Cyberdeviancia

KISS TIBOR
PARTI KATALIN
PRAZSÁK GERGŐ

Dialóg Campus

CYBERDEVIANCIA

Vákát oldal

Kiss Tibor – Parti Katalin – Prazsák Gergő

CYBERDEVIANCIA

Dialóg Campus Kiadó ❖ Budapest 2019

A kiadvány a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó közszolgálat-fejlesztés”
című projekt keretében jelent meg.

Szerzők fejezetek szerint:

Prazsák Gergő: 1. fejezet
Kiss Tibor: 2. fejezet, kivéve 2.6. alfejezet
Kiss Tibor – Parti Katalin: 2.6. alfejezet
Parti Katalin: 3. fejezet

A szerkesztésben közreműködött:

Giricz Anna

Szakmai lektorok:

Rab Árpád
Z. Karvalics László

Tartalom

Rövidítések jegyzéke

ABM: Agent-based Modeling / résztvevőalapú modellezés
APC: Association for Progressive Communication / Progresszív Kommunikáció Szövetség
BIK: Better Internet for Kids
CCTV: Closed Circuit Television / zárt láncú televíziós megfigyelési rendszer
CERT: Computer Emergency Response Team
COC: Cybersecurity Operations Centre
CPNI: Centre for the Protection of National Infrastructure
CSI: Crime Scene Investigation
CSIRT Network: Computer Security Incident Response Network
DNS: Domain Name System
DRI: Digital Rights Ireland
DSM: Diagnostic and Statistical Manual of Mental Disorders / Mentális rendellenességek kórmeghatározó és statisztikai kézikönyve
ECJ: European Court of Justice / Európai Bíróság
EFF: Electronic Frontier Foundation
EFTA: European Free Trade Association / Európai Szabadkereskedelmi Társulás
EJEB: Emberi Jogok Európai Bírósága
EJEE: Az emberi jogok európai egyezménye
EJENY: Az emberi jogok egyetemes nyilatkozata
ENSZ: Egyesült Nemzetek Szervezete / UN: United Nations
ESS: European Social Survey
EVS: European Values Study
FBI: Federal Bureau of Investigation / Szövetségi Nyomozó Iroda
FOMO: Fear of Missing Out / kimaradástól való félelem
GST: General Strain Theory / általános feszültségelmélet
IANA: Internet Assigned Numbers Authority
ICANN: Internet Corporation for Assigned Names and Numbers
IGF: Forum / Internetszabályozó Fórum
IKT: Infocommunication Technologies / infokommunikációs technológiák
IMMA: International Mass Media Agency
INHOPE: Internet Hotline Providers in Europe Association
IoT: Internet of Things / dolgok internete
IRB: Információs Rendszerek Biztonsága (irányelv)
ISPA: Internet Service Providers Association
IT: Information Technology / információs technológia
ITI: Information Technology Industry Council
LAD: Language Aquisition Device
MELANI: Swiss Reporting and Analysis Centre for Information Assurance
MMS: Multimedia Messaging Service / multimédiás üzenetküldési szolgáltatás

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság
NCSC: National Cyber Security Center / Nemzeti Kiberbiztonsági Központ
NCTSO: National Counter Terrorism Security Office
NGO: non-governmental organization / nem kormányzati szervezet
NMHH: Nemzeti Média- és Hírközlési Hatóság
NSA: National Security Agency / Nemzetbiztonsági Ügynökség
NSF: National Science Foundation / Nemzeti Tudományos Alapítvány
NSFNET: National Science Foundation Network / Nemzeti Tudományos Alapítvány Hálózat
OECD: Organisation for Economic Co-operation and Development / Gazdasági Együttműködési és Fejlesztési Szervezet
PPDM: Privacy Preserving Data Mining / magánéletbarát adatbányász
PPJNE: A polgári és politikai jogok nemzetközi egyezségokmánya
PPP: Public Private Partnership
RE: római egyezmény
RFID: Radio Frequency IDentification / rádiófrekvenciás azonosítás (technológia)
SIC: Safer Internet Centres / biztonságosabb internetközpontok
SMS: Short Message Service / rövidüzenet-szolgáltatás
SSD: Solid-state drive /félvezetős memóriát használó adattároló eszköz
TASZ: Társaság a Szabadságjogokért
TISN: Trusted Information Sharing Network for Critical Infrastructure Protection
WGIG: Working Group on Internet Governance / Internetszabályozó Munkacsoport
WHO: World Health Organization / Egészségügyi Világszervezet
WP29: Article 29 Working Party / (az európai adatvédelmi irányelv) 29. cikk által létrehozott munkacsoport

Előszó

Az elektronikus kommunikációs eszközök megjelenése az egyéni és társadalmi élet egyetlen színterét sem hagyta érintetlenül. Megváltozott a társadalmi együttélés egésze, sőt a társas/társadalmi életnek ma már nemcsak az ember-ember, hanem az ember-gép, a gép-gép interakciók is részét képezik. Az internetre költözött társadalom jelenségei új társas együttélési formákat, új szabályokat, új környezetet és a szabályoktól való új típusú deviációkat hoztak létre. Jelen kötetünkben ezeket a változásokat mutatjuk be, és röviden felvázoljuk a legkorszerűbb kommunikációs technológiák okozta társas kihívások értelmezési lehetőségeit.

A következő oldalakon megjelenő kutatások, definíciók az antropológián, a pszichológián, a szociálpszichológián, a szociológián, a kriminológián túl számos egyéb természettudományos területtel érintkeznek. Az újítások, illetve azok terjedése adja kötetünk azon objektív keretét, amely lehetővé teszi a szabályok és a devianciák jelenségkörének értelmezését. Nem kerülhetjük meg az internetes/online kommunikáció megjelenésének történeti bemutatását, amely jól illeszkedik abba a kommunikációtechnológiai változássorozatba, amellyel voltaképpen bemutatható a *zóon politikon* története. A big data alapú mesterségesintelligencia-rendszerek napjainkban indultak hódító útjukra, és a szingularitáselmélet szerint lényegesen rövidebb időre lesz szükség elterjedésükhöz, mint bármely eddigi technológiai újításnak. Amennyiben az erős mesterségesintelligencia-rendszerek valósulnak meg, terjednek el és épülnek ki, úgy az emberiség a gépek számára mindösszesze valamiféle spam lesz (Z. Karvalics 2015), s ebben az esetben jelen kötet tartalma is meghaladottá válik. Egyelőre azonban még mindig azonosíthatók azok a valóságos emberi meghatározottságok, amelyek az internettel élő, illetve az internetre költözött társadalom online tevékenységei mögött megtalálhatók. Így nem kerülhetjük meg ennek a társadalmi csoportnak, társadalmiasulási formának a leírását és a normától eltérő magatartásaik különböző mintázatainak egyszerű bemutatását.

Az offline alapon szerveződő 1.0 online közösségek magukkal vitték az online térbe korábbi szabályrendszerüket. A 2.0 online közösségek egyik jellemzője azonban éppen az, hogy szabályrendszerük az online térben jön létre (amelynek függetlensége a valódi szociokulturális tértől ugyancsak kérdéses). Ennek nem megfelelő vagy hiányos működése devianciákhoz vezet. Áttekintjük azokat a devianciaelméleteket – összefüggésben az újítások terjedésével –, amelyek segítségünkre vannak az online deviancia értelmezésében. A normáktól való eltérések egyik típusa a bűnözés jelenségköre, amely egészének bemutatására nem vállalkozhatunk, annak csupán a napjainkban leggyakrabban megjelenő alakzatait körvonalazzuk. Ennek ellenére igyekszünk részletesebben körüljárni az internetes devianciák jelenségvilágát. Az cybernormasértések fogalmi elválasztásán túl részletesen tárgyaljuk azok szabályozóinak (hatóság, állam, jogi normák) szerepét, jelentőségét és fejlődését. Kutatásaink során igyekszünk úgy eljárni, hogy a napi események, technológiai újítások tárgyalásánál stabil jelenségvilág működésének leírásába vezessük be az olvasót. Természetesen elkerülhetetlen, hogy néhol konkrét példákat használjunk fel érvelésünkhöz, azonban lényeges hangsúlyozni, hogy csakis olyanokat idézünk, amelyek általánosságban

mutatnak rá azokra a rejtekutakra, amelyekkel a cyberdevianciáról gondolkodva találkozhatunk. Könyvünknek nem célja a jelen rendkívüli ütemben változó trendjei után loholni, hanem elsősorban a jövőben várhatóan bekövetkező eseményekhez kíván értelmezési eszközöket biztosítani.

A kézirat lezárva: 2018. május 15.

A szerzők

1. Újítás és terjedés: a nyelv

1.1. Az ember: nyelvében létező lény

Arnold Gehlen szerint az ember leírható mint „cselekvő", „meghatározatlan", „állásfoglaló", saját maga által „kinevelés alatt álló", „tehermentesítő" lény (Gehlen 1976, 41.). Elsősorban azonban „kommunikatív" lény. Ahogy fogalmaz: „Az ember tehát szükségleteitől független (tehermentesített), kommunikatív mozgások és akciók révén átjárja a világot, nyitott gazdagságát bevonja tapasztalásának körébe, »megismeri« és a helyére teszi, s ez a folyamat, mely a gyermekkor legnagyobb részét kitölti, ez teremti meg az észleléseinkben adott világot" (Gehlen 1976, 52.). Vagyis az ember voltaképpen nem más, mint a lehető legösszetettebb szintaxisú nyelvvel kommunikáló lény. Ez a nyelv az, amellyel saját magából, a meghatározatlanból meghatározottat formál. Továbbá ezzel a nyelvvel teremt a körülötte lévő *környezetből* a saját maga számára megfelelő *világot*. A nyelv elsajátításának – azaz megtanulásának – képessége valamennyi ember számára adott biológiai determináns. Az 1960-as években az amerikai nyelvész, Noam Chomsky egyenesen velünk született nyelvelsajátító készülékről *(LAD: language aquisition device)* értekezik (1986). Sőt a nyelvfilozófus Ludwig Wittgenstein egészen odáig megy, hogy az ember által létrehozott nyelv mintegy a vegetatív idegrendszer része, s akár úgy is tűnhet, mint alkotójától függetlenül működő létező. „Az ember rendelkezik azzal a képességgel, hogy nyelveket hozzon létre, amelyek segítségével bármely értelmet kifejezhet anélkül, hogy sejtelme lenne arról, hogyan és mit jelent (bedeutet) minden egyes szó. – Mint ahogy anélkül beszélünk, hogy tudnánk hogyan képződnek az egyes hangok. A köznyelv az emberi szervezet része, és nem kevésbé bonyolult annál. Az ember számára lehetetlen a nyelv logikáját közvetlenül kiemelni a köznyelvből. A nyelv álruhába öltözteti a gondolatot. Mégpedig úgy, hogy a ruha külső formájából nem következtethetünk az eltakart gondolat formájára, mert az öltözet külső formája egyáltalán nem abból a célból készült, hogy a test formájának felismerését lehetővé tegye" (Wittgenstein 2004, 4.002.).

A *nyelv hajlékában lakozó lény* (Heidegger 2003, 293.) legújabb kommunikációs-eszköz-fejlesztésének következtében a kultúra, *nota bene* a civilizáció eddig nem ismert, egészen sajátos változata jelent meg. Ennek mélyén pedig egy nagyon komoly meghatározottságot jelentő, csak az emberre vonatkoztatható jellemző található: a *kulturális változásra való képesség*. A nyelv és az emberi gondolkodás kialakulását kutató legújabb evolúciós, kognitív kutatási eredményeket Merlin Donald a következőképpen foglalja össze: „A kognitív modellálásból gyakran kihagynak egy elemet, mégpedig a kultúrát, azaz az egy fajra jellemző tanult viselkedés közös mintáit. Pedig az állatok kognitív képességei közvetlenül befolyásolják, hogy milyen fajta kultúrát hoznak létre. Az emberek esetében pedig ennek a fordítottja is igaz: az emberi kultúra sajátos típusai közvetlenül hatnak az egyén megismerésére. Valójában azt mondhatjuk, hogy az emberi nem egyedisége nem is annyira

a nyelvben rejlik, mint inkább a gyors kulturális változásra való képességünkben" (DONALD 2001, 22.). Az emberi kultúra esetében nem egyszerűen arról van szó, hogy az ember a *vele született nyelvelsajátító készülékkel* létrehozza azt a nyelvet, amellyel a *környezetből* a saját maga számára élhető *világot* alkot, beleértve ebbe a társas világot, azaz a tanult viselkedésmintákat is. Ezzel együtt ugyanis egy olyan szerkezetet (kultúrát) is létrehoz, amely meghatározza kognitív folyamatait, beleértve ebbe a megismerést is. A folyamat pedig oda-vissza zajlik. A környezet megismerését, a környezet világgá alakítását elősegítő készülék a nyelv, amely által létrehozott kultúra meghatározza nemcsak a környezet, hanem a társas világ megismerését is. Nietzsche (1992) szélsőséges álláspontja szerint a nyelv önmagában hordozza a társas világ struktúráit, az alá-fölé rendeltségi viszonyokat. Nyelvekből, mint ahogy kultúrákból is sok van. Így aztán az ember elsődleges meghatározottságát az jelenti, hogy a nyelv a kultúra által hogyan hoz létre a környezetből világot. Másfelől – hangsúlyozza Donald – az ember speciális adaptációs képességéről is szó van, ez pedig a *gyors kulturális változásra* való képesség (DONALD 2001, 22.).

Sokak szerint a legújabb kommunikációseszköz-fejlesztés, a *tehermentesítés,* a kultúra, a civilizáció új fokozatát, állapotát is létrehozza, illetve létrehozta. Egyelőre inkább elképzelések, mintsem pontos prognózisok vannak arra vonatkozóan, milyen is lesz a jövő. Ezek az elképzelések alapvetően két csoportba sorolhatók. A jövőt az egyik esetben az *erős mesterséges intelligencia* határozza meg. Ebben a jövőben azonban nincs szükségszerűen helye az embernek. Legalábbis abban a formában nincs, ahogy ma még elképzelhetetlen nélküle. A mesterséges intelligencia, az „ipar 4.0" több szempontból is esetlegessé teheti az ember rendszeren belül betöltött helyét. Ha ez a szcenárió valósul meg, akkor az ember, az emberiség *spam* lesz az evolúció következő fokozatában, az intelligens gépek között, tekintettel arra, hogy számos kiszámíthatatlanságot rejt magában. Azonban az is elképzelhető, hogy a kiforrott mesterséges intelligencia sokkal inkább a hibriditásra épül, s ebben az esetben a gép az ember protézisévé válik. Ebben az esetben arról van szó, hogy az ember és a gép teszi a dolgát: mindegyik azt, amihez a legjobban ért. Ezek az ember-gép hibrid rendszerek jelentik a jövőt a másik – a *gyenge mesterséges intelligenciát* leíró – elképzelés szerint (Z. KARVALICS 2015).

1.1.1. A beszélő lény

Az ember mint rendkívül bonyolultan kommunikáló lény megjelenése a Föld nevű bolygón egyáltalán nem triviális. Az ember a múlt végtelenségébe vesző történetét évezredeken át transzcendentális eszközökkel igyekezett megérteni. A csillagászat, a biológia, a paleoantropológia, a kognitív idegtudományok, az orvostudományok – ahogy szinte valamennyi tudomány – saját eszköztárával keresi a válaszokat. A kutatásokhoz hatalmas lökést adott Darwin evolúciós elmélete (DARWIN 1961). Ennek felhasználásával juthatunk arra az immanens álláspontra, hogy az emberi faj más, alacsonyabb komplexitású élőlény utódfaja. Carl Sagan *Az éden sárkányai* című könyvében három mondatban foglalja össze az ember történetét. „A kozmikus kronológiát a legtanulságosabban tudtommal úgy lehet kifejezni, ha a világegyetemnek (vagy legalábbis a Nagy Bumm óta fönnálló, jelenlegi megtestesülésének) tizenötmilliárd éves élettartamát egyetlen év időtartamába képzeljük el" – írja Sagan, majd így folytatja: „Nyugtalanító érzés rájönni, hogy az ilyen kozmikus év során

Földünk csak szeptember elején állt össze a csillagközi anyagból; hogy a dinoszauruszok csak karácsonyeste bukkantak fel; a virágok december 28-án bújtak elő; az emberi nem férfiai és asszonyai pedig csak szilveszter este 10.30-kor keltek életre. Az egész írott történelem december 31-ének utolsó tíz másodperce: a középkor alkonyától a jelenig eltelt idő pedig alig több egyetlen másodpercnél" (Sagan 1990, 24, 27). Azzal együtt, hogy az ember története a Föld történetének parányi része, arra is rávilágít Sagan gondolata, hogy a legintelligensebb faj megjelenése és általa a bolygó benépesítése a korábbi fajokhoz képest egyre gyorsuló tempóban történt.

Tehát az emberi nem egyik sajátja a beszélés képessége, amely fokozatosan alakult ki a homo sapiens esetén. Több eszközre, feltételre is szükség volt hozzá. Például megfelelő nagyságú agyra. A beszéd rendkívül összetett tevékenység: elég nagy számítási kapacitásokkal rendelkező hardverre (agyra) van hozzá szükség, amelyet a megfelelő szoftver teljesít ki – ahogy Chomsky vagy Wittgenstein kutatásai alapján láthattuk.

1.1.2. Nyelv és közösség

A korai emberszabásúak nyelvelsajátító képessége nagymértékben összefüggött a speciális társas kapcsolataikkal. Ezek azért is rendkívül fontosak, mert napjainkban is megfigyelhetők, talán azért, mert az ember genetikai meghatározottságát jelentik, amely azonban nem valamiféle testi jellegzetességgel kapcsolatos, hanem a *társas alakzattal* függ össze. Ez a kettősség már az ókori görögöket is foglalkoztatta. Platón Prótagorasz (321–322) dialógusában mutat rá erre (Platón 1984). A párbeszéd szerint az istenek teremtették az embert, mint ahogy minden más élőlényt is. Két titán, Epimétheusz (megfontolatlan) és Prométheusz (megfontolt) kapta a feladatot, hogy az élőlények között osszák szét a tulajdonságokat. Epimétheusz vállalta magára a feladatot: „Akinek erőt adott, attól megtagadta a gyorsaságot, a gyengébbeket viszont éppen a gyorsasággal ruházta fel; egyeseket felfegyverzett, a védtelen szervezetek oltalmára viszont másfajta képességeket eszelt ki. Amelyiküknek ugyanis kis testalkatot juttatott, a menekülésre szárnyakat adományozott vagy pedig föld alatti lakóhelyet; azokat a lényeket, amelyeket nagysággal tüntetett ki, éppen nagyságuk óvta meg. A többi tulajdonságot is hasonló módon az egyensúly biztosításával osztotta ki. Mindezt pedig annak szem előtt tartásával eszelte ki, hogy egy fajt se tegyen ki a pusztulásnak." (321a). A *megfontolatlan* azonban megfeledkezett az emberről, akinek semmilyen speciális tulajdonságot nem adott. Prométheusz oldotta meg a problémát: ellopta a tüzet az istenektől, s odaadta az embernek. Így jóllehet az embernek nem voltak tulajdonságai, a tűz (a tudás) az övé volt, amivel ellensúlyozni tudta specializálatlanságát. Ezzel Platón dialógusa szerint az ember még csak félig volt kész. „[H]iányzott ugyanis még belőlük a közösségalkotó képesség" (322a), és jogtalanságokat követtek el egymás ellen. Ezért a jogot is oda kellett adniuk az isteneknek: „Végül már Zeusz is aggódni kezdett nemünkért, és hogy teljesen ki ne pusztuljon, elküldte Hermészt, hogy honosítsa meg az emberek között a tisztességet és a jogot: hadd legyen az államokban rend és barátságokat létesítő kötelék. Hermész természetesen megkérdezi Zeuszt, hogy miképpen tegye az embereket a jog és a tisztességérzés részeseivé. »Úgy osszam szét ezeket is köztük, ahogy a különböző mesterségek vannak szétosztva? Ennek az osztálynak ugyanis az az elve, hogy aki például az orvosi mesterséghez ért, számos avatatlan kezelését el tudja látni, és ugyanígy van a többi szakember esetében

is. Mármost a jogot és tisztességérzetet is ilyen módon osszam szét közöttük vagy juttassak belőle mindenkinek?« »Mindenkinek – felelte Zeusz –, és valamennyien részesüljenek belőlük, mert nem jöhetnek létre államok, ha – miként a többi mesterség esetében – csak kevesen részesülnek belőlük«" (322a–c) (PLATÓN 1984). Azaz a közösség létrehozásának képessége ugyancsak különös jelentőséggel bír. Ennek legelemibb eszköze az emberek közötti kapcsolatok kiszámíthatóvá tétele, szabályozása. Mégpedig olyan szabályozása, amely ideáltipikusan a közösség minden tagjára vonatkozik.

Az ember származására vonatkozó többmillió éves leletekből látható, hogy az ember testének beszéléshez szükséges eszközei[1] mintegy kétszázezer évvel ezelőtt már rendelkezésre álltak. Ezzel együtt az is kérdéses, hogy miért, miként, minek a hatására jelent meg a szimbólumhasználat. Robin Dunbar evolúcióbiológus is ezt vizsgálta közvetve, s rendkívül figyelemre méltó eredményekre jutott. A kutató kísérletet tett arra, hogy az agy méretének kialakulására vonatkozóan két hipotézist is megvizsgáljon. Az egyik ilyen hipotéziscsalád az *ökológiai hipotézis,* amelynek több válfaja is van. Mindegyik abból indul ki, hogy a *környezettel* való kapcsolat függvényében alakult az agyméret. Az egyik alhipotézis szerint a környezettel való kölcsönhatás következtében fejlődött ki a „nagy agy": a főemlősöknek összetettebb problémákat kellett megoldaniuk. Egy másik elképzelés szerint az agy nagysága összefügg a *testtömeggel,* azaz a nagyobb állatoknak nagyobb az agyuk. A következő alhipotézis szerint a *gyümölcsevés* nagyobb kognitív teljesítményt követel, hiszen a gyümölcsök nem egyenletesen érnek, így aztán tudni kell, hogy mikor, melyik és hol található. Az ökológiai hipotézis egyik legerőteljesebb alhipotézise a *mentális térkép* hipotézise. Ennek ugyancsak két altípusa van: a „belakott" terület mérete (azaz mekkora területen él az emlős), másrészt pedig, hogy mekkora utat jár be egy nap alatt. Mindkettő lényege, hogy a lakott terület nagysága, illetve hossza „serkentette" az agy növekedését: nagyobb bejárt terület esetén nagyobb agyméretre volt szükség. Az ökológiai hipotézis utolsó alhipotézise a *kitermelési hipotézis*. Ebben az esetben arról van szó, hogy az étkezés során bizonyos *kitermelő tevékenységeket* kell végrehajtanunk. Ezek (a növények ehető részeinek ismerete, az állatok viselkedésének megtanulása) serkentette az agyméret növekedését (DUNBAR 1998).

Mind közül a legvalószínűbb a *társas/társadalmi hipotézis*. Dunbar erre találta a legegyértelműbb bizonyítékokat. A hipotézis az 1980-as években kezdett elterjedni. E szerint a főemlősök agymérete jól tükrözi azokat a komplex társadalmi rendszereket, amelyekben élnek. Ezekben olyan folyamatok vannak jelen, amelyek a főemlősökön kívül más élőlények esetében nem figyelhetők meg. Ilyen például a *szándékos taktikai megtévesztés,* a *koalíciók kötése*. Ezért is nevezik ezt a megközelítést a *machiavelliánus intelligencia* hipotézisének, illetve újabban – Dunbar megfogalmazása szerint – a *szociális agy* hipotézisének. A különböző elgondolásokat empirikus vizsgálatok eredményeivel tesztelte Dunbar. Valamennyi közül a társadalmi hipotézis „nyert". Az agyméretet nem az agy abszolút méretével, hanem a neocortex[2] arányával mérte Dunbar, azaz a neocortex méretét a teljes agy

[1] A hangképzés szempontjából lényeges a garat és a gége egymáshoz viszonyított megfelelő helyzete, az agyban a *Broca-terület* jelenléte.

[2] „Fejlődéslélektani szempontból a legfiatalabb terület a neocortex, amely szintén kulcsfontosságú az érzelmi folyamatokban. Az arckifejezések érzelmi állapot-komponensének felismerésében a jobb félteke vesz részt. A beszéd érzelmi komponenseivel (mind a megértés, mind a produkció tekintetében) a nem-domináns félteke temporális cortexe mutat összefüggést" (LAKATOS–GERVAI 2003, 336.).

méretéhez viszonyította. Amennyiben a rendelkezésre álló adatok és az adott faj agyának neocortex-aránya közötti összefüggéseket nézzük, a társadalmi hipotézis bizonyítottsága egyértelmű. Az egyes főemlős fajok csoportméretei összefüggést mutatnak az agy méretével: *minél nagyobb csoportokban élnek a főemlősök, annál nagyobb az agyuk neocortex állományának aránya* (leegyszerűsítve a tudatos gondolkodásért felelős állomány). Dunbar azt vette észre, hogy a különböző paleoantropológiai, régészeti kutatások szerint egyre nagyobb csoportokban éltek emberelődeink. Továbbá azt is, hogy minél nagyobb csoportokban éltek, annál nagyobb volt agyuk neocortex-aránya. Egyértelműen bizonyítottnak látta ez alapján, hogy az egyre nagyobb csoportméret következtében „nőtt nagyra" az ember agya (Dunbar 1998, 184.).

Tehát az ember agymérete leginkább a rendkívül összetett és nagy csoportméret függvényében alakult. Egyfelől egyre több csoporttagról egyre több információt kellett tudni: ki mit szeret és mit nem, milyen igényei vannak, de összességében a csoportdinamikával kapcsolatban is ismeretekkel kellett rendelkezni. Ennek alapján elég jól megfigyelhető, hogy a különböző antropológiai leírások körülbelül 150 fős embercsoportokról számolnak be – ez a klánok mérete (Dunbar 1998, 187.). Ehhez képest az előemberek, illetve hominidák maximum 100 fős csoportokban éltek. Tehát a nagy csoportokban élő embernek nagy kapacitású agyra (hardverre) van szüksége. Másfelől az információk gyors, pontos és hatékony továbbítása is lényeges, ezért szükség van egy olyan szoftverre is, amely ezt biztosítja. Ez a nyelv, amely azonban nemcsak kognitív, hanem affektív szempontból is lényeges: rendkívül hatékonyan biztosítja a társas kapcsolatok kialakítását és fenntartását. Ezek a szociális interakciók időigényes tevékenységek. Azonban a főemlősök napjuk 20 százalékánál több időt nem fordíthatnak társas kapcsolataik menedzselésére, arra a tevékenységre, amelyet a majmok a kurkászással végeznek. Az ember számára ennél jóval nagyobb hatásfokú eszközre van szükség, hiszen jóval nagyobb csoportokban él. Többek között ehhez is kell a nyelv, amely lehetővé teszi a társas igények kielégítését. A – talán pejoratívnak hangzó – „fecsegés" ebben az értelemben rendkívül fontos társas tevékenység, amely egyfelől a társas támogatás, másfelől a taktikák, a koalíciók létrehozásának egyik legfontosabb eszköze. Mindezzel együtt a nyelv teljesítőképessége sem határtalan: nem vagyunk képesek valamennyi embertársunkkal érdemben kapcsolatba kerülni. Ezért is csalóka az interneten a kapcsolati portálokon egyes felhasználóknál megjelenő tízezres kapcsolatszám. Erre hívja fel Dunbar is a figyelmet tanulmányában (2006), amelynek e szempontból jogos kérdést megfogalmazó címe, hogy *Vannak-e korlátai az e-világnak?*

Nietzsche megfontolása a társas világ struktúráinak a nyelvben való megjelenésére utal. Így fogalmaz: „A fogalmaknak amaz irdatlan gerendázata és pallózata, amelybe kapaszkodva az oltalomra szoruló ember átmenti magát az életen, a felszabadult intellektus számára csupán állványzat és tornaszer legvakmerőbb mutatványaihoz; s ha halomra dönti, feldúlja, ironikusan ismét összerakja, összepárosítva legidegenebb, és szétválasztva legrokonabb elemeit, úgy ezzel azt juttatja kifejezésre, hogy nincs szüksége a gyámoltalanság ezen mankóira, azaz nem a fogalmak, hanem az intuíciók vezetésére bízza magát" (Nietzsche 1992, 13–14.). A nyelv önmagában hordozza a legalapvetőbb társas hierarchiát. „Irdatlan gerendázatával és pallózatával" segítséget, kapaszkodót ad az oltalomra szorulónak. A nyelv azonban nem egy örökké vett rögzített rendszer, hanem folyamatosan változik, és elsősorban a használók hozzák létre, illetve ők alakítják. Ezek alapján vannak olyanok, akiknek a nyelv csupán „állványzat és tornaszer legvakmerőbb mutatványaihoz": rendszerteremtő tevékenysé-

gük nyomán elsősorban rajtuk áll vagy bukik, hogy milyen társas struktúrákat hordoz magában a nyelv. Azaz – nyelvi szempontból – ők a felszabadult intellektusúak (akiknek nincsenek sem materiális, sem szellemi kötöttségeik), a gazdagok, az „urak", szemben az „oltalomra szorulókkal", a szegényekkel (akiknek a szerepe ugyancsak rendkívül lényeges, tekintettel arra, hogy ők tartják fenn a rendszert).

Természetesen a szegény-gazdag, szolga-úr dichotómiákon kívül lényegesen bonyolultabb viszonyokat is kifejez a nyelv. Például a családi kapcsolatok egésze megtalálható benne. Különböző nyelvekben különböző mélységű a családi kapcsolatok számontartása. Sokatmondó, hogy amíg magyarul az egyén *dédapjának dédapját* két szóval határozzuk meg, addig az ókori rómaiak mindezt egy szóval tették: *tritavus* (MORGAN 1961, 374.). Továbbá hogy egyáltalán számontartanak-e egy adott rokonsági relációt (például *anyai nagyanyám nővére lánya lányának fia* – ha férfi beszél – a szeneka irokézeknél *ha-yă'-wän-da,* az India déli részén élő dravida nyelv tamil nyelvjárását beszélőknél *en mărŭmăken,* ahol az *en* a birtokos eset képzője [MORGAN 1961, 345.]). Tehát arra kell rámutatnunk, hogy a különböző nyelvek jelentik az elsődleges határokat a csoportok, közösségek, társadalmak között. Ez a fejlődő vagy kevésbé fejlett országok távoli területein még ma is megfigyelhető helyzet az információs kor viszonyai között egyre inkább értelmét veszítheti. Egyfelől egyre általánosabban elterjed egy *közös első nyelv* használata (többnyire az angol). Másfelől – és ez a nyomósabb ok – egyre precízebbek a fordítóprogramok, amelyek segítségével voltaképpen bármely két nyelv között egyre inkább akadálymentes az átjárás. A fejlett világban tehát – ott, ahol jelen vannak a legkorszerűbb technológiák – egyre inkább megszűnni látszanak azok az elsődleges határok, amelyek a legelemibb szinten, a közösségek szintjén határozzák meg a csoportok elkülönülését. Ezzel együtt rendkívül lényeges, hogy az emberi nyelvek ennyi idő alatt – kialakulásukhoz képest egyik pillanatról a másikra – nem tűnnek el. Jelenleg az információs társadalom elsődleges határai a nyelvi határok.

Összefoglalva: a nyelv, a kommunikáció, a közösségek, a társadalmi rendszerek szétszálazhatatlan folyamatok mentén alakulnak, egymástól elválaszthatatlan jelenségek. A következőkben ezeket tekintjük át röviden. Elsőként vizsgáljuk meg közelebbről a *kommunikáció,* a „kommunikációs modellek" fogalmát! Ezek után Tönnies nyomán áttekintjük a *közösség* és a *társadalom* terminusainak különbségeit (TÖNNIES 2004), végül a *kommunikációs architektúrák* változásainak tárgyalásával jutunk el a *terjedés* jelenségének vizsgálatához.

1.1.3. Kommunikációs modellek

Szükséges előzetesen meghatároznunk a kommunikáció fogalmát, elsődleges modelljét: „a kommunikáció olyan tevékenység, amely abban áll, hogy egy ágens, a Közlő (a hírforrás, a beszélő) egy fizikai Csatornán keresztül egy olyan Küldeményt juttat el a Befogadóhoz (a vevőhöz, a célállomáshoz), amely egy közös Kódba (nyelvi vagy egyéb jelszerű formába) csomagolva információt (üzenetet) tartalmaz a Világ (a kontextus) valamilyen tényállás-(komplexum)ára vonatkozóan" (TERESTYÉNI 2006, 35.).

Ebből a modellből a fenti kontextusnak megfelelően célszerű kiemelnünk a *kódot, a jelet,* amely – ahogy arra Terestyéni is utal – kétféle lehet. A nyelvi jel önkényes „ab-

ban az értelemben, hogy néhány olyan esetet leszámítva, mint amilyenek a hangutánzó szavak, a jelölő és a jelölt kapcsolata nem motivált semmiféle fizikai összefüggéssel, például hasonlósággal vagy ok-okozati viszonnyal, hanem hallgatólagos közmegegyezésen, társadalmi konvención alapul" (Terestyéni 2006, 76.). A jelek ezek alapján két csoportba sorolhatók: *analóg* és *digitális* jelek. Az *analóg jelek* esetében a jel és a jelölt között egyértelmű és szükségszerű kapcsolat van, s ez mederben tartja a jelentést, így a beszélgetést is. A hangutánzó szavak olyan jelek, amelyek egyértelművé teszik ezt a determinisztikus viszonyt. A nyelvi jelek többsége azonban nem ilyen természetű: esetükben semmiféle kapcsolat nincs a jel és a jelölt között, csupán a megegyezés, a konvenció jelenti a kapcsolatot. Ezek a *digitális jelek*.

Ebben a szóhasználatban a „digitális" tehát rendkívül tág értelmű terminus, arra utal, hogy a jel és a jelölt között nincs szükségszerű kapcsolat, amely tehát konvención alapul. Ez a szintaktikus nyelv értelmezéséhez elengedhetetlen. Amikor az előbbiekben a nyelv evolúcióbiológiai megközelítéséről volt szó, erre a nyelvre utaltunk. Mindez azért is lényeges, mert az *epizodikus* és a *mimetikus* kommunikáció esetében még nem beszélhetünk kifejlett fogalmi gondolkodásról (Donald 2001, 242.). A mimetikus kultúra, a mimézis a homo erectusra jellemző. Arról van szó, hogy a kommunikáció egy-egy esemény újraeljátszásával történik. Ebben az esetben rendkívüli szerepe van a vizuális érzékelésnek, amely jóval kisebb kognitív teljesítményt jelent. Talán különös lehet, de a vizuális jelekkel történő kommunikáció napjainkban újra reneszánszát éli. Ennek egyszerűbb válfajait jelentik a *piktogramok,* az *emojik,* amelyek képi, vizuális kommunikációs eszközök. Ezeknél lényegesen bonyolultabbak a játékok. A legkorszerűbb, széles sávú online kommunikációban a vizualitás, a képek szerepe egyértelműen felértékelődik. Az emojik is remek példaként szolgálnak arra, hogy az újabb és újabb kommunikációs architektúrák megjelenése nem jelenti egyszersmind azt is, hogy az új végérvényesen megszünteti az előzőt.

Érdemes és szükséges is néhány kommunikációelméleti modellt áttekinteni figyelemmel arra, hogy az eltérő megközelítések külön-külön és együttesen is megjelennek a legkorszerűbb online kommunikáció során. Ezek olyan értelmezési kereteket adhatnak, amelyek az online térben való konkrét közlekedés értelmezéséhez adekvát eszközökkel szolgálhatnak. Anélkül, hogy ezeket az elméleteket a maguk teljes részletességében tárgyalnánk, Em Griffin *Bevezetés a kommunikációelméletbe* (2001, 35–46.) munkája alapján tekintjük át őket röviden.

1.1.3.1. A kommunikáció szociálpszichológiai modellje

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. Az interperszonális befolyásolás során célszerű megkülönböztetni a *kognitív* és *affektív* elemeket. Az első esetben a közlő a befogadó „értelmére" kíván hatni: azaz logikus érveléssel próbálja meggyőzni a befogadót. Az affektív szempont vizsgálata során arra vagyunk kíváncsiak, hogy a közlő miként, a befogadó milyen érzelmi elemeit kívánja mozgásba hozni a meggyőzés céljából. Természetesen interaktív helyzetről van szó: azaz a közlő és a befogadó szerepe folyamatosan változik, cserélődik.

Csepeli György *A meghatározatlan állat* című könyvében (2005) a kommunikációról és meggyőzésről szóló fejezetének Platón nyomán *A lélek szakácsmestersége* címet adta. A megfogalmazás etikai értelemben is kettős: 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. A befolyásolás ez utóbbi módja autoriter rendszerekben a propaganda, amely egy központi közlő által sugárzott információhalmaz sulykolásáról szól. A hálózati társadalom architektúrája azonban ezzel a befolyásolási módszerrel teljesen ellentétes, hiszen alapvetően nem egyközpontú, hanem sokközpontú, decentralizált hálózatról van szó, amelyben a befolyásolás elsődleges, s normatívan elfogadott eszköze semmiképp sem az egyetlen világkép sulykolása. Habermas *A társadalmi nyilvánosság szerkezetváltozása* című munkájában (1971) a polgári nyilvánosság egyik legfontosabb elemeként jelölte meg az *uralommentes kommunikációt,* amely nemcsak a társadalmi rendszer sajátjaként, hanem az interperszonális kapcsolatok szempontjából is lényeges.

Az információs társadalom körülményei között a *kommunikáció szociálpszichológiai modellje* jól alkalmazható azokban a helyzetekben, amikor valaki erőfölényével akar visszaélni, s egy-egy gyanútlan felhasználót csapdába csalni. Az ilyen típusú e-akciókat a *Cyberdevianciák* című alfejezetben rendszerezzük.

1.1.3.2. A kommunikáció matematikai, technikai, tranzaktív, kibernetikai modellje

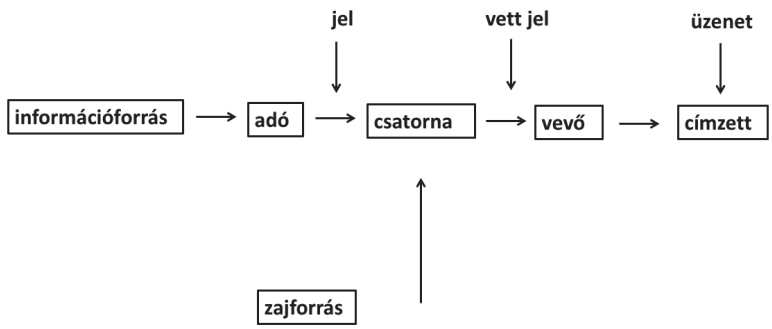
A kommunikáció matematikai, technikai, tranzaktív, kibernetikai modelljében is megtalálhatók azok a szerepek, amelyekre Terestyéni hívta fel a figyelmet imént idézett definíciójában. Griffin (1967, 15–27.) egyértelműen Norbert Wiener, a MIT (Massachusetts Institute of Technology) matematika professzorának munkájára vezeti vissza a kibernetikai hagyományt, aki a mesterséges intelligencia jelölésére használta a szót (GRIFFIN 2003, 36.). Wiener a világháborút követően az üzenetekkel, az *üzenetelmélettel* foglalkozott. A mesterséges intelligencia sok más területet is érintett, például a pszichológiát, a nyelvtanulást, a társadalompolitikát, s mivel nem volt átfogó kifejezés rá, ezért a görög *kübernétész* (kormányos) szóra utalva kibernetikának nevezte az először 1948-ban publikált azonos című munkájában (WIENER 1967, 15). A kibernetika szó már önmagában utal arra a jelenségre, amelynek nyomán a kommunikáció matematikai modelljéről beszélhetünk.

Claude Shannon a Bell Telefontársaság kutatójaként kezdett el foglalkozni a kommunikációval mint információfeldolgozással. Nyilvánvalóan olyan kutatói tevékenységet kellett végeznie, amely hasznos a cég számára is. Szerencsére ennél általánosabb érdeklődésre is számot tartó eredményekre jutott. Kérdése alapvetően az volt, hogy miként lehetséges minél nagyobb vonalkapacitást biztosítani minél kisebb torzítás mellett, azaz ebben az értelemben növelni az információszállítás hatékonyságát. Az pedig, hogy mi az információ, voltaképpen teljesen érdektelen volt a számára: modelljének kidolgozása során semmiféle olyan (etikai) kérdéssel nem kellett foglalkoznia, ami az információ tartalmi jellemzésével lett volna összefüggésben.

Shannon értelmezésében az információ a *bizonytalanság csökkentésére* szolgáló eszköz. Azaz az információ révén lehetséges a bizonyosság fokának a növelése érdekében valamiféle rendezettség kialakítása a káoszban. Ezért roppant lényeges, hogy az információ

önmagában milyen minőségű, de Shannont ennél jobban érdekelte az, hogy miként lehet úgy szállítani, hogy a lehető leggazdaságosabb legyen, és a lehető legnagyobb mértékben megőrizze eredeti minőségét.[3]

A következő ábrát Shannon és Weaver (1949, 7.) közli 1949-ben megjelent könyvükben. Az ábrát a telefonhívás példáján keresztül mutatjuk be, azonban meg kell jegyezni, hogy más esetekben is ez a helyzet, a kibernetika világában pedig különösen.



