GÁTI BALÁZS

A KIBERBŰNÖZÉS JELLEGZETESSÉGEI ÉS A COVID-19 JÁRVÁNY KAPCSOLATA A STATISZTIKÁK TÜKRÉBEN

1. Bevezetés

A digitális forradalom korát éljük. A számítógépek, a nagysebességű internethálózatok elterjedése, a digitalizáció fejlődése a kommunikációra képes digitalizált rendszerek a gazdasági- társadalmi élet, a mindennapi élet területén is jelentős változásokat hoztak a kibővült és felgyorsult információáramlás által. A kibertérben elkövetett jogsértések száma is megsokszorozódott, a számítógépes bűnözés előtérbe került, többek között rosszindulatú programokkal, személyazonosság - lopással[1], pénzügyi-és egyéb online csalással, a szervezetek és személyek adatainak biztonsága veszélybe került. A kiberbűncselekményeknél az adatok a bűnelkövetők elsődleges célpontjai[2,3]. A 2019 decemberében a közép-kínai Vuhanból indult COVID-19 világjárvány rendkívüli módon felgyorsította a digitalizációt. A járvány következményei a társadalmi-és gazdasági krízis, a korlátozások a járvány megfékezésére, a mindennapi élet változásai, az internethez kapcsolódó eszközök használatának előtérbe kerülése növelték az online kommunikációt. Ez a forszírozott digitalizáció a járvány elleni védekezés következménye is, a Dolgok Internete (IoT, IomT), a blockchain technológiák előtérbe kerültek az orvostudomány számos területén is. A digitális környezet átalakulása, a felhasználók magasabb száma jelentősen növelte a potenciális áldozatok számát is. A bűnelkövetési módok is változtak, megnövelve a kiberbűnözés gyakoriságát. A kutatás statisztikai adatok áttekintése alapján vizsgálja a kiberbűnözés körébe tartozó bűncselekmények jellemző változásait, okait, főbb típusait, azok megoszlását gazdasági szektorok szerint, valamint a várható tendenciákat.

2. Változások a bűnelkövetési módokban a pandémia kapcsán

Kemp és munkatársai[4] tanulmányukban arra a következtetésre jutottak, hogy a jellemzően közterületen elkövetett, elsősorban a személy elleni erőszakos, illetve vagyon elleni bűncselekmények száma csökkent a lezárások során az elkövetők és a célpontok közötti fizikai konvergencia lehetőségeinek korlátai miatt, megerősítve az Ashby és Mohler[5] által végzett korábbi vizsgálatok adatait. Piquero feltételezése alapján, a családon belüli

[1] Tóth Dávid: Személyiséglopás az interneten. Büntetőjogi Szemle 2020/1. 7. o.
[2] Marie-Helen Maras: Cybercriminology. Oxford University Press, 2016
[3] Csaba Fenyvesi: *Future Developments* and *Challenges* in *Criminalistics* as *Part* of *Criminal Justice Journal* of *Eastern-European Criminal Law*, *2019*. 72-85. o.
[4] Kemp, Steven, et al. Empty Streets, Busy Internet. A Time Series Analysis of Cybercrime and Fraud Trends During COVID-19, 2021.
[5] Uo.

visszaélések száma a lezárások során növekedhet, mivel az elkövetőknek és az áldozatoknak hosszú ideig ugyanabban a térben kell maradniuk.[6]

A járvány idején a munkáltatók részéről széles körben bevezetett távmunka, valamint az ún. otthoni munkavégzés egyúttal az e-kereskedelmi szolgáltatások iránti megnövekedett igény elősegítheti a bűnözés lehetőségeinek elmozdulását az offline és az online környezet között Collier, Hawdon és Payne tanulmányai szerint[7]. Mivel a természetes személyek a fent említett körülmények következtében több időt töltenek valamilyen digitális szolgáltatás igénybevételével, az információs rendszer elleni bűncselekmények száma növekvő tendenciát mutathat a lezárások során Miró-Llinares és Moneva[8] vizsgálatai alapján.

A pandémia egyedülálló számítógépes bűnözéssel kapcsolatos körülményeket generált, a járvánnyal kapcsolatos fokozott szorongás a felhasználók részéről növelte a kibertámadások sikerének valószínűségét, ami utóbbiak számának és terjedelmének növekedésével párhuzamosan növekvő tendenciát mutatott.

