ELKH | Eötvös Loránd Kutatási Hálózat
MESTERSÉGES INTELLIGENCIA Nemzeti Laboratórium
tkmilab

MTA Law Working Papers
2021/21

A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról

Grund Borbála

ISSN 2064-4515
http://jog.tk.mta.hu/mta-lwp
Társadalomtudományi Kutatóközpont – MTA Kiválósági Kutatóhely Eötvös Loránd Kutatási Hálózat
Centre for Social Sciences – MTA Centre of Excellence Eötvös Loránd Research Network

Grund Borbála*

A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról

I. RÉSZ – A KIBERBŰNCSELEKMÉNYEKRŐL ÁLTALÁNOSSÁGBAN

I.1. BEVEZETÉS

A digitális forradalom, azaz a digitális technológia elterjedése és az adatfeldolgozó eszközök gyors ütemű fejlődése kétségkívül végérvényesen megváltoztatta életmódunkat. Azok, akik az 1980-as évek végén vagy később születtek, életük kezdetétől fogva a digitális korban élnek. E generációnak bizonyosan, és a korábbiak nagyobb részének is megszokott a virtuális térben dolgozni, szociális életet élni, ügyeket intézni vagy szórakozni. Természetes igény az egyének, szervezetek, vállalatok, intézmények és más entitások részéről, hogy a fizikai tér mellett a virtuális térben is biztonságos környezetben tevékenykedhessenek. Ahogy nő és egyre inkább diverzzé válik az online végezhető tevékenységek köre, úgy lesz egyre nagyobb jelentősége az ilyen cselekmények védelmére hivatott biztonsági intézkedéseknek.

A digitalizáció elterjedésének, az információs társadalom kialakulásának mellékhatása a részben vagy egészen online térben folyó bűnözés.[1] Jelen írás alapvető célja az, hogy bemutassa, miért nem szerencsés figyelmen kívül hagyni a kiberbűnözés fenyegetéseit sem az egyén, sem az intézmények szintjén. A kibertér biztonságának kulcsszava az 'együttműködés': büntető igazságszolgáltatási, bűnüldözési és más szervek sorának lokális, illetve globális kooperációja, – kriminológusok, informatikai- és kiberbiztonsági szakértők közreműködésével folyó – interdiszciplináris kutatás és tudományos diskurzus, a privát szektor és az állami szereplők közös erőfeszítései mind szükségesek a kiberbűnözés jelentette probléma komplexitásának megértéséhez és kihívásai megoldásához.

A kibertérben vagy virtuális térben a számítógépes eszközök immár világméretű információcsere-hálózattá kapcsolódnak össze. A 'számítógép' és a különböző egyenértékű eszközök jónéhány éve túlmutatnak hagyományos szerepükön, immár nem csupán olyan különleges apparátusok, amelyek a megfelelő tudással rendelkező szakértők kezében matematikai és statisztikai műveletek elvégzésére szolgálnak.[2] A kibertérre mintegy a valós világunk megkettőződéseként[3] gondolunk, elemei a valós téren alapulnak, a valós tér által jönnek létre,[4] egyszersmind különböznek attól. A valós és virtuális terek kombinációjaként[5]

---

* A szerző az ELTE-ÁJK Büntetőjogi Tanszékének doktorandusza, témavezetője: Dr. Ambrus István egyetemi docens. A dolgozat 2021-ben az Országos Bírósági Hivatal Elnöke által Mailáth György országbíró emlékére kiírt tudományos pályázat büntetőjogi szekciójában II. díjat ért el.

A publikáció a 138965. számú NKFIH pályázat és a Mesterséges Intelligencia Nemzeti Laboratórium keretében készült, az Innovációs és Technológiai Minisztérium, valamint a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatásával.

[1] Zavrsnik, Ales: Cybercrime Definitional Challenges and Criminological Paricularities. In: Masaryk University Journal of Law and Technology, 2008/2.sz., 2.o.

[2] Ződi Zsolt: Platformok, robotok és a jog. Új szabályozási kihívások az információs társadalomban, Budapest, 2018, Gondolat Kiadó, 30.o.

[3] Ződi, 2018, 31.o.

[4] Yar, Majid: The Novelty of 'Cybercrime'. Assessment in Light of Routine Activity Theory. In: European Journal of Criminology, 2006/2.sz., 415.o.

[5] Holt, Thomas J. – Bossler, Adam M.: Cybercrime in Progress. Theory and prevention of technology-enabled offenses, 2016, Routledge, 7.o.

az online környezet többszörösen összekapcsolódó olyan elemekből áll, amelyek magukban őrzik a hagyományos interakció csomópontjait, de a szimultán és többszörös kapcsolódás[6] miatt bővített és összetettebb formában. A kibertérre a fizikai tér devianciáihoz hasonló, de azoktól mégis különböző, komplex cselekmények jellemzőek, amelyek szabályozása korántsem egységes a világ jogrendszereiben. A szabályozás széttagoltságához alapvetően az vezetett, hogy a kibertér bűncselekményei csupán a közelmúltban kezdtek hatni arra a büntetőjogi rendszerre, amelyet a digitális kort megelőzően kizárólag a fizikai, valós térben megvalósuló bűnelkövetés formált.[7]
A dolgozat első részében a kiberbűnözés világában fellelhető kifejezések és a jelenség tartalmának meghatározásával kapcsolatos fogalmi áttekintés után a kiberbűnözés világára leginkább jellemző vonások bemutatása következik. Az elnevezések, meghatározások, csoportosítások összefoglalása, valamint a kiberbűnözés jellegzetességeinek felvázolása után a kibertér szereplőivel: a bűnelkövetőkkel, a célpontokkal és a felügyeleti szerepet betöltő személyekkel foglalkozom. A dolgozat második része az első részben bemutatott fogalmakra épül és két további részre tagolódik. Elsőként a hálózat-bűncselekmények[8] vagy „tiszta" kiberbűncselekmények; majd egyes olyan bűncselekmények elemzése következik, amelyek tényállásukat tekintve „vegyesek", tehát végbe mehetnek akár a fizikai, akár a kibertérben. Az elemzés részeként megjelennek egyes olyan hazai bírósági döntések, amelyek rávilágítanak a digitális forradalom néhány aktuális gyakorlati problémájára.

I.1.1. Terminológiai kérdések

A szakirodalomban és a témával foglalkozó laikus forrásokban jónéhány kifejezés[9] jelen van az olyan bűncselekmények megjelölésére, amelyek valamilyen mértékben az online térben játszódnak le. Az online vagy virtuális szociális térben a „hagyományos" formáktól valamelyest eltérő kriminális viselkedésmódok jelennek meg, ezért nő a megfelelő büntetőjogi – kriminológiai terminológia kialakítására[10] való igény.
Az új terminológia egyik első képviselője a 'számítógépes bűnözés' volt, amelyet később felváltott a 'számítógép segítségével megvalósuló bűnözés' kifejezés. Utóbbi kétféle értelmezésre ad lehetőséget: az egyik értelmezés szerint a számítógép a támadás eszköze vagy tárgya; de e kifejezésből következtethetünk arra is, hogy a bűncselekmény elkövetése az elkövető számítástechnikai szakismeretének eredménye.[11] A második értelmezés alapján feltehető, hogy a számítástechnikai szakismeret alapvető elem a hasonló bűncselekmények elkövetésében, így a 'számítástechnikai bűnözés' megjelölés is indokolható. Egyes szerzők szerint[12] a 'számítógépes bűnözés' a számítógépes technológiákkal kapcsolatos tudás felhasználásával valósul meg, míg a kiberbűnözést a kibertérben való biztos mozgás, a kibertér viszonyainak ismerete segíti elő. Az 'információs bűnözés', 'digitális bűnözés' vagy a 'high-tech bűnözés' jelölte halmazoknak ugyan része a kiberbűnözés, de ezen kategóriák felölelnek más cselekményeket is, emiatt jelen íráshoz nem megfelelőek. Nem speciális jogi, hanem általános társadalomtudományi fogalmak az 'internetes bűnözés', 'technológiai alapú

[6] McGuire, Michael: Hypercrime: the new geometry of harm, 2007, Routledge – Cavendish, 7.o.
[7] Brenner, Susan W. – Clarke, Leo L.: Distributed security: preventing cybercrime. In: John Marshall Journal of Computer and Information Law, 2005/4.sz., 666.o.
[8] Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia, Budapest, 2018, Wolters Kluwer, 497.o.
[9] A kifejezések magyarra fordítása a vonatkozó magyar nyelvű szakirodalom figyelembevételével történt.
[10] Majid, 2006, 408.o.
[11] Zavrsnik, 2008, 9.o.
[12] Holt – Bossler, 2016, 17.o.

bűnözés', 'e-bűnözés' vagy 'virtuális bűnözés'.[13] A dolgozatban az egyértelműség érdekében az „online bűncselekmények" mellett a 'kiberbűnözés', illetve 'kiberbűncselekmény' kifejezéseket használom.

I.1.2. A kiberbűnözés egységes fogalma meghatározásának problémája

A kiberbűnözés egységes fogalma a mai napig nem létezik. Egy egységesen használt fogalom létezése elősegítené a témával kapcsolatos diskurzus fenntartását, a problémák feltérképezését és megoldásuk kidolgozását.[14] Az alapvető elemeket tekintve a kiberbűnözés

(a) a bűncselekmények széles skáláját foglalja magában,
(b) amelyeket az infokommunikációs technológiák (ICT[15]) segítségével,[16]
(c) globális elektronikus hálózatokon át[17] követnek el.

A technológia kulcsfontosságú elem a cselekmények elkövetésében, e nélkül nem beszélhetünk kiberbűnözésről.[18] Ahogy az internet és más számítógépes hálózatok használata exponenciálisan nőtt az utóbbi évek során, úgy bővült a törvénytelen online tevékenységek folytatásának lehetősége is.[19] Mindezt egyesek szerint a konvergencia[20] okozza, az a folyamat, amelyben a kommunikáció és az informatika elkülönülő időpontokban felfedezett újdonságai egységes technológiává állnak össze. Ezen, a fejlett világban élők számára egyértelműen érzékelhető folyamat következtében folyamatosan változik, differenciálódik maga a kiberbűnözés, újra és újra elmosódnak a megszilárduló fogalmi határok.

A növekvő médiafigyelem miatt a kiberbűnözés előtérbe került a nyilvánosság körében. A felhasználók nagy részének egyértelmű, hogy a számítógépes hálózatokon a legális tevékenységek mellett folynak illegális, jogsértő cselekmények is. Mindazonáltal abban közel sincs konszenzus a laikus közönség, illetve az akadémiai élet képviselői között, hogy pontosan melyek ezek a jogsértő tevékenységek, és mekkora kockázatot hordoznak magukban.

A kriminális cselekmények fajait és számát illető zavar egyrészt abból ered, hogy hiányzik egy egységes kiberbűncselekmény-fogalom a hozzá kapcsolódó mérőszámmal, mérési módszerrel.[21] A statisztikai módszerek és mérőszámok egységesítése megkönnyítené a probléma valós kiterjedésének megértését[22] mind a jogalkotó, mind az üzleti érdekeltségű

[13] A 'virtuális bűnözés' kifejezés némely szerzőnél a valós fizikai világ mintájára létrehozott virtuális világokban előforduló jogsértéseket jelöli. E virtuális világok – mint például Cyberworld, Second Life, vagy Ebay – varázsa az arra fogékonyakra abban rejlik, hogy a 'közösség' kifejezés használatával egyfajta közös felelősségérzetet keltenek a felhasználókban, akik így a virtuális térben falvaiban és városaiban építenek szociális kapcsolatokat, a valós fizikai világban egymástól távoli pontokon élik meg a közösséghez tartozás élményét (Wall, David S. – Williams, Matthew: Policing diversity in the digital age: Maintaining order in virtual communities. In: Criminology & Criminal Justice, 2007/4. sz., 391.o.). A dolgozatban az ilyen környezetekben megvalósuló bűncselekményekre nem térek ki, a 'virtuális' kifejezést e tárgykörtől elvonatkoztatva, általános jelleggel használom.

[14] Clough, Jonathan: Cybercrime. In: Commonwealth Law Bulletin, 2011/37.sz., 671. o.

[15] Az 'ICT' az információs és kommunikációs technológia angol nyelvű rövidítése, jelentése a számítógépek és egyéb elektronikus eszközök és rendszerek használata elektronikus adatok gyűjtésére, tárolására, felhasználására és továbbítására. (Cambridge Dictionary) A továbbiakban az információs és kommunikációs technológia kifejezésből képzett 'IKT' rövidítéssel jelölöm.

[16] Buono, Lavriero: Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. In: ERA Forum, 2016/17.sz., 343.o.

[17] Majid, 2006, 409.o.

[18] Clough, 2011, 671.o.

[19] Lavriero, 2016, 343.o.

[20] Clough, Jonathan: The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World. In: Criminal Law Forum, 2012/23.sz., 364.o.

[21] Lavriero, 2016, 349.o.

[22] Clough, 2011, 374.o.

szereplők, illetve a laikus felhasználók számára. Másrészt a perspektíva torzulhat amiatt is, hogy diszkrepancia áll fenn a nyomozó szervek és az ipari szereplők statisztikái között: [23] az internetszolgáltatók, a szoftvergyártók, a banki és biztosítási szektor résztvevői statisztikáikban a valósnál jóval nagyobb számban szerepeltetik az e körben releváns kiberbűncselekményeket. A közös fogalom hiánya miatt nem ritka, hogy a jogsértő cselekmények ugyan szerepeltetve vannak a statisztikában, de nem önálló tényállás alá rendezve, hanem valamely, az adott jogrendszerben hagyományosnak számító bűncselekményi kategóriába épülve.[24]

A kiberbűnözés mibenléte körüli bizonytalanság következménye a publikum tájékozottsági fokában megnyilvánuló ún. 'reassurance gap'.[25] Ez azt jelenti, hogy a közvélemény bűnözéstől való félelme nem követi a bűnözési ráta növekedését, hanem attól eltérően változik. E paradox helyzetet, amely szorosan összefügg a fentebb említett túlzó szolgáltatói statisztikákkal, jól érzékelteti a következő példa. Egy 2010-es évek elején készült felmérés[26] szerint az emberek az információs forradalmat követően jobban tartanak attól, hogy mobiltelefonjukhoz vagy számítógépükhöz mások jogosulatlanul hozzáférést szereznek, mint bármilyen más típusú bűncselekménytől. A kriminológusok egy része szerint az emberek félelmét az egyes iparági szereplők provokálják,[27] könnyen megérthető, hogy miért fontos például a biztonságtechnikai szoftverek gyártóinak folyamatosan napirenden tartani a kiberbiztonság témáját. A kibertér tehát a felhasználók szemében a kezdetben új lehetőségek és addig sosem látott szabadság terepéből veszélyes hellyé vált.[28]

I.1.3. Csoportosítás

Korábban szó volt arról, hogy a kibertér vonatkozásában jellemzően nincsenek stabil, kirajzolódott kategóriák, amelyek eligazítást nyújtanának a laikus, illetve a professzionális szereplők számára; a megszilárdult klasszifikációk pedig nem fedik le az online térben előforduló jogsértő cselekmények teljes körét. Mindezt szem előtt tartva a következőkben röviden bemutatásra kerül egy olyan csoportosítás, amely összefoglalja a kiberbűncselekmények rendkívül szerteágazó fajtáit.

Kiindulópontként meghatározhatjuk ún. „tiszta" kiberbűncselekményeket ('cyber-dependent crime' vagy 'computer-focused crime'),[29] más elnevezéssel hálózat-bűncselekményeket olyan cselekményekként, amelyek kizárólagos eszközei és egyben célpontjai számítógépek, számítógépes hálózatok, vagy információs és kommunikációs technológiák.[30]

A kiberbűncselekmények ezen meghatározása viszonylag szűk határokat szab a kiberbűnözés fogalmának. Léteznek ugyanis olyan bűncselekmények, amelyek esetében csupán az elkövetést elősegítő eszközként[31] jelenik meg a számítógép vagy különféle hálózatok, maguk a cselekmények „hagyományosak", célpontjaik nem az információs és kommunikációs

[23] Lavriero, 2016, 350.o.
[24] Lavriero, 2016, 350.o.
[25] Wall – Williams, 2007, 397.o.
[26] A felmérés a Amerikai Egyesült Államok népessége körében készült. (Maimon, David – Louderback, Eric R.: Cyber-Dependent Crimes: An Interdisciplinary Review. In: Annual Review of Criminology, 2019/2.sz., 9.o.)
[27] Zavrsnik, 2008, 4.o.
[28] Wall – Williams, 2007, 397.o.
[29] Mezei Kitti: Szervezett bűnözés az interneten. In: A bűnügyi tudományok és az informatika, 2019, Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 125.o.
[30] McGuire, Mike – Dowling, Samantha: Cyber crime: A review of the evidence. Chapter 1: Cyber-dependent crimes. In: Home Office Research Report 75, 2013, 4.o.
[31] Knoops, Bert-Jaap: The Internet and its Opportunities for Cybercrime. In: Tilburg Law School Legal Studies Research Paper Series, 2011/9.sz. 739.o.

technológia részei. Példaként szolgálhat a csalás[32], a lopás, a zaklatás, a gyermekpornográfia. A már említett hálózat-bűncselekmények, amelyek elkövetését tehát teljes mértékben a technológia fejlődése teszi lehetővé; és azon „hagyományos" bűncselekmények, amelyek elkövetése számítógép segítségével valósul meg, egy kronológiai skála két végpontját is jelölhetik. A két végpont között számos elkövetési mód található, amelyekben valamilyen szinten jelen van a technológia, de amelyek nem egyforma ütemben kerültek át a kibertérbe: ezeket nevezhetjük 'számítógép segítségével megvalósuló bűnözésnek', (összefoglaló angol kifejezéssel a 'cyber-enabled crime' vagy 'computer-assisted crime').