1. ábra
A kommunikáció matematikai modellje

Forrás: Shannon–Weaver 1949, 7.

Az 1. ábrán az információ forrása a hívó fél. A hívó felveszi a kagylót és belebeszél. A hangot elektromos jelekké alakítja a készülék, és a telefonvonalon keresztül elszállítja a hívott fél készülékéhez. Az a jeleket újra hanggá alakítja, amely eljut a hívott félhez. Mindegyik lépésnél elvész valamennyi információ (a felhasználó azt tapasztalhatja, hogy rossz minőségű, recseg a telefon). Az egyik legjelentősebb hatás ebből a szempontból a *zaj*. Ez három nagyobb zajtípust foglal magában: a *csatornazajt*, a *környezeti zajt,* illetve a *szemantikai zajt.* Ahogy a következőkben majd látni fogjuk, a kommunikáció ezen ártalmatlannak tűnő rendellenességei számos visszaélésre (is) alkalmat adhatnak az információs kor körülményei között. Ennek a kommunikációs modellnek az elemei kifejezetten jól használhatók a rendszerintegritást sértő támadások leírása során.

1.1.3.3. A kommunikáció mint retorika, művészet

A retorika évezredeken át az alkalmazott kommunikációkutatás vezető ága volt. Démoszthenész kövekkel a szájában gyakorolt szónokolni már az i. e. 4. században – hívja fel a figyelmet Griffin (2003, 38.) a kommunikáció retorikai elméletének tárgyalása során. A retorika gyakorlata azonban nem lehet független a politikától, a közügyek intézésétől – mint ahogy Démoszthenész példájából is tudhatjuk, aki maga is gyakorló politikus volt. Ennek követ-

[3] Ez utóbbi feltételt Shannon óta kiterjesztették: nemcsak az a cél, hogy az információ a szállítás alatt minél inkább megőrizze eredeti minőségét, hanem az, hogy kifejezetten jobb minőségben érkezzen meg.

keztében a különböző politikai, társadalmi rendszerekben a közügyek intézésére hivatott fórum által is meghatározott a retorika alkalmazhatósága. A kommunikáció retorikai modellje kifejezetten összefügg a közösség társadalommá alakulásával, a nyilvánosság megjelenésével. A retorika tudományának gyakorlati alkalmazására tulajdonképpen csak bizonyos társadalmi körülmények között nyílik mód, amelyek szempontjából, ha leegyszerűsítve is, de két típust mindenképpen meg kell különböztetni. Demokratikus nyilvánosságban a közügyek intézése az *uralommentes kommunikáció* feltételei között zajlik, azaz mindenkinek lehetősége van arra, hogy szabadon kifejtse és elmondja véleményét – még akkor is, ha az mást nem érdekel. Ez lehetetlen központosított hálózatban: a demokrácia sajátja a *skálafüggetlen hálózat*. A reprezentatív nyilvánosság (az autoriter rendszerek sajátossága) esetén nyilvánosságról a szó valódi értelmében nem beszélhetünk. Ezekben a helyzetekben egyközpontú közlés van, interakciónak helye nincs. Az önálló, esetleg a hatalmi helyzetben lévő véleményével nem egyező gondolatok (nyilvános) kifejtése szankcionált (HABERMAS 1971). Hálózatelméleti jellemzőit tekintve a rendszer *csillaghálózat*. Az interaktivitást kizáró világnézetet közlő kommunikációs formáról van szó, amely modern körülmények között tömegkommunikáció.[4] Ezekben a társadalmi rendszerekben a szónoklat propaganda. Azaz a retorika tudományának gyakorlata jelentős mértékben függ az adott társadalmi berendezkedéstől.

A retorikai hagyomány jellemzőit hat nagyobb csoportba rendezve mutatja be Griffin. 1. Jellemző vonás az a meggyőződés, hogy az embert a beszéd különbözteti meg az állattól. 2. „Annak bizonyossága, hogy a társadalom demokratikus fórumon keresztül történő megszólítása hatásosabb a politikai problémák megoldására, mint a rendeletekkel vagy erőszakkal fenntartott uralom." 3. „Egyetlen beszélő próbál nagyszámú hallgatóságot befolyásolni nyíltan meggyőző szándékú beszéddel." 4. „A szónoklattan a vezetőképzés alappillére." 5. „A hangsúly a nyelv hatalmán és szépségén van, hogy megmozgassák az emberek érzelmeit, és cselekvésre ösztönözzék őket. A szónoklás inkább művészet, mint tudomány." 6. „A nyilvános szóbeli meggyőzés a férfiak privilégiuma" (GRIFFIN 2003, 38–39.).

1.1.3.4. Kommunikáció: a jelek tudománya

A szemiotikai értelmezés szerint a kommunikáció elméleti megközelítése a jelek tudománya. Ezen keresztül vizsgálható a kommunikáció. Ahogy az alfejezet elején Terestyéni Tamás definíciójában is olvashattuk, a jelenség kiemelt elemei az analóg, illetve digitális jelek, valamint ezek kapcsolata a jelölttel. A szemiotikai kommunikációelmélet voltaképpen ennek a megfontolásnak a részletes, rendszerszerű vizsgálata. Tekintettel arra, hogy a jel és a jelentés között az esetek döntő többségében semmiféle kapcsolat nincs, kérdéses, hogy akkor miért is működnek a jelek (speciális verbális értelemben: a szavak, amelyek szimbólumok). Ezzel foglalkozik a *szemiotika*.

A szemiotikai kommunikációelméletre példaként Jakobson (1969) kommunikációs modellje hozható fel. Ebben is megkülönböztetik az „adó", a „vevő", a „csatorna" elemeket, amelyek funkciójukat tekintve megegyeznek a Shannon és Weaver modelljében látottakkal. Jakobson számára azonban sokkal lényegesebb a *kontaktus,* a *kapcsolat,* illetve az, hogy

[4] A tömegkommunikáció a diktatúrákban a propaganda, demokráciákban az információszórás legitim terepe.

ez milyen kulturális közegben jön létre. Ez utóbbit *kontextusnak* hívja; Roman Jakobson kulturális relativista modellje e köré szerveződik. A kontextus voltaképpen a valósággal való összefüggést jelöli. A kommunikáció valamiféle emberi, társas, kulturális közegben zajlik, amely keretet és referenciát szolgáltat a kommunikáció *tárgyi* és *viszonyszintjéhez.* A szemiotikai modell ebből a szempontból arról szól, hogy a kommunikációs helyzetben részt vevők, a tartalom és a referenciák kapcsolata hogyan valósul meg.

A szemiotika azonban nemcsak verbális, hanem nonverbális jelekkel is foglalkozik, például a képekkel, képi szimbólumokkal. A bizonytalanság a képi kommunikáció esetében jóval nagyobb, miközben manapság a fényképeket gyakran valamiféle bizonyíték *(testimony)* értelemben használjuk. Az egyre ritkábban használt MMS egyik funkciója kifejezetten azonnali bizonyítékot adni arra vonatkozóan, hogy az ember hol van, kivel és mit csinál (legújabban a közösségi portálok video- vagy *stream*-funkciói még ennél is valóságosabb képpel szolgálnak, így ki is szorították az MMS technológiáját). Ebből az ellentmondásos helyzetből is következik, hogy a (fény)képi kommunikáció működésének értelmezése ugyancsak kimeríthetetlennek tűnő téma a kommunikáció szemiotikai kutatása során. Az ilyen irányú elemzés igen szoros kapcsolatban áll a kognitív tudományokkal, azzal, hogy az elme hogyan kapcsolja össze a jelet a jelölttel, hogy a gondolkodás fogalmi és/vagy képi modalitásokban zajlik-e.

1.1.3.5. A kommunikáció mint a társadalmi valóság szerkesztésének eszköze

„A szociokulturális tradíció azon alapul, hogy az emberek a kultúrát beszéd közben teremtik újra és újra" – állítja Griffin. (2003, 41.) 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, amit 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). Ez a megközelítés teljesen ellentétes azzal, amely azt mondja, hogy a gondolatoktól, társadalmi jelenségektől független a nyelv: a különböző nyelvek különböző alakú szavakkal jelölik ugyanazt a jelöltet. 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.). Ezért sem véletlen, hogy az információs társadalom viszonyai között leginkább az angol nyelv terjedt el. A kortárs szociokulturális kutatók állítása az, hogy a valóságot a kommunikációs tevékenységükkel az abban részt vevő felek hozzák létre.

1.1.3.6. Kommunikáció és társadalomkritika

A társadalomkritikai elmélet során elsősorban a frankfurti iskola tagjai által létrehozott szellemi közösségre szokás utalni. Az alapvetően marxista és freudista indíttatású szellemi közösség a Harmadik Birodalom idején kényszerült először svájci, majd amerikai emigrációba. 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. Griffin három nagyobb csoportba rendezi az iskola tagjainak társadalomkritikai megfontolásait.

1. *A nyelv kisajátítása a hatalmi előnyök fenntartása érdekében.* Minden olyan szóhasználatot kritizálnak, amely fenntartja az egyenlőtlen, hatalmi pozíciókat, például a nőkkel (ha munkahelyen azt mondja a főnök a női beosztottjának: „cicamica"), a színesbőrűekkel (például „niggerezés") vagy más kisebbségi csoportokkal szemben.
2. *A tömegtájékoztatás szerepe az elnyomással szembeni érzékenység tompításában*. A megközelítés hívei szerint a magas kultúrát kiszorítja a tömegkultúra (TV, rádió), mégpedig azért, hogy elvonja a figyelmet a valóságos folyamatoktól. Marx fogalmait aktualizálva, a tömegmédia „a népek ópiuma". A tömegkultúra feladata az, hogy érzéketlenné tegye a társadalom tagjait a hatalmi helyzetek okozta fájdalmakra, problémákra.
3. *„A tudományos módszerekbe vetett vak hit és a tapasztalati úton szerzett eredmények kritika nélküli elfogadása"* (GRIFFIN 2003, 44.). Ebben az esetben már tudománykritikáról is szó van. A megfontolás lényege, hogy ha a tudomány nyelvén történik a gondolkodás, a közbeszéd, akkor abból sokan kimaradnak. Horkheimer (1976) szerint értékmentes tudomány nem létezik, így aztán a tudományos nyelvezet minden határon túli alkalmazása tulajdonképpen a szakértői hatalmi helyzetek kialakulásához, megcsontosodásához, fennmaradásához vezet.

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.

1.1.3.7. A kommunikáció fenomenológiai modellje

A *fenomenológiai*[5] jelző használata során egy individuálisnak tűnő helyzetből indulnak ki a kommunikáció ilyen szempontú értelmezői. A cél a mindennapi életnek a megértése: annak a beleérző *megértése,* amit a másik ember átél. Természetesen mindenkinek vannak napi történetei, ezért aztán szükséges, hogy mindenki napi történetei is megértő fülekre találjanak. Ez a pszichológiai folyamat voltaképpen arra irányul, hogy a másik embert megértsük,

[5] A fenomenológiai megközelítés lényege, hogy a vizsgálódás magukkal a *dolgokkal* foglalkozik. A szociológiai fenomenológia az emberek mindennapi életével foglalkozó tudományág. Annak megismerésével foglalkozik, hogy a társadalmi valóságot hogyan hozzák létre a tudatukban a társadalom tagjai.

hogy a másik ember megélje a „megértettséget". A kommunikáció fenomenológiai modellje ennek a pszichológiai megértési folyamatnak a vizsgálatát jelenti. Griffin (2003) Carl Rogers pszichiáter tevékenységét hozza példaként, aki pácienseivel való kapcsolatfelvételei, személyes tapasztalatai alapján fogalmazta meg elméletét (1961), miszerint a *feltétel nélküli pozitív odafordulás,* valamint az *empátia* jelenti a fenomenológiai értelemben vett kommunikációelmélet legfontosabb elemét. A pszichológiai megértés folyamata kiterjeszthető az egész társadalomra is. 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.

Az előbbiekben felsorolt és röviden bemutatott kommunikációs modellek mindegyike alkalmas a cybertérben zajló e-akciók elemzésére és értelmezésére. Az internet, az informatika világában többnyire a kommunikáció matematikai modelljét alkalmazzák a kutatók, de a cyberdeviancia különböző formáinak értelmezése során kifejezetten hasznos lehet, ha más kommunikációs modellek is megtalálhatók elemzési eszköztárunkban.

1.2. Közösség és társadalom

Attól fogva, hogy a homo sapiens benépesítette a Földet, folyamatosan emelkedik a népesség száma, ami napjaink egyik legnagyobb kihívása. A népességnövekedés számos kérdést vet fel, és számos társadalmi konfliktus származik belőle. Jelentős kérdéseket vetnek fel az *ökológiai problémák:* egyfelől a Föld eltartóképességének határai (például elegendő mennyiségű ivóvíz hiányának következtében hosszú távú társadalmi konfliktusokra kell berendezkednünk), másfelől a globális felmelegedés. Azt is látnunk kell, hogy ennek következtében a perifériaországok (például Fekete-Afrika) lemaradása tovább fokozódik, s a szegénység ezeken a területeken egyre inkább elviselhetetlen méreteket ölt. Érdekesség, hogy éppen azokon a területeken várható a környezeti feltételek legnagyobb romlása, ahonnan egykor az ember hódító útjára indult. A társas alakzatok szükségszerűen változnak: mások a vándorló hordában, a letelepedett közösségekben vagy akár napjaink metropoliszaiban. Ahogy a következőkben látni fogjuk, az emberi csoportok fejlődésével a társas hálózatok, a közösségek, a társadalom szövete is átalakult. A csoportképződéssel elindult a normaképződés is, amely odáig jutott, hogy napjainkban bizonyos területeken az egész Földet átfogó jogrendszer jött létre.

Az ember története bizonyos értelmezések szerint a modernizáció történetével párhuzamosan alakul. A modernizáció, amelyről Weber (1987), Tönnies (2004), Gellner (1983) és Parsons (1967) voltaképpen egységesen vélekedik, visszavezethető a *racionalizáció,* a *szekularizáció* jelenségeire, s mindezek nyomán az *individualizációra.* Érdemes megfontolni Ferdinand Tönnies gondolatait (2004), aki a modernizáció kapcsán (is) összehasonlította a *társadalmi* és a *közösségi* formációkat. Témánk szempontjából azért lényeges ezen összehasonlítás, mert az online világban, az elektronikus eszközök használatának következtében újra felsejlik a közösségi formáció egy módosult típusa. Marshall McLuhan (2012) például *globális faluról* beszél, hivatkozva arra, hogy az internet olyan távolságokat hidal át, mintha egy faluban élnének a felhasználók.

A legkisebb létszámú társas alakzatok, a hordák (kis csoportok) tagjai szükségszerűen, s rendkívül mélyen ismerték egymást. A modern értelemben vett individuum nem

létezett – mondja Tönnies. A vándorló hordák esetében a *lényegakarat* létezett csak, amely alapvetően a testi jegyek mentén történő specifikációt jelentette. Összességében valamiféle természeti állapotra utal Tönnies, amely az emberi akarat teljes egységét jelenti. „A lényegakarat az emberi test pszichológiai ekvivalense, vagy az élet egységének princípiuma, amennyiben az életet a valóság azon formájának gondoljuk, amelyhez a gondolkodás maga is tartozik" (TÖNNIES 2004, 97.). A közösség tagjai testi jegyeiknek megfelelő speciális tevékenységet végeztek a közösségi állapot körülményei között. Ezek a csoportok a voltaképpeni elsődleges csoportok. Életvitelükre jellemző a *térben mozgás* (nomádizmus); társas kapcsolataik alapvetően a *leszármazás* szerint alakultak. Tönnies három jelentősebb kapcsolati típust különböztet meg: 1. anya és gyermekei közötti kapcsolat; 2. házastársi kapcsolat; 3. testvérek közötti kapcsolat (TÖNNIES 2004, 14.). Rendkívül fontos a *közvetlenség.* A tagok egymással, egymás szeme előtt élnek, ezért ebben az értelemben nem is beszélhetünk nyilvánosságról, hiszen a közösség tagjai mindent együtt csinálnak. A tárgyaknak, eszközöknek elsősorban *használati értéküket* van: az az értékes, amit jól lehet használni. Annak következtében, hogy mindent együttesen élnek át, *sorsuk is közös*. Lényeges az *élők és a holtak egysége,* amely azt jelenti, hogy ha a közösség egy tagja meghal (nincs jelen), gondolatai az élőkkel maradnak, akik figyelembe veszik egy esetleges döntéshozatal során a halott vélelmezett szándékát. Az idő ciklikus az ünnepek, a rítusok körforgása révén. A közösségben *nincs titok.*

A társadalom a modernizáció terméke. Az idő „kiegyenesedik" a társadalmi körülmények között: a ciklikusság mellett megjelenik a valahonnan valahova tartó *idő* képzete. A társadalom a választó akarat terepe: ahol az egyénnek megadatik, hogy különböző alternatívák között kedvére *válasszon*. A társadalomban van *egyén,* a közösségben nincs. Az individuum ebben az értelemben Tönnies szerint nem természetes termék. Mint ahogy a város sem az, amely az individuum elsődleges otthona. A városi életből adódó különböző lélektani problémákat Simmel éleslátóan foglalja össze a *Nagyváros és a szellemi élet* című tanulmányában (1973), amelyben a városi lét egészen speciális lélektani „titkait" tárgyalja. Úgy tűnik, mintha a társadalom tagjai között kapcsolat lenne, miközben nincs: „nem állnak azonban lényegi kapcsolatban egymással, hanem inkább el vannak egymástól választva, s míg a közösség esetében a kapcsolat minden elválasztás ellenére is fennáll, itt fordított a helyzet: az emberek minden kapcsolat ellenére egymástól elkülönülten élnek" – fogalmaz Tönnies (2004, 48.). A társadalom tagjainak együttműködését különböző médiumok biztosítják (ilyen például a pénz), ami már nem a *használati érték,* hanem a sáfárkodásra alkalmat adó *csereérték* terepe. A bürokrácia gondoskodik a rendszer felépítményéről. Megjelenik az *ideológia,* s ennek következtében a *propaganda*. A társadalomban az együttélés feltételeire, normáira a szemtől szembeni *(face to face)* kapcsolatok hiánya miatt szükségképpen (fel)ügyelni kell: így lesz a *szokásokból jog.* A társadalom körülményei között erőteljes szekularizációs és racionalizációs folyamatok zajlanak, aminek következtében egyre inkább jelentőssé válik a tudomány szerepe. Demokratikus berendezkedés esetén a szabad önkategorizáció révén jól körvonalazható csoportok jönnek létre, amelyek elsődlegesen egyéni választások függvényében alakulnak. Azonban ezek a csoportok már *másodlagosak.* A társadalom rétegződik: az egyének eltérő tulajdonságai, érvényesülési lehetőségei miatt *egyenlőtlenségek* keletkeznek.

A közösség és a társadalom imént felsorolt ideáltípusai megjelennek az információs társadalom különböző megközelítéseiben, s érdemes mindig alaposan átgondolni, hogy éppen

melyiket, illetve a különböző megközelítésekből mely részletet érdemes használni. Például a közösség azon jellemzőjét, hogy vérségi kapcsolatok mentén történik a leszármazás számontartása, az online közösségekben egy az egyben nyilvánvalóan nem lehet használni. Különböző online játékok esetén erre mód nyílhat, ugyanakkor azok olyan tematikus közösségek, amelyek kifejezetten egy-egy fikciós játék mentén szerveződnek. Ugyanakkor a közösség Tönnies-féle meghatározásából bizonyos online közösségek esetén érdemes lehet valamiféle lényegakarathoz hasonlatos, szoros együttműködésen alapuló közösségi jellemzőt kiemelni. Az internethasználók magas számának következtében teljesen egyértelmű, hogy mind a közösségi, mind a társadalmi társulási forma releváns az információs korban.

1.2.1. Csoportjelenségek: kategorizáció, normaképződés, többségi és kisebbségi vélemény

Akár közösségi, akár társadalmi együttélési formákról beszélünk, a *kis csoportos helyzet* mindkét esetben megjelenő formáció, amelynek alapegysége a *diád* és a *triád*. A triád nemcsak a vélemények polarizálódása, hanem a csoporton belüli szövetségek, a meghatározó véleménytöbbség szempontjából is rendkívül fontos, elemi alakzat. A hétköznapi nyelvben általában a legalább háromfős formációknál szoktuk a „csoport" szót használni. Tudományos értelemben a csoport határai többnyire az észlelési képességek függvényében alakulnak. A kis csoportok létszámát az egy időben érkező maximális számú ingerek feldolgozása nyomán szokás megállapítani. Így a kis csoport határa 7±2 fő. Ennél több emberre azonos időben nem lehet érdemben odafigyelni. A következő határt a 20–25 fős csoportok jelentik, amelyek még – ugyan hosszabb idő alatt, de – képesek közösen *face to face* alapon döntést hozni (Csepeli 2014). Ebben a formációban modern körülmények között viszont már megjelennek a klikkek. Lényeges hangsúlyozni a „modern körülményeket", tekintettel arra, hogy az egykori közösségekben a *lényegakarat* és az *individuum hiánya* miatt a klikkek kialakulásának a valószínűsége erőteljesen a nullához közelített. A prehisztorikus időszakban ennél nagyobb csoportokat már kifejezetten kisebb (letelepedett) falvaknak tekinthetünk: a 100–150 fős közösségek már kívül esnek a folyamatosan mozgó hordák határain. Ahogy arra Dunbar kutatásai során már utaltunk, ez a nagy csoport határa, amelynek tagjai kellő mélységben ismerik egymást, ahol hálózati értelemben még lehetséges a teljes gráf, illetve az, hogy mindenki ismerje a másikat. Ennél nagyobb csoportok már szükségszerűen formalizálódnak, s a formális csoportokra jellemzően közvetítő eszközök is megjelennek a tagok között (ezek emberek – hidak – éppen úgy lehetnek, mint materiális vagy nem materiális közvetítők).

A csoportokat és a nagyobb társulási formákat is elsődlegesen az emberi elme rendezettség iránti igénye teremti meg.[6] Ahogy arról korábban már volt szó, az egyik, talán leginkább elementáris és totális rendező és rendszerező eszköz a nyelv. Ez kategóriák révén hozza létre azt az állványzatot, amely mind a társas világ, mind a környezet tekintetében támpontul szolgál mindazoknak, akik az adott nyelvet beszélik. Az offline térben voltaképpen a nyelvi határok jelentik a legdurvább kategorizációs határt: a határon innen vagyunk

[6] Ne menjünk bele részletesen a rend filozófiai, metafizikai problémájába, de természetesen nem triviális, hogy mi tekinthető rendnek, rendezettségnek (Polányi 1994).

„mi” – a beszélők –, s azon túl „ők” – a nyelvünket nem beszélők. A kategorizáció azonban ennél elemibb folyamatokra is visszavezethető, egészen az észlelésig.

1.2.1.1. A kategorizáció

A *kategorizáció* jelensége szükségszerű emberi adottság. A világban való eligazodás, a káoszból a rend teremtése, ismeretelmélet és csoportközi viszonyok mind-mind olyan következményei és okai a kategorizációnak, amelyeket napi szinten megfigyelhetünk a társadalmi életben. 1963-ban Tajfel és Wilkes a kategorizációs jelenség elemi voltára hívták fel a figyelmet a ma már klasszikusnak számító kísérletükben.[7] Arra voltak kíváncsiak, hogy a kategorizáció befolyásolja-e az észlelést. Egészen banális feladatot adtak a kísérletben részt vevő egyetemistáknak. Vonalakat mutattak nekik, s az volt a feladatuk, hogy döntsék el, melyek a hosszabbak, s melyek a rövidebbek. A vonalak egymáshoz képest vett hosszúsága egyértelműen megállapítható volt. A kísérlet vezetői elgondolásaiknak megfelelően több feltételt (ingert) használtak a kísérlet során. Az egyik feltétel az volt, hogy nem volt semmi különös feltétel. Azaz a vonalakról kategorizáció nélkül kellett eldönteni a kísérleti személyeknek, hogy mekkorák. A másik két feltételt úgy állították elő, hogy a mutatott vonalak alá egy „A” vagy egy „B” betűt írtak. A vizsgálatban azt is tesztelni akarták a kutatók, hogy a kategorizáción kívül a vonalak valódi hossza is kapcsolatban van-e a vonalak hosszúságának észlelésével. Ezért a kategorizációs feltételt is két külön vizsgálatra bontották: az egyik esetben véletlenszerűen írták a vonalak alá a betűket, azaz a véletlenen múlt, hogy melyik vonal került az „A” feliratú, s melyik a „B” feliratú vonalak csoportjába. A másik feltétel esetén a kategorizációt nem találomra, hanem a vonalak valódi hosszúságának megfelelően alkalmazták. Tehát a négy rövidebb vonal alá az „A”, míg a négy hosszabb vonal alá a „B” jeleket írták. A kategorizáció erőteljesen befolyásolta a vonalak észlelését. Az „A” és „B” betűkkel jelölt vonalakat kategóriánként egymáshoz hasonlóbbaknak látták. Azonban rendkívül fontos kiemelni, hogy releváns különbségek abban az esetben adódtak, amikor a kategorizáció együtt járt a vonalak objektív hosszúságával. A kísérlet eredményeit Csepeli György a következőképpen foglalja össze: „Tajfel és Wilkes eredményei azt bizonyítják, hogy a kategorizáció eredményeképpen létrejövő észlelet egyszerre objektív és szubjektív tényezők műve. Ha nincs objektív támpont, amire a kategorizációs művelet alapulhatna, akkor a csoportosítás irreleváns marad, és nem képez fogódzót a tudat számára az ingerekkel való megbirkózás során. Objektív támpontra alapozva viszont a kategorizáció mintegy önálló életre kel, s tovább mélyíti a valóságos különbséget a látott ingerek egyes osztályai között. E tudati működés révén növekszik az áttekinthetőség és a rendezettség” (CSEPELI 1997, 464.).

[7] A kis csoportok vizsgálatának kézenfekvő módszere a kontrollált kísérletezés. Lényege, hogy a kísérletben részt vevőket két csoportra bontják (kísérleti csoport és kontrollcsoport). A kísérleti csoportot valamilyen inger hatásának teszik ki a kísérlet vezetői, míg a kontrollcsoportot nem. Az ingeren kívül minden feltétel, hatás azonos a két csoport esetében. A kérdés az, hogy az ingerfeltételnek kitett csoportot megváltoztatja-e az inger. Amennyiben igen, akkor az adott inger hatással van a csoportra. Kis csoportok vizsgálata esetén viszonylag jól alkalmazható a kísérleti módszer, tekintettel arra, hogy a külső feltételek igen jól kontrollálhatók. Vegyük példaként a kategorizáció jelenségét.

Tehát a kísérletből láthattuk, hogy a kategorizáció erősen meghatározza az észlelést és azon keresztül a világban való eligazodást. A kísérlet online körülmények között is megismételhető, s az eddigi tapasztalatok szerint az online rendszer feltételei között hasonlóan működik. A vizuális kommunikáció miatt az ingerek a képernyő esetében talán egyértelműbben is hatnak, ezért feltételezhetjük, hogy Tajfel és Wilkes kísérletének az elektronikus környezet körülményei között még a korábbinál is nagyobb jelentősége van. Azért is, mert az online környezetben elmosódottabbak a határok, ami kevesebb támpontot kínál az eligazodáshoz, a közlekedéshez. A kategóriák ebben a környezetben kifejezetten hasznos mankóként szolgálnak. Az online közösségeknek, csoportoknak szükségszerűen ilyen funkciójuk is van, de más irányból is jó szolgálatot tesznek ezek a közösségek. Éppen a támpontok hiánya miatt az önmeghatározás is jelentős nehézségekbe ütközik, ezért például számos tulajdonság, amelyet offline többé-kevésbé azonnal látunk a másikon, online külön hangsúlyozásra szorul. Például az, hogy valaki idősebb-e vagy fiatalabb, egyáltalán a testi vagy a szociológiai jegyek kifejezetten ilyen jellemzők. Az ilyen jellegű identifikálást nagyban elősegítik az online csoporttagságok. A bizonytalan határok a kategóriákkal való játékra is lehetőséget adnak: arra, hogy a különböző virtuális közösségek között a felhasználó ki-be járkáljon. Ebben az esetben a virtuális közösségek valamiféle álarcosbálként értelmezhetők. Negroponte (2002) is utal erre, amikor a bitek és az atomok világa közötti különbséget vázolja fel. Lényeglátó megfogalmazása szerint az atomok világában *testek* vannak, míg a bitek világában (online) *akciók*. Ezek révén alakul ki a virtuális közösség. A bizonytalan határok, kategóriák okozta bizonytalan helyzetek *visszaélésekre* is alkalmat adnak.

Az elektronikus eszközökkel kibélelt világba születetteket talán még nagyobb nehézségek elé állítja a bizonytalanság bizonyossággá változtatása. A személyiségfejlődés során rendkívül fontosak a körülöttünk élő emberek visszajelzései. Nem elég, hogy saját magunkat valamilyennek tartjuk, az is szükséges, hogy mások is annak tartsanak bennünket (amennyiben valamilyen harmonikus közösségben élésre törekszünk). Pontosabban fogalmazva, attól (is) tartjuk magunkat valamilyennek, mert a többiek visszajelzik, visszaigazolják, *visszatükrözik,* hogy olyanok vagyunk. Minden alkalommal, amikor egy társas helyzetbe beépülünk, alakul a felépített énünk (a társas helyzetben kapott visszajelzésekből, tükörképekből összeállított énünket nevezi Mead *me*-nek). Ezen kívül van az énnek az aktuális helyzetben spontán módon működő része – már-már függetlenül az aktuális felépített éntől (ezt nevezi Mead *I*-nak). Ideális esetben a *me* és az *I* harmonikus kapcsolatban van egymással, ezt nevezi Mead *self*-nek (Mead 1973).

Ahogy azt Mead tükör-én elmélete kapcsán is láthatjuk, az identitás kialakulásához nagy szükség van a *társas identitásra* is. Arról van szó, hogy a csoporttagság (beleértve ebbe a nagyobb közösségeket, nota bene a nemzetet is) támpontot ad; olyan koordinátarendszert kínál, amelyben létrejöhet az *I* és a *me* egysége: a *felépített én.* A digitális bennszülöttek – azaz annak a generációnak a tagjai, akik számára születésüktől fogva természetes környezetet jelentenek az elektronikus kommunikációs eszközök (Csepeli–Prazsák 2010, 148.) – esetében ez a koordináta-rendszer az internetre költözött. A határok bizonytalanságával a koordináta-rendszer is bizonytalanabbá vált, kevesebb támpontot nyújt az identitás kialakításához. Az *ontológiai bizonytalanságérzet,* amely offline körülmények között is megoldásra váró feladat, az elektronikus környezetben még nagyobb problémát jelent. Márpedig az életben valamiféle válaszokat kell találni a *Ki vagyok én?* kérdésre, arra, hogy hol a helyem, s mi a feladatom. A csoportokra, közösségekre a kategorizáció miatt is komoly

feladat hárul.[8] Azonban azt is látnunk kell, hogy a nyitott, online csoportok többnyire lényegesen esetlegesebbek, mint az offline csoportok, ezért aztán a stabil koordináta-rendszert is lényegesen nehezebben tudják biztosítani. A digitális bennszülöttek, az online, digitális generáció esetében rendkívüli veszélyt jelent a magukra maradás. *Elveszett generációról* beszélhetünk.

A határok plauzibilitása, a bizonytalanság azonban arra is alkalmat adhat, hogy olyan viszonyítási pontok jöjjenek létre, amelyeket a felhasználók saját maguk hoznak létre saját maguknak. Számukra nem a beleszületett, mások által elkészített struktúrák adják a koordináta-rendszert. Az ilyen típusú folyamatok elindulását a csoporton belüli természetes normaképződés is elősegíti, mégpedig a leginkább elsődleges, észlelési szinttől kezdve.

1.2.1.2. A normaképződés

A *normaképződés* legalább olyan elementáris jellemzője a csoportoknak, mint Tajfel és Wilkes kísérletében az észlelésnek a kategorizáció. Muzafer Sherif kísérlete éppen erre mutat rá. Elképzelése szerint a normaképződési folyamat tulajdonképpen a *vonatkoztatási keret* kialakulása. A kutató a normaképződést vizsgálta, laboratóriumi körülmények között objektíven rendkívül bizonytalan helyzetet előállítva, amelyet az *autokinetikus effektus* felhasználásával hozott létre. Leegyszerűsítve: fénypontot vetített a falra egy teljesen sötét helyiségben, s arra kérte a kísérleti személyeket, hogy számoljanak be a fénypont látszólagos mozgásáról (amely valójában nem mozog, de az autokinetikus effektus következtében mozgónak látja a néző). A helyzet bizonytalansága nemcsak abban állt, hogy a mozdulatlan fénypontot mozgónak észlelték a kísérleti személyek, hanem abban is, hogy saját maguk pozícióját is elveszítették a viszonyítási pontok hiánya miatt. Sherif arra volt kíváncsi, hogy ilyen szélsőségesen bizonytalan helyzetben milyen viszonyítási pontot hoz létre az egyén, illetve a csoport. Ha „egy vonatkoztatási pont hiányzik a külső ingermezőben, belsőleg jön létre, amint az ingerek sorban követik egymást" – vezeti be Sherif (1973, 234.) kísérletének ismertetését tanulmányában. A „belsőleg" az egyén szintjét jelenti, azonban hasonló folyamat zajlik a csoport szintjén is. Ez utóbbi, csoportos helyzetben megjelenik a „sugalmazás" és egyáltalán: a csoporthelyzet. A normaképződés pedig mind az egyén, mind a csoport szintjén végbemegy. Éppen ezeknek a folyamatoknak a vizsgálatáról szólt a kísérlet.

Az elképzelés tisztázása érdekében két nagyobb helyzetet teremtettek: az egyikben csak a vizsgálati személy és a kísérletvezető volt jelen. „Az eredmények félreérthetetlenül azt mutatják, hogyha az egyének mindennemű más összehasonlító standardot nélkülöző mozgást észlelnek, szubjektíven olyan mozgás-tartományt és e tartományon olyan pontot (standardot vagy normát) alakítanak ki, amely sajátosan jellemző az illető egyénre, és különbözhet más egyének tartományától és pontjától (standardjától vagy normájától)" (SHERIF 1973, 239.). Tehát a kialakított standard egyénekre jellemző. Ezek után az azonos, objektív támpontoktól mentes, bizonytalan helyzetek esetében az egyén „ragaszkodik"

[8] Például az önsegítő csoportoknak rendkívüli jelentőségük van a traumatikus helyzetek feldolgozásában. Az offline önsegítő csoportok ma már az internetre költözhetnek. Ilyen például a közösségépítő portálon szerveződő, a családon belüli bántalmazást elszenvedettek csoportja. A csoport zárt, és e jellemzőjének fenntartása különösen fontos a megfélemlítettek biztonságának megőrzése miatt. Ebben az esetben egy olyan csoportról van szó, ahol a kategóriahatárok a fennmaradás, a csoport működésének zálogát jelentik.

a saját maga által korábban kialakított standardhoz. S ez már a kísérleti személyek közös jellemzője. A kísérlet ebből a szempontból is rendkívül tanulságos, tekintettel arra, hogy egyértelmű bizonyítást nyert: önmagában az egyén sem képes vonatkoztatási keret nélkül meglenni. A kísérletet követő beszámolók is kifejezetten erre utalnak. Sherif a kísérlet után írásos visszaemlékezéseket is kért a kísérleti személyektől. A visszaemlékezések a kísérlet hipotéziseinek megfelelően két csoportba rendeződtek. Egyfelől a bizonytalan helyzetre, a vonatkoztatási keret hiányára utaltak a következő válaszok. „A sötétben nem volt támpont a távolsághoz" – mondta az egyik résztvevő. Egy másik kísérleti személy a következőképpen emlékezett vissza: „Nem volt fix pont, amelyről meg lehetett volna ítélni a távolságot." Másfelől, ezzel összefüggésben olyan visszaemlékezések is voltak, amelyek kifejezetten a standardok hiányára adott reakciók kialakítására vonatkozó módszerekre utaltak. „Az előző távolsággal hasonlítottam össze" – számolt be saját módszeréről az egyik résztvevő. Másikuk pedig a következőket írta: „Az első becslést használtam standardnak" (Sherif 1973, 204.). Egyértelműen kiolvasható a fenti mondatokból a bizonytalanság, s a bizonytalan helyzettel kapcsolatos lelki disszonancia. No meg a bizonyosságra való törekvés is.

A kísérlet voltaképpeni lényegét a csoportszituációk vizsgálata jelentette. A csoporthelyzetben végzett vizsgálat kettős volt. Egyfelől voltak olyan kísérleti személyek, akik elsőként egyéni helyzetben végezték el a feladatot, s utána kerültek a csoportba. Másrészt olyanok is voltak, akik rögtön a csoportos feltételbe kerültek. Az sem elhanyagolható különbség, hogy két- és háromfős csoportokat (diádokat, triádokat) alakítottak ki.

A csoporthelyzetben történő vizsgálat lényege nem csak és kizárólag az, hogy miként változtatja meg a csoportnyomás az egyén véleményét. A *konformitás* vizsgálatán túl az is kérdéses, hogy létrejön-e valamiféle egyén feletti minőség a csoportban. Tekintettel az egyéni vizsgálati helyzet eredményeire, amely során teljesen esetleges volt, hogy a kísérleti személyek külön-külön milyen normát alakítottak ki, elképzelhető, hogy a csoportos feltétel esetén – amennyiben igazolódik a hipotézis – olyan norma jön létre, amely közvetlenül egyetlen csoporttag véleményével sem esik egybe. Az egyén feletti minőség ebben az esetben egyértelműen meg is jelenne. A két csoportos feltétel megkülönböztetése azért is lényeges, mert bármilyen helyzetről is legyen szó, felnőtt emberek bizonyos normákkal, diszpozíciókkal lépnek be a különböző helyzetekbe. Ez azt jelenti, hogy ha az egyéni feltétel után vett részt a csoportos feltételben a kísérleti személy, akkor az egyéni feltételben kialakított (belső) standardjával érkezett a csoportba. Fordítva pedig a csoportos feltételben kialakított normával érkezett az egyéni feltételbe. Kérdéses, hogy melyik milyen hatással volt az észlelésre (ha egyáltalán befolyásolta azt). A csoportos feltétel esetén a kísérleti személyek egymás előtt mondták el a fénypont mozgására vonatkozó ítéleteiket. Sherif a természetes helyzet fenntartása érdekében nem adott meg előre sorrendet: a tagok olyan sorrendben válaszoltak, ahogy akartak. Felmerült a véleményvezérség kialakulásának a problémája. Erre azonban az eredmények függvényében azt a választ adták, hogy mivel egymás után több próba is volt, nemcsak az első véleménye hatott az utolsó megszólaló véleményére, hanem fordítva is. Azaz a „ténylegesen kitapintható csoportbefolyás időben alakult ki, nem pedig egyetlen bemutatás eredménye" (Sherif 1973, 246.). Ebből a szempontból rendkívül fontos, hogy több hasonló döntési helyzet legyen (legyen időbelisége a csoportnak), s az is, hogy a döntések a csoport nyilvánossága előtt történjenek. Azaz mindegyik csoporttag tudjon a másik döntéséről. Az online világban természetesen ugyanúgy fontos az időbeliség. A közös sors, a különböző közös jellemzők (érdeklődési körök, hangsúlyozott

szociológiai jellemzők) megélése mindenképpen fontos tényező, azonban az *együttes élmény* is: az, hogy egyszerre, együtt éljenek át valamit a csoport tagjai.

A kísérleti eredmények egyértelműen alátámasztották a hipotéziseket. A kvantitatív eredményekből megfigyelhető volt, hogy a csoportos feltétel hatására közeledtek egymáshoz a vélemények. Azt is jól lehetett látni, hogy a vélemények közeledése akkor volt a legnagyobb, amikor nem egyéni, hanem rögtön csoportos helyzettel indult a kísérlet (függetlenül attól, hogy két- vagy háromszemélyes csoportban történt a vizsgálat). Abban az esetben, amikor az egyéni vizsgálati helyzetre következett a csoportos, a különböző standardok konvergenciája lassabban történt. A csoportnorma kialakulásáról az egyik résztvevő a következőképpen válaszolt arra a kérdésre, hogy befolyásolták-e a többiek vélemények: „Igen, de nem egy-egy alkalmon belül. Ítéletem minden egyes esetben megvolt már, és nem változtattam rajta, bármit mondtak is a többiek. A következő alkalmaknál azonban hozzáigazítottam ítéleteimet az övékéhez. Több alkalom után befolyásolt engem és látásom módosítására késztetett az, hogy addig egyetértettem-e a többiekkel vagy nem" (SHERIF 1973, 249.).

