Volume XIX no. 1 (34)

A cyberdevianciáról

PRAZSÁK Gergő PhD
Eötvös Lóránd University of Sciences
prazsak@gmail.com

Abstract: Cyberdeviance
The study discusses the phenomenon of cyber deviances. It examines the conceptual classification of cyber deviancies, and the processes linked to cyber victim, cyber perpetrator, cyber control, and cyber law enforcement roles in practice. Cyber deviancies (cyber bullying, cyber terrorism, social engineering, phishing, etc.) are analyzed in the light of theories of cyber psychology, communication theory, deviance theory, cyber anthropology and cyber criminology. The discussed delinquencies in cyber space also require special legal regulations (self-regulation, central regulation). The aim of the study, beyond the systemization of cyber deviancies, is to contribute to the prevention of victimization of cyber-induced delinquencies.

Keywords: *uncertainty; cyber psychology; diffusion; cybercrime; dark web*

Amikor 16 évvel ezelőtt közpolitikai munkát végezve elkezdtem foglalkozni az információs társadalom magyarországi kiépítésének lehetőségeivel, még szinte fel sem merült, hogy veszélyeket rejt magában az információs infrastruktúra és azzal együtt az információs társadalom kibontakozása. Igaz, akadtak óvatosabb hangok is, de elsősorban mégis a hálózat gyors és széleskörű kiépítése, valamint a digitális írástudás növelése volt az elsődleges cél. Amikor a 2007/2008-as tanévben az ELTE TáTK Kisebbségszociológia tanszékén *Jón, rosszon túl a kibertérben* címmel kutatószemináriumot hirdettem, akkor még elsősorban filozófiai, metafizikai megközelítésekre építkeztünk. A legjelentősebb nietzschei, heideggeri, foucault-i filozófiai, metafizikai gondolatkörökre támaszkodva azt tárgyaltuk, hogy milyen nehézségekbe ütközik a posztmodern, elektronikus körülmények között devianciáról beszélni. Azért természetesen szóba került William Gibson *Neurománc* című sci-fije is, meg aztán Sigmund Freud nagy ívű kultúra elmélete is. A kurzus utolsó óráján Suler és Phillips 1998-ban megjelent *The Bad Boys of Cyberspace - Deviant Behavior in*

Multimedia Chat Communities című tanulmányáról volt szó. Ebben egy betűszóra leegyszerűsítve (SNERT[1]) jelent meg a cybertér azon deviánsainak csoportja, akik a szerzők szerint inkább fiúk, mint lányok, akik kamaszok (vagy legalábbis regresszált felnőttek). Az online térben megfigyelhető devianciák a szerzők véleménye szerint visszavezethetők a rendszer technikai paramétereire éppen úgy, mint az ebből kialakuló rendszerspecifikus viselkedési szokásokra, normákra, az online tér ismerős és ismeretlen területeire. A *kulturális különbségeket*, a *vandalizmust* ugyancsak olyan devianciaként azonosították a szerzők, amelyek a cybertérben is megjelennek. Mindezzel együtt úgy tűnt, hogy ekkoriban a szerzők valamiféle grundhoz hasonlították a cyberteret, ahol kamasz fiúk kisebb-nagyobb súlyú csínytevéseit lehetett megfigyelni.

