyzetének bűnelkövetők általi kihasználása és a folyamatosan növekvő tendenciát mutató kiberbűnözés indokolja a jogalkotás mihamarabbi válaszát. Az alábbi fejezet ezen problémák áttekintésére és az orvoslásukra tett javaslatokra fókuszál.

9.2.1.1. Az Európai Unió eszköztára a pénzmosás elleni küzdelemben

Az intézményi oldalt tekintve, a pénzmosás elleni küzdelem uniós vetületeiben kiemelkedő szerepe van az Europol-nak, melynek fő feladata ebben a tekintetben hírszerzési és igazságügyi támogatás nyújtása a tagállamok számára a nemzetközi pénzmosási tevékenységek megelőzése

[299] A bűncselekmények egyik alapvető ismérvéről, a társadalomra veszélyességről lásd bővebben: Kőhalmi László: A büntetőjog alapproblémái. Pécs, PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, 2012.

[300] Lásd bővebben: Torma Adrienne; Bendes Ákos: A cybercrime és a gyermekpornográfia összeolvadása. In: Bendes Ákos; Nagy Melánia; Tóth Dávid (szerk.): Lépést tud-e tartani a jog a XXI. század kihívásaival? Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Doktori Iskola, 2019. pp. 5-29.

[301] Lásd bővebben a kriptovaluta-ökoszisztéma kapcsán felmerülő problémákról: Bujtár Zsolt: A kriptovaluta ökoszisztéma szabályozási kihívásai. In: Benke József; Fabó Tibor (szerk.): A puro pura defluit aqva. Ünnepi tanulmányok Nochta Tibor professzor 60. születésnapja tiszteletére. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2018, pp. 61-72.

[302] Lásd bővebben a pénzügyi kultúráról: Szívós Alexander: Az adórendszer és a pénzügyi kultúra összefüggései. In: Szilovics Csaba; Bujtár Zsolt; Ferencz Barnabás; Breszkovics Botond; Szívós Alexander Roland (szerk.): GAZDASÁG ÉS PÉNZÜGYEK A 21. SZÁZADBAN II. - KONFERENCIAKÖTET = BUSINESS AND ECONOMY IN THE 21ST CENTURY II. – CONFERENCE PROCEEDINGS. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2020. pp. 52-64.

és leküzdése érdekében.[303] Az Europol keretein belül több olyan szervezeti egység is működik, melyek a pénzmosás elleni uniós fellépésben aktívan részt vesznek:

- A „Europol Criminal Assets Bureau" (röviden ECAB), amely lényegében az Europol bűnügyi vagyonokat kezelő irodája. Feladata a tagállamok joghatóságán kívül elrejtett bűncselekményekből származó vagyoni eszközök felkutatásában történő támogatás nyújtása. Ezen a szervezeti egységen belül működik a „Camden Asset Recovery Inter-Agency Network" (vagy röviden CARIN), mely a fentebb említett vagyoni eszközök lefoglalásával, kezelésével, illetve elkobzásával járul hozzá az ECAB munkájához.[304]
- Az „Anti-Money Laundering Operational Informal Network" (röviden AMON) egy nemzetközi nyomozókból álló informális hálózat, melyet 2012-ben hoztak létre, célja pedig a nemzetközi együttműködés meglévő jogi kereteinek javítása és optimalizálása a pénzmosás területén.[305]
- A fentiek mellett szintén az Europol keretein belül működik egy ún. pénzügyi bűnözéssel foglalkozó információs központ („Financial Crime Information Centre" vagy röviden FCIC), mely egy, a pénzmosással, vagyon-visszaszerzéssel és bűnügyi hírszerzéssel foglalkozó nyomozók számára biztosított webes felület, amely lehetővé teszi számukra a biztonságos információcserét, illetve egyfajta kommunikációs csatornaként szolgál a nyomozók között.[306]
- 2020 júniusában megalakult (szintén Europol kezdeményezésre) a „European Financial and Economic Crime Centre" (röviden EFECC), mely a pénzügyi- és gazdasági bűnözés – így többek között a pénzmosás – elleni küzdelem szellemében létrehozott intézmény, mely egyszerre funkcionál információs hálózatként, illetve operatív támogatást nyújtó szervként. Megalakulása óta az EFECC otthont ad többek között a CARIN és az AMON titkárságának, emellett közreműködik a FIU.net és más tanácsadó szervekkel, illetve szoros együttműködést folytat az OLAF-al.[307]

Az Europol pénzmosással is foglalkozó szervezeti egységei mellett szintén említést érdemel, hogy a 2018-2021-es EU szakpolitikai ciklus („EU Policy Cicle") is kiemelt ügyekként kezeli többek között a számítógépes bűnözés[308], a szervezett bűnözés, illetve a bűncselekményekből

[303] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering, (2021.01.19.)
[304] Ibid.
[305] Ibid.
[306] Ibid.
[307] Ibid.
[308] A számítógépes környezetben elkövetett bűncselekmények napjainkban nagyobb súllyal bírnak a gazdasági élet szempontjából, mint eddig bármikor, ezért kiemelten fontosnak tartom a számítógépes bűncselekmények,

származó vagyon és a pénzmosás[309] elleni küzdelmet. A szakpolitikai ciklus egy négy fázisból álló folyamat, melynek első lépése a szervezett bűnözés jelentette veszélyek felmérésére irányul. A felmérés („The Serious and Organised Crime Threat Assessment", röviden SOCTA) ajánlásokat fogalmaz meg, mely alapján meghatározhatóak az adott szakpolitikai ciklus prioritásai. A SOCTA alapján készül el egy több éves stratégiai terv, melyet egy tényleges operatív terv követ. A ciklus végül egy értékelő szakasszal zárul, melynek során az EMPACT ciklus elemzését végzik el a szakemberek (szintén a SOCTA-t alapul véve). Ennek során áttekintésre kerülnek a ciklus eredményei, illetve hibái is, ami alapján a későbbiekben eszközölhetőek lesznek a ciklusra vonatkozó módosítások.[310]

A jogszabályi oldal vonatkozásában megállapítható, hogy bár a 2018/1673/EU irányelvben is rögzítésre került a virtuális fizetőeszközök pénzmosásra történő felhasználásának kockázata, az irányelv (a minimálszabályozás indokának hangsúlyozásával) a tagállamokra hárítja a virtuális fizetőeszközökkel kapcsolatos, e téren kilátásban lévő kockázatok kezelését és érdemben nem foglalkozik a terület szabályozásával. A virtuális valutákra vonatkozó további iránymutatást Az Európai Parlament és a Tanács (EU) 2018/843 a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról szóló irányelvben találhatunk. A direktíva a virtuális fizetőeszközök tekintetében a 2015/849/EU irányelv[311] hatályának kiterjesztését szorgalmazza a virtuális fizetőeszközök és rendeleti pénzek közötti átváltási szolgáltatásokat nyújtó szolgáltatókra és a letétkezelő pénztárca-szolgáltatókra.[312]

A probléma a fenti uniós irányelvekkel – a kriptovaluták szabályozásának szemszögéből – legfőképpen az, hogy az Európai Unió nem foglal teljes mértékben állást a szabályozás irányát illetően, hanem megmarad a minimumszabályozás mellett. Ez több jogterületnél járható út lehet, ám jelen esetben problémát jelenthet, főként a határokon átnyúló szervezett bűnözés szempontjából – amely a kriptovaluták esetében jelentős részében közrejátszik – az országonként eltérő jogi minősítés (pl.: a kriptovaluták jogi meghatározása). Az irányelvek a tagállamok között is megosztottságot váltottak ki, több állam nem is tudta megfelelő időn belül

---

illetve elkövetési módok megismerését. A számítógépes bűnözéssel kapcsolatban lásd bővebben: Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Budapest, Ad Librum, 2009.

[309] A szervezett bűnözés gazdasági vonatkozásairól és a pénzmosásban betöltött szerepéről lásd bővebben: Szendrei Ferenc: A szervezett bűnözés gazdasági háttere és a pénzmosás. In: Magyar Rendészet Vol. 18, No. 5, 2018. pp. 77-91.

[310] https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, (2021.01.19.)

[311] Az Európai Parlament és a Tanács (EU) 2015/849 irányelve a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről, a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról, valamint a 2005/60/EK európai parlamenti és tanácsi irányelv és a 2006/70/EK bizottsági irányelv hatályon kívül helyezéséről

[312] 2018/843/EU (8) bekezdése

végrehajtani az implementálást (köztük Magyarország sem), néhány tagállam pedig a kellőnél szigorúbb szabályozást vezetett be. Utóbbira példaként szolgálhat Németország esete, ahol is nagy port kavart a negyedik uniós pénzmosás elleni módosító irányelv implementálására szolgáló törvény[313] 2020. január 1-jei hatályba lépése, amely a kriptovaluták és rendeleti pénzek közötti átváltási tevékenységet folytató szolgáltatók tevékenységét új pénzügyi szolgáltatásként határozta meg[314], illetőleg minden ilyen szolgáltató vállalkozásnak engedélyezetetési eljárást kell kezdeményeznie a BaFin-nál (Német Szövetségi Pénzügyi Felügyeleti Hatóság).[315] A másik fontos változás, hogy a kriptovalutákat bizonyos feltételek teljesülése esetén pénzügyi eszközként kategorizálták. Ezek a konjunktív feltételek a következők:

- nem egy közösségi vagy központi intézmény által kerülnek kibocsátásra[316],
- jogilag nem esnek a fizetőeszközök, rendeleti pénzek kategóriájába,
- magán-, illetve jogi személyek is felhasználhatják, fizetésre vagy árucserére,
- befektetési célokat szolgálnak, és
- a tárolásuk, a velük történő kereskedelem és a továbbításuk elektronikusan történik.[317]

9.2.1.2. A pénzmosás hazai szabályozása[318]

A pénzmosás közgazdasági értelemben olyan legális gazdasági műveletek leplezése alatt folytatott illegális gazdasági szolgáltatás, amelynek eredményeként a bűncselekménnyel szerzett vagyon eredete igazolhatóvá válik, megszabadulva annak felismerhetően jogellenes mivoltától, illetve büntetőjogi szempontból pedig ennek bármely részmozzanata kimeríti a pénzmosás tényállását.[319] A jelenleg hatályos Büntető Törvénykönyvünk[320] (Btk.) a XL.

[313] Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie
[314] A szabályozás a Német Banktörvény (Kreditwesengesetz – KWG) módosításaként került szabályozásra.
[315] https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Zulassung/Kryptoverwahrgeschaeft/kryptoverwahrgeschaeft_node_en.html, (2021.02.15.)
[316] Tehát a Központi Bank által kiadott ilyen valuták már nem esnek a szabályozás alá. A CBDC-ről lásd bővebben: Bujtár Zsolt: Central bank-issued digital currencies: - ready, steady, go? In: Szilovics Csaba; Bujtár Zsolt; Ferencz Barnabás; Breszkovics Botond; Szívós Alexander Roland (szerk.): GAZDASÁG ÉS PÉNZÜGYEK A 21. SZÁZADBAN II. - KONFERENCIAKÖTET = BUSINESS AND ECONOMY IN THE 21ST CENTURY II. – CONFERENCE PROCEEDINGS. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2020. pp. 113-123.
Bujtár Zsolt: Central bank issued digital currencies: is it a solution or a problem? In: Glavanits Judit; Horváthy Balázs; Knapp László (szerk.): EU Business Law and Digital Revolution: Selected Studies from New Fields of Technology. Győr, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, 2019. 71-89. o.
[317] https://kriptoakademia.com/2020/03/04/nemetorszag-a-bitcoin-torvenyes-penzugyi-eszkoz, (2021.02.15.)
[318] A pénzmosás elleni küzdelem történetének hazai vonatkozásairól lásd bővebben: Gál István László: 25 Years of Fight Against Money Laundering in Hungary. In: Journal of Eastern-European Criminal Law Vol. 6, No. 2, 2019. pp. 62-71.
[319] Gál István László: A pénzmosással és a terrorizmus finanszírozásával kapcsolatos jogszabályok magyarázata. HVG-ORAC Lap- és Könyvkiadó, Budapest, 2012. p. 19.
[320] 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.)

fejezetet szentelte a pénzmosásnak. A 399.§-ban a jogalkotó a következő elkövetési magatartásokat rögzíti:

a) a büntetendő cselekményből származó vagyon eredetének, a vagyonon fennálló jognak, a vagyon helyének, ezek változásának elfedése vagy elleplezése,
b) a büntetendő cselekményből származó vagyon eredetének, a vagyonon fennálló jognak, a vagyon helyének, ezek változásának elfedése vagy elleplezése céljából a vagyon mástól történő átvétele, elrejtése, átalakítása, átruházása, felhasználása, az elidegenítésében való közreműködés, pénzügyi tevékenység végzése vagy pénzügyi szolgálatás igénybevétele azzal összefüggésben, illetve az arról történő rendelkezés,
c) a b) pontban felsorolt cselekményekkel a mással szembeni vagyonelkobzás, illetve vagyonvisszaszerzés meghiúsításában közreműködés, vagy a mással szembeni vagyonelkobzás, illetve vagyonvisszaszerzés meghiúsítására törekvés,
d) a más által elkövetett büntetendő cselekményből származó vagyon megszerzése, megőrzése, elrejtése, kezelése, használata, felhasználása, átalakítása, átruházása, elidegenítésében közreműködés vagy rendelkezési jogosultság szerzése a vagyon felett.[321]

A fenti elkövetési módok mellett a Btk. a gondatlan alakzatot is büntetni rendeli, amely vétséget két évig terjedő szabadságvesztéssel szankcionál.[322]

A minősítő körülmények tekintetében a jogalkotó egyrészről az értékhatárok megállapítására alapozta a szabályozást. Ennek értelmében a tényállás alapesetét meríti ki a bűncselekmény, amennyiben a pénzmosást jelentős értéket meg nem haladó értékre követik el. Emellett minősítő körülményként értékeli az üzletszerű elkövetést, a hivatalos személy minőségben történő elkövetést, illetve amennyiben az elkövető a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvényben meghatározott szolgáltatóként[323], annak tisztségviselőjeként vagy alkalmazottjaként a szolgáltató tevékenységével összefüggésben követi el a bűncselekményt.[324]

A régi Btk[325]-hoz képest jelentősen változott a pénzmosás tényállásának büntetőjogi

[321] Btk. 399. §
[322] Btk. 400. §
[323] A Pmt. által felsorolt szolgáltatók közé tartoznak – többek között – az ügyvédek is. Lásd bővebben az ügyvédek és a pénzmosás kapcsolatát:
Kőhalmi László: Ügyvédek és pénzmosás. In: Gál István László (szerk.) A pénzmosás elleni küzdelem aktuális kérdései. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2005. 89-97. o.
Józan Flóra – Kőhalmi László: Lawyers and Money laundering. In: Journal of Eastern-European Criminal Law Vol. 3, No. 2, 2016. pp. 130-136.
[324] Btk. 399. §
[325] 1978. évi IV. törvény a Büntető Törvénykönyvről

meghatározása. A bűncselekmény tárgya a régi szabályozásban a büntetendő cselekményből származó dolog volt, melyet felváltott a büntetendő cselekményből származó vagyon. A vagyon fogalmának a pénzmosás szempontjából releváns meghatározását (az új szabályozással implementált) Az Európai Parlament és a Tanács (EU) 2018/1673 a pénzmosás ellen büntetőjogi eszközökkel folytatott küzdelemről szóló irányelvében[326] találhatjuk, eszerint a vagyon alatt értendő mindennemű vagyoni eszköz, beleértve az anyagi vagy eszmei, ingó vagy ingatlan, materiális vagy immateriális javakat, valamint bármilyen formájú olyan jogi dokumentum vagy okirat, ideértve az elektronikust és digitálist is, amely bizonyítja az ilyen vagyoni eszközökhöz fűződő jogcímet vagy a bennük lévő érdekeltséget.

9.2.1.3. A kriptovaluták a pénzmosás tükrében

Ahogyan az a fentiekben említésre került, már évekkel ezelőtt felmerült a kriptovaluták pénzmosásra történő felhasználásának lehetősége. Az elmúlt évtized során számtalan tanulmány foglalkozott a blokklánc technológián alapuló virtuális fizetőeszközök bűnözők – különösen a szervezett bűnözés - általi felhasználásával, hiszen számos tulajdonságuk kedvező lehet számukra. Használatukhoz legtöbb esetben nem szükséges megadni személyes adatokat, illetve a szolgáltatók nem igénylik a személyazonosító okmányok általi azonosítást az új regisztrációk során, illetve nem is végeznek ügyfél-átvilágítási eljárásokat. Ennek fényében tehát – az anonimitás nagyfokú megőrzése mellett – bárki rendelkezhet kriptovalutákkal, aki rendelkezik egy e-mail címmel. Az anonimitás tehát mindenféleképpen egy kedvező karakterisztikája a kriptoeszközöknek a pénzmosásra történő felhasználást tekintve. Erre példaként szolgálhat a Liberty Reserve névre keresztelt Costa Rica-i származású kriptovaluta-szolgáltató, melynek pénzmosási tevékenységre történő felhasználásának eredményeként dollármilliárdokat (USD) mostak tisztára.[327] A rendszer hatalmas számokkal operált, több, mint 200.000 felhasználóval rendelkezett csak az Egyesült Államok területén. 2013 májusában az Egyesült Államok Igazságügyi Minisztériuma vádat emelt a Liberty Reserve céggel szemben[328], az elsőfokú határozat az üggyel kapcsolatban 2014 decemberében lett

[326] Lásd bővebben a negyedik uniós pénzmosás elleni irányelvről: Gál István László: The 4th EU Directive and the Hungarian AML Practice in 2018. In: Pavlović, Zoran (szerk.): Yearbook. Human Rights Protection: "From Unlawfulness to Legality", Novi Sad, Institute of Criminological and Sociological Research, 2018. 349-360. o.
[327] Alan Brill; Lonnie Keene: Cryptocurrencies: The Next Generation of Terrorist Financing? In: Defence Against Terrorism Review Vol. 7, No. 1, 2014. pp. 18-20.
[328] Valeriia Dyntu; Oleh Dykyi: Cryptocurrency in the System of Money Laundering. In: Baltic Journal of Economic Studies No. 5, 2018. p. 79.

meghozva.[329]

Problémát jelenthet továbbá a kriptovaluták és a rendeleti pénzek közötti átváltási szolgáltatók pénzmosásban betöltött szerepe is. Rossen G. Iossifov és az általa működtetett RG Coins esete kiváló példaként szolgálhat az ilyen szolgáltatók pénzmosási tevékenységére. A bolgár állampolgár RG Coins néven folytatott kriptovaluták és fiat pénzek közti átváltási szolgáltatást, amelynek tevékenységének során fő ügyfelei a Romániából operáló „Alexandriai Online Aukciós Csalások Hálózata" (Alexandria Online Auction Fraud Network, röviden AOAF Network) nevű bűnszervezet tagjai voltak, akiknek a fő tevékenysége az Egyesült Államok állampolgárait célzó, aukciós oldalakon (pl.: Craigslist-en vagy Ebay-en) folytatott csalások voltak. A csalást valótlan hirdetések közzétételével követték el, majd az amerikai állampolgároktól kicsalt pénzeket kriptovalutákra váltották, majd olyan átváltási szolgáltatókhoz küldték, mint Iossifov, aki amellett, hogy nem futtatta át ügyfeleit semmilyen azonosítási folyamaton (személyazonosító okiratok bekérése, a pénz eredetére vonatkozó információ kérése), kedvezményes átváltási árfolyamot kínált az AOAF Network tagjai számára. A folyamat közel 3 évig tartott, mialatt Iossifov közel 5 millió amerikai dollárnak megfelelő összeget mosott tisztára kriptovaluták felhasználásával, az Egyesült Államok Kerületi Bírósága ezért 10 év letöltendő börtönbüntetésre ítélte az 53 éves bolgár elkövetőt.[330]

Szintén előnyös tulajdonságként értékelendő a pénzmosási tevékenységre történő felhasználást tekintve a kriptovaluták magas likviditása. A rendelkezésre álló különféle ún. mixerek (kriptovaluták egymás közötti átváltását lehetővé tévő programok) segítségével a kriptovaluták könnyedén keverhetők, váltogathatók egymásra, illetve a legtöbb fiát pénznemre való átváltásuk is lehetséges. Az ilyen mértékű és gyorsaságú valuta-váltások szintén problémát okozhatnak a nyomozó hatóságoknak, hiszen a legtöbb esetben a kriptovaluta-rendszerekbe történő befizetésekből és a rendszerből a fiát pénzek rendszerébe történő kilépésből próbálnak kiindulni, viszont a rendszeren belül történő változások nyomon követése sokkal több erőforrást igényelne. Az Europol égisze alatt működő SIRIUS-projekt e rendszeren belül nyújt rendkívüli segítséget az egyes tagországok nyomozó hatóságai és igazságügyi szervei számára. E projekten belül az egyes szolgáltatók által elvárt formanyomtatványokat, a megkeresések (adatkérések) követelményeit gyűjtötték össze, ugyanakkor megemlítendő, hogy sok kriptovaluta szolgáltató csak kifejezetten csekély mértékben, hosszú reakcióidővel vagy

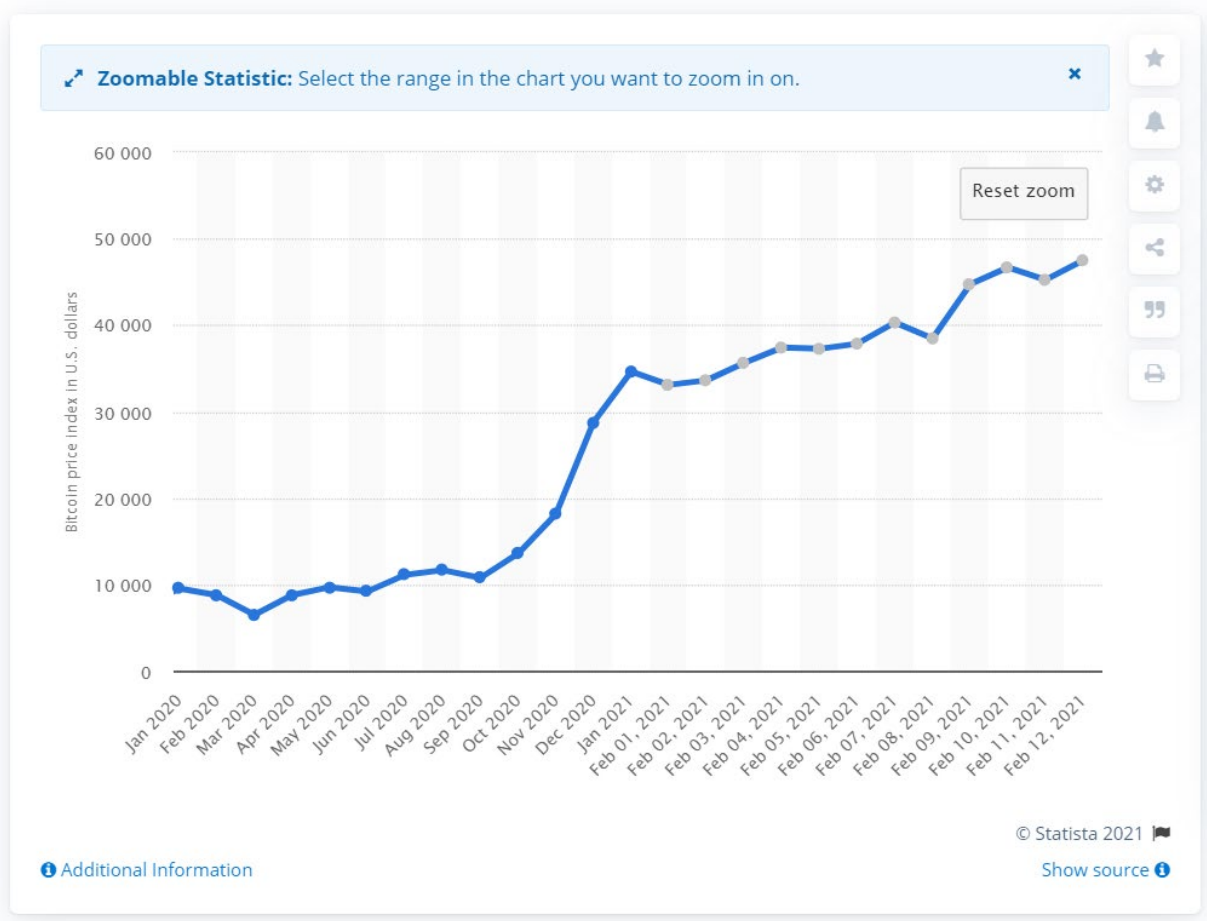
[329] A US v. Liberty Reserve et al. ügyről lásd részletesebben: https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2014/us_v_liberty_reserve_et_al..html, (2021.01.28.)
[330] https://www.justice.gov/opa/pr/owner-bitcoin-exchange-sentenced-prison-money-laundering, (2021.01.29.)

abszolút nem működik együtt a hatóságokkal (például a Monero), így ezekben az alrendszerekben a nyomozó hatóságok fonalat tudnak veszteni.