Az is problémaként merült fel, hogy nem voltak helyes vagy helytelen ítéletek. Senki nem mondta meg, hogy a becslés során mennyit tévedett a kísérleti személy. A közösségi norma kialakulása a csoporthelyzet szükséges velejárója, hiszen megoldásokat kínál az imént jelzett problémákra. Amikor első ízben találkozik a csoport strukturálatlan helyzettel, rögvest elindul a normaképződés (a vonatkoztatási keret kialakítása). „Ha a csoportnál a következő ülések folyamán emelkedik vagy süllyed a kialakult norma, ez csoporthatás" (SHERIF 1973, 247.). Ahogy az egyéni helyzetben az egyéni standardok teljesen különböztek egymástól, úgy csoporthelyzetben is értelemszerűen arra számíthatunk, hogy a kialakított normák csoportonként különböznek egymástól (amennyiben több csoportban is elvégezték a kísérletet). Ebben az esetben viszont már csoportközi viszonyokról van szó. A kísérleti helyzet természetesen változtatható, s így bizonyos esetekben a csoportközi különbségek kategorizációs tényezőkké válhatnak. Sherifnek is az a voltaképpeni célja, hogy kapcsolatot teremtsen a kísérleti szociálpszichológia és a társadalmi folyamatok értelmezése között.

A kísérlet nyomán két dolgot lényeges kiemelni. Egyfelől azt, hogy észlelési helyzetről van szó. Az észlelés és az annak alapján végzett cselekvés közötti kapcsolatok feltárása más kérdés. A kísérlettel kapcsolatban fel kell hívni arra a figyelmet, hogy annak menetét nem befolyásolták érdekek, egyéb erők, nyomások. Ez azért lényeges, mert érdekek által befolyásolva *egyensúlytalan* helyzetek alakulnak ki, amelyek feszültséggel teliek. Ilyen helyzetekben a kialakított normák a feszültség csillapítására, megszüntetésére szolgálnak. Amennyiben a normák nem csökkentik a feszültséget, akkor új normaképződési folyamatok indulnak el. Mindez az online csoportok normaképződése szempontjából is rendkívül lényeges.

Az online térben az általános vonatkoztatási keretek legalább annyira bizonytalanok, mint amennyire az autokinetikus effektus következtében a kísérleti személyek bizonytalanok voltak Sherif kísérletében. Az egyértelmű bizonyosságot adó visszajelzések inkább próba-szerencse játék során működőnek bizonyuló helyzetekre vonatkoznak. Tekintettel arra, hogy az offline világban a közlekedés többnyire valamilyen cél irányába történik (megyünk valahova), az online világ ebben is jelentősen különbözik. Sokkal inkább *keresgélésről,* bóklászásról, ide-oda kattintgatásról, *felfedezésről* van szó az e-akciók során, mintsem konkrét cél irányába való haladásról. Ez a bolyongás ugyancsak a kiszámíthatatlanság

terepe. A bizonytalanságot tovább fokozza, hogy miközben a fizikai térben valamennyi érzékszervünk által jól azonosítható *célállomások* vannak, addig az online világ *kikötőinek* bitjei jóval inkább a képzelet, semmint az érzékszerveink által megfogható vonatkoztatási keretet jelentenek. A Negroponte (2002) megfigyeléseiből és gondolataiból származó előbbi dichotómiák mind-mind arra utalnak, hogy a normaképződés lényegesen nehezebben megy végbe az online világban, miközben roppant szükségük volna rá az online közlekedőknek.

1.2.1.3. A csoport funkciói

Érdemes még legalább egy bekezdés erejéig a csoportok funkciójának néhány további aspektusát megemlíteni. Miért van csoport ahelyett, hogy ne lenne? Miért alakítanak csoportokat az emberek? Bales (1950) a csoportokban megjelenő szerepeket két nagyobb halmazba sorolja. Egyfelől a csoportcél megvalósításáért felelősek szerepeire, másfelől pedig a végrehajtókéra (ebből a szempontból csoportvezetési kérdéseket is felvet Bales elmélete). Ez az elkülönítés alapvetően a csoport munkájának, céljának a szempontját emeli ki: a *produktivitást.* Azonban Bales is felhívja a figyelmet arra, hogy a csoport funkciója kettős: a *produktivitáson* kívül a *szolidaritás* igényét is kielégíti, a kettő pedig egymást erősíti. A huszadik század elején a kísérleti szociálpszichológiai kutatások éppen ennek a két tényezőnek a jelentőségét hangsúlyozták. Frederick Winslow Taylor 1911-ben kiadott, *The Principles of Scientific Management* című munkája (amely magyarul *A tudományos irányítás alapelvei* címen jelent meg) kifejezetten a produktivitás problémáját járja körül. Az üzemszociológiai megfontolások szerint a csoport produktivitása fokozható a munkafolyamat tervezésével, a megfelelő munkaerő kiválasztásával, valamint megfelelő képzésükkel. Azaz a termelékenység (illetve a csoport produktivitásának) fokozásához ezekre a mérnöki precizitással megtervezett elemekre van szükség. Taylort mit sem érdekelte maga az ember. A burzsoá kapitalista logika szerint – Marx (1955) kifejezésével élve – a munkást *beszélő szerszámnak* tekintette.

Az üzemszociológia következő nagy alakja, Elton Mayo az először 1933-ban megjelent, *The human problems of an industrial civilization* (magyarul *Az ipari civilizáció emberi problémái*) című munkájában a Western Electric vállalatnál végzett kutatásának eredményeit mutatta be és általánosította. A vállalatnál túl nagy volt a munkaerő fluktuációja és alacsony a termelékenység. Vagyis a Taylor-féle produktivitással volt baj. Mayo azt vette észre, hogy ez csak a probléma felszíne. Az igazi gond abból adódik, hogy a vezetők gazdasági érdekei – amelyek elsősorban a produktivitással függnek össze – és a munkások társas, érzelmi igényei között hatalmas szakadék tátong. Mayo arra hívta fel a figyelmet, hogy amíg ez a helyzet fennáll, addig nem lehet a produktivitás javulására számítani. Ez utóbbi érdekében el kell kezdeni foglalkozni a munkásokkal. Olyan társas helyzeteket, feltételeket kell teremteni, amelyekben a munkások nem érzik magukat felcserélhető gépeknek. Ki kell emelni minden munkást a névtelenségből: fontosságtudatot kell biztosítani a számukra. Fokozni kell az együttműködést, akár úgy megszervezni a munkafolyamatot, hogy együttesen tudják csak végrehajtani. Erősíteni kell a csoporttudatot. Ez a Mayo-féle elképzelés a munkaszociológiában a *human relations* irányzat nevet kapta. Jóllehet Mayo is a termelékenység, a produktivitás, a kapitalista gazdasági érdekek megvalósulásának problémájából indult ki, Taylorral ellentétben azonban nem az üzemek precízebb mérnöki

tervezése és kialakítása mellett foglalt állást, hanem a társas helyzetek javítása mellett. Tehát a csoportnak legalább két nagyobb funkciója van: a *produktivitás* és a *szolidaritás.* Azaz a csoport összességében nagyobb teljesítményre képes, mint az egyén (elsősorban mechanikus tevékenységek esetén). Másfelől a csoport biztosítja azokat az érzelmi szükségleteket, amelyek a társas helyzetek iránti igényből adódnak. Valódi, koherens csoportról csak akkor lehet szó, ha mind a produktivitás, mind a szolidaritás funkciói megjelennek. Az online csoportok esetében ugyancsak megfigyelhető ennek a két dimenziónak a jelenléte. Illetve ha közvetlenül nem is valamiféle munkacsoportról és munkáról van szó, a kognitív és az affektív jegyek akkor is jól elkülöníthetők. A megfelelően működő csoportnak mindkét dimenzióban sikeresnek kell lennie, így tudja kielégíteni a csoporttagok társas igényeit.

1.2.1.4. A csoport vezetése

Úgy tűnhet, hogy a csoport az ilyen típusú funkciói következtében a világ legcsodálatosabb képződménye. Azonban rengeteg veszélye, árnyoldala is van a csoportnak. Például a csoportvezetés dinamikájának megsértése számos visszaélésre adhat alkalmat. Kurt Lewin két kollégájával, Ronald Lippittel és Ralph White-tal végzett kísérletet szabadidőklubokban, tízéves fiúk körében (1969). Három különböző vezetési stílust alkalmaztak: *demokratikus, autokratikus* (parancsuralmi) és *laissez faire* (azaz ráhagyós) stílust. A produktivitás a „ráhagyós" csoportban volt a legalacsonyabb, ott, ahol voltaképpen mindenki azt csinált, amit akart: hiányzott az együttműködés. Esetenként verekedtek. A tagok nem érezték jól magukat. A *demokratikus* csoportokban folyamatosan dolgoztak, az idő felét produktív tevékenységekkel töltötték. Szívesen, kedvvel végezték ezeket az együttműködésre épülő foglalatosságokat, miközben kreativitásuknak is tér nyílt. Magas volt a szolidaritás és a csoport véleményének tiszteletben tartása. A legmagasabb szintű produktivitás (munkavégzés) a *tekintélyuralmi* rendszerben volt: az idő jelentős részét munkával töltötték. Nem is érezték jól magukat a tagok. Gyakori volt a szitkozódás, megjelent a feljelentés, a rombolás, a bűnbakképzés. Azaz a csoport szolidaritásfunkciója nem működött. A nyilvános konformitás szélsőséges méreteket öltött.

Lényeges a csoport vezetési stílusa, hiszen ennek függvényében a cybertér nemcsak a demokratikus, hanem az autoriter és az extrém csoportok kialakulásának és működésének is kedvez. Az egyoldalú propaganda sulykolásával a zárt csoport tagjainak információszerzési horizontja bezárul, ami kiváló terepet kínál a dogmatikus, tekintélyelvű gondolkodásnak. Mindez rendkívül kedvező körülményeket teremt a tekintélyelvű vezető és csoport megjelenésének.

1.2.1.5. Autonóm, konform, deviáns lelkek

A csoport másik problémája, amely a kategorizáció negatív hatása is lehet, hogy elveszhet az egyediség. Amennyiben a különböző jelenségeket egy-egy kategória alá soroljuk, elvész a jelenségek egyedisége, még akkor is, ha sok szempontból a különböző jelenségek egyediek. Például ha mindössze a „festmény" szóval jelöljük Munkácsy Mihály *A poros út* című alkotását és mondjuk Leonardo da Vinci *Mona Lisa* művét, úgy elvész az alkotások

egyik lényeges eleme: az egyediségük. Ez a folyamat zajlik a csoportban is, amennyiben nem nyílik tér az *autonómiának,* azaz szélsőséges *konformizmus* esetén.

Ahogy Sherif kísérletében (1973) is felvillant már a konformizmus jelensége, úgy más kutatók kifejezetten ezzel a kérdéskörrel foglalkoztak. Solomon Asch (1980) ugyancsak vonalakat használt kísérletéhez. Számára azonban ezek nem a kategorizáció eszközei voltak, hanem kifejezetten a *csoportnyomást* vizsgálta velük. Ő is a vonalak hosszúságával kísérletezett, azonban a vonalak megkülönböztető jegyének kategorizálása nélkül csak a hosszúságukat használta. Négy vonalat használt. A vonalak hosszúsága egyértelmű volt. Volt három különböző hosszúságú vonal, s még egy, amelyik valamelyikkel megegyezett. Nyolctagú csoportokba rendezte a kísérleti személyeket, s arra kérte őket, hogy mondják meg, hogy melyik két vonal egyforma a négy közül. Mindezt több körben, több vonallal: mindig megjelent a négy vonal, s ki kellett választani, hogy melyik kettő hasonlít egymásra. Csak mentek-mentek a körök, amíg egyszer csak valaki egyértelműen téves meghatározást adott. Ő volt (az egyik) beépített ember, akivel a kísérlet előtt a kísérlet vezetője egyeztetett. A kísérlet arról szólt, hogy amennyiben az objektív tényekkel ellentétes, erőteljes csoportvélemény alakul ki, mit tesz a kísérleti személy. Mindegyik csoportszituáció esetében „határozott tendencia volt megfigyelhető a többség álláspontjának a megközelítésére" (Asch 1980, 213.). A csoportnyomás ezzel együtt nem volt teljes. A kísérleti személyek becsléseinek 68 százaléka a csoportnyomás ellenére helyes volt. Nagyok voltak az egyéni különbségek: rendkívül polarizáltak voltak a kísérleti személyek. Több közülük mindvégig független maradt, mások mindvégig behódoltak. A kísérleti személyek egynegyede teljesen független maradt, ragaszkodott ahhoz, amit látott. Egyharmaduk viszont a próbák legalább 50 százalékánál behódolt a csoportnyomásnak. Az egyéni különbségek elemzése során Asch a következő személyiségleírásokat állapította meg. A csoportdinamika, a csoportfejlődés szempontjából is lényeges, hogy milyen típusú „autonómiákat" különböztettek meg a kísérletvezetők. Ezek a típusok az online térben is jól azonosíthatók.

Független (autonóm) kísérleti személyek típusai.

- „A függetlenség az illető személynek a saját észlelésébe és tapasztalatába vetett bizalmán alapul." Ebben az esetben arról van szó, hogy a független személy egészen egyszerűen jobban hitt a szemének, mint a többiek véleményének.
- „Merőben más típusba tartoznak azok a kísérleti személyek, akik függetlenek, de elhúzódók. Ők nem spontán, emocionális jelleggel reagálnak, hanem inkább bizonyos elveket követnek, amelynek értelmében azt vallják, hogy az ember maradjon önálló egyén." A függetlenség ezen típusa valamiféle ideológiailag értelmezhető függetlenséget jelent, mégpedig az egyén döntési jogának a függetlenségét.
- „A független kísérleti személyek harmadik csoportjánál jelentékeny feszültség és kétely tapasztalható, de ragaszkodnak ítéleteikhez, mert az vezérli őket, hogy megfelelően megoldják a feladatot" (Ash 1980, 215). A harmadik független csoport tagjainak legfontosabb jellemzője, hogy pragmatikusak. Adott egy feladat, és ők ezt a feladatot a lehető legjobban kívánják megoldani. Így aztán függetlenségre kényszerülnek.

Engedékeny (behódoló) kísérleti személyek típusai. Asch megállapítása szerint a konformizmusnak is több változata van.

- „Az észlelés torzulása a csoportnyomás alatt. Ebbe a csoportba igen kevés kísérleti személy tartozik. Ők teljes egészében engedtek, de nem voltak vele tisztában, hogy becsléseiket a többség módosította vagy eltorzította. Az interjú alkalmával végül azt mondták, hogy helyesnek észlelték a többség becsléseit."
- „A legtöbb behódoló személy átélte ítélete torzulását. Ebben a legfontosabb tényező a kísérleti személynek az az állásfoglalása volt, hogy saját észlelése pontatlan, és a többségé nyilván helyes. Ezeknek a kísérleti személyeknek a hibája az alapvető belső kétely és az önbizalomhiány; emiatt éreztek erős indítékot arra, hogy a többséghez csatlakozzanak."
- „E kísérleti személyek harmadik csoportjának eltorzult a cselekvése. Ők nem szenvedtek észleletük módosulásától, és arra sem gondoltak, hogy tévesen járnak el. Azért engedtek, mert mindennél nagyobb volt a szükségletük, hogy ne látszódjanak másnak vagy alacsonyabb rendűnek, mint a többiek, mert egyszerűen nem tudták volna elviselni, ha a csoport szemében fogyatékosnak mutatkoznak. Ezek a kísérleti személyek elfojtották a saját megfigyeléseiket, és teljes tudatában annak, hogy mit tesznek, megszavazták a többségi álláspontot" (ASCH 1980, 215–216.). A konformitást több tényező is befolyásolja. Leginkább a „hűséges társ" jelenléte. Amennyiben a kísérleti személynek volt olyan társa, aki ugyancsak a helyest választ adta, akkor a hibás ítéletek aránya 6 százalék alá csökkent. Viszont igen nagy traumát okozott, ha egy idő után eltűnt a hűséges társ: a hibák aránya közel 30 százalékra nőtt. A kompromisszumos társ (ingadozó) jelenléte viszont 75 százalékra növelte a hibás ítéletek arányát.

Asch kísérlete a konformizmus vizsgálatáról szól. A konformizmusnak ez a formája nyilvánvalóan valamiféle elkerülendő jelenség, az autoriter társas/társadalmi rendszerek egyik rendszerkövetelménye. Azonban a konformizmus nem szükségszerűen szitokszó. Nem kell mindig mindent újra kitalálni: érdemes másoktól átvenni a jó gyakorlatot. „Okos ember más kárán tanul" – tartja a mondás. A konformitást befolyásolhatja az inger *egyértelmű jellege* (strukturális világosság vagy zavarosság). Hasonlóan jelentős befolyásoló tényező, hogy mekkora a kísérletben részt vevő kisebbség aránya a többséghez képest. Henry Moore (1981) arra hívta fel a figyelmet, hogy a konformizmus a *témától* is jelentősen függ. Erkölcsi kérdésekben nagyobb konformitás várható, míg esztétikai kérdésekben kisebb. Ezek az autonóm és konform lélektani típusok megtalálhatók a cybertérben is.

A konformizmussal, a csoportnyomással szemben (szervezett) „ellenerők" is felléphetnek. Ők a *deviánsok,* azok, akik eltérő véleményen vannak. A vezetési típustól, a csoport rendszerétől erőteljesen függ, hogy mihez kezd a csoport a nem konform véleménnyel. A kisebbség többséget befolyásoló véleményének feltérképezése szempontjából ugyancsak több kutatás született. Míg Asch kísérletében a kisebbségi véleményt képviselők voltak a kísérleti személyek, addig Schachter kísérletében (1981) a többségi véleményen lévők. Arra volt kíváncsi, hogy mi történik abban az esetben, ha a többséggel ellentétes vélemény jelenik meg a csoportban. A kísérleti dizájnt nem kizárólag a csoport és az azzal ellentétes véleményen lévők között nézte, hanem ő is bevezetett egy „csúszkáló" véleményt. A kísérleti elrendezés szerint tematikus klubokat (szerkesztőklub, filmklub, rádióklub) alakítottak ki, ahol egy erkölcsileg értelmezhető esettel kapcsolatban kellett közös véleményt kialakítani egy fiatalkorú bűnöző történetéről, aki éppen büntetésre vár. Azt figyelték a kutatók,

hogy mi a sorsa a csoportban a „módusz", a „csúszkáló" és a „deviáns" véleményeknek. A csúszkáló vélemény kiszámíthatatlan volt: hol a többséggel volt, hol nem. A módusz vélemény mindig az volt, ami a leggyakoribb volt a csoportban. A deviáns pedig az lett, aki mindig a csoporttal ellentétes véleményen volt. A kutatás eredményeit több dimenzióban is értékelték. A „módusztˮ és a „csúszkálótˮ nem utasították vissza, a deviáns véleményen lévőt viszont igen. A visszautasítás mértéke attól is függött, hogy mennyire volt magas a csoport *kohéziója,* azaz mennyire volt „egybenˮ a csoport. Lényeges volt az is, hogy mennyire fontos az a kérdés, amelyben a deviánsnak eltérő véleménye volt: minél fontosabb volt, annál inkább elutasították a deviáns véleményen lévőt. Összességében az derült ki, hogy nem jó deviánsnak lenni. „A deviancia azzal a következménnyel jár, hogy a csoport szerepstruktúrájának peremjellegű pozícióiba jelölik a deviáns személytˮ (Schachter 1981, 293.).

A kutatások egy másik vonulata éppen annak a lehetőségét tárgyalja, hogy a kisebbségi csoportoknak milyen lehetőségeik vannak a többségi vélemény befolyásolására. Csepeli György a következőképpen foglalja össze ezt az irányzatot. „A hetvenes évek európai szociálpszichológiájában született a fenti kutatásokkal szembeni sajátos reakcióként az a kutatási irány, mely a kisebbség többséget befolyásoló lehetőségeire hívja fel a figyelmet [Moscovici–Faucheux 1972; Nemeth–Swedlung–Kanki 1980]. Ha a kisebbség tagjai határozott meggyőződésűek, jól kidolgozott alternatív ítéletekkel vagy vonatkoztatási keretekkel rendelkeznek, akkor esélyük van a többség befolyásolására. Nemeth és munkatársai szerint a többségnek arra az álláspontra kell jutnia, hogy a kisebbség következetes és határozott álláspontot vall, melyből semmiképpen sem hajlandó engedni. Ez kétkedésre indítja a többséget, s az önvizsgálat folyományaként kialakuló új csoportálláspont már a kisebbség hatását fogja tükrözni" (Csepeli 1997, 429.).

Petrovszkij (1980) tanulmánya a csoporton belüli konformitás jelenségét „balrólˮ előzi. A kutató Asch kísérletének alapvető problémáját a valódi csoport kialakulásának elmaradásában látja. Másfelől – jegyzi meg – nem lényegtelen az sem, hogy milyen tevékenységekről van szó a csoporton belül. Összességében arra mutat rá, hogy a csoporton belüli konformizmust maga a csoporthatás képes felülírni: „a társadalmilag hasznos tevékenységgel összefüggő feladatok megoldására társult emberek csoportjaiban a konformizmus valódi alternatívája nem a negativizmus (nonkonformizmus, makacsság, függetlenség stb.), hanem az igazi, nem színlelt kollektivitás, amelynek legfőbb sajátossága az, hogy lehetőséget biztosít az egyén számára az önmeghatározásra a csoporton belül – ezt nevezzük közösségi önmeghatározásnakˮ (Petrovszkij 1980, 239.). A szerző csak a produktivitás dimenziójában vizsgálódik, ami nyilvánvalóan összefügg azzal a társadalmi-gazdasági-politikai berendezkedéssel, amely a hetvenes években a Szovjetunióban jellemző volt. A diktatúra nyoma – ahogy a vezetési stílus kutatásából is láthattuk – erőteljesen felfedezhető a megközelítés mélyén, hiszen a szerző csak a produktivitást tekinti csoportmeghatározó tényezőnek. Mindenesetre arra a talán ellentmondásos következtetésre jut, hogy a csoport „túlkapásaitˮ a valódi – demokratikus – csoport körülményei között lehet szabályozni. A Petrovszkij által tárgyalt esetben egyértelmű, hogy a csoport formálisan, s nem önszerveződő alapon jött létre, ahol a vezetőket nem demokratikusan választották, hanem autoriter módon jelölték ki. Ezt természetesen a szerző nem mondhatja ki expliciten, de tanulmányában többször is annak hangsúlyozására kényszerül, hogy a csoportlélektani kutatásokat nem lehet egy az egyben alkalmazni a társadalmi rendszer, a társadalmi folyamatok értelmezése során.

A szerző további kritikája, hogy Asch teljesen jelentéktelen ingereket alkalmazott: „a jelentéktelen ingerek esetében az alkalmilag összeverődött csoport véleménye sokkal inkább befolyásolta az egyént, mint annak a közösségnek a véleménye, amelyhez az egyén különben tartozott" (PETROVSZKIJ 1980, 240.).

Amennyiben az önsegítő csoportokról írottakkal összehasonlítjuk Petrovszkij imént idézett mondatának tartalmát, arra juthatunk, hogy az online világban is szükséges a „jelentéktelen" és a „nem jelentéktelen" hajtóerők által létrejövő csoportok között különbséget tenni, még akkor is, ha objektíven nem minden esetben könnyű a kettőt megkülönböztetni. A „jelentéktelen" és a „nem jelentéktelen" nyilvánvalóan függ attól, hogy ki mit élt át az életében. Az átélt örömök, traumák, valamint azok a történések, amelyek sem örömöt, sem bánatot nem idéznek fel, minden ember esetében viszonylag egyértelműen elkülönítik egymástól a világ *jelentéktelen* és *nem jelentéktelen* szegmenseit. Nagyobb sorsközösségek esetében pedig az örömök és a traumák, a nagy sorsfordító események közösek is lehetnek (éppen ez a nemzedékek egyik jellemzője). Újabb elemzési lehetőségeket hordoz magában Petrovszkij sztratometriai elméletének azon része, amely a csoportok aktivitási szintjei közötti különbségeket hangsúlyozza.

- Az *interperszonális réteg* a leginkább felületi szint, ahol a konformitás is végbemegy – idesorolható a közösség kohéziójának, szociometriai jellemzőinek a vizsgálata. Jóllehet – fejti ki véleményét Petrovszkij – ezek nem lényegtelen jellemzők, felületesek a metafunkciók szempontjából. Az online színtéren ezeknek a szabályoknak a megsértése tulajdonképpen a csoportszerkezet megsértését jelenti.
- A kapcsolatokat és az interakciókat a *közösségi jellemzők* rétegében az együttes tevékenység tartalma, céljai, feladatai, értékei közvetítik, amelyek végső soron a társadalom életében gyökereznek (PETROVSZKIJ 1980, 247.). Azaz arról van szó, hogy ez a réteg a társadalmi berendezkedés egészéből származik. E berendezkedések alapján jön létre a „közösség értékorientációs egysége", ami alatt azt értjük, hogy „a csoport mint egész számára fontos tárgyak – személyek, eszmék, események – vonatkozásában a csoport tagjainak értékelései és álláspontjai nagymértékben egybeesnek" (PETROVSZKIJ 1980, 247.). Annak következtében, hogy ezek a csoportértékek kifejezetten összefüggnek a társadalmi rendszerrel, ebben a rétegben már erőteljesen megjelenik az ideológia, a társadalmi rendszer ideológiája. Tekintettel arra, hogy korabeli körülmények közötti diktatúráról van szó, a valódi interaktivitás hiányzott a (formálisan szervezett) csoportok és a társadalmi rendszer között. A terjedésről szóló fejezetben majd láthatjuk, hogy ez alapvetően az egyirányú tömegkommunikáció modellje, amely – mivel nem jelenhetnek meg benne a hivatalostól eltérő vélemények – egyértelműen propagandának tekinthető. A fejlett, demokratikus országokban manapság az internet biztosította interaktivitás révén akár fordított helyzet is elképzelhető, s meg is valósul. Olyan, amikor az alulról szerveződő közösségek vannak hatással a társadalmi rendszer egészére, a társadalmi rendszer ideológiájára (például a toleráns kulturális-társadalmi rendszer szempontjából). Az interaktivitás megjelenése nagyon erőteljesen társadalmi rendszert változtató tényező. Ebből a szempontból az interaktivitást biztosító korszerű kommunikációs eszközök kifejezetten forradalmi helyzeteket idézhetnek elő. Ilyen volt a 2011-ben elindult „arab tavasz" is,

amely végigsöpört Észak-Afrika és a Közel-Kelet diktatórikus berendezkedésű arab országain. A forradalmi hullám az interneten szerveződött, a rendkívüli interaktivitást és szociometriai értelemben szervezési lehetőségeket kínáló, képi és szöveges eszközök integrált használatára épülő közösségi portálokon.

- *„A közösség személyközi aktivitásának még mélyebb rétegeiben tapinthatjuk ki [...] a »felelős függés« kapcsolatait és viszonyait”,* a személyközi függéseket. Ezeket *„a közösség konkrét célra irányuló tevékenysége határozza meg”* (Petrovszkij 1980, 247.). Ez a réteg kifejezetten a csoport mélystruktúráit érinti. Ugyan nem lehetetlen az online közösségek ilyen szintű vizsgálata, azonban nem könnyű. Elsősorban azért nem, mert ebben az esetben nemcsak a „felelős függés” megfigyelése (vizsgálata) szükséges, hanem annak értelmezése során a csoport története is. Ezt pedig online antropológiai módszerekkel, a csoportokba való „beépüléssel” lehet vizsgálni. Energia- és időigényes módszerről van tehát szó.

Petrovszkij vizsgálati eredményei sajátos történelmi korszakban keletkeztek. Miközben a szerző reflektált a korabeli csoportlélektan főáramára, addig nem függetlenedhetett attól a társadalmi rendszertől sem, amely meghatározó ideológiájának meg kellett felelnie. Ha ezt az ideológiai leplet eltávolítjuk, az általa talált „rétegek” olyan elemzési módszert kínálnak, amelyek az online csoportok, közösségek vizsgálata során is jól használhatók.

A társadalmak berendezkedése napjainkban, az információs korszakban is, döntő módon meghatározza, hogy a cybertér mely szegmensei érhetők el a felhasználók számára, és melyek nem. Alapvetően Észak-Amerika, Ausztrália és Európa országainak többsége volt olyan 2016-ban, ahol nem volt bizonyíték a politikai természetű tartalmak szűrésére (World Bank 2016).

1.2.2. Értékrendszerek és az online világ

Sherif normaképződésre vonatkozó kísérleti vizsgálatából jól láthattuk, hogy bizonytalan helyzetben mind az *egyén,* mind a *csoport* szintjén kialakul a vonatkoztatási keret. Ez a vonatkoztatási keret, amelyen belül a cselekvések zajlanak, nagyobb társulási egységek esetén voltaképpen maga a kultúra. Ezen a helyen nem tárgyalhatjuk részletesen a kultúra különböző jelentésváltozatait (Fekete 2018), ezért a következőkben leegyszerűsítve emeljük ki néhány elemét. Kroeber, Kluckhohn és Untereiner 1952-ben megjelent könyvükben a „kultúra” száznál is több meghatározását elemezték (s nyilván azóta ezeknek a definícióknak a száma növekedett). Vizsgálatukból annyit mindenképpen szükséges kiemelnünk, hogy számos tudománynak van mondanivalója a kultúráról, illetve azzal kapcsolatban. A szerzők szerint a különböző meghatározások különböző nézőpontokból tekintenek a kultúrára. Így beszélhetünk leíró, történeti, normatív, pszichológiai, strukturális és genetikus kultúrameghatározásokról. A szerzők meglátása szerint azonban a különbségek mellett számos hasonló eleme is van a definícióknak. Ilyen például az, hogy a kultúra *szimbólumokban* nyilvánul meg. Ezek társadalmilag konstruáltak, az egyén számára többnyire adottak, ezért aztán viselkedését is befolyásolják. A szimbólumok esetében szükséges megkülönböztetnünk a *tárgyiasult* és a *nem tárgyiasult* szimbólumokat: egyáltalán a szimbólumok láthatóságának problémáját. Egy mozdulat, egy szó, akár egy dallam (például a Himnusz)

lehet olyan szimbólum, amelynek nem kell szükségszerűen tárgyi, illetve vizuálisan formalizált alakkal rendelkeznie, miközben nagyon sok ember számára közös vonatkoztatási keretet nyújt. Akár egy gondolat is lehet szimbólum. A szimbólumoknak ez a variabilitása az ember szempontjából igen lényeges tényező. Az ember számára minden lehet információ, minden lehet szimbólum. Ezért aztán egyértelmű, hogy az online világban is vannak olyan toposzok, amelyek szimbólumként funkcionálnak. A közösségek méretének nyilvánvalóan vannak kognitív határai, azonban a hálózatosodás következtében a normaképződés ennél jóval szélesebb körben jelentkező folyamat napjainkban.

1.2.2.1. Az online közösségek – elképzelt közösségek

Természetesen azt nem lehet minden helyzetben tökéletesen meghatározni, hogy bizonyos, főleg létszámuknál fogva nagy csoportok (például a nemzet) esetében hány emberre terjed ki az adott szimbólum meghatározó ereje. Már csak azért sem, mert egy-egy szimbólumhoz nemcsak pozitívan, de negatívan is lehet viszonyulni. A nemzet esetében például az sem egyértelmű, hogy van-e, illetve ha igen, milyen módon van földrajzi relevanciája. Egyáltalán, hogyan képesek megjeleníteni a szimbólumok például a nemzetet, amely ugyancsak nem megfogható, nem látható jelenség. Ezért is nevezi a nemzeteket Benedict Anderson (2006) *elképzelt közösségeknek.* Ebből a szempontból az online világ közösségei rendkívül hasonlatosak a nemzetekhez.

Ha csoportosítani kívánjuk az online tér közösségeit, akkor talán a legelemibb csoportosítást az online-offline természetük alapján végezhetjük el. Ennek alapján vannak olyan közösségek, amelyek csak és *kizárólag online természetűek*. A szereplők soha nem találkoznak szemtől szemben, csak egymás nickneveit ismerik, esetleg néhány homályos sajátosságot arra vonatkozóan, hogy ki is lehet szociológiai jellemzői alapján a másik. Többnyire azonban még ez sem érdekes. Példaként olyan vásárlói csoportokat hozhatunk fel (eBay), amelynek tagjai az egész világról származnak. A közösség tagjai el is adnak és vásárolnak is, a tagoknak mégsem kell szükségszerűen ismerniük egymást. Elég, ha megbízható módon értékelik a közösség többi tagjának eladói, illetve vevői gyakorlatát. A közösség voltaképpen ezekből az értékelő tevékenységekből származó, elképzelt virtuális hálózat. A felhasználó számára „elképzelt", de a rendszer üzemeltetői számára nagyon is valóságos. A gyakorlati tapasztalatok, információk ebben a vásárlói közösségben is rendkívül fontosak.

Az információk egy sajátos megosztási módja (kommunikálása) a Wikipédia. Ennek a közösségnek a tagjai az eBay közösség tagjaival szemben sokkal nagyobb mértékben *ismerik egymást*. Ennek az *egymást ismerő közösségnek* a tagjai időről időre offline is találkoznak, és a nicknevek mögé nézhetnek. Ma már a legtöbbjük először online kapcsolódik a közösségbe, s ezek után vesz részt az offline találkozókon. Szükséges hangsúlyozni, hogy a Wikipédia nem egyenlő a wikiszoftverrel. Számtalan rendszer van, amely wikiszoftvert futtat, azonban értékrendjükben, felfogásukban jelentősen különböznek a Wikipédiától, amelynek filozófiája az, hogy mindenki számára hozzáférhetővé tegye a tudást, amelyet senki sem monopolizálhat. Az emberiség tudásához mindenkinek joga van hozzáférni. Egészen egyszerűen azért, mert embernek született (PRAZSÁK 2014).

Végül, de nem utolsósorban olyan közösségek is vannak, amelyek *elsősorban offline közösségek,* s kiterjesztéseik az online közösségek. Ilyen például egy városi társasház

lakóközössége. Azonos földrajzi helyen élnek, többnyire találkoznak is egymással, s ezzel együtt szervezési és egyéb ügyeiket online intézik. A normák képződése ez utóbbi esetben többnyire az offline létrejött normák online migrációjával valósul meg (például tegeződik-e a lakóközösség két tagja, ami nyilván változhat – természetesen azon nyelvek esetében, ahol van magázó formula).

A Wikipédia, illetve az ahhoz hasonlító online közösségek, amelyek offline-ná válnak, sokkal inkább a tematika, a filozófia, az ideológia mentén szerveződnek. Ahogy a francia enciklopédistáknak, úgy a wikipédistáknak is a tudás összegyűjtése, megosztása, s mások számára elérhetővé tétele jelenti tevékenységük fő célját. Ez az örök érvényűnek tűnő ideológia jelenti a normát. A Wikipédia esetében a (szellemi) közösség online alakul, s onnan kerül át az offline világba. Az eBay típusú kereskedői-vásárlói közösségek alapvetően a rendszeradminisztrátorok (21. századi közösségszervezők) rendszerépítő tevékenységének megfelelő szabálykészlettel rendelkeznek. Természetesen itt is lehetnek önszabályozó elemek (például trágár minősítés kerülése), azonban a normák alapvetően a rendszer vonatkoztatási keretének függvényében alakulnak. Az adminisztrátorok által a rendszerben létrehozott *látens kapcsolatok* jelentik az egyik lehetséges bizalmi alapú kapcsolattípust. A rendszer alapvető problémája éppen a bizalom, amelynek kialakulása kérdéses is, tekintve, hogy a felhasználók nem ismerik egymást személyesen. Maga a rendszer tulajdonképpen arra vállalkozik, hogy ezt a bizalmi helyzetet programozza (még annak árán is, hogy nem eldönthető vita esetén a rendszer üzemeltetője bevállalja a felmerült költségeket). A leginkább kritikus elem a fizetés. Bankkártyaszámot megadni, előre utalni számos kockázatot rejt magában. A kereskedelmi rendszer viszont megvásárolt, és rendszerébe integrált egy olyan fizetési alkalmazást, amellyel garantálni tudja a biztonságos fizetést a világ különböző szegleteiben élő emberek számára. Ennek a fizetési rendszernek a lényege, hogy minden felhasználó megbízhat benne (mert „hivatalos"), s így aztán minden szereplő érdekelt a tranzakció közös sikerében. A fizetési rendszer használatának természetesen ára van. Ez a fizetési rendszer abból él, hogy a bizalommal kereskedik. Az ilyen típusú online közösségekben a bizalmat a *látens kapcsolatok*[9] rendszerbe kódolásával próbálják megteremteni. Ez a kódolási mechanizmus jelenti voltaképpen a rendszer normáját, a rendszer által létrehozott kultúrát.

1.2.3. Az offline normák hatása az online akciókra

A norma olyan vonatkoztatási keret, amely megteremti a társas interakció, a társas élet kereteit. Többé-kevésbé egyértelmű szabályok sorozatával jelöli ki az egyén tiltott és a kívánatosnak tartott viselkedéseinek spektrumát. A normaképződés sajátos emberi tulajdonság; csoportlélektani folyamatokon túl az emberi csoportosulások egyéb eszközei is elősegítik. Mindegyik mögött az (ön)meghatározás igénye áll. A *kommunikációnak* elsődleges szerep jut a meghatározási folyamat során. Bármelyik kommunikációs modellt is alkalmazzuk, az *interaktivitás* – legalább elvi szintű jelenléte – nélkül nem beszélhetünk kommunikációról. A kommunikációra és a társas kapcsolatokra épülve – ahogy láttuk – komoly feladat

[9] Látens kapcsolatoknak nevezzük azokat a potenciális kapcsolatokat, amelyek még nem alakultak ki, azonban a technikai feltételek biztosítottak ahhoz, hogy létrejöjjenek, nota bene technikailag léteznek (Genoni –Merrick–Willson 2005).

hárul a *csoportokra* is, amelyekben kialakulnak az elsődleges normák. Lényeges a *hagyományozás* mechanizmusa, az, hogy a csoporthoz korábban és később csatlakozók között biztosítható legyen a csoport történetének az átadása. Az aktuális tagok számára is nélkülözhetetlen a hagyományozás, tekintettel arra, hogy a közös élmények felemlítése újabb közös élményeket jelent. Ezen túl pedig azért is, mert *célkijelölő,* és fokozza a tagok *elköteleződését.* Rendkívül lényeges a hagyományozás technikája, az online világban ugyanis semmi sem vész el. A bitek nem égnek le (mint az alexandriai könyvtár), szóval a fizikai környezetből érkező támadások kivédhetők.[10] Ezzel együtt az offline világ információtároló modalitásai az interneten is megtalálhatók: orális, írott, képi (mozgófilm) dokumentumok.

A normák ezen összetevőire figyelemmel idézhetjük fel Berger és Luckmann (1998) megfontolásait, akik alapvetően a *fenomenológiai kommunikációs modell* hívei. A szerzőpáros a társadalmi intézményeknek, normáknak, sőt magának a kultúra genealógiájának, meghatározásának ered a nyomába. Intézmények alatt nem csak és nem elsősorban a fizikai fallal körülvett intézményeket értik. Sokkal inkább történetileg tipizált, habitualizált cselekvésekről van szó. Ez azt jelenti, hogy bizonyos cselekvéseket a cselekvők közössége rendez típusokba. Amennyiben ezek történetiségükben, azaz időben fennmaradnak, akkor az intézmény születésének második fázisánál járunk. Habitualizációról pedig akkor beszélhetünk, ha ezek az időben kölcsönösen és együttesen tipizált cselekvések belsővé válnak, belső meghatározottságot jelentenek, amelyhez a közösségek és az egyének a cselekvéseiket igazítják. Ezek a történetileg tipizált, habitualizált cselekvések jelentik a vonatkoztatási keretet, s ebben az értelemben normák.

Szükséges még felhívnunk a figyelmet az értékekre, értékrendszerekre. Kluckhohn és munkatársai ezekre vonatkozóan a következő definíciót adják: „Az érték kívánatos explicit vagy implicit fogalma, amely megkülönböztető az egyénre vagy jellemző a csoportra, és befolyásolja a cselekvés rendelkezésre álló módjainak, eszközeinek és céljainak a kiválasztását" (KLUCKHOHN 1951, 395.). Az érték ezen definíciója egyértelműen a pszichológia, a szociálpszichológia, a szociológia, a társadalomtudományok tárgykörébe tartozik.[11] Egyfelől valami olyasmi, ami *kívánatos,* ami mind az egyén, mind a társadalom számára elérendő, megvalósítandó cél. Rendkívül lényeges, hogy jellemző az egyénre, de a csoportra is. Itt arról van szó, hogy az egyén a szocializáció során megtanulja, elsajátítja azokat az értékeket, értékrendszereket, amelyek a társadalom voltaképpeni kultúráját jelentik. Azaz belsővé válnak a kulturális előírások (bizonyos cselekvések támogatottak, másikak elutasítottak: az európai kultúrkörben például támogatott a *segítségnyújtás,* míg elutasított az étkezés közbeni orrtúrás (lásd: ELIAS 2004).