Azután 2011/2012-es tanév őszi félévétől ugyancsak az ELTE TáTK-n, a Nemzetközi tanulmányok és a Társadalmi tanulmányok BA szakokon Információs társadalom előadássorozatot tartok. Az *anonimitás* a kezdetek óta – jóllehet változó „formában" – egy-egy előadás témáját képezi. Az *anonimitás* mellett megjelenik a *deindividuáció*, az *elszemélytelenítés*, a *tömegjelenségek*, az *integrált* és *integrálatlan* személyiségek problémakörei is, amelyek különböző online devianciákhoz vezetnek, így például a *bullying*-hoz és a *flaming*-hoz. Már az első évektől kezdve lényegesnek tartottam, hogy konkrét adatokkal rendelkezzünk ezen antiszociális online magatartások kiterjedtségéről, arról, hogy mekkora problémát jelentenek ezek a cselekedetek. Így találtam rá az egyesült államokbeli Minneapolisban található PACER's National Bullying Prevention Center, valamint a National Center for Educational Statistics felméréseire. A felmérés adatai szerint 2015-ben a közel 25 millió 12-18 éves tanuló közül mintegy 5 millió volt zaklatás áldozata (20.8%), azaz minden ötödik tanuló. Közülük több mint 2,5 millióan online zaklatás áldozatai voltak. Az adatok szerint mind az online mind az offline térben történő zaklatás szempontjából a lány tanulók veszélyeztetettebbek. Körükben közel 23 % a valamilyen színtéren zaklatottak aránya, és 16% a cyber bullying áldozatainak aránya. Etnikai származás szerint a fehérek és a spanyolajkúak kevésbé, míg a többi etnikum magasabb arányban lesz zaklatás áldozata. Az életkor, az iskolai osztály előre haladtával valamelyest csökken a zaklatások aránya. Ugyanez a helyzet a család jövedelme mentén is: a szegényebb családból származók gyakrabban bullying áldozatok. A zaklatott gyerekek közül a legtöbbjüket évente 1-2 alkalommal zaklatják, de a gyerekek mintegy 5 százaléka számolt be arról, hogy napi szinten zaklatják társai. Alig minden második zaklatási esetben fordulnak segítségért felnőtthöz a gyerekek (43%). A fiatalabbak közül többen (60%), míg a legmagasabb osztályokba járók közül már kevesebben (12%) teszik ezt. Rendkívül lényeges, hogy a kutatás adatai szerint a cyberbullying és más devianciák együtt járnak. Azok a 12-18 éves iskolás gyerekek, akik olyan iskolába járnak, ahol van *gang*, magasabb arányban cyberbullying áldozatok. Azok, akik

[1] "snot-nosed Eros-ridden teenager"

láttak fegyvert az iskolában ugyancsak magasabb arányban számoltak be cyberbullyingról. A *drogok*, az *alkohol* és a *gyűlölet grafitik* iskolai jelenléte ugyancsak jelentősen növeli annak az esélyét, hogy az iskolás gyerek a cyberbullying áldozatává váljon. Ne gondoljuk azt, hogy a fegyver jelenléte kifejezetten amerikai jelenség, és napjaink Magyarországán nincs ilyenről szó, mert az csak a messzi vadnyugat tartozéka. A hírek beszámolói szerint ilyen „vadnyugati" helyek napjaink Magyarországán is előfordulnak (és nem csak a nagyobb városokban vagy a fővárosban).

A felmérés, amely szűk, hiszen csak gyerekek körében végzett vizsgálat, egyértelműen rámutat arra, hogy az offline és az elektronikus térben történő zaklatás szempontjából a hátrányos helyzetű gyerekek veszélyeztetettebbek: a szegényebbek, a színes bőrűek, a kiszolgáltatottak. Egyfelől azért, mert *kevesebb erőforrásuk* van, és ezért kevésbé tudják megvédeni magukat, másfelől pedig azért, mert *kevésbé készítik fel őket* a lehetséges veszélyhelyzetekre. Tehát a prevenció kevésbé éri el őket, még akkor is, ha a nagyobb világnyelveken könnyen elérhetők a prevenciós tartalmak.[1]

Az idősorosan is elérhető adatok elemzése alapján egyértelmű, hogy a téma egyre jelentősebb, ezért egyre nagyobb mértékben kell vele foglalkoznunk. Más témájú, vidéken végzett kutatásaim során is találkoztam azokkal a társadalmi problémákkal, amelyek mind az elkövetővé mind az áldozattá válás szempontjából lényegesek. Természetesen a téma nem csak és kizárólag a fiatalokat érinti, ráadásul az idősebbeket sem csak a fiatalokon keresztül közvetve. Ma már még az EU kevésbé fejlett országaiban is többen vannak azok, akik valamilyen eszközön keresztül belépnek a cybertérbe, mint azok, akik nem. Így semmi különös nincs abban, hogy az online térben történő „mozgás" során egyre nagyobb mértékben van jelen a deviancia. Ezért is támogattam, hogy átfogó tanulmánykötet készítésébe kezdjünk Parti Katalin és Kiss Tibor kollégáimmal a cyberdevianciáról. Ennek a napokban megjelenő tanulmánykötetünknek a főbb megállapításaira utalnék a következőkben.