Stickle és Fergus a hagyományos bűnelkövetési magatartások csökkenésével számoltak[9]. Shayegh és Malpede[10] Gerell[11], valamint Halford[12] kutatásai a „hagyományos" bűnelkövetési módok egyértelmű csökkenését jelezték. Halford tanulmánya szerint az Egyesült Királyságban a 2020. március 23-ai zárolása után egy héttel az általános bűnözési ráta 41%-kal csökkent.

A bűncselekmények bekövetkezéséhez térben és időben együttesen szükséges tényezők Cohen és Felson álláspontja[13] szerint, (1) „motivált elkövető", (2) „megfelelő célpont", valamint (3) „a megfelelő védelem hiánya". A hagyományos bűncselekmények tekintetében csökkenő bűnelkövetési ráta lehetséges okai közé tartozik e feltételek megváltozása a korlátozások következtében, mivel a lehetséges áldozatok védettek a bezártság miatt. A szervezett bűnözés keretében megvalósított bűncselekmények száma azonban nem mutatott csökkenést[14].

3. A COVID-19 és a kiberbűnözés kapcsolata

Az Európa Tanács már 2020 márciusában felhívta a figyelmet a számítógépes bűnözés veszélyeire a járvány kapcsán.[15] A legfrissebb statisztikai adatok igazolni látszanak

[6] Piquero, A., et al: Staying home, staying safe? A short-term analysis of COVID-19 on Dallas domestic violence, 2020, American Journal of Criminal Justice. doi:10.1007/s12103-020-09531-7 (letöltés ideje: 2021. 03.21.)
[7] Idézi: Kemp, Steven, et al. Empty Streets, Busy Internet. A Time Series Analysis of Cybercrime and Fraud Trends During COVID-19, 2021.DOI:10.31235/osf.io/38wfy (letöltés ideje: 2021.03.21.)
[8] Miró-Llinares, Fernanado et al.: What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?" Crime Science, 2019/8 .1-5.o
[9] Stickle, Ben., Felson, M.: Crime Rates in a Pandemic: The Largest Criminological Experiment in History" American Journal of Criminal Justice 4, 2020. 526–536.o
[10] Uo.
[11] Uo.
[12] Halford,Eric. et al.: Crime and Coronavirus: Social Distancing, Lockdown, and the Mobility Elasticity of Crime, Crime Science, 2020/9. 11.o
[13] Cohen, E., et al.:, Social change and Crime Rate Trends :A routin Activity Approach, Amerian Sociological Review, 1979,vol, 44,No. 4, 588-608. o.
[14] Dornfeld László: A koronavírus-járvány hatása a kiberbűnözésre, In medias res: Folyóirat a sajtószabadságról és a médiaszabályozásról, 2020/9.193. o.
[15] Forrás: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (Letöltés ideje: 2020.04.20.)

ezt. A VARONIS COVID-19 specifikus kiberbiztonsági statisztikáinak néhány összesített adatát mutatja az 1.sz táblázat.[16]

Ezen összesítésben kiemelkedő az FBI által jelentett 300%-s növekedés a számítógépes bűnözést illetően. Emellett jól látható a bankszektor és az egészségügyi ágazat érintettsége, valamint az adatvédelmi incidensek számának növekedése, a gyakran használt internetes kommunikációs felületek elleni támadások – jelen táblázatban a Zoom ellen – nagy száma. A statisztikai adatok megerősítik a világjárvány kezdetén prognosztizált tendenciáikat. A 2020 március 3-a és 10-e között lezajlott, Interpol által koordinált 90 országot érintő Pangea művelet- mutatói is jelezték ezt.[17]Néhány erre vonatkozó adat a teljesség igénye nélkül: illegális gyógyszerekből világszerte 4,4 millió egységet, valamint 37 000 engedély nélküli, illetve hamisított orvostechnikai eszközt foglaltak le, továbbá 2500 különböző online felületekre mutató linket távolítottak el.

[16] Forrás: https://www.varonis.com/blog/cybersecurity-statistics/ (Letöltés ideje: 2021.05.21.)

[17] Forrás: https://www.europol.europa.eu/newsroom/news/rise-of-fake-'corona-cures'-revealed-in-global-counterfeit-medicine-operation (Letöltés ideje: 2021.03.21.)