Az egyén tehát továbbviszi azokat a kulturális mintákat, amelyek áthagyományozódnak az elsődleges és a másodlagos szocializáció intézményein keresztül. Természetesen saját maga is alakíthat rajtuk valamelyest, de a kultúra egészének a szintjén ezek az egyszeri variációk nem érik el a kritikus tömeget. Kisebb csoportméretek esetén hasonló folyamatok zajlanak azzal a különbséggel, hogy a szocializáció (a csoport normáinak elsajátítása)

[10] Éppen erre, a digitális tartalmak tárolására hozta létre Brewster Kahle az internet könyvtárát, amely az interneten megjelent tartalmak tárolására szolgál: www.internetarchive.org.

[11] Az „érték" terminusra más tudományterületek is joggal formálnak igényt. Így például a filozófia, azon belül is az etika („jó" vs. „rossz"). Aztán az esztétika: „szép" vs. „csúnya", illetve „harmonikus" vs. „diszharmonikus". A közgazdaság-tudomány számára ez egy-egy jószág használati, illetve csereértéke. Az „érték" normaként történő értelmezése pedig a jogtudomány számára nélkülözhetetlen (PRAZSÁK 2016).

nem tart olyan sokáig, mint a személyiségfejlődés során. Továbbá a meghatározás lényeges eleme, hogy a norma a csoportra, a közösségre is jellemző. A normák összessége a szabályrendszer, amelynek függvényében a cselekvések zajlanak. Az értékek kifejezetten olyan pszichológiai jellemzők, amelyek összekapcsolják az egyént a közösséggel, a csoporttal. Csepeli (1997, 234.) egészen elementáris erővel ruházza fel az értékeket: „Az érték az egyén és a társadalom közötti szociálpszichológiai közvetítések láncában a legerősebb láncszem." Lényeges, hogy nem elsősorban materiális tárgyakról van szó, hanem sokkal inkább elvont tartalmakról. Váriné Szilágyi Ibolya azonban azt is hangsúlyozza, hogy érték bármi lehet: „bármely tárgy érték, amely meghatározott tartalommal és jelentőséggel rendelkezik valamely társadalmi csoport számára" (Váriné 1987, 119.). A számtalan lényeges elem mellett szükséges kiemelni, hogy az értékek hierarchikusan strukturált rendszerbe szerveződnek: vannak nagyon fontos, s kevéssé fontos értékek.[12] Lényeges jellemző az is, hogy – éppen a kultúra hatása miatt – az értékek viszonylag nehezen változnak, jóval nehezebben, mint a nézetek és az attitűdök. Így aztán mind a kultúra, mind az egyén szempontjából lélektani értelemben stabil vonatkoztatási rendszert jelentenek.

Az értékek empirikus vizsgálata rendkívül nehéz több ok miatt is. Hankiss Elemér ezek közül hármat sorol fel; az egyik a *mimikri*. Arról van szó, hogy az emberek nem minden esetben vannak tisztában azzal, hogy milyen értékeket követnek. A *kamuflázs* azt jelenti, hogy nem feltétlenül akarják megmondani, hogy mi a fontos a számukra, s mi nem: azaz, hogy miként rendeződik értékrendszerük. Végül, de nem utolsósorban a *hipokrízis* azt jelenti, hogy az emberek szeretnek jobb színben feltűnni, mint amilyenek (Hankiss 1977).

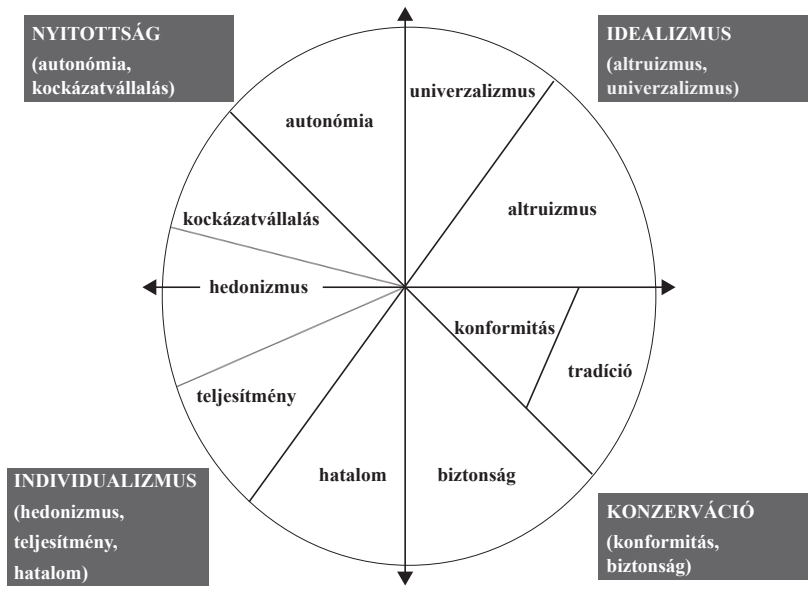
A követett értékek mind társadalmi, mind egyéni szinten integráló funkcióval rendelkeznek (Váriné 1987). Ezért számos kutatás született az értékek e kettős természetének feltérképezésére. Így példaként említhetjük Milton Rokeach (1973) kísérletét, aki eszköz- és célértékeket különített el és vizsgált. Teóriáját és gyakorlati módszereit magyar kutatók is átvették (például Varga 1969; Hankiss 1977). A nyolcvanas évektől Magyarországon is elindult a European Values Study (EVS) és annak alapján a Ronald Inglehart nevével fémjelzett World Values Study (WVS) kutatássorozat, amelynek keretében ma már több évtizednyi távlatban állnak rendelkezésre nagy mintás értékkutatások (Ingelhart 1997, 2003, 2004; Norris–Inglehart 2012).

A következőben kitérünk Schwartz rövidített értéktesztjére, ez képezi a European Social Survey (ESS)[13] alapját. Schwartz az elméletének alkalmazása során azzal az igénnyel lép fel, hogy ötvözze a korábbi értékkutatások leginkább releváns és használható elemeit. Kérdőívébe eredetileg negyvenhét kérdést tartalmazó tesztjéből (1992) huszonegy olyan kérdés került be, amelyek szerinte alkalmasak arra, hogy az általuk megjelenített értéktérben meghatározzuk az egyén és a kultúra egymáshoz viszonyított helyét, valamint összehasonlítsuk a különböző társadalmak, kultúrák értékrendjeit (Schwartz 2003).

Schwartz értéktesztjében különböző személyiségtípusokat sorolnak fel a megkérdezetteknek, akiket arra kérnek, hogy hatfokú skálák segítségével mondják meg, mennyire hasonlít rájuk a leírt személyiség. Az ESS kérdőívbe bekerült huszonegy személyiségleírás az elmélet szerint két nagyobb értéktengely mentén tíz értékosztályba rendeződik.

[12] Az értékekről, értékvizsgálatokról, az értékvizsgálatok alkalmazásáról lásd: Prazsák 2016.

[13] 2000 óta kétévente lefolytatott reprezentatív kutatás Európa népességére vetítve.



2. ábra

Az értékek rendszere Schwartz szerint

Forrás: SCHWARTZ 2003, 270.

Az 2. ábráról leolvasható, hogy a tíz értékosztályból kettő eleve átnyúlik a két nagyobb megkülönböztető tengely által felosztott értéktéren. A *konformitás* és a *tradíció* egyértelműen a *konzervációhoz* áll közel, azonban mindkettő annak külön alosztályát képezi. A két tengely által felosztott négy értéktérszelet közül ez az egyedüli, ahol három értékosztály (illetve alosztály) szerepel. A *konformitás*-értékosztály központi eleme az, hogy a megkérdezett hasonlónak érzi magához az olyan személyt, aki fontosnak tartja, hogy *az embereknek azt kell csinálniuk, amit mások mondanak nekik,* valamint fontos számára, hogy *mindig megfelelően viselkedjen.* A *tradíció* ennél bővebb értékosztály, ugyanis az azt fontosnak tartó megkérdezettek az olyan személyt érzik magukhoz hasonlónak, akinek fontos, hogy *szerény és visszafogott legyen,* továbbá a *hagyományok* és a *vallási,* illetve *családi* szokások is fontosak számára.

A másik különös értékosztályt a *hedonizmus* jelenti. A hedonizmus Schwartz értékelméletében egyaránt tartozik a *nyitottsághoz* és az *individualizmushoz.* A *hedonizmus*-értékosztályban magas értékkel szerepel az a megkérdezett, aki fontosnak tartja, hogy *jól érezze magát,* aki *szereti kényeztetni magát,* akinek fontos, hogy *olyan dolgokat csináljon, amelyek örömöt okoznak neki.* Ennek következtében a hedonista ember ugyan nyitott a változásokra (az éppen aktuális igényeinek megfelelően), de az általános (már-már filozófiai) nyitottsághoz képest sokkal inkább jellemző rá az a materiális beállítottság, amely az *individualizmushoz* közel álló értéktérszelethez tartozó értékeket, a *teljesítményt* és a *hatalmat* fontosnak tartó személyekre jellemző.

A *teljesítmény*-értékosztály azokra az emberekre jellemző leginkább, akiknek fontos, hogy *sikeresek* legyenek, akik szeretnék, hogy *az emberek elismerjék a teljesítményüket,* továbbá alapvetőnek tartják, hogy *megmutassák képességeiket.* Az *individualizmus* értéktengelyéhez közel található értéktérszelethez tartozó harmadik értékosztály a *hatalom.* Az az ember, akiknek az értékrendszerében a hatalom lényeges szerepet tölt be, fontosnak tartja, hogy *gazdag legyen,* valamint azt is akarja, hogy *az emberek azt csinálják, amit ő mond.* Az ilyen ember éppen az ellentéte annak, akinek a materiális értékek kevésbé, míg a posztmateriális értékek sokkal inkább fontosak: ők az *idealisták.*

Az *idealizmus*-értéktérszelet közelében két értékosztály található: az *altruizmus* és az *univerzalizmus.* Előbbi értékosztály annak az embernek az életében van jelen meghatározó elemként, aki egyrészt igen fontosnak tartja a *becsületességet,* másrészt *törődik mások jólétével,* és *életét a hozzá közel álló embereknek akarja szentelni.* Voltaképpen az *altruizmus*-értékosztály általánosítása jelenti az *univerzalizmus*-értékosztályba tartozó értékeket. Az idesorolt értékek azoknak az embereknek fontosak, akik úgy vélik, hogy *mindenkinek egyenlő lehetőséggel kellene rendelkeznie az életben,* s akik fontosnak tartják, hogy még *akkor is megértsék az embereket, ha nem értenek egyet velük.* Az *univerzalizmus*-értékosztály azonban nem csak ezeket az egalitárius értékeket öleli fel. Tartalmazza a környezet védelmét, megóvását is, s ezáltal az egalitárius dimenzió kiegészül a *felelősséggel.* Azok az emberek ugyanis, akik az *univerzalizmus*-értékosztály súlyát fontosnak ítélik meg a saját értékrendszerükben, fontosnak tartják azt is, hogy *vigyázzanak a környezetükre.*

Az *univerzalizmus*-értékosztály mellett, a tengely másik oldalán található az *autonómia*-értékosztály. Ez az olyan ember életében tölt be különösen nagy szerepet, akinek fontos, hogy *új dolgokat találjon ki,* hogy *kreatív legyen,* aki *szereti a dolgokat a saját egyéni módján intézni.* Az *autonóm* ember az újdonságokra való nyitottságon túl *szabad* ember is, akinek fontos, hogy *saját maga döntsön arról, hogy mit csinál.* Az *autonómia*-körszelet másik oldalán a *kockázatvállalás*-értékosztály található. A kockázatvállaló emberhez az *autonómia* és az *individualizmus* egyaránt közel áll, hiszen az *autonóm* egyén a *heteronóm* egyénhez képest kockázatvállalóbb. Azok, akik *szeretik a meglepetéseket, szeretnek új dolgokat csinálni, keresik a kalandokat,* és összességében *izgalmas életet akarnak élni,* ők nemcsak *nyitottak* az újdonságokra, hanem egyszersmind *kockázatvállalók* is. Ez a nyitottság éppen az ellenkezője annak, ami a 2. ábrán bemutatott *konformitás-, tradíció-* és *biztonság-értékosztályokkal*, azaz a *konzervációval* írható le. A *biztonság-értékosztályba* két érték tartozik, amelyek közül az egyik az egyén, míg a másik a közösség szempontjából fogalmaz meg hasonló magatartást, elvárást. A biztonság értékeinek komoly jelentősége van annak az embernek az életében, aki *elkerül mindent, ami veszélyezteti biztonságát,* valamint annak, aki elvárja, hogy *a kormány biztosítsa biztonságát mindenfajta fenyegetéssel szemben,* és azt akarja, hogy *az állam erős legyen, hogy meg tudja védeni polgárait.*

Schwartz úgy véli, hogy a felsorolt értékek jól leírják az emberek értékrendszerét, s ezeknek a különböző léptékű aggregálásával az egyes országok társadalmai, továbbá a különböző kultúrák értékrendszerei is leírhatók és összehasonlíthatók (Mohler–Wohn 2005).

Annak érdekében, hogy meg tudjuk ragadni mind az egyén, mind a kultúra által preferált értékrendszert, Schwartz a következő eljárást javasolja a kérdőívet kitöltő egyének válaszainak aggregálására. Az első lépésben minden megkérdezett esetében ki kell számítani a huszonegy személyiségleírással kapcsolatban adott válaszok átlagpontszámát. Ez voltaképpen az egyén *értékgazdagságát* jelenti: minél magasabb ez a szám, annál inkább

fontosnak tartja az egyén a felsorolt értékeket. Ezt követően ki kell számítani az egyes értékosztályokat megjelenítő személyiségleírások átlagait. Miután megvan a két átlag, azok különbsége alapján – állítja Schwartz (2003) – minden megkérdezett esetében megállapítható, hogy az adott értékosztály mennyire tér el az egyénre jellemző értékgazdagságtól. Így például, ha valaki az *autonómia* értékosztályába tartozó értékeket összességében nagyon fontosnak tartja[14] (például az ehhez tartozó mindkét változó esetében 6 ponttal, míg az összes értéket összességében átlagosan csak 2 ponttal minősítette, vagyis 6–2=4 pontszámmal rendelkezik az *autonómia*-értékosztályban), akkor azoknak az értékklaszterébe fog tartozni, akiknek a saját értékhierarchiáján belül más értékeknél fontosabb az *autonómia*. Ezzel a módszerrel minden értékosztály súlya megállapítható, s így leírható az egyén értékhierarchiája, az egyéni értékpreferenciák aggregálásával pedig azonosíthatók a különböző társadalmak és kultúrák által preferált értékrendszerek.

Csepeli György és Prazsák Gergő (2010) e teszt használatával végzett kutatásának kifejezetten az volt a célja, hogy az ESS-felmérés adatai alapján megállapítsák, hogyan függ össze az internethasználat az értékrendszerekkel. Az értékrendszerek kiváló összefüggést mutattak Európa három történeti régiójával (Szűcs 1983). Ezért, amennyiben az internethasználat és az értékrend között összefüggés jelentkezik, az nemcsak az egyén, hanem a kultúra egészének a következményeként interpretálható. A kutatásba bevont mintegy harmincezer ember esetében a 2010-es adatfelvételen a következő eredmények voltak megfigyelhetők (a részletes, statisztikai eredmények helyett inkább az eredmények közlésére koncentrálunk).

1. táblázat

Értékek és napi rendszerességű internethasználat

	Nem vagy ritkán internetezők	**Gyakori internethasználók**
Konformizmus	+	–
Tradíció	+	–
Biztonság	+	–
Autonómia	–	+
Kockázatvállalás	–	+
Hedonizmus	–	+
Teljesítmény	–	+
Hatalom	nincs különbség	
Univerzalizmus	–	+
Altruizmus	–	+

Forrás: Csepeli–Prazsák 2010 alapján a szerző szerkesztése

Annak ellenére, hogy az adatok már néhány évesek, jól bemutatják azokat a személyiségjellemzőket, amelyek meghatározzák az új kommunikációs technológiák használatát. Ahogy majd a későbbiekben látni fogjuk, az innovációk terjedésének különböző adaptálói kiváló egyezést mutatnak ezekkel az eredményekkel. A táblázatra tekintve jól látható, hogy

[14] Vagyis a kérdőívben leírt autonóm személyiségtípusokat önmagához nagyon hasonlónak tartja.

a konzervatív értékrend követői ritkábban használják az internetet. Azok, akik konformak, ragaszkodnak a tradíciókhoz és a biztonsághoz, nagyobb valószínűséggel maradnak távol az online világtól. Ők egyértelműen a lemaradók. Ezzel szemben azok, akik nem konformak, a tradíciókhoz nem ragaszkodnak, a biztonság sem fontos a számukra, azaz kockázatvállalók, nagy kanállal eszik az életet (hedonisták), teljesítményorientáltak, de úgy, hogy közben felelősséget éreznek környezetükért, fontosak nekik társas kapcsolataik, a barátaik, szóval ők a gyakori internethasználók. Amennyiben a különböző értékrendek és Európa történeti régiói közötti kapcsolatot nézzük, akkor egyértelmű összefüggést találunk. Nyugat-Európában a társadalom nagyobb része mer kockázatokat vállalni, egyszerűen nyitottabb a világra, mint a Kelet-Európa országaiban élők. Ebben nyilván szerepe van az eltérő gazdasági fejlettségnek is, de az meg nem lehet független azoktól a történelmi struktúráktól, amelyeknek jellemzőit Szűcs Jenő kitűnően összefoglalja (1983).[15] Összességében azt lehet megállapítani, hogy minden összefügg mindennel. A kulturális meghatározottságok olyan determinációt jelentenek, amelyek mind az egyén, mind az ország szintjén meghatározzák az innovációk terjedését, használatát. Ezen túl pedig azt is látnunk kell, hogy a személyiség olyan prediszpozíciót jelent, amely döntő mértékben meghatározza az online világba való bekapcsolódást, s annak intenzitását. Mindez nyilvánvalóan olyan alapmeghatározottságot jelent, amely az online világba való bekapcsolódást határozza meg. Ezek a lélektani mintázatok minden bizonnyal meghatározzák az online világban való közlekedést is, azonban erre vonatkozóan jelenleg még nem tudunk empirikus kutatási eredményekkel szolgálni.

1.2.4. A kommunikációs architektúrák metamorfózisa

Az emberi társadalmak összetettségével együtt egyre bonyolultabbá, komplexebbé vált a kommunikációs eszköz is. A kommunikációs szabványok megváltoztatták a társas/társadalmi együttélés formáit. Új alakzatok, új berendezkedések, új irányítások, új politikai-gazdasági-társadalmi-művészeti termékek jelentek meg az architektúraváltások során. Dunbar elmélete és empirikus vizsgálatai (1998, 2006) esetén jól láthattuk, hogy a nyelv megjelenése szorosan összefüggött a társas helyzetek komplexitásával. Ez kiszabadította az egyént az „itt és most" fogságából, s fokozta az időbeliség átélését, hiszen egy eszközzel lehetővé tette a múlt felidézését és a jövőre irányultságot, az eljövendő eseményekről szóló képzeteket. A nyelv és az idő, illetve a kommunikációs architektúrák és az idő kapcsolatának vizsgálata ugyancsak termékeny vállalkozás (Nyíri 2007). Nem csak a kommunikációs architektúrák és az idő kapcsolatának vizsgálata miatt érdemes átgondolni Nyíri (2007, 34.) javaslatát a kommunikációs architektúrák klasszifikációjáról. Azzal együtt, hogy az idő és a tér két olyan determináns, amely rendkívül erőteljesen meghatározza a társadalmi együttélést és a gondolkodást, Nyíri – akárcsak Csepeli és Prazsák (2010) – a *mimetikus* kommunikációra, a taglejtésekkel való kommunikációra is figyelmet fordít. Helyesen emeli ki az egyik legfontosabb kommunikációs jellemző, a reprezentáció és az utánzás képességének a megjelenését.

[15] Ilyen jellemző nyugaton az autonómia, a vállalkozás szabadsága, a szekuralizáció, a polgárság korai megjelenése, keleten a paternalizmus, a hatalomnak való alávetettség és a konformitás.

Csepeli és Prazsák a mimetikus kommunikációs architektúra univerzális kommunikációs eszközként való értelmezési lehetőségére hívja fel a figyelmet. A következő architektúra az *elsődleges szóbeliség* szabványa, amelyben a szavak használatáról, illetve a szavakból készült szövegek állandó ismételgetéséről volt szó. A kimondott szó pontosabb kommunikációra ad alkalmat, tekintettel arra, hogy a taglejtések nyelvének sztenderdizálása nehezebb és esetlegesebb. Az elsődleges szóbeliség ideje ciklikus: ezt sugallja a nap járása, az évszakok. A kommunikáció evolúciójának következő fázisa Nyíri szerint a *kép,* amelynek megjelenését a barlangfestmények idejére teszi (noha vizuális szimbólumok már korábban megjelentek). A képi kommunikáció karrierje a barlangfestményektől napjainkig tart.

A barlangfestményeket követően jelentek meg az első *képírásjelek,* az ideogramok, amelyek már egészen *pontosan* és sokáig rögzíthető információhordozók voltak, és az információ szállítására is alkalmat adtak. Ahogy arra korábban már utaltunk, napjainkban az emojik kifejezett előretörése figyelhető meg. A *szótagírás* és az *alfabetikus írás* megjelenésével az információk tárolása és rekapitulálása a korábbi technológiákhoz képest soha nem látott pontosságot ért el annak ellenére, hogy a szövegek másolása során előfordultak tévedések, amelyek megváltoztathatták az eredeti szöveg jelentését. Ezért is volt rendkívüli kommunikációs innováció a *nyomtatás* megjelenése. No meg azért is, mert azzal együtt elindult a tudás demokratizálódása: technikai értelemben már nem jelentett megoldhatatlan problémát az információk széles körű terjesztése. Természetesen a reprezentatív nyilvánosság utolsó leheletéig próbálta kontrollálni a tudás hozzáférését, és a széles körű analfabetizmus sem támogatta a tudás társadalmon belüli teljes szétterítődését. A nyomtatással együtt megjelent a tömegkommunikáció is. Ahogy Habermas a *Strukturwandel der Öffentlichkeit* (magyarul: *Társadalmi nyilvánosság szerkezetváltozása* című munkájában) (1971) bemutatja, a nyomtatás serkentőleg hatott a polgári nyilvánosság létrejöttére, hiszen a többé-kevésbé rendszeres hírlevelek ösztönözték a közügyekért felelősséget vállaló, nyilvánosan vitatkozó polgárság megjelenését.

A következő kommunikációs architektúra, a *másodlagos szóbeliség* megerősítette a tömegkommunikációs logikát, miközben megjelent az első igazán interaktív kommunikációs eszköz is: a telefon. Ezzel együtt a rádió, a televízió, a mozgókép mind-mind olyan kommunikációtechnológiai fejlesztések voltak, amelyek már a hely és az idő érzékelését is átalakították. A másodlagos szóbeliség körülményei között – hívja fel Nyíri a figyelmet (2007, 37.) – a távíró megjelenésével és az első transzatlanti kábel lefektetésével (1866) lehetővé vált a nagy távolságokban lévő órák szinkronizálása. A telefon megjelenése pedig az információ egyre nagyobb mennyiségének a szállítását tette lehetővé. A következő kommunikációs architektúra a *számítógép közvetítette kommunikáció,* amely lehetővé teszi, hogy a felhasználók hálózatos szerveződéssel nagy mennyiségű képi és hanganyagot osszanak meg egymással. Az egymásra következő kommunikációs architektúrákat a következő táblázatban összefoglalva is bemutatjuk.

2. táblázat
A kommunikációs technológiák korszakai Nyíri (2007) szerint

Kommunikációs korszak	Kommunikációs eszköz
mimetikus kommunikáció	események utánzása, „pantomim”
elsődleges szóbeliség	beszélt nyelv, szavak, szövegek
képi kommunikáció	kép, rajzok, festmények
képírás	ideogramok
szótagírás, alfabetikus írás	betűk
nyomtatás	hírlevelek, újság, könyv
másodlagos szóbeliség	személyközi kommunikáció: távíró, telefon; tömegkommunikáció: mozi, televízió, rádió
számítógép közvetítette kommunikáció	internet, mms, sms stb.

Forrás: Nyíri 2007, 34.

A különböző kommunikációs architektúrák jellemzője, hogy mindegyik egyre több információt képes szállítani, megosztani, továbbítani. Az információk mennyiségén túl további közös jellemző, hogy egyre pontosabb az információk rögzítése, kódolása, egyre kisebb a kommunikációs architektúra modális csatornájának a zaja. Lényeges kiemelni, hogy az elsődleges szóbeliségre következő kommunikációs architektúrák az egyközpontú közlésnek kedveztek. A másodlagos szóbeliség ugyanakkor elhozta az interaktivitás, a hálózati szerveződés lehetőségét.

A különböző kommunikációs technológiák egyre rövidebb idő alatt, egyre gyorsabban terjedtek el. Minden esetben olyan innovációról volt szó, amely a terjedés csatornáját érintette. Az innováció önmagában a kommunikáció egy rendkívül lényeges jellemzője. Ezért is szükséges, hogy a következőkben részletesen áttekintsük az innovációk terjedésének a folyamatát. Ennek során megannyi olyan társas, társadalmi megfontolást tehetünk, amely a 21. századi ember mindennapjainak talán legfontosabb, s gyakran csak automatizmusokként átélt cselekedeteire vonatkozik.

A kommunikációs architektúrák változásának áttekintése az emberiség történetének talán az egyik legnagyobb ívű elemzését teszi lehetővé. Önmagában hordozza azokat a megfontolásokat, amelyeket az információs korra vonatkozóan az előző alfejezetekben tettünk. Ezek közül összefoglalóan is érdemes kiemelni néhány kulcselemet, amelyek a következő oldalakon is szükségszerűen elő-előbukkannak.

1.2.4.1. Határtalanság és gyorsaság

Az egyik jellemző a *határtalanság.* Az internet, a modern elektronikus kommunikációs eszközök megjelenésével egyre kevésbé beszélhetünk földrajzi értelemben vett határokról. Az internetre csatlakozott gép előtt ülve (vagy azt kézben tartva stb.) teljesen lényegtelen, hogy a földrajzilag értelmezett tér mely pontján vagyunk. Ahogy láthattuk, technikai értelemben mindegy, azonban mégis vannak országok, ahol a hatalom nem enged teljes hozzáférést az internet egészéhez (a politikai diktatúra fenntartása miatt bizonyos oldalak használatát korlátozzák, például a Facebookot). Az információs korban az internet adta

határtalanság nemcsak földrajzi, fizikai, de szellemi, lélektani értelemben is biztosított. Az internet mint a tudás tárolásának és megosztásának az eszköze voltaképpen korlátok nélkül teszi lehetővé, hogy bárki, bárhol hozzáférjen azokhoz az ismeretekhez, amelyeket addig felhalmozott az emberiség. Egy olyan szellemi közösségnek lehetünk a tagjai, amelyben Platónnal, Arisztotelésszel vagy Nietzschével gondolkodhatunk együtt, vitatkozhatunk, esetleg feleselhetünk. Mindezt úgy, hogy közben egy videómegosztón hallgathatjuk, ahogy Mozart-szimfóniát dirigál Fischer Ádám *(multitasking).* Ha kedvünk tartja, a szimfónia végén nemcsak, hogy megnézhetjük pénzügyi befektetéseinket, de át is helyezhetjük azokat (vagy megnézhetjük, hogy mennyi villanyszámlával vagyunk elmaradva, esetleg be is fizethetjük azokat). A digitalizált és interneten megtalálható térképek, videók jóvoltából távoli tájakon nézhetünk körül, olyan helyeken is, ahova a valóságban talán sosem jutunk el. A szellemi határtalanság az én szabadságérzetének a felszabadulásával is együtt jár. A mélylélektan felől tekintve a viszonylag kontrollmentes, szabad környezet lehetővé teszi a kultúra által elfojtott cselekedetek megjelenését, szublimációját, ami a kultúra kontrollmechanizmusai hiányában előhívhatja a deviancia számos formáját. Az én szabadságérzetének fokozódása nemcsak proszociális, hanem antiszociális magatartásoknak is táptalaja lehet (például *cyberbullying*). A hálózatba való ki-be kapcsolódás, az online csoportokban való részvétel, illetve a csoportokból való ki- és azokba belépés lehetősége mind-mind olyan szabadságérzetfokozó tényezők, amelyek következtében bátrabb, esetenként vakmerőbb a felhasználó.

A kommunikációs architektúrák történetének előrehaladtával az egyes korszakok egyre *gyorsabban* követték egymást, egyre kevesebb időre volt szükség elterjedésükhöz. Ahogy egyre gyorsabbá váltak a kiforrott kommunikációs architektúrák megszilárdulásai, úgy egyre pontosabbakká és demokratikusabbá is váltak. Az egyiptomi hieroglifák mintegy hatezer évvel ezelőtt jelentek meg, és mintegy négyezer éven át jelentették a viszonylag pontosan újra felidézhető információk rögzített eszközét. Azonban csak egy rendkívül szűk, olvasni tudó rétegnek és többnyire egy – a mai viszonyok között szűk – földrajzi területen. A 15. században a nyomtatás megjelenésével lehetővé vált, hogy a pontosan rögzített információ messzi tájakra is eljusson, és az írástudás egyre szélesebb elterjedésével lehetőség nyílt arra is, hogy ne csak egy szűk réteg sajátja legyen az információkhoz való hozzáférés. Napjaink kommunikációs korszakának egyik lényeges eleme pedig éppen az, hogy határok nélkül juthatnak el információk az interneten.

1.2.4.2. A diffúzió és következményei

Az innovációk terjedése során a közvetítőnek kitüntetett szerepe van, ezért érdemes néhány gondolat erejéig megállni a kommunikációs csatornák, egyáltalán az innovációk terjedésénél. A terjedési folyamatnak általánosan értelmezhető állomásai, összetevői is vannak. Ezeket a jellemzőket és az abból adódó megfontolásokat célszerű Everett Rogers *Diffusion of Innovation* című (2003), ma már a tudományterület klasszikusának számító munkája nyomán áttekinteni.[16]

[16] Az elektronikus, valamint a papíralapú változat kiadója (Free Press) és a kiadás helye (New York) megegyezik, azonban az oldalszámok az elektronikus formátum (epub) sajátosságai miatt eltérnek. A következőkben a citációk során az elektronikus kiadás oldalszámait tüntetjük fel.

„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 részt vevő 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 – ami ugye elviekben csökkenti a bizonytalanságot –, mégis éppen a *bizonytalanság* az információs korszak rendkívül fontos jellemzője. Az interneten való közlekedésnek – összehasonlítva a fizikai világban való mozgással – egyik legfontosabb ismérve ez, ami 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. Ezért is van, hogy napjaink társadalmi berendezkedésének leírására gyakran, s joggal használják 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, s az lesz a jövőben is (Hankiss 2011). A bizonytalanság elkerülésének elősegítése (ahogy például az eBay esetében láthattuk) kifejezetten piaci erővel bír. Ezzel együtt nyilvánvalóan lehetetlen az interneten való közlekedés minden mozzanatát tökéletesen biztonságossá tenni, mint ahogy az utcán sem vagyunk százszázalékos biztonságban. Ezért aztán vannak, akik kockázatvállaló életet élnek, de olyanok is, akik nem autonómak, nem tanították meg nekik az interneten való közlekedés írott és íratlan szabályait, ezért kiszolgáltatott helyzetben vannak. Ahogy az értékek és az internethasználat összefüggéseit bemutató 1. táblázatban láthattuk, a kockázatvállaló attitűd rendkívül fontos az interneten való közlekedés során, míg a biztonságra való szélsőséges törekvés nem segíti elő azt. Az autonómia és a konformizmus ugyancsak aláhúzza ezt a jelenséget. Tehát arról van szó, hogy az *autonóm, kockázatvállaló* magatartás, ha *informatikai ismeretekkel* párosul, kifejezetten elősegíti azt, hogy a felhasználó ne (vagy minél kevésbé) kerüljön kiszolgáltatott helyzetbe az interneten. Mindennek a fordítottja is igaz, a biztonságra törekvő, konform, heteronóm, kívülről irányított felhasználó, aki nem rendelkezik megfelelő informatikai ismeretekkel, rendkívül kiszolgáltatott helyzetben van. A biztonság hiányát tehát nemcsak az újdonság(ok) okozta bizonytalanság fokozza, hanem a virtuális környezet megfoghatatlansága, kiszámíthatatlansága is. *A bizonytalanságtűrés, a kockázatvállalás, a belülről irányítottság, az autonómia olyan diszpozíciók, amelyek lélektani értelemben védelmet, biztonságot szolgáltatnak.* Összességében viszont kevesebben vannak azok, akik rendelkeznek ezekkel, mint akik nem. A skála másik végén – többen – vannak azok, akik kerülik a bizonytalanságokat, kerülik a kockázatokat, és inkább

heteronóm felhasználók. Az egyén szintjén a két véglet közötti feszültség a cyberdeviancia megjelenésének melegágya.

1.2.4.3. Az innováció

Az egyén szintjéről nézve a bizonytalanság ellenére megtörténik az innováció alkalmazása, amennyiben az több előnnyel, mint haszonnal jár – így motiváció ébred az egyénben az innováció alkalmazásával kapcsolatban, ami pedig – az innovátorok kis számú csoportján kívül – az utánzás mechanizmusa szerint történik. „A külső minta létét jelző információ eredményeként az utánzó felfigyel a mintára, melyet vonzónak ítél. Az ítélet következményeként következik be az utánzás első szakasza, a próbálkozás. Ha a próbálkozás inkább sikeres, semmint hiábavaló, akkor jön a gyakorlás. Az utánzás utolsó szakasza, amikor az eredetileg külső minta teljesen interiorizálódik, s rutinműveletté válik" (CSEPELI–PRAZSÁK 2013). Az innováció alkalmazása szempontjából az is lényeges, hogy mekkora a társas környezet nyomásgyakorlása. Ennek több típusát is meg kell különböztetnünk. Demokratikus rendszerekben a „nyomásgyakorlás" abból adódik, hogy a közvetlen környezet, illetve a társadalmi rendszer tagjai hasznosnak ítélik az adott innovációt, és ezért alkalmazzák is. Tekintélyuralmi rendszerekben viszont központi parancsra kell az adott innovációt használni az egyénnek és egyéb szervezeteknek.

1.2.4.4. A terjedés

Rendkívül lényeges az a csatorna, amelyen keresztül az adott innováció terjed. A kommunikációs architektúrák történeti áttekintése esetében látott architektúra-váltások (2. táblázat) összességében egy immanens folyamatot mutatnak be, amelyben egy-egy kommunikációs technika elterjedése – az emberiség körében – elsősorban nem parancsuralmi, hanem funkcionális alapon történt. Ez természetesen nem jelenti azt, hogy egy-egy új technológia bevezetése egy-egy közösségben ne lehetett volna központilag vezérelt és meghatározott. Sőt! Éppen a konzervatív, hagyományokhoz és biztonsághoz ragaszkodó értékrend széles körű jelenléte miatt kifejezetten szükséges is az új technológiáról való központosított kommunikáció. Összességében azonban megfigyelhető, hogy az új és újabb kommunikációs technológiák – azon túl, hogy egyre pontosabb információszállítást tesznek lehetővé – egyre több embert érhetnek el, és egyre több ember interaktív kommunikációját biztosíthatják. Amíg például az írás és a nyomtatás megjelenése, de az elsődleges elektronikus kommunikáció is (TV, rádió) alapvetően a tartalomszórást biztosította, addig az internet technológiája kifejezetten az interaktivitásra épül. Az internet éppen ezért rendkívül „veszélyes" az autoriter rendszerekre nézve – ezért is akarják korlátozni. Ahogy láthattuk Dunbar tanulmányában (1998), kognitív határai vannak annak, hogy mennyi emberrel vagyunk képesek kapcsolatban lenni – még akkor is, ha a technika beláthatatlan mennyiségű kapcsolatra is lehetőséget adna. Ezért is lényeges, hogy a különböző kommunikációs technológiák milyen társas, hálózati modellre épülnek, s hogy ezek hogyan függnek össze a társadalmi berendezkedéssel. Érdemes megidézni Z. Karvalics László (2004) összefoglaló táblázatát (3. táblázat).

1.2.4.5. A társadalomtörténeti korszakok

3. táblázat
Társadalom, világkép, közösségméret

Társadalomtípus	Világkép	Közösségi képlet (tagok száma tól–ig)
halász-vadász-gyűjtögető	statikus	horda (25–50), nagycsaládok (50–150)
agrár	dinamikus	falusi közösség (150–8000), városi/város-szövetségi (4000–4 millió)
ipari	energiacentrikus	nemzeti (60 millióig), nemzeti/regionális (8 millió–2 milliárd)
posztindusztriális	információcentrikus	nemzeti/multiregionális (800 millió–4 milliárd), globális (?)

Forrás: Z. Karvalics 2004, 11.

A fenti táblázat egymásra következő társadalomtörténeti korszakokat sorol fel. Azonban ezek nem egyik pillanatról a másikra váltották egymást, hanem hosszú átmenetek voltak. Ráadásul területi értelemben leghamarabb mindig a centrumhoz tartozó területeken következett be a változás – hangsúlyozza Z. Karvalics.

A négy nagy társadalomtörténeti korszak különböző kommunikációs architektúrákra épült. A 2. és 3. táblázatok összehasonlításából egyértelműen látható, hogy a *halász-vadász-gyűjtögető* társadalomtörténeti korszak kommunikációs architektúrája elsősorban a *mimetikus kommunikáció* és az *elsődleges szóbeliség.* Ez a kommunikációs technológia és együttélési forma lehetővé tette, hogy a közösség tagjai közvetlen kapcsolatban legyenek egymással. Egy teljes hálózatról van szó. Ez az a közösségméret, amelyben a tagok tisztában vannak azzal, hogy milyen igényei vannak a másiknak, mit szeretne, s mit nem. A nyilvánosság eseti, mindent együtt csinálnak, az individuum a mai modern értelemben nem létezik.

A következő társadalomtörténeti korszakok voltaképpen a társadalmi együttélési forma korszakai, amelyekben kisebb-nagyobb mértékben jelen van az egyén. Az *agrártársadalmak* a feudalizmus sajátjai, ahol van olyan uralkodó, akinek a társadalom egésze közvetlenül vagy közvetve lekötelezett. Ezekben a társadalmakban a hatalom birtokosa az uralkodó (réteg tagjai), aki(k) a korszak kommunikációs technológiáit (írás, nyomtatás) a reprezentatív nyilvánosság megteremtésére és fenntartására használják. A reprezentatív nyilvánosságban *nincs interakció,* az uralkodó közöl, kinyilatkoztat, azaz egyirányú kommunikációról van szó. A társadalomtörténeti korszak végén jelenik meg az újság, ami feltételezi, hogy már nem csak a kiváltságosok előjoga az írás-olvasás, a közügyek intézése. Ez az ipari társadalmak sajátja.

Megjelenik a hír, amelynek aktualitása van, s viszonylag sok ember érdeklődésére tart(hat) számot. Ez jelenti voltaképpen a tömegkommunikáció klasszikus korszakának az előestéjét. Hálózatelméletileg *csillaghálóról* van szó, azaz van egy központi eleme, amelyen keresztül az összes többi elem kommunikálni tud egymással. A televízió és a rádió esetében ez történik: interakcióra nincs mód. Ez a kommunikációs technológia – kifejlett

mivoltában – a propaganda megvalósításának terepe. A középkori reprezentatív nyilvánosságnál korszerűbb, több embert elérő, nagyobb hatású eszköz a 20. századi diktátorok kedvelt kommunikációs csatornája: a mozgókép, a rádió, a televízió. A kommunikációs technológia demokratikus körülmények között is jól működik, ekkor propaganda helyett kultivációról beszélhetünk. Ez esetben a tömegkommunikációs eszközök ugyan különböző formában, de nagyon hasonló tartalmat, világképet, ideológiát sugároznak, fenntartva annak illúzióját, hogy a befogadó választhat a különböző termékek közül. Ennek a társadalomtörténeti korszaknak tehát a másodlagos szóbeliség csatornái jelentik a kommunikációs technológiákat. Ezek azonban a személyközi kommunikáció területén is roppant változást hoztak, hiszen megjelent például a vezetékes telefon, egy teljes interaktivitást lehetővé tevő kommunikációs eszköz. A televízió és a rádió jelenléte kifejlett korszakában már nem igényelte a telefont a hírek közléséhez (telefonhírmondó). A telefon a magánjellegű kommunikáció területe maradt. A korszakot alapvetően a tömegkommunikáció uralta: egy közlő, sok befogadó, interakció nélkül. Ez a nemzetállamok kora, amelynek energiacentrikus világképe eleinte a fosszilis, később az atomenergia köré központosult. A korszak vége felé pedig megjelentek a megújuló energiaforrások, amelyek egyre nagyobb mértékben kezdték felváltani az előbbi két energiaforrást. A *posztindusztriális társadalom* információcentrikus világképe az információk előállítása, gyűjtése, feldolgozása, felhasználása köré, elsősorban a szolgáltatószektorra épül.

