Dr. Nagy Zoltán:*

A karantén krimogén veszélyei

2019 októberében már új típusú vírusról, abban megbetegedett személyekről beszéltek egyre többen. Magyar sportolók is a novemberi vuhani játékokról hazatérve e vírusok okozta megbetegedésekről adtak hírt.[1]

Majd január 25-e, a kínai Holdújév-ünnep – amely hagyományosan a családlátogatások, vendéglátások ideje – után ezrével érkeztek kínaiak Európába, köztük Magyarországra is. Magyarországon több mit két és fél ezer kínai diák tanul, amihez számítsuk hozzá a kisebb-nagyobb boltokban, piacokon, vásárokban, éttermekben, és az otthonukban dolgozók ezreit.

Természetesen munkája vagy anyagi helyzete miatt nem minden kínai ment haza újévet köszönteni.

Magyarországon márciusban rendelték el több lépésben a karantént, az oktatási intézmények látogatásának tilalmát, a gyárak, üzemek tevékenyégüket fogták vissza, részint megrendelés, a kereslet, részint munkaerő hiánya miatt, hiszen a kisiskolásokkal valamelyik családtagnak otthon kellett maradni. Bár Magyarországot is érzékenyen érintette (érinti mind a mai napig) az ismeretlen vírus okozta járvány, de nem volt más megoldás. Oltóanyag és biztos, teljes körű terápia hiányában az emberi érintkezéseket csökkenteni kellett, és persze kellene most is. A járvány dinamizmusának visszafogása érdekében tett kormányzati fellépést összességében eredményesnek értékelhetjük.

Emeljük ki, az egészségügyi, a kereskedelmi dolgozók, a katonák és a rendőrök tiszteletet parancsoló áldozatvállalását, valamint lakosság fegyelmezettségét, az egymás iránti szolidaritást, öntevékenységet (nagyon sokan maszkokat gyártottak másoknak is, az idős embereket a bevásárlásokban segítették, az oktatás szereplői a kihívásokra gyorsan, ismét csak összességében eredményesen reagáltak és sorolhatnánk a pozitív tapasztalatokat).

Írásunkat a koronavírus (COVID–19, tudományban használatos elnevezéssel SARS-COV-2) miatt elrendelt a karanténhelyzet[2] inspirálta, ám talán feltárhatók olyan kriminogén veszélyek, amelyek akár koronavírus második (vagy sokadik) hulláma, akár más veszélyhelyzet (egészségügyi, természeti, ipari katasztrófa, háború stb.) idején az otthon maradás, a bezártság miatt potenciálisan fenyegethet egyes személyeket, családokat, együtt élőket, amelyekre fel kell figyelnünk, és fel kell készülnünk.

A karantén során leselkedő potenciális kriminogén veszélyek a valós térben keletkezhetnek, kiéleződhetnek, valamint a virtuális térből érkezhetnek.

Potenciális kriminogén veszélyek a valós térben karantén idején

1. A családon belüli erőszak, stációi, és az adott büntetőjogi reakciók

A valós térben a családtagok között a mindennapi együttélés során léteznek kisebb-nagyobb nézeteltérések, viták. A karantén idején e viták, konfliktusok kiéleződhetnek, gyakoribbá, élesebbé válhatnak, Ennek okait az alábbiakban véljük:

– a hosszabb ideig tartó összezártság,

– ennek monotonitása,

– a betegségtől való idegőrlő félelem, folyamatos aggódás a családtagok, szülők, nagyszülők egészsége miatt,

– a fizikai kapcsolat hiánya a szülőkkel, nagyszülőkkel,

– a híradásokban a halottak és betegek számának folyamatos közlésének (mintha háborúban élnénk) nyomasztó egyhangúságával,

– aggódás az egyéni, illetve a család anyagi biztonsága, a munkahely elvesztése miatt,

– mindezeket megtetézve a bezártságot különösen nehezen megélő gyermekek nevelésének, az őket terhelő új, technikai eszközök használatának jártasságát feltételező oktatási megoldásokban való sokszor nem könnyű szülői feladatával,

– nyilván létezhetnek további okok is, amelyek a bezártság körülményei közt együtt járó problémákat okoznak.

* Egyetemi docens, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Büntetőjogi Tanszék, NKE RTK BGKB Tanszék.

[1] https://hvg.hu/itthon/20200507_katonai_vilagjatekok_vuhan_koronavirus [Letöltés ideje: 2020.07.10.]

https://m4sport.hu/triatlon/cikk/2020/04/07/toth-tamas-lehetett-az-elso-koronavirusos-beteg-magyar-sportolo/ [Letöltés ideje: 2020. 07.10.]

[2] A karantén kifejezés az olasz „negyven” szóból származik. A középkorban az olasz városállamokban járványok idején 40 napig (olaszul: quaranta giorni) a városok kikötőjében – elkülönített helyeken – kellett vesztegelniük a hajókon érkezőknek.