COVID-19 specifikus kiberbiztonsági statisztikák

A járvány kezdete óta az FBI 300% -os növekedésről számolt be a bejelentett számítógépes bűncselekmények terén.	2020 áprilisában a Google napi 18 millió COVID-19-el kapcsolatos malware programot és adathalász levelet blokkolt. (Google)	Félmillió Zoom felhasználói fiók került veszélyeztetésre illetve értékesítésre egy dark web fórumon 2020 áprilisában. (CPO Magazine)
A COVID-19-el összefüggő internetes támadások 27% -a bankokat vagy egészségügyi szervezeteket céloznak meg. A 2020-as év vonatkozásában a COVID-19-nek könyvelik el a bankok elleni kiber támadások 238% -os növekedését. (Fintech News)	A jogi és megfelelőségi vezetők 52% -a aggódik a távoli munkából eredő harmadik féltől származó kiberkockázatok miatt a COVID-19 óta. (Gartner)	A felhőalapú kibertámadások 630%-os növekedést mutattattak 2020 januárja és áprilisa között. (Fintech News)
2020-ban a megerősített adatvédelmi incidensek száma az egészségügyi ágazatban 58% -os növekedést mutatott. (Verizon)	A távmunka megnövelte az adatvédelmi incidensek átlagos költségét 137 000 §-al (IBM)	Távmunkát végző személyek a szervezetek 20% -ában okoztak biztonsági rést. (Malwarebytes)
2020 májusában a Járványügyi Munkanélküliségi Segélyprogram 33 000 munkanélküli kérelmezője lett kitéve az adatbiztonság megsértéséből adódó lehetséges következményeknek. (NBC)	Az alkalmazottak 47% -a figyelemelterelést említette az otthoni munkavégzés során adathalász-csalásoknak történő áldozattá válás okaként. (Tessian)	
Az USA állampolgárai több mint 97,39 millió dollárt vesztettek az COVID-19 és az ingerellenőrző csalások miatt. (Atlasvpn)	A kiberbiztonsági szakemberek 81% -a számolt be arról, hogy megváltozott a munkaköre a világjárvány (ISC) során	

1. sz. táblázat, forrás: varonis.com

3.1. A kibertérben elkövetett bűncselekmények főbb típusai a EUROPOL adatai alapján[18]

Jelentéseiben a EUROPOL a bűncselekmények különböző elemeire összpontosít a COVID-19 világjárvány kezdete óta. A jelentés ismertette a COVID-19 járványhoz kapcsolódó számítógépes bűncselekmények jellegzetes típusait az alábbiak szerint:

- Hamisított és nem szabványos termékek forgalmazása: A hamis gyógyszer- és egészségügyi termékekkel kereskedő bűnelkövetők kihasználták a COVID-19 járványt és termékportfóliójukat az eredeti termékek hiánya és az emberek félelme alapján alakították ki. Jellemző termékek: az arcmaszkok, hamis koronavírus tesztkészletek, latex kesztyűk, fertőtlenítők és ezekhez hasonló termékek - alkoholalapú gélek, szappanok, fertőtlenítő tisztítószerek- törlőkendők és gyógyszerek. A hamisított termékkínálat megjelenik a dark weben, de a felületi kínálathoz képest korlátozottabban.
- Adathalászat: Az adathalász csalások általában bizalmas információk (úgy, mint jelszavak vagy hitelkártyaszámok), illetve hitelesítő adatok és érzékeny adatok megszerzésére irányulnak. Ez jellemzően megtévesztés útján e-mail üzenetek, illetve a megszerezni kívánt információ rögzítésére tervezett weboldalak felhasználásával valósul meg, a célpontok egyaránt lehetnek természetes személyek és szervezetek. Az adathalászati célú SMS-ek[19] és e-mailek nagy számban jelennek meg egyes finanszírozási kampányok során[20].
- Rosszindulatú számítógépes programok (malware-ek): A malware kifejezés magába foglal mindenféle rosszindulatú szoftvert, célja az operációs rendszerek gyengeségeinek kiaknázása. Jellemző a hitelkártyaszámok, banki adatok, érzékeny böngészőadatok lopása. A zsarolóvírus a virtuális világ egyik fő fenyegetése.[21,22] Egy tipikus példa: egy esetben a magánszektor válaszadója arról számolt be, hogy valamely harmadik fél szolgáltatójukat Emotet rosszindulatú program vette célba, ami magas kockázatú helyzethez vezetett a válaszadó rendszerében is. A támadók gondosan tanulmányozzák a célzott vállalat és a válaszadó közötti régi e-mail szálakat, és igyekeznek természetes módon beilleszkedni a beszélgetésbe a személyre szabott üzenetek segítségével az információgyűjtéshez.[23]
- Eltereléses csalás (Business Email Compromise, BEC): e csalásokkal kapcsolatban a jelentés a fejlettebb és célzottabb módszerekre hívja fel a figyelmet. A BEC gyakran követi az adathalász e-maileket, magas szinten személyre szabott, hatékonyan veszi célba a kormányzati-, nemzetközi szervezetektől, a kisvállalkozásoktól kezdve a nagyvállalatokat, valamint a magánszemélyeket is.[24]
- Dark web: Ha egy oldal megtalálható valamely nagy keresőmotor (lsd. Google, Bing) segítségével, akkor az a felszíni web része, ha pedig nem, akkor az az oldal a mély (deep) web részét képezi. A dark web kifejezés az ún. sötéthálózatokon