1.2.4.6. A skálafüggetlenség demokráciája

A posztindusztriális társadalom megjelenése roppant változást idézett elő. Egyik teoretikusa, Daniel Bell a következőképpen fogalmaz: „javakat termelő társadalom átváltozása információs vagy tudástársadalommá" (BELL 1976, 487.). Az internet és a hálózati társadalom megjelenése (CASTELLS 2005), valamint a Szovjetunió felbomlása (CASTELLS 2007) teljesen új korszakot hozott az emberiség történetében. Az internet megjelenése önmagában a demokrácia, a szabadság korábban nem látott formáját hozta el. Mindez kiegészült a szovjet birodalom felbomlásával. Az internet kommunikációs architektúrája a skálafüggetlen hálózatokra épül. Ezekben nem véletlenszerűen, hanem preferenciális elvek mentén kapcsolódnak egymáshoz a hálózat tagjai. A preferenciát az jelenti, hogy kihez/mihez éri meg jobban kapcsolódni. Ezért aztán lesznek a hálózatnak olyan tagjai (viszonylag kevesen), amelyek több, és olyanok is, amelyek kevesebb kapcsolattal rendelkeznek (viszonylag sokan). A hálózat architektúrája lehetővé teszi, hogy a sok kapcsolattal rendelkező pontokon keresztül a hálózat véletlenszerűen kiválasztott pontjai viszonylag könnyedén kapcsolatba kerüljenek egymással. Ez a demokrácia hálózata. Például, ha valaki szeretné saját honlapjának nézettségét gyorsan megemelni, akkor célszerű olyan oldalakon reklámoznia, amelyeknek magas a látogatottsága (például CNN, BBC stb.). A társas hálózatok esetében is hasonló a helyzet. A kapcsolatgazdagok – kontaktokraták – rendelkeznek a társas kapcsolatok (email és mobil) 20 százalékával, és rajtuk keresztül megy valamennyi hívás 30 százaléka is (CSEPELI–PRAZSÁK 2010). A kontaktokraták és a kontaktproletárok kifejezetten a skálafüggetlen hálózati struktúra alapján elkülönülő társadalmi csoportok az információs korban. Akárcsak az autonómia-konformizmus, kockázatvállalás-biztonság dimenziói,

a kontaktproletárok és a kontaktokraták közötti feszültség is a cyberdeviancia potenciális megjelenését vetíti előre.

A különböző hálózatok nem statikusak, hanem folyamatosan változnak, alakulnak. Az egyik hálózati struktúrából a másikba való átmenetet Csermely Péter (2004, 66.) *hálóváltásnak* nevezi.

Az internet hálózata szükségszerűen skálafüggetlen jellemzőkkel írható le (Barabási 2013). A teljes gráf esetében rendkívüli terménybőség adott; ez volt jellemző az ősközösségi társadalmakban (Csermely 2004, 201.). Annak következtében, hogy a népesség száma növekedésnek indult, szűkösek lettek a rendelkezésre álló erőforrások. Ennek következtében esetenként csillagháló (diktatúra), más esetekben skálafüggetlen (demokrácia) fázis alakult ki. Az internet szükségszerűen skálafüggetlen hálózat, hiszen – ahogy korábban utaltunk már rá – az emberiség számára rendelkezésre álló erőforrások egyre szűkösebbek. Másfelől széles körben kapcsolatba léphetnek egymással a felhasználók (többnyire tartalmakat is így nézhetnek/készíthetnek), ugyanakkor vannak kitüntetett pontok az interneten, amelyek több kapcsolattal rendelkeznek.[17] Amennyiben tehát hálózati értelemben eltérés tapasztalható a skálafüggetlen hálózati struktúrától, akkor a hálózat szerkezetét tekintve *devianciáról* van szó.

[17] Lényeges kiemelni, hogy ezek a pontok nem tudják kitüntetett pozíciójukat áthagyományozni, mint ahogy a feudalizmusban a királyi család tagjai. Ezért is írnak plurarchiáról a *Netocracy* című könyv szerzői, akik szerint a netokrácia az új hatalmi elit (Bard–Söderqvist 2002, 72.). Véleményük szerint a plurarchiáról jelentése, hogy minden résztvevő saját maga dönt saját maga sorsáról.

Vákát oldal

2. Deviancia az online térben

A deviancia a legelterjedtebb fogalmi meghatározása szerint *egy adott közösségben uralkodó, és a közösség többsége által egységesen elfogadott normáktól való eltérést, elhajlást jelent*. A *deviáns* jelző sokféle magatartásformára utal: lehet funkcionális és diszfunkcionális, univerzális értékeket sértő, alkalmi vagy többször megismétlődő, egyéni jellemből kiinduló vagy informális és formális reakciókat kiváltó (Andorka–Buda–Cseh-Szombathy 1974; Rosta 2007). A deviánsnak minősített egyén vagy közösség magatartásának veszélyességi fokát leginkább az fejezi ki, hogy a megsértett szabályokhoz milyen közösségi attitűdök kötődnek, vagyis a társadalom tagjai számára mennyire fontos és meghatározó értékeken alapulnak. A társadalmi devianciákat tárgyaló szociológiai irodalom az ilyen magatartási szabályokat a *jogi,* az *erkölcsi normák* és a *szokásnormák* tématerületei között tárgyalja. Míg a jogi normák megsértése jogszabályokban deklarált szankciókkal jár, az erkölcsi normák és a szokásnormák társadalmi rosszallást, informális elítélést, kiközösítést eredményezhetnek. A deviancia hagyományos fogalomköre magában foglal minden olyan egyéni és közösségi viselkedésformát, amelyeket a mindennapokban előforduló legenyhébb szabályszegésektől kezdve a legszélsőségesebb bűncselekményekig ismerünk. Abban viszont a devianciát tárgyaló tudományterületek közt is nagy lehet az egyetértés, hogy a normasértő viselkedéseket a társadalomra való veszélyességük mértékének eltérése miatt nem lehet egységes értelmezési ernyő alatt tartani, ezért szükségképp ki kell jelölni azokat a szempontokat is, amelyek mentén kiemelhető és leszűkíthető a legnagyobb kockázatot jelentő, az egyén és a közösség integritását leginkább veszélyeztető deviációk csoportja. Ugyan társadalmanként eltér, hogy milyen magatartásmintákat tekintenek veszélyesnek és ezáltal deviánsnak, azonban a devianciák meghatározásában vannak közös vonások. Így például a társadalom többsége negatív értékítéletét fejezi ki a deviánsnak minősített magatartásokkal szemben. Lényeges, hogy az adott magatartás komplex reakciót vált ki mind a társadalom tagjaiból, mind a kontrollintézmények részéről. Nyilvánvaló, hogy a deviáns viselkedésforma nem lehet túlsúlyban a konform magatartásformákhoz képest.[18] A deviáns magatartásforma semleges sem lehet: többnyire veszélyt jelent az egyénre és a közösségre, beleértve a deviáns személyt is (ön- és közveszélyesség) (Gönczöl–Kerezsi 1993; Rosta 2007; Giddens 2008).

Egyes megnyilvánulások deviánssá minősítése korszakonként, társadalmanként és néhol társadalmakon belül is eltérő, vagyis nem minden deviancia megítélése egyforma mindenhol és mindenkor. Azaz a normasértő magatartások csak abban a társadalmi kontextusban és korszakban értelmezhetők, ahol és amikor megtörténtek/megtörténnek. Számos példa van arra, hogy a törvénysértő cselekedetet nem követi társadalmi rosszallás. Ez többnyire akkor fordul elő, amikor az adott *normasértés elfogadottá válik,* vagy olyan időlegesen kivételes magatartásról van szó, amelynek *hasznossága felülmúlja veszélyességét.* Egyes magatartásmintázatok megítélése még akkor sem egyértelmű, amikor azok

[18] Kivéve forradalmi helyzetekben, amikor éppen ez jelenti a társadalmi rendszer megváltozását.

olyan gyors lefolyású globális vagy társadalmi változások eredményei, amelyekhez az adott közösség nem tudott rögtön alkalmazkodni. Az elmúlt évtizedekben az *internet és a számítástechnikai eszközök globális forradalma* ilyen jelenség volt. A társadalom és annak különböző csoportjai eltérő tempóban és módon fogadták el azt a virtuális valóságot, amely egy csapásra lehetővé tette a tudásbázisok szabad elérhetőségét, a kultúrák találkozását és keveredését. Az internet és az ahhoz csatlakozó rendszerek és eszközök megjelenése először kizökkentette a hagyományos kommunikációs környezetében élő egyént a megszokott életmódjából, majd az innovációk társadalmi csoportonként eltérő terjedésének következtében a digitális eszközökhöz való *hozzáférés,* valamint az azok *használatában mutatkozó különbségek* mélyítették a társadalom egyes csoportjai közt fennálló szakadékot. Ennek legszélsőségesebb esete a korszerű infokommunikációs eszközökhöz való hozzáférés hiánya, valamint a digitális analfabetizmus. E két tényező még a fejlett világon belül is azonosítható, nem beszélve a perifériához tartozó országokról. Ennek megfelelően még ma is megfigyelhető, hogy a korábbi, *predigitális generáció* tagjai a technikai alapokra helyezkedő globális hálózatosodást gyakran erőn felülinek ítélik meg. Az új környezet kínálta lehetőségeket felismerő és azokhoz alkalmazkodni tudó társadalmakban ma már megkérdőjelezhetetlen, hogy a technikai fejlődés és az internetes hálózatosodás a gazdasági-társadalmi-politikai fejlődés kulcsa.

A villámgyors sebességgel lezajló technikai és hálózati konjunktúra alkalmassá tette a cyberteret arra, hogy ahhoz egyéni és közösségi *érdekek* és *értékek* kapcsolódjanak, aminek szükségszerű következményeként egy sor új normasértő magatartásforma is megjelent ugyanebben a környezetben. A fejlődés meghatározó mérföldköve az ezredfordulót követő időszakban induló web 2.0 volt, ami egyben a *harmadik generációs informatikai bűnözés* kezdetét, vagyis a cyberdeviancia entitásának önállósodását is jelentette. Két évtizeddel ezelőtt kevésbé volt elterjedt a köztudatban a *cyberbullying* vagy az elektronikus bankszámla megcsapolása – ma már jogi eszközökkel is szankcionált magatartások. A deviáns viselkedések efféle átváltozása mögött azonban számos új tényező áll, amelyek korábban nem vagy csak részben voltak érzékelhetők. A következőkben ezeket villantjuk fel.

- *Új javak.* Az informatikai rendszerek és az azokban tárolt adatok *új értéket* szolgálnak, megszerzésük a hagyományostól eltérő *technikai eszközöket, módszereket* igényel, ami a *hacking* különböző formáiban és az automatizált eszközök *malware-ek* használatában nyilvánul meg leginkább.
- *Szabályozatlanság.* A felhasználók köre napjainkra multikulturális közösséggé nőtte ki magát, *sokféle érték- és normarendszert* képviselve. Az egyre több területre kiterjedő társadalmi szabályozó erők ellenére koherens, univerzálisan is érvényes morális szabályrendszer még nem alakult ki, így a normák és a deviáns magatartás értelmezése is bizonytalan.
- *A környezet jelentéktelenségének látszata.* A klasszikus normasértő megnyilvánulások némelyikét a virtuális környezetben enyhébb társadalmi elítélés övezi, mint a valós kontextusban (például a szerzői oltalom alatt álló szellemi termékek jogosulatlan használata). Az ilyen normák megsértésének következményeivel szemben megszilárdulni látszik egyfajta immunitás, amely először az egyén, majd a közösség attitűdjeiben jelenik meg, később pedig általánossá válhat.
- *Anonimitás.* A virtuális tér lehetővé tette anonim akciók felszabadítják az egyént belső és külső kontrolljai alól. Míg a valós életben a személyes identitás felvál-

lalása visszatart a szabályszegéstől, és támogatja a konform viselkedést, addig a cybertérben a hagyományos normák különböző szintjei a *kettős moralitás* következtében könnyebben átléphetők (például online és offline pedofília).

- *Kontrollhiány.* Az online hálózat kontrollintézmények által kevésbé ellenőrzött, privát böngészésre alkalmas *deepweb* és annak része, a *darkweb* működése növeli a cybertérben megvalósuló normasértések latenciáját (például fegyver vagy robbanóanyag készítésének receptje, kábítószeradás és -vétel vagy a pedofília menedzsmentje). Ugyanez a nem rejtett hálózatra *(surface-web)* is igaz, ahol naponta számos jogsértés valósul meg anélkül, hogy a hatóság tudomására jutna, és gyakran még a sérelmet elszenvedőben sem tudatosul a normasértés (például levelezési rendszer feltörése, adathalászat, csalás, jogosulatlan adatkezelés, privát kémkedés).
- *Az offline normák eróziója.* Az anonimitás által támogatott kettős moralitás a digitális bennszülöttek szocializációjának része. A folyamatban a hagyományos normák nem mindegyike internalizálódik és automatizálódik, ami a valós életviszonyokban eligazodási pontot nyújtó normákhoz való alkalmazkodás nehézségeit okozza és termeli újra, főként annak következtében, hogy a netgeneráció tagjaitól ma már a társadalom alapvetően elvárja, hogy a cybertér aktív résztvevője legyen az élet minden területén.
- *Online-offline normakompatibilitás.* Előfordul, hogy az egyén a körvonalazódó virtuális szabályokhoz illeszti viselkedésének online kialakított és alkalmazott mércéjét, majd azt onnét a valós térbe kilépve is működteti. Amennyiben a két mérce nem kompatibilis, úgy problémák adódhatnak: innen nézve ott a gond, onnan nézve itt a gond. Normakompatibilitási probléma keletkezhet, amikor az offline világból történik az online világ szabályozása, illetve fordítva, amikor az online világból történik az offline világ szabályozása. Például az agresszív viselkedés bizonyos erőszakos játékokban az elérendő siker és a hatékonyság alapvető eleme lehet, az offline közösségi viszonyok között viszont kimondottan káros következményeket idézhet elő (például fizikai erőszak), ilyen módon elutasított lehet. A probléma azonban fordítva is megjelenhet. Például amikor olyan online reklámokat látnak a felhasználók, amelyek divatos offline javak könnyű megszerzését sugallják, s azok a valóságban mégis rendkívül nehezen érhetők el. Ilyen esetekben előfordulhat az illegális út, az illegális eszközök választása. A Merton feszültségelméletén (2002) alapuló nézőpont szerint ebben az esetben a két színtér *egymástól eltérő elvárási repertoárral rendelkezik,* nem mindig összeegyeztethető és gyakran normasértést eredményez.
- *A nyilvánosság megváltozása.* A *nyilvánosság* hagyományosan a közügyek intézésének a területe, élesen elhatárolva a magánszférától (például, ahogy Habermas bemutatja [1971]: a polgári korban a kávéházak jelentették az okoskodó nyilvánosság kialakulásának helyszínét). Az internet megjelenésének egyik hatása éppen az, hogy a köz- és a magánszféra közötti határok (is) elmosódnak: gyakran magánügyek jelennek meg a nyilvánosságban. Sőt a *tabloidizáció* következtében a politikusok esetében kifejezetten reklámeszköz a magánélet közüggyé tétele. Azonban nem csak a nyilvánosság előtt élő szereplők esetén

merül fel a magán- és a nyilvános szféra közötti határ elmosódása. Minden olyan esetben, amikor akarva-akaratlanul magánügyek kerülnek a nyilvánosságba, felmerül a személyes információkkal való visszaélés lehetősége. Például az egyén önbecsülését sértő, lejárató tartalmak destruktív erővel hatnak az egyén lelki integritására, ami további konfliktusokat generál (SMITH–MACKIE–CLAYPOOL 2016). Az egyén identitására vonatkozó információk könnyű elérése számos támadási felületet biztosít – ma már az erre irányuló szabályszegés mindennapos.

- *Informatikai kompetencia.* A hagyományos deviáns viselkedések mintázataihoz képest a cybertérben normasértőként leginkább az jöhet számításba, aki *alapvető digitális kompetenciával és az internet hálózatához elegendő hozzáféréssel* rendelkezik. Ugyanez nem mondható el a cyberdevianciákat elszenvedőkről[19] – legfeljebb felbujtóként.

2.1. Bűncselekmények a cybertérben

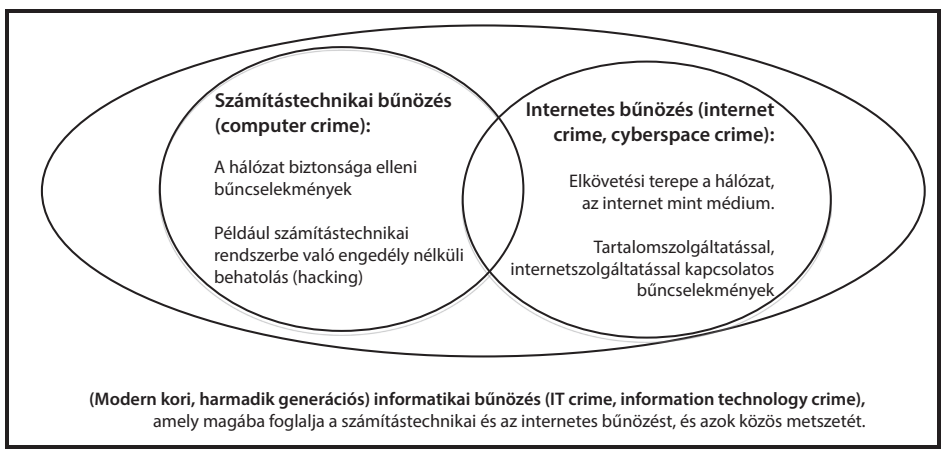
A bűnözés és a bűncselekmények együtt változnak a technikai fejlődéssel. A szakirodalom nemcsak a cybertérhez köthető bűncselekmények elnevezésével kapcsolatban nem egységes, de még annak megállapításában sem, hogy egyáltalán milyen cselekmények tartoznak ebbe a kategóriába. A cyberbűnözés terminológiája 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, az információs technológiával esszenciális kapcsolatban állnak (például hacking, digitális adatok megsértése). Továbbá az olyan cselekmények is cyberbűncselekménynek tekinthetők, amelyek nem kifejezetten információstechnológia-fókuszúak, de mégsem függetlenek attól, tekintettel arra, hogy megvalósításukhoz nélkülözhetetlenek az informatikai eszközök (ilyen például az online elkövetett csalás, a nigériai levél, a *phishing* vagy az online terjesztett gyermekpornográfia). Leukfeldt a *cybercrime* megnevezést ernyőterminológiaként használja azokra a bűncselekményekre, amelyeknek feltétele az információs technológiák igénybevétele. Ezen belül megkülönböztet olyan cselekményeket, amelyekben az információs technológia cél és eszköz is egyben (ez lenne a szűk értelemben vett *cybercrime*), és olyanokat, amelyek megvalósításához az információs technológia (IT) elengedhetetlen, de nem célpont (ez a tág értelemben vett *cybercrime*) (LEUKFELDT 2016, 215.).

A számítástechnikai, valamint a számítástechnikai rendszerekkel kapcsolatos bűnözést, az internetes és az informatikai bűnözést sokan, sokféleképpen határozzák meg (BALOGH 1998, 35.; FÁZSI–FÁZSI 2009, 4.; WALL 1999; GRABOSKY–SMITH, 2001; GRABOSKY 2001). A mai napig nem beszélhetünk azonban kikristályosodott definícióról. Hiányzik az egyetértés abban, hogy az egyes cselekmények mennyiben kapcsolódnak a számítástech-

[19] Amikor a társadalmi élet szempontjából kiemelkedően fontos, kritikus infrastruktúrák informatikai rendszerét támadják, a rendszerbénulásokból adódó zavarok azokat a lakosokat is érintik, akik a számítástechnikai eszközöket közvetlenül sosem használták.

nikai rendszerekhez és mennyiben az internethez, és hogy e két felülettel való kapcsolatuk mennyiben kizárólagos, meghatározó.

Eltekintve attól a nyilvánvalóan bekövetkező jóslattól, hogy a technika fejlődése további új elkövetési felületeket, metódusokat és eszközöket hoz magával a jövőben (Nagy 2009, 12.; Kürti 2002, 24.), jelenlegi ismereteink alapján a következő definíció lehet helytálló: az informatikai bűnözés nem más, mint a számítástechnikai bűnözés *(computer crime),* az informatikai bűnözés *(IT crime, information technology crime)* és az internetes bűnözés *(internet crime, cyberspace crime)* kategóriájába tartozó magatartásokat kizárólagos módon magában foglaló kategória, amely egyben a kétfajta bűncselekmény közös halmazát is tartalmazza (3. ábra). Amíg a számítástechnikai bűnözés a számítástechnikai rendszerek és hálózatok integritását sérti (ilyen például a rendszerekbe való illetéktelen behatolás vagy benn maradás, azaz a *hacking*), addig az internetes bűnözésnél az internet az elkövetés terepeként funkcionál: az internet médiumként jelenik meg a tartalomszolgáltatással, internetszolgáltatással kapcsolatos bűncselekményeknél (például a hamis weboldalak segítségével banki adatok kicsalása a felhasználóktól vagy különféle tiltott tartalmak terjesztése). Az informatikai bűnözés körébe tartozó magatartások kizárólagosan a számítástechnikai és/vagy az internetes bűnözés körébe tartoznak. Az e két kategórián kívül eső cselekmények – annak ellenére, hogy az elkövetéshez informatikai eszközöket is felhasználhatnak (például számítógéppel, esetleg számítógépes hálózatban folytatott kettős könyvelés) – nem tartoznak a modern informatikai bűncselekmények kategóriájába (3. ábra).



3. ábra

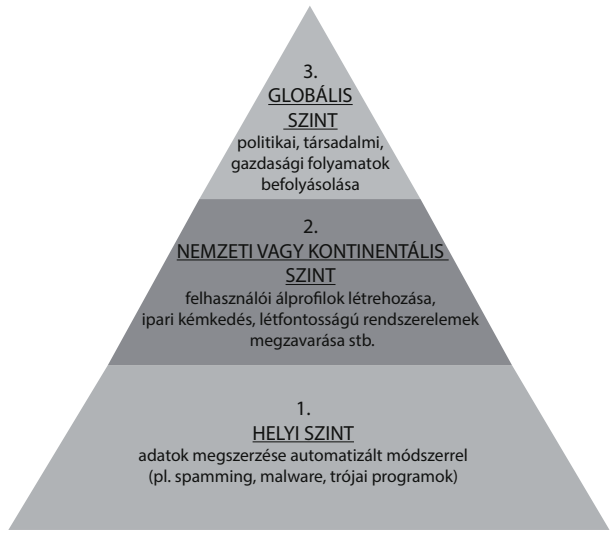
Számítástechnikai bűnözés, internetes bűnözés, informatikai bűnözés

Forrás: Parti–Kiss 2016, 492.

Az informatikai bűncselekmények a technikai fejlődésnek köszönhetően megjelenésüktől, az 1950-es évektől kezdve a 2000-es évek elejéig, azaz a modern információs kor beköszöntéig jelentős változásokon mentek keresztül. Ezt nevezzük az *informatikai bűnözés evolúciójának* (Wall 2008). Az *első generációs* informatikai bűncselekmények még olyan

hagyományos bűncselekmények voltak, amelyek a számítógépet használták eszközül az elkövetéshez, illetve az interneten található információkat használták fel. Ilyen volt, amikor a bűnelkövetők az internetet egyszerűen csak kommunikációs felületként használták, ott léptek kapcsolatba egymással, vagy onnan szerezték meg valamely előállítani kívánt hamis termék (például hamisított gyógyszer vagy kábítószer) receptjét. A *második generációs* informatikai bűncselekmények a hibridek kategóriájába tartoznak; ezek esetében a hagyományos bűncselekmények elkövetéséhez az internet globalitása új alkalmakat teremt. Ilyen például a számítástechnikai rendszerbe való jogellenes behatolás olyan módszerekkel és nagyságrendben, amely ugyan a globális network vagy a fejlett technológiák nélkül is megvalósulhatna, de más módszerekkel (például vállalati dolgozóktól a pszichológiai manipuláció módszerével jelszavak, belépési kódok kicsalása) és sokkal kisebb léptékben (például a hacking, amely a globális hálózat helyett csak a helyi hálózatot érinti). A *harmadik generációs* informatikai bűncselekmények (valódi informatikai bűnözés, modern informatikai bűnözés vagy *hypercrime:* McGUIRE 2007) nem létezhetnének a globális internet és a fejlett technológiák nélkül – lényegük a globális hálózatiság. Az első és a második generációs informatikai bűncselekmények esetében az internetet egyszerűen eltávolíthatjuk a műveletből, ennek ellenére a cselekmény még megvalósítható, éppen csak más csatornákat kell segítségül hívni a kívánt információ megszerzéséhez vagy a szervezőmunka lebonyolításához. Ezzel szemben a modern kori, harmadik generációs, *sui generis* informatikai bűncselekmények az internet nélkül egyszerűen nem létezhetnének (WALL 2008, 55–56.). Ezeket a technikai fejlődés termelte ki, és a bűnelkövetők ki is használják a globálisan összekapcsolható (feltörhető) hálózati rendszerek vulnerabilitását.

Idesorolható az automatizált spamtevékenység vagy kártékony vírusok *(malware)* számítástechnikai hálózatba juttatása az ott található felhasználói adatok megszerzése érdekében, amelynek célja a megszerzett adatok továbbértékesítése a globális „adatpiacon". A vásárló ezek után olyan komolyabb célokhoz használja fel az adatokat/információkat, mint amilyen a fogyasztói álprofilok tömeges létrehozása, az ipari kémkedés vagy a létfontosságú rendszerek (kritikus infrastruktúrák) működésének megzavarása. Az adatvásárló további, messze mutató célja lehet terrorcselekmény végrehajtása, politikai rendszer megdöntése vagy a gazdasági verseny befolyásolása. Látható tehát, hogy az adatok megszerzésétől a végső „csapás" megvalósításáig számos mozzanat valósul meg. Ebben a láncolatban az egyes elkövetői csoportok nem állnak egymással szükségszerűen kapcsolatban, de feltétlenül számítanak az informatikai bűnözésben rejlő potenciálra: az elkövetés egyes mozzanataira szerveződött csoportok aktivitására, valamint az illegális adatpiac folyamatos táplálására (4. ábra). A modern informatikai bűnözés három működési szintje ilyen módon tehát egymástól elválik, de egyik sem létezhetne az alsóbb szintek nélkül.



4. ábra

A harmadik generációs informatikai bűnözés hierarchikus, egymásra épülő rendszere

Forrás: Parti–Kiss 2016, 494.

A modern kor *harmadik generációs, sui generis informatikai bűnözése* olyan, a hálózat biztonsága elleni és/vagy a hálózatot mint médiumot az elkövetéshez felhasználó bűncselekményeket foglal magában, amelyek jellemzője a kész, *előre kifejlesztett számítástechnikai eszközöknek* (software-ek, malware-ek, egyéb alkalmazások) *szervezett és elosztott formában, meghatározott munkavégzési rendben, automatizált módon* való felhasználása valamely más, bűnözői csoportokkal, bűnszervezetek hozzáadott tevékenysége alapján, meghatározott cél elérésére (például információs rendszerek vagy létfontosságú rendszerek működésének megzavarása vagy megbénítása, adatok megszerzése vagy módosítása).

Az informatikai bűncselekmények jellemzője a *nemzetköziség* (az országhatárokon átívelő, transznacionális jelleg), a *gyorsaság* (hiszen az elkövető nem kell hogy jelen legyen az elkövetés helyszínén, illetve az elkövető és a sértett egymástól nagy távolságban is lehetnek), a magas *latencia* (emiatt szükséges a kriminálstatisztikához hozzágondolni a viktimizációs felmérések és a magáncégek fenyegetési jelentéseinek eredményeit), valamint az *intellektuális jelleg* (a fehérgalléros bűnözéssel való rokonság, de nem feltétlen egyezés).

2.2. Az informatikai bűncselekmények csoportosítása

Az utóbbi évtizedekben az elektronikus térben megjelenő devianciák mind szélesebb körének *kriminalizációja figyelhető meg.* A nemzeti szabályozási rendszerek alapvetően két variáció közül választhatnak, ha a számítástechnikai rendszer és az adatok védelmét kívánják biztosítani. Az egyik, hogy önálló ágazati törvényeket alkotnak ennek a speciális

területnek a szabályozására, ami 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 törvénye" (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. Hazánk az utóbbi kategóriába tartozik – még a korábbi, az 1978. évi Büntető Törvénykönyv gazdasági bűncselekményekkel foglalkozó fejezetébe kerültek elsőként (1994-ben) a számítástechnikai csalással, majd később (2002-ben) a számítástechnikai rendszerbe való jogtalan behatolással, benn maradással és a belépést lehetővé tevő technikai intézkedés kijátszásával kapcsolatos tényállások. Ezek a bűncselekmények a PC-k, a személyi számítógépek elterjedésével nyertek teret, amikor a gépek tartalmát, azaz az általuk, bennük tárolt adathalmazt fürkészte ki az elkövető, és a számítástechnikai rendszerbe való jogosulatlan belépésével vagy benn maradásával másnak szándékosan kárt okozott. E bűncselekménytípusok előrevetítették azt a tendenciát, amely a gépek devalválódásával, ezzel párhuzamosan pedig az információ, az adathalmaz felértékelődésével mutat összefüggést.

Az informatikai bűncselekményeknek többféle csoportosítása létezik. Így például *sértetti kör* szerint megkülönböztetünk:

- az egyén elleni informatikai bűncselekményeket (például gyermekpornográfia, online zaklatás, személyi számítógépek feltörése, adatlopás);
- vagyon elleni (szerzői jogokat vagy virtuális tulajdont sértő) bűncselekményeket;
- szervezetek, vállalatok elleni bűncselekményeket (például online terrorcselekmények, amelyekkel vállalatokra, kormányokra és nemzetközi szervezetekre gyakorolnak nyomást);
- társadalom elleni informatikai bűncselekményeket. Utóbbiak közé tartoznak a társadalmi dezorganizációt okozó cselekmények, amilyen a gyűlöletkeltő eszmék terjesztése, az öngyilkosságra buzdító weboldalak (POONIA 2014).

Az Európa Tanács számítástechnikai bűnözésről szóló egyezménye[20] a nyomozástechnikai és nemzetközi bűnügyi együttműködés elveit szem előtt tartva a következő csoportosítást alkalmazza:

- számítástechnikai rendszer és adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények (rendszerbe való jogosulatlan belépés, adatok jogosulatlan megváltoztatása vagy kifürkészése, számítástechnikai eszközökkel való visszaélés);
- számítógéppel kapcsolatos bűncselekmények (a számítógép az elkövetés eszköze: hamisítás, csalás);
- számítástechnikai adatok tartalmával kapcsolatos bűncselekmények (gyermekpornográfia);
- szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények (a materializálódott idea védelme).

[20] Az Európa Tanács Budapesten 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezménye, ETS. No. 185. (a továbbiakban: számítástechnikai bűnözésről szóló egyezmény). Magyarországon kihirdette a 2004. évi LXXIX. törvény.

A rendszerszintű reagálás elve szerint az Egyesült Királyság informatikai bűnözést kezelő operációs rendszere háromfajta bűncselekményt különböztet meg:

- tartalom-bűncselekmények *(crimes in the machine);*
- a számítástechnikai eszközzel elkövetett bűncselekmények *(crimes using the machine);*
- a számítástechnikai rendszer elleni bűncselekmények *(crimes against the machine)* (Wall 2010).

Az elmélet és a gyakorlat összekapcsolására, valamint a törvényalkotó szándékának megvilágítására a *nyomozástechnikai megközelítés* tűnik megfelelőnek, amely *az informatikai bűncselekményeket az internetnek az elkövetők által preferált tulajdonsága szerint közelíti meg.* Eszerint az informatikai bűncselekmények három csoportba sorolhatók:

1. A számítástechnikai rendszer integritása elleni, azaz a hálózat-bűncselekmények

A 2012. évi magyar Büntető Törvénykönyvben (a továbbiakban: Btk.) a számítástechnikai bűnözésről szóló egyezményben taglalt információs rendszer elleni bűncselekményeket négy törvényi tényállás fedi le. Idesorolható *a tiltott adatszerzés, az információs rendszer és adatok megsértése, az információs rendszer védelmét biztosító technikai intézkedés kijátszása és a vagyon elleni bűncselekmények fejezetcím alá tartozó információs rendszer felhasználásával elkövetett csalás.* Pontos meghatározásuk kapcsán fontos megjegyezni, hogy a felsorolt bűncselekmények mindegyikében az elkövetés tárgya maga az információs rendszer és a rendszerben kezelt adatok, nem az ezek mögött álló felhasználó vagy valamely szerzői jogi védelem alá tartozó dolog (például: szoftver). Az információs rendszerbe való jogtalan belépés már önmagában jogsértő cselekedet – attól függetlenül, hogy ezután bármely adat sérül-e. Amennyiben mégis az *adatok* képezik az elkövetés tárgyát, az információs rendszerek megsértése előfeltételként szerepelhet az eredmény megvalósításában – a jogtalan belépést követően fér csak az adatokhoz a rendszerfeltörő. Az információs rendszer elleni bűncselekmények szemléltetésére egyszerű példaként hozható fel a jelszóval védett e-mail-fiók. A levelezési rendszer feltörése napjainkban számos más, rendszerbe történő jogtalan belépésre is lehetőséget biztosít, ahol a regisztráció az e-mail-cím megadásával történik.

Az *információs rendszer felhasználásával elkövetett csalás* elkövetési tárgya ugyancsak a rendszer és a rendszerben kezelt adat. Az információs rendszer jogtalan befolyásolása jogtalan haszonszerzés érdekében történik, és vagyoni érdekeket sért. Az elkövető jogtalan adatkezeléssel hajtja végre műveletét – akár offline, akár online – az információs rendszert feltörve. Az internetes csalás iskolapéldái az internetes banki műveletek különféle formái, ahol adatok bevitelével, módosításával, törlésével végeznek el készpénzátutalásokat, internetes vásárlásokat akár adathalászat *(phishing)* útján megszerzett jelszavak vagy egyéb azonosítók (személyes adatok) további felhasználása révén. Az internetes csalás másik formája a jogosulatlanul megszerzett hamis vagy hamisított elektronikus készpénz-helyettesítő fizetési eszköz felhasználása vagy az azzal történő fizetés elfogadása – ha az kárt okoz.

2. A számítástechnikai adatokkal kapcsolatos tartalom-bűncselekmények

Az internetes hálózaton, az információs rendszerekben sértő, megalázó, a becsület csorbítására alkalmas adattartalmak, kiskorúakat ábrázoló pornográf felvételek elhelyezése, megjelenítése, tárolása, terjesztése annyiban tér el a hagyományos bűncselekményektől, hogy ezeket számítógépes rendszerek segítségével, az internetes hálózaton követik el. A tartalom-bűncselekmények az információs rendszer és adatok megsértésével is meg-

valósíthatók. Ebben az esetben az információs rendszer és adatok elleni bűncselekmény (a hackelés) csak eszközbűncselekmény, ugyanis a tartalom-bűncselekmények esetében az egyénnek és a közösségnek való közvetlen károkozás az elsődleges cél. A tartalom-bűncselekmények többségének szükséges eleme a nyilvánosság (más felhasználók) előtti megjelenítés és a célpontban álló egyénnek vagy közösségnek történő, nem feltétlenül anyagi, sokkal inkább erkölcsi károkozás. Az ilyen jogsértő cselekmények közé sorolható a becsületsértés, a rágalmazás – amikor a becsület csorbítására alkalmas tartalom jelenik meg az internetes közösségekben.

3. Az internet mint médium, azaz kommunikációs csatorna segítségével elkövetett bűncselekmények

Az interakciók sokféleségét nagyban elősegíti a dinamikusan fejlődő infokommunikációs eszközarchitektúra (mobileszközök), amely a földrajzi elhelyezkedéstől függetlenül rövid idő alatt biztosítja a gyors információáramlást a végfelhasználók között. Az internetes hálózat kommunikációs funkciója a kábítószer-kereskedelem, az erőszakos bűncselekmények, a vagyon elleni bűncselekmények, a szexuális bűncselekmények elkövetésében is fontos szerepet tölthet be.

2.3. A cyberdeviancia fogalma

A cyberdeviancia fogalmi megalkotásában feltétlenül figyelembe kell venni két meghatározó tényezőt, mégpedig a deviáns magatartás előidézőjét és megvalósulásának lehetőségeit. Bármely devianciáról is legyen szó (akár bűncselekmény, akár jogsértést elő nem idéző normasértő magatartás), hátterében emberi motivációk és célok rejlenek; végső soron humán cselekvések eredményei. Jó példa lehet erre a vírusok terjesztésével megvalósított károkozás, amikor közvetlenül *malware-ek* okozzák az informatikai rendszer összeomlását vagy a fájlok megsemmisítését, a felelősség mégis annak készítőjét vagy felhasználóját terheli. Abban a cyberdeviancia kutatói között is nagy az egyetértés, hogy a deviáns megnyilvánulás emberi jellemző, mint ahogyan annak megítélése és szankcionálása is egységes, ezért az internet hálózatában a számítástechnikai rendszerek és eszközök együttese eszközként és lehetőségként is számításba vehető.[21] A másik fontos tényező a normasértések mobilitása, amikor egy cselekvés két térben is kifejeződhet. Míg a nyilvános rágalmazás vagy egy e-mail-fiók feltörése teljes egészében történhet cyberkörnyezetben, addig az agresszióra épülő cselekedetek kiterjedhetnek mindkét színtérre, például eszkalálódhat a virtuális platformok bármelyikén, mielőtt fizikai erőszakként megvalósul a hagyományos környezetben. A térbeli mozgást logikus más-más színtéren zajló *mozzanatokként* és *összefüggésében* is vizsgálni. Az előbbi esetben a terekben külön-külön megvalósuló cselekvések eltérő súlya, különböző jogi és társadalmi megítélése, az utóbbi esetben a normasértő magatartás teljes hatása mérhető fel. A színterek közt mobilizálódó deviancia akkor nevezhető cyberdevianciának, ha *a normasértés folyamata valamilyen módon érinti a virtuális teret.* A folyamatban logikailag négy különböző módon jelenhet meg a cybertér.

[21] A mesterséges intelligencia megjelenésével a helyzet nyilvánvalóan bonyolódik, tekintve, hogy nem állapítható meg, ki használja az eszközt.

1. *Eredmény- és színtérmódozat.* Ebben a típusban a normasértés a cybertérben kezdődik, ott zajlik és ott is végződik, vagyis tisztán a számítástechnikai rendszerek és eszközök, illetve az internetes hálózat áll rendelkezésre a normaszegések elkövetésére. Ebben a módozatban a normasértők köre is leszűkül azokra, akik digitális kompetenciával rendelkeznek (IT-eszközök felhasználói szintű kezelését, az információs rendszerek és az internet hálózatában való szörfölés ismeretét és képességét jelenti).[22] Mivel az eredmény és a színtér egyaránt érinti a cyberteret, sőt csak és kizárólag azt, ezért természetesen ez a módozat ad lehetőséget a cyberdeviancia új formáinak megjelenésére, az anonimitásra, a titkos információáramlásra és a szabályozatlan szürke foltok működésére.

2. *Eredménymódozat.* A hagyományos és a cybertér szoros kapcsolatát azok a normasértő magatartások fejezik ki igazán, amelyek történésük folyamatában átfogják a hagyományos és a virtuális teret. A folyamat kiindulópontja az offline tér, azonban ezen deviáns magatartások a virtuális „infrastruktúrákban" végződnek. Azaz olyan magatartásokról van szó, amelyek mind a rendszerintegritás elleni *(social engineering),* mind a tartalommal vagy médiummal összefüggő deviáns magatartásformákat (például a párkapcsolati erőszak verbális, zaklató jellegű formája) magukban foglalják.

3. *Színtérmódozat.* A színtérmódozat az eredménymódozat fordítottjaként működik. Ebben az esetben is mind a valós, mind a virtuális teret érinti a normasértés. Azonban ezúttal a cybertérben kezdődik a folyamat, ott is zajlik, de a valós térben fejeződik be. Ma már gyakori, ha egy virtuális térben eszkalálódó konfliktus testi sértéssé fajul, vagy az internetes kábítószer-kereskedés megrendelője szemtől szemben veszi át a tiltott szereket. Ideköthető a prostitúciós szolgáltatások internetes reklámozása és még sok más folyamat, amely az offline térben zárul. Ebben a módozatban követhetetlen kereskedelmi tevékenységek, konfliktusok és számos előkészítő cselekvéssorozat zajlik.