A hasonló, kronológiai-generációs típusú csoportosításra,[33] illetve a technológia igénybevételének mértékét alapul vevő definíciós kísérletekre vonatkozóan kritikaként jelenik meg a szakirodalomban, hogy azok az említett skála két végpontja közötti variációk nagy száma miatt nem képesek precízen meghatározni a kiberbűncselekmények elemeit.

Az online tér jogsértéseit jelölő kifejezések áttekintése, a meghatározás nehézségeinek bemutatása, illetve egyes klasszifikációk ismertetése után megkísérlem összefoglalni a kiberbűnözés definícióját. A szerzők nagyobb részének[34] álláspontjára helyezkedve[35] egy három konjunktív elemből álló definíciót használok, amely a technológia bűnelkövetésben betöltött szerepének mértékén alapul. Kiberbűncselekmények

> (1) az olyan bűncselekmények, amelyekben a számítógép vagy a számítógépes hálózat biztonságát fenyegeti a kriminális tevékenység, ezek az IKT létrejövetelével karöltve alakultak ki (szűk értelemben vett kiberbűnözés), továbbá
>
> (2) az olyan hagyományos bűncselekmények, amelyekhez a számítógépet az elkövetés eszközeként használják fel, ezek léteztek az IKT előtt is, de új életre keltek a kibertérbe való bizonyos fokú integrálódással (számítógép segítségével megvalósuló bűnözés), valamint
>
> (3) a számítógépes tartalommal kapcsolatos bűncselekmények, amelyeknél az eszköz tartalma az elkövetés bizonyítékául szolgálhat (számítógépen tárolt adatok tartalmával kapcsolatos bűnözés).

A legújabb hazai szakirodalomból pedig kiemelhető Ambrus István álláspontja, aki *szorosabb és tágabb értelemben vett digitális bűncselekmények* között tesz különbséget. Előbbi alatt azon deliktumok értendőek, amelyek kizárólag a virtuális térben, vagy elektronikus formában, illetve eszmeileg létező tárgyak és eszközök kapcsán követhetők el, mint például az információs rendszerrel, a készpénz-helyettesítő fizetési eszközökkel vagy az adatokkal kapcsolatos deliktumok. A tágabb értelmű digitális bűncselekmény pedig olyan, egyébként nem-digitalizált környezetben is elkövethető cselekményeket jelöl, amelyek napjainkra egyre inkább a digitális világban valósulnak meg. Erre példa a gyermekpornográfia, a pénzmosás, a zaklatás, illetve számos, közzététellel megvalósuló bűncselekmény.[36]

---

[32] A kibertérben megvalósuló csalások egyik legérdekesebbje az előlegfizetéssel kapcsolatos átverés ('advance fee scheme' vagy 'Nigerian' vagy '419 Fraud'). Spamek segítségével a csalók a célpontoktól díjak formájában anyagi segítséget kérnek vagyonuk külföldre csoportosításához, befektetéséhez. Az afrikai (főleg nigériai) „üzletemberek" a külföldi valuta biztosításáért cserébe felajánlják a profit bizonyos részét. A célpontok abban a hitben adják meg bankszámláik adatait, hogy a csalóknak valóban szükségük van befektetésük megvalósításához bizonyos összegekre, mígnem világossá válik számukra, hogy sem a beígért profithányadhoz, sem befizetett díjaikhoz nem jutnak többé hozzá. (Clough, Jonathan: Principles of Cybercrime, Cambridge, 2010, Cambridge University Press, 183.o.)

[33] Knoops, 2011, 739.o.

[34] Zavrsnik, 2008, 11.o.; Clough, 2011, 672.o.; Majid, 2006, 409.o., Wall – Williams, 2007, 398.o.

[35] Az, hogy a szakirodalomban legelterjedtebbnek e három elemből álló, bizonyos fokig a kiberbűncselekmények generációit kifejező felosztás nevezhető, egyértelműen utal az Európa Tanács Budapesten, 2001-ben kelt Számítástechnikai Bűnözésről szóló Egyezményének (a továbbiakban: Budapesti Egyezmény) jelentőségére. Az Budapesti Egyezmény volt az első olyan nemzetközi egyezmény, amely büntetőjogi eszközökkel szabályozta a kiberbűnözést: fogalmakat határoz meg, tartalmaz anyagi jogi rendszerezést és eljárási szabályokat is.

[36] Ambrus István: Digitalizáció és büntetőjog. Budapest, 2021, Wolters Kluwer, 290. o.

I.2. A KIBERBŰNÖZÉS JELLEGZETESSÉGEI

Az online környezet azonnali kapcsolatba lépést és interakciót tesz lehetővé egymástól bármekkora távolságra tartózkodó cselekvők között.[37] A népesség széles köre számára hozzáférhető hálózatokat (például az internetet) 'kölcsönös összekapcsoltság'[38] jellemzi: a globalizált hálózatokon az egyén képessé válik arra, hogy más felhasználókat (esetenként akár azok millióit is) egy időben érjen el. A térbeli-időbeli korlátok összeomlása[39] következtében kialakult egy olyan állandóan működő virtuális tér, amely pontjai között nulla a távolság. A globális, nemzetközi jelleg a hálózatokon folyó legális és illegális tevékenységek folytatására 'erősokszorozóként'[40] hat: ahogy bővül a digitalizáció nyitotta lehetőségeink köre, az ezáltal egyszerűbbé váló tevékenységeink száma, úgy a veszélyeinek való kiszolgáltatottság és a jogsértések száma is növekszik. Ezt tovább bonyolíthatja az automatizáció[41] lehetősége, amely szintén kétarcú: egyrészt megkönnyíti a legális célú felhasználást, de ezzel együtt az illegális tevékenységek elkövetőit is mentesíti az erőbefektetés bizonyos része alól.

A fizikai távolság hiánya nem csupán azzal a következménnyel jár, hogy az immár online térbe áthelyeződött folyamatok felgyorsulnak és hatókörük robbanásszerűen növekszik. A kapcsolattartási környezet, amelyet az online tér elemei alkotnak, kihat a felhasználók viselkedésére, „poszt-digitalizációs" szocializációjára is. Az online tér ugyanis megnyitja a teljes anonimitás lehetőségét. A büntetlenség érzését kölcsönző[42] anonimitást különböző titkosítási módszerekkel lehet elérni, az erre alkalmas eszközök a digitális bizonyítékok eltüntetésére készült szoftverekkel együtt elérhetőek az online kereskedelemben.[43] A titkosítás amellett, hogy védekezési eszközként szolgálhat a jogosulatlan hozzáférési kísérletek megakadályozása érdekében, az elkövetők beazonosításának egyik akadályát is jelentheti.[44] Az anonimitással szorosan összefügg az identitásválasztás szabadsága. A valós személyiség és szociális helyzet könnyen manipulálható a kibertérben.[45] A virtuális személyiség, ahogy az egész virtuális tér, rugalmas és képlékeny, így lehetőség nyílik megszabadulni a kulturálisan közvetített, adott esetben rákényszerítettnek érzett mintáktól. A rugalmasság megjelenik abban is, hogy a valamilyen szempontból értékkel rendelkező információk mobilizálása nagyon egyszerű feladat. A hordozóeszközök, megosztási felületek paramétereitől és az adatmennyiségtől függően az elektronikusan tárolt adatok rövid idő alatt azonos formában és minőségben helyezhetők át, gyors ütemben és végtelenül sokszorosíthatók.

Kiemelendő, hogy a digitalizáció kiegyenlítetlen, azaz nem azonos ritmusban folyik a világ egyes részein. Ennek alátámasztására szolgálnak a lentebb található ábrán megjelenített globális internethasználatról szóló adatok. 2020 első negyedévében legnagyobb mértékben az ázsiai országokban használták az internetet: az internethasználati statisztikák szerint az összes internethasználó 52,2%-a ázsiai, ez körülbelül 2,5 milliárd embert jelent.[46] Az észak-amerikai

---

[37] Majid, 2006, 410.o.
[38] Clough, 2011, 671.o.
[39] Majid, 2006, 411.o.
[40] Clough, Jonathan: Principles of cybercrime, Cambridge, 2010, Cambridge University Press, 5.o.
[41] Clough, 2011, 673.o
[42] Lavriero, 2016, 351.o.
[43] Clough, 2011, 673.o.
A felhasználók nagy része a nyilvánosan elérhető 'Surface Web' internethálózatot használja legális, mindennapi tevékenységekhez. Emellett létezik a sokkal terjedelmesebb 'Darkweb' is, amely nem érhető el szokványos módon, azehhez való kapcsolódáshoz speciális keresőmotorok szükségesek. A 'Deepweb' részét képező hálózat sokféle törvénytelen tevékenységnek ad helyet, kapcsolattartási felület, rosszindulatú vagy más illegális termékek, szolgáltatások online piactere. (Kitti, Mezei – Zoltán, Nagy: Organised Cybercrime Groups and Their Illicit Online Activities. In: Studia Iuridica Auctoritate Universitatis Pécs Publicata, 2016/154.sz., 149.o)
[44] Zavrsnik, 2008, 10.o.
[45] Majid, 2006, 411.o.
[46] Az adatok a https://internetworldstats.com/ weboldalról származnak. Utolsó letöltés dátuma: 2020.10.28.

kontinens penetrációs rátájával emelkedik ki: a földrész lakosságszáma a Föld teljes népességének alig 5%-át teszi ki, viszont ott a legmagasabb internethasználat penetrációs aránya: az emberek 90,3%-a használ internetet, nyomukban az európai felhasználókkal, akik körében ez az arány 87,2%.[47] Ellenpéldaként az afrikai földrész ugyanezen vonatkozású adata 42,2%. Az itt felsorolt számokból az látható, hogy a digitalizációra való kapacitás alakulása megfeleltethető a fennálló gazdasági hierarchia földrajzi elosztásának, amely egyesek szerint arra enged következtetni, hogy a virtuális környezethez való hozzáférés mértéke követi a társadalomban egyébként jelen lévő inkluzivitást, vagy éppen kirekesztettséget.[48]

WORLD INTERNET USAGE AND POPULATION STATISTICS
2020 Year-Q2 Estimates

World Regions	Population (2020 Est.)	Population % of World	Internet Users 30 June 2020	Penetration Rate (% Pop.)	Growth 2000-2020	Internet World %
Africa	1,340,598,447	17.2 %	566,138,772	42.2 %	12,441 %	11.7 %
Asia	4,294,516,659	55.1 %	2,525,033,874	58.8 %	2,109 %	52.2 %
Europe	834,995,197	10.7 %	727,848,547	87.2 %	592 %	15.1 %
Latin America / Caribbean	654,287,232	8.4 %	467,817,332	71.5 %	2,489 %	9.7 %
Middle East	260,991,690	3.3 %	184,856,813	70.8 %	5,527 %	3.8 %
North America	368,869,647	4.7 %	332,908,868	90.3 %	208 %	6.9 %
Oceania / Australia	42,690,838	0.5 %	28,917,600	67.7 %	279 %	0.6 %
WORLD TOTAL	7,796,949,710	100.0 %	4,833,521,806	62.0 %	1,239 %	100.0 %

1. ábra - A világ népessége és internethasználói 2020 II. negyedévében

Nem utolsó sorban a kiberbűnözés jellegzetességei közé tartozik a nagymértékű látencia is. A látencia okait vizsgálva más-más képet mutat az egyén, illetve az üzleti szereplők köre. Egyrészt, előbbieknél az őket ért jogsértések bejelentésének akadálya lehet tájékozatlanságuk, illetve tapasztalatlanságuk. A számítógépes rendszerek megtámadása nehezen észlelhető, ez kellő technikai hozzáértéssel alkalmazott szoftveres védelemmel érhető el.[49] Jellemző tehát, hogy az egyének, ha szerencsésen érzékelnek is valamilyen változást online viszonyaikban, nincsenek tisztában azzal, hogy kiberbűncselekmények áldozatává váltak.[50] A digitális nyomok feltérképezése még az erre specializálódott szakértőknek sem egyszerű feladat, az amorf és könnyen eltüntethető[51] bizonyítékok rögzítése nem várható el a mindennapi felhasználóktól. Másrészt, az egyének körében magas látenciát indokolhatja az is, hogy ugyan tisztában vannak az őket ért jogsértésekkel, a cselekményekről valamilyen okból mégsem értesítik a bűnüldözés szerveit. Különösen a zaklatás jellegű cselekményekre jellemző, hogy a sértettek nem jelentik az őket ért jogsértéseket, mivel attól tartanak, hogy a bűnüldöző szervek nem vennék komolyan a problémájukat.[52]

Az üzleti szereplőket ért jogsértések esetében könnyebben meghatározható okok vezetnek a látenciához, hiszen e szereplőknél akármilyen enyhe cselekménynél is prioritás, hogy annak megtörténte ne kerüljön nyilvánosságra,[53] így ellenérdekeltek lehetnek egy esetlegesen meginduló nyomozás során. Az üzleti világban gazdasági érdek, az állami és kormányzati szerveknél politikai tényezők diktálta igény, hogy hitelességük ne szenvedjen csorbát amiatt, hogy esetlegesen nyilvánosságra kerül egy rendszerüket ért kibertámadás. A gazdasági

[47] Az adatok a https://internetworldstats.com/ weboldalról származnak. Utolsó letöltés dátuma: 2020.10.28.
[48] Majid, 2006, 415.o.
[49] Zavrsnik, 2008, 12.o.
[50] McGuire – Dowling, 2013, 12.o.
[51] Brenner, Susan W.: Cybercrime and The Law. Challenges, Issues and Outcomes, 2012, Lebanon, Northeastern University Press, 118.o.
[52] Holt – Bossler, 2016, 15.o.
[53] McGuire – Dowling, 2013, 12.o.

szereplők jó hírnevének megőrzéséhez financiális okok fűződnek: egy-egy támadás után az adatok, illetve a rendszer helyreállításának költségein túl az adott entitás szembesülhet az előbbi sokszorosát jelentő olyan költségekkel, amelyeket a fogyasztói bizalom elvesztése okoz. A másodlagos viktimizáció tehát súlyosabb következményekkel járhat, mint az informatikai rendszerbe történő (akár egyetlen) jogosulatlan behatolás.[54]
A magas látenciához az is hozzájárul, hogy a rendőri szervek nem feltétlenül rendelkeznek kellő szakértelemmel és erőforrással[55] ahhoz, hogy észleljék és nyomozzák e cselekményeket. E szervek a világ minden pontján elkerülhetetlenül szembesülnek azzal, hogy az online tér illegális tevékenységei tevékenységek a digitális kor kezdetéig jellemzően lokális kezelést igénylő bűnözéssel ellentétben globálisan folynak. A felhasználók hatalmas köre és a modern kommunikáció hálózati jellege miatt az online tér felderítése radikálisan új módszereket igényel. Ezzel kapcsolatban fontos kiemelni, hogy az online tér ellenőrzésének feladatát nem célszerű kizárólag a bűnüldöző szervekre hagyni, szükséges, hogy a társadalom széles köre hozzájáruljon a minél nagyobb fokú kiberbiztonság eléréséhez.

I.3. A KIBERTÉR SZEREPLŐI

Egyes szerzők szerint a kibertér szereplőinek beazonosításához használhatjuk az élő szervezetek és jellegzetes környezetük alkotta 'ökoszisztéma' fogalmát. E fogalom az emberi társadalmakra vetítve azt kifejezi ki, hogy a populációk szociális szerveződés és technológia útján fejlődnek és alkalmazkodnak környezetükhöz, létrehozva egy olyan egyedi ökoszisztémát, amelyben minden egyes szereplő cselekvése befolyásolja más szereplők magatartását.[56] Ennek alapján a következőkben a kibertér ökoszisztémájában jelenlévő szereplők négy nagy csoportját tekintem át.