A Dialóg Campus Kiadó gondozásában megjelenő kötetünk három nagyobb részből áll. A kötet meta-elméleti keretét a *kommunikáció*, az emberi lét nyelvi meghatározottságai, a *csoport és normaképződés*, az *újdonságok* és *terjedésük* vizsgálata jelenti. A tankönyvnek is készült kötetünk ezen részében áttekintjük azokat a kommunikációs modelleket, amelyek különböző szempontok szerint leírják a kommunikáció egészét. A látszólag kevésbé innovatív és viszonylag rövid leírások célja, hogy rámutassunk azokra a devianciaformákra, amelyek eltérnek (esetleg „megsértik") a különböző kommunikációs modellek szerinti folyamatokat. Így például a kommunikáció *szociálpszichológiai modellje* azt vizsgálja, hogy a kommunikációban résztvevő felek, hogyan győzik meg

[1] Érdemes ebből a szempontból a Youtube-on kipróbálni a „cyberbullying" keresőszót. Szerencsére már magyar nyelvű tartalom is akad, de azért van hova fejlődni....

egymást (Csepeli, 2005). A *szociálpszichológiai hagyomány* szerint a kommunikáció az interperszonális befolyásolás folyamata, s értelemszerűen az elmélet is erre a jelenségre vonatkozik. A modell annak vizsgálatára lehet alkalmas, hogy *ki, mit, kinek, hogyan, milyen szándékkal* mond, közöl. Az interperszonális befolyásolás, a másik befolyásolása szükségszerűen a kommunikáció része. Másfelől, amennyiben ez a befolyásolás *nem szabad kommunikáció* útján, hanem erőszakkal történik, etikai és szociális értelemben rendkívül problémás helyzetről van szó. Az információs társadalom körülményei között megjelenő devianciák elemzése szempontjából a *kommunikáció szociálpszichológiai modellje* jól alkalmazható azokban a helyzetekben, amikor valaki *erőfölényével akar visszaélni*, s egy-egy gyanútlan felhasználót csapdába csalni.

A kommunikáció *matematikai modelljében* annak vizsgálatáról van szó, hogy az információt minél nagyobb hatásfokkal, minél gyorsabban és pontosabban juttassák el egymáshoz a kommunikációban résztvevő felek (Shannon és Weaver, 1949, 7). Mégpedig azért, hogy az információhiányból adódó *bizonytalanságot* csökkentsék. Ebben a kommunikációs modellben teljesen lényegtelen, hogy mi az információ. Lényegtelen, hogy milyen etikai minősítéssel értelmezhető az információ. Az viszont nagyon is lényeges, hogy kiszámítható a csatornazaj *nagysága*, az átvitt információ *mennyisége*, amelytől nem független annak *minősége*. Természetesen ebben a modellben is adódhatnak gondok, hiszen lehetséges például a csatornát *szándékosan* zajjal zavarni, esetleg az információkhoz jogosulatlanul hozzáférni. A *rendszerintegritás elleni bűncselekmények* sorolhatók abba a kategóriába, amelyek a kommunikáció matematikai modelljének segítségével jól elemezhetők.

A kommunikáció *retorikai modell*jében viszont nagyon is lényeges a tartalom. A különböző politikai, társadalmi rendszerekben a közügyek intézésére hivatott fórum által is meghatározott a retorika alkalmazhatósága (Habermas, 1971). Hálózatelméleti terminológiát használva demokráciákban *skálafüggetlen*, míg diktatúrákban *csillaghálózat* a rendszer architektúrájának a jellemzője. Az információs társadalom körülményei elsősorban skálafüggetlen jellemzőkkel írhatók le (Barabási, 2013). Így aztán az ettől való eltérés deviáció, deviancia. Ebből a szempontból elsősorban olyan devianciákra kell gondolnunk, amelyek például a hálózathoz való hozzáféréssel függnek össze (bizonyos országokban korlátozottak az interneten elérhető tartalmak). Továbbá a nyilvánosság és a cyberdeviancia kapcsolatának elemzése szempontjából lényeges a *dark* ill. a *deepweb*.

A *szemiotikai értelmezés* szerint a kommunikáció elméleti megközelítése a jelek tudománya. A szemiotikai kommunikációelméletre példaként Jakobson (1969) kommunikációs modellje hozható fel. Jakobson számára Shannon és Weaver matematikai modelljéhez képest azonban sokkal lényegesebb a *kontaktus,* a *kapcsolat,* illetve az, hogy ez milyen *kulturális közegben* jön létre. Ez utóbbit Jakobson *kontextusnak* hívja; kulturális relativista modellje e köré szerveződik. A kontextus

voltaképpen a valósággal való összefüggést jelöli. A kontextus (félre)értelmezéséből természetesen számos probléma adódhat, amelyek ugyancsak a devianciák megjelenésének lehetséges terepei az online világban is. Sőt, azt mondhatjuk, hogy a szemiotikai megközelítés szerint maga a *bizonytalanság* (a jelek és jelentések okozta bizonytalanság) jelenti a deviációk elsődleges forrását.