4. *Katalizáló módozat.* Ebben az esetben arról van szó, hogy a cselekvés egy szakasza kerül kapcsolatba az adott térrel – miközben nem ott kezdődik, és nem ott végződik. Ebből a szempontból mind az offline, mind az online térnek lehet katalizáló funkciója a normaszegő magatartás folyamata során. Ebből következően a katalizáló módozat két alcsoportra osztható, a *cybertér* és az *offline tér* katalizáló funkciója szerint. Az első esetben a cybertér gyakorol valamilyen hatást az eredményre, például amikor a hagyományos környezetben kialakuló féltékenység internetes konfliktussá formálódik, majd fizikai erőszakká fajul. A második esetben a hagyományos színtér katalizáló funkciója érvényesül. Ha ezt modelleznénk, akkor arra a napjainkban esetenként ciklikusan változó irányú *cyberbullyingot* hozhatnánk fel példaként, ahol az online lejáratást offline kiközösítés követi, majd ennek folytatásaként újabb internetes nyomásgyakorlás következik.

[22] Iskolapéldája lehet az internetes zaklatás, ahol a rendszeres fenyegetés a kommunikációs csatornák valamelyikén történik, és a megfélemlítés lelki erőszak formájában manifesztálódik. Az információs adatok megsértése vagy az információs rendszer felhasználásával elkövetett csalás is ebbe a kategóriába tartozhat, ha a vagyoni kárt okozó műveleteket egy programalapú vírussal valósítják meg, és a károkozás úgy teljesül, hogy nem lép ki a hagyományos színtérre, vagyis elektronikus úton befejeződik. Idesorolható még a gyermekkorúakról készített pronográf felvételek terjesztése, kereskedelme, a terrorszervezetek infrastruktúrák működésének megbénítására alkalmas támadásai vagy a becsület csorbítására alkalmas kifejezések, valótlan tényeket tartalmazó információk közzététele. Más kérdés, ha a színterek kapcsolódnak, és a magatartás folyamata kiterjed a hagyományos, valós színtérre is, mert ebben az értelemben – mint ahogy azt fentebb leírtuk – a megvalósítás módjai vegyesek.

Az elmúlt évtizedekben a normasértő magatartások társadalomra veszélyességük szerinti súlyozása és a fogalmi frissítések különféle definíciók megszületését eredményezték, amit leginkább a normasértésekkel szembeni társadalmi attitűdök folyamatos változásával lehet magyarázni. Valamely magatartás deviánsnak minősítése társadalmak közt, sőt még egy adott társadalmon belül sem minden esetben egységes, vagyis az attitűdváltozás gyakran csak idő kérdése. Más a helyzet a súlyosabb normasértésekkel, ahol a többségi társadalom negatív viszonyulása sokkal stabilabb. Hagyományos devianciákhoz hasonlóan a súlyosabb normaszegések a cybertérben is a jogi normák megsértését jelentik, vagyis aktivizálódásuk a kontrollintézmények felőli reakciót váltják ki. Mindez a cyberdevianciák esetében azt jelenti, hogy vannak olyan önbecsülést sértő faktorai, amelyekkel szemben inkább a közömbösség erősödik, mintsem az elítélés. Emellett léteznek olyanok is, amelyek időben és térben állandó elítélés tárgyai. A durva normaszegő magatartásmintákat és az enyhébb megítélésű elhajlásokat ennek okán egy szűkebb és egy tágabb fogalmi keretbe célszerű beillesztenünk úgy, hogy a korábban már felsorolt sajátosságokat és feltételeket nem hagyjuk figyelmen kívül. A szűkebb és tágabb fogalommeghatározást ezért a hagyományos feltételek mentén kíséreljük meg, hozzátéve a cybertér jellegzetességeit. Azaz cyberdevianciának az olyan cselekedetet nevezhetjük,

- amely érinti a cyberteret;
- amely jogi normát sért, vagy ön- és közveszélyes a cybertérben;
- amelyhez a társadalom többsége negatívan viszonyul;
- amely kiváltja a kontrollintézmények reakcióját;
- amely kisebbségben van az elfogadott magatartásmintákhoz képest;
- amelynek megvalósítója digitális kompetenciával rendelkezik;
- amelynek hátterében humán tényezők állnak (vagyis emberi célok, szándékok, motivációk, szükségletek).

A cyberdeviancia szűkebb értelemben a cybertérben megvalósított olyan közvetett vagy közvetlen, digitális kompetencián alapuló emberi magatartás, amelyhez az adott társadalom tagjainak többsége negatívan viszonyul, jogi normákat sért, formális reakció kiváltására alkalmas, gyakoriságát tekintve kisebbségben van az adott társadalom többsége által elfogadott magatartásmintákhoz képest, valamint veszélyt jelent az egyénre és/vagy a közösségre.

A föld egészét átölelő hálózat felhasználóinak körében az értelmezés egy cseppet sem egyszerű, sőt egy-egy magatartás lehet egyik mérce szerint normasértő, a másik szerint elfogadott. A legtöbb társadalomban a gyermekkorúakról készült pornográf felvételek terjesztése jogsértő, a rágalmazás vagy a becsületsértés azonban eltérő értelmezésű lehet. A fentiekben meghatározott szűkebb fogalom szerint a cybertérben manifesztálódott szabályszegő magatartás deviánsnak minősítése – bár nagyjából azonos feltételek fogalmazhatók meg – függ attól, hogy *mely társadalom felhasználóinak körében került nyilvánosságra, és a deviáns magatartásokat megvalósító és elszenvedő mely társadalom tagja*.

A cyberdeviancia tágabb fogalomköre a szűkebbet is magában foglalja, de annál jóval több megnyilvánulásra terjed ki, és nem csak a súlyosabb normasértésekhez áll közel. Ennek alapján cyberdevianciának az olyan cselekedetet nevezhetjük,

- amely érinti a cyberteret;
- amely normát sért, vagy ön- és közveszélyes a cybertérben;
- amely kiváltja a társadalom többségének negatív értékítéletét;

- amely a társadalom többségének negatív reakcióját váltja ki;
- amely kisebbségben van a társadalom többsége által elfogadott magatartásmintákhoz képest;
- amelynek megvalósítója digitális kompetenciával rendelkezik;
- amelynek hátterében humán tényezők állnak (vagyis emberi célok, szándékok, motivációk, szükségletek).

A cyberdeviancia tehát tágabb értelemben a cybertérben megvalósított olyan közvetett vagy közvetlen, digitális kompetencián alapuló emberi magatartás, amellyel szemben az adott társadalom tagjainak többsége negatív értékítéletét fejezi ki, legalább informális reakció kiváltására alkalmas, kisebbségben van az adott társadalom többsége által elfogadott magatartásmintákhoz képest, az adott társadalom valamely normáját sérti.

A cyberdeviancia szűkebb és tágabb fogalmi meghatározásának célja olyan fogalmi keret biztosítása, amely eligazodási lehetőséget nyújt a normasértő magatartásformák besorolása és csoportosítása során.

2.4. A cyberdevianciák motivációi

A cyberdevianciák tárgyalásában kiemelt szerepe van azoknak a motivációknak, amelyek a legtöbb deviáns megnyilvánulás hátterében állnak, stabil kiindulópontot nyújtanak a normasértő magatartások oksági vizsgálatában, és a cybertérre adaptálhatók. A cyberdevianciák tárgyalása során sem kerülhetjük meg az agresszióra, a szexuális és a haszonszerzési szükségletekre épülő motivációkat, ezért a következőkben ezeket vesszük sorra.

2.4.1. Agresszióra épülő motivációk

Az agresszió belső lelki tartományban rejtőző késztetésekhez, külső környezeti tényezők által alakított lelkiállapotokhoz köthető, támadó jellegű magatartás, ellenséges belső rezdületek, élmények hatására keletkezik, és igen gyakran belső feszültséggel jár (Hárdi 2010, 29). Megjelenése szerint lehet *belső,* az egyén lelkivilágában, érzelmekben, lelki feszültségben, indulatok formájában, illetve *külső,* vagyis egyének és közösségek interakcióiban manifesztálódó jelenség. Irányulhat egyéntől *önmaga felé* vagy *a külső környezet irányába,* előbukkanhat tudatos vagy tudattalan formában, közvetlenül vagy közvetve, de átalakult alakzatban is (agresszió szublimálása) (Hárdi 2010, 30.). A cybertérben az agresszív megnyilvánulások széles palettáját találhatjunk, kifejeződhetnek kép, hang, szöveg, gif, internetes mém tartalmakban, heves párbeszédben. Az agresszív érzelmek ahogy a hagyományos térben, úgy a cybertérben is a legsúlyosabb erőszakos normasértésekhez vezethetnek, azzal a különbséggel, hogy utóbbi keretek között az erőszaknak nem a fizikai vetületeivel számolhatunk (például pszichikai erőszak).

Az agresszió reaktív és instrumentális típusa – a legenyhébb sértegetésektől a rendszerintegritást sértő magatartásokon át – a kényszerítésig tartó magatartások ösztönzője, amivel kapcsolatban az agresszióelméletek széles irodalma ad különböző magyarázatokat. A virtuális környezetben megjelenő agresszív megnyilvánulások nem mindegyike eredmé-

nyez jogi normát sértő cselekvéseket és pszichés erőszakot sem, ugyanakkor a legenyhébb formája is negatív hatással van a résztvevőkre. A cybertérben megnyilvánuló agresszió társadalomra veszélyességének mértéke szerint szükséges az *erőszak* és az *agresszió* megkülönböztetése. Ennek alapján az *agresszív cselekvésnek a virtuális térben* – hasonlóan a hagyományos környezethez – több jellemzője van:

- az egyén negatív érzelmeiből fakad;
- a cybertérben valamely normát sért, de minimálisan magára az agresszorra vagy más felhasználó(k)ra van negatív hatással (de nem minden esetben váltja ki a társadalom többségének rosszallását és a kontrollintézmények reakcióját);
- jellemzője a terek közti mobilizálódás.

Az agresszióból fakadó magatartás úgy értelmezhető, mint minden olyan, az egyén negatív érzelmeiből fakadó, cybertérbe megnyilvánuló manifesztáció, amely magára az egyénre vagy másra negatív hatással van, vagy valamely normát sért, de még nem tartalmazza a fenyegetést, a kényszerítést és a megfélemlítést.

Az agresszió meghatározásához képest az erőszak szűkebb fogalom, a kriminológiai erőszakfogalom szerint „embertől eredő, másik személyre közvetlenül irányuló, a cél elérésére alkalmas fizikai vagy pszichikai erőt jelent" (VIGH et al. 1973, 42.). A WHO megfogalmazása szerint „az erőszak fizikai erő vagy hatalom szándékos alkalmazása – az ezzel való fenyegetés vagy tényleges alkalmazás –, amely önmaga, más személy, egy csoport vagy egy közösség ellen irányul, és amely fizikai sérülést, halált, pszichés ártalmat, fejlődési elakadást vagy deprivációt eredményez, vagy nagy a valószínűsége, hogy ilyen eredményre vezet" (KRUG et al. 2002, 5.; idézi: VIRÁG–KULCSÁR–ROSTA 2016, 554.). A cybertérbe az erőszak nem fizikai formái illeszthetők, meghatározásához a fenti erőszakfogalmakban és az erőszakos bűncselekmények büntetőjogi tényállásaiban is megtalálható elemeket, *a kényszerítést és a fenyegetést* vesszük alapul, amelyek a virtuális környezetben is irányulhatnak személy ellen, manifesztálódhatnak szexuális magatartásokban és vagyon elleni normasértésekben. A cybererőszakra is érvényes az a megállapítás, hogy minden esetben agresszióból keletkezik, de az nem minden esetben válik erőszakos magatartássá (VIRÁG–KULCSÁR–ROSTA 2016, 555.). Ha ebből indulunk ki, akkor a cybertérben megnyilvánuló erőszak az egyén vagy közösség irányába ható agressziónak a virtuális tér „infrastruktúrái" mentén megnyilvánuló tudatos, szándékos, károkozásra képes formája.

A cyberkörnyezetben az erőszakos magatartás-mintázatok megvalósításuk szerint két csoportra oszthatók. Amikor a *kényszerítés,* a *fenyegetés* alkalmazását követően a normasértés a *hagyományos térben végződik* (közvetett), és amikor a *cybertérben fejeződik* be (közvetlen). Az előbbire példaként a szexuális kényszerítés hozható fel, ahol maga a kényszerre irányuló cselekvés az internetes csatornákon történik, viszont az eredmény (szexuális aktus) már fizikai kontaktussal végződhet. A másodikra a zsarolás bűncselekményét említjük példaként, ahol a fenyegetéssel, kényszerítéssel a cselekmény befejezése is a virtuális térben marad (Skype-os zsarolás, majd ennek következményeképpen az összeg banki átutalása). Az cybererőszak fogalmába tartozhat a zsarolószoftver *(ransomware).* A szoftvert az elkövető eljuttatja a kiszemelt felhasználó rendszerébe, ahol rendszerbénulást okoz. Amíg a felhasználó nem fizet „váltságdíjat", a rendszere blokkolva marad (Symantec 2015).

A cybererőszak két alapvető eleme valamelyikének vagy mindegyikének meglétéhez kötött, súlyosabb cyberdeviancákat eredményez, valamely normát sért és a társadalom szé-

les köre által elítélt. Az erőszak cyberkörnyezetben zajló mechanizmusának – hasonlóan az agresszióhoz – több jellemzője van:

- szándékos károkozásra vagy szükségletkielégítésre irányul, és agresszióból fakad (kényszerítéssel, fenyegetéssel megnyilvánuló agresszió);
- a cybertérben jogi normát sértő magatartás (legalább erkölcsi vagy szokásjogi normát sért);
- alapvető eleme a kényszerítés, a fenyegetés vagy a megfélemlítés;
- az egyénre vagy a közösségre káros hatással van;
- jellemzője a terek közötti mobilizálódás.

A cybertérben megnyilvánuló erőszak a fenti jellemzők szerint *minden olyan, nem fizikai formában megjelenő kényszerítéssel, fenyegetéssel megvalósított agresszív cselekvés, amely pszichikai erőszak előidézésére alkalmas, másra mindenképp káros hatással van, társadalmi elítélés övezi, minden esetben normasértő, továbbá jogi normasértést idéz elő.*

Abban az esetben, ha az erőszakos magatartás hagyományos színtéren fejeződik be, csak akkor sorolható a cybererőszak fogalmi körébe, ha a kényszerítés, a fenyegetés valamelyike vagy mindegyike a cybertérben is megtörténik. A hagyományos térben erőszakos bűncselekményeknek minősített és a cybertérben megnyilvánuló erőszakos magatartások közt lehet különbség, ugyanis az offline térben a fenyegetés büntetőjogi értelmezés szerint nem feltétlenül tartozik az erőszakosnak tartott magatartások közé, attól függetlenül, hogy a kriminológiai értelmezés szerint pszichés nyomás előidézésére alkalmas. A cybererőszak megfogalmazását viszont a pszichés erőszak feltételei – vagyis a kriminológiai fogalom – mentén határoztuk meg. Míg tehát a cybertérben megjelenő zaklatás a büntetőjog értelmezése szerint nem tartozik az erőszakos bűncselekmények körébe, addig kriminológiai értelemben annak minősíthető.[23]

A virtuális térben az agresszió által motivált cselekvések oksági folyamatát és társadalomra veszélyességét akkor lehet optimálisan feltérképezni, ha a magatartást több irányból vizsgáljuk, vagyis az *agresszort,* az agresszív magatartás *elszenvedőjét,* a magatartás *környezetét, időbeliségét* és más motivációkkal való összefüggéseit is górcső alá vesszük. Az agresszió és az erőszak különböző megközelítése tisztán rámutat a cselekvések veszélyességére, és lehetőséget biztosít a normasértések e szerinti besorolására.

[23] Btk. 222. §.

4. táblázat
Agresszióra és erőszakra épülő normasértések a cybertérben

Agresszióra épülő normasértések	• negatív érzelmeken alapuló párbeszéd (flaming), vagy negatív érzelmek által motivált tartalommegjelenítés; • negatív érzelmek által motivált, önbecsülést sértő vagy becsületcsorbító kifejezés, tényközlés kommunikációban vagy tartalommegjelenítéssel (például a becsületsértés, rágalmazás); • egyén vagy közösség elleni szándékos károkozó magatartás rendszerintegritás megsértésével (például információs rendszer befolyásolása bosszúból); • egyén és közösség elleni károkozó magatartás kommunikációs csatornákon vagy tartalommegjelenítéssel (például karaktergyilkosság, kollektív normasértés internetes mémek segítségével).
Erőszakra épülő normasértések (kényszerítés, fenyegetés, megfélemlítés vagy félelemkeltés alapvető eleme)	• cybertérben történő zsarolás; • cybertérben történő zaklatás; • extrém csoportok cybertérben történő erőszakos működése; • terrorszervezetek cybertérben történő erőszakos működése.

Forrás: Kiss Tibor szerkesztése

2.4.2. Szexuális szükségletekre épülő motivációk

Az egyén életében a szexualitás az egyik legfontosabb életfunkció: mindazon biológiai mechanizmusok és viselkedési manifesztációk összessége, amelyek biztosítják a nemek találkozását, a megtermékenyülést és a szaporodást. Az ember esetében azonban a biológiai funkciók az örömszerzéssel is kiegészülnek (BUDA 2002, 51.). Ennek következtében a választás szabadsága a szexualitásra is kiterjed: mind a biológiai, mind a gender-, mind a szexuális viselkedés tekintetében. A szexuális viselkedést meghatározó szexuális késztetéseket (libidót) a hagyományos magyarázó elméletek mentális, illetve szociális energiaként is említik, amelyek valamely módon szükségszerűen leképeződnek a külvilágban. Sigmund Freud szerint a libidó pszichés energia, szexuális *drive,* szexuális ösztönkésztetések hordozója, amelynek valósághűvé tétele az egyén pszichés működésétől függ (OZSVÁTH 2011; PLÉH–BOROSS 2010). Az ember esetében a szexuális viselkedés genetikai determináltsága bonyolult mozzanatok sorával kapcsolódik össze, amiben kiemelkedő szerepe van a szexuális viselkedés tanulásának, az élményszerzésnek, a szexuális viselkedési minták internalizálásának, továbbá a tiltásnak az elfogadott és az elfogadhatatlan szexuális viselkedés határainak kijelöléséhez. A kultúra kialakulása éppen a szexuális tabuknak a megjelenésével veszi kezdetét: Freud elmélete szerint ezek a tiltások jelentik az ösztönén *(id)* felettes én *(szuperego)* általi megzabolázását, amelynek következtében

jön létre a kultúrában élő én *(ego)*.[24] A tanulás ebbéli fontossága, hogy az egyén megfelelő szexuális viselkedésre legyen képes, megfeleljen a szexuális szerepelvárásoknak és kihívásoknak (például párválasztás), adaptálódni tudjon környezetéhez, és képes legyen a szexuális viselkedés társadalmilag elvárt módon való megjelenítésére. Az ember szexuális fejlődésének szakaszában – szól a hagyományos elmélet – előbb a nemi azonosságtudat alakul ki, majd a nemi szerepviselkedés, ami eleinte többnyire szexuális fantáziákban, majd valós cselekvésekben jelenik meg. Ha a szexuális fejlődés szükséges mozzanatai nem megfelelőek, akkor feszültségek lépnek fel, amelyek felnőttkorban is meghatározók lehetnek (Buda 2002, 54.). A szexuális megnyilvánulások különböző rendellenes alakzatai egyes magyarázóelméletek szerint a szocializáció zavaraiból, a szexuális diszfunkciókból és a parafíliákból eredeztethetők, más elméletek ezzel szemben arra világítanak rá, hogy a destruktív szexuális magatartások hasonlóképp előfordulhatnak konform egyéneknél is, a napi feszültséglevezetés eredményeként.

Cybertérben a normasértő szexuális viselkedések az adott helyzetben részt vevő személyek egységes akaratának hiányában, fizikai kapcsolat nélkülözésével vagy a fizikai érintkezés előkészítéseként, előzményeként zajlanak. *Olyan, szexuális ösztönkésztetéseken alapuló magatartások ezek, amelyek a felek egységes akaratának hiánya miatt olykor agresszióval vagy a pszichés erőszak elemeivel karöltve közvetlen kommunikációban, szexuális tartalmak küldésével, fogadásával, közzétételével vagy rendszerintegritás elleni támadások által manifesztálódnak.* A szexuális viselkedés hagyományos és virtuális alakzataiban meghatározó szerepe van a kommunikációnak, pontosabban a partner szexuális vágyát közvetíteni képes hanghatásoknak és a másodlagos nemi jegyek, erogén zónák látványát nyújtó vizuális ingereknek (Buda 2002, 56.). A kommunikáción alapuló normasértő szexuális interakciók elsősorban a gyermek- és fiatalkorú felhasználókra, de az anonimitás miatt másokra nézve is különösen kockázatosak. Olyan fizikai védelmi bástyákat iktatnak ki, mint az elsődleges és a másodlagos szocializációs színtér, a kortárscsoportokból álló baráti közösségek, a szemtől szemben történő észlelés és a beazonosítás lehetősége. Az anonimitás emellett olyan rejtett lehetőség, amely a gátlások nélküli perverz fantáziálásoknak és a parafíliák (például pedofília) megjelenésének is melegágya lehet.

A cybertérben megvalósuló szexuális motivációk által ösztönzött normasértő magatartások veszélyességük szerint legalább három csoportba sorolhatók:

1. A szexuális tartalmak a szexuális feszültség normasértő eredménnyel járó levezetését szolgálják (például szexuális tartalmak küldése, fogadása, közzététele).
2. A cybertérben zajló cselekvés bármely színtéren megvalósuló szexuális normasértés előzménye vagy előkészítő stádiuma (például a behálózás, a *grooming*).
3. A szexuális erőszak lenyomata vagy annak következményei a virtuális környezetben észlelhetők (például zaklatás, zsarolás a cybertérben).

A három csoportba sorolt viselkedésforma mindegyike valamilyen normasértést keletkeztet, és céljuk *a szexuális szükséglet kielégítése vagy feszültség levezetése*. Eltérés viszont abban van, hogy más-más súlyú deviáns magatartásformák részei: a szexuális tartalmak küldésétől a behálózáson át az erőszak alkalmazásáig. Mindemellett a szexuális tartalom

[24] Bizonyos kutatások szerint ez a Freud megfontolásaira visszavezethető elmélet kultúrafüggetlen.

küldése és nyilvánosságra hozatala *(szexting)* nagyon gyakran anyagi haszonszerzés céljából elkövetett zsarolás vagy a féltékenység által ösztönzött lejáratás eszköze, mint ahogy a szexuális zaklatásnak vagy zsarolásnak az erőszak. Ebből az is következik, hogy szexuális indíttatású normasértések gyakran összefonódnak az agresszióval.

5. táblázat

A szexuális motivációkra épülő normasértések a cybertérben

Szexuális motivációk	• szexuális tartalmak szerepeltetésével való visszaélés (például *szexting,* szexuális témájú kommunikáció); • behálózás *(grooming)*
Szexuális motivációk agresszióval vagy erőszakkal összefonódva	• szexuális tartalmak szerepeltetésével történő visszaélés (például *szexting,* szexuális témájú kommunikáció bosszúból); • cybertérben történő szexuális zsarolás; • cybertérben történő szexuális zaklatás.

Forrás: Kiss Tibor szerkesztése

2.4.3. Haszonszerzési szükségletekre épülő motivációk

A haszonszerzési szükségletek – ahogy a hagyományos térben is – markáns motivációként szerepelnek a cyberdeviancák hátterében. Nagyon gyakran kapcsolódnak az agresszív vagy erőszakos motivációkhoz, és kimondottan anyagi vagy más haszon megszerzésére irányulnak. A magatartást megelőzheti a behálózás szakasza, és eszköze lehet a szexuális tartalmak szerepeltetése *(szexting),* főként zsarolás esetében. A haszonszerzés szükséglete körül felépített műveletek a virtuális infrastruktúrák mentén, illetve a terek közti mozgásban zajlanak a normasértést elkövető és a elszenvedő fél közti közvetlen vagy közvetett kapcsolatban. A cybertérben a haszonszerző normasértések három nagyobb csoportja különböztethető meg megvalósításuk módja és terepe szerint.

1. *Haszonszerzés információs rendszerek elleni támadásokkal,* technikai módszerek segítségével. A rendszerintegritás elleni magatartások különböző szintű információs rendszerekbe történő behatolásra irányulnak. A már önmagában normasértést megvalósító rendszerfeltörés célja, hogy a rendszer működését befolyásolja, az elkövető adatokat szerezzen és semmisítsen meg, módosítson, továbbadjon vagy felhasználjon, és ezért közvetetten vagy közvetlenül jogtalan előnyt szerezzen, legyen szó anyagi vagy más ellenszolgáltatásról.

2. *Az illegális kereskedelmi tevékenységek útján történő jogtalan haszonszerzés* valamely engedély nélküli kereskedelmi tevékenység, illegális áruk, szolgáltatások adásvétele anyagi haszonszerzés vagy más előnyhöz jutás céljából. Ha a magatartás aktív interakcióra épül, akkor minimum két személy megegyezésén alapul. A cybertérben kereskedelmi tevékenységet végző szereplőknek több formális előírásnak kell eleget tenniük. A legális működéshez a pénzügyi mozgások ellenőrizhetősége, az áruk és a szolgáltatások legalitása, a fogyasztói jogok betartása, a tevékenység folytatására való alkalmasság feltétlenül szükséges. A virtuális ügyletek lebonyolítóinak egy része a feltételeknek egyáltalán nem

vagy csak részben felel meg, sőt esetenként kifejezetten tudatosan nélkülözik a legalitást. A virtuális feketepiac működésének mozgatórugója az óriási adózatlan jövedelem megszerzésének lehetősége és a tiltott vagy illegális forrásból származó árukra és szolgáltatásokra való fizetőképes kereslet kihasználása. A cybertér nehezen szabályozható és nehezen elérhető piacterén illegálisan működő kereskedelmi tevékenység annak a haszonszerzési láncolatnak a szerves része, amely a harmadik generációs informatikai bűnözés legalsó és globális szintjét köti össze. A cybertér feketepiaca az internet hálózatának egy területe (a *deepweb* bizonyos területei), ahol kábítószer- és fegyverkereskedelemre, prostitúciós szolgáltatások nyújtására szakosodott egyének és közösségek értékesítik „portékáikat" igen nagy kereslettel. A titkosság és az anonim működés emberek sokaságát motiválja az efféle helyek látogatására és az ott nyújtott, nyilvánvalóan tiltott szolgáltatások igénybevételére. Olybá tűnik, mintha a követhetetlen keresőmotorokkal elérhető „sötét" oldalakon a hagyományos morális és erkölcsi dogmák szándékos ignorálása történne mind a felhasználók, mind a szolgáltatók részéről.

3. *Az információs csatornákon át történő információközléssel vagy kommunikációval* megvalósított haszonszerzési folyamat valójában minden olyan virtuális cselekvést magában foglal, amelyben a haszonszerzés két vagy több felhasználó közt létrejövő közvetett (tartalomközlés) vagy közvetlen kapcsolat (kommunikáció) útján történik, és része a megtévesztés, a meggyőzés vagy az erőszak (zsarolás egy kommunikációban).

Az első esetben nem feltétel a normasértést elszenvedővel való közvetlen kapcsolat, a másik kettőben alapvető feltétel, vagyis a felek közti megegyezésen alapul. A haszonszerző magatartásformák szorosan kapcsolódó láncolatának egyik legismertebb modellje, amikor gyermekkorú felhasználót ejtenek tévedésbe internetes ismerkedés útján, kicsalják zárt információs rendszerének belépési kódját, majd oda jogtalanul belépve az ott talált fotókat egy adatpiacon értékesítik egy harmadik félnek, aki felvásárlást követően pornográf tartalmú weboldalakra tölti fel azokat.

6. táblázat

Haszonszerzési motivációkra épülő normasértések a cybertérben

Haszonszerzési motivációk	• engedély nélküli tevékenységgel illegális áruk és szolgáltatások kereskedelme (például kábítószer, fegyver, pornográf tartalmak kereskedelme); • engedély nélküli kereskedelmi tevékenység (például nem bejelentett, hatóságok által nem nyilvántartott vagy nem engedélyezett); • behálózás *(grooming)*; • cybertérben megvalósuló csalás.
Haszonszerzési motivációk agresszióval vagy erőszakkal összefonódva	• cybertérben történő zsarolás; • cybertérben történő zaklatás.

Forrás: Kiss Tibor szerkesztése

2.5. Cyberdevianciák

A cyberdeviancia fogalma két feltétel mentén tér el a hagyományos devianciafogalomtól, mégpedig a *cybertérben való megvalósulás szükségességében* és a *digitális kompetencia* meglétében. A térhez kötöttség és a digitális kompetencia viszont csak a normasértő részéről állandó, míg a normasértést elszenvedő esetében nem mindig (például egy rendszerbénítással okozott áramkimaradás a számítástechnikai ismeretekkel nem rendelkezőkre is hatással van).

A hagyományos, társadalmi együttélésre veszélyes devianciák szűk fogalomkörébe olyan stabil magatartásminták és cselekvések tartoznak, mint az alkoholizmus, a kábítószer-fogyasztás, az öngyilkosság, az antiszociális viselkedést megalapozó mentális betegségek és a bűnözés. Fizikai megjelenésüktől eltekintve igen gyorsan integrálódtak a cyberkörnyezetbe, mégpedig az anonim működés lehetőségének a következtében – lásd: kábítószer-kereskedelemben való részvétel. Az interneten és az ahhoz kapcsolódó információs rendszerekben megvalósuló devianciák egyfelől az offline térből történő „egyszerű" migrációval kerülnek az online világba, s gyakran arra is korlátozódnak. Ezek többnyire a szexuális ösztönkésztetésekből, agresszív érzelmekből, anyagi haszonszerzéshez kötődő szükségletekből eredeztethetők, miközben a társadalom és kontrollintézményei jelentik megítélésük alapját.[25] Másfelől bizonyos devianciák kifejezetten az online tér megjelenésével állnak elő. A cyberdevianciák okainak magyarázatára egyre több átfogó kutatás indul, amelyekhez a hagyományos devianciaelméletek tézisei adnak kiindulási pontot. Az alábbiakban röviden felvázoljuk azokat a normasértéseket, amelyek a virtuális térben a leggyakrabban előfordulnak.

2.5.1. Szexuális tartalmak szerepeltetése *(szexting)*

A szexuális tartalmak cybertérben történő szerepeltetése (szexting) a felhasználó által önmagáról vagy másról készített szexuális témájú, valós vagy módosított kép, videó, gif,[26] *internetes mém, szexuális témájú szöveges üzenet küldésével, fogadásával, továbbításával, közzétételével megvalósított cselekvések összessége.*

A *szexting* agresszióból, szexuális és haszonszerzési szükségletekből egyaránt eredeztethető, gyakori eszköze az internetes lejáratásoknak, a konfliktusokból eredő feszültségek levezetésének (például rágalmazás vagy becsületsértés), ugyanakkor súlyosabb normasértésekhez is kötődik, mint a zaklatás, a közösségi zaklatás, a zsarolás, az információs rendszer és adatok megsértése vagy a mindezeket előkészítő behálózás. A szexuális tartal-

[25] A szexuális indíttatású behálózás a köztudatban súlyosabb megítélés alá esik, mint az agresszív érzelmek által generált konfliktus eredményét képező rágalmazás.

[26] A *gifek* olyan hangulatkeltő, rövid, összevágott videók, amelyek lényegi eleme a bemutatott esemény eredeti környezetéből való kiragadása, a tartalmak szisztematikus kreatív összemosása. Ezekben az esetekben nem értelmezhetők a „hamis", „hamisított" jelzők, ugyanakkor mára az online véleménynyilvánítás bevett eszközei. A *gif* csak egy az innovatív online kifejezőeszközök közül, amelynek értelmezési kereteit a jogalkalmazás fogja kijelölni, eközben azonban ügyelnie kell a szabad véleménynyilvánítás követelményének érvényesülésére. Az okostelefonos applikációk lehetőséget adnak a mémek más formában történő megjelenítésére is, ilyen például a *wink* vagy a *snap,* amelyek lehetővé teszik, hogy a felhasználó képet, montázst készítsen, és azokat tetszés szerint, meghatározott ideig tegye láthatóvá a címzett számára.

mak küldése, fogadása része a mindennapi virtuális kommunikációnak. Önmagában addig nem minősül normasértésnek, amíg a bizalomra és diszkrécióra épülő zárt kommunikáció része. Ha e rendszerből a nyilvánosság elé kerül, de jogi normát nem sért, akkor csupán „virtuális illetlenségként" definiálható. A tartalmak elküldése és fogadása elsősorban akkor súlyos szabályszegő magatartás, ha azokat *tulajdonosának rendelkezése és irányítása alól engedélye nélkül vagy akarata ellenére kivonják, majd visszaélés céljából nyilvánosságra hozzák, harmadik félnek továbbítják, illetve minden esetben akkor, ha a tartalmak szereplői gyermekkorúak*. A *szexting* a zárt elektronikus levelezőrendszertől a nyilvános közösségi platformokig sokféle kommunikációs csatornán keresztül megvalósítható, de leginkább az előzőekben tárgyalt *eredmény- és színtérmódozatban,* valamint az *eredménymódozatban* valósul meg önálló normasértésként, más funkciókban csak más normasértésekkel együtt.

7. táblázat

Szexuális tartalmak szerepeltetésével megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	Szexuális tartalmak szerepeltetése (szexting)
Nem normasértő	• nem nyilvános; • felnőtt korú felhasználók közt zajló zárt interakció része; • a küldő és fogadó felek, illetve a tartalmak szereplőjének beleegyezésével és elfogadásával történik.
Erkölcsi szokást, normát sértő	• szándékos közzététel nyilvánosság előtt, de nem visszaélés eszköze.
Jogi normát sértő	• szándékos közzététel azonosítható képmások engedély nélküli felhasználásával vagy visszaélés, károkozás céljából; • más jogsértő magatartásokhoz kapcsolódik (cyberzaklatás); • gyermekkorúakról készült felvételek felhasználása.

Forrás: Kiss Tibor szerkesztése

2.5.2. Pornográf tartalmak szerepeltetése

A pornográf tartalmak internetes szerepeltetése a felhasználó által önmagáról vagy másról készített, pornográf aktusokat ábrázoló, valós vagy módosított képi anyag (videó, gif, internetes mém stb.) küldésével, fogadásával, továbbításával vagy közzétételével megvalósított cselekvések összessége.

A pornografikus események (például a nemi közösülés különböző módjai, nemi szervekről vagy meztelen testekről készült tartalmak) közzétételét, küldését, fogadását, illetve efféle tartalmú weboldalak látogatását sokan erkölcsi elhajlásnak tartják. A *nyilvánosan elérhető weben* számos gyűjtőoldal vagy videómegosztó működik, amelyek megjelenítése nem minden esetben váltja ki a kontrollintézmények vagy a társadalom többségének negatív reakcióit. A tartalmak elítélésében vagy elfogadottságában a különböző kultúrák szexualitással kapcsolatos előírásai is meghatározók, ezért nem minden társadalomban elfogadott az explicit szexualitást bemutató oldalak látogatása. Ettől függetlenül az internetes pornográfia a legtöbb társadalomban a rosszallás és az elfogadás határmezsgyéjén mozog,

normasértővé minősítése két nagyon érzékeny feltétel meglététől függ. Az egyik a tartalmak *közzétételének módjában,* a másik a pornográf *tartalmakban* keresendő. Az azonnali formális és informális reakciót az előbbi esetben a közzététel szabályainak megsértése,[27] az utóbbi esetben gyermekkorúak szerepeltetése váltja ki, vagyis *a gyermekkorúakról készült szexuális aktusokat, pornografikus elemeket tartalmazó valós vagy módosított kép (videó, gif, internetes mém stb.) közzétételében, küldésében, fogadásában, tárolásában megnyilvánuló magatartás.*

A gyermekek egészséges testi, lelki, erkölcsi fejlődése érdekében a róluk készített szexuális tartalmú információs egységek tiltása evidens; szexuális visszaélést valósít meg. A szigorú társadalmi elítélés és kontroll hatására a gyermekpornográfiával kapcsolatos weboldalak működése egyre inkább a nehezen elérhető weboldalakra szorul vissza, hozzáférésük a titkos szörfölést biztosító keresőmotorok által biztosított. A tiltott felvételekkel szemben kialakult stabil társadalmi rosszallás és az azonnali hatósági reakció egyébként annak is köszönhető, hogy a képmások és az aktusok más cyberdevianciák és számos, hagyományos színtéren zajló normasértés előzményei és következményei lehetnek. A gyermekekről készült képek, videók felhasználásának egyik iskolapéldája az Európában is elterjedt és napjainkra már szigorú szabályozás alatt lévő virtuális szerepjáték. *A tiltott szexuális játék olyan interaktív részvételt biztosító tartalom, amelyben a grafikus szereplők karakterét gyermekkorúak testrészleteiből, teljes testéből, felismerhető képmásából formálták.* A szerepjátékok normasértő jellege egyes társadalmakban megkérdőjelezhető, ha a grafikus szereplők gyermekkorúak valósághű és felismerhető képmásait nem hordozzák. A korábban Second Life játékokon belül ismert *age play* igénybevevői egyben másodlagos felhasználói a gyermekkorúak kizsákmányolásából származó pornográf felvételeknek (PARTI–KISS 2016). A nyersanyagnak számító képmások több állomáson haladnak végig, míg azokból megformázott virtuális figura elkészül. Először a gyermekkorúak képmását, pornográf felvételeit készítik el – vagy szerzik meg –, majd azokat az adatpiacon értékesítve vagy közvetlen kapcsolat útján juttatják el a virtuális játékok készítőihez. Ezután kerül újból piacra ellenszolgáltatás fejében vagy nyilvános elérhetőséggel már szerepjátékként. A szabálytalan internetes pornográfiával szemben kialakult társadalmi elítélés és a gyermekpornográfia büntetendősége ellenére az interneten számos támogató platform és gyűjtőoldal működik.[28]

A pornográf felvételek szerepeltetése a cybertér *eredmény- és színtérmódozatában,* a gyermekekről készült pornográf felvételek szerepeltetése pedig az *eredmény- és színtérmódozatokban, valamint* az *eredménymódozatban* manifesztálódik, leginkább normasértő magatartásként.

---

[27] A tartalomszolgáltató a weboldal elérhetőségére vonatkozó szabályokra, az oldal használatára vonatkozó figyelmeztetésekre és az üzemeltetőjének elérési adataira vonatkozó kötelezettségeinek nem tesz eleget, illegálisan üzemelteti a weboldalt.

[28] Az ilyen oldalak növekvő népszerűségét egyébként igazolni látszik, hogy a gyermekekről készült pornográf felvételek készítéséért, közzétételéért, tárolásáért, kereskedelméért egyre több egyén és közösség kerül szembe a hatóságokkal.

8. táblázat

Pornográf tartalmak szerepeltetésével megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	Pornográf tartalmak szerepeltetése	Gyermekekről készült pornográf tartalmak szerepeltetése
Nem normasértő	• nem nyilvános vagy szabályozott környezetben elérhető; • felnőtt felhasználók közt zajló zárt interakció része; • a küldő és fogadó felek, illetve a tartalmak szereplőjének beleegyezésével és elfogadásával történik.	–
Erkölcsi normát, szokásjogot sértő	• szándékos, de még nem jogsértő közzététel.	–
Jogi normát sértő	• pornográf tartalmú oldalak szabálytalan működtetése, azonosítható képmások engedély nélküli felhasználása, vagy azzal való visszaélés; • más jogsértő magatartásokhoz kapcsolódik.	• elkészítés, közzététel, küldés, fogadás, tárolás.

Forrás: Kiss Tibor szerkesztése

2.5.3. Behálózás a cybertérben *(grooming, cybergrooming)*

A behálózás olyan, szisztematikusan felépített, gyakran manipulatív, közvetlen vagy közvetett kommunikáció, amelynek célja a másik fél meggyőzésén át valamely szükséglet kielégítése vagy azt szolgáló cselekvés előkészítése.

A *behálózás* hátterében szexuális szükségletek és haszonszerzési motivációk egyaránt állhatnak, ugyanakkor számos normasértő cselekvéshez kapcsolódhat. A szexuális célzatú behálózás célja szexuális kapcsolatkötés, olykor pornográf tartalmak megszerzése, de némely esetben súlyosabb abúzusok *előkészítő folyamata is lehet* (például zsarolás, zaklatás). A *grooming* megítélésében szükséges figyelembe venni az érintett életkorát, az interakcióban betöltött szerepét és a behálózó célját. A behálózás anyagi vagy más kárt okozó haszonszerző műveletek eszközeként legtöbbször jogi normát sértő magatartás, viszont ha nem jár együtt anyagi vagy lelki károkozással, megmarad az erkölcsi normasértés szintjén. A behálózás deviáns magatartásnak minősítéséhez ezért alapvető feltétel, hogy valamely normasértő magatartáshoz kapcsolódjon, és megjelenjen a megvalósító céljai, képzetei között.