I.3.1. BŰNELKÖVETŐK

A kiberbűnözés fogalmi határainak tárgyalása során a 'számítástechnikai bűnözés' kifejezésnél említésre került a technológiai szaktudás kiberbűncselekmények elkövetésében betöltött szerepe. Az 1970-es években a 'számítógépes bűnözés' a számítógépek és az azokon tárolt adatokkal való visszaélést jelentette, amelyet főként az adatokhoz hozzáféréssel rendelkező alkalmazottak követtek el.[57] Hagyományosan a kiberbűnözők világa olyanokból állt, akik szaktudással rendelkeztek a számítógépes nyelvezetek, programozástudomány vagy hálózati architektúra terén, és képesek voltak technikailag összetett bűncselekmények elkövetésére.[58] Azáltal, hogy az ún. C2C ('criminal to criminal') csatornákon[59] bárki bárkivel kapcsolatba tud lépni, megjelentek a nem professzionális kiberbűnözők, vagyis azok, akik csekély technikai tudással és szakértelemmel rendelkeznek.[60] Ez a csoport egyrészt azért tudott létrejönni, mert ahogy a számítógépes rendszerek egyre stabilabb részét képezik a személyes és üzleti életünknek,[61] úgy nő azok köre, akik képesek megérteni a kibertér alapvető jelentőségét és az általa kínált (potenciálisan jogsértő) lehetőségeket. Másrészt a nem professzionális elkövetői csoport kialakulását nagyban elősegítette az, hogy létrejött egyfajta

[54] Zavrsnik, 2008, 13.o.
[55] Clough, 2011, 674.o
[56] Maimon – Louderback, 2019, 3.o.
[57] Holt – Bossler, 2016, 17.o.
[58] Yang – Hoffstadt, 2006, 205.o.
[59] Mezei – Nagy, 2016, 149.o.
[60] Mezei – Nagy, 2016, 145.o.
[61] Yang – Hoffstadt, 2006, 205.o.

szolgáltatóipar, amely a rosszindulatú szoftvereknek kereskedelmére fókuszál.[62] Ez azt jelenti, hogy a nagyobb szaktudással rendelkező elkövetők technikai tudásukat felhasználva mások számára könnyen használható eszközöket – például adathalász, levélszemét-terjesztő szolgáltatásokat – készítenek és adnak tovább,[63] ezzel megkönnyítve a kevésbé képzett közönség számára hasonló cselekmények elkövetését. Nevezhetjük ezen szakértelemmel rendelkező, tevékenységüket vállalkozás keretében folytató elkövetőket „feketesapkás" kiberbűnözőknek, szürkesapkásoknak pedig azokat, akik legális, és emellett illegális tevékenységre berendezkedett üzletek számára is nyújtanak szolgáltatásokat.[64] Létezik továbbá az államok vezetése által megbízott kiberbiztonsági szakértők köre, akik a kiberbűnözés elleni küzdelem keretében „beépülnek" az online alvilágba, adatokat gyűjtenek, megfigyelik az elkövetők módszereit és idővel rajtaütést visznek véghez.[65] Végül elengedhetetlen megemlíteni azokat az elkövetőket, akiket a profitszerzés helyett ideológiai okok vezetnek a kiberbűnözés körébe eső cselekmények elkövetésére ('hacktivisták'[66]).
A szakirodalomban keveredik a 'kiberbűnözők' és a 'hackerek' kategóriája. 'Hacker'[67] szűk értelemben véve az a személy, aki számítógép felhasználásával jogosulatlan hozzáférést szerez mások számítógépes rendszereihez, az általuk használt hálózatokhoz vagy az ezeken tárolt adatokhoz.[68] A 'hacker' fogalom a 'kiberbűnöző', illetve 'kibertérbeli támadó' kifejezéseket megelőzve alakult ki. Kezdetben a 'hacker' megnevezés nem hordozott pejoratív vagy kriminális jelentéstartalmat, hiszen tevékenységük önmagában nem jelentett pusztító vagy rongáló jellegű cselekményt[69]. Az 'etikus hackerek' vagy 'fehérsapkások' hozzájárultak az internethálózat kifejlesztéséhez, részt vettek különböző számítógépes rendszerek tesztelésében.[70] A kép árnyaltabbá vált, amikor az 1980-as évek végéhez közeledve 'hackelés' kifejezés negatív értelemet kapott, immár a technológiai rendszerek rosszindulatú manipulációját fejezte ki, szemben a számítógépes programozók karbantartó, fejlesztő tevékenységével. Az „eredeti" hackerkultúra a szociológiai elemzők szerint alapvetően pozitív és konstruktív elvrendszerre épült, az információs megosztására, komplex együttműködésre és egymás közötti kapcsolattartásra, kiegészülve a kreativitással és kritikus hozzáállással.[71] Később a hackerkultúra több egymás mellett létező szubkultúrára vált szét, ezek egyikét a 'crackerek' alkotják: e csoport tagjai olyan elkövetők, akik szakismeretüket rosszindulatú tevékenységekre, rongálásra használják,[72] mások szerint a crackerek tipikusan valamely szerzői jog megsértői.[73]
A szakirodalomban számos helyen olvashatunk a hackerek és kiberbűnözők tulajdonságairól, motivációiról, céljairól, csoportjaik formáiról. A két fogalom keveredése miatt e részben a 'kiberbűnözők' mint elkövetők, illetve az őket segítő személyek bemutatását kísérlem meg azzal, hogy ahol szükséges, kiemelem a szűk értelemben vett hackerek sajátosságait. Az elkövetőkről feltételezhetjük, hogy magas szinten értenek a technológiához,[74] azonban ez nem minden esetben felel meg a valóságnak. A piramis tetején valóban egy képzett, többéves

[62] Zavrsnik, 2008, 4.o.
[63] Yang, Debra Wong – Hoffstadt, Brian M.: Countering the Cyber-Crime Threat. In: American Criminal Law Review, 2006/43.sz., 5.o.
[64] Mezei – Nagy, 2016, 145.o.
[65] Maimon – Louderback, 2019, 4.o.
[66] Mezei – Nagy, 2016, 145.o.
[67] E kifejezés magyar megfelelője a „virtuális betörő" lehetne. A dolgozatban továbbra is az angol nyelvű kifejezést használom.
[68] Maimon – Louderback, 2019, 5.o.
[69] Zavrsnik, 2008, 15.o.
[70] Knoops, 2011, 741.o.
[71] Zavrsnik, 2008, 16.o.
[72] Zavrsnik, 2008, 16.o.
[73] Nagy Zoltán András: Bűncselekmények számítógépes környezetben, Budapest, 2009, Ad Librum, 68.o.
[74] Knoops, 2011, 742.o.

tapasztalattal rendelkező szűk réteg[75] helyezkedik el, akik szaktudásuk birtokában képesek újabb és újabb gyengepontokat találni a potenciális célpontokon. Őket követik azok, akik nem rendelkeznek ekkora tudással, viszont képesek arra, hogy rálépjenek a képzett réteg által kijárt útra, használják az általuk kifejlesztett eszközöket és technikákat. Utánuk a képzetlenek jóval tágabb rétege következik, ők képtelenek arra, hogy saját maguk használják az előbb említett fejlesztéseket, ehelyett készen vásárolnak olyan eszközöket, amelyekkel elérhetik céljaikat.
A lehetséges motivációk két alapvető irányba ágaznak, tehát hajthat valakit a haszonszerzés, illetve személyes indíttatás. A személyes indíttatás lehet szexuális jellegű, illetve eredhet például ideológiai megfontolásból, bosszúvágyból vagy szórakozás, kikapcsolódás iránti vágyból.
A kiberbűnözővé váló személyek rendszerint egyedül kezdenek jogsértő cselekményekbe.[76] A haszonszerzési célú elkövetések esetében a csoportokba rendeződés, illetve egyfajta munkamegosztásban[77] való részvétel célja a profit maximalizálása.[78] A 'malware' a programozók vagy kódolók keze által jön létre, ők felelősek a rosszindulatú szoftverek tervezéséért és kivitelezéséért. A programírókat a technikusok támogatják, akik rendelkezésre bocsátják és karbantartják az elkészült termékek értékesítésére alkalmas felületeket.[79] A marketingtevékenységet és terjesztést a 'kereskedők' végzik, ők adják el a termékeket azoknak, akik készen kívánják megvásárolni azokat. Átmeneti szerepet töltenek be a bűnelkövetők és a célpontok között a pénzfutárok ('money mule'). Ők azok, akiket beleegyezésükkel vagy tudtuk nélkül arra használnak, hogy valamilyen kereskedelmi tevékenység útján tisztára mossák a pénzösszegeket.[80]

I.3.2. CÉLPONTOK

Általános jellemzők
A szűk értelemben vett kiberbűnözés és a számítógép segítségével megvalósuló bűnözés körébe tartozó cselekmények kimenetele nemcsak az elkövető technológiai tudásszintjétől, hanem a célzott áldozatok viselkedésétől is jelentős mértékben függ. Az információtechnológia nemzetközivé válása széleskörű viktimizációhoz vezetett mind a high-tech eszközök felhasználói (a vállalatok és állami szervek[81]), mind az egyéni felhasználók körében.[82] Tulajdonképpen minden és mindenki, amelynek vagy akinek a kibertérben jelen lévő valamely formájú digitális kódhoz érdeke fűződik, célponttá válhat.[83] A leggyakoribb célpontokat a vállalatok adják, amelyeket az állami intézmények követnek. Az üzleti szektor szereplői válnak tehát leggyakrabban áldozatokká. Erre számos magyarázatot adhatunk. A vállalatok tetemes része számítógépek segítségével vált képessé termékek nagy mennyiségű és földrajzilag kiterjedt kereskedelmére, így a fizikai erőforrások (például raktárak, árukészletek) megrongálásának, ellopásának alternatívája az üzleti tevékenységet kiszolgáló számítógépes rendszerek megtámadása[84] lett. A mai vállalkozások értékes adataik, üzleti

[75] McGuire – Dowling, 2013, 24.o.
[76] Maimon – Louderback, 2019, 5.o.
[77] Maimon – Louderback, 2019, 4.o.
[78] Mezei – Nagy, 2016, 147.o.
[79] Legitim vállalkozások is biztosíthatnak felületeket a malware terjesztéséhez. A jogalkalmazás során felmerülhet a kérdés, hogy az egyébként legitim gazdasági tevékenységet folytató vállalkozások felismerik-e azt, hogy illegitim tevékenység folytatásához járulnak hozzá. (Mezei – Nagy, 2016, 147.o.)
[80] Mezei – Nagy, 2016, 148.o.
[81] Holt – Bossler, 2016, 17.o.
[82] Zavrsnik, 2008, 11.o.
[83] Majid, 2006, 419.o.
[84] Yang – Hoffstadt, 2006, 201.o.

titkaik túlnyomó részét elektronikus formában tárolják.[85] Az elektronikus adatok birtoklása helyett az azokhoz való hozzáférés, a rendszerek használatának képessége[86] rendelkezik értékkel. Ha a rendszer, amelyben az adatok tárolásra kerülnek, elérhető az internetről, megnyílik az adatokhoz való hozzáférés lehetősége és ezzel megnövekszik a bűncselekmények elkövetésének veszélye. Ma már nincs jelentősége annak, hogy milyen termékprofillal működik vagy mely szolgáltatásra épül egy vállalkozás, a szektor szereplői majdnem kivétel nélkül számítógépes hálózatoktól függnek mindennapi tevékenységük során.[87] Az áldozati „dobogó", vagyis a 'vállalatok – állami szektor – egyéni szereplők' sorrend első ránézésre meglepőnek tűnhet, mivel az egyéni felhasználókkal ellentétben a szervezeti felhasználók rendszerint rendelkeznek védelmi potenciállal, nevezetesen speciálisan kiberbiztonsági célokra alkalmazott személyzettel,[88] akiknek kizárólag az a feladata, hogy karbantartsák a vállalkozás vagy a szervezet számítógépes és hálózati rendszereit. Az egyének ezzel ellentétben általában nem rendelkeznek megfelelő technológiai felkészültséggel számítógépes eszközeik védelméhez,[89] a biztonsági célú szoftverek kellő frissítés és megfelelő konfiguráció hiányában viszont nem tudnak megfelelően működni.[90]

Viktimizáció

Ahogy nő a potenciális támadók száma – többek között a támadásinfrastruktúrák globális online kereskedelme[91] miatt –, úgy bővül a potenciális áldozatok köre is. A kiberbűncselekmények célpontjai, ahogy a fizikai világban megvalósuló bűncselekmények célpontjai is, nagyon változatosak és különbözőféleképpen értékelhetők.[92] A könnyebb megértés végett csoportosíthatjuk az áldozatokat. Ehhez megfelelő szempontrendszert biztosít a Routine Activity Theory.[93] A 'RAT', magyar elnevezéssel rutintevékenységi elmélet alapján egy célpont támadáshoz megfelelő volta négy tulajdonságon múlik: a célpont 'értékességén', 'tehetetlenségén', 'láthatóságán' és 'elérhetőségén'.[94]

1) Értékesség

   A célpont értékességét a javak adott időben a társadalom és a gazdaság általi értékelése[95] határozza meg. Ez összefügg egy korábban tett megállapítással, miszerint az online térhez való hozzáférés megfeleltethető a gazdasági erőviszonyok rajzolta térképnek. A hálózatokhoz való hozzáférés mértékével a viktimizáció veszélye is

[85] Zavrsnik, 2008, 13.o.
[86] Szathmáry Zoltán: Az internet mint a bűncselekmények elkövetésének helye. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika, 2019, Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 193.o.
[87] Yang – Hoffstadt, 2006, 204.o.
[88] Zavrsnik, 2008, 12.o.
[89] Zavrsnik, 2008, 12.o.
[90] McGuire – Dowling, 2013, 19.o.
[91] McGuire – Dowling, 2013, 25.o.
[92] Majid, 2006, 419.o.
[93] Az elsőként Lawrence E. Cohen és Marcus Felson által 1979-ben kidolgozott elmélet kiindulópontja az a feltevés volt, mely szerint a társadalom tagjai mindennapi ún. rutincselekvéseinek szerkezete hatással van a bűnalkalmakra, s ezáltal befolyásolja a „közvetlen kapcsolattal járó ragadozótípusú szabályszegések" kategóriájába tartozó bűncselekmények előfordulását. (Borbíró – Gönczöl – Kerezsi – Lévay (szerk.), 2018, 243.o.) A két szerző elméletében a rutintevékenységek, amelyek különféle lehetőségeket teremtenek az elkövetésre, mindig sajátos helyszíneken és sajátos időpontokban valósulnak meg. A célpontok lehetséges támadók számára való tér-és időbeli elérhetősége döntő jelentőséggel bír abban, hogy elkövetik-e, és ha igen, milyen valószínűséggel követik el a bűncselekményt. (Andresen, Martin A. – Farell, Graham (szerk.): The Criminal Act. The Role and Influence of Routine Activity Theory, London, 2015, Palgrave Macmillan, 19.o.)
[94] Majid, 2006, 419.o.
[95] Majid, 2006, 419.o.

növekszik, különösen azokban az országokban, ahol magasabb technológiai színvonal szabadabb politikai viszonyokkal találkozik.[96]

2) Tehetetlenség
A kiberbűnözés célpontjai „súlytalanok”,[97] az információ nagyon rövid idő alatt letölthető, másolható, megosztható. Hatalmas mennyiségű adat tárolható kis helyen, ezek a minőség számottevő romlása nélkül és végtelenül reprodukálhatók.[98]

3) Láthatóság
A magas számú potenciális elkövetőhöz való közelség meghatározza a célponttá válás valószínűségét.[99] Az elkövetőnek tudnia kell a célpont létezéséről ahhoz, hogy jogsértést kövessen el, tehát minél láthatóbb az online térben egy személy vagy egy adat, annál valószínűbb, hogy kiberbűncselekmény célpontjává válik. Például, ha valaki hosszabb időt tölt közösségi médiához tartozó felületeken vagy online kereskedelemmel foglalkozó oldalakon, az növeli a viktimizáció valószínűségét.[100] Az internet egy publikus, inherensen nyilvános[101] hálózat, amely a potenciális áldozatok hatalmas köréhez ad hozzáférést a támadóknak.[102] Ezzel szemben léteznek zárt, vállalati vagy intézményi belső IKT hálózatok is, ún. ’intranetek’ vagy virtuális privát hálózatok,[103] amelyekhez sok lépcsős beléptetés után korlátozott közönség tud hozzáférni, bizonyos mértékű „láthatatlanságot” biztosítva használóiknak.

4) Elérhetőség
Az ’elérhetőség’ kifejezés a támadó célponthoz való eljutási képességére utal.[104] Az elérhetőség ellen a potenciális célpontok biztonsági eszközökkel védekeznek, amelyek a jogosulatlan hozzáférést hivatottak megakadályozni, valamint a jogsértő tevékenység folytatásának lehetőségét csökkenteni, megszüntetni. Ezek az online térben jelenthetnek például technikai eszközöket (antivírus szoftverek[105]), nagyvállalatoknál az alkalmazottak számára irányadó biztonsági előírásokat, weboldalakon elhelyezett figyelmeztető jelzéseket (’surveillance’ vagy ’warning banner’).