A kommunikáció, mint a társadalmi világ szerkesztésének egyik eszköze, a szemiotikai modellhez képest fordított megközelítést használ. A *szociokulturális megközelítés* megfordítja a jel és a jelölt közötti kapcsolatot. A szociokulturális megközelítés azt feltételezi, hogy a jelölt a jel által teremtődik meg. A jelölt a jel által olyan, amilyen. Leegyszerűsítve ez a Chicago Egyetem két nyelvészének az elmélete, amelyet a két kutató nevével szokás Sapir–Whorf-hipotézisként fémjelezni. A Sapir–Whorf-hipotézis szerint a kultúra tagjainak gondolkodását az általuk használt nyelv szerkezete formálja (Sapir 1961, Whorf 1956). Griffin az angol *you* szót hozza példaként. Azokon a nyelveken, ahol van hivatalos, magázó formula (például német) két külön szóval fejezzük ki: *du* és *Sie,* és a kettő közötti átváltásra, azaz a helyzet intimebbé, kevésbé formálissá válására még egy „ünneplő" szavuk is van – nevezi meg ezen a módon a német *Bruderschaft* szót Griffin (2003, 43). Ennek a csúcsát talán a japán nyelv jelenti. „A japán nyelvben tíz különböző megszólítás lehetséges, a nemtől, a kortól és a beszélő helyzetétől függően – melyek mindegyikét az angol *you* jelöli, holott az eredeti nyelvben egyik sem cserélhető fel a másikkal" (Griffin, 2003, 43). Az online világban azonban legnagyobb mértékben az angol nyelv használata terjedt el, ahogy arra pl. a különböző nyelvű Wikipedia oldalak száma utal (Prazsák, 2017). Az angol azonban – ahogy a japán példa esetében is láthattuk – nem alkalmas minden olyan elem kifejezésére, amely más nyelveken viszont elemi jelentőségű. Ez pedig félreértésekhez és devianciához is vezethet egy-egy közösségen belül.

A *kommunikáció társadalomkritikai elmélete* elsősorban a frankfurti iskola tagjainak munkásságára vezethető vissza. Az iskola attól kritikai, hogy bírál minden egyenlőtlen, egyenlőtlenségeket termelő, autoriter helyzetet, rendszert. A frankfurti iskola tagjainak kritikai elméleti megközelítései a nyelvben is létező, történelmileg igazságtalan helyzetekre hívják fel a figyelmet. A kommunikáció társadalomkritikai elemzése ugyancsak hasznos eszközként szolgálhat a cybertérben megjelenő deviáns viselkedések elemzése során, hiszen bizonyos online csoportok normáktól való eltérése a nyelvhasználatban is tetten érhető. Az *extrémizmus* par excellence ebbe a kategóriába tartozik.

Végül meg kell említenünk a kommunikáció *fenomenológiai* modelljét (Rogers, 1961). A cél a mindennapi élet megértése: annak a beleérző *megértése,* amit a másik ember átél. Ez a pszichológiai folyamat voltaképpen arra irányul, hogy a másik embert megértsük, hogy a másik ember megélje a „megértettséget". A kommunikáció fenomenológiai modellje ennek a pszichológiai megértési folyamatnak a vizsgálatát jelenti.

Carl Rogers pszichiáter tevékenységét hozhatjuk példaként, aki pácienseivel való kapcsolatfelvételei, személyes tapasztalatai alapján fogalmazta meg elméletét, miszerint a *feltétel nélküli pozitív odafordulás,* valamint az *empátia* jelenti a fenomenológiai értelemben vett kommunikációelmélet legfontosabb elemét. A megértés nem valósulhat meg kommunikáció nélkül. Ebben az értelemben a fenomenológia kifejezetten kommunikációkutatás. A kommunikáció ezen alapvetően pszichológiai modellje elsősorban proszociális indíttatású. Ezzel a helyzettel azonban nyilvánvalóan vissza is lehet élni, amellyel gyakran operálnak a *cyberbullying* elkövetői.