E tényezők, önmagukban, halmazottan jelentkezve, egymást erősítve komoly feszültségforrást jelentettek (és jelentenek) az együtt élő személyek számára, amelyekre – korábbi tapasztalatok, életélmények hiánya miatt – nem volt felkészülve.

Tegyük hozzá a különböző anyagi és egzisztenciális élethelyzetek, a családi kapcsolatok minősége, az emberek közötti fizikai és mentális különbségek (pl. a toleranciatűrő képességük, a kapcsolat megtartásának prioritása és más körülmények) eltérőek, és ezek a konfliktusok keletkezését, dinamizmusát döntően befolyásolják.

A családon belüli konfliktus jellemzően valamely vélt vagy valódi okból keletkezett vitából fejlődik ki, amely elvezethet – sajnos tapasztalatok szerint el is vezet – személy elleni vagy tulajdon elleni erőszakos bűncselekményéig.[3]

A konfliktus következő stációja a sértegetés, mely már jogi beavatkozásra lehetőséget teremtene. Ha az egyik fél tények említésével (a másik fél származása, vallása, jövedelme nagysága, korábbi szexuális kapcsolatára, kapcsolataira utalva stb.) sérti a másik felet, ha ez a tényállításon alapuló sértegetés, harmadik fél előtt zajlik, akkor rágalmazás (Btk. 226. §), ha négyszemközt történt, akkor becsületsértésként értékelhető (Btk. 227. §). Mindkét bűncselekmény magánindítványra büntethető, amely esetben, az elkövető kilétének megismerésétől (az elkövetés pillanatában természetesen már ismert) számított egy hónapig [Be. 378. § (3) bekezdése] átgondolhatja azt, hogy indítsanak-e büntetőeljárást a másik féllel szemben.

A sértés, sértegetés folyamatossá válhat, egyre fenyegetőbb, egyre durvább kifejezések hangoznak el, és már nem is vélt vagy valódi okokról, tényekről folyik a vita, hanem a másik fél megfélemlítése, rettegésben tartása a cél, amely személy elleni erőszakos (a sértett vagy a gyermek bántalmazása megverésével, megölésével), vagy közveszélyt okozó (pl. felgyújtja a lakást) bűncselekmény kilátásba helyezésével is történhet. Tegyük hozzá, ha a zaklatást házastársa, élettársa sérelmére követi el, akkor a zaklatás minősített esetéért felelne [Btk. 222. § (3) bekezdése].

Amennyiben a vita eldurvulása az emberi méltóságot súlyosan sértő, megalázó, erőszakos magatartásba fordul vagy a közös gazdálkodás körébe tartozó, közös vagyonba tartozó tárgyat elvon, akkor kapcsolati erőszak bűncselekményéért (Btk. 212/a. §) felel.

A tényállásban a testi sértés szintjét el nem érő de a sértett emberi méltóságát sértő rendszeres, erőszakos magatartása és a gazdasági lehetőségektől megfosztás a büntetendő magatartás.

A rendszerességkapcsán megjegyzendő, hogy e fogalmon a visszatérően, de nem rövid időközönként történő erőszakos fellépésre (ezáltal az egységes akaratelhatározás hiányában), állapítható meg.[4] Másképp szólva, az elkövető magatartásában jelen van az erőszakos beállítottság. A rendszeres elkövetést az ugyanazon sértett sérelmére megvalósított testi sértés és a tettlegesen elkövetett becsületsértés [Btk. 227. § (2) bekezdése], akár egymást követő, ismétlődő elkövetése is megalapozza.[5]

Vélhetően a sértegető, zaklató, megalázó magatartások, melyek esetében fizikai sérülések nem, ám lelki sérülések annál inkább bekövetkeznek zöme, sajnálatosan látens marad.

Súlyos következménye ennek a folyamatnak, ha személy vagy tulajdon elleni erőszakos bűncselekmények meg is valósulnak. A Btk. a büntetendő cselekmények a testi sértéstől (Btk. 164. §), a szexuális kényszerítésen (Btk. 196. §), illetőleg a szexuális erőszakon (Btk. 197. §), a rongáláson (Btk. 371. §), a közveszélyokozáson (Btk. 322. §) át az emberölésig (Btk. 160. §) terjedhetnek.

A fizikai erőszakot mindig lelki, verbális erőszak kíséri, egyszerre éri a sértettet, amely a sértett fájdalmát tovább fokozza.

Látható, hogy a törvényhozó törekedett ennek a konfliktusfolyam (ennek durvábbá válását) követve, annak egyes fázisaira büntetőjogi tilalmat vonni, ami önmagában dicsérendő. Ugyanakkor a családon belüli erőszak megelőzése ennél összetettebb feladat, amely során az alkalmazandó eszközrendszerbe a családgondozás, pszichológusok, a gyermekeket is elérő konfliktusok esetében a pedagógusok, nem utolsósorban a rendőrség tevékenysége vonható.

E kriminogén folyamatba történő beavatkozásnak legális megoldásait, ami által megszakítható lenne ez a folyamat. mielőtt abból tragikus végkifejlett lesz.