I.3.3. FELÜGYELET

A kiberbűnözés témaköréhez tartozó angolszász ’guardianship’ kifejezés leginkább kifejező magyar megfelelője a ’felügyelet’.[106] A ’felügyelők’ – legyenek ezek személyek vagy eszközök – funkciója bűnelkövetés megelőzése érdekében a kibertér megfigyelése, monitorozása, a gyors problémamegoldás.[107] A kibertér felügyeletét elláthatják fizikai személyek, elsősorban a hivatalos, állami kontrollt megtestesítő bűnüldöző szervek. E szervek mellett más szereplők közreműködése is szükséges az online tér rendjének megőrzésében. Üzleti oldalon a vállalatok belső szakértői, adminisztrátorai, rendszergazdái, tágabb körben pedig internetszolgáltatók és domain nyilvántartók az internet adatainak „kapuőreiként”[108] felügyelik a virtuális terek viszonyait. Jellemzően nem üzleti, hanem informális, személyes

[96] Maimon – Louderback, 2019, 10.o.
[97] Majid, 2006, 420.o.
[98] Clough, 2011, 673.o
[99] Majid, 2006, 414.o.
[100] Maimon – Louderback, 2019, 11.o.
[101] Majid, 2008, 420.o.
[102] Clough, 2011, 671.o
[103] Majid, 2006, 420.o.
[104] Majid, 2006, 421.o.
[105] McGuire – Dowling, 2013, 14.o.
[106] A magyar szakirodalomban használják a ’megfigyelők’ kifejezést is. (Parti Katalin: A számítógépes bűnözés és az internet. In: Kriminológiai Tanulmányok, 2003/40.sz., 194.o.)
[107] Maimon – Louderback, 2019, 12.o.
[108] Clough, 2010, 8.o.

alapú felügyeleti szerepet tölthetnek be az online csoportok önjelölt moderátorai, illetve az online közösségek adminisztrátorai is, akik fellépnek az adott csetszobában, csoportban, fórumon, virtuális világban irányadó szociális normák megszegői ellen. Az eszközök oldalán technológiai, illetve „szabályozási" jellegű felügyeletről beszélhetünk. A technológiai jellegű eszközök közül említhetők a különböző szoftveres megoldások (pl. vírusszűrő vagy jogosulatlan belépést jelző programok, kiskorúak védelmére fejlesztett webtartalom-szűrők) vagy állami finanszírozású, e-kommunikációt monitorozó projektek.[109] A szabályozási jellegű felügyeleti eszközök a technológiai fejlesztésű védelmi eszközökhöz képest kevésbé professzionálisak, ilyenek például az online közösségek szabályozási gyakorlatai, magatartáskódexei („netikett").[110]
A személyekre és eszközökre feloszthatő felügyelet más megközelítésben a kibertér viszonyainak online, illetve offline formájú kontrolljaként is vizsgálható. Online formához sorolhatók a korábbiakban említett felügyeleti eszközök körébe tartozó technológiai és szabályozási jellegű megoldások, illetve a személyek tevékenységei közül mindaz, amely a virtuális térben nyilvánul meg. Offline felügyeletként fogható fel a jogalkotás. A jogalkotás, mint felügyeleti erő egyik problémája, hogy viszonylag lassan reagál[111] a kibertér növekvő kockázataira. A mindent átfogó folyamat, amelyben a társadalom egyre inkább az internettől kezd függővé válni, gyorsabban játszódik le annál, mint ahogy ahhoz a jogérvényesítés alkalmazkodni tudna.[112] A kibertérbeli bűnözés gyors ütemű innovációja folyamatos kihívás s jogalkotás számára. A szereplők általában könnyen megkerülik a szankciókat, megelőző intézkedéseket,[113] így a hagyományos büntetőszabályozás jellemzően lemaradásban van a technológiai változásához képest.[114] A jogi szabályozás, mint felügyeleti erő problematikus amiatt is, hogy a büntető szabályok megalkotása a nemzeti szuverenitás része, amely sajátosság ellentétben áll a kibertér markánsan globalizált jellegével.
Az online tér állandó, átfogó, minden tevékenységre és személyre kiterjedő felügyelete lehetetlen feladat, a fizikai világban meglévő mértékű figyelmet képtelenség fenntartani egy olyan térben, amelynek szereplői ilyen könnyedén mozognak, ahol az idő- és térbeli viszonyok ennyire szabálytalanok, széttöredezettek.[115] A felügyelet eddigiekben kifejtett elemei mind azt az alapvető célkitűzést szolgálják, mely szerint az online tér szabályozottsági szintje legalábbis érje el a fizikai világét a kiberbűnözés okozta sérelmek elkerülése, következményeik csillapítása érdekében.

II. RÉSZ – A KIBERBŰNCSELEKMÉNYEK HAZAI GYAKORLATA

A II. rész célja, hogy a kiberbűncselekmények hazai szabályozásának áttekintése után kiemelje a szűkebb értelemben vett kiberbűncselekmények, azt követően pedig a vegyes jellegű deliktumok lényegét. E részben tehát először a hálózat-bűncselekmények törvényi szabályozását, illetve joggyakorlatát tekintem át, ezt követően pedig rátérek egyes vegyes jellegű deliktumok törvényi tényállásának elemzésére és annak bemutatására, hogy elkövetésük során hogyan jelenik meg, milyen szerepet tölt be az online tér és a közvetítő technológiai eszközök. E rész nem foglal magában minden olyan cselekményt, amely egészen vagy valamely részben az online térben realizálódik. Arra törekszem, hogy azon

[109] Majid, 2006, 423.o.
[110] McGuire, 2007, 278.o.
[111] Wall – Williams, 2007, 400.o.
[112] Lavriero, 2016, 244.o.
[113] Knoops, 2011, 740.o.
[114] Clough, 2011, 671.o
[115] Majid, 2008, 423.o.

cselekményeket mutassam be, amelyek rendelkeznek a kiberbűncselekmények jellegadó sajátosságaival, bizonyos értelemben klasszikus online bűncselekményeknek nevezhetők, illetve – a vegyes jellegű deliktumok között – aktuálisnak nevezhető problémákat vetnek fel. Nem foglalkozom a cselekmények eljárásjogi vonatkozásaival, illetve egyes olyan anyagi jogi kérdésekkel sem, amelyek a kiberbűnözés elméletében jelentős problémákat felvetve túlmutatnak a dolgozat keretein, ideértve a bűncselekmények elkövetési helyét.

A kiberbűnözés hazai szabályozásának bemutatása előtt érdemes kitérni az Európai Unió vonatkozó jogalkotási aktusaira. Uniós jogalkotási aktusként az irányelvek meghatározzák az Európai Unió által elérendő célokat, e célok megvalósításának miként jét azonban a tagállamokra bízzák. Az Európai Unióban Az Európai Parlament és a Tanács 2013. augusztus 12-i az információs rendszerek elleni támadásokról és a 2005/22/1B tanácsi kerethatározat felváltásáról szóló 2013/40/EU irányelve[116] (a továbbiakban: Irányelv) vonatkozik a információs rendszerek elleni támadásokra. Az Irányelv fő célkitűzése, hogy közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén. Emellett az Irányelv céljai között szerepel, hogy javítsa a bűnüldözés szervei közötti együttműködést, elősegítse az ilyen rendszerek megfelelő szintű védelmét és a kritikus infrastruktúrák[117] támadásának megelőzését, továbbá szorgalmazza a közös fogalommeghatározások kialakítását is. Az Irányelv szerint a tagállamoknak közös megközelítést követve kell kialakítaniuk a bűncselekmények tényállási elemeit, valamint szankciókat kell megállapítaniuk a rendszerek elleni támadások elkövetése esetére. Az Irányelv és a magyar szabályozás elemei közötti kapcsolatra az egyes tényállások elemzésénél utalok.

Uniós tagállamként Magyarországnak az irányelvek tekintetében implementációs kötelezettsége áll fenn. A magyar jogalkotó e kötelezettségnek tett eleget azzal, hogy Irányelv adta kereteket követve alakította át az információs rendszereket fenyegető magatartásokat szankcionáló tényállásokat. A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban Btk.) rendelkezései között a potenciálisan online térben megnyilvánuló cselekmények közül kiemelésre kerültek a hálózat-bűncselekmények. A Tiltott adatszerzés és információs rendszer elleni bűncselekmények című XLIII. fejezet tartalmazza[118] a tiltott adatszerzés (422. §) információs rendszer vagy adat megsértése (423. §) és az információs rendszer védelmét biztosító technikai intézkedés kijátszása (424. §) tényállásokat. E rendelkezések mellett megemlítendő a vagyon elleni bűncselekményekről szóló XXXVI. fejezetben önálló tényállással szereplő információs rendszer felhasználásával elkövetett csalás (375. §).[119] E szabályozási mód arra enged következtetni, hogy a jogalkotás során figyelemmel voltak a kiberbűncselekmények korábban említett elméleti csoportosítására, közelebbről arra, hogy léteznek a kibertér által lehetővé vált bűncselekmények, illetve olyan vegyes jellegű deliktumok, amelyek elkövetési magatartásába valamilyen szinten beszivárgott az információs és kommunikációs technológia. Utóbbi csoport a cselekmények széles körét

[116] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013L0040&from=EN utolsó letöltés dátuma: 2020.09.04.

[117] A kritikus infrastruktúrák alatt az irányelv azokat a rendszereket, illetve eszközöket érti, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok, az egészségügy, a biztonság, a védelem, valamint az emberek gazdasági és szociális jólétének fenntartásához, és amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. A fogalom magyar szabályozással fennálló összefüggését később tárgyalom.

[118] A Btk. 465. § (1) bekezdésének f) pontjában az Európai Unió jogának való megfelelésről szóló szakaszban szerepel, hogy a magyar büntetőtörvény 375. §-a és XLIII. Fejezete az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló, 2013. augusztus 12-i 2013/40/EU európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

[119] Lásd bővebben az információs rendszer felhasználásával elkövetett csalásról: Mezei Kitti: A kiberbűnözés aktuális kihívásai a büntetőjogban. L'Harmattan – TK JTI, Budapest, 2020. 104-111.o.

öleli fel, ezek közül a gyermekpornográfia (204. §) és a zaklatás (222. §) tényállásával részletesen foglalkozom.
A XXI. *Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények* fejezetbe tartozó más bűncselekmények (személyes adattal visszaélés magántitok megsértése, levéltitok megsértése, rágalmazás, becsületsértés) tárgyalása túlmutatna jelen dolgozat keretein, így azok elemzésre nem kerül sor. Jelen dolgozatnak nem képezi tárgyát, mégis a kibertérben elkövethető bűncselekmények közé tartozhat még a törvény XXXVII. Szellemi tulajdonjog elleni bűncselekmények, XXXVIII. *A pénz- és bélyegforgalom biztonsága elleni bűncselekmények* és XL. *Pénzmosás* című fejezeteiben foglalt bűncselekményi kör,[120] továbbá csak röviden térek ki a XXXVI. *A vagyon elleni bűncselekmények* fejezetébe tartozó csalás (373. §) tényállására.

II.1. HÁLÓZAT-BŰNCSELEKMÉNYEK

1) Elsőként az információs rendszer vagy adat megsértése tényállással foglalkozom. A 423. § első bekezdése a vétségi alakzatot szabályozza. A vétségi alakzat jogi tárgya az információs rendszerek[121] megfelelő, biztonságos működéséhez fűződő érdek. A cselekmény elkövetési tárgyát illetően Nagy Zoltán András elkülöníti egymástól az egyes számítógépet, illetve a számítástechnikai rendszert, valamint a számítógépes programokat és elektronikus adatokat.[122]
Első fordulata az információs rendszerbe az annak védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történő jogosulatlan belépést szankcionálja; második fordulat pedig a belépési jogosultság kereteinek túllépésével vagy megsértésével történő bennmaradást. A Btk. e rendelkezése véleményem szerint megfeleltethető az Irányelv Információs rendszerekhez való jogellenes hozzáférés című 3. cikkének, hiszen mindkettőnek eleme a jogosulatlan[123] tevékenység, a belépés pedig – jelen esetben – jelentheti a hozzáférést, és mindkét rendelkezés szövege tartalmazza valamely biztonsági intézkedés megsértését. A belépés nem jogosulatlan, ha az információs rendszer nem védett, illetve a védelem nem aktivált.[124]
A második fordulat révén a vonatkozó magyar szakasz az irányelvi rendelkezéshez képest részletezőbbnek tekinthető, ugyanis a jogosultsággal történő belépést követően megvalósuló, jogosultságot túllépő vagy megsértő bennmaradást különválasztották a jogosulatlan belépéstől. Az Irányelv (1) preambulumbekezdésének alapján a tagállami jogalkotó lehetőséget kap arra, hogy az irányelvi szabályokon túlmenően – adott esetben szigorúbban – szabályozza az információs rendszerek elleni támadó jellegű magatartásokat, mivel mind az említett preambulumbekezdésben, mind az Irányelv tárgyára vonatkozó cikkben szerepel, hogy az minimumszabályokat állapít meg.

---

[120] Ehhez lásd Ambrus István: Büntetőjog 2021. A pénzmosás újrahangolt tényállása és a hálapénz kriminalizálása. In: Büntetőjogi Szemle, 2020/2.sz., 3-7.o.
[121] A Btk. értelmező rendelkezései között a 459. § (1) bekezdés 15. pontjában meghatározás szerepel az 'információs rendszer' fogalmára vonatkozóan. Információs rendszer tehát az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.
[122] A 423. § vonatkozásában az (5) bekezdés tartalmazza az 'adat' fogalmát, amely információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.
[123] A jogosulatlanság fogalma az Irányelv fogalommeghatározásai között található, a 2. cikk d) pontja szerint olyan magatartás, ideértve a belépést, beavatkozást vagy adatszerzést, amelyet a rendszernek vagy a rendszer részének tulajdonosa vagy egyéb jogosultja nem engedélyezett, vagy amelyet a nemzeti jog nem tesz lehetővé.
[124] Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In: Magyar jog, 2019/5.sz., 306.o.

Ahogy az első fordulat megvalósulásához, a második fordulat szerinti elkövetéshez is szükséges a rendszervédelmi technikai intézkedés megsértése vagy kijátszása. Egy olyan cselekmény esetén, amely során valamely személy – felhasználva a belépéshez meglévő jogosultságát – belép az adott informatikai rendszerbe, majd jogosultsága kereteit túllépve vagy megsértve bennmarad ugyan, de sem a belépés érdekében, sem a bennmaradás biztosítása végett nem sért meg és nem játszik ki védelmi intézkedést; pusztán a jogosultság kereteinek túllépése okán nem éri el azt a veszélyességi szintet, amit az első fordulat megkíván.[125] Az idevágó 2017-es kúriai döntés foglalkozik egy bűnügyi technikus adatkeresésével a rendőrség ügyfeldolgozásra szolgáló Robotzsaru Neo nevű rendszerében. A tényállás szerint a vádlott jogosultság birtokában lépett be a rendszerbe, de további tevékenysége, amely során két esetben keresést indított különböző bűncselekmények terheltjével kapcsolatban, az adatkezelési szabályokba ütközött. A bűnüldözési célból gyűjtött és tárolt adatok felhasználására a rendőrségi törvény és a belső utasítások irányadóak. Az üggyel foglalkozó másodfokú bíróság szerint megalapozott volt az információs rendszer megsértésének vétsége, mivel a jogosultság kereteinek túllépése bizonyítást nyert, és az már önmagában megvalósítja a 423. § (1) bekezdésének második fordulatát. E döntés szerint tehát a vétségi alakzat második alakzatának megállapításához nem szükséges az, hogy a terhelt védelmi célú technikai intézkedés megsértésével, kijátszásával maradjon a rendszerben.[126] A Kúria ezzel ellentétben – az ügyben eljárt elsőfokú bírósággal egyetértve[127] – azt állapította meg, hogy a vádlottat cselekményéért nem terheli büntetőjogi felelősség, mivel a rendőrségi adattárba saját jelszóval való (tehát jogosult) belépést követően a jogosultság keretein túllépés (és bennmaradás) csak akkor minősült volna bűncselekménynek, amennyiben a cselekmény védelmi intézkedés megsértésével vagy kijátszásával ment volna végbe.[128]

A 423. § második bekezdése tartalmazza a bűntetti alakzatokat. Jogvédte értékként az első bekezdéshez hasonlóan az információs rendszerek biztonságos működése jelölhető meg. Az a) pontban az információs rendszer működésének jogosulatlan vagy a jogosultság kereteit megsértő akadályozása, a b) pontban az információs rendszerben lévő adat jogosulatlan vagy a jogosultság kereteit megsértő megváltoztatása, törlése vagy hozzáférhetetlenné tétele szerepel (ún. adatvisszaélés[129]). Utóbbi jogi tárgya az információs rendszer biztonságos működéséhez fűződő érdek, amely az adatok megbízhatóságához, hitelességéhez fűződő érdekkel, illetve kiegészül – az adatok tartalmától függően – az azok által megtestesített értékkel.[130] A Btk. 423. § (2) bekezdés a) pontja és az Irányelv 4. cikkének (’Rendszert érintő jogellenes beavatkozás’), ugyanezen bekezdés b) pontja pedig az Irányelv 5. cikkének (’Adatot érintő jogellenes beavatkozás’) magyar szabályozásba történő átültetése. A Btk. a

[125] A Kúria Bhar.I.537/2017/5. sz. határozata és BH2017. 392.
[126] A Fővárosi Ítélőtábla Kbf.28/2016/5. sz. határozata.
[127] A Kaposvári Törvényszék Katonai Tanácsának Kb.26/2015/12. sz. határozata.
[128] A döntések közötti jelentős eltérés – tekintve, hogy az Ítélőtábla pénzbüntetést szabott ki, míg az elsőfokú bíróság és a Kúria felmentette a vádlottat – abból adódhatott, hogy a jogalkotó nem választotta külön a *jogosulatlan belépés*, illetve a *belépési jogosultság kereteit túllépő vagy megsértő bennmaradás* elkövetési magatartásokat, hanem azokat az *információs rendszer védelmét biztosító technikai intézkedés megsértése vagy kijátszása* elkövetési mód megjelölését követően vesszővel elválasztva egy mondatba foglalta. A másodfokú bíróság a sorrendben második elkövetési magatartás megállapítására alapította döntését, amely szerint a terhelt *túllépte* jogosultsága kereteit, és ezáltal a rendszerben bennmaradt, azonban – hivatkozva egy, a számítástechnikai rendszer elleni bűncselekmény vétségével foglalkozó 2014-es kúriai döntésre – nem tartotta lényegesnek vizsgálni, hogy a terhelt sértett-e, illetve kijátszott-e valamilyen védelmi intézkedést. Amennyiben e cselekmények két külön pont alá kerülnének, egyértelművé válna, hogy mindkét elkövetési magatartás megállapíthatóságához szükséges-e a tényállás első tagmondatában szereplő elkövetési mód, vagy azt csupán az első fordulatra vonatkozik.
[129] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[130] Nagy Zoltán András: A számítógépes környezetben elkövetett bűncselekmények új szabályozásáról. Háttér és elemzés. In: Ügyészek Lapja, 2014/3-4.sz., 32.o.

rendszer működésének akadályozását nyitott törvényi tényállással szabályozza, míg az adatvisszaélés elkövetési magatartásaira vonatkozóan felsorolást tartalmaz. Az Irányelv mindkét idevágó rendelkezése tartalmaz olyan lehetséges magatartásokat, amelyekkel az adott cselekmény elkövethető. A rendszerek működésének akadályozása megvalósulhat például szándékos és jogosulatlan adatbevitellel, adattovábbítással vagy adattörléssel, az adatokat célzó támadásoknál pedig az elrejtést, törlést, minőségi rontást és hozzáférhetetlenné tételt emeli ki.