A behálózó virtuális karaktere nem mindig valós, lehet változatos nemű és életkorú, szexuális bűncselekményeket gyakran elkövető, gyermekkorúakkal szexuális kapcsolatot létesíteni szándékozó személy vagy épp prostitúciós tevékenységet szervező csoport tagja. A folyamatnak bárki részese lehet, de leginkább a gyermek- vagy fiatalkorú felhasználók

esetében a legkockázatosabb. Az információszerzés a művelet része; ez történhet közvetlen kommunikációs kapcsolatban, információs rendszer megsértésével (például trójai program telepítésével), levelezőrendszerek, közösségi profilok feltörésével és jogellenes adatkezeléssel. Potenciális veszélyforrásnak számítanak a szexuális kapcsolatok létesítését támogató társkereső weboldalak, mobilapplikációk vagy a közösségi oldalak, ahol a gyanútlan felhasználó teszi közzé adatait, és így kerül kapcsolatba a deviáns szereplővel. Gyermek-felnőtt kapcsolatokra vágyó felhasználók céltudatosan keresik a társkereső vagy közösségi oldalak sebezhető résztvevőit abból a célból, hogy kifinomult módszerekkel a behálózni szándékolt áldozatról személyes információkat gyűjtsenek. A behálózás manipulatív, a zárt kommunikáció része, nehezen észlelhető a külvilág számára, ezért a súlyosabb normasértések egy olyan szakasza, amelyre nagy fokú latencia jellemző. A behálózó művelet legtöbbször a cybertér *eredmény- és színtérmódozatában* zajlik, de ha hagyományos normasértő magatartásokhoz kapcsolódik előzményként, akkor a cybertér *színtér-* és *katalizáló módozataiban* is értelmezhető.

9. táblázat

Behálózással megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	**Behálózás**
Nem normasértő	–
Erkölcsi normát, szokásjogot sértő	• Nem kapcsolódik jogi normát sértő hagyományos és cyberdevianciákhoz, de a kommunikáció tartalmaz megtévesztő, manipulatív elemeket.
Jogi normát sértő	• Jogi normát sértő cyberdevianciákhoz vagy hagyományos normasértő magatartásokhoz kapcsolódik, azok előkészítő folyamata, illetve a manipulatív és megtévesztő kommunikációra alapul.

Forrás: Kiss Tibor szerkesztése

2.5.4. Megfélemlítés a cybertérben *(cybermegfélemlítés, cyberbullying)*

A cybermegfélemlítés szándékos tartalomküldés, tartalommegjelenítés vagy kommunikáció útján valamely szükségletkielégítés, feszültséglevezetés céljából alkalmazott fenyegető, megfélemlítő, pszichés erőszak előidézésére alkalmas magatartások összessége. Irányulhat egyén vagy közösség ellen, származhat egyéntől vagy közösségtől, a legtöbb esetben rendszeres. Közvetett módon sérthet információs rendszereket, és fizikai erőszak formájában is megnyilvánulhat.

A megfélemlítés olykor teljes egészében, néhol előzményeiben, időnként pedig eredményében kötődik a cybertérhez, de előfordul, hogy a virtuális környezet katalizáló szerepet tölt be a hagyományos térben zajló nyomásgyakorlás folyamatában. Az interperszonális kapcsolatokban zajló fenyegetések és rendszeres megfélemlítések szándékos cselekvések hozadékai, agresszióból vagy szexuális motivációkból fakadnak, egyes esetekben pedig haszonszerzési indíték köthető hozzájuk. Személyközi kapcsolatokban kialakuló mintázatainak egyike az *egyéntől egy vagy több egyén irányába ható nyomásgyakorlás,* megjelenését

tekintve leginkább személyközi konfliktusok része (például párkapcsolati vagy kapcsolati erőszak *[relational aggression]*), olykor pszichés betegségek következménye (például parafíliák). A megfélemlítés normasértő formája magában foglalja a cybererőszak elemeit, a becsületcsorbító tényeket és kifejezéseket tartalmazó kommunikációt vagy információs rendszer és adatok elleni bűncselekményt.

A cyberbullying közismert formája a gyermekkorúak között megvalósuló kortárserőszak. A cybertérben történő abúzust fiatal felhasználói közösség gyakorolja, és igen gyakran előzménye vagy következménye a kortárscsoportok hagyományos iskolai környezetben zajló kollektív magatartásának. A cybermegfélemlítés normasértő jellege állandó, de nem minden esetben váltja ki a kontrollintézmények reakcióit, ami az érintett felhasználó azon szubjektív megítélésétől függ, hogy a felé irányuló nyomásgyakorlást normasértőnek minősíti-e vagy jelzi-e a környezetének.

Ugyanakkor vannak olyan cselekvések a virtuális térben, amelyek nem tartalmazzák az erőszak elemeit és becsületcsorbító, rágalmazó kifejezéseket, mégis kellemetlenül érintik a felhasználót. Ilyen a rendszeresen megjelenő, nem kívánt és tolakodó reklámtartalom termékekről, szolgáltatásokról, amelyek ugyan nem törvénysértőek, de hatásukat tekintve gyakran az elviselhetőség határvonalán állnak.

A cybermegfélemlítés egyénről egyénre irányuló, közösségtől egyénre ható modelljei lehetnek *nyílt* (külvilág részéről érzékelhető) és *látens* (környezet számára láthatatlan) megjelenésűek, de az egyéni zaklatók működhetnek *anonim* módon is (személyazonosságuk elrejtésével). A megfélemlítés a cybertér minden funkciójában érvényesülhet, vagyis az egyik legösszetettebb cyberdevianciának minősül.

10. táblázat

Megfélemlítéssel megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	Megfélemlítés
Nem normasértő	–
Erkölcsi normát, szokásjogot sértő	• Jogi normát sértő alakzata nem valósul meg, cybererőszak elemeit nem tartalmazza, kellemetlen zavaró tartalomküldés, tartalommegjelenítés vagy kommunikáció (például rendszeresen küldött reklámtartalom vagy hirdetés: *spam*).
Jogi normát sértő	• Az erőszak elemei megvalósulnak (például fenyegetés, megfélemlítés), a zaklatás áldozatát a rendszeres életvitelében akadályozza, lelki presszíót eredményez vagy más jogi normát sért.

Forrás: Kiss Tibor szerkesztése

2.5.5. Zsarolás a cybertérben

A cybertérben megvalósuló zsarolás szándékos tartalomküldés, tartalommegjelenítés vagy aktív kommunikáció útján, valamely szükséglet kielégítése céljából alkalmazott kényszerítő, fenyegető, megfélemlítő, lelki erőszak előidézésére alkalmas magatartások összessége. Irá-

nyulhat egyén vagy közösség ellen, származhat egyéntől vagy közösségtől, közvetett módon sérthet információs rendszereket, és fizikai erőszakként is végződhet.

A zsaroló jellegű magatartásoknak a számítástechnikai rendszerintegritást sértő *közvetett* és kommunikációs csatornákon át *közvetlen* formában megnyilvánuló, *szexuális, valamint haszonszerzési motivációkhoz* köthető alakzatai a leggyakoribbak. A szexuális szükségletekből eredő zsarolásban *(sextortion)* a normasértő valamilyen (többnyire szexuális) tartalom nyilvánosságra hozatalával vagy továbbküldésével zsarolja a felhasználót, illetve aktív virtuális párbeszédben kényszerítéssel veszi rá őt a szexuális érintkezésre vagy a szexuális szükségletek kielégítésére irányuló más cselekvésre (például szexuális vagy pornográf tartalmak küldésére).

Az anyagi vagy más előny megszerzését célzó zsarolás közvetett alakzata abban tér el a szexuális zsarolástól, hogy a kényszerítés vagy a fenyegetés hátterében anyagi vagy más előny megszerzésére irányuló motivációk és követelések állnak (például Skype-os zsarolás).

A cyberzsarolást gyakran *automatizált eszközökkel* (zsarolóvírusokkal) *közvetett* módon hajtják végre, ahol *nincs közvetlen személyes kapcsolat a normasértő és az áldozat között*. A kártékony szoftver a célrendszerekbe (információs rendszerekbe) jutva annak működését megbénítja vagy befolyásolja, és egy előre megírt textuális tartalom arra utasítja a normasértést elszenvedőt, hogy rendszere korábbi állapotának visszaállításáért elektronikus banki átutalással vagy virtuális fizetőeszközzel (kriptovalutákkal) fizessen a program készítőinek. A blokkolt rendszerekben gyakran értékes és nagy mennyiségű adat kezelése történik, vagy fontos infrastruktúrákat működtet, ezért a megtámadott rendszer tulajdonosának vagy üzemeltetőjének érdeke a kérés teljesítése – miközben a rendszer normál állapotának visszanyerése bizonytalan. A világ bármely pontjáról elvégezhető műveletben több eszköz erőforrásait használhatják, akár globális hálózatokat is érinthetnek, és ezzel manipulatív hatalmi szándékokat érvényesíthetnek. Abban az értelemben eltérő az általános rendszertámadásoktól és jogtalan adatkezelésektől, hogy ennek fejében *a normasértő ellenszolgáltatást vár, tevékenységét haszonszerzési motiváció ösztönzi.* A latencia óriási, gyakran hosszú idő elteltével derül fény az incidens megtörténtére.

A zsarolás néhol kapcsolódik a cybermegfélemlítéshez, előzménye lehet a behálózás és eszköze a szexting, ugyanakkor gyakori, hogy a hagyományos térben folytatódik és fejeződik be. A cybertérben történő zsarolás minden formája valamely normát sért, de nem minden esetben váltja ki a kontrollintézmények reakcióit. Jogi normát sértő szintre emelése attól függ, hogy a cybererőszak elemeinek valamelyikét tartalmazza-e, megnyilvánulási formáját az elszenvedő felismeri vagy veszélyesnek tartja-e. Mindezektől függetlenül kevés olyan változata létezik, amely ne sértene valamilyen társadalmi normát (kivétel lehet két személy kapcsolatában megnyilvánuló érzelmi zsarolás, amelynek része ugyan a kényszerítés, de ritkán történik külső beavatkozás).

11. táblázat
Zsarolással megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	Zsarolás
Nem normasértő	–
Erkölcsi normát, szokásjogot sértő	• Jogi normát sértő alakzata nem valósul meg (például: érzelmi zsarolás egy online kapcsolatban).
Jogi normát sértő	• Jogi normát sértő magatartásként manifesztálódik; • A cybererőszak elemei megjelennek és az anyagi károkozás megvalósul.

Forrás: Kiss Tibor szerkesztése

2.5.6. Csalás a cybertérben

A cybertérben megnyilvánuló csalás jogtalan anyagi vagy más előny megszerzése céljából, szándékos tartalomküldéssel, -megjelenítéssel, aktív kommunikációval vagy rendszerintegritást sértő műveletekkel megvalósított megtévesztő, anyagi vagy más károkat (bizalomvesztést) okozó magatartások összessége.

A cybertérben megvalósuló csalás haszonszerzési motivációk által ösztönzött magatartás, sok esetben a zsarolás, a zaklatás haszonszerzésre alapuló alakzataihoz kapcsolódik, ugyanakkor előzménye lehet a behálózás. A technikai módszerekkel megvalósított csalás legismertebb formája az adathalászat *(phishing),* amely során az adatkérésre vonatkozó megtévesztő tartalommal a csaló arra veszi rá a felhasználót, hogy *elektronikus úton* adja meg személyes vagy online bankfiókja, bankkártyája adatait, amelyeket később felhasznál. A személyes vagy banki adatokkal banki műveleteket (készpénzátutalásokat, vásárlási tranzakciókat) folytat – megkárosítva a megtévesztett felhasználót. Az adathalászat esetében a felhasználóval való *közvetett* kapcsolat útján valósul meg a megtévesztés.

A számítástechnikai módszerekkel megvalósított csalás további formája az információs rendszerek megsértésével szerzett adatok jogosulatlan felhasználása, úgymint az elektronikus készpénz-helyettesítő fizetési eszköz előállítására, hamisítására és annak offline vagy online felhasználására irányuló művelet vagy egyéb visszaélés. Az előbbi és az utóbbi esetében a cybertér színtérfunkciója érvényesül akkor, ha a rendszerfeltörés vagy a megtévesztés online, a felhasználás offline térben zajlik (Parti–Kiss 2016). A rendszerfeltörés és a megtévesztéssel történő adatszerzés (belső rendszerek azonosítóihoz való hozzájutás) lehet ipari kémkedés része, vagyis új technológia, felfedezés vagy eljárási metodikák feltérképezése és másolása. A kettős haszonszerzési műveletben az adatokat megszerző normasértő jut anyagi haszonhoz, valamint az ellopott információt megrendelő szereplő, aki az adatok felhasználásával piaci előnyt szerez.

A virtuális csalás másik típusa *tartalmakkal* vagy *aktív kommunikációval* történik. A tartalmakban a normasértő adományt kér, nyereményekre hivatkozik, nem létező szolgáltatásokat, termékeket kínál (gyakran hivatalos weboldalakon) anyagi ellenszolgáltatásért cserébe. Ebben az esetben ugyancsak a felhasználó megtévesztéséről van szó közvetlen interakcióban (párbeszédben) vagy közvetett módon (tartalommegjelenítéssel), ahol a nor-

masértést elszenvedő aktív tevékenységével segíti a jogtalan haszonhoz való hozzájutást. A csalás abban nyilvánul meg, hogy sem a kínált terméket, szolgáltatást, nyereményt nem kapja meg a felhasználó, sem az adomány címzettje nem egyezik a tartalomban feltüntetettel, illetve nem azt a terméket vagy szolgáltatást kapja, amelyért fizetett. Ebbe a kategóriába sorolhatók az aukciós csalások különböző módozatai, így például:

- Az aukciós oldalakon licitáló felhasználók a fizetést követően nem kapják meg a terméket, vagy nem a kívánt terméket kapják.
- A kiküldött terméket a vásárló egy hasonló, de sérült termékre cseréli, és azzal az ürüggyel, hogy sérülten érkezett, követeli annak cseréjét.
- Az aukciós oldal licitálási folyamatát manipulálják, ezzel jelentős és aránytalan értéket kérnek az áruért.
- A megjelenített értéket fizetett felhasználók pozitív véleményekkel megerősítik, ezzel befolyásolva a jóhiszemű vevőket.

Az aktív kommunikációban zajló csalás a megtévesztő és a gyanútlan felhasználó közti közvetlen interakciót jelenti (például Skype vagy valamely chatalkalmazás segítségével), vagyis tartalmazza a manipulálás, megtévesztés, befolyásolás technikáit. A személyes vagy banki adatok megszerzésében a kommunikáció színterének központi szerepe van. Abban az esetben, ha a megtévesztő kommunikáció hagyományos környezetben zajlik, majd a károkozás az online hálózatban, akkor a cybertér *eredménymódozata* érvényesül, ha fordítva, akkor a *színtérmódozat,* ha a megtévesztés és a károkozás is cybertérben történik, akkor az *eredmény- és színtérmódozat* aktivizálódik. A csalás nem minden esetben váltja ki a kontrollintézmények reakcióját, de e mögött a normasértésben érintett felhasználó részéről a normasértés észlelésének nehézségei vagy a felelősségre vonásról való szubjektív döntés áll (kivétel lehet egy virtuális szerepjátékban történő megtévesztés, amely ugyancsak okozhat anyagi károkat, de ritkán minősül jogsértő magatartásnak).

12. táblázat

Csalással megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	**Csalás**
Nem normasértő	–
Erkölcsi normát, szokásjogot sértő	• Jogi normát sértő alakzata nem valósul meg (például virtuális játékokban történő megtévesztés és ezzel történő előnyszerzés).
Jogi normát sértő	• Jogi normát sértő magatartásként manifesztálódik (megtévesztés módszerével anyagi vagy más károk okozása); • a cybererőszakhoz közvetett módon kötődik.

Forrás: Kiss Tibor szerkesztése

2.5.7. Internetfüggőség

Az internetfüggőség a hagyományos közösségi terektől és társas kapcsolatoktól való szándékos elhúzódás és a hálózat társas tereihez, kommunikációs csatornáihoz, szolgáltatásaihoz vagy technikai platformjához való kényszeres ragaszkodás. Olyan életvitelként írható le, amelyben az egyén élete, értékítélete megváltozik, egyre gyengülő offline kapcsolatait a virtuális világ biztosította kapcsolatokkal pótolja.

Az addikció a pszichológia szerint egy olyan állapot, amelyet valamely természetes vagy szintetikus anyagok egymást követő alkalmazása vált ki, kényszeres cselekvés és sajátos életforma jellemezheti. Két alapvető formája a kémiai és a viselkedési addikció, amelyek közül az előbbi esetében valamely függőséget okozó szer rendszeres fogyasztása, az utóbbi hátterében egyes cselekvések, mint például a kóros játékszenvedély állhat (Ozsváth 2011, 11.). A kémiai és a viselkedési addikció esetén egyaránt észlelhetők a függőség jelei, vagyis a szer megvonása, illetve a kényszeres cselekvés megakadályozása fizikai vagy lelki tünetekkel járhat. Az internetfüggőség inkább a viselkedési addikciókhoz áll közelebb, amit a köztudatban az internetesjáték-szenvedéllyel, az online pornográfia iránti szenvedéllyel és az internetes vásárlási szenvedéllyel említenek együtt. Az internetfüggőség ennél sokkal több magatartás-mintázatban észlelhető; deviáns magatartássá minősítésében fontos hangsúlyozni, hogy nem feltétlenül internetfüggő az, aki valamely társadalmi elvárás okán használja intenzíven a cyberteret (például munkahelyi követelmények miatt), és az internetfüggő felhasználók mindegyike sem feltétlenül deviáns. *Az internetfüggőség a cyberdeviancia körébe akkor sorolható, ha alapja más normasértő cselekvéseknek* (például gyermekkorúakkal kapcsolatos normasértések), *más addikciókhoz kapcsolódik, és az egyén életvitelére, szociális kapcsolataira, lelki és fizikai egészségére nézve káros, destruktív hatással van, vagyis naponta fizikai, pszichés vagy szociális problémákat okoz.* A Mentális rendellenességek diagnosztikai és statisztikai kézikönyvének (DSM) V. melléklete tartalmazza az internetfüggőség tünetcsoportjának a leírását. Elsősorban pszichológiai problémáról és nem jogi kérdésről van szó.

13. táblázat

Internetfüggőséggel megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	Internetfüggőség
Nem normasértő	• A cybertér használata rendszeres, és huzamosabb időt vesz igénybe, nincs negatív hatással az egyénre és környezetére, nem kapcsolódik más normasértő magatartásokhoz és addikciókhoz.
Erkölcsi normát, szokásjogot sértő	• Káros hatással van az egyén testi, lelki integritására, szociális kapcsolataira, jogi normát sértő magatartásokhoz nem, de más addikciókhoz kapcsolódik.
Jogi normát sértő	• Jogi normát sértő magatartás része (például pedofil cselekvések) lehet.

Forrás: Kiss Tibor szerkesztése

2.5.8. Károkozó, destruktív cselekvések a cybertérben

A károkozó destruktív folyamatok az egyénre vagy a közösségre vonatkozó tények, információk szándékos meghamisításával, módosításával, megsemmisítésével, hamis információk terjesztésével járó, gyakran becsületcsorbító, provokáló cselekvések, amelyek némely esetben számítástechnikai rendszerintegritást sértő magatartásokkal járnak együtt.

A köztudatban karaktergyilkosságként, provokatív trollkodásként és ezen okokból megvalósított rendszerfeltörésként ismert magatartások célja kimondottan az anyagi vagy az erkölcsi károkozás. Az alábbi vetületei emelhetők ki.

- Nem haszonszerzési célból történő rendszerintegritást sértő magatartások köre, vagyis a *rendszerek működésének olyan befolyásolása, megbénítása vagy jogtalan adatkezelés,* amelynek hátterében tekintélyes szerepet tölt be az agresszió (például frusztrációból vagy bosszúból fakadó agresszivitás), az élményszerzés, a társadalomnak vagy más közösségnek való megfelelés vágya és a kíváncsiság. Az efféle ösztönzők a rendszersértő fiatal hackerek (például *skiddie*-k, *cyberpunkok, crackerek*) jellemző indítékai közé tartoznak, ami végső soron megbélyegzi közösségüket. A szándékos rongálás a külső szemlélő számára motiválatlan cselekvésnek tűnhet, ezért sokan a digitális vandalizmushoz hasonlítják, bosszantó, szándékos rongálásnak tekintik.
- A *karaktergyilkosságként* ismertté vált cyberdevianciában a virtuális karakter mindazon információk és adatok összessége, amelyek az egyén életéről a cybertérben megtalálhatók. Az információk többségét a gyanútlan felhasználó teszi közzé vagy tárolja külső adattárolókon és különféle rendszerekben. A karaktergyilkosság célja az ilyen adatok megszerzésével, megváltoztatásával, megsemmisítésével vagy negatív tartalmú elleninformációk gyártásával és közzétételével a jó hírnév céltudatos és szándékos megsértése nagy nyilvánosság előtt. Hátterében olykor olyan hatalmi szándékok állnak, mint egy választási eljárás manipulálása azzal, hogy a jelöltek egyikéről koholt információkat közölnek, ezzel befolyásolva a választók döntését. Szélsőséges ideológiák mentén működő radikális közösségek részéről szinte reflexszerű a gyűlölt csoportok közismert tagjainak negatív átszínezése vagy társadalmi kontrollintézmények képviselőjének démonizálása a társadalom többi tagja előtt.
- *Ma Zhichun* nincs még 40 éves, Kínában él, újságírásból diplomázott, és a munkája „internetkommentelő". E beosztásában Siquan város Propaganda Hivatalának dolgozik, és naphosszat kommenteket és posztokat helyez el különböző online közösségi felületeken azért, hogy pozitívan befolyásolja a pártról kialakított közvélekedést (SUQIAN 2005). A fizetett online kommentelők gyakorlata – akik a fogyasztói preferenciák mellett akár a politikai döntéseket is befolyásolhatják – tehát nem új keletű. Legutóbb például az Amerikai Egyesült Államok elnökválasztási kampányát alakító bérkommentelőkről hallhattunk 2016-ban (PERROTT 2016).
- A virtuális karaktergyilkosság kétféleképp történhet:
  – Rendszerintegritás elleni támadással. Ebben az esetben az egyén információs rendszeréből adatokat szereznek meg, módosítanak, vagy oda adatokat

juttatnak be (például a célszemély levelezőrendszeréből megszerzik az adatait, és azokat módosítva az áldozatot lejáratják).
  - A nyilvánosság befolyásolásával – rendszerintegritás elleni cselekmények nélkül – becsületcsorbító, valótlan tények, kifejezések vagy önbecsülést sértő koholt hírek terjesztésével. A karaktergyilkosságok hátterében legtöbbször az irigység, a féltékenység, a bosszú vagy a gyűlölet áll. A karaktergyilkosság e módozata nagyon szoros összefüggésben áll a haszonszerzési szükségletekre épülő motivációkkal is: azzal, amikor valaki a karaktergyilkosság technikai vagy más műveleteit anyagi haszon reményében hajtja végre.
- A személyközi kapcsolatok megzavarására, a bosszúságkeltésre, provokációra vagy bántó kritikai véleményformálásra irányuló cselekvés, amelynek modern kifejezője a *trollkodás.* Csepeli György szerint a troll „az online közegben az eltorzult én ideáltípusa". A trollkodás olykor olyan játék, amelynek motiváló ereje az uralomvágy, az agresszivitás és hiperaktivitás hátterében frusztráció és kielégületlenség húzódik (Csepeli 2014, 366.). A trollkodás destruktív eredménye manifesztálódhat rendszerfeltörésben, aktív kommunikációban vagy nyílt tartalomközlésben. Gyakran humoros, időnként jogi normát sértő cselekvések összessége, kapcsolódik az önérvényesítő agresszió által motivált magatartásokhoz, legnépszerűbb eszköze az internetes mém. A karaktergyilkosság és a trollkodás nem feltétlenül jár együtt kontrollintézmény reakciójával, nagyon gyakran a társadalmi elítélés szintjén megreked, erkölcsi és szokásnormát sért.
- A károkozásnak egy további formája is elterjedt, amely *a virtuális játékok szereplőinek céltudatos megsemmisítését* jelenti. A normasértés célkeresztjében az internetes hálózatokon működő stratégiai játékok grafikus eszközökkel megformált hősei vagy virtuális birodalmai és ahhoz tartozó eszközök és tárgyak állnak, amelyeket a hagyományos színtéren a játékos hónapokig tartó játékidő alatt, sok energiával és anyagi ráfordítással épített fel. Jogi normát sértő szerepgyilkosság akkor valósul meg, ha a virtuális szereplőket a játékos információs rendszerének megsértését követően semmisítik meg, nem a játékszabályok betartásával történő korrekt játék közben.

A közösségekkel szemben megvalósuló normasértések közé sorolhatók a vállalatok, szolgáltatók elleni támadások különböző formái. A profitorientált, piaci előnnyel rendelkező multinacionális vállalatok vagy információs szolgáltatók ellen indított hitelrontó, lejáratómű veletek hátterében globális méretű gazdasági vagy más hatalmi érdek, szervezett bűnözői közösségek manipulációja áll (például fizetési tranzakciók befolyásolása). Néha a motivációk láncolatban fonódnak össze, vagyis a vállalatok információs rendszerének megsértését, az adatok jogtalan kezelését vagy azokkal való visszaélést fizetett számítástechnikai szakemberek közössége hajtja végre, gazdasági vagy más hatalmi szereplők megrendelésére. A hackerek az erőfitogtatáson és az önérvényesítési késztetéseiken túl feltörhetnek egy vállalati rendszert akkor is, ha annak működése ütközik életszemléletükkel, világnézetükkel vagy más meggyőződésükkel. A mai napig működő legnagyobb hackercsoportok számos ilyen vállalat és szolgáltató információs rendszerét blokkolták csupán azért, mert üzleti módszerei nem egyeztek a hackercsoport igazságérzetével és rendszerellenes nézeteivel.

2010-ben például az Anonymus hackercsoport tiltakozott a Paypal, a Visa és a Mastercard szolgáltatóinak a Wikileaks ellentmondásos tevékenységét támogató, számlákat befagyasztó megmozdulása ellen azzal, hogy az említett bankok, illetve online fizetőalkalmazások honlapjait és elektronikus rendszerét bosszúból napokra megbénította (HAMPSON 2012).

14. táblázat

Károkozó destruktív cselekvésekkel megvalósított normasértések szintjei a cybertérben

Normasértés szintje	Károkozó destruktív cselekvések
Nem normasértő	• Humoros, egyéni vagy kollektív kritikai megfogalmazások, amelyek egyes esetben kellemetlen, nem kívánt hatásúak, de nem minősülnek normasértőnek.
Erkölcsi normát, szokásjogot sértő	• Szándékos, önbecsülést sértő, de jogi normahatárokat nem sértő megnyilvánulások.
Jogi normát sértő	• Rendszerintegritást sértő magatartások, • becsületcsorbító tények, kifejezések használata, manipulatív befolyásolás, anyagi vagy erkölcsi károkozás rendszerintegritás megsértésével vagy anélkül.

Forrás: Kiss Tibor szerkesztése

2.5.9. Információs rendszerek megsértése

A rendszerintegritás elleni magatartások a modern informatikai bűnözés meghatározó részét képezik. A normasértések tárgyaként szereplő információs rendszerek megsértése és az azokban tárolt adatok jogtalan kezelése már önmagukban jogi normát sértő cselekvések, amiről a büntető törvénykönyv *információs rendszer és adatok elleni bűncselekményként* rendelkezik. Az információs rendszer fogalmát a büntető törvénykönyv értelmező rendelkezései között találjuk: „az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége."[29] Az információs rendszerek köre a lakossági használatú infokommunikációs és számítástechnikai eszközökből álló rendszerektől a lakosság ellátása szempontjából kiemelkedően fontos infrastruktúrákat támogató rendszerekig terjed. Legnagyobb részük valamilyen úton kapcsolódik az internethez, így könnyen elérhetők és sebezhetők elektronikus úton. A bejutás gyakran bonyolult technikai megoldásokkal, olykor a felhasználó befolyásolásával történik (például *social engineering*), és azt jelenti, hogy a behatoló jogtalanul szerez hozzáférést, és ugyanazokkal a jogosultságokkal tevékenykedhet a rendszereken belül, mint annak tulajdonosa vagy üzemeltetője. A jogosultság megszerzésével adatokat módosítanak, törölnek, de előfordul, hogy a rendszer használati jogosultságának megszerzése és az ezért járó dicsőség elnyerése a cél.

[29] Btk. 459. § (1) bekezdés 15. pont.

Az információs rendszerek megsértése és a jogtalan adatkezelés nagyon sokféle motivációból eredeztethető, és számos célja lehet. Egyes esetekben a jogosultságot a már korábban említett automatizált eszközökkel *(malware-ekkel)* közvetett módon vagy az egyén megtévesztésével közvetlenül szerzik meg, nem egyszer csak az automatizált eszközök végzik a műveleteket a rendszereken belül. A jogtalan bejutást és károkozást általában a számítástechnikai ismeretekkel rendelkező szakemberekhez, felhasználókhoz kötik, akiket a köznyelv hackereknek nevez. A rendszerintegritás elleni normasértések az összes cyberdevianciával összefonódhatnak, és többségében jogi normasértésként zárulnak. A rendszersértő műveletek felhasználói szintű ismereteknél magasabb számítástechnikai kompetencia meglétéhez kötöttek. A technikai műveletekre épülő rendszersértés alapvetően a cybertér *eredmény- és színtérmódozatában* zajlik, személyes érintkezés útján történő befolyásolással, megtévesztéssel együtt egy eseményláncolatban a cybertér *eredménymódozatába* illeszthető. Az információs rendszerek megsértése akkor nem normasértő, ha hibák kiszűrésére, rendszertesztelésre irányuló legális cselekvés[30] vagy a rendszersértéshez magasabb társadalmi érdek fűződik, mint amekkorát sért az azzal okozott kár (például hatóságok tevékenysége, veszélyelhárítás).

15. táblázat

Információs rendszer megsértésével megvalósított normasértések szintjei a cybertérben

Normasértés szintje	Információs rendszer és adatok megsértése
Nem normasértő	• Legális úton történő rendszertesztelés, hibakeresés esetén, illetve a rendszerfeltörés által okozott kárnál magasabb társadalmi érdekből.
Erkölcsi normát, szokásjogot sértő	–
Jogi normát sértő	• Minden esetben jogsértő, ha nem legális körülmények közt, vagy nem magasabb társadalmi érdekből történik.

Forrás: Kiss Tibor szerkesztése

2.5.10. Extrémizmus és terrorizmus a cybertérben

A szélsőséges közösségek és 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 tevékenységeinek egy formája a cyberterrorizmus, vagyis olyan agresszív cselekedetek láncolata, amely a cybertér infrastruktúrái mentén valósul meg, és min-

[30] A tevékenység olyan számítástechnikai szakemberekre vonatkozik, akik egy-egy információs rendszer megsértését a rendszer tulajdonosának megbízásából legálisan teljesítik. A legtöbb olyan vállalat vagy szolgáltató, amelynek működését információs rendszerek biztosítják, olyan szakembereket alkalmaz, akik a rendszer tesztelésével annak gyenge pontjait kutatják fel, hogy azt később kijavítsák.

den esetben kárt okoz, vagy a károkozó magatartást készíti elő. A terrorszervezetek célja a cybertérben is a rettegés, a félelemkeltés, a gátlástalan erőszak alkalmazása a legnagyobb veszteség elérésével. Tevékenységeik legismertebb alakzata a jelentős infrastruktúrák működését és védelmét biztosító információs rendszerek befolyásolása, megbénítása. A terrorszervezetek műveleteit számítástechnikai szakértők vagy velük közreműködő egyének a világ bármely pontjáról képesek végrehajtani automatizált eszközökkel (programalapú vírusok, terheléses támadások), vagy más módon *(social engineeringgel)*. A világháló a 21. század egyik legveszélyesebb kriminális jelenségének *a látens együttműködésben, a hálózatos terjeszkedésben, szervezésben, koordinációban és a toborzás lehetőségében* kedvez leginkább. Több egységként egy célból azonnal mozgósítható csoportok instrumentális tevékenysége sokáig titkosan zajlik, majd egy egész társadalom elleni raptorszerű támadásban végződik, a célközösség minden tagjának közvetve vagy közvetlenül kárt okozva. A terrorszervezetek mindig az agresszió által motivált kulturális ideológiákra hivatkozva viszik véghez terveiket, tekintet nélkül a lebukás kockázatára.

A cyberműveletek gyakran előkészítői a hagyományos terrorcselekményeknek, vagyis a kapcsolattartás, az irányítás, a szervezés optimális eszközei. Napjainkban a kivétel nélkül minden társadalmat érintő cyberterrorizmus olyan deviancia, amely univerzálisan normasértő és mindenhol elítélt. A terrorszervezetekhez céljában hasonló, ám szervezettségében és hatékonyságában eltérő a szélsőséges meggyőződésű (például rasszista, antiszemita, homofób) csoportok működése. Tagjai egységben egy társadalmon belüli közösséggel szemben tevékenykednek. Kollektív cselekedeteiket negatív attitűdjeik táplálják, megnyilvánulásaikra a köztudatban gyűlölet-bűncselekmények terminológiáját használják. A cybertér társas platformjain vagy az általuk működtetett weboldalakon becsület csorbítására, közösség elleni gyűlöletkeltésre, uszításra utaló tartalmakat tesznek közzé, vagy ebbéli érzületek mentén kommunikálnak. Több szélsőséges csoport egy közös cél eléréséért virtuális szerveződést követően képes hagyományos színtéren egy nagyobb közösséggé formálódni és fizikai erőszakot alkalmazni. A cybertérben működő terrorszervezetek és a szélsőséges közösségek közt sok hasonlóság van, de a legszembetűnőbb *a hosszú távú együttműködés, a toborzás, a mozgósíthatóság, az ideologizálás és az erőszak alkalmazása.* Az extrém közösségek interakciói nem minden esetben váltják ki a kontrollintézmények reakcióját, ami csak annak kérdése, hogy átlépi-e a jogsértő határokat. Egy etnikai kisebbségről közzétett tartalomban lehetnek olyan negatív attitűdöket tartalmazó elemek, amelyek közvetlenül nem tűnnek gyűlöletkeltőnek vagy önbecsülést sértőnek, de mégis hangulatkeltők.

16. táblázat

Extrémizmussal és terrorizmussal megvalósuló normasértések szintjei a cybertérben

Normasértés szintje	**Extrém közösségek tevékenységei**	**Terrorszervezetek tevékenységei**
Nem normasértő	–	–
Erkölcsi normát, szokásjogot sértő	• Jogi normát nem sértő negatív tartalomközlés és kommunikáció.	–
Jogi normát sértő	• Jogi normát sértő tartalom (önbecsülést sértő, becsületcsorbító, gyűlöletkeltő, diszkriminatív).	Minden formája.

Forrás: Kiss Tibor szerkesztése

2.6. Cyberdevianciák és szereplőik a devianciaelméletek tükrében

2.6.1. A felhasználók mint potenciális elkövetők és áldozatok

Az internet által hozott társadalmi, kulturális, gazdasági és politikai változást sokan sokféle fogalommal illetik, mint amilyen például az „információs társadalom", az „információ kora", a „virtuális társadalom", a „posztindusztriális társadalom", a „tudástársadalom", a „hálózati társadalom" (Yar 2016). Az infokommunikációs technológiák (IKT) transzformatív ereje újrakonfigurálja az emberi cselekvéseket és interakciókat, ezzel egy olyan társadalmi rendet teremtve, amely az előzőekhez képest teljesen új elemeket is hordoz. A kriminológiai elméletek az IKT korában másként működnek: mind a normaszegés, mind annak mintázata és gyakorisága megváltozott.

Az internetfelhasználók mint lehetséges normaszegők – deviánsok vagy bűnelkövetők – és mint speciális áldozati csoportok is megjelennek. A felhasználók potenciális résztvevői a cyberdevianciáknak, mivel önként közzéteszik személyes adataikat, így növelik a lehetséges visszaélések számát, valamint hajlamosabbak kipróbálni a hagyományos térben nem szokásos tevékenységeket.

A bűnözés mint a deviancia térbeli átmenetének elmélete *(space transition theory of cyber crimes)* Karuppannan Jaishankar nevéhez fűződik (Jaishankar 2008). Az emberek cybertérben megváltozó magatartását az opportunista bűnözéselméletekkel rokon módon az anonimitással, a láthatatlanság érzetével magyarázza, amely egyéb körülményekkel együttállva vezet normaszegéshez. Ilyen körülmény például a személyiség: bizonyos, elnyomott kriminális személyiségjegyekkel rendelkező emberek hajlamosabbak a bűnelkövetésre. Mivel a cybertérben láthatatlanok, tehát nincs meg a normakövetéstől elrettentő faktor, itt könnyen előbújnak, és ennek a belső személyiségi jellemzőnek engedelmeskednek. Habár az anonimitás a „látható világban" már azonosított bűnelkövetővé válási faktor, az online térben hatása fokozottan érvényesül. Éppen ezért a kriminogén személyiségjegyeket hordozó egyének az online térben még inkább hajlamosak a bűnelkövetésre. Ebben az értelemben a bűnözés térbeli átmenetének elmélete a rutincselekvés-elmélet fő elemeinek a cybertérre való adaptálása (Jaishankar 2008).

A Suler által leírt online gáltásfeloldó hatás (Suler 2004) abban ragadható meg, hogy az emberek, ha nem kell megmutatniuk az arcukat, és ha tetteikért nem kell vagy legalábbis nem azonnal kell felelősséget vállalniuk, inkább mondanak vagy tesznek olyasmit, amivel másokat megbántanak. Agustina egyenesen online skizofréniának nevezi a kettős – a valós és a virtuális világban is aktív – életet élők viselkedését (Agustina 2012). A cybertér gátlásfeloldó hatása hat elemből tevődik össze. Az első az *anonimitás,* amely lehet valós vagy képzelt – minthogy minden online tettünknek digitális nyoma van (Furnell 2002). A második alkotóelem *a láthatatlanság:* nem egyszerűen név nélkül teszünk-veszünk az online térben, hanem titokban. Így léphetünk be egy chatszobába, vagy látogathatunk el olyan weboldalakra, ahová egyébként a látogatót megbélyegző szégyenteljes stigma miatt talán soha nem tennénk be a lábunkat. A harmadik alkotóelem *az aszinkronicitás:* az online interakciók jellemzője, hogy a címzett válaszadása, reagálása nem mindig azonnal történik. Érzelmileg túlfűtött, hosztilis üzeneteket küldhetünk annak, aki megsértett minket, azaz emocionális cserbenhagyásos gázolók lehetünk (Valkenburg–Peter 2011). További jellemző *az online kommunikáció szolipszisztikus énközpontúsága,* amely abból

adódik, hogy az üzenet küldője nem kap azonnali visszjelzést a címzettől, nem látja az arcát, nem lehet részese az általa generált érzelmeknek. A *disszociatív képzelet* egy további attribútum: az online közösségekben képzeletben eltávolítjuk fizikai valónktól a virtuális személyiségünket, és úgy érezhetjük, hogy ez a „digitális én" *(digital self)* (TURKLE 2005) teljesen elkülönül. A végső elem *a státusz és az autoritás minimalizálása:* az interneten mindenki egyenlő, nem számít, hogy híresek vagyunk-e, és nem kell hűnek lennünk a valós énünkhöz tapadó szerephez sem. Ez nemcsak azt jelenti, hogy lerázhatjuk a társadalmi státuszból eredő felelősségünket, de azt is, hogy könnyen azonosulhatunk a többi, velünk egyenlő, digitális szereplővel (AGUSTINA 2015).

2.6.2. Tipikus áldozati csoportok

Lényeges kérdés, hogy vannak-e az *online áldozattá válásnak ismérvei.* Miért lesznek az érintettek áldozatokká, és melyek azok a körülmények, amelyek megóvnak az áldozatiságtól? E cím alatt tárgyaljuk az online áldozattá válás tipikus helyzeteit, azokat a „csapdákat", illetve közösségeket, amelyek az elővigyázatlan felhasználót könnyen magukba szippanthatják, emellett olyan helyzeteket teremtenek, amelyekben nemcsak célpontként, hanem támadóként is „kipróbálhatják" magunkat.

A kontinuitáshívők azt hirdetik, hogy az online közegben elkövetett bűncselekmények nem térnek el a hagyományos bűncselekményektől. Azt is hangsúlyozzák, hogy erre akkor fogunk rájönni, ha egyszer a jövőben minden cselekménynek köze lesz valamilyen módon – az elkövetés vagy az előkészület helyét, közvetlen vagy közvetett hatását illetően – az internethez. Szerintük az internetes bűnözés nem más, mint régi bor új hordóban (GRABOSKY 2001, 243.), és az ennek ellenkezőjét hirdetőket a „pszeudodistinkció" vádjával illetik (MCGUIRE 2007, 5.). Ehhez képest számos próbálkozás születik arra vonatkozóan, hogy a valós világra ráhúzott bűnözéselméleteket a cybervilágban is adaptálják. Hogy megragadjuk az online bűncselekmények áldozatává válás lényegét, tekintsük át a tárgyban született legfontosabb empirikus kutatásokat!