Könyvünkben a kommunikációs modellekből levezethető devianciatípusok bemutatása után, Tönnies nyomán a *közösség* és a *társadalom* társulási formáinak megkülönböztetéseit tárgyaljuk. A kisebb és nagyobb csoportokba rendeződő emberiség a *modernizáció*, a *racionalizáció*, a *szekularizáció* folyamatainak a következtében egyre inkább az *individualizáció* felé halad. Az individualizáció önmagában az online tér olyan jellemzője, amely a devianciák kialakulásának bölcsője. Természetesen kérdéses, hogy egy szélsőségesen individualizált társadalmi állapotban milyen szabályokról beszélhetünk (egyáltalán beszélhetünk-e szabályokról). Ebből a szempontból azonban lényeges, hogy még a legszélsőségesebben individualizálódott társadalmi berendezkedésben is társas lények mozognak az online térben, hajtanak végre *e-akciókat* (Negroponte, 2002). Legalábbis megközelítésünknek ez egy központi axiómája. Hiszen abban az esetben, ha egy *erős mesterséges intelligencia* nézőpontjából tekintünk a cyberdevianciára – egyáltalán az e-akciókra – akkor vizsgálataink, megállapításaink egy jelentős részét újra kell gondolni. Mint ahogy nem is oly soká – éppen ezen ok miatt – elavulttá is válhat kötetünk. Elavulttá, hiszen ha az online térben létrejövő teljes *összekapcsoltság*, a *dolgok internete* és a *datafikáció* következtében megjelenő erős mesterséges intelligencia szcenárió kerül fölénybe, akkor nyilvánvalóan az online tér szabályai is annak függvényében alakulnak majd. Szerzőtársaim egyike gyakorlati bűnüldöző múlttal is rendelkezik (Kiss Tibor), másikuk pedig a kriminológia tudományában járatos (Parti Katalin), ezért aztán sokat támaszkodtunk munkánk során napi gyakorlatukra, tudásukra.

Lényeges, hogy a gyakorlat felől érkező kolléga is van köztünk, hiszen az elektronikus körülmények között elkövetett bűncselekmények felgöngyölítése kifejezetten olyan tevékenység, amelynek során *naprakésznek* kell lenni mind a technológiával, mind a technológiára épülő normasértő tevékenységekkel kapcsolatban. Kriminológiai értelemben pedig rendkívül fontos, hogy mind az elkövetői, mind az áldozati oldal jogi szabályozása munkánk részét képezze, hiszen amennyiben minden online akció mögött valamilyen emberi cselekedetet feltételezünk, akkor innen, az emberi (offline) világból történik ezek minősítése is. Erről pedig jogi értelemben a jogszabályok gondoskodnak.

Természetesen nem minden deviancia antiszociális, üldözendő, a közösség számára káros tevékenység. Éppen ezért tárgyaljuk Everett Rogers nyomán a terjedést, az újdonságok terjedését.

> A diffúzió az a folyamat, amelynek során egy innováció az idő múlásával számos kommunikációs csatornán elterjed a társadalmi rendszerben. A kommunikáció különleges formájáról van szó, amelyben az üzenet kifejezetten az innovációról szól. A kommunikáció olyan folyamat, amelynek során a résztvevők információkat hoznak létre és osztanak meg egymással a kölcsönös megértés érdekében"
>
> Rogers, 2003, 45

Azt is megjegyzi Rogers, hogy a diffúzió voltaképpen nem más, mint a kommunikáció egy különleges típusa, amelyben a résztvevő felek információkat cserélnek ki egymással az *újdonsággal*, az *új* ötlettel (innovációval) kapcsolatban. Az „újdonság" azt jelenti, hogy bizonyos mértékű bizonytalanság van a diffúziós folyamat során – emeli ki Rogers. „A bizonytalanság annak a mértékét jelenti, hogy egy esemény kimenetelével kapcsolatos alternatívák számának percepciója, illetve az alternatívák relatív valószínűsége mekkora" (Rogers, 2003, 46). Miközben egyre több és több információ áll a rendelkezésünkre – amely ugye elviekben csökkenti a bizonytalanságot – mégis éppen a *bizonytalanság* az információs korszak rendkívül fontos jellemzője, egyben a devianciák megjelenésének egyik kiváltó oka. Az interneten való közlekedésnek – összehasonlítva a fizikai világban való mozgással – egyik legfontosabb ismérve az a *bizonytalanság*, amely abból adódik, hogy nincsenek stabil és egyértelmű, negropontei értelemben (2002) vett „útjelző táblák", amelyekhez minden felhasználónak szükségszerűen igazodnia kellene. Ebben az értelemben a terjedés során szükségszerűen megjelenő bizonytalanság az egész rendszer alapvető működési jellemzője, s azon keresztül hat a társadalmi berendezkedésre. Napjaink társadalmi berendezkedésének leírására ezért is használják gyakran s joggal a *bizonytalanság* szót, amely például Hankiss Elemér szerint sokkal nagyobb mértékben van jelen az elmúlt két évtizedben, mint korábban bármikor. Még annak ellenére is ezen az állásponton van, hogy bizonyos szerzők szerint maga a bizonytalanság az emberi lét szükségszerű jellemzője volt korábban is, manapság is az, s lesz a jövőben is (Hankiss, 2011). A bizonytalanságot nem mindenki állja. Az innovátorok (a társadalom alig 3 %-a) jellemzője, hogy rendkívül jól tűrik a bizonytalanságot. Ezek az emberek újítanak, meghallják a közösség szükségleteinek „hangját", amelyre választ keresnek. Úgy gondolkodnak a közösséggel együtt, hogy közben nagyon is „feltaláló" attitűdjük van, már-már kívülálló, fura alakok. Ők is deviánsak, akik olyan tevékenységet végeznek, amely egyáltalán nem üldözendő, nem bűncselekmény. Sőt, bizonyos innovációra épülő kultúrákban éppen hogy becsben tartják a közösség ezen tagjait (Florida, 2002).