Érdemes megemlíteni továbbá az egyes online videójátékokat, melyek szintén közreműködhetnek a pénzmosásban. Az elkövetők által különösen kedveltek a World of Warcraft-hoz hasonló, online, ún. MMORPG („massive multiplayer online role-playing game", magyarul masszív, többszereplős, online szerepjáték) kategóriába tartozó játékplatformok, melyek saját „fizetőeszközzel" rendelkeznek, s melyeket világszerte több tízmillióan használnak napi szinten. Az elkövetők e játékokban több különböző profilt létrehozva bevásárolnak a játék fizetőeszközéből, majd azt akár fiatvalutákra, akár kriptovalutákra válthatják, ilyen módon átmosva azt.[331]

A kriptovaluták legnagyobb problémája a bűnelkövetők szemszögéből a stabilitás hiánya. Ezen tulajdonságuk ugyanakkor több problémakört is hordoz magában. Egyrészről a bűnelkövetők egy bizonyos köre is szkeptikusan áll a kriptoeszközökhöz, hiszen jelentős összegeknél még egy kisebb infláció lehetősége is hatalmas károkat tud okozni, a kriptovaluták árfolyamainak kilengései pedig olykor drasztikus méreteket ölthetnek. Ez természetesen nem riasztja vissza a nagyobb kockázatot vállaló, vakmerőbb bűnözőket, de a bűnelkövetők bizonyos hányadát ugyanakkor visszatartja a vagyon elvesztésének lehetősége az adott kriptovaluta esetleges összeomlását követően. Másrészről szintén problémát okoz az árfolyamok jelentős változása a lefoglalás, illetve a vagyonelkobzás szempontjából, ugyanis amennyiben a bűncselekmény felderítése megtörtént, kérdéses lehet a büntetendő cselekményből származó vagyon és az árfolyamváltozások során keletkezett többlet elhatárolása. Példának említhető a Bitcoin árfolyama, amely csak 2020. januárja és 2021. februárja között a négyszeresére nőtt (lásd 1. ábra). Tegyük fel, hogy egy bűnelkövető 2020. januárjában vásárolt 10.000 USD értékű Bitcoint büntetendő cselekményből származó pénzen. Az árfolyam drasztikus növekedésének eredményeként 2021. februárjára már 40.000 USD értékű Bitcoin-nal rendelkezett.

[331] Dornfeld László: Pénzmosás a kibertérben. In: Farkas Ákos; Dannecker Gerhard; Jacsó Judit (szerk.): Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre. Budapest, Wolters Kluwer Kft., 2019. pp. 456-457.



4. ábra: A Bitcoin árfolyamának változásai 2020. január és 2021. február között. Forrás: https://www.statista.com/statistics/326707/bitcoin-price-index/, 2021.02.13.

Amennyiben a fent említett bűnelkövető Bitcoin-számláján szereplő összeg lefoglalására, illetve vagyonelkobzásra kerül a sor, felmerül több kérdés. Egyrészről, kiterjeszthetőek-e a büntetendő cselekményből származó vagyon hasznaira is a kényszerintézkedések, nevezetesen például a vagyonelkobzás? Egyfelől logikus megoldása lehetne a kérdésnek a lefoglalt Bitcoin – akár árverés útján, akár más úton történő – értékesítése, így a befolyt összegből kielégíthetőek lehetnének a sértettek, illetve az eljárási költségek, ugyanakkor kérdéses a fentmaradó összeg problémája. A másik oldalról szemlélve azonban, ha az adott kriptovaluta – tehát jelen esetben a Bitcoin – éppen úgymond „leszállóban van" és a töredékét éri a befektetett összegnek, evidens, hogy az értékesítés során befolyt összeget a bűnelkövetőnek kell kiegészítenie, így ésszerű lenne, ha a fennmaradó összeg is visszaszolgáltatásra kerülne, hiszen az üzleti lépés – jelen esetben a Bitcoin-ba történő befektetés – az ő ötlete volt, tehát a haszon végeredményben az ő tevékenységének eredménye. Másrészről motivációként hathatna a bűnelkövetőkre a folyamat, hiszen – ha a fenti példát vesszük alapul – a sértettek kielégítése és az eljárási költségek megfizetése után fennmaradó összeg – amennyiben visszaszolgáltatásra kerülne –

még így is jelentős haszont képezne.

A fentiek tükrében megállapítható tehát, hogy a kriptovaluták pénzmosási tevékenységre történő felhasználása – egyelőre – nem veszélytelen, hiszen a kiszámíthatatlan árfolyam-ingadozások a bűnelkövetők számára is rizikófaktorként értékelendők, habár meg kell említeni, hogy ez természetesen nem minden bűnözőt riaszt el az ilyen célú felhasználásuktól. Ez a tény ugyanakkor nem jelenti azt, hogy a jövőben nem válik majd bevett gyakorlattá a kripto-alapú pénzmosás, hiszen – a Bitcoint vagy az Ethert alapul véve – elmondható, hogy egyre nagyobb számú felhasználóval rendelkeznek a rendszerek, melyek nagy mértékben befolyásolják ezen kriptoeszközök stabilitását és amennyiben ez a szabályozatlansággal jelenlegi fokával társul, komoly problémákat fog okozni.

Szorgalmazandó tehát egy nemzeti szintű kriptoeszközökre szakosodott felügyeleti szerv létesítése, mely nagyobb informatikai szakképzettséggel rendelkező szakemberekből álló szervként feladat- és hatáskörét a pénzügyi felügyeletet ellátó hazai és uniós szervekkel összhangban látná el. Mivel egyre többen foglalkoznak – és foglalkoznak majd – kriptovaluták és fiát pénzek közötti átváltási tevékenységgel, illetve mivel az átváltási árfolyamok sincsenek kellőképpen szabályozva, ennek eredményeként két – egymástól független – szolgáltató között magas lehet az árfolyam-különbség. Ebből kifolyólag a fent javasolt szerv feladatkörébe lehetne utalni a kriptovaluták átváltási árfolyamának felügyeletét is, amely szerv – mint hivatalos informatív fórum – közzé tenné a napi árfolyamokat, ezzel segítve a magán- és jogi személyek tájékozódását, illetve korlátozná az átváltási tevékenységet végző szolgáltatók tevékenységét minimum és maximum vételi és eladási ár megszabásával. Ez azzal az előnnyel is járna, hogy amennyiben egy büntetőeljárás során kényszerintézkedésre van szükség, amelyben kriptovaluta-számlákon szereplő összegek kerülnének értékesítésre, lenne egy hivatalos fórum, amelyet alapul lehetne venni az értékesítésnél.

Továbbá érdemes lenne átgondolni a blokklánc alapú kriptovaluták pénzügyi eszközökként történő elismerését, hiszen – véleményem szerint – ezúton lehetne a legegyszerűbben beilleszteni mind a polgári jogi, mind a büntetőjogi szabályrendszerbe a jelenséget. A kriptovaluták jogi szabályozása[332] – mivel egyre gyakrabban képezik bűncselekmények tárgyát[333], illetve eszközét – mostanra halaszthatatlan kérdéssé vált. A bűnözési tendenciák változásaival lépést tartva elvárható a reakció jogalkotói részről, hiszen a jogalkalmazás

[332] Lásd bővebben: Kecskés András; Bujtár Zsolt: Felvetések a kripto eszközök szabályozása terén. In: CONTROLLER INFO Vol. 7, No. 2, 2019. pp. 49-53.

[333] Lásd bővebben: Tóth Dávid: Crimes in Connection with Cryptocurrencies. In: Journal of Eastern-European Criminal Law Vol. 6, No. 2, 2019. pp. 193-206.

számára irreális elvárás lenne – mind büntetőjogi, mind polgári jogi ügyekben – a szabályozás hiányában történő működés.

9.2.2. Piramisjátékok szervezése a kriptovaluták vonatkozásában

Az online térhez fűződő mind szorosabb kötődésünk és az internettől való függőségünk vitathatatlan következménye a kibertérben elkövetett bűncselekmények növekvő tendenciája. A piramisjátékok szervezői, a csalás más formáinak elkövetőihez hasonlóan felfedezték az internet nyújtotta előnyöket, melynek révén a közösség egy szélesebb spektrumát vonhatják be a játékba.
A hatályos jogi szabályozást a Btk. 412. paragrafusában találhatjuk, „Piramisjáték szervezése" cím alatt[334]:

„Aki mások pénzének előre meghatározott formában történő, és kockázati tényezőt is tartalmazó módon való összegyűjtésén és szétosztásán alapuló olyan játékot szervez, amelyben a láncszerűen bekapcsolódó résztvevők a láncban előttük álló résztvevők számára közvetlenül, vagy a szervező útján pénzfizetést vagy más szolgáltatást teljesítenek, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."[335]

A piramisjáték szervezése egyrészről az állam pénzügyi szolgáltatás nyújtására, másrészről a szerencsejáték szervezésére vonatkozó monopóliumát sérti, a játék résztvevői azonban büntetőjogi értelemben nem sértettjei a cselekménynek.[336]
Amennyiben a piramisjátékokat viktimológiai szempontok alapján vizsgáljuk, megállapítható, hogy az áldozattá válás leggyakoribb okát abban kell keresni, hogy az áldozatokat nagyrészt a saját barátaik vagy a bizalmasaik hívják meg a játékba.[337]
A piramisjátékot vagy Ponzi-sémát a szokásos formájuk mellett a virtuális térben is meg lehet valósítani.[338] A bűncselekmények online formája még veszélyesebb is lehet, mint a

[334] A hatályos magyar szabályozásban a „Ponzi-séma" nem szerepel, helyette a piramisjáték elnevezés használatos, ezek rendkívül sok tekintetben hasonlítanak egymásra, a különbségekkel kapcsolatban az alábbi felület adhat tájékoztatást: https://academy.binance.com/en/articles/pyramid-and-ponzi-schemes (2020.1 0.10.)
[335] 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.) 412. §
[336] Kúria Bhar.III.1.321/2018/6. számú ítélete indokolásának [77] pontja
[337] Hague; David R.: Expanding the Ponzi Scheme Presumption. DePaul Law Review Vol. 64, No. 3, 2015. pp. 867-868.
[338] Több információért lásd bővebben: Nagy Zoltán András: A csalás-jellegű cselekmények az e-kereskedelem körében. In: Mezei Kitti (szerk.) A bűnügyi tudományok és az informatika. Pécs – Budapest. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, 2019. pp. 148-168.

hagyományos elkövetési módok, mivel így sokkal nehezebb eldönteni, hogy az online hirdetés vagy a (például e-mail útján történő) meghívás átverés-e vagy valós üzlet. Egy esetleges piramisrendszerű bűncselekmény azonban komoly veszteségeket okozhat a befektetők számára. Ugyanakkor vannak bizonyos árulkodó jelek, melyek segíthetnek megkülönböztetni a csalásokat a valós befektetési lehetőségektől. A US. Securities and Exchange Commission (röviden SEC) internetes oldalán található egy felsorolás azokról a jelekről, melyekre érdemes figyelni és amelyek indikátorként szolgálhatnak egy piramisjátékhoz. Ezek a következők:

- magas befektetési hozam kockázat nélkül vagy csekély kockázattal,
- túlságosan egyenletes visszatérítések,
- bejegyzetlen beruházások,
- engedéllyel nem rendelkező eladók,
- túlságosan bonyolult és/vagy titkos stratégia,
- könyveléssel kapcsolatos problémák, illetve
- a kifizetések során felmerülő nehézségek.[339]

A Bitcoin egyre növekvő értékével (amelyet Ethereum, ZCash és más valuták követnek) a kriptovaluták gyorsan berobbantak a köztudatba, és természetesen a befektetők is elkezdtek érdeklődni irántuk. Ennek a virtuális valutákkal kapcsolatos hatalmas érdeklődésének az oka több tényezőn alapul: a „blokklánc-technológia" bizonyos fokú pszeudonimitást biztosít a felhasználóinak, semmilyen ügynökség, illetve kormány nem szabályozza, emellett könnyen átváltható különböző pénznemekre, tehát megfelelő likviditással is rendelkeznek.

Egyes kutatók állítása szerint a Bitcoin is maga is egy piramisjáték, de a helyzet az, hogy ebben az esetben a befektetők valóban értékkel bíró valutát kaptak a pénzükért, amelyet képesek elkölteni bármire, amit csak szeretnének, emellett átváltható bármilyen más valutára. Ez tehát nem jelent közvetlen kockázatot a befektetők számára, illetve nem is kínál hihetetlenül magas hozamot.[340] Ezen tényeket figyelembe véve a Bitcoin viszonylag biztonságos befektetési formának tekinthető, megjegyzendő ugyanakkor, hogy minden kriptovaluta más eredetű, ezért a befektetőknek még mindig körültekintően kell eljárni a virtuális valutákkal kapcsolatban.

Példaként megemlíthető a OneCoin-eset, amely befektetőinek kockázatmentes havi 5%-os vagy heti 1%-os nyereséget ígért, de végül kiderült, hogy egy nemzetközi piramisjáték része az

[339] https://www.sec.gov/fast-answers/answersponzihtm.html (2020.10.07.)

[340] Eszteri Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécs, 2015, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, pp. 159-161.

egész.[341] BitConnect-eset is jó példaként szolgálhat. Ennek lényege az volt, hogy egy cég egy matematikai algoritmus segítségével több 1000%-os nyereséget kínált. Ez a szervezett bűnözéssel foglalkozó csoport jutalékot ajánlott befektetőinek, hogy több embert gyűjtsenek, akik beteszik a pénzüket, és betétjeiket meghatározott ideig a cégben tartják.[342]
A magas hozamú befektetési programok (röviden HYIP-k) az online piramisjátékok tipikus formái. Ezek olyan weboldalak, amelyek folyamatos nyereséget és hatalmas hozamot kínálnak kockázat nélkül, de a valójában ezek csalók által vezetett regisztrálatlan befektetések.[343]
T. Moore, J. Han és R. Clayton kutatásai alapján a kibertérben jártas befektetők valószínűleg tudatában vannak e weboldalak mögé rejtett illegális tevékenységeknek, de céljuk, hogy korai befektetéseik révén magas pozíciót töltsenek be a piramisban. Állításuk szerint a kriptovaluták, mint például a Liberty Reserve vagy a Perfect Money elengedhetetlen elemei az ilyen játékoknak, hiszen névtelenséget biztosítanak az elkövetők számára. Ezen pénznemek többsége latin-amerikai országokban, például Costa Ricában vagy Panamában található, és profitjuk nagy része a HYIP-okból származik.[344]
Az fentiek alapján láthatjuk, hogy a kriptovaluták kétféleképpen kapcsolódhatnak a piramisjátékokhoz: ha a valuta azzal a szándékkal jön létre, hogy maga is piramisjáték legyen, vagy ha a virtuális valuta eredetileg nem piramisjáték, hanem ahhoz használják fel.
Kétségtelen, hogy a befektetési szokások az idő múlásával gyökeresen megváltoztak, ez egy folyamatos folyamat, amelyben a kibertérnek meghatározó szerepe van. Bár ezen terület a legtöbb befektető számára még mindig nem teljesen ismert, kellő körültekintéssel és óvatossággal elkerülhető lehet a csalókkal való találkozás, emellett elengedhetetlen a pénzügyi kultúra[345] szintjének emelése is.
Azok számára, akik nem rendelkeznek kellően mély ismeretekkel a digitális világról, hasznos lehet annak ellenőrzése, hogy a SEC által kiadott árulkodó jelek ráillenek-e az adott befektetési lehetőségre. Az ilyen típusú online csalások rendkívül változatos formában fordulhatnak elő, ezért szükséges, hogy a befektetők mindig kétszer ellenőrizzék az adott lehetőséget, mielőtt pénzt fektetnek be.

---

[341] Tóth Dávid: A virtuális pénzekkel kapcsolatos visszaélések. In: Baráth Noémi Emőke – Mezei József (szerk.) Rendészet-Tudomány-Aktualitások. A rendészettudomány a fiatal kutatók szemével. Budapest. Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, 2019, p. 244.
[342] Simon Béla: Kriptovaluták – rendészeti válaszok. In: Belügyi Szemle Vol. 66, No. 10, 2018. p. 82.
[343] https://www.investor.gov/protect-your-investments/fraud/types-fraud/high-yield-investment-programs (2020.10.07.)
[344] Moore, Tyler; Han, Jie; Clayton, Richard: The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs. In: A.D., Keromytis (szerk.): Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol 7397. Springer, Berlin, Heidelberg, 2012, pp. 41-56.
[345] Lásd bővebben: Szívós Alexander: A pénzügyi kultúra. https://arsboni.hu/a-penzugyi-kultura/ (2020.10.20.)

A kriptovaluták, mint alternatív fizetési módok, alapvetően ugyanazt a funkciót töltik be a piramisjátékokban, mint a fiát valuták, tehát ezek tehát inkább a bűncselekmények eszközei, és nem a bűncselekmény tárgyai, bár a gyakorlati tapasztalatok alapján előfordulhat, hogy egyes kriptovalutákat csalás szándékával hozták létre.

A hazai jogalkalmazás szempontjából Teleki tanulmányában kiemeli, hogy utóbbi esetben a magyar szervezet-rendszer képes arra, hogy hatékony lépéseket tegyen a jogsértés megszüntetése és az elkövetők büntetőjogi felelősségre vonásának érdekében.[346]

Megjegyzendő, hogy a kriptovalutákat a csalás más, a piramisjátékokhoz vagy a hólabda-csalásokhoz képest kevésbé specifikus formáira is gyakran felhasználják az elkövetők. Ennek néhány lehetséges megnyilvánulásai lehetnek az alábbiak:

- a kezdeti költségek megelőlegzésével történő, közös kriptovaluta-bányászatra felhívás (tényleges bányászati kapacitás nélkül),
- a kriptovaluták árfolyammozgásának egy titokzatos algoritmus használatával történő prognosztizálása, melynek során az elkövető garantáltan magas hozamot ígér,
- scamcoinok létrehozása.[347]

9.2.3. A kriptovaluták terrorizmus finanszírozására történő felhasználása

Az egyes terrorista csoportok internethasználatának ún. „soft" típusú formáinak vizsgálatakor kétséget kizáróan megállapítható, hogy ennek a leggyakrabban előforduló válfaja a terrorszervezetek működésének fenntartását szolgáló finanszírozás megoldása.

Serbakov Márton a terrorizmus finanszírozásának internethez kötődő technikáit a következőképpen kategorizálta:

- az online kiskereskedők és piacok felhasználása (pl.: Amazon, Alibaba, eBay),
- a közösségi média platformjain történő adománygyűjtés és közösségi finanszírozás (crowfunding):
    - új fizetési termékek és szolgáltatások,
    - virtuális fizetőeszközök,
    - internetes pénzügyi szolgáltatások.[348]

[346] Teleki Bálint: Kriptovaluták és bűnözés, különös tekintettel a piramisjáték szervezésére. In: MAGYAR BŰNÜLDÖZŐ Vol. 10, No. 1-2, 2019. p. 80.
[347] Lásd bővebben több példával: Simon, 2018: Kriptovaluták – rendészeti válaszok, Op.Cit. p. 81-83.
[348] Serbakov Márton Tibor: A szélsőséges terrorista csoportok internethasználatának elemzése. Doktori értekezés. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2022. pp. 84-98.

A közösségi finanszírozás (crowfunding) keretében az egyes terrorszervezetek előszeretettel kérik a követőiket, hogy működésüket kriptovalutákkal támogassák. 2019-ben az al-Qassam brigádok közzétettek egy felhívást a közösségi média felületeiken, melyben arra buzdították a közösség tagjait, hogy Bitcoin felhasználásával juttassák el hozzájuk a felajánlásaikat, mivel azok nem nyomon követhetőek. Ezt követően a kampányt áthelyezték a hivatalos weboldalaikra.[349] A kampány végül nem járt sikerrel, ugyanis az IRS (Internal Revenue Service), a HSI (Homeland Security Investigations) és az FBI (Federal Bureau of Investigation) ügynökei sikeresen azonosítottak és lefoglaltak nagyjából 150 kriptovaluta számlát, mellyel a terrorszervezetet támogatták. Ennek során több ízben amerikai állampolgárokról bizonyosodott be, hogy így kívántak anyagi forrásokat felajánlani terrorista célokra.[350]

A fenti kategorizálás kritikájaként rögzítendő ugyanakkor, hogy mind az új fizetési eszközök és szolgáltatások, mind a virtuális fizetőeszközök, illetőleg az internetes pénzügyi szolgáltatások – álláspontom szerint – külön, önálló kategóriákként is felfoghatóak, nem kizárólag a közösségi finanszírozás kategóriáján belül helyezhetőek el, azt jóval meghaladják. Ennek egyik oka, hogy a terrorizmus finanszírozásához az adománygyűjtés és az ún. crowfunding mellett hozzátartozik más gazdasági tevékenységek végzése[351] (például bizonyos árucikkek adás-vétele, cseréje), melynek bevételét a terrorista szervezetek a működésük költségeire fordíthatják, esetlegesen fegyvereket vagy más illegális (harcászati) anyagokat vásárolhatnak belőle. Tipikusan ide tartoznak azok az esetek, amikor a terrorszervezet tagjai kábítószereket árulnak a dark weben és a bevételből fegyvereket, bombákat vagy azok alapanyagait veszik meg ugyanott, jellemzően kriptovaluták segítségének a felhasználásával.

Egy másik okként a terroristák által elkövetett kisebb-nagyobb vagyon elleni bűncselekményeket[352] emelném ki, mely bűncselekményeket követően az így ellopott, kicsalt (sokszor eleve már kriptovalutában lévő) pénzösszegeket használják fel a működésükhöz. Példaként kiemelhető egy 2020-as eset, mely lényege, hogy egy, a „Murat Cakar" álnevet felvett, ISIS-hoz köthető terrorista – kihasználva a COVID-19 járvány kitörését és az emberek félelmét – 2020. február 26. napján létesített egy weboldalt (facemaskcenter.com), melyen koronavírus elleni védőfelszereléseket, gumikesztyűket, szemüvegeket és N95-ös típusú arcmaszkokat „árult", azzal a különbséggel, hogy a vásárlók által megrendelt áruk általában

[349] alqassam.net, alqassam.ps, qassam.ps
[350] https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (2023.12.11.)
[351] Az ilyen források akár legális vállalkozásokból is származhatnak. Lásd például:
Tóth Zoltán Balázs: A pénzmosás és terrorizmus-finanszírozás visszaszorítását célzó szabályozási környezet vizsgálata az Európai Unió esetében II. In: SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA Vol. 17, No. 4, 2019. p. 195.
[352] Lásd például: Tóth Z. B., Op.Cit. p. 195.

nem érkeztek meg. A nyomozás során megállapítást nyert, hogy az elkövető az ISIS-hoz köthető, feltehetően a terrorszervezet működését kívánta támogatni a csalással szerzett profittal.[353]

A Pénzügyi Akciócsoport (FATF) 2015. októberi jelentésében a terrorizmus finanszírozásának új tendenciáit és az általuk jelentett fenyegetéseket a következőképpen kategorizálták:

- külföldi terrorista harcosok (FTFs),
- a közösségi média felületein történő közösségi finanszírozás,
- új fizetési szolgáltatások és termékek:
    - virtuális valuták,
    - előre feltöltött kártyák,
    - internet alapú fizetési szolgáltatások,
- természetes erőforrások kihasználása.[354]

A tudományos életben élénk diskurzus alakult ki a terroristák kriptovalutákkal történő finanszírozási megoldásainak tekintetében. E körben az egyes szerzők eltérő véleményeket képviselnek. Dion-Schwarz, Manheim és Johnston álláspontja szerint a kriptovaluták nem alkalmasak a terroristák általi használatra, ugyanis egyetlen rendelkezésre álló kriptovaluta sem képes kellő mértékű biztonságot és anonimitást biztosítani a terrorszervezetek részére.[355] A hivatkozott tanulmányban a szerzők ugyanakkor felvetik, hogy a jövőben számolni kell olyan kriptovaluták megjelenésével, melyek már rendelkezni fognak a terrorista célú felhasználáshoz szükséges tulajdonságokkal.[356] Petrétei Dávid a kriptovaluták terrorizmus finanszírozására és a pénzmosásra történő felhasználásának akadályát az akár rövid idő alatt is jelentős (akár 20-25% körüli) árfolyamkilengésekkel, a stabilitásuk hiányával indokolja, ugyanakkor az illegális felhasználás jövőbeli lehetőségét nem veti el.[357] Felméry Zoltán tanulmányában akként fogalmaz, hogy *„az Európában elkövetett támadások egyike esetén sem tűnik úgy, hogy azok finanszírozásában kriptopénzek is szerepet játszottak volna.”*[358] Más szerzők (Király[359],

[353] Ibid.
[354] FATF Report: Emerging Terrorist Financing Risks, Párizs, October 2015., hozzáférhető: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Emerging-Terrorist-Financing-Risks.pdf (2023.12.12.)
[355] Dion-Schwarz, Cynthia; Manheim, David; Johnston, Patrick B.: Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats. Santa Monica, California, RAND Corporation, 2019. p. 35.
[356] Op.Cit. p. 45.
[357] Petrétei Dávid: A modern kriminalisztika egyes jogi és etikai kérdései. In: Magyar Rendészet Vol. 18, No. 2, 2018. p. 110.
[358] Felméry Zoltán: A szervezett bűnözés általi internetes fenyegetettség értékeléséről szóló Europol-jelentés ismertetése. In: Nemzet és Biztonság: Biztonságpolitikai Szemle Vol. 12, No. 2, 2019. pp. 132-133.
[359] Lásd: Király Péter Bálint: A terrorizmus finanszírozásának új eszközei: a blokkláncok és a kriptovaluták. In: Bartkó Róbert (szerk.): A terrorizmus elleni küzdelem aktuális kérdései a XXI. században. Budapest, Gondolat Kiadó, 2019. p. 151.

Sánchez Medero[360]) ezzel ellentétben kifejezetten állítják, hogy a kriptovaluták alkalmasak a terrorizmus finanszírozására és napi szinten fel is használják ezeket az eszközöket a terrorszervezetek finanszírozására.[361] E körben a szerző azon álláspontot vallja, miszerint az egyes terrorszervezetek számára bizonyos, az első generációs kriptovaluták után megjelent eszközök (pl.: Monero) kifejezetten alkalmasak a terrorizmus finanszírozására történő felhasználásra, hiszen a hatóságokkal csekély mértékben vagy egyáltalán nem működnek együtt, nem adják ki a felhasználók adatait. Emellett az egyes kriptovaluta-keverők akár többszöri, szisztematikus alkalmazása, a különböző kriptivaluták oda-vissza váltogatása is magas szintű védelmet nyújthat az elkövetők számára. Ezen előbbi eszközökhöz társul továbbá az is, miszerint a terrorizmus finanszírozásának felderítésére a kibertérben kiemelkedő szakértelmet előfeltételez a nyomozó hatóságok részéről, mely gyakran hiányzik vagy éppen a magas munkaterhelés miatt a kellő szakértelemmel rendelkező különleges szervek sem képesek megfelelő időn belül és kellőképpen foglalkozni az üggyel. A fentiek okán a szerző álláspontja szerint a terrorista szervezetek fel tudják és fel is használják a kriptovaluták egyes típusait, ugyanakkor a magas fokú látencia miatt ritkán kerülnek felderítésre az ilyen cselekmények.