Visszautalva tanulmányunk fő vonulatára, a veszélyhelyzetből eredő bezártság, a mindennapi aggódás, bizonytalanság megmérgezhetik, nehéz helyzetbe hozhatják a családi kapcsolatokat, felszínre hozhatják, kiélezhetik a már lappangó konfliktusokat. E konfliktusok verbális és fizikai erőszakba torkollhatnak. A hivatalos bűnügyi statisztikában sokszor meg sem jelennek, látensen fejtik ki drámai hatásukat.

Magunk a társadalomban, a mindennapjainkban érzékelhető tolerancia fogyását érzékelve e konfliktusok növekedését vélelmezzük.

2. A távol levő vagyontárgyak biztonsága

Az otthon maradás kötelezettsége miatt a tulajdonosok távol eső, más településen található tulajdonainak védelme is csorbát szenvedett. A nyaralók, üdülők, présházak, pincék, építkezési területek, telkek és más ingatlanok több hónapig védtelenül maradtak. Az egy-

[3] Virág, György – Kulcsár, Gabriella – Rosta, Andrea: Családon belüli erőszak In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay, Miklós (szerk.) Kriminológia Budapest, Magyarország: Wolters Kluwer Kft., (2019) 578–586. o. Hornyák Szabolcs: Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények. In. Tóth Mihály – Nagy Zoltán (szerk.) Magyar Büntetőjog Különös rész. Budapest, Osiris Kiadó, 2014. 184–185. o.

[4] Dr. László Balázs: A kapcsolati erőszak erőszak fogalmának dogmatikai beilleszthetőségéről. Büntetőjogi Szemle, 2020/1. 68–69. o. https://ujbtk.hu/wp-content/uploads/lapszam/BJSZ_202001.pdf [Letöltés ideje: 2020.07.11.]

[5] 17/2017, Büntető Elvi Határozat. https://kuria-birosag.hu/hu/elvhat/172017-szamu-bunteto-elvi-hatarozat [Letöltés ideje: 2020.07.11.]

máshoz közel levő épületek tulajdonosai, bérlői, akik év közben, ha különböző időpontokban, de megjelentek és figyelhettek a szomszédos ingatlanokra, most nem mehettek ingatlanjaikhoz. Ugyanakkor a karantén szabályait sem betartó, tipikusan magánlaksértést (Btk. 221. §), lopást (Btk. 370. §), rongálást (Btk. 371. §) vagy más bűncselekményt elkövetni kívánók számára ez lehetőséget teremtett.

Egy következő karanténidőszakban különösen üdülő-, vagy szőlőműveléssel érintett területeken szükséges a kényszerűségből nem látogatott ingatlanok védelmére figyelmet fordítani. Fontos lenne, a településen a rendőrség, polgárőrség az ingatlantulajdonosok, bérlők anyagi hozzájárulásával történő járőröztetése.

3. Vagyoni kárt okozó megtévesztő magatartások

a) A hatékony járványügyi védekezés sikerességéhhez az állampolgári fegyelmezettség nélkülözhetetlen volt. Ehhez az egyéni védőeszközök használata mind az adott személy, mind a közösség számára szükségszerű volt (és jelenleg is az). Sajnos, az egyéni védőeszközökkel a kereskedelemben „üzleteltek", a megnövekedett keresleten felbuzdulva felháborító, elképesztő drága árakért lehetett ezekhez hozzá jutni. A legvédtelenebbek voltak (és lesznek) a jelen járványban az idősek, akik életkoruknál voltak a legveszélyeztetebbek. Az önkormányzatok maszkot készíttettek a településeken élőknek. A pécsiekhez a postaládákba dobták be a lakásonkénti két maszkot. De ismertté vált olyan eset is, amikor az elkövetők önkormányzati dolgozóknak kiadva magukat védőeszközök, vírus elleni „csodaszerek" átadása vagy lakások fertőtlenítésének színlelése címén kívántak a gyanútlan (idős) sértett házába bejutni.[6]

Cselekményük majdan minősülhet magánlaksértésnek (Btk. 221. §) vagy lopás (Btk. 370. §) kísérletének.

b) A különböző okok folytán nehéz helyzetbe került emberek, közösségek segítése az egyik legemberibb tényked és. Ma Magyarországon bárki, bármikor csatlakozhat egy-egy adománygyűjtéshez, sőt gyakorlatilag indíthat is ilyen nemes kezdeményezést.

Jelen esetben az önkéntesen nyújtott és a rászorult emberek támogatását célul kitűző adománygyűjtést emeljük ki. A koronavírus-járvány miatt elrendelt karantén idején az állampolgári aktivitásról, segítőkészség megnyilvánulásáról már szó volt, és e körben az egészségügyi intézmények és dolgozói sok-sok példamutató támogatásban részesültek, így gépjárműveket kölcsönöztek, naponta gyümölcsöket és más élelmiszereket, tisztálkodási eszközöket vittek cégek és magánszemélyek a kórházakba, egészségügyi és szociális intézményekbe.