A bűncselekmény tényállása két minősített esetet tartalmaz. Egyfelől súlyosabban minősül a bűntetti alakzatot megvalósító elkövetés akkor, ha jelentős számú információs rendszert érint. A törvény nem ad iránymutatást azzal kapcsolatban, hogy milyen kiterjedésű elkövetés szükséges e minősített eset megállapíthatóságához. A jogirodalom ide sorolja az ún. „hálózatbiztonsági bűncselekményeket", amelyek lényege, hogy illetéktelenek a felhasználók tudta és akarata ellenére átveszik a számítógépes rendszer feletti uralmat, és a gép, illetve az internetkapcsolat erőforrásait saját céljaik elérésére fordítják.[131] A külföldi szakirodalom ezeket „terheléses" vagy „szolgáltatásmegtagadással járó" támadásnak nevezi (angolul 'distributed denial of service' és 'denial of service'). Ezek a bűncselekmények az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak elérhetetlenné tételével,[132] illetve alapfeladatuk ellátásának akadályozása vagy annak elvégzésére képtelenné tétele útján valósulnak meg.[133] Mindkét forma a túlterhelés módszerére épül: a számítógépes rendszer olyan mennyiségben és gyakorisággal kap adatcsomagokat – normál vagy illegális kérelmek formájában –, hogy képtelen azokra választ adni, s ezúton nagymértékben lelassul, illetve működésképtelenné válik.[134]

Másfelől mind a vétségi, mint a bűntetti alakzat elkövetése súlyosabban minősül, ha a bűncselekményt közérdekű üzem ellen követik el. A közérdekű üzem fogalmát a Btk. 459. § (1) bekezdés 21. pontja tartalmazza. Közérdekű üzem a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek, a hadianyagot, haditechnikai eszközt termelő üzemet, energiát vagy üzemi felhasználásra szánt alapanyagot termelő üzem. Korábban említésre került, hogy az Irányelv célkitűzései között a kritikus infrastruktúrák kiberbűnözéssel szembeni védelmét jelöli meg. E fogalomba az Európai Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló 2019. május 17-i 2019/796. számú tanácsi rendelet[135] szerint minden olyan információs rendszer beletartozik, amely elengedhetetlen a társadalom

---

[131] Peszleg Tibor: Az adatbűnözés és gazdasági hatásai. In: Infokommunikáció és jog, 2009/3.sz, 76.o.

[132] Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. In: Pro Futuro, 2018/1.sz., 66.o.

[133] Zsolt, Bederna – Tamás, Szadeczky: Cyber espionage through Botnets. In: Security Journal, 2020/33.sz, 48.o.

[134] A 'DoS' támadás egy számítógéptől érkezik, nincs közvetítő eszköz, míg 'DDoS' *elosztott* szolgáltatásmegtagadással járó támadás elkövetője igénybe veszközvetítő számítógépes rendszereket, azokat egy időben irányítva folytatja le a támadást. A támadásokat lehetővé tevő kapcsolat többféleképpen létrejöhet, leggyakrabban ún. botneteket használnak ezek megteremtéséhez. A botnet – elnevezése a 'robot' és a 'network' angol szavak összevonásából keletkezett – olyan hálózati csomópontok összessége, amelyek fennmaradását a megfertőzött eszközök biztosítják, jellemzően azok tulajdonosainak, használóinak tudta nélkül. A lényeget tekintve a 'DoS' vagy 'DDoS' támadások előfeltételeként a támadó, utóbbi fajta esetében a 'botherder' először megkísérli eljuttatni a rosszindulatú irányító programokat a számítógépes rendszerekre. Ha ez sikeres, a 'DoS' feltételei megteremtődtek, míg a 'DDoS' támadásnál erre a megfertőzött rendszerek feletti irányítás biztosítása után kerülhet sor. (Mezei, 2018, 67.o.) Az elkövető az elosztott túlterheléses támadások esetén nem csupán az első, általa közvetlenül elért rendszer működését akadályozza, hanem az összes olyan információs rendszer működését is, amelyet közvetve ért el és távolról támadásra utasít. (Sorbán Kinga: Információs rendszer és adatok megsértése, avagy vírusok, férgek és trójai falovak a büntető törvénykönyvben. In: Belügyi Szemle – Ordinem Facere, 2018/1.sz., 72.o.)

[135] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0796&from=EN
utolsó letöltés dátuma: 2020. 09.04.

létfontosságú funkcióinak vagy az emberek egészségének, biztonságának, védelmének, illetve gazdasági vagy szociális jólétének fenntartásához. A közérdekű üzem magyar fogalma szűkre szabottnak tűnhet az uniós szinten használt fogalmakhoz képest, amely például az egészségügyi ellátóhálózat informatikai rendszerét ért esetleges támadás esetén kihathat a minősített eset megállapíthatóságára.

2) Az irányelv tényállásainak soron következő, egyben utolsó része a jogellenes adatszerzés címmel ellátott 6. cikk, amely a jogellenes adatszerzésről szól. E rendelkezés elemeinek leginkább a Btk. 422. § (1) bekezdésének e) pontjában található elkövetési magatartás feleltethető meg. Az irányelvi rendelkezés az információs rendszerbe, onnan kívülre, illetve azon belül továbbított nem nyilvános számítógépes adatok technikai eszközökkel szándékosan és jogellenesen történő megszerzéséről szól. A magyar szabályozásban e cselekmény a tiltott adatszerzés tényállásába építve jelenik meg, és azt az elkövetési magatartást szankcionálja, amely során az elkövető az információs rendszerben kezelt adatokat titokban kifürkészi és azokat rögzíti is.
E bűncselekmény lényege tehát az adatok megismerése és valamilyen formában történő megőrzése. A védett jogi tárgy elsősorban az adatok (személyes adatok, üzleti vagy gazdasági titkok) integritását biztosítani kívánó magántitok védelméhez fűződő személyiségi jog, a személyes adatokhoz, üzleti és gazdasági titok megőrzéséhez fűződő érdek, ellentétben a 423. § – és ahogy később bemutatásra kerül, a 424. § – bűncselekmények védett jogi tárgyával. A magatartások szankcionálása által védendő jogi tárgyak különbözősége indokolja, hogy az adatok megismerését és rögzítését célzó elkövetések nem a szűkebb értelemben vett kiberbűncselekmények részeként, hanem azoktól valamelyest elkülönülve kerültek szabályozásra. Meg kell jegyezni, hogy jelen tényállásnál – a 423. § (1) bekezdésének első fordulatával ellentétben – a hozzáférés nem feleltethető meg a belépésnek, hiszen az adatok megismeréséhez vezető hozzáférés mozzanata nem jár szükségképpen jogosulatlan belépéssel.[136]

3) A XLIII. fejezetben szerepel továbbá az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétsége (424. §). Jogi tárgya megegyezik a megelőző szakaszéval. E tényállás az információs rendszerek támadásának megágyazó előkészületi lépések szankcionálására szolgál. A bűncselekmény elkövetési tárgya a károkozó adatvisszaélés, a tiltott adathalászat egy formája, illetve az információs rendszer vagy adat megsértése cselekményeknek elkövetéséhez szükséges vagy az elkövetést megkönnyítő jelszó, számítógépes program (a) pont), illetve az ezek készítésére vonatkozó gazdasági, műszaki, szervezési ismeretek (b) pont).
Az elkövetési magatartásokat két fordulat alá rendezi a törvény. Az (1) bekezdés a) pontjának elkövetési magatartásai a készítés, az átadás, a hozzáférhetővé tétel, a megszerzés és a forgalomba hozatal. A készítés a jelszót, számítógépes programot alkotó kódok létrehozatalából áll, az átadás a másnak való birtokba adást jelenti, ugyanakkor jelentheti a rendelkezésre bocsátást is.[137] A hozzáférhetővé tétel aktív és passzív magatartásban is megnyilvánulhat, mások ennek következtében juthatnak az adott elkövetési tárgy birtokába. A megszerzés a más által készített jelszavak, számítógépes programok birtokbavétele.[138] A forgalomba hozatal a jelszó, számítógépes program egy vagy több személy részére ellenérték fejében vagy ingyenesen történő eljuttatását jelenti. Jelen fordulattal kapcsolatban büntethetőséget megszüntető okot is tartalmaz a Btk. Amennyiben az elkövető a jelszó vagy számítógépes program készítésének hatóságok tudomására jutása előtt tevékenységét a

[136] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[137] Mezei, 2019, 314.o.
[138] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)

hatóság előtt felfedi, az elkészített dolgot átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását, úgy nem büntethető cselekményéért.
Az (1) bekezdés b) pontja az adott jelszó, illetve számítógépes program készítésére vonatkozó gazdasági, műszaki, szervezési ismeretek más számára való rendelkezésre bocsátást szankcionálja. E második fordulat elkövetési magatartása akár aktív, akár passzív formát is ölthet.[139] Lényege, hogy az elkövető nem vesz részt a készítési folyamatban, hanem cselekményének közvetítő szerepe van, más személyek ennek eredményeképpen juthatnak olyan információkhoz, amelyek birtokában képessé válnak a fent említett súlyosabb bűncselekményi formák elkövetésére.

4) A vagyon elleni bűncselekményekről szóló XXXVI. fejezetben a 375. § alatt az (1) – (4) bekezdésben szerepel az információs rendszer felhasználásával elkövetett csalás ún. károkozó adatvisszaélés[140] alakzata. Az (1) bekezdés tartalmazza az elkövetési magatartásokat, amelyek a következők: információs rendszerbe történő adatbevitel, az abban kezelt adat megváltoztatása, törlése, hozzáférhetetlenné tétele. A jogalkotó „nyitva hagyja" az elkövetési magatartások körét azzal, hogy a tényállás részévé teszi az információs rendszer működésének egyéb művelettel történő befolyásolását is. Jelen bűncselekmény elkövetési magatartásai részben megegyeznek a korábban vizsgált 423. § (2) bekezdésének b) pontjában szabályozott információs rendszer vagy adat megsértése elkövetési magatartásaival. A két bűncselekmény elhatárolása során a stádiumokat és a célzatot érdemes vizsgálni. A károkozó adatvisszaélés esetében egyenes szándéknak kell fennállnia a jogtalan, mások megtévesztésével károkozásra irányuló[141] haszonszerzésre vonatkozóan. A károkozást – a kár bekövetkezését és a kár mértékét – illetően elegendő az eshetőleges szándék.[142] A kár[143] keletkezhet magában az információs rendszerben is, de jellemzően az információs rendszer útján kezelt vagyonban bekövetkezett kár tényállásszerű.[144]
Károkozó adatvisszaélés kísérlete valósul meg akkor, ha bizonyítható a haszonszerzési cél, és bármelyik elkövetési magatartás megkezdődik ugyan, de károkozás nem következik be, ezáltal nem válik befejezetté a bűncselekmény. Haszonszerzési cél hiányában a korábban megjelölt elkövetési magatartások bármelyikének fennállása esetén az információs rendszer vagy adat megsértése tényállásának második alakzata (423. § (2) bekezdés b) pont) állapítandó meg. Amennyiben a károkozó csalás elkövetése érdekében az elkövető jelszót, illetve számítógépes programot készít, a 424. §-ban foglalt információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétsége valósul meg. Ugyanakkor ha bármilyen további, az adott információs rendszer befolyásolását célzó cselekményre sor kerül, illetve a nevesített elkövetési magatartások bármelyikének megvalósítása esetén az elkövető károkozó csalás bűntettének kísérlete miatt felel.[145] A szakasz (2) – (4) bekezdése a bűncselekmény súlyosabban minősülő eseteit a vagyon elleni bűncselekményeknél alkalmazott szabályozási technikához hasonlóan a bekövetkezett kár összegéhez igazodóan szabályozza, illetve a minősítési rendszer részeként a bűnszövetségben történő és üzletszerű elkövetés is szerepel.[146]
E tényállás vizsgálata során el kell különíteni az első négy bekezdés és ugyanezen szakasz (5) – (6) bekezdése által lefedett bűncselekményi kört. A szakasz két utolsó bekezdése az

[139] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[140] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[141] Kónya István (szerk).: A magyar büntetőjog. Kommentár a gyakorlat számára II., Budapest, 2013, HVG-Orac, 1413.o.
[142] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[143] A Btk. 459. § (1) bekezdés 16. pontja szerint a törvény eltérő rendelkezése hiányában a bűncselekménnyel a vagyonban okozott értékcsökkenés.
[144] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[145] Kónya (szerk.), 2013, 1414.o.
[146] Kónya (szerk.), 2013, 1415.o.

elektronikus készpénz-helyettesítő fizetőeszközzel való visszaéléssel megvalósuló alakzatot foglalja magában. Ezen alakzat elkövetési tárgya az elektronikus készpénz-helyettesítő fizetési eszköz, amely fogalmának meghatározására a Btk. 459. § (1) bekezdésének 20. pontja utal. E pont szerint elektronikus készpénz-helyettesítő fizetési eszköz a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszköz, kincstári kártya, valamint a személyi jövedelemadóról szóló törvény felhatalmazása alapján kiadott elektronikus utalvány, feltéve, hogy ezek információs rendszer útján kerülnek felhasználásra. A hitelintézetekről és a pénzügyi vállalkozásokról 2013. évi CCXXXVII. törvény 6. § (1) bekezdésének 55. pontja szerint készpénz-helyettesítő fizetési eszköz a csekk, az elektronikus pénz, a pénzforgalmi szolgáltató és az ügyfél közötti keretszerződésben meghatározott olyan személyre szabott dolog vagy eljárás, amely lehetővé teszi az ügyfél számára a fizetési megbízás megtételét. Mindkét alakzat védett jogi tárgya a információs rendszerekkel és készpénzkímélő eszközökkel történő fizetési műveletekkel érintett vagyoni jog. Mindazonáltal az (5) bekezdést megvalósító magatartás véleményem szerint akkor tartozna a szűkebb értelmű, tiszta kiberbűncselekmények közé, amennyiben az elkövető a hamis, hamisított vagy jogosulatlanul megszerzett eszköz felhasználását, illetve az ilyen eszközzel történő fizetés elfogadását túlnyomórészt az online térben valósítaná meg.
Azon vádlott cselekménye, aki jogosulatlanul megszerzi a sértett bankkártyáját, majd azzal néhány nap letelte alatt kisebb összegeket vesz fel a sértett bankszámlájáról, megvalósítja ugyan az (5) bekezdés szerinti bűncselekményt,[147] ennek során információs rendszert felhasználva jár el, de ezen felül nem az online térben cselekedve viszi véghez az elkövetési magatartást. Jellemzően e cselekményeknél az elkövetési tárgyat a fizikai térben szerzik meg – vagy hamisítva szerzik meg, illetve hamisítják –, majd szintén a fizikai térben történik a károkozás, tehát a felhasználás, illetve a fizetés elfogadása. Az idő előrehaladtával és a technológiai lehetőségek kiterjedésével, széleskörű felismerésével valószínű, hogy az alakzat alá tartozó magatartások egyre inkább közelebb kerülnek majd a szűkebb értelemben vett kiberbűncselekmények fogalmához, például akkor, ha az elkövetők nem készpénzfelvétellel, hanem online vásárlással valósítják meg a károkozást.
Az (1)-(4) bekezdésben szabályozott károkozó adatvisszaélés és az (5) – (6) bekezdések szankcionálta magatartások feltűnő különbségük ellenére egy szakasz alatt találhatók, alátámasztva azon korábbi megállapítást, mely szerint a kiberbűnözés körébe vonható cselekmények a hagyományos bűnelkövetési magatartások részbeni átalakulása következtében jelentek meg, illetve komplex és diverz jellegüknél fogva megnehezítik a jogalkotó kategorizálási törekvéseit.