[18] Forrás: https://www.europol.europa.eu/newsroom/news/catching-virus (Letöltés ideje: 2021.03.21.)
[19] Andrea Kraut, László Kőhalmi, Dávid Tóth: Digital Dangers of Smartphones. Journal of Eastern-European Criminal Law 2020. 36.o.
[20] Forrás: https://www.europol.europa.eu/COVID-19 "COVID-19-phishing-and-smishing-scams (Letöltés ideje: 2021.03.21.)
[21] Forrás: https://gatefy.com/blog/ransomware-top-2019-cyber-threat-europol-iocta (Letöltés ideje: 2021.03.22.)
[22] Uo.
[23] Uo.
[24] Uo.

létező világháló (World Wide Web) tartalmaira utal: ezek ún. átfedő hálózatok, amelyek internetet használnak, de speciális szoftvert, konfigurációt vagy engedélyt igényelnek a hozzáféréshez. Ezek közül a három legismertebb program a Tor, az I2P és a Freenet, a legnagyobb forgalmat pedig a Tor bonyolítja le közülük, amelyek a rajtuk keresztül áramló adatforgalmat titkosítják, így a végfelhasználók IP-címei nem, vagy csak más felhasználók IP-címeivel együttesen azonosíthatók.

- A dark weben elérhető piacok illegális termékekkel, illetve szolgáltatásokkal kapcsolatos ügyletekben töltenek be közvetítő szerepet. Az itt megjelenő bűnelkövetési ráta ingadozik, főként az illegális termékek kereskedelmével kapcsolatban, amely a beszerzési és/vagy szállítási lehetőségtől függ adott termék vonatkozásában. E platformokon nőtt a maszkok, hamis tesztkészletek és gyógyszerek száma, a sötét webfelületen pedig széles körben elterjedtek a csalások elkövetésére is alkalmas illegális termékek stb.[25]
- Gyermekek szexuális kizsákmányolása[26]: Mivel a gyermekek egyre több időt töltenek online, különösen könnyű célpontjai a számítógépes bűnelkövetőknek. A COVID-19 járvány több lehetőséget kínált a gyermekek szexuális bántalmazására és szexuális kizsákmányolására. Az NCMEC- az eltűnt és kizsákmányolt gyermekek nemzeti központja, (USA) – továbbítja az adatokat a EUROPOL felé, ha az, az EU szempontjából releváns. A tagállamokban a 2020 március-április közötti lezárás során az ilyen jellegű bűncselekmények száma emelkedett, de a korlátozások feloldásával visszatért a szokásos szintre, nyár vége felé azonban az ügyek száma ismét növekedést mutatott. Az esetek száma mérsékelt növekedést mutatott a 2020-as év utolsó hónapjában az EU egész területén[27,28].