E tiszteletet érdemlő, őszinte segíteni akarást azonban ki is használhatják azok, akik csalárd szándékkal gyűjthetnek adományokat. A csalárdság abban valósul meg, hogy az összegyűjtött adományokat saját célra fordítják.[7] A magyar Btk. a csalárd célú adománygyűjtés színlelését akkor is büntetni rendeli, ha „csupán" ötvenezer forintot meg nem haladó, szabálysértési értékre követték el [Btk. 373. § (2) bekezdés bd) alpontja].

Csalás bűncselekménye gyanúja miatt az egészségügyi vészhelyzet idején 116 esetben indult büntetőeljárás.[8]

4. Rémhírterjesztés supplementuma

A koronavírus elleni védekezést megalapozó jogi keretek közül kiemeljük a rémhírterjesztés büntetőjogi tényállásának bővítését. Magyarország Kormánya a 40/2020. (III. 11.) Korm. rendelettel hirdette ki a veszélyhelyzetet az élet- és vagyonbiztonságot veszélyeztető tömeges megbetegedést okozó humán járvány következményeinek elhárítása, a magyar állampolgárok egészségének és életének megóvása érdekében Magyarország egész területére.

2020. március 30-án lépett hatályba az a Btk. módosítása amely a törvény 337. §-ában meghatározott rémhírterjesztés tényállását egészítette ki egy minősített esettel: „(2) Aki különleges jogrend idején nagy nyilvánosság előtt olyan valótlan tényt vagy való tényt oly módon elferdítve állít vagy híresztel, amely alkalmas arra, hogy a védekezés eredményességét akadályozza vagy meghiúsítsa, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő."

A tényállás módosításával, majd egyes megtörtént eljárási cselekményekkel összefüggő vitákat itt és most mellőzzük. A Btk. új rendelkezésével szemben alkotmányjogi panaszt nyújtottak be, melyet az Alkotmánybíróság 15/2020 (VII. 8.) sz. határozatában bírált el. Az Ab. leszögezte, hogy „a rémhírterjesztés csak szándékosan követhető el. Következésképpen az elkövetőnek tudatában kell lennie annak, hogy cselekményét különleges jogrend idején valósítja meg; hogy az általa állított tény valótlan, vagy a valós tényt jelentősen elferdítette, valamint annak is, hogy állításának közlése (objektíve) alkalmas arra, hogy a védekezés eredményességét akadályozza vagy meghiúsítsa. Az elkövető szándékának pedig ki kell terjednie a fentiek szerinti tudatos közlés nagy nyilvánosság előtti elkövetésére. Ha a tudattartama, illetve szándéka bármelyik elemre nem terjed ki, vagy ha az állítás objektíve nem alkalmas arra, hogy a védekezés eredményességét akadályozza vagy meghiúsítsa,

[6] http://www.zknp.hu/koronavirus-jarvannyal-kapcsolatos-csalasok-megelozese/ [Letöltés ideje: 2020.07.11.] https://hirvilag.hu/article/milliokat-kert-koronavirus-elleni-vakcinakert-egy-siofoki-csalo-4286655 [Letöltés ideje: 2020.07.11.]

[7] https://24.hu/belfold/2020/05/07/koronavirus-tamasi-csalas-vademeles/ [Letöltés ideje: 2020.06.11.]

[8] https://ezalenyeg.hu/kozugy/363-buntetoeljaras-indult-a-jarvannyal-osszefuggesben-4760 [Letöltés ideje: 2020.06.11.]

a bűncselekmény a büntetőjog szabályai szerint nem valósul meg" (ABH 46.pont).[9]

Kriminogén veszélyek a virtuális térben

A virtuális térből jelentkező fenyegetettség megnövekedett a karantén miatt. Ennek okai az alábbiakban összegezhető:

A köz- és felsőoktatás a digitális oktatás irányába nagy lépést tett azáltal, hogy a tananyag eljuttatása, a beszámoltatás, az önálló munkára ösztönzés számítógéppel, interneten történt.

A környezetem tapasztalatai alapján rögzíthető az, hogy a nagyon rövid idő (kb. egy hét iskolai szünet) alatt a pedagógustársadalom összességében rendkívül kreatívan, a technikai-személyi feltételekkel adekvátan hozta létre a tananyag átadásának és a tanulás ellenőrzésének a lehetőségét. E-mailben, szöveg-, hang- és videófájlban kiküldött elméleti feladatoktól, testnevelési gyakorlatokon, a személyes telefonbeszélgetéseken, interneten található feladatok megoldásán, a kiküldött dokumentum és az internetes feladat összekapcsolásán át a visszaküldeni kötelező videófelvételekig számos ötletes megoldás született. Azt gondoljuk, hogy ezeket a tapasztalatokat kellene best practice formában, minden pedagógus számára elérhetővé tenni, amely a bármely okból elrendelt karantén esetén alkalmazható, illetve a jelenléti oktatást kiegészíthetné, sőt kiválthatná. Hasznos abból a szempontból is, hogy a diákokat, hallgatókat az internet hasznos(abb) használatára ösztönözze.