9.2.3.1. Következtetések

A terrorista szervezetek – ahogyan a fentiekben is kifejtésre került – aktívan jelen vannak a kibertérben. E jelenlét egyik legfontosabb megnyilvánulása a finanszírozás különböző formákban történő megoldása. Ez történhet legális gazdasági tevékenység végzésével, illegális tevékenységek (pl.: fegyver- vagy kábítószerkereskedelem) vagy közösségi finanszírozás megvalósításával. A kriptovaluták szerepe és közrehatása egy olyan körülmény, mely rendkívüli módon megosztja a kutatókat. Egyes szerzők álláspontja, hogy a kriptovalutákat nem tudják és ezért nem is használják a terrorszervezetek, mivel nem nyújtanak kellő anonimitást. Más szerzők állítják, hogy a kriptovaluták megfelelő alternatívát nyújtanak a terrorszervezetek számára a finanszírozásuk megoldására. Álláspontom szerint szükségszerű számolni a kriptovaluták terrorizmus finanszírozására történő felhasználásával, ugyanis egyes kriptovaluták (például a Monero vagy XMR) teljes anonimitást biztosítanak azzal, hogy a hatóságokkal semmilyen szinten sem működnek együtt, a feléjük benyújtott adatszolgáltatást megtagadják, így megakadályozva a felderítés sikerességét. Emellett léteznek ún. mixerek vagy másszóval keverőprogramok, melyek használatát kreatívan lehet párosítani a hatóságokkal nem

[360] Sánchez Medero, Op.Cit. pp. 74-75.
[361] Op.Cit. p. 157., továbbá p. 163.

vagy nagyon kis mértékben együttműködő kriptovalutákkal. Ilyen módon – álláspontom szerint – kellő mértékben biztosított az anonimitás a terrorszervezeket számára, így hatékonyan megvalósulhat a tevékenységeik online finanszírozása. Véleményem szerint a probléma megoldása a nyomozó hatóságokkal, ügyészségekkel semmilyen mértékben sem együttműködő kriptovaluta szolgáltatók tevékenységének korlátozásában, illetőleg ezen típusú kriptovaluták kriminalizálásában rejlik. Ez egy sokkal transzparensebb környezetet teremtene, hiszen a hatóságokkal együttműködő szolgáltatók által kibocsátott kriptovaluták használatával a bűncselekményre történő felhasználás idővel csökkenne, a sikeres felderítések, vagyonvisszaszerzések száma pedig növekedne.

9.2.4. Adócsalás

Halász Viktor tanulmányában felveti annak a lehetőségét, hogy a bűnelkövetők kihasználhatják a kriptovaluták tároló funkcióját az adócsalásokhoz. Ezekben az esetekben az elkövetők legális forrásokból, gazdasági tevékenységek végzése útján anyagi javakra tesznek szert, melyek után el kívánják kerülni az adóterhek megfizetését. E végből az elkövetők rákényszerülnek arra, hogy e javakat valamilyen módon elrejtsék az adóhatóságok elől. Ahogy Halász is kiemeli, a kriptovaluták az illegális adóelkerülés szempontjából egyfajta „adóparadicsomként" foghatóak fel, hiszen általuk az adóhatóságok feladata jelentősen megnehezül, ugyanis a fizikai javak, készpénz vagy számlapénz helyett a hatóságoknak a privát kulcsot kellene felkutatniuk.[362]
Ilyen bűncselekmények kapcsán hazai példa is rendelkezésünkre áll. Egy hazai bűnszervezet tagjai az Európai Unió több tagállamából nettó áron szereztek be okostelefonokat, tableteket, napelemeket és egyéb elektronikai eszközöket. Az importált elektronikai eszközök fiktív számlázási láncokon keresztüli értékesítésével, több mint 3 milliárd forint ÁFA befizetését kerülték el az elkövetők. Az elkövetők a bűncselekmény elkövetéséből származó vagyont kriptovalutába, továbbá egy kriptovaluta-kereskedelemmel foglalkozó online platformba, illetőleg egy kriptovaluta-bányászatra használt számítógépbe fektette. A specialisták a helyszíneken felkutatták a fizikai és virtuális formában jelen lévő privát kulcsokat, tárcákat, majd a többféle, összesen nagyjából 1 millió amerikai dollár, azaz közel 420 millió forint értékű kriptovalutát a NAV külön erre a célra létrehozott hatósági tárcájába helyezve foglalták le.[363]

[362] Halász Viktor: A bűncselekményekből származó vagyon nyomon követésének új kihívásai a kibertérben. In: Farkas Ákos; Dannecker Gerhard; Jacsó Judit (szerk.): Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre. Budapest, Wolters Kluwer Kft., 2019. pp. 440-441.
[363] Kriptovalutába bújtatott bűnös milliárdok.
https://nav.gov.hu/sajtoszoba/hirek/Kriptovalutaba_bujtatott_bunos_milliardok (2024.02.03.)

9.3. Egy kriptovalutákkal kapcsolatban felmerült új típusú bűncselekmény: a jogellenes kriptovaluta-bányászat

A bűncselekmény könnyebb megértése érdekében érdemes foglalkozni az ún. bányászat (mining) fogalmával. Annak érdekében, hogy egy adott tranzakciót véglegesnek lehessen tekinteni, szükség van a műveletek hitelesítésére. A kriptovaluták rendszerében ezeket a folyamatokat többnyire a felhasználók végzik akképpen, hogy a számítógépük számítási képességét kihasználva az egyes blokkokba gyűjtött tranzakciókat matematikai képletek segítségével kódsorozatokká (hash) alakítják.[364] Mivel az előbbi folyamat meglehetősen energiaigényes, a bányászatot folytató felhasználók számára – kompenzáció gyanánt – a rendszer új kriptovalutákat állít elő, melyeket a bányászó által előre meghatározott kriptovaluta tárcához ad hozzá. Voltaképpen ez a folyamat tekinthető a kriptovaluták eredeti szerzésmódjának is. Ahogy az egyes kriptovaluták rendszerében egyre több tranzakció megy végbe, egyre bonyolultabb matematikai képleteket kell a számítógépeknek megoldani. Ennek eredményeképpen sokkal több energiába kerül egy adott egységnyi kriptovaluta bányászata, emellett jóval előbb elhasználódnak a számítógépek bizonyos hardverjei is.

A fenti fogalmi alapvetések áttekintése után megállapítható, hogy a kriptovaluta bányászat teljes mértékben az önkéntesség elvére épít, ideális esetben tehát a felhasználó szabadon mérlegelheti a művelet várható kiadásait, bevételeit és egyéb hasznait. Egyre sűrűbben fordulnak elő azonban olyan esetek, amikor a bűnelkövetők a bányászat negatív velejáróit, következményeit másik személy(ek)re hárítják át és e személy(ek) eszközeinek számítási kapacitását használják fel a folyamat véghezvitelére. A cselekmény több módon is megvalósulhat, továbbá aggasztó tény, hogy egyre több, a szervezett bűnözés körében előforduló jogesetre is találunk példákat.

9.3.1. Első esetkör: a jogosultság kereteinek túllépésével elkövetett jogellenes kriptovaluta-bányászat

A jogellenes bányászat megvalósulásának egyik lehetséges (és talán a legegyszerűbb) módja, ha az elkövető olyan számítástechnikai eszközöket használ fel kriptovaluta bányászatára, melyek könnyen elérhetőek számára akár előzetes cselekmények elvégzése nélkül is. Ennél az

[364] Mátyás Szabolcs; Frigyer László; Prilenszky Géza: A virtuális fizetőeszközök szerepe és jelentősége a vagyonvisszaszerzés során. In: Belügyi Szemle Vol. 69, No. 3, 2021, p. 423.

esetkörnél a számítástechnikai eszközök gyakran az elkövető birtokában vannak vagy könnyen hozzáférhetőek a számára. Ez megtörténhet például olyan módon, hogy az elkövető munkahelyi számítástechnikai eszközét használja jogellenesen kriptovaluta bányászatára. Ebben az esetben az elkövető az adott információs rendszer vonatkozásában rendelkezik ugyan belépési jogosultsággal, azonban e jogosultság kereteit túllépve, haszonszerzés végett saját maga vagy harmadik személy(ek) részére végezteti el a folyamatot az érintett eszközzel. Ezen cselekmény – amennyiben más jogsértés nem történik – alkalmas lehetne a Btk. 423. § (1) bekezdésébe ütköző információs rendszer (adat) megsértésének vétségének megvalósítására, ezt azonban el kell határolni a Btk. 375. § szerinti információs rendszer felhasználásával elkövetett csalás bűntettétől.

A Btk. 375. § (1) bekezdése a következőképpen fogalmaz az információs rendszer felhasználásával elkövetett csalás vonatkozásában:

„Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.”

Alapvetően a két bűncselekmény elhatárolásának az alapját a károkozás ténye képezi, így tehát a jogellenes kriptovaluta-bányászat esetében, mivel a károkozás a bűncselekmény alapvető tényállási eleme, egyenesen következik, hogy az ilyen esetekben az információs rendszer felhasználásával elkövetett csalást kell megállapítani. Ennek oka, hogy a két bűncselekmény bűnhalmazatot nem képezhet, mivel az információs rendszer felhasználásával elkövetett csalás bűntettének szükségszerű eszközcselekménye az információs rendszer vagy adat megsértésének vétsége (vagy bűntette).[365] Ebben az esetben egy látszólagos anyagi halmazat áll fent a két bűncselekmény között.

A fenti példa esetében meg kell jegyezni, hogy lényeges körülmény ugyanakkor a munkahely minősége. A Btk. 423. § (4) bekezdése értelmében ugyanis az előbbi cselekmény – amennyiben az információs rendszer (adat) megsértését közérdekű üzem[366] ellen követik el – már bűncselekménynek minősül, melynek büntetési tétele két évtől nyolc évig terjedő szabadságvesztés. Amennyiben ez a minősítő körülmény fennáll, abban az esetben – a

[365] Akácz József: A vagyon elleni bűncselekmények. In: Kónya István (szerk.): Magyar Büntetőjog. Kommentár a gyakorlat számára, Budapest, HVG-ORAC, 2015, p. 1415.

[366] A Btk 459. § (1) bekezdés 21. pontjának értelmében közérdekű üzemnek minősül a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek, a hadianyagot, haditechnikai eszközt termelő üzemet, energiát vagy üzemi felhasználásra szánt alapanyagot termelő üzem.

konszumpció elvére hivatkozva – látszólagos alaki halmazatot kellene megállapítani, hiszen ebben az esetben súlyosabb bűncselekményt valósít meg a cselekmény, így tehát a jogrendnek is adekvát szankcióval kell rá reagálnia. Ennek értelmében, ha közérdekű üzem sérelmére követnek el jogellenes kriptovaluta-bányászatot, véleményem szerint a Btk. 423. § (1) bekezdésébe ütköző és (4) bekezdése szerint minősülő információs rendszer (adat) megsértésének bűntettét kell megállapítani, hiszen a cselekmény teljes egészében kimeríti a tényállást. A fentebb említettek jelentőségét szemléletesen bemutatja egy 2018-as oroszországi incidens, melynek során atomkutatók egy csoportját tartóztatták le, miután – a vádak szerint – egy szigorúan titkos, nukleáris atomfejek összeszerelésére szolgáló létesítményben próbáltak meg jogellenesen Bitcoin-t bányászni. A média értesülései szerint az elkövetők a nyugat-oroszországi Szarovban található Szövetségi Nukleáris Központ alkalmazottai voltak, akik a létesítmény szuperszámítógépével tettek kísérletet a kriptovaluta-bányászatra. Az incidenst az érintett központ sajtószolgálata is megerősítette. Az elkövetőkkel szemben bűntetőeljárás indult, miután a nukleáris központ biztonsági osztálya átadta őket a Szövetségi Biztonsági Szolgálatnak.[367]

9.3.2. Második esetkör: a jogellenes kriptovaluta-bányászat céljából indított kibertámadások (avagy az ún. „cryptojacking")

A jogellenes kriptovaluta-bányászat egy másik lehetséges formája az angolszász szakirodalomban az ún. „cryptojacking" elnevezéssel jelölt bűncselekmény. Ennek lényege, hogy az elkövető jogosulatlanul fér hozzá az áldozatok számítástechnikai eszközeihez, majd ezek számítási kapacitását felhasználva bányászik kriptovalutát – haszonszerzés végett – saját maga vagy harmadik személy(ek) részére. Ez a gyakorlatban általában úgy valósul meg, hogy az áldozat számítógépére feltelepítésre kerül egy rosszindulatú (scripteket tartalmazó) program, amely lehetővé teszi az elkövető számára, hogy hozzáférjenek az adott eszközhöz. A leggyakrabban erre e-mailben található – ismeretlen eredetű – linkekre történő kattintással vagy ún. „fertőzött" weboldalak látogatásával kerül sor.[368] Az előző esetkörhöz képest a jogellenes kriptovaluta-bányászat ezen formája tehát lényegesen több előkészületet igényel az elkövető részéről, hiszen ebben az esetben nincs a birtokában, illetve nem áll rendelkezésére egy számítástechnikai eszköz. Az elkövetés első fázisa – a scripteket tartalmazó – program e-mail

[367] „Russian nuclear scientists arrested for 'Bitcoin mining plot'"
https://www.bbc.com/news/world-europe-43003740 (2022.03.06.)
[368] https://www.interpol.int/Crimes/Cybercrime/Cryptojacking, (2021.12.19.)

üzenetekben vagy internetes weboldalakon történő elhelyezése, mely minden esetben egy burkolt formában történik. Gyakori, hogy az elkövetők közszolgáltatók, bankok, illetve más – az átlagos felhasználók által hitelesnek vélt – szolgáltatók „arculatának" lemásolásához, jellemzően promóciós levelek, díjbekérők, számlák, illetve egyéb, a hétköznapi életben nagyobb gyakorisággal előforduló elektronikus levelek felhasználásához folyamodnak, mellyel egyfajta hamis bizalmat keltenek a sértettekben. Az ilyen e-maileket a levelezőprogramok egy része viszonylag nagy pontossággal kiszűri és levélszemétként azonosítja, ugyanakkor (főként) a sérülékenyebb levelezőprogramok esetében különös gondossággal kell eljárni az ilyen típusú üzenetek megnyitásánál.

A másik esetkörhöz hasonlóan, a jogellenes kriptovaluta-bányászat ezen típusánál is az anyagi haszonszerzésre terjed ki az elkövető szándéka. Az ökoszisztéma egyik kulcseleme, hogy a bányászatot végző felhasználó ún. „kompenzációt" kap a számítási kapacitásának a rendszer számára történő rendelkezésre bocsátásáért cserébe, ugyanakkor megjegyzendő, hogy ez a kompenzáció az értékesebb, legtöbb felhasználó által használt kriptovaluták tekintetében meglehetősen alacsony, a kevésbé ismert, értéktelenebb kriptovaluták tekintetében pedig – a kriptovaluta kisebb értékéből adódóan – értéktelenebb. Az értékesebb kriptovaluták bányászatához általában nem feltétlenül elegendő az egyszerű személy számítógépek számítási kapacitása, erre a feladatra ún. „bányászgépeket" vagy komplett szervergépeket szoktak alkalmazni. Ez alapján az elkövető – mivel a legtöbb felhasználó egy kisebb teljesítményű személyi számítógéppel rendelkezik – meglehetősen kevés haszonra tehet szert sértettenként. Ebből kifolyólag az ilyen jellegű bűncselekmények nyomozása során kiemelt figyelmet kell fordítani a teljes sértetti kör felderítésére, hiszen a fent említett ok miatt az elkövetők – az esetek többségében – egy minél tágabb réteget próbálnak megcélozni; arra törekednek, hogy minél több sértettje legyen az általuk elkövetett bűncselekménynek. A jogellenes kriptovaluta-bányászat ezen formája tehát – ha az arányosság szempontja alapján vizsgáljuk – nem feltétlenül nyújt kedvező helyzetet a bűnelkövetők számára.

Példaként szolgálhat a fentiekre egy japán jogeset, melynek lényege, hogy a 24 éves elkövető, Yoshida Shinkaru a Monero nevezetű kriptovaluta bányászatára szolgáló Coinhive nevű programot használta fel jogellenesen. E tevékenysége során a programot egy olyan programba ágyazott be, melyet számítógépes játékokban, videójátékokban alkalmaznak a játékban történő részvétel „megkönnyítésére", a játékokban történő „csalásokra". A programot ingyenesen hozzáférhetőként és letölthetőként tette közzé az elkövető a saját online blogján. A gyanútlan letöltők eszközeire feltelepített program ezek után az elkövető számára bányászta a Monero nevezetű kriptovalutát. Alátámasztva az aránytalanságot és a feltételek kedvezőtlen mivoltát,

érdemes kiemelni, hogy dacára a ténynek, hogy több, mint 90 alkalommal töltötték le az elkövető által hozzáférhetővé tett programot, Yoshida Shinkaru összesen 5000 japán jen haszonra tett szert, mely összeg 2022. február 25-ei árfolyamon számolva cirka 14.000 forintra tehető, ugyanakkor a Sendai Kerületi Bíróság az elkövetővel szemben egy év szabadságvesztés büntetés kiszabására került sor, melynek végrehajtását három évre felfüggesztették.[369] Ezekben az esetekben is kiemelt jelentőséggel bír a sértettek számának meghatározása, hiszen a sértetti kör terjedelme a bűncselekmény konkrét meghatározásánál is elengedhetetlen. A hatályos Btk. alapján tehát ezekben az esetekben az információs rendszer felhasználásával elkövetett csalás bűntettének megállapítása lenne a törvényi követelmény, ugyanakkor – tekintettel arra a tényre, hogy ezen bűncselekményeknél a károkozás ténye elenyésző a sértettek számához képest, amennyiben jelentős számú információs rendszer érintett a bűncselekményben – újfent – hivatkozva a konszumpció elvére, véleményem szerint ezekben az esetekben a Btk. 423. § (2) bekezdésébe ütköző és a (3) bekezdése szerint minősülő jelentős számú információs rendszer vagy adat megsértésének bűntettének megállapítása lenne helyes a törvény céljainak érvényre juttatása és az elkövetett bűncselekményhez leginkább igazodó jogalkalmazói reakció kiváltása érdekében.

A sértetti kör növelésén túlmenően az elkövetők másféleképpen is próbálnak megoldásokat keresni a fenti problémára. Ennek egy bevált módja az, ha a mennyiség helyett a minőségre helyezik a hangsúlyt. Célszerűen tehát olyan áldozatokat céloznak meg, melyek nem az átlagos felhasználók által folytatott egyszerű tevékenységekre elegendő teljesítményű eszközöket, hanem a – főként nagyvállalati környezetben alkalmazott – nagy számítási kapacitású gépeket alkalmaznak, így tehát az ilyen vállalkozások fokozottan ki vannak téve a jogellenes kriptovaluta-bányászat veszélyének. 2018. februárjában például a Tesla autógyártó vállalat által használt „Kubernetes" névre hallgató nyílt forráskódú alkalmazáskezelő szoftver „sérülékenységét" használták ki az elkövetők jogellenes bányászatra[370], de hasonlóképpen járt az Aviva nevű multinacionális biztosítócég és a Gemalto nevű nemzetközi digitális biztonsági vállalat is.[371] A RedLock 2018-as évre vonatkozó, a felhőszolgáltatások biztonsági trendjeiről szóló jelentésében közzétették, hogy a nagyvállalatok 25%-a tapasztalt jogellenes kriptovaluta-

[369] Osborne, Charlie: „Japan issues first-ever prison sentence in cryptojacking case" https://www.zdnet.com/google-amp/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/?fbclid=IwAR00OIs2mLn5akKQKdoSZ0_lySM6Y2KeQ4_vlD2tfaKdQlRjPH0RMU86qfo (2022.02.25.)

[370] Osborne, Charlie: „Tesla cloud systems exploited by hackers to mine cryptocurrency" https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/ (2022.02.28.)

[371] Ashford, Warwick: „Unprotected Kubernetes consoles expose firms to cryptojacking" https://www.computerweekly.com/news/252435544/Unprotected-Kubernetes-consoles-expose-firms-to-cryptojacking (2022.02.28.)

bányászattal kapcsolatos visszaéléseket a felhőszolgáltatásaik vonatkozásában, mely jelentős növekedést mutat a tárgyévet megelőző, 2017. év során számított 8%-hoz képest.[372] Az ilyen jelentősebb technológiai erőforrásokkal rendelkező vállalatok szempontjából – az egyszerű felhasználókhoz képest – sokkal jelentősebb károkkal kell számolni. Ezt kiválóan alátámasztja annak a két iráni állampolgárnak az ügye, akik – a vád szerint – egy Missouriban található vállalat által igénybe vett felhőszolgáltatásokat[373] törték fel jogellenes kriptovaluta-bányászat céljából, melynek eredményeként a felhőszolgáltató 760.000 dollárt számlázott ki a vállalat részére.[374] A kritikus infrastruktúrák védelme – az előző esetkörhöz hasonlóan – kiemelt jelentőséggel bír, így az ilyen objektumok ellen irányuló – akár belső, akár külső – támadásokat kellő mértékben kell szankcionálni a büntetőjog eszközeivel. Hangsúlyozandó, hogy Európa területén belül is történtek már hasonló incidensek, ahol a jogellenes kriptovaluta bányászatára irányuló szándékkal törték fel az elkövetők az érintett közérdekű üzem informatikai rendszerét.[375]

9.3.3. További kérdéseket felvető esetkörök

A jogellenes kriptovaluta-bányászatnak – a fentebb említett két esetkörön túlmenően – léteznek nehezebben megítélhető előfordulási módjai is. Tipikusan ilyen esetnek számít, ha az elkövető az egyes közösségi terekben (könyvtárakban, internet kávézókban, egyetemeken, iskolákban) található eszközökkel követi el a cselekményt. Amennyiben az érintett közösségi téren olyan szolgáltatások elérhetőek, melyek keretében a szolgáltató időkorláthoz kötötten bocsátja a szolgáltatást igénybe vevő felhasználók rendelkezésére az adott eszközöket, illetőleg az internet-hozzáférést, abban az esetben – ha az adott szolgáltató által meghatározott belső szabályzatok másképpen nem rendelkeznek – úgy véleményem szerint csak a felhasználók által kifizetett időkereten túlmenően lehet megállapítani a jogellenes kriptovaluta-bányászatot, pontosabban az információs rendszer felhasználásával elkövetett csalás tényállását, tekintettel

---

372 https://redlock.io/news/redlock-cloud-security-trends-report-highlights-lack-of-compliance-with-industry-standards (2022.02.28.)

373 Lásd a témáról részletesebben: Klein Tamás: A felhőszolgáltatások egyes jogi kérdései - különös tekintettel az Európai Unió szabályozására. In: Klein Tamás (szerk.): Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről. Budapest, Médiatudományi Intézet, 2018. 89-122. o., továbbá
Máté István Zsolt: A felhőszolgáltatások igazságügyi informatikai szakértői vizsgálata. In: Infokommunikáció és Jog Vol. 62-63, 2015. pp. 86-90.

374 https://www.justice.gov/usao-edmo/pr/two-iranian-nationals-indicted-local-cryptojacking-case?fbclid=IwAR0fNFkcbq1qXDXDLD5o3Ill9RVBjetXK78VhBb3YB5Dg7oSLKYk8b_KsoM (2022.03.06.)

375 Példaként szolgál a fentiekre egy víziközmű esete is, lásd részletesebben:
Lily Hay Newman: „Now Cryptojacking Threatens Critical Infrastructure, Too”
https://www.wired.com/story/cryptojacking-critical-infrastructure/ (2022.03.06.)

a károkozás tényére. Ez ugyanakkor csak az első esetkörnél taglalt elkövetési mód fennállása esetén alkalmazandó, hiszen amennyiben az elkövető a második esetkörben említettek szerint jár el, úgy – értelemszerűen – semmiféle jogosultsággal nem rendelkezett, illetve nem nyújtott részlegesen sem ellenszolgáltatást a szolgáltató felé, így ezekben az esetekben a teljes időszakra vonatkozóan meg lehet állapítani az információs rendszer felhasználásával elkövetett csalást. Azokban az esetekben, amikor konkrét időkorlátról nem beszélhetünk (tipikusan ilyen az iskolákban, egyetemeken, egyes könyvtárakban történő kriptovaluta-bányászat), kevésbé egyértelmű az ilyen cselekmények megítélése. Kiemelendő ugyanakkor, hogy ezekben az esetekben is különbséget kell tenni a fentebb részletezett elkövetési módok között. Hasonlóképpen az előzőkhez, a helyszíni elkövetés megítélése jelenti a kérdést. Ennek oka, hogy a nem minden esetben állapítható meg bűncselekmény elkövetése, hiszen – ha az adott szolgáltató korlátozások nélkül a felhasználók rendelkezésére bocsátotta az eszközeit, illetve az internet-hozzáférést, úgy – a cselekmény egyetlen a Btk. által nevesített tényállást sem meríti ki. Amennyiben ilyen helyzet áll elő, álláspontom szerint az adott szolgáltató felelőssége, hogy a saját, belső szabályzatainak keretein belül meghatározott keretek közé szorítsa az erőforrásainak használatát, melynek során fel kell hívni a felhasználók figyelmét a szabályzatokban foglaltak betartásán túlmenően az azokkal ellentétes magatartás tanúsításának büntetőjogi és polgári jogi következményeire. Amennyiben ez megtörténik, úgy a későbbi incidensek esetén – véleményem szerint – már lehet hivatkozni a belépési jogosultság kereteinek túllépésére, mely megalapozza az információs rendszer vagy adat megsértésének vétségét. Az információs rendszer felhasználásával elkövetett csalás bűntettének megállapításához nem lenne szükség a belső szabályzatokban történő felhívásra sem, ugyanakkor a bűncselekmény megállapításának szükségszerű tényállási eleme a károkozás, melyet meglehetősen nehéz megállapítani azokban az esetekben, amikor a felhasználók korlátozások nélkül használhatják a szolgáltató erőforrásait, legyen az internet-hozzáférés vagy konkrét eszközök (számítógépek, tabletek, okostelefonok[376]) használata. A károkozás ezeknél a cselekményeknél általában a megnövekedett villamosenergia-fogyasztásban, illetve a hardverek élettartamában tud megnyilvánulni, ugyanakkor ezek egyike sem egzaktan mérhető, nem lenne életszerű és elvárható a sértettektől e tényeknek a bizonyítása. Ezek alapján úgy gondolom, hogy célszerűbb és hatékonyabb megoldás a belső szabályzatok kiegészítése, az egyszerűbb jogi megítélés érdekében.