5) Végül szükséges megvizsgálni a jelen tényállás és a csalás (373. §) viszonyát, mely bűncselekményt szakirodalom az online térben megvalósuló elkövetések szempontjából a vegyes deliktumok közé sorolja. Leszögezendő, hogy utóbbi előbbinek nem speciális esete, mert a specialitás kizárólag az egymást az általános elemekben fedő tényállások kapcsolatában értelmezhető.[148] A specialitás esetében a jogalkotó az egyik bűncselekményi tényállásból további ismérvek megjelölésével kiemel egy másikat, amely folytán a két diszpozíció a generális és speciális viszonyába kerül egymással, a kettő közül pedig csupán a speciális bűncselekmény kerülhet megállapításra.[149] Mindkét tényállás eleme a jogtalan haszonszerzési célzat és a kár mint eredmény. Ugyanakkor a csalás más (a passzív alany) tévedésbe ejtésével vagy tévedésben tartásával valósulhat meg, míg az információs rendszer felhasználásával elkövetett csalás tényállásában nincs passzív alany, természetes személyek

[147] BH2019. 218.
[148] Kónya (szerk.), 2013, 1416.o.
[149] Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I., Budapest, 2019, ELTE Eötvös Kiadó, 476.o.

megtévesztése helyett a vagyoni károsodást az információs rendszer közvetlen felhasználásával, befolyásolásával okozzák.[150]

II.2. ÚN. VEGYES TÍPUSÚ DELIKTUMOK

Minden cselekmény, amely elkövetése az információs és kommunikációs technológiák, eszközök valamilyen fokú igénybevételével történik, ugyanakkor a technológia bárminemű jelenléte, felhasználása nélkül is megvalósítható/véghezvihető lenne, a vegyes deliktumok közé sorolható. Szathmáry Zoltán a vegyes deliktumok egy részéről tartalom-bűncselekményekként ír, más részüket közléssel elkövetett bűncselekményekként jelöli.[151] A tartalom-bűncselekmények közé sorolja a gyermekpornográfiát és a szerzői vagy szomszédos jogot sértő bűncselekményeket. Ugyanő a közléssel elkövetett bűncselekmények között említi a zaklatást, a becsületsértést, rágalmazást és a csalást. E dolgozatban részletesen a zaklatás és a gyermekpornográfia jelenségét, büntető törvénykönyvi tényállásait, gyakorlatát vizsgálom.

1) A vegyes deliktumok közül elsőként a zaklatás jellegű magatartásokkal és a zaklatás Btk.-beli tényállásával foglalkozom. A *zaklatás* kifejezés a hétköznapi szóhasználatban jelenthet zavaró, nyugtalanító, tolakodó és fenyegető magatartást, függetlenül annak módjától, gyakoriságától, illetve az ahhoz használt eszköztől.[152] Az olyan zaklató jellegű, ártó, támadó szándékos magatartásokat, amelyekben közrejátszik az információs és kommunikációs technológia, a nemzetközi szakirodalom egy része a 'cyberbullying' kifejezése alá vonja,[153] magyar megfelelője az 'online megfélemlítés'.[154] Ez az áldozatok fizikai integritását, emberi méltóságát, magánéletének védelmét sértő[155] ártalmas, káros vagy veszélyes tartalom készítését, terjesztését, vagy az azokhoz való hozzáférés lehetővé tételét foglalja magában, célja a sérelemokozás,[156] az áldozat önbecsülésének, méltóságának lerombolása.[157] Rendkívül szerteágazó módon kerülhet sor az online megfélemlítésre. Egyik tipikus példa az internetes zaklatás ('cyber-harassment'), amely a célpontra irányuló ismétlődő támadó kommunikációban jelenik meg. Az erőszak legfőképpen az áldozat pszichéjének sérelmét okozza,[158] az ilyen jellegű támadásokat jellemzően szorongás, pszichoszomatikus problémák, szégyenérzet követ, de nem ritkák a depressziós tünetek, a szuicid gondolatok sem.[159]Az online megfélemlítés egy ernyőfogalom, egyik tipikus formája, az online zaklatás ('cyber-harassment', a magyar szakirodalomban jellemzően 'stalking') mellett számos más deviancia

[150] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[151] Szathmáry, 2019, 195.o.
[152] Monori, 2016, 246.o.
[153] Meg kell jegyezni, hogy közel sincs egyetértés a szakírók között abban, hogy a 'cyberbullying' csupán az oktatási környezetben történő magatartásokat öleli fel, avagy azon túlmutatva a korosztálytól, illetve intézményi környezettől független, tágabb körű jelenség. E dolgozatban a 'cyberbullying' nem az iskolai környezetben megvalósuló viselkedési formákat jelöli. Lásd például Pongó Tamás 'cyberbullying' kérdésével foglalkozó tanulmányát, amelyben az iskolákban és az azokhoz tartozó környezetekben történő szándékos sérelemokozást értendő e fogalom alatt. A szerző az egységes meghatározásra irányuló javaslatába kifejezetten a 'diák, vagy iskolai alkalmazott által vagy annak sérelmére' fordulatot emeli be.
[154] Monori Zsuzsanna Éva: Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. In: In Medias Res. Folyóirat a sajtószabadságról és a médiaszabályozásról, 2016/2.sz., 246.o.
[155] Langos, Colette: Cyberbullying: The Shades of Harm. In: Psychiatry, Psychology and Law, 2015/22.sz., 19.o.
[156] Langos, 2015, 8.o.
[157] Langos, 2015, 18.o.
[158] E megállapítás alól kivételt képez a 'happy slapping' elnevezésű cselekmény, amely során fizikai erőszak közvetítése vagy arról készült felvétel eljuttatása történik a célpont részére azzal a céllal, hogy az elé tárt erőszakot indirekt fenyegetésként érzékeltetve megijesszék vagy megfélemlítsék. (Langos, 2015, 4.o.)
[159] Holt – Bossler, 2016, 15.o.

is tartozik ide.[160] Ezek bemutatására készült a mellékletben található áttekintő jellegű táblázat.[161] A táblázat az online megfélemlítés formáit angol nyelven sorolja fel, emellett magyarázatot ad a megvalósítás módjait illetően, valamint a magatartásokat „sérelem-skálán" elhelyezve megjelöli, hogy a cselekmények súlyossága és az általuk az áldozatnak okozott sérelem valószínűsége figyelembevételével szükségesnek látszik-e azok kriminalizációja.
Azon felül, hogy a jogalkotó állást foglal abban, hogy mely magatartások igényelnek büntetőjogi reakciót, felmerül az a kérdés is, hogy e kiterjedt cselekményi körből melyek szubszumálhatók egy, a magyar jogrendszerben már meglévő tényállás alá. A tág értelemben vett zaklatáson belül jelen dolgozat szempontjából azon magatartások jelentősek, amelyek elkövetése az internet közvetítésével valósul meg, és amelyek illeszkednek a Btk. különös részi tényállásai között szereplő valamely bűncselekmény keretei közé. A zaklatás tényállása (222. §) a Btk. XXI. fejezetében, az emberi méltóság és az egyes alapvető jogok elleni bűncselekmények között szerepel. A tényállás részletes és gazdag elemzést kapott jogirodalomban, ennek összefoglalására és a zaklatással kapcsolatos számos kérdés megvitatására (például egység-halmazati kérdések kifejtésére, a védett jogi tárgy részletes alkotmányjogi vonatkozásainak ismertetésére) jelen dolgozatban nem kerül sor. A tényállás csupán néhány jellemzője kerül bemutatásra, e rész fókuszában az online megfélemlítés hazai jogrendszerben való elhelyezése áll.
A zaklatás jogi tárgya a személy általános és legtágabb értelemben vett *magánszférája*. A e fejezetében található bűncselekmények a magánszféra számos nevesített aspektusát védik, így például a magántitkot, a levéltitkot, a magánlakást és a becsületet.[162] Az Alkotmánybíróság a 8/1990. (IV. 23.)[163] és az 56/1994. (XI. 10.) AB határozataiban[164] kifejtette, hogy a magánszférához való jog – amely ugyan a hazai alapjogi rendszerben nem nevesített mint alapjog – az emberi méltósághoz való jogból ered, annak szubszidiárius alapjoga. A jogalkotó alkotmányos eredetű cselekvési kötelezettségéből (ún. intézményvédelmi kötelezettség) adódóan, illetve kétségkívül a jogirodalom képviselőinek szorgalmazására és a társadalmi elvárások hatására döntött a zaklatás átfogó törvényi tényállásának kialakítása mellett.[165]
A 222. § két, egymástól jól elkülöníthető alapesetet tartalmaz. Passzív alanyként mindkét esetben a természetes személyek szerepelhetnek. Az (1) bekezdésben található az első alapeset, amelynél az elkövetési magatartás a háborgatás, az elkövetés módja pedig a rendszeresség vagy tartósság. A *háborgatás* alatt azon cselekvések értendők, amelyek révén az elkövető a sértettet nyugtalanítja, zavarja, életét megnehezíti, feldúlja azt.[166] Az Ambrus – Ujvári szerzőpáros szerint a rendszeresség elkövetési mód alatt előre nem meghatározható, de nagyobb számú, az alkalomszerűséget kizáró, hosszabb időintervallumon belül időről időre, akár nagyobb időközökkel is megszakítottan visszatérő elkövetés; a tartósság alatt pedig akár heteken át folytatott elkövetés értendő.[167] A cselekmény vagylagos célzata a megfélemlítés vagy a magánéletbe, mindennapi életbe való önkényes beavatkozás.
A (2) bekezdésben található második alapeset az elsőtől lényegesen különböző magatartással foglalkozik. A 222. § második bekezdésének célzata a félelemkeltés, amely első ránézésre az első alapeset célzatainak egyikével, a megfélemlítéssel egybevágónak tűnhet. Azonban a második alapesetben foglalt magatartás az első bekezdésben foglalttal ellentétben nem egy

[160] Pongó Tamás: Minek nevezzelek? – Avagy a *cyberbullying* magyar terminológiájának kérdései. In: Közjogi Szemle, 2018/2.sz., 9.o.
[161] Az 1. számú táblázat Colette Langos, Monori Zsuzsanna Éva és Parti Katalin munkái alapján készült.
[162] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[163] 8/1990. (IV. 23.) AB határozat, ABH 1990, 42, 44 – 45.
[164] 56/1994. (XI. 10.) AB határozat, ABH 1994, 312, 313.
[165] Ambrus – Ujvári, 2016, 424.o.
[166] Ambrus István – Ujvári Ákos: A zaklatás bűncselekményének gyermekévei. In: Magyar Jog, 2016/7-8.sz., 426.o.
[167] Ambrus – Ujvári, 2016, 427.o.

hosszabb folyamat eredményeképpen létrejövő érzelmi állapothoz vezet (megfélemlítés), hanem egymozzanatos fenyegető cselekmény megvalósításával félelmet vált ki. A második bekezdés a) pontjában személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével fenyeget az elkövető, a b) pontban azt a látszatot kelti, hogy más életét, testi épségét vagy egészségét sértő vagy közvetlenül veszélyeztető esemény következik be. A (3) bekezdés a minősített eseteket tartalmazza, amelyek bármely fordulathoz kapcsolódhatnak. A minősített esetek az elkövető és a sértett közötti családi, érzelmi kapcsolatra, illetve a c) pont révén hatalmi, befolyási helyzetre, a d) pont szerepeltetésével pedig hivatalos személy ilyen minőségére utalnak. Kiemelendő, hogy a zaklatás minden esetben magánindítványra büntethető.

Az online megfélemlítés szempontjából elsősorban az zaklatás tényállásának (1) bekezdése releváns, ugyanakkor meg kell jegyezni, hogy nem zárható ki a (2) bekezdésben foglalt magatartás révén megvalósuló félelemkeltés, illetve ezek együttes jelenléte sem. A zaklatás joggyakorlatában az emailek, SMS üzenetek küldése, a számos telefonhívás, személyes megkeresés, követés mellett a kiberbűnözés szempontjából jelentős újdonságként jelenik meg a közösségi oldalak felhasználása. Például aki azért hoz létre álnéven Facebook-profilt, mert más módon képtelen elérni a sértettet, és – miután az nem válaszol SMS-eire, nem veszi fel neki a telefont – az álprofil révén veszi fel a kapcsolatot a sértettel, szintén a tényállás első bekezdésében foglalt vétséget követi el.[168] Nem tipikus történeti tényállás mellett, ugyanakkor szemléletesen mutatja be az (1) bekezdés szubszidiaritását a Szekszárdi Törvényszék 2014-es határozata.[169] A döntés alapját képező történeti tényállás szerint a terhelt súlyos, másodfokon emberölés előkészülete bűntettének minősített cselekmények mellett különböző módokon megvalósította a zaklatás bűncselekményét is. Az elkövető a perbeli időszakban a többször fizikailag bántalmazta (rúgás, késsel bökdösés), emellett figyelte, követte a sértettet, számos alkalommal igyekezett kapcsolatba lépni vele telefonon és Facebook üzenetek útján. A sértett életét fenyegető szöveges üzenetek küldése megvalósítja a 222. § (2) bekezdésének a) pontjában foglalt magatartást, hiszen a „meg foglak ölni" és ennek különböző variációi alkalmasak voltak arra, hogy a megfenyegetett sértettben – különösen a zaklatást kísérő bántalmazó cselekményekre tekintettel – komoly félelmet keltsenek. A korábban említett szubszidiaritás miatt a terhelt ún. félelemkeltéssel megvalósuló zaklatás miatt felelt, amely látszólagos halmazatban áll a szintén megvalósult (1) bekezdésbe tartozó, háborgatást megvalósító magatartásokkal.

Az idézett joggyakorlat, de a hazai és nemzetközi jogirodalom alapján is látható, hogy a zaklatás tényállását alkotó cselekmények megnyilvánulási formái igen eltérőek lehetnek. A korábbi büntetőtörvény, a Büntető Törvénykönyvről szóló 1978. évi IV. törvény (a továbbiakban: korábbi Btk.) 176/A. § (1) bekezdése tartalmazta a *különösen mással, annak akarata ellenére telekommunikációs eszköz útján vagy személyesen rendszeresen kapcsolatot teremteni törekszik* elkövetési módot. A korábbi Btk. ezen tényálláshoz fűzött indokolása utal arra, hogy a telekommunikációs eszköz útján való elkövetés a zaklatás tipikus esetei közé tartozik, ennek ellenére a hatályos tényállás nem tartalmaz hasonló „fogódzót". E körben magyarázatként szolgálhat az, hogy a technológia folyamatosan fejlődik és ezzel párhuzamosan a társadalom kapcsolattartási szokásai formálódnak, változnak. Az online megfélemlítés vonatkozásában Parti Katalin arra figyelmeztet, hogy óvakodni kell a túlszabályozástól, és törekedni kell arra, hogy a tényállások kellőképpen absztraktak – s ezáltal a jövőbeli magatartások befogadására, kezelésére alkalmasak – legyenek.[170]

[168] A Kaposvári Törvényszék Kb.31/2014/19. sz. határozata.
[169] A Szekszárdi Törvényszék B.89/2013/55. sz. határozata.
[170] Parti Katalin: A megfélemlítés (bullying) szabályozása Magyarországon és külföldön. In: In Medias Res. Folyóirat a sajtószabadságról és a médiaszabályozásról, 2016/1.sz., 146.o.

2) A vegyes jellegű deliktumok közül a zaklató jellegű magatartások vizsgálata után a tartalom-bűncselekmények közé sorolható gyermekpornográfia jelenségével kapcsolatos egyes problémák bemutatása következik. Ahogyan a zaklatás esetében, úgy a jogirodalomban szintén magas fokon elemzett gyermekpornográfiát illetően sem cél a tényállás minden eleme és a hozzá kapcsolódó joggyakorlat teljes körű elemzése. Ehelyett a dolgozat utolsó érdemi része a gyermekpornográfia jelensége, illetve konkrét különös részi tényállása és a virtuális tér kapcsolatáról szól.