Mindezek miatt a cyberdevianciáról szóló összefoglaló munkánkból nem maradhattak ki azok a definíciók sem, amelyek a használt fogalmakról szólnak. Már csak azért sem, mert önmagában sem egyértelmű a használt terminológia. Így például, ahogy azt Leukfeldt remekül bemutatja, a cyberbűnözés terminológiája magában foglalhatja a „virtuális", „cyber" vagy „kiber", a „computer" vagy „számítógépes", „számítástechnikai", az „e-", „internet-" vagy „digitális", valamint az „információs" elnevezéseket (Leukfeldt, 2016, 214). Cyberbűncselekménynek vagy *cybercrime*-nak nevezzük azokat a bűncselekményeket, amelyek az információs térrel, információs technológiával esszenciális kapcsolatban állnak (például hacking, digitális adatok megsértése). Továbbá az olyan cselekmények is cyberbűncselekménynek tekinthetők, amelyek nem kifejezetten információstechnológia-fókuszúak, de attól mégsem függetlenek, tekintettel arra, hogy megvalósításukhoz nélkülözhetetlenek az informatikai eszközök (ilyen például az online elkövetett csalás, a nigériai levél, a *phishing*, vagy az online terjesztett gyermekpornográfia). Már ebből a felsorolásból is sejthető, hogy éppen úgy, ahogy az offline világban rendkívül szerteágazók, a társadalmi, gazdasági, politikai élet minden területén megfigyelhetők a normasértések, bűncselekmények, úgy az online térben sincs ez másként. Ezért aztán rendkívül lényeges, mind az online devianciák, mind a cyberbűncselekmények szempontjából ezeknek az internetes, számítógépes bűncselekményeknek a csoportosítása. Kötetünkben ezt a feladatot is elvégezzük, mégpedig az online e-akciók kategorizálásával. A csoportosításokat, definíciókat a nemzetközi szakirodalom maximális figyelembe vételével, annak átvételével közöljük. Nem is tehetünk másként, hiszen például az informatikai bűncselekmények jellemzői a *gyorsaság*, a *magas látencia*, az *intellektuális jelleg* mellett a *nemzetköziség*. A deviancia manapság nem csak és kizárólag egy színteret érint. Azaz elképzelhető, hogy egy deviáns cselekedet az offline térben kezdődik és a cybertérben fejeződik be. Esetleg fordítva. Minden olyan esetben cyberdevianciáról beszélhetünk, amikor a normasértés folyamata – akármelyik stádiumában – érinti a cyberteret. További jellemző, hogy maga után vonja a kontrollintézmények reakcióját, ön- ill. közveszélyes, a széleskörűen elfogadott magatartásmintákhoz képest kisebbségben van. Lényeges, hogy a megvalósítója *digitális kompetenciával* rendelkezik. A cyberdeviancia motivációi – tekintettel arra, hogy emberi mozgatók állnak mögötte – az *agresszió* (flaming, becsületsértés, zaklatás, zsarolás, kényszerítés, fenyegetés). A motivációk egy másik csoportját a *szexuális szükségletek* jelentik: szexuális tartalmak, szexting, behálózás, zaklatás, szexuális zsarolás (sextortion). A motivációk harmadik csoportját pedig a *haszonszerzés* jelenti. Ennek egyik formája az információs rendszerek elleni támadás (adatok megszerzése, rendszerintegritás elleni támadások). A másik az illegális kereskedelem (illegális szerek, eszközök kereskedelme, adóelkerülés). Végül egy sajátos típust jelent, amikor egyszerűen „csak" információközléssel, kommunikációval valósul meg a haszonszerzés. Könyvünkben külön alfejezetet szentelünk a motivációk egy sajátos körének: az