Természetes a részletezett elkövetési alakzatokon kívül is előfordulhat jogellenes kriptovaluta-

[376] Lásd az okostelefonok sérülékenységéről bővebben: Kraut Andrea; Kőhalmi László; Tóth Dávid: Digital Dangers of Smartphones. In: Journal Of Eastern-European Criminal Law Vol. 7, No.1, 2020. pp. 36-49.

bányászat, sőt egészen absztrakt jogesetek is megjelenhetnek. Erre jó példaként szolgál az ún. Siacoin-ügyként elhíresült eset, mely 2017-ben valósult meg Kínában. Ekkor hackerek egy csoportja konspiratív módon megállapodást kötött a kínai internetkávézók karbantartásáért felelős cégekkel arról, hogy az általuk elkészített, a Siacoin nevezetű kriptovaluta bányászatára kifejlesztett programot – egyfajta rendszerfrissítés részeként – a cégek elhelyezik az általuk karbantartott internetkávézók eszközein. Az elkövetők százezernél is több számítógéppel folytattak jogosulatlan kriptovaluta-bányászatot,[377] mellyel több, mint 5 millió kínai jüan (akkori árfolyamon 800.000 amerikai dollár) haszonra tettek szert.[378]

9.4. A kriptovaluták vonatkozásában elkövetett bűncselekmények felderítése és nyomozása

9.4.1. Problémafelvetések, aktuális helyzetkép

Hazánkban általános problémát jelent, hogy a kriptovalutákkal összefüggésben elkövetett bűncselekmények nyomozása akadályokba ütközik, melynek oka, hogy a nyomozó hatóságok és a nyomozás felügyeletére illetékességgel rendelkező, törvényszék melletti járási ügyészségek személyi állománya sok esetben nem rendelkezik a bűncselekmények felderítéséhez szükséges, kellő mértékű informatikai ismeretekkel. A kiberbűnözés[379] bizonyos válfajai[380] – függetlenül attól, hogy érintettek-e kriptovaluták az elkövetésben – dacára annak a ténynek, hogy immár több évtizede elterjedtek a világon, még mindig egy olyan fenomén, mellyel sok esetben nem tudnak, illetve előfordul, hogy – az összetettségük és a nehézkes

[377] A bűncselekménnyel kapcsolatban a tanulmány elkészítésekor még folyt a nyomozás, az ügy tárgyi súlyára tekintettel a Zheijang Tartományi Közbiztonsági Osztály és a Közbiztonsági Minisztérium felügyelete alatt. A helyi sajtó értesülései szerint országszerte legalább 30 városban több, mint 100 karbantartó vállalat érintett az ügyben. Lásd részletesebben:
https://hznews.hangzhou.com.cn/shehui/content/2018-06/16/content_7020998_2.htm (2022.03.02.)
[378] Wolfie Zhao: „Internet Cafes Hacked to Mine $800k in Siacoin Cryptocurrency"
https://www.coindesk.com/markets/2018/06/19/internet-cafes-hacked-to-mine-800k-in-siacoin-cryptocurrency/ (2022.03.02.)
[379] Lásd: Herke Csongor: A kiberbűnözés és a teljesen önvezető járművek. In: Barabás Andrea Tünde; Christián László (szerk.): Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est. Budapest, Ludovika Egyetemi Kiadó, 2021. pp. 211-221.
[380] Ide tartoznak például az interneten elkövetett személyiséglopás esetei is. Lásd a témáról részletesebben:
Tóth Dávid: Identity crimes on the darknet and the social media. In: Büntetőjogi Szemle Vol. 10, Különszám, 2021. pp. 85-89., továbbá
Tóth Dávid: Személyiséglopás az interneten. In: BÜNTETŐJOGI SZEMLE Vol. 9, No. 1, 2020. pp. 113-119., illetve
Tóth Dávid: Az identitáslopás kriminológiai sajátosságai. In: Gaál Gyula; Hautzinger Zoltán (szerk.) A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2019. pp. 207-213.

nyomozási feladatok miatt – nem is akarnak mit kezdeni a bűnüldöző szervek.[381] Hangsúlyozandó ugyanakkor, hogy ezek az eszközök – kiváltképp, de nem kizárólagosan a fiatalabb korosztályok körében – egyre inkább elterjedni látszanak, egyre nagyobb rétegek, befektetői körök, vállalatok, de bizonyos esetekben egész országok állnak át a használatukra.[382] A kriptovaluták vonatkozásában elkövetett egyes bűncselekmények tárgyi súlya is megköveteli, hogy az ügyek ne egy megszüntető határozattal legyenek lezárva, az elkövető kilétének azonosíthatatlan mivoltára vagy a joghatóság hiányára hivatkozva. Tény, hogy az ilyen típusú bűncselekmények szinte kivétel nélkül több joghatóságot érintenek, emellett az esetek túlnyomó részében külföldön tartózkodó, nem magyar állampolgárok az elkövetők, ugyanakkor a vonatkozó uniós, illetve az azokat implementáló hazai jogszabályok teljes mértékben megalapozzák a joghatóságot, azokban az esetekben is, amikor csak részben követték el a bűncselekményt Magyarország területén,[383] emellett a tanulmányban vizsgált kutatási időszakban már több olyan lehetőség is rendelkezésére áll a nyomozó hatóságoknak, mely eredményes felderítéshez és felelősségre vonáshoz vezethet.

Amennyiben a személyi állomány kellő szaktudása rendelkezésre áll, egy további problémával kell megbirkózni. Sok esetben a piacon elérhetőek olyan, a nyomozást jelentős mértékben megkönnyítő szolgáltatások vagy számítógépes szoftverek, melyek felhasználásával jelentősen meg lehetne növelni a hatóságok effektivitását. Ennek általában az akadálya azonban az, hogy a termékek beszerzésére nem állnak rendelkezésre megfelelő anyagi források.

9.4.2. Kényszerintézkedések a kriptovaluták biztosítására

A kényszerintézkedések jogszerű foganatosításához elsőkörben elengedhetetlen volt egy – legalább a minimumra törekvő – definíció megalkotása, mellyel az alapkő letétetik és elkezdődhet a jogszabályi környezet felépítése. Ez a definíciós alap az 5. uniós pénzmosás

[381] Mátyás Szabolcs, Frigyer László és Prilenszky Géza is megfogalmazták a Belügyi Szemlében megjelent tanulmányukban, hogy mind a rendvédelmi szervek, mind az ügyészség számára szükséges lenne összetettebb képzéseket szervezni a kriptovalutákkal kapcsolatos gyakorlati ismeretek átadása végett. Lásd: Mátyás; Frigyer; Prilenszky, Op.Cit. p. 427.

[382] Példaként kiemelhető El Salvador esete, ahol a világon első ízben fogadták el a legismertebb kriptovalutát, a Bitcoint. Ezzel a mérföldkővel az országgal kapcsolatban álló gazdasági szereplőknek is alkalmazkodniuk kellett a kriptovalutákkal bővített pénzügyi szolgáltatásokhoz és kihívásokhoz. Lásd részletesebben: Kate Linthicum: „El Salvador's president buys bitcoins 'naked,' he boasts. His experiment is costing his nation millions" https://www.latimes.com/world-nation/story/2022-02-23/el-salvador-bitcoin-experiment (2022.03.19.), továbbá
Marco Quiroz-Gutierrez: „El Salvador says tourism is up 30% since it made Bitcoin legal, but the country is still on the brink of economic disaster" https://fortune.com/2022/02/23/el-salvador-bitcoin-law-tourism-up-30-percent-imf-senate/ (2022.03.19.)

[383] Lásd részletesebben: Tóth Dávid; Gáspár Zsolt: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. In: Büntetőjogi Szemle Vol. 9, No. 2, 2020. pp. 140-150.

elleni irányelv fényében módosított Pmt. 3. § 47. pontja, mely immár tartalmazza a virtuális fizetőeszköz definícióját. Ez alapján a virtuális fizetőeszköz olyan *„digitális értékmegjelenítés, amelyet nem központi bank vagy közigazgatási szerv bocsát ki, illetve garantál; nem rendelkezik törvényes fizetőeszköz jogi státuszával; elektronikusan tárolható, csereértékként elfogadott, így különösen elektronikusan átadható, illetve elektronikus kereskedésre alkalmas."*

Bár mind a büntető eljárásjogi kódexünk, mind a hazai gyakorlat[384] a fizetésre használt elektronikus adat fogalma alá vonja a kriptovalutákat, a definícióval nem minden szerző ért egyet. Halász Viktor szerint sem a bitcoint, sem az ahhoz hozzáférést biztosító privát kulcsot nem lehet elektronikus adatként definiálni, hiszen maga a kriptovaluta egy pillanatnyi értékmegjelenítés, míg a privát kulcs pedig pusztán egy karaktersor, melyet akár fizikailag (például egy papírfecnire) is fel lehet jegyezni.[385]

Álláspontom szerint ugyanakkor, ha ezen logika szerint tekintünk a kérdésre, akkor más, egyébként az elektronikus adatok fogalma alá tartozó dolgokról is elmondható, hogy leírható különböző kódok sorával vagy még inkább kisarkítva, egyesekkel és nullákkal, melyeket akár – ha elméleti síkon nézzük – szintén képesek lennénk felírni e karakterekkel egy papírfecnire. Dacára annak, hogy a privátkulcs tárolható fizikai vagy más formában is, nem szabad elvonatkoztatni attól a ténytől, hogy az általa biztosított vagyoni érték csak elektronikus adat formájában, egy számítástechnikai rendszer segítségével kinyerhető, illetőleg értékesíthető.

Másodkörben szükségszerű volt megteremteni az eljárásjogi kereteket, felhatalmazást a lefoglaláshoz, melyre a Be. 308. § (3) bekezdése alapján kerülhet sor. A bonyolultabb kérdéskör inkább az, hogy hogyan is kell a lefoglalást foganatosítani. E körben a Be. 315. § tartalmaz útmutatást. Az (1) bekezdésben meghatározott módok ugyanakkor nem feltétlenül működőképesek a kriptovaluták vonatkozásában. Az a) és c) pontok másolat készítését, a b) pont az adat áthelyezését, a d) pont pedig magának az információs rendszernek a lefoglalását teszi lehetővé, míg az e) pont más jogszabályokra utal. A kriptovaluták vonatkozásában – mivel az elkövető vagy más harmadik személy – más eszközről is be tud lépni és az adott kriptovalutákat át tudja utalni, értékesítheti, ezen módok nem megfelelőek. A jogalkotó ugyanakkor ennek orvoslására a (2) bekezdésben lehetőséget nyújt arra, hogy a fizetésre használt elektronikus adattal olyan műveletet végezzenek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza, s így

[384] Vö.: Eszteri Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. In: Infokommunikáció és Jog Vol. 14, No. 1, 2017. p. 30. Cit.:
Szatmáry, 2015. Op.Cit. p. 646.

[385] Halász Viktor: A bitcoin működése és lefoglalása a büntetőeljárásban. In: Belügyi Szemle Vol. 66, No. 7-8. 2018. p. 123.

foganatosítsák a lefoglalást. A lefoglalás legcélszerűbb megvalósítási módja, hogy ún. hatósági tárcákat hozzon létre a nyomozó hatóság, melyen a lefoglalt kriptovalutákat lehet tárolni. Erre a jogszabályi keretet *a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló 11/2003. (V. 8.) IM–BM–PM együttes rendelet 67. § (5)-(6) bekezdései* teremtik meg a lehetőséget. A rendelet 67/A. § (1) bekezdése előírja, hogy a lefoglalás végrehajtásához indokolt esetben szaktanácsadót kell igénybe venni, ugyanakkor a további rendelkezéseket nem tartalmaz arra vonatkozóan, hogy mi számít indokolt esetnek, ez a nyomozó hatóság mérlegelési körébe tartozik. A (4) bekezdés a fizetésre használt elektronikus adat vagyonelkobzás érdekében történő lefoglalásával kapcsolatban rögzíti, hogy a lefoglalást követően haladéktalanul fel kell hívni az érintettet, hogy a bűnjel előzetes értékesítése vagy megváltása kérdésében nyilatkozzon. Az (5) bekezdés alapján – amennyiben az érintett kéri a fizetésre használt elektronikus adat értékesítését – ez csak abban az esetben mellőzhető, ha arra a bizonyítás érdekében szükség van.[386] Az értékesítéssel kapcsolatban felmerülnek azonban a következő gyakorlati problémák:

Milyen platformon/tőzsdén keresztül kerüljenek értékesítésre a kriptovaluták?

E kérdés megválaszolásakor az egyik legfontosabb szempont a megbízhatóság és az, hogy leinformált csatornán folyjon le a tranzakció. Ezen követelményeknek több platform is eleget tud tenni, ugyanakkor – gyakorlati példák hiányában – jelenleg nincsen olyan kiforrott gyakorlat, mely útmutatással szolgálhatnak annak terén, hogy a nyomozó hatóságoknak melyik tőzsdét vagy szolgáltatót kellene választania.

Mikor és milyen árfolyamon kerüljön értékesítésre a lefoglalt kriptovaluta?

E körben szükségszerű vizsgálni, hogy az adott kriptovaluta értékesítése alkalmatlan időre esik-e, hiszen rendkívül nagy árfolyam-ingadozások is elképzelhetőek ebben a rendszerben, úgyhogy álláspontom szerint a lefoglalással érintett nyilatkoztatása során rögzíteni szükséges, hogy milyen árfolyamon kívánja értékesíteni az adott kriptovalutát a nyomozó hatóság és ettől

[386] A fizetésre használt elektronikus adat vonatkozásában a hivatkozott rendelkezéseket (a 67. §, 67/A. §, illetve a 67/B. §) az egyes büntetőeljárási jogi tárgyú igazságügyi miniszteri rendeleteknek a büntetőeljárásról szóló 2017. évi XC. törvénnyel összefüggő módosításáról, illetve hatályon kívül helyezéséről szóló 17/2018. (VI. 27.) IM rendelet ültette be az együttes rendelet szövegébe.

a nyilatkozattétel és az értékesítés foganatosítása között eltelt időben csak bizonyos százalékban (például 5-10%-ban) térhet el. Amennyiben ezt túllépi, úgy szükségszerű lenne az érintett újbóli nyilatkoztatása. Ezáltal az árfolyamkockázatból eredő eltérés és az azzal járó felelősség a lefoglalással érintettre hárítható.

Amennyiben az érintett nem kéri az értékesítést vagy ahhoz nem járul hozzá, van-e lehetősége a nyomozó hatóságoknak a lefoglalt kriptovaluta értékesítésére?

Az értékesítéssel kapcsolatban a Be. 319. § (2)-(3) rendelkezései irányadóak. A (2) bekezdés általános konjunktív feltételeket fogalmaz meg a lefoglalt dologgal kapcsolatban:

- a lefoglalt dologra a bizonyítás érdekében már nincs szükség,
- a lefoglalás megszüntetésének nincs helye, és
- a lefoglalt dologgal kapcsolatban senki nem jelentett be megalapozott igényt.

Amennyiben a fenti feltételek együttesen fennállnak, úgy a (3) bekezdés alapján a bíróság – vádemelés előtti ügyészi indítványra – elrendelheti a lefoglalt dolog értékesítését, ha az

a) gyors romlásnak van kitéve,
b) huzamos tárolásra alkalmatlan,
c) kezelése, tárolása, illetve őrzése – különösen a dolog értékére vagy az előreláthatólag hosszú ideig tartó tárolására tekintettel – aránytalan és jelentős költséggel járna, vagy
d) értéke a lefoglalás várható ideje miatt lényegesen csökkenne vagy ennek veszélye megalapozottan feltehető.[387]

A kriptovaluták esetében, mivel e rendszerben különösen jelentős árfolyamingadozásokkal kell számolni, álláspontom szerint fennáll a d) pontban meghatározott feltétel, mivel a lényeges értékcsökkenés megalapozott veszélye elegendő a feltétel teljesüléséhez. Így tehát a nyomozati szakban vádemelésig, ügyészi indítványra meghozott bírói döntés alapján lehetőség nyílhat az értékesítésre.

Amennyiben a lefoglalt kriptovaluta értékesítésre kerül, úgy ki viseli az árfolyamingadozásokból eredő kockázatot?

[387] Halász Viktor 2018-as tanulmányában még akként vélekedett, hogy a lefoglalt dolgok előzetes értékesítéséhez a szükséges feltételek egyike sem áll fent. Ennek során az új Be.-re tekintettel is fenntartotta álláspontját, hiszen nem volt teljes bizonyossággal kijelenthető, hogy a hosszú tárolás miatt a bitcoin (vagy más kriptovaluta) értéke biztosan csökkenne. Lásd: Halász, 2018. Op.Cit. p. 143.
Az új Be.-nek a 2020. évi XLIII. törvénnyel történő módosítását követően ugyanakkor már az is elegendő, ha ennek a lényeges értékcsökkenésnek a veszélye megalapozottan feltehető. Vö. Be. 319. § (3) bekezdés d) pontja.

Álláspontom szerint érdemes vizsgálni azt a kérdéskört is, hogy a lefoglalt kriptoeszközök értékesítése során ki viseli az árfolyam-kockázatot. A tranzakció lehet negatív, illetőleg pozitív irányú. Negatív irányú, ha a nyomozó hatóság által értékesített kriptovalutáért kevesebb fiat valutát kapunk, mint az elkövetéskori értéke volt. Pozitív irányú az értékesítés, amikor a hatóság általi értékesítés eredményeként nagyobb összegű fiat valutát kapunk, mint az elkövetéskori érték. Ez felvet két lehetséges kimenetelt, melyeket hipotetikus példákon keresztül mutatok be:

1.) Egyrészről, tételezzük fel, hogy az elkövető bűncselekmény útján 200.000,- forint értékű „ABC" kriptovalutát szerzett meg a sértettől. A nyomozó hatóság bizonyos idővel később sikerrel felderítette az elkövető kilétét, akitől sikeresen lefoglalták a kriptovalutát. Az elkövetőt lenyilatkoztatta a nyomozó hatóság az értékesítéssel kapcsolatban, melynek során az elkövető kérte az értékesítést. Az eljárás során eltelt idő alatt azonban az „ABC" nevű kriptovaluta árfolyama „beszakadt", így értéke már csak 40.000,- forintnak felel meg. Ebben az esetben, mivel az elkövetéskori érték számít, a különbséget az elkövetőtől lefoglalt további vagyonból tudja biztosítani a nyomozó hatóság (pl.: számlapénz, ingóságok, zár alá vett ingatlan, stb.). Konkretizálva, az árfolyam-ingadozást az érintett viseli.

2.) Ha maradunk az előző példánál, tehát az elkövetéskori értéke az „ABC" kriptovalutának 200.000,- forint, viszont a nyomozás alatti időszakban az értékesítésig a tízszeresére nő az értéke, akkor hogyan kezelhető ez a változás? Több perspektíva szerint is vizsgálható a helyzet. Egyrészről, ha a sértetti oldalt vizsgáljuk, a sértett részére okozott kár ebben az esetben ugyanúgy 200.000,- forint, tehát ő erre tarthatna jogosan igényt, ugyanakkor az is igaz, hogy amennyiben ebben az időszakban ő rendelkezett volna a saját kriptovalutája felett, akár 2.000.000,- forintért is értékesíthette volna, mellyel 1.800.000,- forinttól esett el az elkövető cselekménye miatt. Másrészről, ha a terhelti oldalt nézzük, a bűncselekmény elkövetése után az elkövető döntése volt, hogy mit kezd a kriptovalutával, végső soron az ő tevékenységének is betudható az értéknövekedés. Harmadrészről, a kriptovalutát a nyomozó hatóság értékesítette, tehát az értéknövekedés végső soron a nyomozó hatóság tevékenysége során teljesedett be, akkor ment végbe, tehát közvetetten az államot is megillethetné a fennmaradó összeg.

Érdekes lehet továbbá annak a vizsgálata, hogy a bűncselekmények tárgyát képező kriptovalutát miként kezeljük. Egyrészről, ha a Be. 319. § alapján kívánja értékesíteni a nyomozó hatóság, akkor a (2) bekezdésben meghatározott konjunktív feltételeknek mindenképpen teljesülniük kell. Ugyanakkor, amennyiben az eljárás során valaki megalapozott igényt jelent be, ez már az értékesítés akadályát képezi. További eljárásjogi kérdést vet fel a sértett viszonya az eltulajdonított kriptovalutájával. E körben felmerülhet problémaként, hogy a sértett a kriptovalutákat, mint polgári jogi igény jelenti-e be és ekként kívánja érvényesíteni, ezt forintosítja-e, az elért értéknövekedés érvényesíthető-e polgári jogi igényként, stb. E kérdések megválaszolása ugyanakkor túlnyomó részben a polgári jog és polgári eljárásjog feladata.

A Pmt. és a Be. fentebb részletezett újításainak köszönhetően tehát megállapítható, hogy a vagyonvisszaszerzés terén eszközölendő intézkedések[388] foganatosításához is biztosított a jogi alap a nyomozó hatóságok számára. Ehhez nagy segítséget nyújt a korábban már említett, Europol keretein belül működő SIRIUS-projekt[389], hiszen a nagyobb kriptovalutákkal foglalkozó szolgáltatók nyomozó hatóságok általi megkeresésére összeállítottak egy listát, mely tartalmazza többek között, hogy az adatkéréssel érintett szolgáltatóval hogyan és miképpen lehet felvenni a kapcsolatot, továbbá, hogy a gyakorlati tapasztalatok alapján milyen többletelvárásokat támasztanak az adatok kiadásához (például ügyészi engedély vagy bírói engedély). Természetesen a lista nem minden szolgáltatót fed le, ugyanakkor az esetek nagy részében segítséget jelenthet az elkövető kilétének megállapításához, illetve a nyomozás folytatásához. Rögzíteni szükséges ugyanakkor, hogy továbbra is léteznek olyan kriptovaluta szolgáltatók, melyek a nyomozó hatóságokkal nem vagy csak meglehetősen csekély mértékben működnek együtt, a megkereséseket figyelmen kívül hagyják, nem szolgáltatnak adatot a számlatulajdonosok személyéről, az egyes tranzakciókról.

10. El-Salvador különleges jogi és gazdasági helyzete: a Bitcoin, mint törvényes fizetőeszköz

El Salvador a Bitcoin-törvény hatályba lépésével a világ első országává vált, ahol törvényes fizetőeszközként ismerték el a Bitcoint. Az törvény elfogadása után a lakosság, a hasonló gazdasági helyzetben lévő környező országok és – talán nem túlzás kijelenteni, hogy – az egész

[388] Lásd: Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. In: Magyar Jog Vol. 62, No. 11, 2015. p. 639-647.
[389] https://www.europol.europa.eu/operations-services-innovation/sirius-project (2022.03.15.)

világ izgatottan figyeli a latin-amerikai országban zajló eseményeket. Egyesek lehetőséget látnak a Bitcoinban arra, hogy hosszútávú és fenntartható gazdasági fejlődést érjen el az ország, mások szkeptikusak és aggályaikat fejezik ki az intézkedéssel szemben. A továbbiakban El Salvador gazdasági hátterének rövid felvázolása után a Bitcoin-törvény és az annak bevezetésére irányuló részletszabályokat tartalmazó szabályzat vizsgálatát, illetve a törvény nemzetközi és nemzeti szintű fogadtatásának áttekintését tűztem célul.

10.1. Áttekintés

A 2021-es év nyarának talán a legnagyobb – a kriptovaluták világához kapcsolódó – története volt a Bitcoin törvényes fizetőeszközként történő bevezetéséről szóló törvény elfogadása El Salvadorban. A törvényről szóló első hírek 2021. júniusában, az elfogadását követően járták be az online médiát, mely egyrészről köszönhető annak, hogy az ország elnöke, Nayib Bukele meglehetősen erős propagandát folytatott a Bitcoin legitim fizetőeszközként történő elfogadása mellett. A politikus reményei szerint éves szinten mintegy 400 millió dollárral csökkennek az el salvadoriak kiadásai, mivel az ország bruttó hazai termékének cca. 23 százalékát teszik ki az Egyesült Államokban élő salvadoriak hazautalásai, mely tranzakciók jutalékai ekképpen kikerülhetőek lennének.[390]

A Bitcoin rákényszerítése a lakosságra kétséget kizáróan egy kockázatos döntés, melynek lehetséges negatív hatásai megbecsülhetetlenek. Felmerül a kérdés, hogy miért határozott így az el salvadori vezetés, illetve milyen okok állnak a lépés hátterében. A kérdés megválaszolásához adekvátnak tartom El Salvador gazdaságának áttekintését az elmúlt néhány évtized viszonylatában. A térségben fennálló problémák gyökere meglehetősen régre nyúlik vissza, ugyanakkor a legnagyobb hatásukat az 1980-1990-es évek alatt fejtették ki, ekkor ugyanis az országban egy jelentős polgárháború zajlott, mely teljes egészében tönkretette El Salvador gazdaságát és infrastruktúráját. Az 1990-es évek közepére az ország kibővítette a szolgáltatóiparát, továbbá a 2000-es évek elejére megfigyelhető volt a növekedés a mezőgazdasági termékek exportja terén is, illetve gyarapodtak az újjáépítési projektek is.[391] Az ország hivatalos pénzneme eredetileg a peso volt az 1883-as első pénzügyi törvény óta, melyet 1892-ben Carlos Ezeta elnök neveztetett át colónra, ezzel tisztelegve Kolombusz Kristóf előtt.