3.1 A kibertérben elkövetett bűncselekmények főbb típusai az INTERPOL, ENSZ, ACFE és IBM –X FORCE kutatások adatai alapján

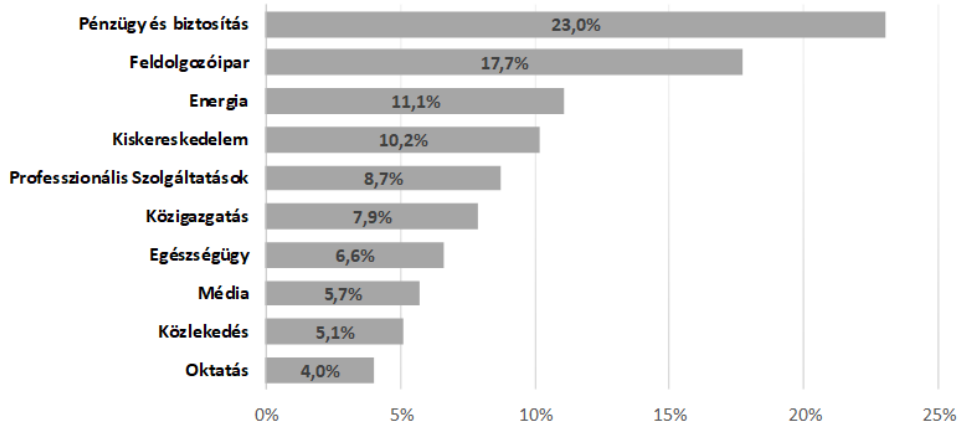
- A COVID-19 alatt a kibertámadások növekvő aránya az INTERPOL jelentésében[29] is megmutatkozik. A COVID-19 járvány kapcsán a kiberbűnözésről szóló INTERPOL-értékelés által kiemelt legjellemzőbb elkövetés típusok az online csalások és adathalászat, rosszindulatú programok és domainek használata valamint álhírek terjesztése, továbbá beszámol a gyermekek szexuális kizsákmányolásához kapcsolódó bűncselekmények számának jelentős növekedéséről is.
- A beszámoló alapján az adathalász csalások és online csalások aránya a legmagasabb 59%-kal, ezt követik zsarolóvírusok 36%-kal, a rosszindulatú domain-ek 22%-kal, és az álhírek terjesztése 14%-kal.

[25] Forrás: https://www.europol.europa.eu/newsroom/news/catching-virus (Letöltés ideje: 2021.03.21.)
[26] Forrás: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-COVID-19-pandemic (Letöltés ideje: 2021.03.21.)
[27] Forrás: https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020 (letöltés ideje: 2021.03.21.)
[28] Forrás: https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime (Letöltés ideje: 2021.03.21.)
[29] Forrás: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (Letöltés ideje: 2021.03.21.)

- Az ENSZ által feltárt adatok [30] szintén a már ismertetett főbb jellemzőket támasztják alá, úgy, mint a rosszindulatú kampányok, dezinformáció és a közösségi média előtérbe kerülése a kibertámadások által. A WhatsApp, Facebook, Instagram, WeChat és Weibo közösségi oldalak használata 40%-kal növekedett, a WhatsApp alkalmazás a járvány végéig 51%-os növekedést mutatott, egyes országokban pl. Spanyolországban elérte a 76%-ot is. A felhasználók megnövekedett száma ugyanakkor kiszélesíti a potenciális áldozatok körét is.[31]
- A legelterjedtebb csalási típusok a COVID-19 járvány első 12 hónapja alatt az ACFE Benchmarking Tanulmány adatai alapján 88%-ban a kibercsalás, 73%-ban a személyiséglopás, 72%-ban a fizetési csalás, 69%-ban munkanélküliséggel kapcsolatos csalás, és 67%-ban az eladók által elkövetett csalások (vendor fraud)[32] (ideértve elsősorban a számlázási rendszerekkel, csekk manipulációval, valamint megvesztegetéssel vagy zsarolással kapcsolatos csalásokat).
- Az IBM 2020 január és december között több milliárd adatot gyűjtött össze ügyfeleitől valamint nyilvános forrásokból, az egyes kibertámadás típusok, fertőzési vektorok, elemzése, valamint a globális és iparági összehasonlítások elvégzése céljából, amelyeket az X-Force Threat Intelligence Index ismertet. A zsarolóvírus volt a legnépszerűbb támadási módszer 2020-ban, amely valamennyi adatvédelmi incidens 23%-át tette ki. A kibertámadások első 10, azok által leginkább érintett iparág közötti[33] megoszlását mutatja a 1. sz. ábra. A legtöbb támadás a pénzügyi és biztosítási ágazat ellen irányult 23%-kal. A feldolgozóipart a támadások 17,7%-a célozta, ezt követte az energiaszektor 11,1%-kal és a kiskereskedelem 10,2%-kal, míg a többi ágazat ellen a támadások kevesebb mint 10%-a irányult.