A *gyermekpornográfia* e dolgozatban több helyen említésre került. Egyrészt a felhasználók anonimitásának mint az internet egyik jellegzetességének letagadhatatlan szerepe van a hasonló cselekmények mindinkább gyakoribbá válásában. Másrészt szó volt arról is, hogy világszerte különösen nagy egyetértés övezi a gyermekpornográf tartalmak készítése, terjesztése és fogyasztása mögött álló személyek megbüntetését. Ebből arra lehetne következtetni, hogy a nemzetközi szintű egységes fellépést és a nemzetek jogrendszereiben nagyon hasonló – még ha nem is teljesen egyező – fogalomrendszer kialakítását a kiberbűnözésre egyébként igen jellemző akadályok nem fogják vissza. Ennek ellenére nincs egy olyan definíció, amely minden jogrendszerben egységesen iránymutatást jelentene abban, hogy milyen részletességgel, illetve mely minimális fogalmi elemekre kiterjedően érdemes szabályozást alkotni.

A gyermekpornográfia jelenségének megjelölésére e kifejezés helyett egyes szerzők a 'CEM' (Child Exploitation Material) vagy 'CSAM' (Child Sexual Abuse Material) terminológiát ajánlják. Ezek magyarul a gyermekek kizsákmányolását, illetve a gyermekek szexuális bántalmazását tartalmazó anyagokat jelentik, és a fogalmak előtérbe helyezését szorgalmazó szakírók szerint – amellett, hogy precízebben utalnak a jelenség megnyilvánulásaira – a 'gyermekpornográfia' kifejezéssel ellentétben kizárják bármiféle, a gyermek részéről történő beleegyezés sugalmazását.[171] A lényeget tekintve a *gyermekek kizsákmányolását tartalmazó anyagok* a kizsákmányoló tartalmak készítését, terjesztését, birtoklását jelentik. Szintén megjelenhet a 'grooming'[172], a szexuális kizsákmányolás és zsarolás. Mindez pedig az internet által, illetve az online környezettel valamilyen kapcsolatban valósul meg.[173] A *gyermekek szexuális bántalmazását tartalmazó anyagok* a gyermekek szexuális bántalmazásának információs és kommunikációs technológiák által lehetővé tett voltára, illetve az olyan szexuális bántalmazásra utalnak, amelyet gyermekek ellen az internet környezetén kívül követnek el, de amelyről készült tartalom később megosztás útján mégis az online térbe kerül.

Az egységes meghatározás és nemzetközi szabályozás hiányának egyik oka bizonyosan a *gyermek* fogalma körüli bizonytalanság, amelyet tovább bonyolít különböző gyermek-fogalmak *szexuális beleegyezés korhatárával*[174] való keveredése. Utóbbihoz viszonyítva a *gyermek* fogalom többé-kevésbé egységes, gyermek az a személy, aki a tizennyolcadik életévét nem töltötte be.[175] Ez alól bizonyos vonatkozásban nemzeti jogszabályok kivételt tehetnek és korábban nagykorúnak minősíthetik az adott személyt.[176] *Kiskorúként*

[171] Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. In: Infokommunikáció és jog, 2017/1.sz., 33.o.

[172] A 'grooming' során az online tér segítségével férkőznek a gyermekek bizalmába, így érve el azt, hogy később a gyermek könnyebben beleegyezzen szexuálisan kizsákmányoló cselekményekbe. (Clough, 2012, 381.o.)

[173] Broadhurst, Roderic: Child Sex Abuse Images and Exploitation Materials. In: Leukfeldt, Roger – Holt, Thomas (szerk.): Cybercrime: the human factor, 2019, Routledge, 3.o.

[174] A szexuális beleegyezés korhatára irányadó arra, hogy mely életkor alatt minősül törvénybe ütközőnek szexuális tevékenység folytatása. Magyarországon a szexuális cselekményekbe való beleegyezés korhatára a tizennegyedik életév.

[175] Lanzarote Egyezmény meghatározása.

[176] Az Gyermekek Jogairól Szóló ENSZ Egyezmény meghatározása.

megjelölve[177] minden olyan személy e fogalom alá tartozik, aki még nem töltötte be a tizennyolcadik életévét, de ehhez képest alacsonyabb korhatár (de minimálisan tizenhat év) is meghatározható.
A magyar büntetőtörvény 204. §-a gyermekpornográfia néven rendeli büntetni a hasonló cselekményeket.[178] A gyermekpornográfia esetében a nagykorúságtól-kiskorúságtól függetlenül a tizennyolcadik életévét be nem töltött személy a passzív alany. Védett jogi tárgya a gyermekek zavartalan szexuális fejlődése és a szexuális fejlődési folyamat tényéből fakadó korlátozott szexuális önrendelkezésük védelme.[179] A tényállás (7) bekezdése tartalmazza az elkövetési tárgyak, azaz a pornográf felvétel és pornográf műsor meghatározását. Az (1) bekezdés a) pontjában foglalt elkövetési magatartások külön alapesetet képeznek, ezek a megszerzés és a tartás. A megszerzés a felvétel bármilyen módon történő birtokba vételét jelenti, ide tartozhat a digitális bizonyítékok rögzítése szempontjából jelentős bizonyítási problémákat felvető[180] 'live streaming' is, amely a gyermekek szexuális kizsákmányolásáról, szexuális bántalmazásáról készült tartalom letöltés nélküli megjelenítését jelenti. A tartás folyamatos birtoklást jelent.
Ugyanezen bekezdés b) pontja magasabb büntetési tétellel fenyegeti a készítés, a kínálás és az átadás elkövetési magtartásokat. A készítés[181] felvétel bármely módon történő létrehozását jelenti, de nem vonatkozik a virtuális tartalmak készítésére, azaz nem valós események rögzítésére. Ezen alapesetet tekintve a készítés mellett a kínálás (a felvétel átvételére való eredménytelen felhívás) és az átadás (a felvételnek azt megszerezni kívánó fél tényleges birtokába adása) szerepel.[182]
Az első bekezdés c) pontja tartalmazza a gyermekpornográfia tényállásának leginkább súlyos eseteit.[183] A forgalomba hozatal a felvételek felhasználhatóságának a személyek pontosan meg nem határozható köre számára való elérhetővé tételt jelenti. A nagy nyilvánosság számára hozzáférhetővé tétel elkövetési magatartása utóbbinál annyiban enyhébb cselekvést feltételez, hogy ennél nincs lehetőség a felvételek letöltésére, sokszorosítására vagy továbbítására, csupán azon megtekintésére. A kereskedés haszonszerzési célú, rendszeresen történő forgalomba hozatalt jelent. A (4) bekezdés a pornográf műsorban való szereplésre felhívást és szerepeltetést szabályozza, megkönnyítve a jogalkalmazás feladatát például a 'live streaming' és más olyan formák beazonosításával kapcsolatban, amelyek során nem történik felvételrögzítés. Az (5) bekezdés a) pontja a pornográf felvételen való szereplésre felhívást, b) pontjában a részvételt, illetve a c) pontban anyagi eszközök szolgáltatását vonja e körbe.

---

[177] Budapesti Egyezmény meghatározása.
[178] A 'grooming' jelensége a Dornfeld – Mezei szerzőpáros elemzése szerint a Btk. 198. § (2) bekezdésében kapott helyet. A szexuális visszaélés e formáját az a tizennyolcadik életévét betöltött személy követi el, aki tizennegyedik életévét be nem töltött személyt arra törekszik rábírni, hogy vele vagy mással szexuális cselekményt végezzen. (Dornfeld – Mezei, 2017, 33.o.)
[179] Nagykommentár (Karsai Krisztina szerk.), Wolters Kluwer Jogtár (online)
[180] A Dornfeld – Mezei szerzőpáros szerint a kizárólagosan megtekintéses szolgáltatást nyújtó gyermekpornográf tartalmakat elérhetővé tévő internetes oldalakon az ilyen tartalmak megtekintése megállapíthatóságához a látogatás szándékosságát és a tartalomról való tudomást kell bizonyítani. A szándékosságra és a tudomásra a látogatás gyakoriságából, illetve a tartalmak megtekintéséért szolgáltatásként fizetésből lehet következtetni. (Dornfeld – Mezei, 2017, 34.o.)
[181] A 204. § (5) bekezdésének a) pontja a készítéshez kapcsolódóan nevesített előkészületi magatartást tartalmaz, amely a passzív alanynak pornográf felvételen való szereplésre felhívásával valósul meg.
[182] A 204. § (1) bekezdésének b) pontjában foglalt három elkövetési magatartáshoz kapcsolódó minősített esetet tartalmaz a szakasz (2) bekezdése, amely az elkövető és a sértett közötti családi, érzelmi, hatalmi-befolyási viszonyra épül.
[183] A 204. § (3) bekezdése a felvétel készítéséhez, forgalomba hozatalához vagy kereskedelméhez kapcsolódó sui generis bűnsegédi cselekményt foglal magában az *anyagi eszközök szolgáltatása* révén. Ugyanezen szakasz (6) bekezdése utóbbi elkövetési magatartások elkövetéséhez szükséges vagy azt könnyítő feltételek biztosítását – mint előkészületi magatartás – vétségként szankcionálja.

A tényállás rendkívül szerteágazó magatartásokat hivatott szankcionálni. Látható, hogy a magyar szabályozásban széles körben került sor a gyermekeket érintő szexuális kizsákmányolás formáinak kriminalizációjára. A problémakörből egy konkrét jelenséget kiemelve e ponton a *megszerzés* és *készítés* elkövetési magatartásával kapcsolatos, a közelmúltban hangsúlyt kapott 'sexting' kérdéskörének vizsgálata következik.

E kifejezés sok más online környezettel kapcsolatos fogalomhoz hasonlóan több mindent jelenthet. Egyrészt a konszenzuson alapuló szexuálisan provokatív, saját készítésű kép- vagy videofelvételek, illetve szexuális tartalmú üzenetcserére utalhat,[184] de jelentheti, illetve előkészítheti azt a magatartást is, amely során az elkövető – további képfelvételek megosztása érdekében – a már birtokában lévő tartalmak megosztásával fenyegetőzik (más néven 'sextortion', szexuális tárgyú zsarolás).[185] A 'sexting' – amely tehát magában foglalhatja a szöveges üzenetek mellett szintén szexuális tartalmú kép- vagy videofelvételek készítését, majd ezek más személyeknek való elküldését – nem ritka a tizennyolc éven aluli, de már szexuális beleegyezési korhatárt betöltött személyek között. Elviekben gyermekpornográfia miatt büntethető lenne az a tizennyolcadik életévét be nem töltött személy is, aki szexuális tartalmú felvételeket *szerez meg* vagy *készít* egy tizennyolc éven aluli személyről.[186]

A témát illetően az egyik internetes híroldal gyermekpornográfiáról szóló cikkével kapcsolatosan fejtette ki álláspontját Gyurkó Szilvia gyermekjogi szakértő. Gyurkó szerint[187] a tizennégy és tizennyolc év közötti fiatalok körében a szexuális tartalmú képek egymással való megosztása a „normális párkapcsolat, az elköteleződés része", és mivel a jogalkotó a *megszerzés* és *tartás* elkövetési magatartásokat nem e cselekményi körre szabta, ezért a birtoklással (*megszerzés*) kapcsolatban a dekriminalizációt tartaná megfelelőnek. A kérdésben Ambrus István ellentétes álláspontra helyezkedett. Véleményében[188] kifejtette, hogy a jogalkalmazó az ún. teleologikus értelmezés alkalmazásával jogosult felmentő ítéletet hozni egy olyan esetben, amikor a hasonló jellegű cselekmények társadalomra veszélyesség hiányában nem valósítják meg a gyermekpornográfia bűncselekményét. Gelányi Anikó a témával kapcsolatban utal arra, hogy ugyan valóban szükséges konkrét korhatárt meghatározni a gyermekpornográfia passzív alanyaira vonatkozóan, paradoxnak tartja az a helyzetet, hogy a tizennyolcadik életévüket be nem töltött – tehát a gyermekpornográfia szempontjából passzív alanynak minősülő –, de a szexuális beleegyezés alsó határát meghaladó korú személyek szexuális cselekményeket végezhetnek egymással, ugyanakkor erről bármilyen felvétel készítése törvénybe ütköző magatartásnak minősül.[189]

Véleményem szerint a kérdésnek leginkább elméleti síkon van jelentősége. Nem tűnik életszerűnek, hogy a jogalkalmazó elé kerüljenek azok a tizennyolc éven aluli személyek által egymással kölcsönösen megosztott, szexuális tartalmú felvételek, amelyekkel a készítést követően nem éltek vissza, tehát például nem küldték tovább harmadik személynek, illetve nem osztották meg azokat a közösségi média felületein. A dekriminalizáció ellen szól, hogy a

---

[184] Holt – Bossler, 2016, 188.o.

[185] Dornfeld – Mezei, 2017, 33.o.

[186] A kérdéshez kapcsolódóan meg kell jegyezni, hogy a gyermekpornográfiáról szóló rész bevezetőjében megjelölt meghatározások forrásai között a Budapesti Egyezmény lehetőséget ad arra, hogy – az egyezmény szóhasználatában – kiskorúak életkorát a gyermekpornográfiával kapcsolatos bűncselekmények esetében (minimálisan) tizenhat évben lehessen meghatározni.

[187] https://tldr.444.hu/2020/08/01/ha-a-pedofilok-nyilvantartasa-a-csodafegyver-akkor-miert-nem-vetettek-be-eddig.
utolsó letöltés dátuma: 2020.10.28.

[188] https://444.hu/2020/08/22/szexkepeket-kuldozgeto-kamaszok-mihez-kezdjen-veluk-a-torveny?fbclid=IwAR2oK1HoEXMJcoasKMyAM_N19lmHw23M0Zc3Q46J-5yBtJ-Bh4B0rxytsZM.
utolsó letöltés dátuma: 2020.10.28.

[189] Anikó, Gelányi: An examination of effective regulations against illegal pornographic materials and the possible alternatives for the prevention of and fighting against such crimes. In: Selected essay of Facultaty of Law University of Pécs, 2009, 91.o.

gyermekpornográfia tényállásának *megszerzés* elkövetési magatartása magában foglalhat olyan esetet is, amelyek során az elkövető olyan felvételek birtokába jut, amelyek a rajtuk szereplő személy tudta, beleegyezése nélkül készültek, illetve konszenzus megléte esetén a felvétellel való visszaélés következtében kerültek hozzá. Ezt támasztja alá Clough általános jellegű megállapítása, mely szerint a gyermekpornográf tartalmak gyártását a piac igényei alakítják, amennyiben pedig a birtoklás is szankciókkal fenyegetett magatartás, úgy a hasonló tartalmak birtoklása iránti igény csökkenhet, a piac szűkülhet, összességében pedig kevesebb gyermeket érhet el a szexuális kizsákmányolás.[190]
A kiberdevianciák közül a kriminológia és szociológia művelői között különös figyelmet kap a szexuális jellegű online tevékenység, így a gyermekpornográf tartalmak megtekintésére, gyermekekkel való szexuális tartalmú kommunikációra irányuló cselekmények is. A kitüntetett figyelem oka abban áll, hogy a technológia és az internethálózat széles körű elérhetősége nagyban megkönnyítette a hasonló tartalmak készítését, megosztását és megtekintését,[191] a kibertérbeli anonimitás pedig megnehezítette az elkövetők azonosítását és felelősségre vonását. A hasonló tartalmak kereskedelme jövedelmező üzlet, jellemzően szervezett bűnözői csoportok is részt vesznek a terjesztésben,[192] amely alátámasztja a bűnelkövetési lánc minden lépése és az elkövetők körének minden szereplője elleni összehangolt nemzetközi fellépés fontosságát.[193]

III. RÉSZ – ZÁRÓ GONDOLATOK

A kiberbűnözés jelentős társadalmi hatással bír, legyen szó akár a szerzői jogi bűncselekményekről, adathalász tevékenységről, amelyek kiemelkedő gazdasági kárt okozhatnak; avagy a magánszféra integritását fenyegető zaklatásról, az egyén anyagi biztonságát veszélyeztető csalásról; nem utolsó sorban a társadalom következő generációinak szocializációját, lelki egészségét romboló internetes zaklatásról vagy gyermekpornográfiáról.
A folyamatos technikai fejlődés újabb és újabb veszélyhelyzeteket hoz felszínre, szüntelenül új elkövetési felületek és metódusok jelennek meg, büntetőjogi reakciót vonva maguk után.[194] Véleményem szerint a jelenleg hatályos Btk. tényállások megfelelően fedik le az online tér bűncselekményeit, tehát a tényállások bővítése a kiberbűnözés markánsan új formáinak megjelenése esetén lenne indokolt. Esetlegesen érdemes lehet egy önálló különös részi fejezetbe foglalni a kibertér bűncselekményeit, legalábbis azon bűncselekményi tényállások tekintetében, amelyek a dolgozatban mint hálózat-bűncselekmények kerültek bemutatásra. E körben megjegyezhető az is, hogy a 375. § tekintetében az elektronikus készpénz-helyettesítő fizetőeszközzel való visszaéléssel megvalósuló alakzatot érdemes lenne leválasztani a szakasz első négy bekezdése alkotta károkozó adatvisszaélésről, és utóbbi cselekményt a „tiszta" kiberbűncselekményekkel egy helyen szabályozni.
A büntetőjog eszközei csak részét képezik azoknak az intézkedéseknek, amelyek segíthetnek a kibertér védelmének megteremtésében és biztonságának megőrzésében. A kiberbűnözés elleni védekezésben kiemelt szerepe van az államnak. Ez teendők sorát jelenti a tájékoztatástól kezdve az állami infrastruktúrák rendszerei védelmének biztosításán át a bűnüldözés és a jogalkalmazás felkészítéséig. A dolgozatban utaltam azon kihívásokra,

[190] Clough, 2010, 252.o.
[191] Holt – Bossler, 2016, 8.o.
[192] Mezei, 2019, 140.o.
[193] Clough, 2011, 677.o.
[194] Szathmáry Zoltán: Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban, Budapest, 2012, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 181.o.

amelyekkel bűnüldözésnek meg kell küzdenie, ideértve a digitális bizonyítékok megőrzésének problémáját. Különösen fontos lenne a nyomozást végző személyek folyamatos felkészítése, hiszen a digitális bizonyítékok megőrzésének szükségessége nem csupán a hálózat-bűncselekmények esetében, de a vegyes bűncselekmények nyomozása során is egyre gyakoribbá válik.[195] Emellett érdemes biztosítani a jogalkalmazásban részt vevők képzését is. A kiberbiztonságot megteremtő eszközrendszer része maga az egyén is. A körültekintő internethasználat a kiberbiztonságra törekvés megnyilvánulhat abban is, hogy jelentjük a minket ért jogsértéseket – különösen az online megfélemlítés különböző formáit –, hozzájárulva a kiberbűnözés valós kiterjedésének megismeréséhez. A egyéni felhasználók belátása nagymértékben hozzájárulhat társadalom nagyobb fokú tudatosságához.
A legtöbb nemzetnek ugyan eltérő büntetőszabályai vannak az egyes kiberbűncselekményeket illetően,[196] a kulturális különbségekből és hagyományokból adódóan nem minden cselekmény vált ki széleskörben azonos reakciót. Az olyan cselekmények esetében, amelyek szabályozása államonként nagymértékben eltér, bonyolultabbá válik a joghatósági problémák kezelése, a nyomozási hatáskörök elosztása, valamint lassul az információcsere. A kiberbűnözés globális jellegét újra aláhúzva megállapítható, hogy az egyes országok szervei közötti nagyfokú együttműködés, a szabályozás harmonizációja és a tudományos eredmények megosztása azért is kívánatos lenne, mert a fejlett világ államainak nagy része nagyon hasonló kihívásokkal[197] küzd, így más államok és szervek tapasztalatai hasznosnak bizonyulhatnak akármelyik nemzet számára.