[390] „Elindult a kísérlet, mától hivatalos fizetőeszköz a bitcoin a világ egyik országában” https://www.portfolio.hu/uzlet/20210907/elindult-a-kiserlet-matol-hivatalos-fizetoeszkoz-a-bitcoin-a-vilag-egyik-orszagaban-499444, (2021.09.20.)
[391] „Economy of El Salvador” https://www.britannica.com/place/El-Salvador/Economy, (2021.09.21.)

A salvadori colón (SVC) váltópénze a centavo volt, melyből 100 egység jelentett egy colónt. Ugyan a colón teljes mértékben csak 1919-re váltotta fel a peso-t, értéke 1931-ig az amerikai dollárhoz kötődött. A 20. század ezt követő részében a colón önálló valutaként állt helyt, míg végül a polgárháború után az ország gazdasági stabilizálásának céljából a 2001-es pénzügyi integrációs törvény[392] egy rögzített árfolyamot határozott meg az amerikai dollár és a salvadori colón között. A törvény értelmében emellett az amerikai dollár is elfogadásra került az országban, mint törvényes fizetőeszköz, a salvadori colón mellett, melyet azóta sem vontak ki a forgalomból.[393] Óscar Cabrera, a Központi Bank korábbi elnöke szerint az alkalmazott árfolyam[394] nem teremtette meg kellőképpen a vásárlóerő paritását, hiszen aki 875 colónt keresett, a törvény értelmében 100 dollárra tudta átváltani, míg ugyanez az intézkedés bevezetése előtt meghaladta a 200 dollárt. A lakosság tehát a gyakorlatban egy éjszaka alatt elveszítette a vásárlóerejének felét.[395] A dollarizáció tehát csak részben működött El Salvadorban, ugyanakkor elmondható, hogy jelentősebb gazdasági fejlődést nem hozott az országnak. Nayib Bukele, aki 2019-ben kezdte meg öt évre szóló elnöki megbízatását, ígéretet tett arra, hogy javítani fogja El Salvador befektetési környezetét, melyet átjár a bizonytalanság a befektetők részéről, akik a korrupciótól[396] tartva nem mernek nagy beruházásokat kötni az országban. Emellett célul tűzte, hogy fellendíti a gazdaságot[397], így részben ennek az ígéretének köszönhető a Bitcoin-törvény bevezetése. A törvény rendkívül megosztó fogadtatásban részesült a lakosság körében, de egy dologban mindenki egyetért, mégpedig abban, hogy az elnök politikai karrierjének sorsa a Bitcoin-törvény rövid- és hosszútávú eredményeivel fog összefonódni. A tanulmány a továbbiakban a fent említett törvény és a bevezetésének megkönnyítése céljából kiadott szabályzat egyes elemeinek áttekintését, valamint az intézkedés nemzeti és nemzetközi fogadtatásának összevetését célozza.

[392] Decreto No. 201. – Ley de Integración Monetaria. A teljes törvényszöveget lásd eredeti nyelven: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072919515_archivo_documento_legislativo.pdf, (2021.09.21.)
[393] „SVC (El Salvador Colon)" https://www.investopedia.com/terms/forex/s/svc-el-salvador-colon.asp, (2021.09.21.)
[394] 1 USD = 8,75 SVC
[395] „El Salvador marks 20 years of dollarization with weak economic impulse" https://ticotimes.net/2021/01/04/el-salvador-marks-20-years-of-dollarization-with-weak-economic-impulse, (2021.09.21.)
[396] Lásd bővebben: Kőhalmi László: A korrupció. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2015, továbbá
Kőhalmi László: A korrupcióprevenció lehetőségei az üzleti szektorban. In: Magyar Jog Vol. 63, No. 5, 2016. pp. 290-298.
[397] „El Salvador" https://www.heritage.org/index/country/elsalvador, (2021.09.21.)

10.2. A Bitcoin-törvény rendelkezései

El Salvador helyzete kiemelkedő jelentőséggel bír, hiszen a 2021-es „Bitcoin-törvény”[398] („Ley Bitcoin”) elfogadásával a világ legelső országaként ismerte el a Bitcoint törvényes fizetőeszközként.[399] A törvény 2021. június 9-es elfogadásával és annak 2021. szeptember 7-ével történő hatályba léptetésével[400] rendkívül kevés idő állt rendelkezésére az új szabályozásnak megfelelő körülmények előteremtésére, illetve a lakosság átállására, ami jelentős nehézségeket okozhat, hiszen az új jogszabály az eddig fennálló állapothoz képest nagy mértékű változást célzott. Ezeknek a változásoknak a tartalma a következő:

- az amerikai dollár és a Bitcoin közötti átváltási árfolyamot a piaci viszonylatok határozzák meg[401],
- minden árat fel lehet tüntetni Bitcoinban[402],
- bármely adójellegű hozzájárulás teljesíthető Bitcoinnal[403],
- a Bitcoin átváltása – a többi törvényes fizetőeszközhöz hasonlóan – nem esik többé a tőkejövedelem adó hatálya alá[404],
- számviteli célokra az amerikai dollár használatos referenciaként[405],
- minden gazdasági szereplőnek el kell fogadnia a Bitcoint, mint fizetőeszközt, ha valaki azt áruért vagy szolgáltatásért cserében felajánlja[406],
- az állam – a magánszektor sérelme nélkül – olyan alternatívákat kínál, melyek lehetővé teszik a felhasználók számára a Bitcoin tranzakciók lebonyolítását, mint például a Bitcoin és az amerikai dollár közötti azonnali és automatikus átváltás lehetősége[407], emellett az állam támogatja továbbá a szükséges képzést, illetve a kellő mechanizmusokat, hogy a lakosság hozzáférhessen a Bitcoin tranzakciókhoz[408],

[398] Decreto Legislativo No. 57, de fecha 8 de junio de 2021
[399] „El Salvador, primer país del mundo en reconocer al Bitcoin como moneda de curso legal” https://www.asamblea.gob.sv/node/11282?fbclid=IwAR0caEsCLqZvcZeBFv1r6VsVqeDqOarJ7f0SHDth4GE9E7zxwe2f5bLlr9U, (2021.08.31.)
[400] „La Ley Bitcoin de El Salvador” https://www.forbes.com.mx/nuestra-revista-la-ley-bitcoin-de-el-salvador/, (2021.08.31.)
[401] Ley Bitcoin, 2. cikk
[402] Ley Bitcoin, 3. cikk
[403] Ley Bitcoin, 4. cikk
[404] Ley Bitcoin, 5. cikk
[405] Ley Bitcoin, 6. cikk
[406] Ley Bitcoin, 7. cikk
[407] Az átváltási lehetőség működését, illetve annak korlátait a törvény 9. cikkének értelmében az erre a célra kiadott szabályzat határozza meg.
[408] Ley Bitcoin, 8. cikk

- az állam a 10. cikkben hangsúlyozza, hogy vállalja – egy végrehajtó szerven keresztül – a törvény alkalmazásához szükséges intézményi struktúra kiépítését.

A törvény záró rendelkezéseiben, pontosabban a 12. cikkben került rögzítésre a 7. cikkben taglalt kötelezettség (tehát a Bitcoin, mint fizetőeszköz elfogadására irányuló kötelezvény) alóli felmentés esete, mely azon gazdasági szereplőket mentesíti, akik „ismert és nyilvánvaló okokból kifolyólag nem rendelkeznek a Bitcoin tranzakciók lefolytatásához szükséges technikai feltételekkel". Ugyanezen cikken belül újfent megjelenik egy állami kötelezettségvállalás, miszerint megteszi a szükséges lépéseket annak érdekében, hogy a népesség számára elérhetővé váljanak a Bitcoin tranzakciók.[409] Szintén ezen rendelkezések között szerepel egy visszaható hatályú intézkedés bevezetése is, miszerint minden olyan dollárban kifejezett kötelezettség, mely a törvény hatályba lépése előtt keletkezett, teljesíthető Bitcoin-nal.[410] Kiemelendő a törvény 14. cikkében rögzített rendelkezés, miszerint a Bitcoin-törvény különleges jogerővel rendelkezik az alkalmazását illetően, melynek értelmében minden, a rendelkezéseivel ellentétes törvényt derogál.

10.3. A törvény alkalmazása és annak részletszabályai

A Bitcoin-törvény elfogadását követően El Salvador központi bankja (Banco Central de Reserva de El Salvador) 2021. augusztus 17. dátummal kihirdette a Bitcoin-törvény gyakorlati alkalmazásának megkönnyítésére irányuló szabályzatát[411] (továbbiakban Szabályzat). Ennek célja, hogy különböző elektronikus mechanizmusokon keresztül szabályozza azon, a pénzügyi szervezetek és szolgáltatók közötti kereskedelmi kapcsolatokban fennálló jogokat és kötelezettségeket, amelyek a digitális tranzakciók és fizetések megfelelő működéséhez járulnak hozzá.[412] Alanyi körét tekintve a Szabályzat kiterjed minden olyan bankra, hitelintézetre és takarékszövetkezetre, amelyek a Bitcoin és a dollár közötti átváltási szolgáltatást kívánnak nyújtani digitális Bitcoin tárca-szolgáltatásokon, pénzváltókon, Bitcoin és dollár közötti pénzforgalmi szolgáltatásokon, vagy bármilyen – a Szabályzathoz kapcsolódó termékek vagy szolgáltatások értékláncában résztvevő – ügynökön keresztül.[413]

[409] Ley Bitcoin, 12. cikk
[410] Ley Bitcoin, 13. cikk
[411] „Normas técnicas para facilitar la aplicación de la Ley Bitcoin"
[412] Szabályzat 1. cikk
[413] Szabályzat 2. cikk

10.3.1. Fogalmi alapvetések

A norma első fejezetében a célmeghatározáson és az alanyi kör behatárolásán kívül megjelenik egy viszonylag rövid fogalomgyűjtemény, melyben a Szabályzat – és azon keresztül a Bitcoin-törvény – alkalmazásának szempontjából lényeges kifejezések szerepelnek. A jogalkotó a fogalommeghatározásoknál inkább praktikussági szempontok alapján járt el, így részleteiben nem boncolgatta a szakkifejezések technikai sajátosságait, mélységében tehát nem foglalkozott az informatikai nézőpontból releváns jellegzetességekkel. Ennek egyik vetülete, hogy a fogalmak egy része nem kellően tisztázott, ugyanakkor nem informatikai szakemberek számára készült szabályzatról lévén szó, a jogalkotó a közérthetőséget helyezte előtérbe. Fontosabb tény viszont, hogy mivel a Szabályzatot El Salvador központi bankja a kormánnyal együttműködve dolgozta ki és jelentette meg, így ezek a fogalmak az állam álláspontját is tükrözik bizonyos definíciókkal kapcsolatban. Kiemelendőek az említett elemek közül – a teljesség igénye nélkül – a következők:

- Bitcoin: a Bitcoin-törvény szerinti törvényes fizetőeszköz, mely blokklánc-technológiára épül.
- Bitcoin-ATM: olyan elektromechanikai vagy digitális eszközökkel felszerelt gép, mely lehetővé teszi – más szolgáltatások mellett – készpénz felvételét, az egyes számlák közötti átruházásokat, illetve szolgáltatások fizetését.
- Digitális pénzváltó (exchange): a Pénzügyi Felügyelet által hitelesített, részvénytársaság formájában működő olyan gazdasági szervezet, mely Bitcoin és dollár közötti átváltási szolgáltatást nyújt, illetve aminek tevékenysége a Bitcoin adás-vétele elektronikus platformon vagy informatikai alkalmazáson keresztül a piaci kereslet-kínálati viszonyok által meghatározott árfolyamon.
- Bitcoin-letétkezelő: olyan vállalatok, amelyek 3. fél nevében letétkezelési szolgáltatásokat nyújtanak Bitcoin, vagy az ahhoz történő hozzáférés eszközei számára, privát titkosítási kulcsok formájában.
- Bitcoinnal és dollárral fizetési szolgáltatást nyújtó vállalkozások: olyan fix tőkével rendelkező részvénytársaságok, melyek célja a Bitcoinban, illetve dollárban történő fizetési szolgáltatásokra korlátozódnak, az erre a célra meghatározott követelményeknek megfelelve.
- Decentralizált nyilvántartás vagy blokklánc-technológia: olyan támogatási infrastruktúra és protokollok, melyek lehetővé teszik a különböző helyeken található

számítógépek számára tranzakciók lefolytatását és érvényesítését és a nyilvántartás aktualizálását egy hálózaton keresztül történő szinkronizálás útján.[414]

10.3.2. A felügyelet alatt állók kötelezettségei

A Szabályzat második fejezetében általános, illetve speciális kötelezettségeket állapít meg a felügyelet alatt álló piaci szereplők részére, melyek az alanyi kör tárgyalásánál már felsorolásra kerültek. Az általános követelmények között szerepel, hogy a szolgáltatók az üzleteiket becsülettel és sértetlenül folytassák le, legyenek kellő figyelemmel az ügyfelek szükségleteire és érdekeire, a velük történő kommunikáció során tisztán és világosan fogalmazzanak, legyen elegendő pénzügyi és nem pénzügyi forrásuk a szolgáltatások nyújtásához és az ügyfelek kezeléséhez, illetve hogy hatékonyan, kellő hozzáértéssel, óvatossággal és szorgalommal lássák el az adminisztrációs feladataikat, illetve ezeket az elveket tartsák szem előtt az üzletek lebonyolítása során, beleértve a megfelelő kockázatkezelést, mind a vállalkozás, mind az ügyfelek számára. Az általános kötelezettségek között szerepel továbbá, hogy a vállalkozás rendelkezzen megfelelő tőkével az ügyfeleik pénzének, illetve eszközeinek védelmére, amennyiben felelősek értük. Emellett rendelkezzenek hatékony vállalatirányítási megállapodásokkal, magas színvonalú biztonsági hozzáférési protokollal és rendszerrel, pénzügyi bűncselekmények (pl.: pénzmosás, terrorizmus finanszírozása) megelőzésére és felderítésére irányuló szabályrendszerrel, illetve ún. készenléti megállapodásokkal a vállalkozás lehetséges felszámolására irányulóan.[415]

A Szabályzat az 5. cikkben nevesíti az üzleti modellre vonatkozó speciális követelményeket, melyek a következők:

- fogyasztóvédelmi politika és eljárás szabályozása,
- meghibásodások vagy megszakítások esetére történő készenléti mechanizmusok létrehozása,
- minden műveletről biztonsági mentés készítése, illetve annak megőrzése az adott művelet végrehajtásától számított 15 évig,
- a pénzmosás elleni törvény alanyaként a nemzeti, illetve emellett a nemzetközi pénzmosás elleni rendelkezések betartása, amely kiterjed különösen:
    - a kockázatalapú megközelítésre és kezelési intézkedésekre;
    - az ügyféladatok nyomon követhetőségére és továbbítására;

[414] Szabályzat 3. cikk
[415] Szabályzat 4. cikk

- az ügyfél -átvilágításra;
- a politikai személyek átvilágítására;
- az új technológiák alkalmazására;
- az elektronikus átutalások nyomon követésére, ellenőrzésére és jelentésére;
- a belső ellenőrzésekre; illetve egyebek mellett
- a gyanús tranzakciók jelentésére.

- világos és időszerű felvilágosítás az ügyfeleknek a nyújtott szolgáltatásokról, a hozzájuk való hozzáférés feltételeiről, beleértve az árakat és jutalékokat,
- információszolgáltatás a hatóságok részére, az általuk megszabott határidőn belül,
- a felhasználási szabályok és a Bitcoin használatával kapcsolatos kockázatok közzététele,
- oktatási programok létrehozása az adott piaci szereplő termékeiről és a Bitcoin használatáról,
- képzési programok létrehozása az alkalmazottak számára,
- a vállalatirányítási és kockázatkezelési politikájának a Szabályzathoz történő egyeztetése.[416]

10.3.3. A Szabályzat előírásai a pénzmosás és a terrorizmus finanszírozásának vonatkozásaiban

A törvény ellenzőinek egy része a kriptovaluták és a pénzmosás összefüggéseiben[417] látja az új fizetőeszköz veszélyeit, nem alaptalanul, hiszen a pénzmosásnak, illetve a terrorizmus finanszírozásának[418] egy olyan, viszonylag új keletű metodikáját segítik elő, melyek mind a nyomozás, mind a büntetőeljárás számára jelentős kihívásokat támasztanak, illetve az

[416] Szabályzat 5. cikk
[417] Lásd: Gál István László: A pénzmosás új elkövetési tárgya. In: Bujtár Zsolt; Szívós Alexander Roland; Gáspár Zsolt; Szilovics Csaba; Breszkovics Botond (szerk.): Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet - Válogatott tanulmányok. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2021. pp. 105-112.
[418] Lásd bővebben: Gál István László: A terrorizmus finanszírozásának fogalma és technikái a XXI. században. In: Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata Vol. 14, No. 2, 2016. pp. 81-98.,
Gál István László: The sources and techniques of the terrorist financing. In: Nikolina Grbić Pavlović (szerk.): Usaglasavanje Pravne Regulative sa Pravnim Tekovinama (Acquis communautaire) Evropske Unije: stanje u Bosni i Hercegovini i iskustva drugih: zbornik radova. Banja Luka, Think Tank Banja Luka, 2017. pp. 163-173., továbbá
Gál István László: Freedom, security, terrorism and terrorist financing. In: Zoran Pavlović; Ivana Stevanović (szerk.): Freedom, Security: the Right to Privacy = Međunarodna naučna konferencija "Sloboda, bezbednost--pravo na privatnost: zbornik radova. Novi Sad, Instituta za kriminološka i sociološka istraživanja, 2017. pp. 419-437.

említetteken túlmenően más bűncselekmények megkönnyítésére vagy elfedésére is alkalmazzák a bűnelkövetők. A Szabályzat VII. fejezetében foglalkozik a pénzmosás, a terrorizmus finanszírozása és a tömegpusztító fegyverek elterjedésének megelőzésével. A 36. cikkben a szervezeti struktúrával kapcsolatosan előírja egy megfelelési tisztségviselő megválasztását a kötelezett intézetek részére. Előírja továbbá, hogy a kötelezetteknek létre kell hozniuk egy pénzmosás elleni bizottságot (továbbiakban Bizottság) – A pénzmosás és a terrorizmus finanszírozásának kezeléséről szóló technikai szabályokkal összhangban –, melyet a Központi Bank Szabályozási Bizottságának is jóvá kell hagynia.[419] A Bizottságnak legalább öt taggal kell rendelkeznie, melyek: az igazgatótanács igazgatója vagy azzal egyenértékű személy, a vezérigazgató vagy az ügyvezető igazgató, a kockázati és műveleti vezető vagy igazgató, a jogi igazgató vagy azzal egyenértékű személyek, illetve a fent említett megfelelőségi tisztségviselő.[420]

A Szabályzat 43. cikke foglalkozik részletekbe menően a digitális azonosításra vonatkozó követelményekkel. Ennek eszközei között nevesíti többek között a digitális adatlábnyomok rekordját, a hitelesítési folyamatokat, a biometrikus adatokat, a személyi azonosító okmányok szkennelését, a földrajzi helymeghatározást, az IP-cím felismerését, más hasonlóképpen szigorú és megmásíthatatlan technikák alkalmazásával együtt.

Az állami tisztségviselőkkel és a politikai közszereplőkre is kitér a Szabályzat a 46-47. cikkben, ahol felsorolja azokat a személyeket, akiknek a második mellékletben szereplő adatlapot kell kitölteniük. Ennek keretein belül nyilatkozniuk kell a betöltött tisztségükről, a kinevezésük időtartamáról, a gazdasági tevékenységükkel kapcsolatba hozható üzleti partnereikről, a házas- vagy élettársukról, illetve azon gazdasági társaságokról, melyek hozzá kapcsolhatóak.

10.4. A Bitcoin-törvény fogadtatása

Az új törvénnyel szembeni kétségek és a Bitcoin-szkepticizmus jegyében El Salvadorban 2021 augusztusában és a törvény hatályba lépését követő napokban folyamatos tüntetésekkel kívánta demonstrálni a nép az aggodalmát. A tiltakozók egy része egyfajta korrupt, állami pénzmosást vélt gyanítani az újonnan bevezetett fizetőeszköz mögött, míg mások a jövőjüket, többek között

[419] Szabályzat 37. cikk
[420] Szabályzat 38. cikk

például a nyugdíjukat féltették[421], hiszen az – El Salvador által immár viszonylag régóta[422] törvényes fizetőeszközként használt – amerikai dollár továbbra is egy stabilabb, megbízhatóbb opció a salvadoriak szemében.[423] A Közép-Amerikai Egyetem (Central American University) augusztusi felmérése szerint az el salvadori lakosság 65%-a nem ért egyet a szóban forgó törvénnyel, mindazonáltal ugyanezen felmérés eredményei szerint – dacára a népszerűtlen új törvénynek – Nayib Bukele támogatottsága az ország lakosságának körében cca. 76% körülire tehető.[424]

Miközben a lakosság nagy része szkeptikusan fogadta a törvényt, nem túlzás kijelenteni, hogy a fél világ kíváncsian követi figyelemmel az el salvadori eseményeket. Egyrészről a kripto-befektetők számára sem tiszta, hogy miképpen fogja befolyásolni a kísérlet a Bitcoin árfolyamát, másrészről több hasonló gazdasági helyzetben – és az Egyesült Államok valutájától való gazdasági függésben – lévő ország számára is felmerülhet a Bitcoin törvényes fizetőeszközként történő bevezetésének lehetősége, amennyiben a kísérlet pozitív tapasztalatokkal zárul.

A nemzetközi életben is megosztó a fogadtatása a Bitcoin törvényes fizetőeszközként történő elismerésének. A törvény hatályba lépése előtt El Salvador a Világbankhoz fordult az új fizetőeszköz bevezetéséhez történő segítségnyújtás reményében, ugyanakkor a kérelem elutasításra került. Ennek okául a Világbank egyrészről a transzparencia hiányát, másrészről a Bitcoin-bányászat környezetkárosító hatásait jelölte meg.[425] A Világbank mellett a Nemzetközi Valutaalap (International Monetary Fund, a továbbiakban IMF) is kifejezte aggályait az el salvadori helyzettel kapcsolatban. A szervezet szerint a Bitcoin egy túlságosan ingatag rendszer, amely elrugaszkodott az igazi gazdaságtól, így ehelyett egy saját, eddig nem létező rendszert kellett volna létrehoznia El Salvadornak.[426] A kriptovaluták előnyeinek említése

[421] „Bitcoin law protests break out in El Salvador as Central American neighbours wait to see its success" https://www.euronews.com/next/amp/2021/08/28/bitcoin-protests-break-out-in-el-salvador-as-central-american-neighbours-wait-to-see-its-s?fbclid=IwAR3xrHi-HIJ2QhLpWTf3yAwlxgp59CCzom0ylwXJVjnPMH9FNm2fH4vDOfY, (2021.09.15.)

[422] Lásd: https://elpais.com/diario/2001/01/03/internacional/978476403_850215.html, (2021.09.15.)

[423] Fontos megjegyezni, hogy a törvény értelmében a Bitcoin nem váltja fel az amerikai dollárt teljesen, az USD továbbra is törvényes fizetőeszköz marad El Salvadorban.

[424] „Glitches, protests as Bitcoin becomes legal tender in El Salvador" https://www.aljazeera.com/economy/2021/9/7/glitches-protests-as-bitcoin-becomes-legal-tender-in-el-salvador, (2021.09.15.)

[425] „World Bank rejects El Salvador request for Bitcoin help" https://www.bbc.com/news/business-57507386, (2021.09.20.)

[426] Akár a digitális jegybankpénz (CBDC) is felmerülhetett volna egy lehetőségként, mely nagyobb mértékű függetlenséget és stabilitást biztosított volna az ország részére vagy a stabilpénzek közül azok, melyek USA dollárhoz kötött értéke a lakosság az új pénznem bizalmát is erősíthette volna. A témáról lásd bővebben: Bujtár Zsolt: A digitális jegybankpénz kihívásai a monetáris politika területén. In: Bujtár Zsolt; Szívós Alexander Roland; Gáspár Zsolt; Szilovics Csaba; Breszkovics Botond (szerk.): Kriptoeszközök világa a jog és gazdaság

mellett az IMF kiemelte, hogy bár léteznek viszonylag biztonságos kriptoeszközök, az azok által hordozott veszélyek és kiadások túlmutatnak a potenciális előnyökön. Végül az IMF is megjegyezte a Bitcoin-ökoszisztéma környezetkárosító hatásait – kiváltképp a bányászat és az áramfogyasztás összefüggésében – melyek jelentős ökológiai problémákat eredményezhetnek.[427]

10.5. Összegző gondolatok

A rövidtávú tapasztalatok alapján kijelenthető, hogy a Bitcoin törvényes fizetőeszközként történő használatának veszélyei már a törvény hatályba lépésének első napján megmutatkoztak, ugyanis egy nap leforgása alatt majdnem 10.000 dollárt esett a Bitcoin árfolyama[428], ami tökéletesen tükrözi a stabilitás és a szabályozottság hiányát. Az alábbi grafikonon jól látható az el salvadori kísérlet hatása a Bitcoin árfolyamára:

szemszögéből: Konferenciakötet - Válogatott tanulmányok. Pécs, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2021. pp. 123-135., továbbá
Bujtár Zsolt: Central Bank issued digital currency – digital dollar: US CBDC. In: Szilovics Csaba; Bujtár Zsolt; Ferencz Barnabás; Szívós Alexander Roland; Breszkovics Botond; Gáspár Zsolt (szerk.): Gazdasági kihívások a XXI. században: Konferenciakötet. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Pénzügyi Jogi és Gazdasági Jogi Tanszék, 2021. pp. 13-22.