Mindazonáltal az elektronikus környezetben történt oktatás még inkább kiemelte azokat a különbségeket, amelyek a társadalomban a technikai eszközök, az internet elérésében megmutatkoztak. Úgy véljük, ezen mindenképpen javítani kell, hogy a „technológiai eszköz és tudás" közötti különbségek csökkenjenek.

Az eddig ritkán, ritkábban, sokszor szórakozási céllal számítógépet, internetet használók egyfelől a diákok tanulásának, feladatmegoldásának segítése miatt, másfelől a kényszerhelyzet szülte felszabaduló idő miatt többet használták, használhatták a számítógépet, internetet, mint korábban.

A fentiek kapcsán egy kitérőt érdemes tenni. Több tízezer (vagy akár ennél is több) felhasználó volt kénytelen személyes adatait megosztani olyan alkalmazások igénybevétele miatt, amely az oktatás terepe volt vagy ahhoz segítséget nyújtott, pl. KRÉTA, Google Classroom, Microsoft Teams, Skype, továbbá ennek Business változata (más audió- vagy videóchat-programok). Tehát amíg küzdünk (reálisan küzdenénk) a személyes adatok védelméért, addig most hatalmas magyar adatmennyiség (személyes adatok, tananyagok stb.) landoltak egyesült államokbeli szervereken.

A személyes adatok védelme kapcsán vessünk egy pillantást a közelmúltra. Az Edward Snowden által leleplezett egyesült államokbeli adatkezelési gyakorlat miatt Max Schrems osztrák ügyvéd 2013-ban megtámadta az addig az Európai Unió és az Egyesült Államok között élő adatvédelmi megállapodást, az ún. Safe Harbourt, majd az Európai Bíróság megsemmisítette az USA és az Európai Unió között az adatvédelmet biztosító Safe Harbour keretrendszerét (C-362/14. számú ítélettel). A Safe Harbour keretrendszert követte az EU–USA közötti *Adatvédelmi Pajzs* (Privacy Shield) 2016-tól.[10] Remélhetjük, hogy a magyar felhasználók adatai védettek maradnak.

A külföldi szerverekre feltöltött, a levelezési rendszerben továbbított adatokból betekintés nyerhető a mai magyar oktatási rendszer állapotára, a tananyagokról, a számonkérés módjára. Ez „kényelmes" OSINT feladat a téma iránt érdeklődők számára.

A karantén idején, nagyszámú szolgáltatást igénybe vevő belépésével a célzott hacker- és zsarolóvírus-támadások a megnövekedtek felkészületlen felhasználók ellen: személyes adataik megszerzése, zsarolóvírus eljuttatása, illetőleg a kutatóintézetek szerverei ellen a COVID–19 vírus kutatásainak, az ellenszer kidolgozásában tett lépések, eredmények jogellenes kifürkészése céljából.

Milyen támadások érhettek, érhetik a felhasználót?

Wardriving

A jelenség nem olyan félelmetes, amint az az angol elnevezésből következnék. Ez a bulvárízű, kicsit fellengzős elnevezés a számítástechnika területén jellemző tünet, talán ez az oka, hogy ez egy átlagos magyar felhasználó számára ezek a jelenségek úgy tűnnek, mint ami csupán a távoli „Amerikában" történhet meg. A wardriving lényege, talán elnevezése is lehetne: védett Wi-Fi-jel „lopás".

A visszaélés nem képzelhető el vezeték nélküli adatátvitel technológiája nélkül. Az 1991-ben megalkotott vezeték nélküli kapcsolat több technológiát is felölel: az infravörös adatátvitelt, a vezeték nélküli hálózatot, például a WiFi-t (Wireless Fidelityt). Mindegyik technológiában közös az, hogy az adatátvitel rádiófrekvenciás hullámokon keresztül zajlik.

A mobilinternet használata azon alapszik, hogy egy hordozható eszköz kapcsolódik a vezeték nélküli hálózathoz.

A Wi-Fi hálózatot felhasználónév/jelszó biztosítja a felhasználónak az exkluzív használatot. A szolgáltatás ingyen vagy fizetés ellenében vehető igénybe. Általában havi díjban foglalt adatforgalomra lehet előfizetni,

[9] Magyar Közlöny 2020. évi 163. szám, 4641. o. https://magyarkozlony.hu/dokumentumok/6f3b8e942b9948a826c0e152c9d4652ae7c83a04/megtekintes [Letöltés ideje: 2020.07.11.]