[195] Clough, 2012, 370.o.
[196] Wall – Williams, 2007, 401.o.
[197] Clough, 2011, 672.o

MELLÉKLET

1. táblázat

A támadási forma megnevezése	**A támadási forma leírása**	**Büntetőjogi reakció szükségessége**
Happy Slapping	Fizikai erőszak közvetítése vagy arról készült felvétel eljuttatása a célpont részére azzal a céllal, hogy az elé tárt erőszakot indirekt fenyegetésként érzékeltetve megfélemlítsék.	Szankció bevezetése egyértelműen indokolt.
Denigration (szexuális jellegű képfelvétel, videofelvétel)[198]	Befeketítés, azaz a hírnév rontására alkalmas képfelvétel vagy videófelvétel megosztása, terjesztése.	
Cyber-stalking	A zaklatás súlyos, esetleg hírnévrontással kombinálódó formája. Az enyhébb formájú zaklatás az áldozat felé egyre intenzívebb fenyegetések révén alakul súlyos formává, amelynek következtében a célpont személyes biztonságát kezdi félteni.	
Masquerading/ Impersonation	Személyiséglopás vagy profillopás, azaz az elkövető egy másik, létező személy online profiljában jelenik meg, és a nevében hírnevének rontására alkalmas üzeneteket küld harmadik személyeknek.	Indokoltnak látszik a kriminalizáció, azonban a jogalkotónak egy esetleges szankcionálás során figyelemmel kell lennie a cselekmények egyedi vonásaira.
Outing and Trickery	Az elkövető, az áldozat bizalmába férkőzve ráveszi,	

[198] A 'cyberbullying' körében számos szexuális tartalommal kapcsolatos deviancia is jelen van. A szerteágazó jelenség ismertebb elemei a következők.
Az 'RSA' ('recorded sexual assault) rögzített szexuális bántalmazást jelent, a szexuális erőszaktevők az általuk az erőszakról készített kép- vagy videofelvétel nyilvánossá tételével fenyegetik meg az áldozatot arra az esetre, ha az az őt ért erőszak miatt hatóságokhoz fordulna. A 'sexting' magatartásáról korábban már volt szó. Ezzel rokon a 'nonconsensual pornography', azaz másik személy beleegyezése nélkül, de akár konszenzus alapján készített, megosztott szexuális tartalmak konszenzus nélküli (további) megosztása. Ennek nem haszonszerzési, hanem személyes jellegű célból, például a bosszúállás céljából véghezvitt alfaja a 'revenge porn'(bosszúpornó), amely esetében bármely, szexuális jellegű tartalmat az azon szereplő személy ellehetetlenítése, megalázása végett bizonyos körben nyilvánosságra hoznak. Hazánkban hasonló tényállásnál a bíróság kimondta, hogy a szexuális szokások, a nemi identitás és azezek körébe tartozó tények az intim szféra részét képezik, s azoknak nagy nyilvánosság elé tárása a sértett személyiségi jogát, emberi méltóságát sérthetik, ezért alkalmas lehet a becsület csorbítására, s a rágalmazás vétségének megvalósítására (EBH 2013. B.21.)

	hogy személyes információkat osszon meg vele, amelyeket később a megalázás céljával publikussá tesz.	
Indirect threat	Olyan fenyegetés, amely egy egyszeri fizikai sérelem bekövetkezését helyezi kilátásba. (A súlyosabb formájú zaklatáshoz képest különbségként emelendő ki, hogy utóbbinál a fizikai sérelemmel fenyegetés rendszeres, az indirekt fenyegetésnél pedig alkalmi jellegű.)	
Denigration (nem szexuális jellegű, sértő képfelvétel, videofelvétel)	Befeketítés, azaz a hírnév rontására alkalmas képfelvétel vagy videófelvétel megosztása, terjesztése.	
Harassment (hosszú távon)	A zaklatás enyhébb formája, amely során a célpontnak támadó, bántó jellegű üzeneteket küldenek.	
Denigration (kizárólag szövegesen, hosszú távon)	Befeketítés, azaz a hírnév rontására alkalmas szöveg (pletyka, szóbeszéd) megosztása, terjesztése.	
Harassment (rövid távon)	A zaklatás enyhébb formája, amely során a célpontnak támadó, bántó jellegű üzeneteket küldenek.	Szankcionálásuk során különös figyelemmel kell eljárni, e formák nem valósítanak meg súlyos jogsértést.
Denigration (kizárólag szövegesen, rövid távon)	Befeketítés, azaz a hírnév rontására alkalmas szöveg (pletyka, szóbeszéd) megosztása, terjesztése.	
Exclusion (hosszú távon)	Kiközösítést, online csoportból való kirekesztést jelent.	
Exclusion (rövid távon)	Kiközösítést, online csoportból való kirekesztést jelent.	Szankció nem szükséges.
Denigration (kizárólag szövegesen, egy-egy elszigetelt eset)	Befeketítés, azaz a hírnév rontására alkalmas szöveg (pletyka, szóbeszéd) megosztása, terjesztése.	

BIBLIOGRÁFIA

Monográfiák és tanulmányok

Ambrus István: Digitalizáció és büntetőjog, Budapest, 2021, Wolters Kluwer

Andresen, Martin A. – Farrell, Graham (szerk.): The Criminal Act. The Role and Influence of Routine Activity Theory, London, 2015, Palgrave Macmillan

Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia, Budapest, 2018, Wolters Kluwer

Brenner, Susan W.: Cybercrime and the law. Challenges, issues and outcomes, 2012, Lebanon, Northeastern University Press

Broadhurst, Roderic: Child Sex Abuse Images and Exploitation Materials. In: Leukfeldt, Roger – Holt, Thomas (szerk.): Cybercrime: the human factor, 2019, Routledge

Clough, Jonathan: Principles of cybercrime, Cambridge, 2010, Cambridge University Press

Anikó, Gelányi: An examination of effective regulations against illegal pornographic materials and the possible alternatives for the prevention of and fighting against such crimes. In: Selected essay of Facultaty of Law University of Pécs, Pécs, 2009, Studia Iuridica Auctoritate Universitatis Pécs Publicata

Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I., Budapest, 2019, ELTE Eötvös Kiadó

Holt, Thomas J. – Bossler, Adam M.: Cybercrime in Progress. Theory and prevention of technology-enabled offenses, New York, 2016, Routledge

McGuire, Michael: Hypercrime: the new geometry of harm, New York, 2007, Routledge - Cavendish

Mezei Kitti: Szervezett bűnözés az interneten. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika, 2019, Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont

Mezei Kitti: A kiberbűnözés aktuális kihívásai a büntetőjogban, L'Harmattan – TK JTI, Budapest, 2020

Nagy Zoltán András: Bűncselekmények számítógépes környezetben, Budapest, 2009, Ad Librum

Szathmáry Zoltán: Az internet mint a bűncselekmények elkövetésének helye. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika, 2019, Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont

Ződi Zsolt: Platformok, robotok és a jog. Új szabályozási kihívások az információs társadalomban, Budapest, 2018, Gondolat Kiadó

Folyóirat-cikkek

Ambrus István – Ujvári Ákos: A zaklatás bűncselekményének gyermekévei. In: Magyar jog, 2016/7-8. sz., Budapest

Ambrus István: Büntetőjog 2021. A pénzmosás újrahangolt tényállása és a hálapénz kriminalizálása. In: Büntetőjogi Szemle, 2020/2.sz.

Zsolt, Bederna – Tamás, Szadeczky: Cyber espionage through Botnets. In: Security Journal 2020/33.sz.

Buono, Lavriero: Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. In: ERA Forum, 2016/17.sz.

Brenner, Susan W. – Clarke, Leo L.: Distributed security: preventing cybercrime. In: John Marshall Journal of Computer and Information Law, 2005/4.sz.

Clough, Jonathan: Cybercrime. In: Commonwealth Law Bulletin, 2011/37.sz.

Clough, Jonathan: The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World. In: Criminal Law Forum, 2012/23.sz.

Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. In: Infokommunikáció és jog, 2017/1.sz., Budapest

Knoops, Bert-Jaap: The Internet and its Opportunities for Cybercrime. In: Tilburg Law School Legal Studies Research Paper Series, 2011/9.sz.

Langos, Colette: Cyberbullying: The Shades of Harm. In: Psychiatry, Psychology and Law, 2015/22.sz.

Maimon, David – Louderback, Eric R.: Cyber-Dependent Crimes: An Interdisciplinary Review. In: Annual Review of Criminology, 2019/2.sz.

Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In: Magyar jog, 2019/5.sz., Budapest

Kitti, Mezei – Zoltán, Nagy: Organised Cybercrime Groups and Their Illicit Online Activities. In: Studia Iuridica Auctoritate Universitatis Pécs Publicata, 2016/154.sz., Pécs

Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. In: Pro Futuro, 2018/1.sz., Debrecen

Monori Zsuzsanna Éva: Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. In: In Medias Res. Folyóirat a sajtószabadságról és a médiaszabályozásról, 2016/2.sz., Budapest

Nagy Zoltán András: A számítógépes környezetben elkövetett bűncselekmények új szabályozásáról. Háttér és elemzés. In: Ügyészek Lapja, 2014/3-4.sz., Budapest

Parti Katalin: A megfélemlítés (bullying) szabályozása Magyarországon és külföldön. In: In Medias Res. Folyóirat a sajtószabadságról és a médiaszabályozásról, 2016/1.sz., Budapest

Parti Katalin: A számítógépes bűnözés és az internet. In: Kriminológiai Tanulmányok, 2003/40.sz., Budapest

Peszleg Tibor: Az adatbűnözés és gazdasági hatásai. In: Infokommunikáció és jog, 2009/3.sz., Budapest

Pongó Tamás: Minek nevezzelek? – Avagy a *cyberbullying* magyar terminológiájának kérdései. In: Közjogi Szemle, 2018/2.sz., Budapest

Sorbán Kinga: Információs rendszer és adatok megsértése, avagy vírusok, férgek és trójai falovak a büntető törvénykönyvben. In: Belügyi Szemle – Ordinem Facere, 2018/1.sz, Budapest

Wall, David S. – Williams, Matthew: Policing diversity in the digital age: Maintaining order in virtual communities. In: Criminology & Criminal Justice, 2007/4.sz.

Yang, Debra Wong – Hoffstadt, Brian M.: Countering the Cyber-Crime Threat. In: American Criminal Law Review, 2006/43.sz.

Yar, Majid: The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory. In: European Journal of Criminology, 2006/2.sz.

Zavrsnik, Ales: Cybercrime Definitional Challenges and Criminological Paricularities. In: Masaryk University Journal of Law and Technology, 2008/2.sz.

Jogforrások

2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról

2012. évi C. törvény a Büntető Törvénykönyvről

2005. évi XCII. törvény az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és szexuális zaklatás elleni védelméről szóló Egyezménye kihirdetéséről, valamint ezzel összefüggésben egyes törvények módosításáról

2004. évi LXXIX. törvény az Európa tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

1991. évi LXIV. törvény a Gyermek jogairól szóló, New Yorkban, 1989. november 20-án kelt Egyezmény kihirdetéséről

1978. évi IV. törvény a Büntető Törvénykönyvről

A Tanács 2019. május 17-i 2019/796 rendelete az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0796&from=EN

Az Európai Parlament és a Tanács 2013. augusztus 12-i 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/22/1B tanácsi kerethatározat felváltásáról
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013L0040&from=EN

Az Európa Tanács egyezménye a gyermekek védelméről a szexuális kizsákmányolás és bántalmazás ellen (Lanzarote Egyezmény, 2007. október 25.)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1d2

Az Európa Tanács Budapesten, 2001. november 23-án kelt Egyezménye Számítástechnikai Bűnözésről (Budapesti Egyezmény, 2001. november 23.)
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

A Gyermek Jogairól Szóló, New Yorkban, 1989. november 20-án kelt Egyezmény (Gyermekjogi Egyezmény, 1989. november 20.)
https://www.unhcr.org/hu/wp-content/uploads/sites/21/2016/12/AGyermekjogairolszoloegyezmenyNewYork1989.pdf

Egyéb

AB határozatok:

8/1990. (IV. 23.) AB határozat, ABH 1990, 42 – 45.
56/1994. (XI. 10.) AB határozat, ABH 1994, 312 – 315.

Bírósági döntések:

BH2019. 218.
BH2017. 392.
EBH 2013. B.21.
Kúria Bhar.I.537/2017/5. sz. határozata
Fővárosi Ítélőtábla Kbf.28/2016/5. sz. határozata
A Kaposvári Törvényszék Katonai Tanácsának Kb.26/2015/12. sz. határozata
A Szekszárdi Törvényszék B.89/2013/55. sz. határozata

Kommentárok:

Kónya István (szerk): Magyar büntetőjog I-IV. Kommentár a gyakorlat számára („Kapcsos kommentár”), Budapest, 2013, HVG-Orac, II. kötet

Karsai Zsuzsanna (szerk.): Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, Wolters Kluwer Jogtár (online)

Jelentések:

McGuire, Mike – Dowling, Samantha: Cyber crime: A review of the evidence. Chapter 1: Cyber-dependent crimes. In: Home Office Research Report 75, 2013 1-34
utolsó letöltés dátuma: 2020.02.11.

Doktori értekezések:

Mezei Kitti: Büntetőjogi válaszok az informatikai kihívásokra, Pécs, 2019, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola

Szathmáry Zoltán: Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban, Budapest, 2012, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola

Internetes oldalak:

https://eur-lex.europa.eu/
https://dictionary.cambridge.org/
https://internetworldstats.com/ utolsó letöltés dátuma: 2020.10.28.
https://444.hu/2020/08/22/szexkepeket-kuldozgeto-kamaszok-mihez-kezdjen-veluk-a-torveny?fbclid=IwAR2oK1HoEXMJcoasKMyAM_N19lmHw23M0Zc3Q46J-5yBtJ-Bh4B0rxytsZM utolsó letöltés dátuma: 2020.10.28.
https://tldr.444.hu/2020/08/01/ha-a-pedofilok-nyilvantartasa-a-csodafegyver-akkor-miert-nem-vetettek-be-eddig utolsó letöltés dátuma: 2020.10.28.

MTA Law Working Papers

Kiadó: Társadalomtudományi Kutatóközpont (MTA Kiválósági Kutatóhely

Székhely: 1097 Budapest, Tóth Kálmán utca 4.

Felelős kiadó: Boda Zsolt főigazgató

Felelős szerkesztő: Kecskés Gábor

Szerkesztőség: Hoffmann Tamás, Mezei Kitti, Szilágyi Emese

Honlap: http://jog.tk.mta.hu/mtalwp

E-mail: mta.law-wp@tk.mta.hu

ISSN 2064-4515