[427] „El Salvador Adopting Bitcoin Is "An Inadvisable Shortcut": International Monetary Fund” https://finance.yahoo.com/news/el-salvador-adopting-bitcoin-inadvisable-230759697.html, (2021.09.20.)

[428] „El Salvador’s Bitcoin Law Is a Farce”
https://foreignpolicy.com/2021/09/17/el-salvador-bitcoin-law-farce/, (2021.09.20.)

5. ábra: A Bitcoin árfolyama 2021. szeptember 5-11. között. Forrás: https://coinmarketcap.com/hu/currencies/bitcoin/ (letöltés dátuma: 2021. 09. 20.)

Felmerül a kérdés, hogy a Bitcoin elfogadására kötelezett gazdasági szereplők árfolyam-ingadozásokból fakadó nagy mértékű veszteségei milyen mértékben kerülnek megtérítésre az állam által. További kérdéseket vet fel az is, hogy milyen gazdasági hatásai lesznek az országra nézve az állam által vásárolt nagyjából 700 Bitcoin[429] értékcsökkenése esetén. Az állami szintű kripto-befektetés mellett El Salvador elkülönített továbbá egy 150 millió dolláros alapot a törvény bevezetésének megkönnyítésére[430], mely amennyiben felhasználásra kerül és a kísérlet nem vezetne pozitív eredményre, további veszteségként lesz értékelhető.

A törvény kiszámíthatatlan gazdasági hatásain túlmenően megemlítendőek az új pénzügyi környezet miatt felmerült jogalkotási és jogalkalmazási kérdések is, hiszen a jogszabály értelmében a Bitcoin nem csak gazdasági, de jogi értelemben is a törvényes fizetőeszközök kategóriájába esik. Ebből kifolyólag mind a polgári, mind a büntető törvénykönyvek revíziója, mind az eljárásjogi szabályok[431] aktualizálása szükséges lenne az esetlegesen kialakuló

[429] „El Salvador buys 150 more bitcoins, president says" https://www.reuters.com/business/finance/el-salvador-buys-150-more-bitcoins-president-says-2021-09-20/, (2021.09.21.)

[430] „El Salvador Congress backs $150 million fund for Bitcoin ahead of adoption as legal tender" https://www.euronews.com/next/2021/09/01/el-salvador-congress-backs-150-million-fund-for-bitcoin-ahead-of-adoption, (2021.09.21.)

[431] Lásd: Tóth Dávid: Digitalization trends in the Hungarian Criminal Procedure. In: Belaj, Ivan; Vajda, Halak Željka; Slobodan, Stojanović (szerk.): 10. Međunarodna Konferencija Razvoj Javne Uprave. Vukovar, Veleučilište Lavoslav Ružička u Vukovaru, 2020. pp. 309-316.

jogviták, illetőleg a jövőben elkövetett bűncselekményekre történő felkészülés szempontjából, ugyanis ennek hiányában a jogalanyok ki fogják használni a szabályok hiányából vagy kétes értelmezéséből fakadó bizonytalanságokat.

11. A kutatási eredmények összefoglalása

11.1. A kutatás és a doktori értekezés áttekintése

A kutatás során a kiberbűnözés fogalmi alapjainak és büntetőjogi kategorizálásának, valamint elkövetői köreinek áttekintését követően megvizsgáltam a kiberbűnözés kialakulásához vezető egyes mozzanatokat, illetőleg a hazai jogalkotásnak az egyes technológiai fejlődési szakaszokra adott válaszát, tehát a hazai jogfejlődést. Ezt követően az értekezés következő részében áttekintettem a kiberbűncselekmények vonatkozásában relevánsnak tekinthető nemzetközi egyezményeket és európai uniós szintű jogforrásokat, majd pedig az uniós és hazai intézményi rendszert. Ezután egyes országok intézményi és jogszabályi környezetének áttekintésével kerestem lehetőségeket és jó gyakorlatokat, melyek felhasználhatóak a kiberbűnözés ellen. Ezt követően vizsgálatom tárgyát a kibertér vonatkozásában új formában megjelent hagyományos bűncselekménytípusok képezték. A tanulmány további részében kiemelt figyelmet szenteltem a kriptovalutákra, illetőleg az azokhoz valamilyen formában kapcsolódó bűncselekményekre, a kriptovaluták vonatkozásában megjelent új bűncselekménytípusokra, illetőleg az általuk emelt büntető anyagi és eljárásjogi aggályokra, kérdésekre. Az értekezés utolsó részében pedig áttekintettem az el salvadori helyzetképet, mely országban a világon elsőként fogadták el a Bitcoin-t hivatalos fizetőeszközként.

Az első fejezetben ismertettem a kutatási célokat és hipotéziseket, a témaválasztásom indokolást, a dolgozat tárgykörének aktualitását, illetőleg a nemzetközi és hazai szakirodalom, valamint a vonatkozó jogforrások feldolgozásának módszereit.

A második fejezetben áttekintettem a kiberbűnözés kapcsán felmerült definíciós törekvéseket, az egyes szerzők álláspontját, illetőleg ahol szükséges volt, ott elhatároltam a társfogalmaktól és határterületektől. Az egyes szerzők a kiberbűnözés típusainak meghatározására is törekedtek, e fejezetben ezen tipizálásokat is megvizsgáltam, illetőleg állást foglaltam annak kapcsán. E fejezet végén a kiberbűncselekmények elkövetői körét vizsgáltam, melynek kapcsán meglehetősen nagy differenciákat találtam a motívumok és a szakképzettség korrelációjában.

A harmadik fejezet célja a kiberbűnözés kialakulásához vezető előzmények és a technológia fejlődésének áttekintése volt. Ennek során megállapítást nyert, hogy az egyes korszakok

technológiai fejlődését lekövető bűnözésre nem mindig tudott megfelelő és időtálló jogszabályokkal reagálni a jogalkotás. A hazai büntetőjogi jogforrások elemzése során rögzíthető, hogy a jelenleg hatályos Büntető Törvénykönyv egy igen hosszú jogfejlődés eredménye, ugyanakkor folyamatos revízióra szorul, hiszen rendelkezései nem örökérvényűek. A technológia fejlődése egyes időszakokban stagnál, máskor kiugró mértékeket produkál, így arra sincsen bevált recept, hogy mennyi időnként kellene elvégezni a jogszabályok revízióját. Erre a gyakorlati jogalkalmazásból kell következtetni.

A negyedik fejezetben áttekintettem a kiberbűnözés kapcsán napvilágot látott legfontosabb nemzetközi szintű egyezményeket, melyek közül kétségtelenül a legjelentősebb a Budapesti Egyezmény. A 2001-ben szövegezett egyezmény kapcsán több kritika is felmerült a témával foglalkozó szerzők tollából. E körben az álláspontom, hogy az egyezmény joghatósági rendelkezései módosításra szorulnak, elavultnak számítanak, dacára annak, hogy az egyezményt kétízben is kiegészítő jegyzőkönyvekkel látták el. A fejezetben úgyszintén megvizsgáltam a legfontosabb európai uniós szintű jogi normákat. Ennek kapcsán a legújabb, legmodernebbnek számító, leginkább releváns irányelvek és rendeletek képezték érdeklődésem tárgyát, megfigyelve ezzel az EU jogalkotási irányait, kereteit a jövőre nézve. A jogforrások felsorolása nem a teljesség igényével történt, ugyanis terjedelmi okokból az értekezés keretein belül erre nem volt lehetőség.

Az ötödik fejezetet az Európai Unió kiberbűnözés elleni eszköztárának szenteltem, melynek során egyrészről összegyűjtöttem az uniós kibervédelmi és kiberbűnözésre szakosodott intézményrendszerének jelentősebb elemeit. Ennek során kiemelt figyelmet kapott az Europol, az ENISA és az Eurojust szerepe. Az uniós intézmények mellett továbbá külön alfejezetet kapott az európai elfogatóparancs, mely jelentősen segíti a kiberbűncselekmények kapcsán folyamatban lévő büntetőeljárásokat.

A hatodik fejezetben áttekintettem a hazai intézményrendszert. Ennek során vizsgáltam az ügyészség és a nyomozó hatóságok felkészültségét a kiberbűnözés vonatkozásában, továbbá azon intézményeket, melyek az ő munkájukat hivatottak segíteni. Megállapítást nyert, hogy a 2020-as évek során a bűnüldöző szervek körében egyfajta paradigmaváltás ment végbe. A rendvédelmi szervek és az ügyészség is kiemelt bűncselekményekként kezeli a kiberbűncselekményeket. Rögzíthető, hogy hangsúlyos szerepe van a kiberbűnözés elleni hatékony fellépésben a személyi állomány képzettségének, szaktudásának, így a kriptovalutákkal és a kiberbűnözéssel kapcsolatos képzések egyre gyakoribbak.

A hetedik fejezetben az egyes országok jogszabályi és intézményi rendszerének vizsgálatával kívántam megtalálni azokat a jó gyakorlatokat, melyek sikeresen hasznosíthatóak a hazai jogalkotásban és jogalkalmazásban. Ennek kapcsán arra a következtetésre jutottam, hogy a hazai intézményi rendszer és a jogforrások más államokéval összehasonlítva meglehetősen fejlettek. Jó gyakorlatként az adathalász tevékenységek önálló tényállásban történő kriminalizálását lehet kiemelni a kolumbiai gyakorlatból.

A nyolcadik fejezetben a hagyományos bűncselekményeket helyeztem górcső alá, illetőleg az állt az érdeklődésem középpontjában, hogy ezen bűncselekmények miként viszonyulnak a kibertérhez és az új technológiai vívmányokhoz. A fejezetben kiemelt hangsúlyt helyeztem a kiberterrorizmus vizsgálatára, azon belül is a kritikus infrastruktúrák ellen elkövetett terrorista motivációjú kibertámadásokra. A második alfejezetben pedig a csalások különböző új elkövetési formáit gyűjtöttem össze, a teljesség igénye nélkül.

A kilencedik fejezet az értekezés magját képezi. E fejezetben részletes áttekintést kívántam nyújtani a kriptovalutákról. A célom a fogalmi áttekintéssel az, hogy a témában laikusnak számító szakemberek számára is érthető képet tudjak vetíteni a kriptovaluták rendszeréről, működéséről. Ezt követően a kriptovaluták vonatkozásában elkövethető hagyományos bűncselekményeket vizsgáltam. Ennek során megállapítást nyert, hogy a pénzmosás, a terrorizmus finanszírozása, a csalás, a piramisjáték szervezése, a lopás, valamint az adócsalás, adóelkerülés is elkövethető a kriptovaluták felhasználásával. Ezt követően a kriptovaluták megjelenését követően felmerült új bűncselekményeket kutattam, melynek során megállapítottam, hogy a kriptovaluták jogellenes bányászata, mint eddig szankcionálatlan cselekmény kriminalizálása szükséges. A fejezet utolsó részében a kriptovaluták vonatkozásában elkövetett bűncselekmények nyomozási problémáit, a büntetőeljárás során felmerülő nehézségeket gyűjtöttem össze.

A tizedik fejezetben egy részletekbe nyúló elemzést kívánok nyújtani El Salvador helyzetéről, ahol a világon elsőként hivatalos fizetőeszközzé avanzsált a Bitcoin. Ennek kapcsán elemzem az ún. „Bitcoin-törvény” rendelkezéseit és rövidtávú hatásmechanizmusát.

Az értekezés záró szakaszában összefoglaltam a kutatás nagyobb mérföldköveit, megállapításait, illetőleg választ kívánok adni a kutatási hipotézisekre.

11.2. A hipotézisekre adott válaszok

1. A hazai büntető jogszabályok meglehetősen nehezen követik a technológiai vívmányok által támasztott új jogi kihívásokat, melynek okán a joghézagot a gyakorlati szakemberek – az analógia tilalmának okán – gyakran nem tudják betölteni.

A hazai büntető anyagi és eljárásjogi szabályanyag áttekintését, annak a gyakorlattal történő összevetését követően megállapítható, hogy a fenti feltételezés igaznak bizonyult. A technológiai fejlődés sosem látott mértéket öntött a 2020-as évek folyamán. E folyamatra a hatályos jogszabályok nem minden esetben adnak megfelelő útmutatást. Az értekezés során több helyen is joghézagok feltárására került sor. Egy új bűncselekménytípus, a kriptovaluták jogellenes bányászatának tényállása álláspontom szerint nem illeszthető be a hatályos büntető anyagi jogszabályanyagba (a Btk. tényállásai alá). E körben szükségesnek tartom egy új büntetőjogi kategória megalkotását.
A büntető eljárásjog vonatkozásában szintén hiányosságokat véltem felfedezni a kutatás során, javarészt a kriptovaluták vonatkozásában.

2. A kriptovaluták és a technológiai alapjukat nyújtó blokkláncok – mint a 21. század egyik legjelentősebb technológiai újítása a hazai jogrendszerben – nincsen kellő mértékben szabályozva, mely meglehetősen sok kérdést vet fel, többek között a büntetőjog és a büntető eljárásjog területén is.

A kriptovaluták megjelenése és elterjedése önmagában rendkívül sok bonyodalmat okozott a jogalkotás számára, melyre nem kizárólag az egyes nemzetek, de a nemzetközi jog és az európai uniós jogalkotás sem tudott azonnali reakcióval szolgálni. A 2020-as évek számtalan jogalkotási novumot hoztak magukkal, melyek körében megemlíthető a DORA-rendelet, a MICA-rendelet és még sok más uniós jogforrás. Mindazonáltal, dacára az új jogalkotási hullámnak, bizonyos jelentős kérdések még mindig fennállnak. Az általános helyzetkép abban áll, hogy sem a nemzeti, sem pedig a regionális vagy nemzetközi jogalkotás nem foglal állást a kardinális jelentőséggel bíró jogkérdésekben. A teljesség igénye nélkül:

- Mi a kriptovaluta jogi definíciója?
- Mi a kriptovaluta jogi besorolása?
- Dolognak minősül-e a kriptovaluta?

A hazai jogrendszerben, azon kívül, hogy a „fizetésre használt elektronikus adat” fogalma alá tudjuk besorolni a kriptovalutákat, nem szolgál megfelelő információval annak jogi kategorizálásával kapcsolatban, illetőleg adós marad a fogalommeghatározással is. Polgári jogi

értelemben nem számít dolognak, hiszen a Ptk. 5:14. § (1)-(3) bekezdéseiben szereplő feltételeknek nem tesz eleget (nem testi tárgy, nem pénz vagy értékpapír, illetőleg nem is állat). A büntetőjogi és büntető eljárásjogi megoldás kulcsa jelenleg abban áll, hogy a lefoglalás tárgya a Be. 308. § (3) bekezdése alapján az ingó dolog mellett a számlapénz, az elektronikus pénz és az elektronikus adat kategóriájára is kiterjed. Ezzel a lépéssel megoldódott ugyan az a kérdés, miszerint a kriptovalutákat le lehet-e foglalni, melynek a vagyonbiztosítás és vagyonvisszaszerzés szempontjából rendkívül nagy relevanciája van. Számos probléma ugyanakkor továbbra is fennáll, melyekre a hatályos szabályozás nem ad megfelelő választ:

- Ki szenvedi el a lefoglalt kriptovaluták árfolyamingadozását? A sértett, az elkövető vagy az állam (nyomozó hatóság)?
- Ki a jogosultja a lefoglalt kriptovaluták árfolyamnövekedéséből eredő bevételnek?
- Be lehet-e jelenteni polgári jogi igényt kriptovalutában?
- A büntetőeljárás során vagy annak befejeztével ki lehet-e adni a sértett részére az ellopott, kicsalt, stb. kriptovalutáját természetben?
- Szóba jöhet-e a kriptovaluták megváltása a büntetőeljárás során? Amennyiben igen, úgy vagy dologként kell kategorizálni vagy pedig a Be. 318. § kiegészítése szükséges az elektronikus adat vagy a fizetésre használt elektronikus adat fogalmával.
- Lehet-e értékesíteni a lefoglalt kriptovalutákat a büntetőeljárás során? Amennyiben igen, úgy a Be. 318. §-hoz hasonlóan dologként kell kategorizálni vagy pedig a Be. 319. § kiegészítése szükséges is az elektronikus adat vagy a fizetésre használt elektronikus adat fogalmával.
- Amennyiben lehetne értékesíteni vagy megváltani, létezik-e alkalmatlan idő a kriptovaluták értékesítésére, megváltására?
- Amennyiben lehet értékesíteni, milyen tőzsdén vagy mely szolgáltató közvetítésével kell értékesíteni azt? Megváltásnál milyen árfolyamot kellene figyelembe venni?

A fentiek alapján a második feltevés is igaznak deklarálható.

3. A kriptovaluták megjelenésével párhuzamosan új típusú bűncselekmények evolválódnak, az ún. „hagyományos" bűncselekmények egy bizonyos része pedig átalakul, melyet a hatályos büntető jogszabályokkal összhangba kell hozni.

A kriptovaluták büntető anyagi és eljárásjogi hatásai a tanulmány egyik fő kutatási vonalát jelentette.

Harmadik hipotézisem két részre bontható, egyrészről feltételezi, hogy új típusú bűncselekmények jelennek meg a kriptovalutákkal kapcsolatosan. E körben álláspontom szerint a kriptovaluták jogellenes bányászatának megjelenésével a hipotézis első felét igazoltnak tekintem. E bűncselekménytípus a kriptovaluták megjelenését megelőzően nem létezett, kialakulásában nagy szerepet játszott a Bitcoin és az Ethereum árfolyamának drasztikus emelkedése, a kriptovaluta-bányászat növekvő népszerűsége.

A feltevés második fele a hagyományos bűncselekményekre fókuszál, melyek egy része a kriptovaluták megjelenésével átalakult, hiszen az elkövetők alkalmazkodtak az új technológiák alakította környezethez és megpróbálják annak előnyeit kihasználni. Az értekezésben vizsgált bűncselekmények közül megállapítható, hogy a kriptovaluták vonatkozásában elkövethetőek az alábbi bűncselekmények:

- pénzmosás,
- terrorizmus finanszírozása,
- csalás,
- piramisjáték szervezése,
- adócsalás, adóelkerülés.

A kriptovalutákkal kapcsolatosan a szerzők jellemzően nem értenek egyet abban, hogy alkalmasnak bizonyulnak-e a pénzmosásra és a terrorizmus finanszírozására. A legtöbb szerző, aki a nemleges álláspontot képviseli arra hivatkozik, hogy a kriptovaluták nyújtotta „védőköpeny" csak pszeudonimitást és nem pedig anonimitást biztosít a felhasználók számára. E körben rögzítendő, hogy egyes kriptovaluták (például a Monero) abszolút nem hajlandóak az egyes államok nyomozó hatóságaival együttműködni, hatósági adatkérésekre, megkeresésekre nem válaszolnak vagy azt kifejezetten megtagadják. Az ilyen kriptovaluták használatával az elkövetők a teljes névtelenség előnyeit élvezhetik, illetőleg, ha ezeket még mixer programokkal párosítják, tovább növelhetik a biztonság fokát. Ez alapján kimondható, hogy a kriptovaluták jelenleg is alkalmasak ezen bűncselekmények elkövetésére.

A fentiek alapján pedig az a konklúzió vonható le, miszerint a harmadik feltevés is igaznak bizonyult.

4. Léteznek olyan új, absztrakt jogesetek, új technológiai megoldásokon alapuló bűncselekmények, melyeket a Büntető Törvénykönyvről szóló 2012. évi C. törvény tényállásai nem fednek le. A Btk. bizonyos mértékű módosítására van szükség.

A kriptovaluták jogellenes bányászata egy olyan új, absztrakt jogeset, mellyel eddig a jogalkotás nem foglalkozott, a jogalkalmazó szervek pedig nem találkoztak olyan gyakorisággal, hogy kiforrott eljárásjogi válaszokkal szolgáljanak a jelenségre.
Az egyes kriptovaluták rendszerében a validációt végző „bányászok" kompenzációt kapnak a rendszertől. A jogellenes kriptovaluta-bányászat elkövetői ezen kompenzációt kívánják a saját kripto-tárcáikba küldeni, míg az annak ellenértékeként megvalósuló számítási kapacitást a sértett(ek) eszközei termelik ki. Úgy vélem, hogy ezen magatartás nem szorítható egyetlen a Btk.-ban nevesített tényállások alá, annak komplexitása miatt külön szabályozandó. Véleményem szerint – összevetve más, a Büntető Törvénykönyvben szereplő tényállásokkal – megállapítható, hogy a jogellenes kriptovaluta-bányászat társadalomra veszélyessége megalapozza a magatartás kriminalizálását.

12. Summary of the Doctoral Research

12.1. Overview of the doctoral research and the thesis

During the research, after reviewing the conceptual bases and criminal categorization of cybercrime, as well as the types of perpetrators, I examined the timeline of the development of cybercrime, as well as the response of the domestic legislation to the individual stages of technological development, i.e. the domestic legal development. After that, in the next part of the thesis, I reviewed international conventions and the legal sources at the European Union level that are considered relevant in relation to cybercrimes. This was followed by the examination of the EU and domestic institutional system. Then, by reviewing the institutional and legislative environment of some countries, I looked for opportunities and good practices that can be used against cybercrime. After that, the subject of my investigation was the traditional crime types that appeared in new forms in relation to cyberspace. In the remaining part of the study, I paid special attention to cryptocurrencies, as well as to the crimes related to them in some form, to the new types of crimes that appeared in relation to cryptocurrencies, and to the concerns and questions raised by them in the field of criminal law and criminal procedural law. In the last part of the dissertation, I reviewed the situation in El Salvador, which country was the first in the world to accept Bitcoin as an official currency.
In the first chapter, I explained the research goals and hypotheses, the justification for my choice of topic, the actuality of the topic of the thesis, as well as the methods of processing the international and domestic literature and the relevant legal sources.

In the second chapter, I reviewed the definitional efforts that arose in connection with cybercrime, the viewpoints of individual authors, and where necessary, I distinguished them from associated concepts and border areas. The individual authors also tried to define the types of cybercrime, in this chapter I also examined these categorizations and took a position in relation to them. At the end of this chapter, I examined the range of perpetrators of cybercrimes. In this regard, I found quite large differences in the correlation of motives and professional expertise.

The purpose of the third chapter was to review the history leading to the evolution of cybercrime and the development of technology. In the process, it was established that during the individual eras, the legislation was not always able to respond to crime with appropriate and durable legislation. During the analysis of the domestic criminal legal sources, it can be noted that the currently effective Criminal Code is the result of a very long legal development, but at the same time it needs constant revision, since its provisions are not valid forever. The progression of technology stagnates in some periods, and produces extraordinary measures in others, so there is no proven recipe for how often legislation should be revised. This must be inferred from the practice of the law enforcement bodies.

In the fourth chapter, I reviewed the most important international conventions that have come to light in connection with cybercrime, of which the Budapest Convention is undoubtedly the most significant. Regarding the convention drawn up in 2001, several criticisms arose from the pens of authors dealing with the subject. In this regard, my position is that the jurisdictional provisions of the convention need to be modified, they are considered outdated, even though the convention was provided with additional protocols twice. In the chapter, I also examined the most important legal standards at the European Union level. In this regard, the latest, most modern, and most relevant directives and regulations were the subject of my interest, thereby observing the legislative directions and frameworks of the EU for the future. The list of legal sources was not done with the intention of completeness, because for reasons of scope this was not possible within the framework of the present thesis.

I dedicated the fifth chapter to the European Union's toolbox against cybercrime, during which I collected on the one hand the major elements of the EU's cyber defense and cybercrime specialized institutional system. In this process, the role of Europol, ENISA and Eurojust received special attention. In addition to the EU institutions, the European Arrest Warrant (EAW) has also received a separate subsection, which significantly helps the ongoing criminal proceedings related to cybercrimes.

In the sixth chapter, I reviewed the domestic institutional system. In doing so, I examined the preparedness of the prosecutor's office and investigative authorities in relation to cybercrime, as well as the institutions that are supposed to assist their work. It was established that a kind of paradigm shift took place among law enforcement agencies during the 2020s. Law enforcement agencies and the prosecutor's office also treat cybercrimes as priority crimes. It can be noted that the training and expertise of personnel plays an important role in effective action against cybercrime, so trainings related to cryptocurrencies and cybercrime are becoming more and more common.

In the seventh chapter, by examining the legal and institutional systems of some countries, I wanted to find good practices that can be successfully utilized in domestic legislation and law enforcement. In this regard, I concluded that the domestic legislation and institutional system are quite developed compared to other states. As a good practice, the criminalization of phising activities in an independent article can be highlighted from the Colombian practice.

In the eighth chapter, I scrutinized traditional crimes, and the focus of my interest was how these crimes relate to cyberspace and new technological achievements. In the chapter, I placed special emphasis on the investigation of cyberterrorism, including terrorist-motivated cyberattacks against critical infrastructures. And in the second sub-chapter, I collected different new forms of frauds in an exemplary manner.

The ninth chapter forms the core of the thesis. In this chapter, I wanted to provide a detailed overview of cryptocurrencies. My goal with the conceptual overview is to be able to project an understandable picture of the system and operation of cryptocurrencies even for professionals who are considered laymen regarding cryptoassets. Afterwards, I investigated the traditional crimes that can be committed in relation to cryptocurrencies. In the process, it was established that money laundering, terrorist financing, fraud, organizing a pyramid scheme, theft, as well as tax evasion and tax fraud can also be committed using cryptocurrencies. After that, I researched new crimes that arose after the appearance of cryptocurrencies, during which I found that the illegal mining of cryptocurrencies, as a previously unsanctioned act, needs to be criminalized. In the last part of the chapter, I collected the investigation problems of crimes committed in relation to cryptocurrencies and the difficulties that arise during criminal proceedings.