[10] W Kuan Hon: Data Localization Laws and Policy. Edgar Elgar Publ. Ltdf., London. 2017. 162–187. o.

az ezenfelül a letöltött adatmennyiséghez igazodóan kell további pénzösszeget fizetni. Amennyiben a felhasználó felkészületlensége vagy gondatlansága miatt nem védi előfizetéses hálózatát azonosítókkal vagy a védelmi funkciót kikapcsolja vagy egyszerű, könnyen kiismerhető jelszót használ vagy azonosítóit megosztja másokkal, akkor előfordulhat a jogosulatlanul kapcsolódó felhasználó a szerződéses adatmennyiséget eléri vagy annál több adatmennyiséget tölt le vagy fel, amiért viszont az előfizetőnek fizetni kell.[11] Ez a többletköltség jelenti a büntetőjogi értelemben vett kárt. Ezzel több, mint a hacking Btk.-beli tilalma [Btk. 423. § (1) bekezdése].

Persze, az is felvet etikai kérdést, hogy egy exkluzív szolgáltatást egy másik felhasználó miért vesz jogosulatlanul igénybe, bár cselekményének – a fentieken kívül – jogi relevanciája nincs.

Az internet szabad elérhetőségének bővülésével a wardriving, amilyen gyorsan felszínre került, olyan gyorsan el is tűnik, átlép felette a technológia fejlődése.

A szolgáltatás publikus hálózaton (közterekben, középületekben stb.) szabadon, publikus-zárt hálózaton (pl. szállodában, vendéglátóhelyeken stb.) jelszóval, míg magánhálózaton felhasználónév/jelszó megadásával vehető igénybe. A hacking sajátos megvalósulása a wardriving, amikor is az elkövető jogellenesen használja a más által előfizetett (publikus-zárt, illetve magánhálózatot) és használt wifi-hálózatot.

Phishing (adathalászat)

Az *adathalász* technikák rendkívül szofisztikáltak,[12] ahogy az ún. social engineering[13] legkülönfélébb imposztori formái is színesítik adathalászat változatosságát.

Az ún. phishing már nagyobb vagyoni kár okozására teremt lehetőséget. Első lépésben jellemzően pénzintézetek, más szolgáltatók honlapjait „lemásolják" – weboldalszerkesztő, karakterfelismerő stb. programokkal. E-mailekben keresik meg ezen bankok, vállalkozások ügyfeleit. Az ügyfelek e-mail-címeit a legkülönfélébb adatbázisokból szerzik meg legálisan vagy illegálisan. Rögtön felmerül a kérdés, hogy banki ügyfelek adatai hogyan kerülnek az adathalászokhoz? Csalárd szándékú mobilhívások révén vagy netán „házon belülről"?[14]

A következő lépésben az ügyfelektől e-mailben, mint az internetszolgáltatójuk, számlavezető bankjuk, vagy más vállalkozás, számlaszámukat, kódjaikat, személyi adatait stb. általában ezek ellenőrzésének színlelésével, azaz csalárd szándékkal kérnek információkat. Pl. az intézmény szerverének szervizelése miatt megkérik az ügyfelet, hogy lépjenek be a bank, más vállalkozás rendszerébe és ellenőrizzék adataikat, számláikat stb.

Az e-mailben szereplő linkre klikkelve a felhasználók bankjuk, szolgáltatójuk weboldalához kísértetiesen hasonlító, de hamis weboldalra lépnek be, ahol az ügyfél felhasználónevét, jelszavát vagy más azonosítóját kérik. A gyanútlan ügyfél, ha ezeket begépeli, kap egy hibaüzenetet, amely szerint a rendszer nem érhető el, például karbantartása még folyik és térjen vissza később. Ám az előzőleg begépelt azonosítókkal az adathalászok már hozzáférnek az ügyfelek számláihoz, más adataihoz.

Az adathalászat másik módszere az ún. VoIP-csalás (más elnevezéssel vishing-csalás), azaz telefonos csalás. Az elkövetők ebben az esetben az ügyfél telefonszámát tárcsázzák (pl. mert letiltották bank-, illetve hitelkártyáját), és arra kérik az ügyfelet, hogy hívjon fel egy adott számot, amelyen pl. ellenőrzés céljából akadja meg nevét, kártyaszámát, vagy reaktiválja a „letiltott" bank- vagy hitelkártyáját stb.

További módszer az ún. sms-csalás (más elnevezéssel: smishing-csalás), amely során az adatkérés sms-ben történik és sms-ben kérnek válaszokat az elkövetők. Az adathalász technikák rendkívül szofisztikáltak,[15] ahogy az ún. social engineering[16] legkülönfélébb imposztori formái is színesítik adathalászat változatosságát.

Az adathalászattal történt károkozásra legyen figyelmeztető az a brazíliai eset, amelyben 240 millió realt (kb. 45 millió dollárt) szerzett banki ügyletek révén 53 elkövető.[17]

A magyarországi kereskedelmi bankok által kiadott figyelmeztetésekből tudjuk, hogy sajnos magyarországi felhasználók is elszenvedői az adathalászatnak és az ebből eredő károknak.

Az e-bankba, a közösségi oldalakra és más weboldalakra történő nemrég bevezetett kétlépcsős azonosítás, vagy más szóval kéttényezős hitelesítés (2FA, azaz Two Factor Authentication) is jelzi azt, hogy az adathalászat sajnos, létező veszély.