[30] https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf (Letöltés ideje: 2021.03.21.)
[31] Forrás: https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-COVID-19-pandemic/ (Letöltés ideje: 2021.03.21.)
[32] Forrás:https://www.acfe.com/uploadedFiles/ACFE_Website/Content/resources/Covid-19%20Benchmarking%20Report%20September%20Edition.pdf, (Letöltés ideje: 2021.03.21.)
[33] Forrás: https://www.ibm.com/downloads/cas/AWJ3PE1M, (Letöltés ideje: 2021.03.21.)

A kibertámadások megoszlása iparágak szerint



1. sz. ábra Forrás: IBM- X FORCE 2021

3.2. Egyes bűncselekmények száma Magyarországon, a COVID-19 járvány idejéhez köthető adatok

A KSH adatai szerint a bűncselekmények száma 2009 és 2020 között jelentősen csökkent, 394 034-ről, 162 416-ra. 2019-ben 165 648-ről is csökkenés mutatkozik[34]. A KSH oldalán 2020 április és 2021 áprilisa közötti időszak vonatkozásában közétett statisztikai adatok a pandémia mindhárom hazai hullámának idejéhez köthetőek. A feltüntetett hagyományos bűncselekmények száma csökkent, így a testi sértések száma csökkent 660-ról 561-re, a rongálásoké 507-ről 383-ra, a lopások száma 3788-ról 3251-re. A közokirat-hamisítások száma növekedett, 223-ról 523-ra, a csalások száma 974-ről 1093-ra, a személyes adattal visszaélés 30-ról 125-re.[35] Ez utóbbiak vonatkozásában az online történő elkövetések nagyobb száma is feltételezhető. A Nemzeti Kibervédelmi Intézet számos kiberbűncselekmény elkövetésre hívja fel a figyelmet, beszámol többek között a 2020 szeptemberében az Emotet malware fertőzésről amellyel kapcsolatosan több egészségügyi intézmény infrastruktúrájának érintettsége merült fel.[36] Gál István tanulmányozta a magyar számítógépes bűnözés trendjeit a COVID-19 világjárvány közepén.[37] Gál kitért a globális gazdasági válság bűnözési tendenciákra gyakorolt lehetséges hatásaira is.[38]

[34] Forrás: https://www.ksh.hu/stadat_files/iga/hu/iga0003.html (Letöltés ideje: 2021.03.21.)
[35] Jelenleg a 2020. július és 2021. júliusi adatok érhetőek el, hasonló tendenciát jelezve. https://www.ksh.hu/heti-monitor/buncselekmeny.html, (Letöltés ideje: 2021.03.21.)
[36] Forrás: https://hirlevel.egov.hu/2020/09/27/informatikai-kartevo-tamadja-az-egeszsegugyi-intezmenyek-infrastrukturajat-figyelmeztet-a-nemzeti-kibervedelmi-intezet/ (Letöltés ideje:2021.03.21.)
[37] István L. Gál: The Possible Impact of the COVID-19 on Crime Rates in Hungary Journal of Eastern-European Criminal Law, 2020. 165.o.
[38] Gál István László: A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre. Magyar Jog 2020/5. 9. o.

4. Hogyan várható a bűnözés alakulása egy járvány alatt?

Egy az ENSZ által közölt tanulmány[39] elemezte, hogy a bűnözés várhatóan hogyan fog változni a járvány idején. Ez a tanulmány elsősorban a bűnözési tendenciák társadalmi és gazdasági hatásával összefüggésben a COVID-19 világjárvány rövid- és hosszú távú hatásait vizsgálta. Rövid távon a bűnözésre hatást gyakorolhatnak a korlátozások, valamint a már meglévő tényezők, amelyek országonként eltérőek. A korlátozó intézkedések kétségkívül csökkentik számos bűncselekmény elkövetésének lehetőségét. Hosszabb távon a vállalkozások tevékenységének korlátozása, az azt követő munkanélküliség és jövedelemkiesés is hatással lehet a bűnözési rátára[40], különös tekintettel a nyereségorientált bűnözésre, ideértve továbbá a személy elleni erőszakos, valamint vagyon elleni bűncselekményeket is, különös tekintettel azon helyekre, ahol a gazdasági és szociális védőháló nem elegendő a megélhetés biztosításához. A bűnözésre gyakorolt rövid és hosszú távú hatás a „lehetőségelmélet" (opportunity therory) és „feszültségelmélet" néven ismert kriminológiai elméletek összefüggése (strain theory). Ezek az elméletek a bűncselekmények két eltérő tendenciáját prognosztizálják: a lehetőségelmélet szerint a zárolási intézkedések potenciálisan csökkenthetik a bűncselekmények elkövetésének lehetőségét a mobilitás és a társadalmi interakció korlátozásai miatt, a feszültségelmélet szerint a társadalmi-gazdasági feszültségek, amelyek a lakosság nagy rétegét, különösen a legkiszolgáltatottabb csoportokat érintik, képesek olyan nyomás légkörét létrehozni, amely az egyéneket bűncselekmények elkövetésére készteti. Így a feszültségelmélet a bűnözés helyzetének növekedését jósolja a lezárások következtében. Ez utóbbi ok-okozati mechanizmus hatása valószínűleg hosszabb ideig tartó hatással jár, még a lezárási intézkedések feloldása után is.

5. Összefoglalás

A tanulmány statisztikai adatok összevetése alapján a COVID-19 világjárvány bűnelkövetési módozatait, elsősorban a kiberbűnözésre gyakorolt hatását vizsgálta. A statisztikai adatok alapján a COVID-19 világjárvány alatt a kiberbűnözés jelentős emelkedést mutat, míg a hagyományos, „offline" elkövetett bűncselekmények száma csökkent. Ennek okai között a társadalmi- gazdasági változások, a járvány elleni védekezés különböző eszközei szerepelnek. A korlátozó intézkedések a hagyományos bűnelkövetési módokat háttérbe szorítják, míg ezzel párhuzamosan az internet használatának szignifikáns növekedése a természetes személyeket, a gazdasági szféra szereplőit, de a kormányzati és egészségügyi szektor egyes területeit is érintve szélesebb körben biztosít lehetőséget a számítógépes bűncselekmények elkövetésére. A digitalizáció előtérbe kerülésével a járvány elleni védekezés érdekében az egészségügyi rendszerek is kibertámadások célpontjaivá váltak, ugyanakkor a hagyományos bankszektor változatlanul az első célpontok egyike.[41]

Az idézett kutatási eredmények, felmérések elsősorban a rosszindulatú programok, az adathalászat kockázatait emelik ki. Ugyanakkor a kiberbűnözés körébe tartozó

[39] Forrás: https://www.unodc.org/documents/data-and-analysis/covid/Property_Crime_Brief_2020.pdf, (Letöltés ideje: 2021.03.21.)
[40] Ambrus István: A koronavírus-járvány és a büntetőjog. MTA Law Working Papers 2020/5. 22. o.
[41] Tóth Dávid: Credit Card Fraud with a comparative law approach. In: Goran, Ilik; Angelina, Stanojoska (szerk.) "Towards a Better Future: Democracy, EU Integration and Criminal Justice." International Scientific Conference Conference Proceedings Volume I. Faculty of Law - Kicevo, University "St. Kliment Ohridski" - Bitola, 2019. 232-243. o.

bűncselekmények elkövetési módjai is folyamatos fejlődésen mennek keresztül. A feldolgozott statisztikák a kiberbűnözés elleni küzdelemben elsődleges szerepet játszó nemzetközi szervezetektől származnak, és a kibertámadások elleni védekezés stratégiáinak kiindulópontjai is egyben. Az ENSZ, az EU szervezetei és speciális tagállami szervezetek szintjén szükséges a megfelelő kiberbiztonsági stratégiák kidolgozása és alkalmazása, amelyek a társadalmi- gazdasági szféra adott területein alkalmazandók. Társadalmi szinten kiemelendő az egyének védelme- itt a média, közösségi média, a fórumok, az oktatási intézmények szerepét emelném ki- elsősorban a figyelemfelhívás, és védekezés módozatait tekintve.

A világjárvány egyaránt rendkívüli körülményeket teremtett a társadalmi és gazdasági környezetben és az egyének mindennapi életében, amelyek az empirikus kriminológiai kutatások számára is lehetőséget kínálnak a bűnelkövetések módozatainak, körülményeinek, valamint a társadalom tagjait ért szocio-pszichológiai hatások tekintetében.