In the tenth chapter, I want to provide a detailed analysis of the situation in El Salvador, which is the first country in the world to accept Bitcoin as its official currency. In this regard, I analyze the provisions of the so-called ‘Bitcoin Act’ and its short-term effect-mechanism.

In the final part of the dissertation, I summarized the major milestones and findings of the research, and I want to give answers to the research hypotheses.

12.2. Reflection to the hypotheses

1. It is rather difficult for domestic criminal legislation to follow the new legal challenges posed by technological achievements, which is why practitioners often cannot fill the legal gap, due to the prohibition of analogy.

After reviewing the material and procedural rules of domestic criminal law and comparing them with the practice, it can be concluded that the above assumption proved to be true. During the 2020s, technological development reached an unprecedented level. The current legislation does not provide adequate guidance for this process in all cases. During the dissertation, loopholes in the law were revealed in several places.
In my opinion, the facts of a new type of crime, the illegal mining of cryptocurrencies, cannot be included in the current criminal material legislation (under the facts of the Hungarian Criminal Code). In this context, I consider it necessary to create a new criminal law category.
In relation to criminal procedure law, I also thought I discovered shortcomings during the research, mostly in relation to cryptocurrencies.

2. Cryptocurrencies and the blockchains (that provide their technological basis) are one of the most significant technological innovations of the 21st century. In the domestic legal system these are not sufficiently regulated, which raises quite a lot of questions, including in the field of criminal law and criminal procedure law.

The appearance and spread of cryptocurrencies in itself caused a lot of complications for legislation, to which not only individual nations, but also international law and European Union legislation could not provide an immediate reaction. The 2020s brought numerous legislative innovations, among which the DORA regulation, the MICA regulation and many other sources of EU law can be mentioned. However, despite the new wave of legislation, some significant issues remain. The general picture of the situation is that neither the national, nor the regional or international legislation takes a position on legal issues of cardinal importance. Including but not limited to:

- What is the legal definition of cryptocurrency?

- What is the legal classification of cryptocurrency?
- Is cryptocurrency a thing?

In the domestic legal system, apart from the fact that we can classify cryptocurrencies under the concept of 'electronic data used for payment', it does not provide adequate information regarding its legal categorization and remains indebted to the definition.

In the sense of civil law, cryptocurrency does not count as a thing since it does not meet the requirements of the 5:14. § (1)-(3) paragraphs of the Hungarian Civil Code (it is not a physical object, not money or security, or not an animal). The key to the criminal law and criminal procedure law solution currently lies in the fact that the subject of the seizure, based on 308. § (3) paragraph of the Hungarian Criminal Procedure Code, which covers not only movable property (thing), but also the categories of cash, electronic money, and electronic data. With this step, the question of whether cryptocurrencies can be seized, which is extremely relevant in terms of asset insurance and asset recovery, has been resolved. However, many problems still exist, to which the current regulations do not provide an adequate answer:

- Who suffers from the exchange rate fluctuations of seized cryptocurrencies? The victim, the perpetrator, or the state (investigative authority)?
- Who is entitled to the income resulting from the price increase of seized cryptocurrencies?
- Is it possible to file a civil claim in cryptocurrency?
- During the criminal proceedings or at the end of the proceedings, is it possible to issue the stolen, defrauded, etc. cryptocurrency to the victim?
- Is it possible to redeem cryptocurrencies during criminal proceedings? If so, it must either be categorized as a thing, or 318. § paragraph of the Hungarian Criminal Procedure Code needs to be supplemented with the concept of electronic data or electronic data used for payment.
- Can seized cryptocurrencies be sold during criminal proceedings? If so, it must be categorized as a thing, similarly to those mentioned above, or it is also necessary to supplement 319. § paragraph of the Hungarian Criminal Procedure Code with the concept of electronic data or electronic data used for payment.
- If it could be sold or redeemed, is there an unsuitable time for selling or redeeming cryptocurrencies? - If it can be sold, on which stock exchange or through which service provider should it be sold? What exchange rate should be considered when redeeming?

Based on the above, the second assumption can also be declared true.

3. Parallel to the emergence of cryptocurrencies, new types of crimes are evolving, and a certain part of the so-called 'traditional' crimes is being transformed, which must be brought into line with the current criminal legislation.

The criminal law and procedural law effects of cryptocurrencies was one of the main research lines of the study.

My third hypothesis can be divided into two parts, on the one hand, it assumes that new types of crimes related to cryptocurrencies will appear. In my opinion, with the appearance of illegal mining of cryptocurrencies, I consider the first half of the hypothesis to be justified. This type of crime did not exist before the appearance of cryptocurrencies, the drastic rise in the price of Bitcoin and Ethereum, and the growing popularity of cryptocurrency mining played a major role in its development.

The second half of the premise focuses on traditional crimes, some of which have been transformed by the appearance of cryptocurrencies, as the perpetrators have adapted to the environment shaped by new technologies and are trying to take advantage of it. Among the crimes examined in the thesis, it can be established that the following crimes can be committed in relation to cryptocurrencies:

- money laundering,
- terrorist financing,
- fraud,
- organizing a pyramid scheme,
- tax fraud, tax evasion.

Regarding cryptocurrencies, authors typically disagree on whether they prove suitable for money laundering and terrorist financing. Most of the authors who take the negative position refer to the fact that the so-called 'protective cloak' provided by cryptocurrencies only provides users with pseudonymity and not full anonymity. In this context, it should be noted that some cryptocurrencies (such as Monero) are absolutely unwilling to cooperate with the investigative authorities of individual states, they do not respond to official requests of information, or they expressly refuse to do so. By using such cryptocurrencies, the perpetrators can enjoy the benefits of complete anonymity, and if they are combined with mixer programs, they can further increase the level of security. Regarding this, it can be said that cryptocurrencies are currently still suitable for committing these crimes.

Based on the above, the conclusion can be drawn that the third assumption is also true.

4. There are new, abstract legal cases, crimes based on new technological solutions, which are not covered by the facts of Act C of 2012 on the Criminal Code. A certain amount of modification of the Criminal Code is necessary.

The illegal mining of cryptocurrencies is a new, abstract legal case that has not yet been dealt with by legislation, and law enforcement bodies have not experienced it in such a frequency that they can provide adequate procedural responses to the phenomenon.
In the system of each cryptocurrency, the 'miners' who perform the validation receive compensation from the system. The perpetrators of illegal cryptocurrency mining want to obtain this compensation to their own crypto-wallets, while the computing capacity realized as a counter value is produced by the devices of the victim(s). I believe that this behavior cannot be limited to the facts listed in the Criminal Code, and should be regulated separately due to its complexity. In my opinion, when compared to other facts in the Criminal Code, it can be established that the danger to society of the illegal cryptocurrency mining gives basis for the criminalization of the behavior.

13. Irodalomjegyzék

(dátum nélk.). Letöltés dátuma: 2020. 09 24, forrás: https://www.policija.si/eng/areas-of-work/other-areas/international-cooperation/europol

(dátum nélk.). Letöltés dátuma: 2020. 09 21, forrás: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

(dátum nélk.). Letöltés dátuma: 2021. február 15, forrás: https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Zulassung/Kryptoverwahrgeschaeft/ kryptoverwahrgeschaeft_node_en.html

(dátum nélk.). Letöltés dátuma: 2021. február 15, forrás: https://kriptoakademia.com/2020/03/04/nemetorszag-a-bitcoin-torvenyes-penzugyi-eszkoz

(dátum nélk.). Letöltés dátuma: 2021. január 28, forrás: https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2014/us_v_liberty_reserve_et_al..html

(dátum nélk.). Letöltés dátuma: 2021. január 29, forrás: https://www.justice.gov/opa/pr/owner-bitcoin-exchange-sentenced-prison-money-laundering

(dátum nélk.). Letöltés dátuma: 2020. október 10, forrás: https://academy.binance.com/en/articles/pyramid-and-ponzi-schemes

(dátum nélk.). Letöltés dátuma: 2020. október 7, forrás: https://www.sec.gov/fast-answers/answersponzihtm.html

(dátum nélk.). Letöltés dátuma: 2020. október 7, forrás: https://www.investor.gov/protect-your-investments/fraud/types-fraud/high-yield-investment-programs

(dátum nélk.). Letöltés dátuma: 2021. december 19, forrás: https://www.interpol.int/Crimes/Cybercrime/Cryptojacking

(dátum nélk.). Letöltés dátuma: 2022. március 2, forrás: https://hznews.hangzhou.com.cn/shehui/content/2018-06/16/content_7020998_2.htm

(dátum nélk.). Letöltés dátuma: 2023. 12 23, forrás: https://nki.gov.hu/intezet/tartalom/karrier-lehetosegek/#whitehat

(dátum nélk.). Letöltés dátuma: 2024. 02 19, forrás: https://ugyeszseg.hu/az-ugyeszsegrol/nemzetkozi-kapcsolatok/magas-szintu-nemzetkozi-kapcsolatok/

(dátum nélk.). Letöltés dátuma: 2023. 12 03, forrás: https://ugyeszseg.hu/kozos-nyilatkozatot-fogadtak-el-a-visegradi-negyek-legfobb-ugyeszei-fotoval-a-legfobb-ugyeszseg-sajtokozlemenye/

(dátum nélk.). Letöltés dátuma: 2023. 12 03, forrás: https://ugyeszseg.hu/szandeknyilatkozat-a-visegradi-negyek-es-ausztria-legfobb-ugyeszei-kozott/

(dátum nélk.). Letöltés dátuma: 2023. 12 03, forrás: https://ugyeszseg.hu/nemzetkozi-konferencia-az-ugyeszseg-150-eves-evfordulojan-a-visegradi-negyek-es-ausztria-legfobb-ugyeszei-valamint-az-eurojust-elnoke-reszvetelevel/

(dátum nélk.). Letöltés dátuma: 2023. 12 03, forrás: https://www.jogiforum.hu/hir/2018/09/06/egyuttmukodo-ugyeszek-europaert-a-visegradi-csoport-legfobb-ugyeszei-alairtak-a-visegradi-nyilatkozatot/

(dátum nélk.). Letöltés dátuma: 2024. 02 19, forrás: https://www.eppo.europa.eu/en/background

(dátum nélk.). Letöltés dátuma: 2024. 02 20, forrás: https://www.consilium.europa.eu/hu/policies/eppo/#eppo

(dátum nélk.). Letöltés dátuma: 2024. 02 21, forrás: https://nki.gov.hu/figyelmeztetesek/archivum/megjelent-a-halozati-es-informacios-rendszerek-biztonsagarol-szolo-eu-s-iranyelv/

(dátum nélk.). Letöltés dátuma: 2024. 02 24, forrás: https://www.enisa.europa.eu/about-enisa/regulatory-framework

(dátum nélk.). Letöltés dátuma: 2024. 02 24, forrás: https://www.enisa.europa.eu/about-enisa/about/hu

(dátum nélk.). Letöltés dátuma: 2024. 03 04, forrás: https://e-justice.europa.eu/23/HU/eurojust

(dátum nélk.). Letöltés dátuma: 2024. 03 04, forrás: https://www.eurojust.europa.eu/sites/default/files/2020-12/2020-08_Generic-factsheet_public_Final4_HU.pdf

(dátum nélk.). Letöltés dátuma: 2024. 03 04, forrás: https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

(dátum nélk.). Letöltés dátuma: 2024. 03 04, forrás: https://www.europarl.europa.eu/topics/hu/article/20221103STO48002/harc-a-kiberbunozes-ellen-az-uj-unios-kiberbiztonsagi-torvenyek-magyarazata

(dátum nélk.). Letöltés dátuma: 2024. 03 05, forrás: https://eur-lex.europa.eu/HU/legal-content/summary/european-cybersecurity-network-and-competence-centre.html

(dátum nélk.). Letöltés dátuma: 2024. 03 05, forrás: https://nav.gov.hu/navit/tartalmak/allaspalyazatok/informaciobiztonsag/etikus-hacker-informatikai-biztonsagi-osztaly-20221121

(dátum nélk.). Letöltés dátuma: 2022. 09 19, forrás: https://www.teamviewer.com/en

(dátum nélk.). Letöltés dátuma: 2022. 09 19, forrás: https://anydesk.com/en

(dátum nélk.). Letöltés dátuma: 2024. 03 20, forrás: https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf

(dátum nélk.). Letöltés dátuma: 2024. 03 20, forrás: https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

(2023. 06 20). Forrás: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

(2023. 06 20). Forrás: https://bitcoin.org/hu/

(2023. 06 20). Forrás: https://academy.binance.com/hu/articles/what-is-crypto-mining-and-how-does-it-work

Acerca de colCERT. (2022. 02 07). Letöltés dátuma: 2024. 03 13, forrás: https://www.colcert.gov.co/800/w3-article-198657.html

Akácz, J. (2015). A vagyon elleni bűncselekmények. In I. Kónya (Szerk.), *Magyar Büntetőjog. Kommentár a gyakorlat számára* (old.: 1378-1437). Budapest: HVG-ORAC.

Ashford, W. (dátum nélk.). *Unprotected Kubernetes consoles expose firms to cryptojacking*. Forrás: https://www.computerweekly.com/news/252435544/Unprotected-Kubernetes-consoles-expose-firms-to-cryptojacking

Az európai felügyeleti hatóságok közzétették a DORA rendelet első csomagjába tartozó, az IKT- és harmadik fél kockázatkezelésre és az incidensek osztályozására vonatkozó részletszabályokat. (2024. 01 17). Letöltés dátuma: 2024. 03 05, forrás: https://www.mnb.hu/felugyelet/felugyeleti-keretrendszer/felugyeleti-hirek/hirek-ujdonsagok/az-europai-felugyeleti-hatosagok-kozzetettek-a-dora-rendelet-elso-csomagjaba-tartozo-az-ikt-es-harmadik-fel-kockazatkezelesre-es-az-incidensek-osztalyozasara-vonatk

Balogh, R. (2017). A légiközlekedés biztonsági kihívásai és kockázatai, a velük szembeni terrortámadások elleni védelem követelményei és módszerei. *Hadtudományi Szemle, 10*(3), 463-475.

Bányász, P. (2014). A közlekedést támogató alkalmazások biztonsági aspektusai. In A. Horváth, P. Bányász, & Á. Orbók (szerk.), *Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről* (old.: 47-60). Budapest: Nemzeti Közszolgálati Egyetem (NKE).

Bányász, P. (2014). A közösségi médiahasználat biztonsági kérdései a védelmi iparban. *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 24*(1), 49-67.

Bányász, P., & Orbók, Á. (2013). A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 23*(1 (E-szám)), 188-209.

Bárd, P. (2015). *Az európai elfogatóparancs Magyarországon.* Budapest: Országos Kriminológiai Intézet.

Bardócz, C. (1997). Pénzmosási technikák. *Belügyi Szemle, 35*(3), 74-76.

Barroso Toledo, R. (2011). Los Delitos en Internet: Un enfoque desde la pornografía infantil en la red. *Revista F@ro*(13), 59-71.

Bőczné Neparáczki, A. V. (2020). A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja, 27*(1), 71-86.

Brenner, S. W., & Koops, B.-J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law, 4*(1), 1-46.

BRIGADA CENTRAL DE INVESTIGACIÓN TECNOLÓGICA (B.C.I.T.). (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php

Brill, A., & Keene, L. (2014). Cryptocurrencies: The Next Generation of Terrorist Financing? *Defence Against Terrorism Review*(1), 7-30.

Budapest, U. E. (2018. 08 01). *Vigyázat! Romantikus átverések*. Letöltés dátuma: 2024. 03 10, forrás: https://hu.usembassy.gov/hu/vigyazat-romantikus-atveresek/

Bugár, G., & Somogyvári, M. (2020). Bitcoin: digitális szemfényvesztés, vagy a jövő valutája? *Hitelintézeti Szemle, 19*(1), 132-153. doi:10.25201/HSZ.19.1.132153

Bujtár, Z. (2018). A kriptovaluta ökoszisztéma szabályozási kihívásai. In J. Benke, & T. Fabó (szerk.), *A puro pura defluit aqva. Ünnepi tanulmányok Nochta Tibor professzor 60. születésnapja tiszteletére* (old.: 61-72). Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar.

Bujtár, Z. (2019). Central bank issued digital currencies: is it a solution or a problem? In J. Glavanits, B. Horváthy, & L. Knapp (szerk.), *EU Business Law and Digital Revolution: Selected Studies from New Fields of Technology* (old.: 71-89.). Győr: Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar.

Bujtár, Z. (2020). Central bank-issued digital currencies: - ready, steady, go? In C. Szilovics, Z. Bujtár, B. Ferencz, B. Breszkovics, & A. R. Szívós (Szerk.). *GAZDASÁG ÉS PÉNZÜGYEK A 21. SZÁZADBAN II. - KONFERENCIAKÖTET = BUSINESS AND ECONOMY IN THE 21ST CENTURY II. – CONFERENCE PROCEEDINGS*, old.: 113-123. Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Bujtár, Z. (2021). A digitális jegybankpénz kihívásai a monetáris politika területén. In Z. Bujtár, A. R. Szívós, Z. Gáspár, C. Szilovics, & B. Breszkovics (szerk.), *Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet - Válogatott tanulmányok* (old.: 123-135). Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Bujtár, Z. (2021). Central Bank issued digital currency – digital dollar: US CBDC. In C. Szilovics, Z. Bujtár, B. Ferencz, A. R. Szívós, B. Breszkovics, & Z. Gáspár (szerk.), *Gazdasági kihívások a XXI. században: Konferenciakötet* (old.: 13-22). Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Pénzügyi Jogi és Gazdasági Jogi Tanszék.

Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2014). Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian and New Zealand Journal of Criminology, 47*(3), 391-408. doi:10.1177/0004865814521224

Cámara Arroyo, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*(60), 470-512.

Cano Paños, M. Á. (2016). Odio e incitación a la violencia en el contexto del terrorismo islamista. Internet como elemento ambiental. *Indret*(4).

Castorál, Z., & Bimová, A. (1990). A számítástechnikával kapcsolatos bűnözés. *Belügyi Szemle, 28*(1), 116-121.

Chawki, M., Darwish, A., Khan, M., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction* (Studies in Computational Intelligence. kötet). Springer. doi:10.1007/978-3-319-15150-2

Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism, 7*(1), 80-91.

Criminalidad informática. (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.fiscal.es/web/fiscal/-/criminalidad-informatica?assetCategoryIds=36767

Cyber Resilience Act: MEPs back plan to boost digital products security. (2023. 07 19). Letöltés dátuma: 2024. 03 04, forrás: https://www.europarl.europa.eu/news/hu/press-room/20230717IPR03029/cyber-resilience-act-meps-back-plan-to-boost-digital-products-security

Cybercrime Convention Committee. (dátum nélk.). Letöltés dátuma: 2023. 12 03, forrás: https://www.coe.int/en/web/cybercrime/tcy

Cybercrime Programme Office (C-PROC). (dátum nélk.). Letöltés dátuma: 2023. 12 03, forrás: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

Dávid, G. (1975). Számítástechnika és kriminálstatisztika. *Jogtudományi Közlöny, 30*(1), 32-35.

Delincuencia informática. (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/gdt/index.html

DELITOS INFORMÁTICOS. (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos

Déri, A. (2018). Napjaink informatikai kihívásai - gondolatok a kritikus infrastruktúrák informatikai sérülékenységéről és védelméről. *Rendvédelem, 7*(1), 268-294.

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats*. . Santa Monica, California: RAND Corporation.

Dornfeld, L. (2019). Kiberterrorizmus – a jövő terrorizmusa? In K. Mezei (Szerk.), *A bűnügyi tudományok és az informatika* (old.: 46-63). Pécs - Budapest: Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK), MTA Társadalomtudományi Kutatóközpont.

Dornfeld, L. (2019). Pénzmosás a kibertérben . In Á. Farkas, G. Dannecker, & J. Jacsó (szerk.), *Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre* (old.: 451-461). Budapest: Wolters Kluwer Kft.

Dulin, T., & Kó, J. (1996). A hitelkártya-visszaélésekről. *Belügyi Szemle, 34*(11), 45-60.

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies*(5), 75-81. doi:https://doi.org/10.30525/2256-0742/2018-4-5-75-81

Eszteri, D. (2015). A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a pénz helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola.

Eszteri, D. (2017). Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. *Infokommunikáció és Jog, 14*(1), 25-31.

Ethical Hacker. (dátum nélk.). Letöltés dátuma: 2024. 03 05, forrás: https://www.purdue.edu/science/careers/what_can_i_do_with_a_major/Career%20Pages/ethical_hacker.html

EUCTF. (2022. 08 17). Letöltés dátuma: 2024. 02 24, forrás: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival, 53*(1), 23-40. doi:10.1080/00396338.2011.555586

FATF. (2015. Október). FATF Report: Emerging Terrorist Financing Risks. Párizs. Letöltés dátuma: 2023. 12 12, forrás: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Emerging-Terrorist-Financing-Risks.pdf

Fázsi, L., & Fázsi, L. M. (2009). Megjegyzések a számítógépes bűncselekmények hatályos szabályozásához. *Rendészeti Szemle, 57*(5), 3-11.

Felméry, Z. (2019). A szervezett bűnözés általi internetes fenyegetettség értékeléséről szóló Europol-jelentés ismertetése. *Nemzet és Biztonság: Biztonságpolitikai Szemle, 12*(2), 125-133. doi:10.32576/nb.2019.2.9

Felügyelet. (dátum nélk.). Letöltés dátuma: 2024. 03 05, forrás: https://www.mnb.hu/web/felugyelet

Franco Mahecha, R. (2016). Ciberseguros, la mejor forma de transferir riesgos de ataques informáticos. Universidad Piloto de Colombia.

Funciones del CeCiP. (dátum nélk.). Letöltés dátuma: 2024. 03 13, forrás: https://caivirtual.policia.gov.co/conocenos/funciones

Gábor, T., & Kiss, G. D. (2018). Bevezetés a kriptovaluták világába. In: , Vol. 5, No. 1, 2018. 38. o. *Gazdaság és Pénzügy, 5*(1), 31-65.

Gál, I. L. (2012). *A pénzmosással és a terrorizmus finanszírozásával kapcsolatos jogszabályok magyarázata.* Budapest: HVG-ORAC Lap- és Könyvkiadó.

Gál, I. L. (2016). A terrorizmus finanszírozásának fogalma és technikái a XXI. században. *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 14*(2), 81-98.

Gál, I. L. (2017). Freedom, security, terrorism and terrorist financing. In Z. Pavlović, & I. Stevanović (szerk.), *Freedom, Security: the Right to Privacy = Međunarodna naučna konferencija "Sloboda, bezbednost--pravo na privatnost: zbornik radova* (old.: 419-437). Novi Sad: Instituta za kriminološka i sociološka istraživanja.

Gál, I. L. (2017). The sources and techniques of the terrorist financing. In N. Grbić Pavlović (Szerk.), *Usaglasavanje Pravne Regulative sa Pravnim Tekovinama (Acquis communautaire) Evropske Unije: stanje u Bosni i Hercegovini i iskustva drugih: zbornik radova* (old.: 163-173). Banja Luka: Think Tank Banja Luka.

Gál, I. L. (2018). The 4th EU Directive and the Hungarian AML Practice in 2018. In Z. Pavlović (Szerk.), *Yearbook. Human Rights Protection : "From Unlawfulness to Legality"* (old.: 349-360). Novi Sad: Institute of Criminological and Sociological Research.

Gál, I. L. (2019). 25 Years of Fight Against Money Laundering in Hungary. *Journal of Eastern-European Criminal Law, 6*(2), 62-71.

Gál, I. L. (2021). A pénzmosás új elkövetési tárgya. In Z. Bujtár, A. R. Szívós, Z. Gáspár, C. Szilovics, & B. Breszkovics (szerk.), *Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet - Válogatott tanulmányok* (old.: 105-112). Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Germán, P. (2020. 01 17). *A kriptopiac legveszélyesebb befektetése - Mi is az az ICO?* Letöltés dátuma: 2024. 03 08, forrás: https://cryptofalka.hu/blokklanc/mi-az-ico

Glavanits, J., & Király, P. B. (2018). A blockchain-technológia alkalmazásának jogi előkérdései: a fogalmi keretek pontosításának szükségessége. *JOG ÁLLAM POLITIKA: JOG- ÉS POLITIKATUDOMÁNYI FOLYÓIRAT, 10*(3), 173-183.

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. (2020. 08 13). Letöltés dátuma: 2023. 12 11, forrás: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

Grund, A. B. (2021). A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. *MTA Law Working Papers*(21), 1-37.

Gulyás, O. (2022). A kiberbiztonság és a banki kibervédelem fejlődése napjainkig. *Biztonságtudományi Szemle, 4*(2), 1-13.

Hague, D. R. (2015). Expanding the Ponzi Scheme Presumption. *DePaul Law Review 64, 64*(3), 867-909.

Halász, K. (1975). A polgári ügyek statisztikájának fejlődési távlatai a számítógépre figyelemmel. *Jogtudományi Közlöny, 30*(1), 35-44.

Halász, V. (2018). A bitcoin működése és lefoglalása a büntetőeljárásban. *Belügyi Szemle, 66*(7-8), 117-146.

Halász, V. (2019). A bűncselekményekből származó vagyon nyomon követésének új kihívásai a kibertérben. In Á. Farkas, G. Dannecker, & J. Jacsó (szerk.), *Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre* (old.: 433-443). Budapest: Wolters Kluwer Kft.

Hámori, M. (1973). *Ismerkedés a komputerrel.* Budapest: Tankönyvkiadó.

Hayes, A. (2024. 02 12). Letöltés dátuma: 2024. 03 08, forrás: Stablecoins: Definition, How They Work, and Types: https://www.investopedia.com/terms/s/stablecoin.asp

Herke, C. (2021). A kiberbűnözés és a teljesen önvezető járművek. In A. T. Barabás, & L. Christián (szerk.), *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est* (old.: 211-221). Budapest: Ludovika Egyetemi Kiadó.