Minden ügyfélnek tudnia kell azt, hogy a magyar pénzintézetek e-mailben, sms-ben, vezetékes vagy mo-

[11] Blutmann László – Karsai Krisztina – Katona Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle, 2008/1. I. évf. 1. szám 42–49. l.

[12] Tipikusak egy kiválasztott célcsoporttal szembeni adathalász támadások (spear phishing – szigonyozás), a felsővezetőket célba vevő támadás (executive whaling – bálnavádaszat) a hamis címről függelmi viszonyt színlelő CEO e-mailek.

[13] Mitnick, Kevin – Simon, William: *A megtévesztés művészete*. Budapest, Perfect. 2002. 3–338. o. Mitnick az 1990-es évek legendás hackere, háromszor ítélték el. Három könyve jelent meg magyarul, melyek valóban autentikus források a számítógépes világ infernójáról. Láthattunk váratlanul szerelőként megjelent elkövetőt, ajándékot hozót, udvarlót, házasságot ígérő elkövetőt stb.

[14] Az ún. Tyupkin-malwaret, amely „végteleníti" a pénzkiadást az ATM-ből, szintén „házon belülről" kell offline feltölteni, majd azonnal használni a bankkártyát és tartani a zsákot.

[15] Tipikusak egy kiválasztott célcsoporttal szembeni adathalász támadások (spear phishing – szigonyozás), a felsővezetőket célba vevő támadás (executive whaling – bálnavádaszat) a hamis címről függelmi viszonyt színlelő CEO e-mailek. A célzott adathalász-támadások reálisak.

[16] Mitnick, Kevin – Simon, William: *A megtévesztés művészete*. Budapest, Perfect. 2002. 3–338. o. Mitnick az 1990-es évek legendás hackere, háromszor ítélték el. Három könyve jelent meg magyarul, melyek valóban autentikus források a számítógépes világ infernójáról. Láthattunk váratlanul szerelőként megjelent elkövetőt, ajándékot hozót, udvarlót, házasságot ígérő elkövetőt stb. Ez utóbbi megtévesztések természetesen karantén idején életszerűtlenek.

[17] http://software.silicon.com/malware/0,3800003100,39125173,00.htm [Letöltés ideje: 2020.06.25-én]

biltelefonon soha nem kérnek személyes adatot, más azonosítót. Ha probléma keletkezik, akkor levélben, esetleg rövid úton kérik az ügyfelet, hogy fáradjon be a pénzintézetbe, ahol orvosolják a felmerült problémát.

Ha adathalászattal nem sikerül a felhasználó számítógépét elérni, akkor az elkövetők a hacking révén, „elektronikus betöréssel" kísérletezhetnek, kísérleteznek. A *hacker* a számítástechnikai rendszerbe történt jogellenes belépését követően a számítógép működését malware-ekkel,[18] adat- vagy programmanipulációval akadályozhatja, ezzel anyagi kárt okozhat, továbbá a számítógépen tárolt könyvtárakat, fájlokat lemásolhatja, titkot sérthet, webtartalmat felülírhat.

Az aktív védelemmel ellátott számítástechnikai rendszerbe történő jogellenes belépés büntetni rendelt cselekmény a magyar jogban [Btk. 423. § (1) bekezdése].

A *zsarolóvírusok* (WannaCry, Petya, NotPetya, Jaff, CryptoLocker stb.) napjaink legveszélyesebb visszaélései,[19] irányulhatnak főként a kisvállalati szféra ellen, továbbá a védekezéssel keveset törődő, felkészültlen felhasználók ellen is. A zsarolás bár többféle módon történik, de célja minden esetben jogosulatlan anyagi ellenszolgáltatás.[20] A zsarolás tradicionális tényállása alapján büntetendő (Btk. 367. §).

A felhasználók naivságát használják ki a *clickjacking*-támadók (kattintásos csalók).[21] Különlegesnek szánt videó-, más tartalomelérhetőségét kínálják, ám az odakattintó felhasználót meglepetés éri, mivel a felkínált tartalom nem elérhető, azt törölték stb. Ugyanakkor a felhasználó részletes profilja, posztolásai az elkövetők birtokába került. Jelenleg a kattintásos csalás akkor büntetendő, ha vagyoni kár keletkezik (Btk. 375. §).

A bűnözés elterjedtségének okai a könnyelmű, felkészületlen, *felelőtlen felhasználók* is. A könnyelműség kétszintű, egyfelől lehetővé teszik a visszaélések elkövetését, másfelől maga válik sértetté. Bármekkora is a sértetti önhiba, a cselekmény jogellenessége elvitathatatlan, és büntetőjog szempontjából is fontos értékelni.

Az elkövetők azt a lehetőséget használják ki, hogy a felhasználók ismeretei, tudása, felkészültsége, elmarad az elkövetők tudásához képest.