extrémizmusnak, a terrorizmusnak, a cyberterrorizmusnak: „A szélsőséges közösségek és a terrorszervezetek normasértései elvont ideológiák mentén, közvetett vagy közvetlen módon, valós vagy módosított képi anyag (videó, szöveg, gif, internetes mém stb.) tartalmakkal vagy aktív kommunikációban megnyilvánuló, közösség irányából közösség irányába ható károkozó cselekvések összességét foglalja magában. Sérthet információs rendszereket, de fizikai erőszakként hagyományos térben is végződhet." A terrorszervezetek alapvető célja a rettegés és a félelemkeltés. Az ilyen típusú célokat számos eszközzel igyekeznek megvalósítani: *program alapú vírusokkal, terheléses támadásokkal* vagy *pszichológiai manipulációval (social engineering*). Külön kategóriát jelentenek ebből a szempontból azok az e-akciók, amelyek a terrorszervezetek részéről a *toborzással*, *együttműködés megvalósításával*, *ideologizálással*, *erőszak alkalmazásával* és *terjesztésével* függnek össze. Az informatikai bűncselekményeket alapvetően két módon szokás szabályozni. Az egyik, hogy önálló ágazati törvényeket alkotnak ennek a speciális területnek a szabályozására, amely biztosítja a büntetőeljárási együttműködést, a bizonyítékok szabályszerű rögzítését, megőrzését és bíróság előtti felhasználását – ilyen például az Egyesült Királyságban az 1990-ben hatályba lépett „számítógépes visszaélés törvény" (Computer Misuse Act). A másik megoldás, ha meglévő büntetőkódexekbe iktatnak be önálló, a számítástechnikai rendszer és az adatok integritását védő tényállásokat – ez történt például Németországban 1986-ban a büntető törvénykönyv (Strafgesetzbuch) felülvizsgálata során. Magyarország az utóbbi kategóriába tartozik – még a korábbi, 1978. évi Büntető Törvénykönyv gazdasági bűncselekmények fejezetébe kerültek, elsőként (1994-ben) a számítástechnikai csalás; majd a számítástechnikai rendszerbe való jogtalan behatolással, bennmaradással és a belépést lehetővé tevő technikai intézkedés kijátszásával kapcsolatos tényállások (2002-ben).

Erre már ugyan a tanulmány elején utaltunk, de lényeges külön szót ejtenünk az áldozati csoportokról. Nyilvánvalóan az elsődleges áldozati csoportok a védekezni nem tudók, a kevesebb anyagi, kulturális, társadalmi erőforrásokat mozgósítani képest csoportok. Így a gyermekek és a fiatalok, a Z generáció. Ők mind a cyberbullying, mind a szexuális kizsákmányolás gyakoribb áldozatai. A szexuális zsarolás (sextortion) és a bosszúpornó (revenge porn) áldozatai inkább a nők, mint a férfiak. A gyerekeken és a nőkön kívül a harmadik leginkább veszélyeztetett csoportot az idősek jelentik, akik gyakran válnak phishing áldozataivá.

Könyvünk utolsó fejezete a cybertér szabályozásáról szól. Arról, hogy milyen eszközökkel védekeznek az előbbiekben (is) megjelölt problémák ellen az online térben. Alapvetően két nagyobb megközelítés létezik. Az egyik az önszabályozásra, míg a másik az államok, kormányok által lefektetett szabályokra, központi szabályozásokra helyezi a hangsúlyt. Az előbbi szereplői jellemzően magánvállalatok, ipari szereplők, akadémiai kutatóintézetek. Az utóbbi esetben közigazgatási és kormányzó szervekről van szó. Ők inkább reagálnak, mintsem megelőznek. A proaktív szerep inkább az