Hertelendi, L. (2022). Egy dark weben elkövetett bűncselekmény felderítésének tanulságai, a nemzetközi összefogás jelentősége. *Belügyi Szemle, 70*(3), 607-618. doi:10.38146/BSZ.2022.3.9

Hogyan tároljuk a bitcoint? (2021. 05 12). Letöltés dátuma: 2024. 03 06, forrás: https://www.bitcoinbazis.hu/utmutato/hogyan-taroljuk-bitcoint/

Horváth, J. (2015). Az elektronikai zavarás napjainkban. *Hadmérnök, 10*(1), 183-192.

Informe de Gestión CERT.ar 2022. (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.argentina.gob.ar/noticias/informe-de-gestion-certar-2022

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA 2022. (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

Jasenszky, N. (1990). A számítógépek felhasználási lehetőségei elsőfokú rendőri szerveknél. *Belügyi Szemle, 38*(6), 22-26.

Jekyné Wohlfarth, Z. (1999). Számítógép segítségével elkövetett bűncselekmények. *Belügyi Szemle, 37*(11), 43-50.

Józan, F., & Kőhalmi, L. (2016). Lawyers and Money laundering. *JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW, 3*(2), 130-136.

Kara, I., & Aydos, M. (2019). The Ghost in the System: Technical Analysis of Remote Access Trojan. *International Journal on Information Technologies & Security, 11*(1), 73-84.

Károlyi, L. (1990). A személyi számítógépes rendszerek adatvédelmi problémái. *Belügyi Szemle, 38*(4), 46-51.

Kecskés, A., & Bujtár, Z. (2019). Felvetések a kripto eszközök szabályozása terén. *CONTROLLER INFO, 7*(2), 49-53.

Khan, M., & Yoshihiko, K. (2023). Who Became Victims of Financial Frauds during the COVID-19 Pandemic in Japan? *Sustainability, 15*(4), 1-17.

Király, P. B. (2019). A terrorizmus finanszírozásának új eszközei: a blokkláncok és a kriptovaluták. In R. Bartkó (Szerk.), *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században* (old.: 151-166). Budapest: Gondolat Kiadó.

Klein, T. (2018). A felhőszolgáltatások egyes jogi kérdései - különös tekintettel az Európai Unió szabályozására. In T. Klein (Szerk.), *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről* (old.: 89-122). Budapest: Médiatudományi Intézet.

Korinek, L. (1988). *Rejtett bűnözés.* Budapest: Közgazdasági és Jogi Könyvkiadó.

Kőhalmi, L. (2005). Ügyvédek és pénzmosás. In I. L. Gál (Szerk.), *A pénzmosás elleni küzdelem aktuális kérdései* (old.: 89-97.). Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Kőhalmi, L. (2012). *A büntetőjog alapproblémái.* Pécs: PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet.

Kőhalmi, L. (2015). *A korrupció.* Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Kőhalmi, L. (2016). A korrupcióprevenció lehetőségei az üzleti szektorban. *Magyar Jog, 63*(5), 290-298.

Kőhalmi, L. (2020). Szervezett bűnözés. In A. T. Barabás (Szerk.), *Alkalmazott kriminológia* (old.: 461-474). Budapest: Luvodika Egyetemi Kiadó.

Kökényesi-Bartos, A. (2009). Számítástechnikai rendszerek használatával elkövetett bűncselekmények jogi megítélése. *Ügyészek Lapja, 16*(Különszám), 61-72.

Kökényesi-Bartos, A. (2018). A Számítógépes Bűnözéssel Foglalkozó Ügyészi Hálózat. In B. Bencsik, & I. Sabjanics (szerk.), *Digitális környezetünk fenyegetettsége a mindennapokban* (old.: 105-110). Budapest: Dialóg Campus Kiadó.

Krasznay, C. (2021). Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése. *Külügyi Szemle, 20*(Különszám), 191-214.

Krasznay, C., & Simon, B. (2017). Kiberbűncselekmények az online kereskedelemben. *Hadmérnök, 12*(2 „KÖFOP-különszám"), 122-135.

Kraut, A., Kőhalmi, L., & Tóth, D. (2020). Digital Dangers of Smartphones. *Journal of Eastern-European Criminal Law, 7*(1), 36-49.

Kriptovalutába bújtatott bűnös milliárdok. (2023. 09 20). Letöltés dátuma: 2024. 02 03, forrás: https://nav.gov.hu/sajtoszoba/hirek/Kriptovalutaba_bujtatott_bunos_milliardok

Kube, E. (1998). Technikai fejlődés és a bűnözés formái. *Belügyi Szemle, 36*(9), 43-56.

Kunos, I. (1999). A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. *Belügyi Szemle, 37*(11), 28-42.

LA CCIT. (dátum nélk.). Letöltés dátuma: 2024. 03 13, forrás: https://www.ccit.org.co/la-ccit/

Lajtár, I. (2019). A kiberbűnözésről. *Ügyészek Lapja, 26*(1), 47-52.

Langner, R. (2013). *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve.* München: The Langner Group. Forrás: https://www.cs.yale.edu/homes/jf/Langner.pdf

Linthicum, K. (dátum nélk.). El Salvador's president buys bitcoins 'naked,' he boasts. His experiment is costing his nation millions. Letöltés dátuma: 2022. március 19, forrás: https://www.latimes.com/world-nation/story/2022-02-23/el-salvador-bitcoin-experiment

MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). *Cyber Security Countermeasures to Combat Cyber Terrorism. Strategic intelligence management.* Butterworth-Heinemann.

Maillart, J.-B. (dátum nélk.). The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime. *ERA Forum, 19*(3), 375-390. doi:10.1007/s12027-018-0527-2

Máté, I. Z. (2015). A felhőszolgáltatások igazságügyi informatikai szakértői vizsgálata. *Infokommunikáció és Jog, 62-63*, 86-90.

Mátyás, S., Frigyer, L., & Prilenszky, G. (2021). A virtuális fizetőeszközök szerepe és jelentősége a vagyonvisszaszerzés során. *Belügyi Szemle, 69*(3), 417-430. doi:10.38146/BSZ.2021.3.4

Moise, A. C. (2016). Types of Bank Cards Related Frauds. *Journal of Law and Public Administration, 2*(4), 113-120.

Molnár, G. (2009). *Gazdasági bűncselekmények.* Budapest: HVG-ORAC Lap- és Könyvkiadó Kft.

Moore, T., Han, J., & Clayton, R. (2012). The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs. Financial Cryptography and Data Security. (K. A.D., Szerk.) *Lecture Notes in Computer Science, 7397*, 41-56.

Nagy, M., & Tóth, D. (2019). The types of terrorism - with special attention to cyber and religious terrorism. *JURA, 25*(1), 413-422.

Nagy, Z. A. (1991). Az informatika és a büntetőjog. *Magyar Jog, 38*(1), 21-26.

Nagy, Z. A. (1993). Konferencia az információtechnikai bűnözésről. *Magyar Jog, 40*(2), 102-104.

Nagy, Z. A. (1997). A számítógéppel elkövethető hamisításokról. *Belügyi Szemle, 35*(3), 28-38.

Nagy, Z. A. (1999). A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda. *Belügyi Szemle, 37*(11), 16-27.

Nagy, Z. A. (2001). Informatikai bűncselekmények. *Magyar Tudomány, 48 (108)*(8), 946-957.

Nagy, Z. A. (2009). *Bűncselekmények számítógépes környezetben.* Budapest: Ad Librum.

Nagy, Z. A. (2016). Kiberbűncselekmények, kiberháború, kiberterrorizmus - avagy ébresztő Magyarország! *Magyar Jog, 63*(1), 17-24.

Nagy, Z. A. (2019). A csalás-jellegű cselekmények az e-kereskedelem körében. In M. Kitti (Szerk.), *A bűnügyi tudományok és az informatika.* Pécs – Budapest: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont.

Newman, L. H. (dátum nélk.). *Now Cryptojacking Threatens Critical Infrastructure, too*. Forrás: https://www.wired.com/story/cryptojacking-critical-infrastructure/

Nikač, Ž. (2014). The European Arrest Warrant-Europol. *International Journal of Economics and Law, 4*(12), 91-99.

Osborne, C. (dátum nélk.). *Japan issues first-ever prison sentence in cryptojacking case*. Forrás: https://www.zdnet.com/google-amp/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-

coinhive/?fbclid=IwAR00OIs2mLn5akKQKdoSZ0_lySM6Y2KeQ4_vlD2tfaKdQlRjPH0RMU86qfo

Osborne, C. (dátum nélk.). *Tesla cloud systems exploited by hackers to mine cryptocurrency*. Forrás: https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/

Palicz, T., Sas, T., Tisóczki, J., Bencsik, B., & Joó, T. (2020). „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben. *Orvosi Hetilap, 161*(36), 1498-1505.

Papp, Z. I. (2018). *A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái. Doktori értekezés.* Budapest: Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

Parti, K. (2015). Cyberbullying, Bitcoin, Silk Road, Darknet, TOR: Az internetes bűnözés tárgyában tartott nemzetközi konferenciák kurrens témái 2014-ben. *Ügyészek Lapja, 22*(1), 71-85.

Parti, K., & Kiss, T. (2016). Informatikai bűnözés. In A. Borbíró, K. Gönczöl, K. Kerezsi, & M. Lévay (szerk.), *Kriminológia* (old.: 491-517). Budapest: Wolters Kluwer Kft.

Peszleg, T. (2000). Internet és bűnözés. *Belügyi Szemle, 38*(12), 30-35.

Petrétei, D. (2018). A modern kriminalisztika egyes jogi és etikai kérdései. *Magyar Rendészet, 18*(2), 103-115.

Póczik, S., Sárik, E., Vass, P., & Bolyky, O. (2021). A COVID-19 pandémia egyes kriminológiai aspektusai. *Belügyi Szemle, 69*(3), 375-396. doi:10.38146/BSZ.2021.3.2

Polt, P. (1983). A számítógépes bűnözés. *Belügyi Szemle, 21*(6), 60-64.

Polt, P. (2021). A 21. század kihívásainak hatása a büntetőeljárásra: Kriptovaluták, azaz az új vagyoni értékek büntetőjogi kérdései. In A. T. Barabás, & L. Christián (szerk.), *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est* (old.: 419-428). Budapest: Ludovika Egyetemi Kiadó.

Qué es INCIBE. (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe

Quiroz-Gutierrez, M. (dátum nélk.). El Salvador says tourism is up 30% since it made Bitcoin legal, but the country is still on the brink of economic disaster. Letöltés dátuma: 2022. március 19, forrás: https://fortune.com/2022/02/23/el-salvador-bitcoin-law-tourism-up-30-percent-imf-senate/

Raffai, M. (2000). A hazai számítástechnika története. Letöltés dátuma: 2021. január 22, forrás: http://www.sze.hu/~raffai/org/raffai-infotort.pdf

Rouse, M. (2013. 12 16). *Remote Desktop Software*. Letöltés dátuma: 2022. 09 19, forrás: https://www.techopedia.com/definition/29710/remote-desktop-software

Russian nuclear scientists arrested for 'Bitcoin mining plot'. (dátum nélk.). Forrás: https://www.bbc.com/news/world-europe-43003740

Rüther, W. (2003). Az internet és az „informatikai bűnözés" a kriminológia számára is kihívás. *Belügyi Szemle, 51*(2-3), 249-262.

Sánchez Medero, G. (2012). Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI. *Revista Enfoques: Ciencia Política y Administración Pública, 10*(16), 71-87.

Saul, B., & Heath, K. (2014). Cyber Terrorism. *Sydney Law School Legal Studies Research Paper, 14*(11). Forrás: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2387206

Schukkert, A. (1995). A magyarországi számítógépes bűnözés helyzete, a szoftverek illegális használata. *Belügyi Szemle, 33*(13), 117-123.

Senker, C. (2017). *Cybercrime and the Darknet. Revealing the hidden underworld of the internet.* London: Arcturus Holdings Ltd.

Serbakov, M. T. (2020). Az utóbbi évek jelentős nemzetközi szélsőjobboldali terrorcselekmények elkövetőinek internethasználata és globális összefüggései. *Jogelméleti szemle, 21*(3), 60-69.

Serbakov, M. T. (2020). Legújabb tendenciák a terroristák internethasználatát illetően. *Büntetőjogi Szemle, 9*(2), 122-139.

Serbakov, M. T. (2022). *A szélsőséges terrorista csoportok internethasználatának elemzése. Doktori értekezés.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola.

Simon, B. (2017). A bűnüldözés előtt álló digitális kihívások. *Magyar Rendészet, 17*(5), 83-103.

Simon, B. (2018). A rendőrség állományának felkészültsége a kiberbűnözésre. *Hadtudományi Szemle, 11*(1), 385-405.

Simon, B. (2018). Kiberbűnözés elleni képzésfejlesztés. *Magyar Rendészet, 18*(3), 193-208.

Simon, B. (2018). Kriptovaluták – rendészeti válaszok. *Belügyi Szemle, 66*(10), 71-87. doi:10.38146/BSZ.2018.10.5

Simon, B., & Gyaraki, R. (2020). Kiberbűnözés. In T. Kiss (Szerk.), *Kibervédelem a bűnügyi tudományokban* (old.: 95-119). Budapest: Dialóg Campus Kiadó.

Simon, L., & Magyar, S. (2017). A terrorizmus és indirekt hatása a kibertérben. *Nemzetbiztonsági Szemle, 5*(3), 89-101.

Simonka, G., & Tóth, A. (2019). *A magyar FIU tevékenysége és szerepe a pénzmosás elleni küzdelemben* (Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai különös tekintettel az adócsalás, a korrupció, a pénzmosás és a büntetőjogi compliance nemzeti szabályozására, valamint a kiberbűnözésre. kötet). (Á. Farkas, G. Dannecker, & J. Jancsó, szerk.) Budapest: Wolters Kluwer Kft.

Sirius-project. (dátum nélk.). Letöltés dátuma: 2022. március 15, forrás: https://www.europol.europa.eu/operations-services-innovation/sirius-project

Sorbán, K. (2015). Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. *THEMIS: Az ELTE Állam- és Jogtudományi Doktori Iskola Elektronikus Folyóirata, 13*(1), 343-375.

Sorbán, K. (2018). A videomegosztó platformok európai szabályozásának aktuális kérdései. *MÉDIAKUTATÓ: MÉDIAELMÉLETI FOLYÓIRAT, 19*(1), 9-20.

Subijana Zunzunegui, I. J. (2008). El ciberterrorismo: una perspectiva legal y judicial. *Eguzkilore: cuaderno del Instituto Vasco de Criminología*(22), 169-187.

Szathmáry, Z. (2015). Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog, 62*(11), 639-647.

Szendrei, F. (2018). A szervezett bűnözés gazdasági háttere és a pénzmosás. *Magyar Rendészet, 18*(5), 77-91.

Szívós, A. (2020). Az adórendszer és a pénzügyi kultúra összefüggései. In C. Szilovics, Z. Bujtár, B. Ferencz, B. Breszkovics, & A. Szívós (Szerk.). *GAZDASÁG ÉS PÉNZÜGYEK A 21. SZÁZADBAN II. - KONFERENCIAKÖTET = BUSINESS AND ECONOMY IN THE 21ST CENTURY II. – CONFERENCE PROCEEDINGS*, old.: 52-64. Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Szívós, A. (dátum nélk.). *A pénzügyi kultúra.* Letöltés dátuma: 2020. 10 20, forrás: https://arsboni.hu/a-penzugyi-kultura/

Teleki, B. (2019). Kriptovaluták és bűnözés, különös tekintettel a piramisjáték szervezésére. *MAGYAR BŰNÜLDÖZŐ, 10*(1-2), 67-80.

Torma, A., & Bendes, Á. (2018). Cybercrime, a jelen és a jövő kihívásai. In C. Szabó (Szerk.). (old.: 256-268). Budapest: Doktoranduszok Országos Szövetsége (DOSZ).

Torma, A., & Bendes, Á. (2019). A cybercrime és a gyermekpornográfia összeolvadása. In Á. Bendes, M. Nagy, & D. Tóth (Szerk.). (old.: 5-29). Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Doktori Iskola.

Tóth, D. (2014). A terrorizmus típusai és a kiberterrorizmus. In V. Rab (Szerk.). *XII. Országos Grastyán Konferencia előadásai*, old.: 286-296. Pécs: Pécsi Tudományegyetem Grastyán Endre Szakkollégium.

Tóth, D. (2015). The history and types of terrorism. *LAW OF UKRAINE: LEGAL JOURNAL: SCIENTIFIC-PRACTICAL PROFESSIONAL JOURNAL, 11*(1), 1-24.

Tóth, D. (2019). A virtuális pénzekkel kapcsolatos visszaélések. In N. E. Baráth, & J. Mezei (Szerk.). *Rendészet-Tudomány-Aktualitások. A rendészettudomány a fiatal kutatók szemével.*, old.: 242-250. Budapest: Doktoranduszok Országos Szövetsége, Rendészettudományi Osztály.

Tóth, D. (2019). Az identitáslopás kriminológiai sajátosságai. In G. G.-H. Zoltán (Szerk.), *Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport*, *A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői*, old.: 207-213. Pécs.

Tóth, D. (2019). Crimes in Connection with Cryptocurrencies. *JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW, 6*(2), 193-206.

Tóth, D. (2020). Digitalization trends in the Hungarian Criminal Procedure . In I. Belaj, H. Ž. Vajda, & S. Stojanović (szerk.), *10. Međunarodna Konferencija Razvoj Javne Uprave* (old.: 309-316). Vukovar: Veleučilište Lavoslav Ružička u Vukovaru.

Tóth, D. (2020). Személyiséglopás az interneten. *Büntetőjogi Szemle, 9*(1), 113-119.

Tóth, D. (2021). Identity crimes on the darknet and the social media. *Büntetőjogi Szemle, 10*(Különszám), 85-89.

Tóth, D. (2022). How the Cyberspace Changes Terrorism. *JURA, 28*(3), 97-106.

Tóth, D., & Gáspár, Z. (2020). Jurisdictional Challenges of Cybercrime. *JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW, 7*(2), 101-118.

Tóth, D., & Gáspár, Z. (2020). Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. *Büntetőjogi Szemle, 9*(2), 140-150.

Tóth, D., Gál, I. L., & Kőhalmi, L. (2015). Organized Crime in Hungary. *Journal of Eastern-European Criminal Law, 2*(1), 22-27.

Tóth, M., & Kőhalmi, L. (2016). A szervezett bűnözés. In A. Borbíró, K. Gönczöl, K. Kerezsi, & M. Lévay (szerk.), *Kriminológia* (old.: 603-625). Budapest: Wolters Kluwer Kft.

Tóth, Z. B. (2019). A pénzmosás és terrorizmus-finanszírozás visszaszorítását célzó szabályozási környezet vizsgálata az Európai Unió esetében II. *SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA, 17*(4), 190-208.

Trencsényi, Z. (2023. 10 20). *Mátrix Projekt a kiberbiztonságért*. Letöltés dátuma: 2024. 01 30, forrás: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/matrix-projekt-a-kiberbiztonsagert

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). (dátum nélk.). Letöltés dátuma: 2024. 03 22, forrás: https://www.mpf.gob.ar/ufeci/

Varga, Á. (2019). Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. *In Medias Res, 8*(1), 145-167.

Waulen Kranenbarg, M. (2018). Cyber-offenders versus traditional offenders: An Empirical Comparison. Doktori értekezés. Vrije Universiteit. Forrás: http://dare.ubvu.vu.nl/bitstream/handle/1871/55530/complete_dissertation.pdf?sequence=6&isAllowed=y

What is Ethical Hacking? (dátum nélk.). Letöltés dátuma: 2024. 03 05, forrás: https://www.itgovernance.co.uk/ethical-hacking

Yasar, K. (dátum nélk.). *RAT (remote access Trojan)*. Letöltés dátuma: 2022. 09 19, forrás: https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan

Zhao, W. (dátum nélk.). *Internet Cafes Hacked to Mine $800k in Siacoin Cryptocurrency*. Forrás: https://www.coindesk.com/markets/2018/06/19/internet-cafes-hacked-to-mine-800k-in-siacoin-cryptocurrency/

Zsigovits, L. (2014). Globalizációból fakadó rendészeti kihívások a korszerű információtechnológia tükrében. *Pécsi Határőr Tudományos Közlemények, 15*, 61-66.

Felhasznált jogforrások

Nemzetközi és európai uniós szintű jogforrások:

- az Arab Liga (korábban Arab Államok Ligája) egyezménye az információs technológiai bűnözés elleni küzdelemről (Kairó, 2010. december 21.),
- a Független Államok Közösségének egyezménye a számítógépes információhoz kapcsolódó bűncselekmények elleni küzdelemről (2001),
- a Sanghaji Együttműködési Szervezet egyezménye a nemzetközi információbiztonság terén folytatott együttműködésről (2010),
- az Afrikai Unió egyezménytervezete az afrikai kiberbiztonságot elősegítő jogi keretek meghatározásáról (2012),
- az Afrikai Unió egyezménye a kiberbiztonságról és a személyes adatok védelméről (Malabo, 2014. június 27.),
- az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (Budapesti Egyezmény),
- a Budapesti Egyezmény 2003. január 28. napján, Strasbourg-ban kelt ETS. no. 189. számú, a számítástechnikai rendszereken keresztül elkövetett rasszista és idegengyűlölő cselekmények kriminalizálásáról szóló kiegészítő jegyzőkönyve,
- 02/2021. sz. nyilatkozat az Európa Tanács számítástechnikai bűnözésről szóló egyezményéhez (budapesti egyezmény) tartozó második kiegészítő jegyzőkönyv új rendelkezéseinek tervezetéről,
- az Európai Unióról szóló szerződés (Maastrichti Szerződés),
- az Európai Parlament és a Tanács (EU) 2018/1673 irányelve (2018. október 23.) a pénzmosás ellen büntetőjogi eszközökkel folytatott küzdelemről,
- az Európai Parlament és a Tanács (EU) 2018/843 irányelve a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról,
- az Európai Parlament és a Tanács (EU) 2015/849 irányelve a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről, a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról, valamint a 2005/60/EK európai parlamenti és tanácsi irányelv és a 2006/70/EK bizottsági irányelv hatályon kívül helyezéséről,

- a Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről,
- az Európai Parlament és a Tanács (EU) 2013/40 irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról,
- az Európai Parlament és a Tanács (EU) 2011/93 irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról,
- a Tanács (EU) 2017/1939 rendelete az Európai Ügyészség létrehozására vonatkozó megerősített együttműködés bevezetéséről,
- Magyarország Legfőbb Ügyészsége és az Európai Ügyészség (EPPO) közötti együttműködésről szóló munkamegállapodás (2021. március 26.),
- az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről,
- az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről,
- az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály),
- az Európai Parlament és a Tanács (EU) 2018/1727 rendelete az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről,
- az Európai Parlament és a Tanács (EU) 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról,
- az Európai Parlament és a Tanács (EU) 2021/887 rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról,
- az Európai Parlament és a Tanács (EU) 2019/713 irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök

hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról

Külföldi jogszabályok:

- Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (Németország),
- Gesetz über das Kreditwesen (Kreditwesengesetz – KWG) (Németország),
- Decreto No. 201. – Ley de Integración Monetaria (El Salvador),
- Decreto Legislativo No. 57. – Ley Bitcoin (El Salvador),
- NRP-29 Normas técnicas para facilitar la participación de las entidades financieras en el ecosistema Bitcoin (El Salvador),
- Ley 599 de 2000 (Código Penal de Colombia) (Kolumbia),
- Ley 1928 de 2018 (Kolumbia),
- Resolución PGN No. 3743/15 (Argentína),
- Ley No. 11.179 de 1921 (Código Penal de la Nación) (Argentína),
- Ley No. 26.388 de 2008 (Argentína),
- Ley No. 27.436 de 2018 (Argentína),
- Ley Orgánica 10/1995 del Código Penal (Spanyolország)

Hazai jogszabályok:

1. 2012. évi C. törvény a Büntető Törvénykönyvről,
2. 1978. évi IV. törvény a Büntető Törvénykönyvről,
3. 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről,
4. 1994. évi IX. törvény a büntető jogszabályok módosításáról,
5. 1996. évi LII. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról,
6. 1998. évi LXXXVII. törvény a büntető jogszabályok módosításáról,
7. 1999. évi CXX. törvény a büntető jogszabályok módosításáról,
8. 2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról,

9. 2003. évi II. törvény a büntető jogszabályok és a hozzájuk kapcsolódó egyes törvények módosításáról,
10. 2003. évi XV. törvény a pénzmosás megelőzéséről és megakadályozásáról,
11. 2005. évi XCI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény és más törvények módosításáról,
12. 2007. évi XXVII. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény és más büntetőjogi tárgyú törvények módosításáról,
13. 2007. évi CXXXVI. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról,
14. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,
15. 2020. évi XLIII. törvény a büntetőeljárásról szóló törvény és más kapcsolódó törvények módosításáról,
16. 17/2018. (VI. 27.) IM rendelet az egyes büntetőeljárási jogi tárgyú igazságügyi miniszteri rendeleteknek a büntetőeljárásról szóló 2017. évi XC. törvénnyel összefüggő módosításáról, illetve hatályon kívül helyezéséről,
17. 11/2003. (V. 8.) IM–BM–PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról,
18. 1/2022. (IV. 29.) OAH rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről,
19. 1/1981. (I. 27.) BM számú rendelet a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről,
20. 1/1983. (X. 13.) KSH rendelkezés a statisztikai adatok számítástechnikai eszközök útján végzett rögzítéséről, feldolgozásáról, tárolásáról, továbbításáról,
21. 25/1986. (VIII. 8.) MT rendelet az állami népességnyilvántartásról szóló 1986. évi 10. tvr. végrehajtására,
22. 26/2020. (VIII. 25.) MNB rendelet a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól