TANULMÁNYOK

A koronavírus-járvány hatása a kiberbűnözésre

DORNFELD LÁSZLÓ*

A digitális átalakulás, amit gyakran neveznek a negyedik ipari forradalomnak,[1] jelentősen megváltoztatta mindennapi életünket. Ám ez nemcsak előnyökkel járt, hanem számos új kihívással is, így például a kibertérben zajló bűnözést is felerősítette. A kár mértéke a Center for Strategic and International Studies 2018-as felmérése szerint 600 milliárd dollár volt világszinten, vagyis a globális GDP 1%-a.[2] Az online tér iránti bűnözői érdeklődés növekedése számos tényezővel függ össze, így például a gyorsasággal, a viszonylagos anonimitással, és persze az is szerepet játszik benne, hogy a modern információtechnológiát használók száma évről évre nő.[3]

Az utolsó nagy világjárvány a pontosan száz évvel ezelőtt dúló spanyolnátha volt.[4] A 2020-ban világjárványt kiváltó koronavírus (tudományos megnevezéssel Covid–19)[5] miatti korlátozások felgyorsították a digitális átállást, amely számos területen nagyon rövid időn belül kellett megvalósuljon, például az oktatásban, a munkahelyek egy jelentős részében, a szórakoztatóiparban stb. Március végére a napi adatforgalom mintegy 60%-kal emelkedett meg,[6] ennek következményeként a Cable brit telekommunikációs tanácsadó oldal június 30-ig elvégzett kutatása

* A szerző jogász, a Mádl Ferenc Összehasonlító Jogi Intézet és a Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézetének kutatója. E-mail: dr.laszlo.dornfeld@gmail.com.

[1] Klaus SCHWAB: The Fourth Industrial Revolution: What it Means, how to Respond. *WEF,* 2016. január 14., https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.

[2] James LEWIS: Economic Impact of Cybercrime – No Slowing Down. *CSIS* (2018), https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.

[3] David Wall véleménye szerint egyre inkább a számos, kis kárt okozó bűncselekmények sorozata válik jellemzővé. David S. WALL: *Cybercrime*. Cambridge, Polity, 2007. 3.

[4] Erről bővebben l. GÁL István László: A spanyolnátha, a koronavírus és a büntetőjog. *Büntetőjogi Szemle,* 2020/1., 57.

[5] WHO Director-General's Opening Remarks at the Media Briefing on COVID-19. *WHO,* 2020. március 11., https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.

[6] Március végére a napi adatforgalom 60%-kal megnőtt a járvány előtti időhöz képest. Daniele LEPIDO – Thomas SEAL – Natalia DROZDIAK: Internet Traffic is Surging but the Pipes Aren't Bursting Yet. *Bloomberg*, 2020. március 20., https://www.bloomberg.com/news/articles/2020-03-20/internet-traffic-is-surging-but-the-pipes-aren-t-bursting-yet.

alapján az internet átlagos sebessége világviszonylatban 6,31%-kal csökkent, ám egyenlőtlen eloszlással: míg Kínában a visszaesés 50%-os volt, addig például hazánkban 13% körüli, egyes régiókban és országokban pedig még enyhén nőtt is a sebesség.[7] A Deutscher Commercial Internet Exchange frankfurti internetcsatlakozási pont mérései alapján a világ internetes összforgalmának csúcsa a tavaszi 9,1 terabit per másodperc volt (a korábbi rekord 8,3 terabit volt).[8]

A nagyobb számú felhasználó jelentősen növelte a potenciális áldozatok számát is. Erre az élet minden részét alaposan érintő változásra a bűnelkövetők is nagyon hamar reagáltak, és akárcsak a fizikaiban, a kibertérben is megjelentek a járvánnyal összefüggő bűncselekmények.[9] A jogászi szakma számára a bűnelkövetések megemelkedett száma mellett nagy kihívást jelent azok minősége,[10] például a járvány elleni védekezést nehezítő álhírek és összeesküvés-elméletek terjedése, amelyek ellen a fellépés komoly alapjogi kérdéseket is felvet.

Jelen tanulmányban röviden áttekintem, hogy milyen módszereket alkalmaznak az elkövetők, és hogy milyen káros online folyamatok erősödtek fel a járvány hatására. Célom annak bemutatása, hogy a bűnözés – mint a társadalmi innováció egy sajátos formája – hogyan képes igen gyorsan reagálni a környezeti változásokra, és ez milyen új kihívásokat jelent a bűnüldözés és a jogász szakma számára. E tapasztalatok most, a járvány második hullámának tetőzése környékén, illetve a későbbiekben, a vírus leküzdéséig – de talán még azt követően is – hasznos tudást jelenthetnek nemcsak elméletben, de gyakorlatban is.

1. A járvány hatása a bűnözésre

A járvány és az ellene való védekezésként hozott állami rendelkezések igen sajátosan hatottak a bűnözésre. Egy júliusban publikált kutatás az Egyesült Királyságban kriminálstatisztikával vizsgálta a jelenséget, a tavaszi adatokat az ötéves átlaggal vetve össze. Az ott március 23-án elrendelt országos lezárás eredményeként a bűnözés egy héten belül átlagosan mintegy 41%-kal esett vissza: a bolti lopások 62%-kal, a lopások 52%-kal, a testi sértések 36%-kal, míg a betörések 25%-kal.[11] Hasonló tendencia volt megfigyelhető világszinten is, például az Egyesült Államok területén végzett számos, egy-egy nagyvárosra koncentráló kutatás is jelentős visszaesést mutatott a bűnözés mértékében.[12]

[7] How Global Broadband Speeds Changed During COVID-19 Lockdown Periods. *Cable,* https://www.cable.co.uk/broadband/speed/broadband-speeds-covid-19-lockdown/.

[8] Johannes Wiggen: *The Impact of COVID-19 on Cyber Crime and State-Sponsored Cyber Activities*. Berlin, Konrad Adenauer Stiftung, 2019. 2.

[9] Europol: Catching the Virus Cybercrime, Disinformation and the COVID-19 Pandemic. https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic, 3.

[10] Ambrus István: A koronavírus-járvány és a büntetőjog. *MTA Law Working Papers,* 2020/5., 1.

[11] Eric Halford et al.: Crime and Coronavirus: Social Distancing, Lockdown, and the Mobility Elasticity of Crime. 9 *Crime Science* 1 (2020) 11.

[12] Ben Stickle – Marcus Felson: Crime Rates in a Pandemic: The Largest Criminological Experiment in History. 45 *American Journal of Criminal Justice* 4 (2020) 526–527.

Erre Lawrence E. Cohen és Marcus Felson rutintevékenység-elmélete adhat magyarázatot: eszerint három elem együttes meglétére van szükség a bűnelkövetéshez, ezek pedig a motivált elkövető, a megfelelő célpont és a megfelelő védelem hiánya. Mindezek együttes fennállására a napi rutintevékenységek során van leginkább lehetőség, hiszen ekkor kerülhet az elkövető és az áldozat a legnagyobb eséllyel kapcsolatba egymással.[13] Vagyis a társadalmi érintkezések csökkentése a járvány visszaszorítása érdekében egyúttal a bűnelkövetési lehetőségek jelentős csökkenésével is járt. Ezt a megközelítést támasztja alá az is, hogy Svédországban – amely a nyugati világban a legenyhébb korlátozó intézkedéseket hozta a járvány idején[14] – a visszaesés sokkal kevésbé volt drámai, mindössze 8,8%-os volt, és bizonyos bűncselekménytípusokat, így például a kábítószerkereskedelmet nem is érintette.[15]

Ez a csökkenő tendencia azonban csak a fizikai térben elkövetett bűncselekmények kapcsán igaz, ahol a tradicionális rendészet eszközei már kellően kifinomultan működnek. Egészen más a helyzet a kibertérben, ahol az otthon maradó embereknek köszönhetően jelentősen megnőtt a bűnelkövetési lehetőségek száma. Az Interpol augusztusi jelentése alapján január és április között 737 kiberbiztonsági incidens történt, 900 ezernél is több spam üzenetet küldtek el, és 48 ezer kártékony webcímet regisztráltak csak a járvánnyal összefüggésben. A nemzetközi szervezet főtitkára szerint az elkövetők a járvánnyal kapcsolatos félelmeket és bizonytalanságokat használták ki,[16] és más források is ezt a tényezőt emelték ki az áldozattá válás egyik lehetséges kiváltó okaként.[17]

1.1. Kiberbűnözés a járvány idején

Az Európa Tanács honlapja márciusban részletesen foglalkozott azokkal a kiberfenyegetésekkel, amelyek a koronavírus-járvány idején előtérbe kerültek.[18] Az azonosított fenyegetések technikai szempontból két típusra oszthatók: csalásra és rosszindulatú programokra, illetve ezen belül is az ún. zsarolóvírusokra. Ezek egyike sem számít újdonságnak a kibertérben, azonban tavasszal jelentős növekedést mutatott az elkövetések száma. Jogi értelemben azonban egészen más felosztás érvényesül. A csalás meghatározása kapcsán érdemes arra utalni, hogy a kibertérben elkövetett nem minden bűncselekmény tekinthető kiberbűncselekménynek.[19] A Számítástechnikai

[13] Kiss Tibor: *Agresszió a cybertérben*. Doktori értekezés. Budapest, 2018. 130–131.

[14] Gretchen Vogel: „It's been so, so Surreal." Critics of Sweden's Lax Pandemic Policies Face Fierce Backlash. *Science,* 2020. október 6., https://www.sciencemag.org/news/2020/10/it-s-been-so-so-surreal-critics-sweden-s-lax-pandemic-policies-face-fierce-backlash.

[15] Stickle–Felson i. m. (12. lj.) 527.

[16] https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

[17] Wiggen i. m. (8. lj.) 3.

[18] Európa Tanács: Cybercrime and COVID-19, https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19.

[19] Wall „generációs felosztása" szerint kizárólag a harmadik generációs kiberbűncselekmények tekinthetők valódi kiberbűncselekményeknek. Wall i. m. (3. lj.) 44–48.

Bűnözésről szóló Budapesti Egyezmény[20] 8. cikke alapján a csalás másnak jogosulatlanul és szándékosan történő vagyoni károkozás, amelyet számítástechnikai adatok bármilyen bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével, vagy a számítástechnikai rendszer működésébe való bármilyen beavatkozással követnek el anyagi haszonszerzés céljából. Ezt a magyar Büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 375. §-a „információs rendszer felhasználásával elkövetett csalás" néven ismeri. Ez, a nevével ellentétben, nem a csalás bűncselekmény (Btk. 373. §) egy sajátos változata, sőt ebben az esetben a csalást meg sem lehet állapítani. Ezen elsősorban a technikai jellegű károkozást kell érteni, például hackelés vagy a már említett kártékony programok segítségével.[21] Az online csalás a digitális környezet ellenére a csalás bűncselekmény tényállása alá tartozik.

Ősszel az Europol 2020-as Internet Organised Crime Threat Assessment jelentése is megjelent, amely szintén érdekes információkkal szolgál a járvány kiberbűnözésre gyakorolt hatásairól.[22] Az elkövetők az adathalászat, az online csalások és az álhírek segítségével adtak el olyan eszközöket, amelyektől a vásárlók a járvány elleni védekezést remélték. A kártékony programok használata is jelentős veszélyt jelentett, például az egészségügyi intézmények elleni támadások formájában. Az online csalások mellett új fejlemények voltak a fizetési csalásoknál is, ahol a SIM kártyák cseréje vált új trenddé. Mindezek mellett az illegális javak (pl. kábítószer) kereskedelmével és a gyermekpornográfiával összefüggő bűncselekmények is megszaporodtak az online térben.

A jelentés 1.3. pontja szerint a kibertérben a legalapvetőbb veszélyt az adatsértések jelentik, amelyek segítségével az elkövetők egyes felhasználók adataihoz vagy sok felhasználó adatait tartalmazó adatbázisokhoz férhetnek hozzá, és azokat felhasználhatják saját céljaikra. Ezek megszerzésének módszerei lehetnek a pszichológiai manipuláció *(social engineering),* ahol a felhasználót megtévesztéssel próbálják rávenni saját adatai kiadására, valamint az adathalászat *(phishing),* ahol technikai eszközökkel igyekeznek ugyanezt megszerezni. Ezen információk birtokában könnyebb később célzott hirdetésekkel vagy megkereséssel megkárosítani az áldozatokat.

1.1.1. Online csalás

Az online csalás jelentős részét teszi ki a kiberbűncselekményeknek, és ez a járvány idején is igaznak bizonyult. Számos módon elkövethető, ami a vírus sajátosságaiból kifolyólag főleg az azzal szembeni védekezés és a megelőzésének eszközeit érintette. A brit kormány által a jótékonysági szervezetek számára tavasszal kiadott figyelmeztetés számos ilyen esetet felsorol,[23] például a be-

[20] Idehaza kihirdette a 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

[21] Mezei Kitti: *A bűnügyi tudományok és az informatika*. Doktori értekezés. Pécs, 2019. 79–80.

[22] Europol: COVID-19 Sparks Upward Trend in Cybercrime, https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime.

[23] Coronavirus (COVID-19): Increased Risk of Fraud and Cybercrime Against Charities, https://www.gov.uk/government/news/coronavirus-covid-19-increased-risk-of-fraud-and-cybercrime-against-charities.

szerzési csalás egy formáját, amikor különböző védőeszközöket, maszkot, fertőtlenítőszert kínálnak eladásra online, ám azok sosem érkeznek meg a fizetést követően. Egy másik lehetséges változat az, hogy előleget kérnek valamely szolgáltatásért cserébe (pl. fertőtlenítés), azonban a szolgáltatás nyújtására már nem kerül sor. Csalás céljaira használhatók fel az adathalász levelek is, amelyek elég információt biztosíthatnak például ahhoz, hogy a pénzügyekért felelős munkatársat a főnöke nevében egy nagyobb összegű utalásra szólítsák fel a csalók. Németország Észak-Rajna-Vesztfália tartományában bűnözők hamis weboldalakat hoztak létre, ahol a regisztráló egyéni vállalkozóknak állami támogatást ígértek, ám a valóságban ellopták az adataikat.[24]

Az Interpol által koordinált egyik tavaszi akcióban olyan bűnözői kört sikerült kézre keríteni, amelynek tagjai március közepén egy zürichi és egy hamburgi beszállító cég nevében keresték meg a német egészségügyi hatóságokat azzal, hogy tízmillió szájmaszkot tudnak nekik szállítani. Másfél millió eurós fizetséget kaptak az első szállítmányért, majd a német megrendelő eleget tett annak a kérésüknek is, hogy további 880 ezer eurót utaljon át a számukra, amit azonnal továbbutaltak egy dublini számlára, ám a maszkok sosem érkeztek meg. Mint kiderült, csalás áldozatai lettek, az elkövetők csak kiadták magukat ezen cégek képviselőinek, amelyeknek a weboldalát is lemásolták a siker érdekében. Az így szerzett összeg biztonságos számlára menekítésére azonban már nem jutott idejük – a hatóságoknak sikerült követniük a pénz nyomát, és az érintett számlákat befagyasztották, az elkövetőket pedig letartóztatták.[25] Az Europol sajtóközleményében egy olyan ügyre hívta fel a figyelmet, amelyben egy cég munkatársait vették rá az elkövetők arra, hogy egy szingapúri cég számlájára utaljanak 6,6 millió eurót kézfertőtlenítőkért és szájmaszkokért cserébe, ám ezeket sosem szállították le.[26]

Azonban nemcsak a vállalatok és a szervezetek vannak kitéve a csalás veszélyének. A Palo Alto Networks amerikai kiberbiztonsági cég elemzéséből kiderül,[27] hogy számos esetben az egyszerű felhasználók jelentik a célpontot: a webshopok, amelyek maszkokkal és más védekezési eszközökkel igyekeznek pénzt kicsalni az áldozatokból, a bankkártyaadatok ellopására létrehozott oldalak, a tiltott gyógyszereket árusító weboldalak, a pánikkeltéssel vásárlásra ingerlő oldalak és a kriptovalutákat bányászó kódot tartalmazó oldalak mind őket célozzák meg.[28]

A fizetési csalásoknál is megfigyelhetők voltak újdonságok, ám ezek nem annyira a vírushelyzettel, mint inkább egy módszerrel, a SIM kártya cseréjével állnak összefüggésben. Az elkövetési mód nagyon célzott, és alapos információgyűjtés előzi meg: valamilyen módon meg kell szerezni a célpont banki hitelesítő adatait, majd ezek birtokában hamis dokumentumok segítségével új SIM kártyát igényelnek a célpont mobilszolgáltatójától, és arra irányítják a netbanki belépés-

[24] Wiggen i. m. (8. lj.) 3.

[25] Interpol: Unmasked: International COVID-19 Fraud Exposed, https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed.

[26] Europol: How Criminals Profit from the COVID-19 Pandemic, https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic.

[27] Janos Szurdi et al.: Studying How Cybercriminals Prey on the COVID-19 Pandemic. *Unit42,* https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/.

[28] Ezek a programok a felhasználó tudta nélkül települnek az eszközére, és annak hardverkapacitását arra használják, hogy az elkövetők számára kriptovalutákat termeljen. Ezt a szakirodalom *cryptojacking*nek nevezi. Részletesebben l. Karl Sigler: Crypto-Jacking: How Cyber-Criminals are Exploiting the Crypto-Currency Boom. 9 *Computer Fraud & Security* (2018) 12–14.

hez és a tranzakciók megerősítéséhez szükséges SMS kódot, aminek birtokában aztán a számlán található pénz elutalható.[29] A módszer elterjedtsége minden tagállamban különbözik. A SIM kártya cseréjének módszerével kapcsolatban idehaza is több eset nyilvánosságra jutott,[30] bár ebben az esetben a járvány nem közvetlenül kapcsolódik az elkövetéshez, de az ennek idején megemelkedett számú digitális fizetési tranzakció több csalási alkalmat is teremt az elkövetők számára.

1.1.2. Kártékony programok

A rosszindulatú programok *(malware)* olyan szoftverek, amelyek a felhasználó tudta és akarata nélkül települnek az eszközére, és aztán valamilyen módon károsítják is azt, például adatlopást vagy a támadó számára az eszközhöz való hozzáférést eredményezhetnek.[31] Ezek potenciális terjedéséről a Palo Alto Networks már említett elemzése is ír,[32] így például az elkövetők a koronavírussal összefüggésben információt kínáló weboldalakat hoznak létre, amelyekről ezek a programok a gyanútlan felhasználók eszközére települnek, amikor informálódni próbálnak. Az orosz Kaspersky Lab kiberbiztonsági cég is arra figyelmeztetett, hogy a karantén idején megnövekedett népszerűségű *streaming* szolgáltatások kapcsán is érdemes körültekintőnek lenni, ugyanis a megbízhatatlan oldalak látogatása kártékony programok településével járhat.[33]

A zsarolóvírus *(ransomware)* a rosszindulatú programok egy különleges válfaja, amely olyan módon okoz kárt, hogy titkosítja az eszközön található adatokat, és azokhoz újra hozzáférést csak bizonyos összeg megfizetése érdekében enged, ennek elmaradása esetén az adatokat végleg törli. Ezt a fizetést jellemzően anonim módon, általában valamely kriptovalutában (pl. Bitcoin) kérik az elkövetők.[34] 2017-ben végigsöpört a világon a WannaCry zsarolóvírus, majd később a Petya és a NotPetya, amelyet követően Kalifornia állam önálló büntetőjogi tényállásként vezette be jogrendjébe a zsarolóvírus készítését.[35] Azóta úgy tűnik, hogy az ilyen hatalmas visszhangot keltő támadások ideje lejárt. Ezek hazai jogi megítélése is nehézkes, például a zsarolás (Btk. 367. §) tényállása, amely a fogalomban is szerepel, nem feltétlenül állapítható meg.

[29] Europol, IOCTA 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, 4.2 pont.

[30] Horváth Csaba László: Krimibe illő csalással nullázták le egy magyar család bankszámláját. *24.hu,* 2020. szeptember 22. https://24.hu/fn/gazdasag/2020/09/22/mkb-bank-telenor-sim-kartya-csalas-internetbank-sms-bankszamla.

[31] A kártékony programok különböző fajtáiról bővebben l. Sorbán Kinga: Vírusok és zombik a büntetőjogban. Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res*, 2018/2., 376–377.

[32] Szurdi i. m. (27. lj.).

[33] David Emm: COVID-19 Survival Guide for Your Digital Life. *Kaspersky Daily,* 2020. április 7., https://www.kaspersky.com/blog/coronavirus-digital-survivor-guide/34715.

[34] Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modernkori magyar rendészettudományig*. Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2017. 167.

A kriptovaluták bűnözésben betöltött szerepével kapcsolatban bővebben l. Mezei Kitti: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban. *Pro Futuro,* 2019/1., 79–98.

[35] Mezei i. m. (21. lj.) 60–61.

Ezzel kapcsolatban még folyik a vita a hazai jogirodalomban, de jelenleg a legvalószínűbbnek az tűnik, hogy a zsarolóvírus használata a Btk. 423. § szerinti információs rendszer vagy adat megsértésének minősül.[36]

Az Europol április 3-án készült jelentése szerint a járványhelyzet a zsarolóvírussal operáló bűnözők számára is lehetőséget jelent, különösen a kórházak és az egészségügyi intézmények elleni támadásoktól kell tartani, mivel ezekben sokkal nagyobb a valószínűsége annak, hogy az áldozat fizet, hiszen ellenkező esetben életek kerülnek veszélybe. Az Europol arra is felhívja a figyelmet, hogy a járványidőszak alatt az eddig ilyen tevékenységet folytató bűnözői körök új közreműködők után néztek, hogy maximalizálni tudják a nyereségüket.[37] Az Interpol ebben a tárgyban kiadott figyelmeztetése is megerősíti, hogy világszintű probléma lett a kórházakat célzó zsarolóvírusokból.[38] Csehországban március 13-án érte zsarolóvírus-támadás az ország legnagyobb kórházát, a brnói egyetemi klinikát, aminek eredményeképp az informatikai rendszereik egy részét le kellett állítani, és a tervezett beavatkozásokat későbbre halasztani, ám ez szerencsére az alapellátást és a vírussal kapcsolatos feladatokat nem érintette.[39]

Az Europol 2020 IOCTA jelentésének 2.2 pontja is részletesen foglalkozik a jelenséggel. Az elmúlt időszakban a zsarolóvírusos-támadások egyre célzottabbá váltak, és főként a központi és a helyi közigazgatási szervek, az egészségügyi és oktatási intézmények, valamint az alapvető szolgáltatók ellen irányulnak. Az egészségügy elleni zsarolóvírusos támadások nem jelentenek újdonságot, ám a járvány hatására megnőtt a számuk. További újdonságnak számít, hogy az elkövetők már nemcsak a titkosított adatok törlésével fenyegetnek, hanem azzal is, hogy azokat online elárverezik, ami különösen akkor lehet hatásos fenyegetés, ha a célpont sok harmadik személy adatait – ideértve az érzékeny, pl. egészségügyi adatokat – kezeli és tárolja. (A Sodinokibi nevű zsarolóvírussal szerzett adatok esetében már dokumentáltak ilyen árverési próbálkozásokat.) További problémát jelent a zsarolóvírusos támadások nagy látenciája, ugyanis az áldozatok sokszor inkább fizetnek, semmint a hatóságokhoz forduljanak és vállalják ennek következményeit, például a reputációjuk csökkenését. Az egyre inkább a támadók fókuszába kerülő vállalkozások szívesebben dolgoznak együtt magán IT biztonsági cégekkel, mint a hatóságokkal.

1.1.3. Egyéb bűncselekmények

A fenti két kategória mellett számos egyéb, a kibertérben megjelent bűncselekményfajtára is hatással volt a járványhelyzet. Ezek között említhető az online gyermekpornográfia is. Az ilyen felvételek online terjesztése már az 1990-es évektől elkezdődött, és egyre nagyobb problémává vált.[40] Az ilyen típusú felvételek különösen nagy kárt képesek okozni az áldozatoknak, hiszen

[36] Nagy–Mezei i. m. (33. lj.) 168.

[37] Europol i. m. (9. lj.) 5.

[38] Interpol: Cybercriminals Targeting Critical Healthcare Institutions with Ransomware, https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

[39] Wiggen i. m. (8. lj.) 4.

[40] Yaman Akdeniz: *Internet Child Pornography and the Law National and International Responses*. Ashgate. Routledge, 2008. 1.

nemcsak azok elkészítése során válnak áldozattá (elsődleges viktimizáció), de azt követően is bármikor, amikor ezek a felvételek újra előkerülnek (másodlagos viktimizáció).[41] A kibertérben történő elkövetés számos új eszközt adott a gyermekpornográfiát készítő és fogyasztó elkövetők kezébe: az új készítési technikák és módok mellett új platformokat, titkosított kommunikációt és anonimitást, globális lehetőségeket.[42]

Az Europol 2020-as IOCTA jelentésének 3.2 pontja alapján az online gyermekpornográf tartalomra rekord mennyiségű bejelentés érkezett a lakosságtól, a piaci szereplőktől és harmadik országokból. Az Európai Unió tagállamai is arról számoltak be, hogy a lezárások idején nőtt a gyermekpornográf tartalmú oldalakhoz való blokkolt hozzáférési kísérletek száma. Hasonló növekedés volt megfigyelhető a *peer-to-peer* (P2P) fájlcserélő hálózatokon is a gyermekpornográfia terjesztésében márciusban. Különösen aggasztó, hogy a lezárások idején megnőtt a fiatalok által saját magukról készített gyermekpornográf tartalmak száma, amelyeket hasonló korú ismerőseiknek küldenek el *(sexting)*. Számos hasonlóan aggasztó trend létezik még ezenkívül, például a gyermekek szexuális abúzusának élő közvetítése *(streamelése),* amely a gyermekpornográfiával összefüggő büntetőjogi szabályozás kereteit is szétfeszíti (például az elkövetési magatartások terén), és a hatóságok egyébként is korlátozott erőforrásait még jobban leterheli. Mindemellett a fiatalok internethasználatuk során kitettek a szexuális ragadozóknak is. Az Egyesült Nemzetek Szervezete Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala (UNODC) jelentésében arra figyelmeztet, hogy a gyermekek behálózása *(grooming)* és szexuális zsarolása egyaránt jelentős probléma, valamint az online tartott órákra történő beszivárgás lehet az elkövetők egyik módszere.[43]

A járvány hatással volt az illegális javak kereskedelmére is. A legtöbb lezárással érintett országban jelentősen visszaesett az utcai kábítószer-terjesztéssel összefüggő bűncselekmények száma, ugyanakkor azok egyre inkább az online térbe helyeződtek át, a *dark web*re. Az internetnek ezt a részét sokszor övezi misztikum, ami a média által róla festett képnek is köszönhető, ám az itt tevékenykedő elkövetők inkább a felhasználó-barátság megteremtésében és a bizalom kiépítésében érdekeltek, hiszen ezek elengedhetetlenek ahhoz, hogy az itteni illegális kereskedelem még jobban fellendüljön. Az IOCTA jelentés 5.2 pontja részletesen foglalkozik ezekkel, megállapításai szerint az eladók megbízhatóságának ellenőrzésére saját rendszert alakítottak ki a DarkNet Trust oldalon, amely digitális ujjlenyomatok és felhasználónevek alapján végez kereséseket tízezernyi *dark web*es piacon. Mindezek mellett információs oldalakat is létrehoznak, és saját keresőszolgáltatásokat is (pl. Recon, Kilos), amelyek az eladó megbízhatósága mellett az elérhető kábítószerfajtákat is mutatják. Az online kábítószer-kereskedelemmel foglalkozó platformok üzemeltetői gyakran szándékosan rövid ideig tartanak csak fent egy oldalt, ami szinte lehetetlenné teszi a hatósági fellépést ellenük.

41 Alisdair Gillespie: *Cybercrime: Key issues and debates*. New York, Routledge, 2015. 228.

42 Ezekről bővebben l. Dornfeld László: ICTs and Sexual Exploitation of Children in Europe. In: Mehdi Khosrow-Pour (szerk.): *Encyclopedia of Criminal Activities and the Deep Web*. Hershey, IGI Global, 2020. 565–579.

43 UNODC: Cybercrime and COVID19: Risks and Responses, https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf.

A jelentés 5.3 pontja az illegális termékek árusításával foglalkozó oldalak üzemeltetőivel foglalkozik. Akadtak olyanok, akik a profitszerzés lehetősége ellenére betiltották a járvány elleni védekezéssel összefüggő hamis termékek árusítását. Az 5.4 pont megállapításai szerint azonban ez korántsem általános: az OpenBazaar nevű *dark web*es piacon például fegyverek és fentanyl mellett az előbbiekben említett, a járvány elleni védekezéssel összefüggő hamis termékek is megjelentek.

2. Járvány és dezinformáció

A dezinformáció és szűkebben az álhírek nem tartoznak szorosan a kiberbűncselekmények közé, ugyanakkor a járvány kapcsán elengedhetetlen foglalkozni a jelenséggel. A dezinformáció az ebben érdekelt államok mellett a bűnelkövetők egyik kedvelt eszköze is, mint arra korábban már láthattunk példákat a járvánnyal összefüggésben (pl. védekezésre nem alkalmas termékek árusítása). A dezinformáció elleni fellépés azért is nagyon fontos kérdés a büntetőjog kontextusában, mert például a csalás, megtévesztés eszköze is lehet, hiszen az elkövetők szándékosan félelmet kelthetnek, hogy azt kihasználva tudjanak bűncselekményeket elkövetni, mint arra korábban is utaltam az Interpol és mások kutatásainak fényében.

A járványhelyzet drasztikusan megemelte az álhírek számát. A hamis információk terjesztése mögött eltérő szereplők állhatnak eltérő motivációkkal, például bűnözők, akik ezáltal akarnak profitot szerezni, államok vagy politikai csoportok, amelyeket geopolitikai érdekek mozgatnak, illetve opportunisták, akik a hivatalos forrásokat akarják diszkreditálni.[44] Érdemes továbbá a „hasznos idiótákat" is megemlíteni, akik őszintén elhiszik az álhírekben található hamis információkat, és tovább terjesztik azt ismerőseik között.[45] Az álhír nagyon eredményes lehet, és viszonylag kis költséggel jár: a 2016-os amerikai elnökválasztás kapcsán – amely az angol *„fake news"* kifejezés elterjedését hozta magával – a Twitteren végzett kutatás alapján az összes hírfogyasztás 6%-át tette ki, és a felhasználók 0,1%-a felelt az álhíreknek való kitettség 80%-ért, ugyanakkor a kitettség 80%-a a felhasználók 1%-át érintette.[46]

2.1. Állami szereplők

A mostani járványhelyzet újdonsült növekedést hozott az álhírterjesztés mértékében. Az Európai Külügyi Szolgálat által az orosz állami propaganda ellen létrehozott EUvsDisinfo oldalon ennek a jelenségnek is nagy figyelmet szentelnek. Az álhírek kapcsán tavasszal közreadott elemzésből kitűnik, hogy az államilag szponzorált álhírek elsősorban az Egyesült Államok ellen

[44] Europol: COVID-19: Fake News, https://www.europol.europa.eu/covid-19/covid-19-fake-news.

[45] Hogy mi alapján hisz el valaki nagyobb eséllyel álhíreket, arról nincs tudományos konszenzus. Már a vírus terjedése kapcsán is folynak ez irányú kutatások. L. Gordon Pennycook et al.: Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy-Nudge Intervention. 31(7) *Psychological Science* (2020) 770–780. https://journals.sagepub.com/doi/full/10.1177/0956797620939054.

[46] Nir Grinberg et alii: Fake News on Twitter During the 2016 US Presidential Election. *Science,* 2019. január 25., 374–378.

irányultak, másodsorban pedig az EU tehetetlenségét pellengérezték ki, azt állítva, hogy ez az Unió szétesését fogja eredményezni. Harmadik helyen az a teória állt, hogy a járvány egy kínai fegyver a gazdaság tönkretételére, míg a negyedik leggyakoribb narratíva az volt, hogy a koronavírus a „globális elit" tervének a része. A 10 legnagyobb közösségimédia-eléréssel rendelkező álhír közül öt orosz, három arab, és csak egy-egy angol, illetve spanyol nyelvű. Az oldal által vizsgált 152 álhír együttesen mintegy 260 ezer emberhez jutott el.[47]

Érdemes megemlíteni a kínai állami propagandát is, amely április elején azzal a váddal állt elő, hogy az Egyesült Államok áll a vuhani fertőzés mögött. A kínai Külügyminisztérium szóvivőjének ilyen értelmű kijelentését április elején 160 millió alkalommal tekintették meg.[48] A kínai állami média igyekszik elterelni a járvány világméretűvé válása miatti felelősséget az ország hatóságairól, azt a képet építve ehelyett, hogy „Kína áldozata időt nyert a világ számára". A két ország néha hajlamos egymás narratíváit átvenni, amennyiben érdekük úgy kívánja: a kínai állami média nyomán az Oroszországhoz köthető álhírgyártók is cikkeztek arról, hogy titkos amerikai biológiai laboratóriumok működnek Ukrajna területén, ahol állításuk szerint a vírust „létrehozták". Az orosz támogatásból működő médiumok többször védelmükbe vették Kínát, alaptalannak és boszorkányüldözésnek nevezve minden ellenük irányuló kritikát.[49] Mindezek mellett fontos megemlíteni, hogy a nem demokratikus berendezkedésű államokban a járványhelyzetet gyakran használták a független sajtó és újságírók ellehetetlenítésére. Ez történt például Latin-Amerika több országában, így Venezuelában is, ahol több tucat újságírót vettek önkényesen őrizetbe,[50] valamint a délkelet-ázsiai régióban, ahol például Kambodzsában került sor ilyesmire.[51]

2.2. Nem állami szereplők

Témánk szempontjából sokkal lényegesebb azonban a nem állami szereplők által terjesztett álhírek és dezinformáció. Jelentős számú emberhez eljutott az az álhír, ami szerint a vírust valójában az 5G adótornyok okozzák. Ezen teória kiötlői azt állítják, hogy az 5G adótornyok gyengítik az immunrendszert, vagy e technológia segítségével „aktiválják" a vírust az ember szervezetében. Az információ természetesen teljes képtelenség, már csak azért is, mert számos olyan országban is terjed a vírus, ahol nincs is ilyen hálózat. Ez azonban nem akadályozta meg az elmélet hívőit abban, hogy március folyamán több mint 20 darab 5G adótornyot felgyújtsa-

[47] EUvsDisinfo: Throwing Coronavirus Disinfo at the Wall to See what Sticks, https://euvsdisinfo.eu/throwing-coronavirus-disinfo-at-the-wall-to-see-what-sticks.

[48] Robert Boxwell: How China's Fake News Machine is Rewriting the History of COVID-19, even as the Pandemic Unfolds. *Politico,* 2020. április 4., https://www.politico.com/news/magazine/2020/04/04/china-fake-news-coronavirus-164652.

[49] EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may.

[50] Margarita R. Seminario: Free Press, Fake News, and Repression During COVID-19: Venezuela and Nicaragua. *CSIS,* 2020. június 4., https://www.csis.org/analysis/free-press-fake-news-and-repression-during-covid-19-venezuela-and-nicaragua.

[51] Mu Sochua: Coronavirus „Fake News" Arrests are Quieting Critics. *FP*, 2020. május 22., https://foreignpolicy.com/2020/05/22/coronavirus-fake-news-arrests-quiet-critics-southeast-asia.

nak az Egyesült Királyságban.[52] Az álhírek kitalálóinak fő célja azonban általában a profit, hívja fel a figyelmet jelentésében az Europol. Így például az álhíreket terjesztő oldalon próbálnak minél nagyobb látogatottságot generálni, hogy jelentős hirdetési bevételekhez jussanak. Hatalmas bevételt hozhat, ha valamely szerről elterjesztik, hogy az gyógyítja a betegséget, így az iránta való keresletnövekedést használhatják profitszerzésre.[53]

A járványhelyzet során jelentkező dezinformációra és álhírterjesztésre az állami és nem állami szereplők egyaránt próbáltak reagálni, így azok visszaszorításában részt vesz a magánszektor és a tudományos élet is. A nem állami szereplők az álhírek terjedését a saját eszközeikkel próbálják visszaszorítani, például számos tudós igyekszik cáfolni a téves információkat, és az Egészségügyi Világszervezet (WHO) egy dedikált oldalt is indított az álhírek cáfolására.[54] A Facebook, ahol nagyon eredményesen terjedtek álhírek a 2016-os amerikai elnökválasztás idején, már igyekszik új eszközökkel fellépni a jelenség ellen. Ennek része például a külső „tényellenőrzők" igénybevétele és az álhírek megjelölése azok cáfolatával együtt. Miután kiderült, hogy korábbi törekvései ellenére az álhíreknek jelölt tartalmak 40%-a továbbra is elérhető a Facebook oldalán, a járvány kapcsán a közösségi oldal úgy válaszolt erre, hogy azokat a felhasználókat, akik ilyen álhírekkel találkoztak, külön értesíti.[55]

Az állami válasz elsősorban az álhírterjesztők elleni fellépést foglalja magában. Hazánkban a koronavírus elleni védekezésről szóló 2020. évi XII. törvény a Btk. 337. § alatt szabályozott rémhírterjesztés tényállását is módosította, megalkotva az eredetileg közveszélyhez és annak helyszínéhez kapcsolódó bűncselekmény új, második alapesetét, amelynél csak a nagy nyilvánosság feltétel, és a különleges jogrendi állapot fennállása esetén alkalmazandó. A módosítás heves vitákat váltott ki a politikai közéletben és a jogtudományban egyaránt. Míg az előbbi részéről főleg a szólásszabadság aránytalan korlátozása miatt,[56] addig az utóbbiéról a bizonytalan megfogalmazás és a gyakorlati alkalmazási problémák miatt érte kritika.[57] A rendelkezéssel kapcsolatban alkotmányjogi panasz is érkezett, ám ezt az Alkotmánybíróság május 11-én tartott soron kívüli teljes ülésén elutasította.[58] A testület érvelése szerint a tiltás csak a tudottan valótlan vagy elferdített tényállításokra vonatkozik, a kritikus véleményekre, tévedésekre nem, így az nem korlátozza aránytalanul a szólásszabadságot. A veszélyhelyzet hazai fennállása során több személlyel szemben is indult eljárás az új tényállás alapján, ám erről jelenleg nem érhetők el statisztikai adatok.

52 Rachel Schraer – Eleanor Lawrie: Coronavirus: Scientists Brand 5G Claims „Complete Rubbish". *BBC*, 2020. április 15., https://www.bbc.com/news/52168096.

53 Europol i. m. (9. lj.) 12–13.

54 WHO: Coronavirus disease (COVID-19) advice for the public: Mythbusters, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters.

55 Mark Scott: Facebook to Tell Millions of Users They've seen „Fake News" about COVID-19. *Politico*, 2020. október 27., https://www.politico.eu/article/facebook-avaaz-covid19-coronavirus-misinformation-fake-news/.

56 Magyar Helsinki Bizottság: Rémhírterjesztés újratöltve (2020. március 27.), https://www.helsinki.hu/remhirterjesztes-ujratoltve.

57 Bencze Mátyás – Ficsor Krisztina: A koronavírus kihívásai és a jogtudomány: a rémhírterjesztés tényállásának jogalkalmazási kérdései. *JTI,* 2020. április 2., https://jog.tk.mta.hu/blog/2020/04/a-remhirterjesztes-tenyallasanak-jogalkalmazasi-kerdesei.

58 http://public.mkab.hu/dev/dontesek.nsf/0/BD83430C4D2A942AC125855E005C4028?OpenDocument.

3. Összegzés

Mint az előzőekben láthattuk, a koronavírus-járvány és a rá adott állami reakciók alapvetően határozták meg a 2020-as bűnözési trendek alakulását, mind az offline, mind az online térben. Az Europol sajtóközleménye is rámutat, hogy a bűnelkövetők hamar reagáltak a járványhelyzetre, és igyekeztek azt saját céljaikra használni. Az online csalás, a zsarolóvírusok és az álhírek terjesztése jelentős növekedést mutatott ebben az időszakban. Jelentősen megnőtt továbbá a gyermekpornográfiával összefüggő bűncselekmények száma is, valamint az illegális javak *dark web*es kereskedelme. Mindeközben a hagyományos, személyes interakciókra épülő elkövetések száma jelentősen visszaesett tavasszal. A rutintevékenység-elmélet alapján ez nem is olyan meglepő, hiszen ebben az időszakban a társadalom működése jelentős mértékben az online térbe került át a közösségi távolságtartás kívánalmainak megfelelően, ezért a potenciális áldozatok már nem az utcákon, hanem a kibertérben voltak megtalálhatók.

Adatvédelemmel kapcsolatos kérdések is felmerültek. A Google a változó utazási szokásokról tett közzé anonimizált adatsorokat,[59] míg számos országban a mobiltelefonok cellaadatainak gyűjtésével próbálják lassítani a járvány terjedését. Ennek hosszú távú veszélyeire azonban nem más figyelmeztetett, mint Edward Snowden, aki évekkel ezelőtt a hatalmas mértékű állami digitális megfigyelés veszélyeire hívta fel a figyelmet.[60] Argentínában például az országba beutazóknak kötelező egy, a mozgásukat követő kormányzati applikáció telepítése a mobiltelefonjukra.[61] Norvégiában is létezett hasonló program, ugyanakkor annak használata önkéntes alapon történt. Látható, hogy a járvány során felmerülő kérdések egy jelentős része az adatvédelemre utal vissza.[62]

Más, a kihívásokra adott válaszok is kritikára adtak okot, például idehaza a rémhírterjesztés tényállásának kiterjesztése a járványhelyzettel kapcsolatos hamis információk közzétételére. Ugyan az aggodalom nem alaptalan, hiszen maga is a WHO is egymásnak ellentétes információkat tett közzé a járványról (pl. az ember–ember közötti terjedés vonatkozásában), illetve később a korábbiaknak ellentmondó ajánlásokat tett (pl. a maszkhasználat és a lezárások hasznossága kapcsán), a sietve meghozott rendelkezést az Alkotmánybíróság nem találta a szólásszabadságot aránytalanul korlátozónak, rámutatva, hogy az csak a tudatosan terjesztett hamis hírek vonatkozásában alkalmazandó, a valós tények terjesztésére és a jóhiszemű tévedésekre nem vonatkozik. Mindezekből azonban látható, hogy nemcsak a fenyegetések, de az azok ellen hozott intézkedések terén is akadnak még kérdések, amelyeket érdemes alaposan megvizsgálni. Számos olyan jogi és technikai természetű probléma van a digitális világban, amelyeknél a szabályozás jelenlegi szintje egyértelműen nem elegendő. A járvány ezekre is ráirányítja a figyelmet, ugyanakkor az érdemi diskurzusra csak a járványhelyzet után, annak tapasztalatai birtokában kerülhet sor.

---

[59] Korona az adatvédelmen: a Google részben kiteregette lapjait. *Mandiner*, 2020. április 20., https://precedens.mandiner.hu/cikk/20200420_korona_az_adatvedelmen_a_google_reszben_kiteregette_lapjait.

[60] Dömös Zsuzsanna: Kétélű fegyver a koronavírus-járvány lassításának egyik hatékony eszköze. *24.hu*, 2020. április 5., https://24.hu/tech/2020/04/05/koronavirus-jarvany-technologia-pandemia-adatvedelem-mobiltelefon-cellaadat-helymeghatarozas/.

[61] A Nemzeti Bevándorlási Igazgatóság 1771/2020. rendelkezése, https://www.boletinoficial.gob.ar/detalleAviso/primera/227170/20200326.

[62] Európa Tanács i. m. (18. lj.).