önszabályozásra hárul. Ez esetben kevésbé jogszabályok, mint inkább etikai kódexek, információ-megosztás, káros tartalmak szűrése, tudatosság növelés az alkalmazott eszközök. A központi szabályozás eszközei ezzel szemben többnyire jogi eszközök, így az igazságszolgáltatás, a nyomozás. Könyvünkben lényegesnek tartottuk mind az önszabályozás, mind a központi szabályozás eszközeinek ismertetését, elemzését. Rendkívül fontos, hiszen számos problémába ütközünk, amikor ezek használatáról gondolkodunk. Egyfelől a cyberdeviancia, a cyberbűncselekmények nem állnak meg az országhatároknál. Ezért megfelelő eszközre van szükség a visszaszorításuk során. Másfelől lényeges, hogy a használt eszköz arányos legyen, ne korlátozza az információkhoz való hozzáférést, a véleménynyilvánítás szabadságát. Ezeket a kérdéseket mind-mind tárgyaljuk az idén megjelenő *Cyberdevianca* című kötetünkben.

BIBLIOGRÁFIA

BARABÁSI, Albert, László. 2013. *Behálózva – A hálózatok új tudománya*, Budapest, Helikon Kiadó.

CSEPELI, György, 2005. *A meghatározatlan állat*, Budapest, Jószöveg.

FLORIDA, Richard, 2002. *The Rise of the Creative Class: And How It's Transforming Work, Leisure, Community and Everyday Life*, New York, Perseus Book Group.

FREUD, Sigmund, 2014. *Rossz közérzet a kultúrában*, Budapest, Kossuth Kiadó.

GIBSON, William, 1999. *Neurománc,* 2. Kiadás, Budapest, Valhalla Páholy Kft.

GRIFFIN, Em, 2003. *Bevezetés a kommunikációelméletbe,* Budapest, Harmat Kiadó.

HABERMAS, Jürgen. 1971. *A társadalmi nyilvánosság szerkezetváltozása*, Budapest, Gondolat Kiadó.

HANKISS, Elemér. 2011. *Életstratégiák a bizonytalanság korában.* TEDX-előadás. Elérhető: https://www.youtube.com/watch?v=evw2qQRQziM&vl=hu (letöltés: 2019. március 2.)

JAKOBSON, Roman. 1969. *Hang, jel, vers*, Budapest, Gondolat Kiadó.

KISS, Tibor, PARTI, Katalin, PRAZSÁK, Gergő, 2019. *Cyberdeviancia*, Budapest, Dialóg Kiadó (megjelenés alatt).

LEUKFELDT, Rutger. 2016. *Cybercriminal Networks. Origin, Growth and Criminal Capabilities,* Portland, Eleven International Publishing.

National Center for Educational Statistics, 2016 december, *Student Reports of Bullying: Results From the 2015 School Crime Supplement to the National Crime Victimization Survey*, https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2017015 (letöltés: 2019. március 2.)

NEGROPONTE, Nicholas, 2002. *Digitális létezés.* Budapest, Typotex Kiadó.

PACER's National Bullying Prevention Center, https://www.pacer.org/bullying/resources/cyberbullying/

PRAZSÁK, Gergő, 2017. A virtuális tömegek bölcsességén innen és túl, *Symbolon*, 18 (32), p. 5-16.

ROGERS, Everett, 2003. *Diffusion of Innovations.* 5th Edition. iBooks. New York–Toronto–Sydney–Singapur, Free Press.

ROGERS, Carl, 1961. *On becoming a Person*, Boston, Houghton Mifflin.

SAPIR, Edward, 1961. *Culture, Language and Personality,* [Selected Essays. ed.: Mandelbaum, David G.] Berkeley–Los Angeles, University of California Press.

SHANNON, Claude és Weaver, Warren, 1949. *The mathematical theory of communication. Urbana and Chicago, University of Illionis Press.* Urbana and Chicago, University of Illionis Press. Elérhető: http://raley.english.ucsb.edu/wp-content/Engl800/Shannon-Weaver.pdf (letöltés: 2019. március 2)

SULER, John és Phillips, Wendell, 1998. The Bad Boys of Cyberspace - Deviant Behavior in Online Multimedia Communities and Strategies for Managing it, *CyberPsychology and Behavior*, I. (3) p. 275-294.

TÖNNIES, Ferdinand, 2004. *Közösség és társadalom.* Budapest, Gondolat Kiadó.

WHORF, Benjamin, 1956. *Language, Thought and Reality*, [Selected Writings. ed.: Carroll, John B.] New York–London, MIT–J.Wilky–Chapinaon & Hall.