Fel kell hívni a figyelmet arra is, hogy a felhasználók könnyelmű közlései (jellemzően a közösségi oldalakon vagyoni helyzetükről, tartózkodási helyükről, gyűjtőszenvedélyükről, hobbijukról, szexis szelfifotóik) a bűnözők számára „hívó szó" lehet.[22]

Napjaink pedofil bűncselekményei is arra hívják fel a figyelmet, hogy közösségi oldalakon ne osszunk meg kicsi gyermekeinkről képeket hiányos öltözetben, fürdőruhában.

A pedofilok ezeket a képeket is gyűjtik, megszerzik [Btk. 204. § (1) bekezdés a) pont], sőt hálózatba tömörülve ezeket a képeket meg is osztják, hozzáférhetővé teszik [Btk. 204. § (1) bekezdés b) pont] a hálózatot alkotó felhasználókkal, ezáltal óriási „választékot" nyújtva e képekről.

Valós problémát jelent az, hogy a felhasználók sokszor nem is érzékelik, hogy sérelemükre bűncselekményt követtek el. A fájlok, könyvtárak, helyükön vannak, ám a fájlok, könyvtárak tartalmát az elkövetők „ellopták" (le-, illetve kimásolták). Majd e szöveges, fénykép, audió-, videótartalmakat (pl. manipulálva vagy anélkül zsarolási illetőleg lejáratási célzattal) felhasználják a sértettel szemben. Megjeleníthetik közösségi oldalakon vagy másutt az interneten, ami a sértett számára kedvezőtlen, kínos következményekkel járhat. Ezzel szemben valós térben a sértett általában közvetlenül és azonnal érzékeli az ellene indított támadást, mert testi sérülést szenvedett, a dolgát megrongálták, ellopták az őt ért támadással.

Továbbmenve a felhasználó azt látja, hogy számítógépe működik, minden funkcióját ellátja, tud böngészni, e-mailt írni, rádiót hallgatni stb. De nem kizárt, hogy a felhasználó számítógépe már „zombi-gép", része egy robot networknek, egy másik személy (a botnet gazdagép felhasználója) átvette az uralmát a sértett számítógépe felett, számítógépe, mobiltelefonja már másnak „bányászik" bitcoint vagy más virtuális valutát. Az „átlag" felhasználó, már ha érzékeli, számítógépe lassabb, nehezebben tölti be a kívánt web-oldalt, meg-megszakad az internetes rádió, televízió adása stb. valószínűleg nem is gyanakszik arra, hogy a számítógépe egy terheléses támadásban vesz részt, és éppen egy célzott szerver működésképtelenné tételében használják azt, mint eszközt.

A virtuális térben a sértetté válást el kell kerülnünk. Számítógépeink védelméről ugyanúgy kell gondoskodnunk, mint bármely más vagyontárgyunk védelméről.

Meg kell tanulnunk azokat a fontos védelmi megoldásokat (tűzfal, vírus-, kémszoftverirtó, jelszóváltoztatások, a mobileszközök fizikai védelme stb.), amelyek segítenek abban, hogy ne váljunk sértetté és nyugodtan száguldjunk az információs sztrádán, hiszen ez a jelen, még inkább a jövő!

[18] https://docplayer.hu/25373281-Muha-lajos-informatikai-biztonsag.html [Letöltés ideje: 2020.06.25.]

[19] Mezei Kitti – Nagy Zoltán: A zsarolóvírus és a botnet, mint napjaink két legveszélyesebb számítógépes vírusa. Szent Lászlótól a modernkori rendészettudományig. [In: Gaál, Gyula – Hautzinger Zoltán (szerk.) Pécsi Határőr Tudományos Közlemények XIX. kötet.] Pécs, 2017. 155–163. o.

[20] A zsarolóvírusok egyik formája az, amely esetében egy letöltött vírus a felhasználó fájljai, könyvtárai elérését lehetetlenné teszi azzal, hogy azokat letitkosítja és a feloldásért cserébe – tipikusan – valamilyen kriptovalutát követel a zsaroló. A kifizetést követően vagy megérkezik a feloldó kód (patch stb.) vagy nem és folytatódik a zsarolás. A police malware lényege az, hogy hatóságok nevében küldött levelek ezek, amelyek „megzsarolják" a felhasználót, egy olyan indokolással „a felhasználó tiltott tartalmat töltött le vagy szélsőséges csoportokkal tartott kapcsolatot, és ha fizet, akkor nem indul büntetőeljárás". Zsarolás végrehajtható terheléses támadással történő fenyegetéssel is.

[21] Közösségi oldalon egy-egy látványos videó megjelenítéséért a videóra kattintást kérik, aztán egy üzenet „pl. a videó nem megjeleníthető" „a videót törölték, eltávolították" stb.

[22] Dr. Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és a ellenük való küzdelem. Büntetőjogi Szemle, 2020/1. 94–97. o. https://ujbtk.hu/wp-content/uploads/lapszam/BJSZ_202001.pdf [Letöltés ideje: 2020.07.11.]