2.6.2.1. A gyermekek és a fiatalok mint áldozatok

A 2000-es években született generáció már teljesen a világhálóval átszőtt környezetben nőhet fel. Ez azt jelenti, hogy nincs számukra „internet előtti" idő, a netgeneráció életéhez hozzátartozik az online jelenlét a nap minden órájában. A korábban részletezett gátlástalanító hatás tehát a Z-generációt (TARI 2011) potenciális áldozati csoporttá teszi. A tinédzserek agyi plaszticitása nagy, gyorsan tanulnak, és – szemben az idősebbekkel – nem okoz gondot számukra a technikai újdonságok használatának elsajátítása. A fejlődéspszichológia szerint önállósodási folyamaton mennek keresztül, előszeretettel próbálják ki magukat új, kockázatos helyzetekben. Sokszor éppen az IKT-eszközök használata és az internet adta lehetőségekkel élés önmagában kockázatos – amilyen például az online ismerkedés. Ehhez járul a kortárscsoport erőteljes befolyása, a még kialakulatlan belső értékrend és az önkontroll alacsony szintje, de legalábbis fejletlensége (MARCUM 2011). Így a fiataloké az egyik szupervulnerábilis csoport.

A *cyberbullying* a fiatalokat veszélyezteti leginkább, mind áldozatai, mind elkövetői tipikusan a kortárscsoportból kerülnek ki. Kamaszkorban a kortárscsoport szerepe felerősödik, így az elszenvedett sérelem jelentősége is felértékelődik, rejtve marad, és feldolgozása sokszor elhúzódik. A *cyberbullying* a legtöbbször az áldozat külső testi jegyeit, testsúlyát, szexuális vagy intim viselkedését érinti. A köznyelvben a megfélemlítés *(bullying)* leírására használatos az erőszakoskodás, a kegyetlenkedés, a zsarnokoskodás, az elnyomás és a fenyegetéssel, erőszakkal való kényszerítés, a „terrorizálás". A *cybermegfélemlítés* eleme ezen felül a digitális térben, illetve a telekommunikációs eszközzel és csatornán való elkövetés, amely megvalósulhat például online közösségi oldal, chatszolgáltatás felhasználásával, de telefonon vagy okoseszközön verbális, szöveges vagy audiovizuális tartalom küldésével is (Hinduja–Patchin 2015, 11.). A kutatások szerint a fiatalok kortárscsoportjában előforduló cyberbullying-magatartások nemzetköziek és kultúrafüggetlenek, és a fiatal generáció frekventált közösségioldal-használatával, valamint a kortárscsoport jelentős szerepével függenek össze (Parti et al. 2014).

Az online abúzusok további dimenziója a gyermekek online szexuális kizsákmányolása. A világ figyelme az 1990-es években az online pedofília mint a szexuális kizsákmányolás egyik legelterjedtebb formája felé fordult. Ennek oka az volt, hogy a pornográf tartalmak megjelenésére, az anonim terjesztésre és felhasználásra terepet biztosító, az egyéni felhasználók között gyorsan terjedő internet új lehetőséget adott (Parti 2009). A Carnegie Mellon Egyetem kutatása szerint a korabeli interneten egyszerű véletlen módszerrel kiválasztott hírcsoportok *(newsgroups)* által letöltött tartalom 83,5 százaléka pornográf volt (Campbell 2015). A cselekmény aggasztó mértékére reflektáltak a jogalkotás nemzetközi szervezetei is: az Európa Tanács számítástechnikai bűnözésről szóló egyezménye a tartalombűncselekmények között nevesíti az online gyermekpornográfiát.[31] Kifejezetten a gyermekek szexuális kizsákmányolása ellen az Európa Tanács 2007-ben, az Európai Unió pedig 2011-ben fogadott el nemzetközi dokumentumot. Az Európa Tanács lanzarotei egyezménye a gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen (a továbbiakban: lanzarotei egyezmény)[32] előírja a tagállamoknak, hogy gondoskodjanak a gyermekkel (18. életévet be nem töltött személlyel) online kapcsolatot teremtő felnőttek ellen büntetőeljárás megindításának lehetővé tételéről, ha a kapcsolatfelvétel célja az (offline) szexuális kizsákmányolás (online *grooming*).[33] Az Európai Unió 2011/93/EU irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről[34] az Európai Unió egész területén harmonizálja a gyermekek szexuális kizsákmányolásával kapcsolatos jogalkotást. Említést érdemel az irányelvben a gyermekkel való, szexuális célzattal történő internetes kapcsolatfelvétel kriminalizálása, amely átveszi a lanzarotei egyezmény koncepcióját. A dokumentumok a tagállamok közötti bűnügyi célú adatátadást és kölcsönös segítségnyújtást is szabályozzák, megkönnyítve az online abúzusok esetén való felderítést, adatgyűjtést, nyomozati cselekmények elvégzését és a büntetőeljárás lefolytatását.

---

[31] Számítástechnikai bűnözésről szóló egyezmény, 9. cikk: Gyermekpornográfiával kapcsolatos bűncselekmények.

[32] Az Európa Tanács egyezménye a gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen. Lanzarote, 2007. 10. 25. CETS. 201. Magyarországon kihirdette a 2015. évi XCII. törvény.

[33] Lanzarotei egyezmény, 23. cikkely: Gyermekek rábírása szexuális jellegű tevékenységre.

[34] Megjelent az Európai Unió Hivatalos Lapjában: L 335., 2011.12.17.

2.6.2.2. A nők mint áldozatok

A nők áldozatul esésének fokozott kockázatát egyfelől a közösségi oldalakon tanúsított nagyobb aktivitással, másfelől pedig a szexuális visszaélési célzatú bűncselekmények áldozattá válási arányaival magyarázzák: a nők mindkét területen felülreprezentáltak. A Pew Research 2017-ben publikált felmérése szerint az amerikai nők 72, míg a férfiak csak 66 százaléka rendelkezik profillal legalább egy közösségi felületen. A közösségi platformok közül az instant személyes kommunikációt előnyben részesítő Facebook, az Instagram és a Pinterest felhasználói között nagyobb arányban szerepelnek nők, míg az inkább a szakmai kapcsolattartásra koncentráló LinkedIn a férfiak között népszerűbb. A Twitteren, amelyet a mai napig az online sajtóban megjelenő hírek rövid szöveggel ellátott továbbítására használnak, ugyanolyan arány jellemzi a női, mint a férfi felhasználókat (Pew Research 2017).

Snell és Englander főiskolás pszichológushallgatókat kérdezett meg arról, milyen típusú cyberbullying-magatartásoknak estek már áldozatul (SNELL–ENGLANDER 2010). A lányokat nagyobb arányban érte a rosszindulatú pletykaterjesztés és a rágalmazás (hazugságok terjesztése, rossz hírük keltése; 45 százalék szenvedte el), mint a fiúkat (30 százalék). Az egyedüli olyan cselekmény, amely mindkét nemet egyformán sújtotta, az a hamis profil készítése és a nevükben méltatlan üzenetek küldözgetése volt. Az is kiderült, hogy a szexuális tartalmú üzenetváltás csaknem teljes egészében azért következik be a lányoknál, mert erre vonatkozóan nyomást gyakoroltak rájuk – a vágyott vagy az elhagyott szexuális partnertől vagy éppen a közösségtől (ENGLANDER 2013). Az *anti-bullying* programokat fejlesztő és kutató Massachusetts Aggression Reduction Center[35] az alapítása óta minden évben megismétli az adatfelvételt, és hasonló arányokat mutat ki (ENGLANDER 2013).

Dressing és munkatársai szerint a szexuális zsarolás *(sextortion)* és a bosszúpornó *(revenge porn)* munkanéven futó szexuális tartalmú visszaélések elkövetőinek 70 százaléka férfi, 30 százaléka nő. Az áldozatok esetében ez az arány megfordul – az online szexuális visszaélésről beszámolók 80–90 százaléka nő és csak 10–20 százaléka férfi (DRESSING et al. 2014). Éppen ezért a szexuális tartalmú zsarolás és a bosszúpornó a nők elleni zaklatás formáinak tekintendők. Az online szexuális zsarolás keretében az elkövető általában már a birtokában lévő, intim részleteket is ábrázoló képi anyag nyilvánosságra hozatalával zsarolja a sértettet. A sértett az első szexképeket általában önként bocsátja a későbbi zsaroló rendelkezésére vagy egy intim érzelmi kapcsolat, vagy üzletkötés reményében – például, hogy az elkövető a videós szexszolgáltatásában állást ajánljon a sértettnek (WITTES et al. 2016). A *bosszúpornó* ehhez nagyon hasonló: az a cselekmény, amelynek során egy szakítás után a volt intim partner a birtokában lévő intim képeket az ábrázolt személy beleegyezése nélkül nagy nyilvánosság számára közzéteszi egy erre a célra létrehozott weboldalon. Az *online szexuális visszaélés* imént tárgyalt formái hazánkban a *becsületsértés,* a *visszaélés személyes adattal,* valamint a *zaklatás* tényállásait valósíthatják meg, és a sértett személyes bejelentésére indulhat büntetőeljárás.

Lehetséges, hogy az áldozatiságot nemcsak a *nem,* hanem a *kultúra* is befolyásolja. Halder és Jaishankar a női áldozatoknak az indiai közösségi oldalakon való felülreprezentáltságát mutatta ki a következő cselekményeket vizsgálva (HALDER–JAISHANKAR 2011, 305–307.).

[35] Massachusetts Aggression Reduction Center. Elérhető: www.marccenter.org (A letöltés dátuma: 2017. 11. 10.)

- verbális abúzus gyűlöletkifejező csoportok által – mind a közös üzenőfalon, mind pedig privát üzenetben főként nőket érő abúzus;
- rágalmazás vagy becsületsértés, amely az adott személy ellen irányul – Citron (2009), Halder és Jaishankar (2008) szerint a szakítás után jellemzi főként az önérzetében sértett férfi elkövetőt;
- zaklatás – a felhasználó falára vagy privát chatablakába folyamatos, zavaróan nagy mennyiségű vagy tartalmú posztolás;
- fotómontírozás *(morphing)* – az áldozat által posztolt kép egy részének egy másik testre montírozása, jellemzően pornográf felhanggal;
- obszcenitás – fotómontírozás azzal a céllal, hogy a szexuális tartalmú képet terjesszék, és alatta sértő, degradáló kommenteket helyezzenek el megszégyenítési céllal;
- klónozás – a felhasználó adataival hamis profil létrehozása, és annak nevében posztolás;
- megfélemlítés – félelemkeltő, obszcén üzenetek, fenyegetések küldése, posztolása;
- csoportból való kizárás – a felhasználót kizárják az online közösségből;
- cyberbullying (magyarázatát lásd korábban);
- kibeszélés – az áldozat titkainak, személyes információinak a beleegyezése nélküli megosztása;
- zsarolás – kifejezetten szexuális tartalmak megosztásával vagy fizikai bántalmazással való zsarolás, ha az áldozat nem küld további intim képeket;
- online családi erőszak – partner vagy volt partner által megvalósított bármilyen online visszaélési forma.

2.6.2.3. Az idősek mint áldozatok

Az idősek csoportja nemcsak a cybertérben, hanem azon kívül is vulnerábilis: társadalmilag izolált életet élnek, magányosak, ezért kiszolgáltatottak az érzelmeiknek, és bizalmuk könnyen megszerezhető. Korcsoportjukban nem ritka a demencia és a rossz emlékezőképesség. Az online bűnelkövetők ezeket a tulajdonságokat használják ki áldozataik kiválasztásánál. A banki és hitelkártyaadatok könnyen megszerezhetők a postaládából vagy a szemetesbe kidobott levelekből – az adathalászatnak ez a korai típusa a szeméthalászat *(dumpster diving)*. Bevett szokás, hogy *phishing* e-mailt küldenek az áldozatnak. A levél hivatalosnak tűnik, de átvezet egy hamis weboldalra, amelyen a felhasználónak meg kell adnia a belépési adatait. Lehetséges, hogy valamely jótékonysági célú telefonhívást kap az idős személy, aki a megadott, az elkövető által létrehozott bankszámlaszámra átutalja a szóban forgó összeget. Előfordul, hogy az idős személy az éjszaka közepén telefonhívást kap, és a bejelentkező az unokájának adja ki magát azzal, hogy bajban van, és csak tőle mer pénzt kérni. A sértett pénze a valódi unokához soha nem érkezik meg. Hasonló megkeresést küldhetnek a bűnelkövetők valamely online közösségi felületen keresztül, így még a hang alapján történő felismerés veszélye sem áll fenn.

A cybertér által kifejlesztett és a cyberdeviancia-diskurzusnak speciális áldozati csoportként gyakorta tárgyát képező életkori, gender-, társadalmi, etnikai csoportok és szubkultúrák

bemutatását követően a már ismert elméletekkel és cyberkörnyezetben folytatott kutatásokkal elkövetői, normasértői oldalról is megközelítjük a deviáns magatartások különböző megjelenési formáit és legismertebb mintázatait.

2.6.3. A deviáns szubkultúra elemei az online közösségekben

A szubkultúra klasszikus értelemben a társadalmon belül kialakuló és annak részeként definiálható közösség, amelynek normarendszere eltér a társadalmi többségétől. Kialakulásának hátterében olyan társadalmi jelenségek emelhetők ki, mint a modernizáció, a népvándorlás, a társadalmi címkézés vagy épp a szegénység. Egyes megfogalmazások szerint a kulturális pluralizmussal megjelenő különböző szubkultúrák egyfajta válaszként alakultak ki a társadalomban létrejövő speciális problémákra, amelyekkel a többségi társadalom tagjainak nem kellett szembenézniük (ROSTA 2007, 144.). A szubkultúrák tagjai nem a többségi társadalom normarendszere, hanem kisebb közösségük értékrendszere mentén értelmezik önmagukat. A közösség a biztonságot, a valahová tartozás érzését, az önmegvalósítás lehetőségét és a kollektív felelősséget teremti meg tagjai számára. Sajátosan megformált szabályrendszer alapján szubkulturális magatartási mintázatot vár el tagjaitól, ami egy eltérő életformát eredményez, és nem feltétlenül negatív hatású a domináns társadalomra nézve. Ennek feltétele a többségi társadalmi normák elismerése és nem a szándékos aktív ellenállás. A szubkultúrák lehetnek akár vallási, nemzeti, etnikai alapon szerveződő közösségek, amelyek optimális működése inkább értékessé, mintsem hátrányossá teszi a társadalmi közösségek együttélését. Ezzel szemben a deviáns szubkultúrák káros hatással vannak a társadalmi integritásra. A kriminológusok és a szociológusok már közel egy évszázaddal ezelőtt is vizsgálták a deviáns szubkultúrákat létrehozó bűnelkövető bandákat, főként az Amerikai Egyesült Államokban.[36]

A vizsgálatok azokra a bűnelkövető csoportokra és dezorganizálódott területekre fókuszáltak, amelyek koruk sajátjaként alakultak és működtek. A deviáns szubkultúra főbb meghatározottságait a bűnözés tanulásában, a mertoni feszültségelméleten alapuló státuszfrusztrációban, a társadalmi kontroll hiányában, a bűnelkövetés eszközeihez való hozzáférés és a lakóterület adta lehetőségekben vagy épp a csoport sajátos szellemiségének elemeiben látták. A bűnöző bandákról eddig alaposan összegyűjtött ismeret a modern bűnözés kriminológiai kutatásainak, köztük a cybertérben működő közösségek etiológiai vizsgálatainak is jól alkalmazható alapjai.

A cybertérben szabadon létrejövő csoportok sokféleképp értelmezhetik önmagukat, ezért szinte elkerülhetetlen, hogy a domináns társadalmi normákkal szöges ellentétben álló deviáns csoportok is a virtuális tér részét képezzék. Napjainkra a cybertérben kialakuló közösségek normasértéseinek esszenciális tulajdonsága, hogy mindkét színtérre kiterjedhetnek, rendszerintegritás elleni vagy tartalmakkal összefüggő magatartásformákban is megjelenhetnek. A közösségek különféle motivációk köré csoportosulnak, céljuk, összetételük és működésük szempontjából eltérő struktúrákat alkotnak. Lehetnek hosszú

[36] A mai napig meghatározó kriminológiai vizsgálatok kiemelkedő teoretikusai voltak Frederick M. Thrasher, Edwin H. Sutherland, Albert Cohen, Richard Cloward, Lloyd Ohlin, Robert E. Park, Ernest Burgess, Clifford Shaw és Henry McKay.

távon (éveken keresztül tartó, folyamatosan reprodukálódó) és rövid távon együttműködő csoportok; ezekhez eltérő súlyú és megítélésű normasértések társíthatók. A *deviáns szubkultúra* elméletei viszont olyan virtuális szerveződésekben értelmezhetők, ahol a nem kívánt cselekvés valamely elfogadott magatartásminta része, érvényesülnek továbbá az ismeretek átszármaztatásán alapuló sajátos értékek és a normarendszer hatásai is. Egy csoport akár szeparáltan és nyilvánosan is működhet bárki számára elérhető formában, amiből az következik, hogy egy csoportnak eltérő kultúrából, társadalmi közösségből származó tagjai is lehetnek. A virtuális egyesülésekben az egyén a csoport szellemiségével és céljaival azonosulva működik, információkat oszt meg, küld, fogad és dolgoz fel, vagyis a csoport céljaitól függően egy tanulási és tanítási folyamat része. *Azokat a cybertérben létrejövő csoportokat, amelyek tagjai egységesen vallanak olyan szemléletet, amely a társadalmi normákkal szemben áll és életmódjuk része, virtuális deviáns közösségeknek vagy virtuális deviáns szubkultúráknak is nevezhetnénk.* A cybertérben formálódó deviáns közösségekre napjainkban az is jellemző, hogy működésük egyszerre az online és az offline színtérre is kiterjed. Az ilyen közösségek cselekvései az erőszakos magatartásokkal szoros kapcsolatban állnak, talán a legjobb példa erre a közösségi zaklatók, a futballszurkolók, a szélsőséges csoportok vagy a terrorszervezetek kettős működése (például toborzás és kommunikáció a virtuális környezetben, erőszak alkalmazása az offline terepen).

A szubkultúrára vagy deviáns szubkultúrára jellemző egyedi közösségi értékek, amelyek a normától eltérő viselkedésminták kiformálódását támogatják, és tisztán a cybertérben maradnak, elsősorban a hackerközösségeket határozzák meg. A hackerek tevékenységének deviánssá minősítése mellett számos érv és ellenérv szól, egyesek hasznos közösségként, mások deviáns szubkultúraként tartják számon formációikat, és működésüket is negatív sztereotípiákhoz igazítják. Egyesek szerint a hackerkultúra annyira összefonódik a számítástechnikai devianciákkal, hogy azoknak csaknem szinonimájává vált. A *hacking* azonban nem egyszerűen kártékony szoftverek előállítását, weboldalak összeomlásáért felelős tevékenységet jelent. Bernhard Lieberman a kutatásában például azt támasztotta alá, hogy néhány tényezőt kivéve egyáltalán nem mutatható ki szélsőséges eltérés a „hétköznapi" egyén és a hacker személyiségjellemzői közt. Nézőpontja szerint megcáfolható az a hiedelem, hogy a hackerek magányosak, vagyis annak ellenére, hogy egyedül tevékenykednek, és fizikai kapcsolataik lehetnek szegényesek, a virtuális lét bőven nyújt lehetőséget a társas lét szükségleteinek kielégítésére. Az általa megkérdezett hackerek többsége valós párkapcsolattal rendelkezett, és a szexuális életük sem volt szélsőségesen elhanyagolt. A károkozó magatartásuk is annak függvénye, hogy betartják-e a hackerközösségek íratlan szabályait, vagy engednek a könnyű haszonszerzési lehetőségek csábításának, ami egyébként a hagyományos elméletek alapján minden ember számára adott.

Lieberman két szélsőséges motivációt állított fel a hackerek körében. Az egyik az alacsony szintű, amely törvényszegő viselkedésre ösztönző, a másik a magas szintű motiváció, amely a szellemi kihívást és a számítástechnikai ismeretek elsajátításának vágyát támogatja. Megállapításainak a sztereotípiákkal egyező része a magas intelligencia, a külső ápolatlanság, a túlzott soványság vagy elhízottság, a fizikai környezet elhanyagoltsága – ami otthonukon kívül, munkahelyi környezetükre is igaz. A kutatás érdekes következtetése, hogy azok a hackerek, akik önszorgalomból sajátították el a technikai ismereteket szabad környezetben, elkötelezettebbek és motiváltabbak, mint azok, akik ugyanezt iskolai keretek között tanulták meg (Fötinger–Ziegler 2004, 9–17.). Valójában a sokféle megközelítés

mindegyike valós tapasztalatokon alapul, ugyanis a hackerek között működnek olyanok, akik normasértő magatartások elkövetésére specializálódtak, a legegyszerűbb rendszersértésektől a legnagyobb kárt okozó bűncselekményekig. A hackerek az ismereteiket – akár károkozó, akár hasznos cél érdekében – egy sajátos tanulási folyamat során származtatják át, zárt közösségben.

A *filmekben* a hackerek szubkultúrája autonóm, vakmerő, kreatív, okos, önfejlesztő, versengő.[37] A popkultúra teremtette imázs szerint a hackerek összetett számítástechnikai problémákat oldanak meg. A korai hackerfilmek szerint zárt közösségükbe való belépést valamely szigorúan védett rendszerbe való sikeres behatolással nyerhetünk, technikai úton vagy elővigyázatlan dolgozók megtévesztésével (MITNICK–SIMON 2003). A róluk szóló korai, pozitív hangvételű tudományos irodalmak szerint a cybertér építői, rendszerek és programok alkotói, fejlesztői és védelmezői. A számítástechnikai szakemberekből és magas digitális kompetenciával rendelkező felhasználókból álló közösségek tagjait az új kihívások motiválják, valamint a legmagasabb kompetencia elsajátítására való igény, a folyamatos kitartó fegyelmezett tanulás jellemzi őket. A hackerekről ugyanakkor olyan kutatási eredmények is születtek, amelyekben szubkulturális jellegük hangsúlyozásával együtt negatív tulajdonságaikat is kiemelik.

A kilencvenes évek végén készült szociológiai tanulmányokban a hackerekét olyan föld alatti közösségekként *(underground groups)* definiálták, amelyek tagjai ugyan különböző stílusban, de életük legnagyobb részét az információs és kommunikációs világban élik, és rejtett csatornákon működnek (JORDAN–TAYLOR 1998, 759.). A róluk szóló kutatások eredményei szerint a *technológiai érdeklődés,* a *titkosság,* az *anonimitás,* a *motiváció,* a *férfidominancia,* a *tagság és az új dolgok változékonysága* egységesen jellemzi a hackercsoportokat. A hat ismérv szubkultúrává alakító központi elemként is felfogható. A „technológiai érdeklődés" a számítástechnikai eszközök és rendszerek használatához fűződő szoros viszonyt fejezi ki, amely új utakat nyit a jövőbe, és alkalmas lehet új célok elérésére. A technikai ismeretek megosztása és fejlesztése, a mindent átfogó innováció a hackerek szabad képzelőerejének köszönhető. A „titkosság" a közösség tagjainak titkos működését és a tagok közti kommunikáció elérhetetlenségét jelenti, ami hűen kifejezi a hatóságokkal szembeni távolságtartást és bizalmatlanságot. Olyan csatornákon kommunikálnak, ahova a belépéshez azonosítás szükséges, ezáltal elkerülhető a nem kívánt megfigyelés. Az elérhetetlenség mögött a lebukást jelentő szabad „hackerképzés" részletei és a normasértő trófeagyűjtést (rendszerfeltörést) bizonyító információk állnak. A közösségeken belüli megosztás hallgatólagosan elfogadott cselekvés, ezért a csatornák titkosítása társul a hackerek titoktartásával, ami az egymás iránti lojalitást tükrözi. A titkossággal és a titoktartással szoros kapcsolatban lévő anonimitás valójában a fantázianeveken történő nyilvános működést is magában foglalja. Olykor hátrahagyják virtuális névjegyüket – tájékoztatva ezzel a környezetet arról, hogy az eredmény az ő munkájukhoz fűződik. A „tagság változékonysága és az új dolgokra való fogékonyság" a hálózati közösségekben való dinamikus információáramlás és a folyamatos személyi változások követésének szükségességére utal, a kötelező naprakészséget jelenti. A „férfidominancia" a férfiak szocializációjában a számítástechnikai ismeretek hangsúlyosabb oktatásával áll összefüggésben, a közösségeken belül a nőket elriasztó sze-

[37] A hackerekről szóló filmek bizonyos szempontból összeállított gyűjteményét lásd például az IMDB oldalán: www.imdb.com/list/ls055167700/ (A letöltés dátuma: 2017. 09. 03.)

xista és zaklató interakciókban nyilvánul meg. A hackerek szerint a számítástechnikával összefüggő tevékenység férfias hivatás, amelyben a nők sokkal inkább rendszereket építenek, és nem is értenek a rendszerek befolyásolásához. A szerzőpáros szerint szinte minden hackerre jellemző az *internetfüggőség,* a *kíváncsiság,* az *izgalom- vagy élménykeresés,* a *hackerközösség tagjainak pozitív visszajelzése,* a *pozitív társadalmi célzatú hackelés,* illetve a *nagyobb vonzerejű rendszerek megdöntésére és a hatalom megszerzésére irányuló vágy* (Jordan–Taylor 1998, 763–769.).

Jordan és Taylor meghatározásán túl Jakub Lickiewicz vizsgálata is – amelyhez McCrae és Costa ötfaktoros modelljét használta fel – sajátos működést feltételez. Az FFT-modellben *(five-factor theory)* eredetileg az emberi személyiségjegyek öt központi eleme szerepel: a barátságosság, a lelkiismeretesség, az újdonságra való nyitottság, az érzelmi stabilitás és az extrovertáltság. Az öt faktor olyan alapvető és általános tendencia meghatározó elemei, amely az emberi személyiség holisztikus felfogására alkalmas (McCrae–Costa 2004, 587–596.). McCrae és Costa modellje azonban nem magyarázza kellőképp a hackerközösségek normasértő magatartásait, ezért Lickiewicz a modell mentén a hackerek leggyakoribb személyiségjegyeiből egy faktorcsoportot állított fel. Modelljében az első elem *a magas intelligencia,* amely a logikai gondolkodás és a hatékony támadás szempontjából kiemelkedően fontos, de legalább átlagos intelligencia szükséges a műveletek eredményességéhez. A második elem a *specifikus személyiségjegy,* amelyhez az extraverzión és az intraverzión kívül a tapasztalatokat, az érzelmi stabilitást, az újdonságokra való nyitottságot, a barátságosságot és lelkiismeretet sorolta (vagyis McCrae és Costa modelljének öt elemét). Mindez a kreativitást, az új módszerek használatát, a hirtelen felmerülő probléma megoldását, a támadás szofisztikált módját és a befolyásolási technikákat alapozza meg (például *social engineering*). A harmadik elem a *szociális készségek* faktora, amely az egyik oldalról a hackerek csoportokban történő együttműködését hangsúlyozza, a másik oldalról hiányosságot fed fel, ugyanis a legtöbb szakirodalom alacsony szociális készségekről és az elidegenedésről szól. A negyedik *a magas technikai tudás,* amely szorosan kapcsolódik a programnyelvek ismeretéhez, a programozás, a hálózatok, a rendszerek és az adatbázisok készségszintű kezeléséhez. Ötödik elemként az *internetfüggőséget* emelte ki; ez az internet hálózatának, a számítástechnikai rendszerek és eszközök kényszeres, napi használatát jelenti – de nem minden esetben jellemző.

Lickiewicz szerint az általa definiált öt faktort két csoporttényező befolyásolja. Az *endogén* tényezők csoportja az egyén pszichológiai, biológiai meghatározottságait foglalja magában (például pszichikai jellemzők, szociális szorongás, trauma). Az *exogén* tényezők csoportjába pedig az egyén környezete és annak hatásai tartoznak (például család, iskola, társas kapcsolatok, munkahely). A két csoporttényező az öt elemmel együtt a hacker *motivációjára* van hatással (például unalom, gazdasági haszonszerzés, bosszú, kíváncsiság). A motiváció pedig hatást gyakorol a hacker *normasértő magatartására,* vagyis a támadás módjára, hatékonyságára és a virtuális helyszínen való viselkedésre (Lickiewicz 2011, 240–245.).

A deviáns hackerközösségek tagjainak individuális meghatározottságaira irányuló további kutatások az internetfüggőség következményeit az enyhe kábítószerfüggőség tüneteivel azonosították. A kutatók szerint az internetfüggő hackereknél hasonló viselkedési minták figyelhetők meg, mint a kábítószerfüggők esetében. A párhuzamosság nemcsak az elvonási tünetekben, hanem az egyén normasértő tevékenységekre való hajlamossága

és a környezet elhanyagolása szempontjából is kimutatható (YOUNG 2011). A pszichológiai elméletek közt olyan elképzelés is szerepel, hogy a hackeléssel megvalósuló normasértés alapvetően a *kényszermaszkulinitás* eredménye, ami a társadalom férfias viselkedésre vonatkozó elvárásából eredeztethető. A tizenéves fiúk a maszkulin viselkedésre vonatkozó társadalmi nyomás terhét a rendszerfeltörésekkel és dicsekvéssel enyhítik. Ezzel kiélik hatalomvágyukat, bizonyítják férfiasságukat, a másokon vagy a rendszereken való uralkodást és dominanciát. Ugyanezen elmélet megalkotói a túlzott férfidominanciát is hangsúlyozzák: hackerkörökben túlsúlyban vannak a szexista megnyilvánulások, jellemző a nőket megalázó és zaklató kommunikáció; ezek pedig elriasztják e közösségekből a nőket (YAR 2006, 24–31.).

Egy másik pszichológiai és szociológiai felmérés eredményei szerint az információs rendszereket sértő magatartások a *fiatalkori bűnözés* hozadékai. A tizenéves korosztály identitáskereső időszakában egyébként is valószínűbb a normasértő viselkedés, aminek könnyen lehet következménye a hackelés és az ezzel való károkozás. A *fejlődéspszichológiai* elméletek követői ehhez hozzáfűzik, hogy a fiatal felhasználó még nem érte el azt az erkölcsi fejlettségi szintet, hogy a morális szabályokat alkalmazni tudja, vagyis nem érett személyiség (YAR 2006, 37.). A fiatalkorúak válságos időszakán kívül a kutatók összefüggést látnak a hackelés mint normasértés és a fiatalkorú rossz családi háttere és iskolai környezete között. A destruktív szülő-gyermek kapcsolat, az elhanyagoló környezet, a szülői vagy az iskolai bántalmazás alakítja a fiatal társadalomellenes magatartását, ezért a hackeléssel és egyéb virtuális normasértésekkel kezdődik bűnözői karrierje (VERTON 2003; YAR 2006). Mások szerint a rendszerfeltörés és az ezzel okozott kár egyáltalán nem a patológiás személyiséggel és a családok deficites működésével rokonítható, ugyanis a hacker nagyon gyakran magas társadalmi státuszú, sikeres családban szocializálódik, mégis a normasértés mellett dönt, vagyis olyan tényezők állnak a háttérben, mint az élménykeresés, az unalom, a kihívás, a kíváncsiság vagy az önérvényesítés. A hackerműveletek hátterébe néhány kutató a frusztrációból eredő agressziót helyezi. A károkozó magatartás oka az általános stressz levezetésétől a társadalmi címkézés miatt érzett tehetetlenségen át a rendszerellenes szellemiségből fakadó ellenállásig sokféle lehet. A frusztrációból gyökerező rendszerfeltörések főként a *script kiddie-k (skiddie-k)* esetében gyakoriak, ahol egyenesen korosztályi attribútumként jelenik meg az agresszív feszültségek levezetése (CHIESA–DUCCI–CIAPPI 2009, 158.). A valóságban a fiatalkorú populáció az individuális diszpozíciói és a társadalmi környezet minősége szempontjából olyannyira heterogén közösséget alkot, hogy minden, itt bemutatott megközelítés magyarázatul szolgálhat, de csupán az egyiket vagy másikat nem célszerű minden fiatal hacker magatartására vonatkoztatni.

A tipológiák közül azok fejezik ki az adott közösség deviáns működését optimálisan, amelyek elkülönítik az egyént a tevékenységtől és a technikától, vagyis megkülönböztetik a technikai műveletek mögött a jó és a rossz szándékú hackereket. A csoportosítások egyike *a fehér-, a fekete- és a szürkekalapos* kategorizálás. A *fehérkalapos hackerek* műveletei legálisak, feladatuk a rendszerhibák kiszűrése, feltárása és javítása. A *feketekalapos hackerek* körébe azok tartoznak, akik magas számítástechnikai tudásukat szándékos károkozásra használják. Számos információs rendszer feltörését végzik el, a legtöbbször haszonszerzési célzatból, megrendelésre tevékenykednek. Az amatőr és a professzionális tudás ebben a kategóriában is a két szélsőséges pólust adja. Az egyik a számítástechnikai tudás professzionális szintjén álló hacker, a másik az amatőr, legtöbbször fiatalkorú *skiddie,*

aki inkább valamely agresszív cselekedet vagy élménykeresés által ösztönözve okoz kárt. A fehér- és a feketekalaposok közti csoport a *szürkekalapos hackerek* közössége, akik magukat semelyik közösséghez sem sorolják. A rendszerek feltörése gyakran jogellenes, cselekvésük hátterében álló izgalom, kihívás, kíváncsiság, az ellenálló szemlélet és ezzel együtt az agresszió is régóta fennálló meghatározottság. A tipizálás alátámasztja azt a vélekedést, miszerint a motivációk markáns elhatárolói lehetnek a cselekvés legális és illegális jellegének (Chiesa–Ducci–Ciappi 2009, 47.).

A hackerközösségek tevékenységét társadalomra veszélyességük szerint Marc Rogers négy csoportba sorolta. Az *old school hackerek* azok a magas számítástechnikai tudással rendelkező programozók, akik a hackerkultúra szabályai mentén jó szándékból tevékenykednek. Főként elemzési rendszerekkel, kódokkal foglalkoznak, az információs rendszereket inkább fejlesztik, mintsem rongálják: a rendszerek gyenge pontjaira mutatnak rá. A *cyberpunkok* csoportjába tartoznak azok, akiket hivatalosan is *crackereknek* neveznek. Ők azok a fiatalkorú felhasználók, akik a legtöbb kárt okozzák, miközben nem rendelkeznek magas számítástechnikai kompetenciával. Céljuk a rongálás és a rendszerek megzavarása, mindezt unalomból, élménykeresésből, a hírnév megszerzése és az önérvényesítés céljából teszik, és nyilvánosan büszkélkednek normasértéseikkel. A *számítástechnikai bűnelkövetők* már komoly tudással rendelkeznek, és magabiztosan befolyásolnak információs rendszereket, végeznek jogtalan adatkezelést anyagi vagy más ellenszolgáltatásért. A bűncselekményt általában megrendelésre végzik, vagy ha saját elhatározásból tevékenykednek, az adatokat az adatpiacon értékesítik. A számítástechnikai bűncselekmények legtöbb és legnagyobb kárt okozó alakzatait ők valósítják meg, gyakran szervezett bűnözői közösségek, terrorszervezetek tagjai vagy megbízottjai. Végül a *programozók és vírusírók* közösségébe azok tartoznak, akik a kártékony szoftvereket készítik. A megírt programok egyben a névjegyükként szolgálnak; ezeket saját rendszerükben tesztelik, majd értékesítik. A programozók és vírusírók által elkészített *malware-ekkel* képesek óriási méretű hálózatok megbénítására (Fötinger–Ziegler 2004, 5.).

A technika, illetve az informatikai bűnözés fejlődésével a hackerek szerepe is átalakult. A deviáns fiatalokból álló szubkultúra (Yar 2005) mára „felhígult" olyan szereplőkkel – szervezett bűnözői csoportok, hackereket felbérlő egyéni bűnelkövetők, állami, katonai szervezetek, biztonságtechnikai szolgáltatók, politikai rend ellen protestáló civilek, illetve terrorszervezetek –, akik a hacking technikáit felhasználva érvényesítik érdekeiket (Yar 2016). Ma már nem csupán a szubkultúrához tartozás a hackerek legfőbb motívuma, hanem a pénzszerzés – amely manifesztálódhat valamely nagy adattömeg vagy titkos információ megszerzésében, majd értékesítésében (CSI/FBI 2003). Lehetséges, hogy a megbízó éppen valamely üzleti szereplő, aki versenytársaitól próbál ilyen módon bizalmas adatokat megkaparintani (Eichenwald 1998).

A hackerek jellemzői között a kutatások eredményei szerint egységesen megtalálható a titkosság, a szoros kapcsolódás, az egymástól való tanulás, a zártság és a sajátos normarendszer, ami markánsan körvonalazza szubkulturális jellegű működésüket. A tipizálásokból az is kiderül, hogy egyes magatartásformák – mint a haszonszerző, bosszúálló, károkozó megnyilvánulások – a deviáns szubkultúrákhoz is illeszthetők.

2.6.4. Normasértések tanulása a cybertérben

A hackerközösségek szubkulturális tevékenységének magyarázatát a kriminológia és a szociológia legtöbbször a tanuláselméletekben találja meg. A hackerek tevékenységein kívül sok más, szintén a cybertérben megvalósuló normasértésre is ráilleszthető Edwin H. Sutherland *differenciális asszociáció elmélete*. Sutherland szerint az egyén a bűnözést a környezetében élő emberekkel történő érintkezésével egy tanulási folyamat nyomán sajátítja el, épp úgy, mint minden mást az élete során. A deviáns viselkedésminták készségszintű internalizálása attól függ, hogy az egyénnek a deviáns közösségekben sikerül-e szoros kapcsolatot kialakítania olyan személlyel vagy személyekkel, akitől a normasértések mechanizmusait, a normasértő attitűdöket, a neutralizációs technikákat megtanulhatja. A deviáns szerepkörrel való azonosulás sikere részben a tanuláshoz szükséges közvetlen kapcsolatoktól függ, illetve attól, hogy a közösségben túlsúlyba kerülnek-e a többségi társadalmi normákkal szemben álló magatartásminták – vagyis az eltérő nézetek (differenciális asszociációk). A normasértő közösségekbe való beilleszkedés további feltétele, hogy a deviáns cselekvés a közösségben pozitív megítélés alá essen, és az egyén el tudjon szigetelődni a többségi társadalom cselekvésmintáitól. A differenciális asszociáció elmélete arra mutat rá, hogy az egyén deviáns életformájának kialakulásában jelentős szerepe van a kulturális környezeti hatásoknak (SUTHERLAND–CRESSEY 1978).

Hackerközösségekben az ismeretek megosztása és a „hackeretika" betartása alapvető elvárás és egyben a közösségek fennmaradásának legfőbb garanciája. Az ismereteket a közösség tagjai utánzással, koncentrált gyakorlással származtatják át. Mindez nem csupán a műveletek és a neutralizációs technikák elsajátításából, hanem az életstílus átvételéből áll. A hackerek közt az egyik legfontosabb érték egymás elismerése és a folyamatos visszajelzés, ami lojalitással és szolidaritással párosul, így az autoriter struktúra a legkevésbé jellemzi körüket. A precizitás, a problémamegoldásra való érzékenység és a folyamatos érdeklődés a közösségben maradás egyik alapfeltétele, egyéni szinten tisztán a produktummal kívánják csoporttagságukat és státuszukat stabilizálni. A tanulás középponti tézis: az állandóan változó, bonyolult műveleteket egy sajátos kulturális közegben tanulják. Érintkezési felületeik a csevegőszobák, sajátos közösségi platformjaik és az offline konferenciák, ahol személyesen találkozhatnak, és megoszthatják tapasztalataikat (JORDAN–TAYLOR 1998; FÖTINGER–ZIEGLER 2004).

A folyamatos egymástól tanulás minden hackerközösség általános jellemzője. A tanulás folyamatán belül a sutherlandi elméletet igazolja a már korábban említett neutralizációs technikák alkalmazása is. Marc Rogers szerint a hackerek köreiben a rendszerek jogellenes, de jó szándékú megsértését a társadalom számára hasznos szolgáltatásnak tartják, a felelősségre vonás során pedig neutralizálnak (FÖTINGER–ZIEGLER 2004). A rendszersértő magatartást és az abból eredő kárt a rendszer fenntartójának gyenge védekezésére vagy hanyagságára vezetik vissza, vagyis az áldozat tagadása és elítélése és a társadalmi lojalitás hangsúlyozása a hackerközösségek sajátja, amit a szakirodalom *Robin Hood-szindrómának* nevez (YAR 2006, 56.).

A szoftverek vagy a szellemi termékek illegális használata annyira elterjedt a felhasználók köreiben, hogy a műveletek elsajátításának folyamata már szinte a digitális szocializáció része. A szellemi alkotások megosztását, letöltését, használatát az egyén nem feltétlenül egy elkülönült közösségben tanulja meg, hanem olyan társadalmi közegben, mint a család,

a baráti kör és az iskolai kortárscsoport. A szellemi termékekkel való visszaélés módja és az ezekhez fűződő technikai ismeretek elsajátítása a rendszerintegritás elleni magatartásoknál jóval egyszerűbb műveletek összessége, normasértő jellegükkel szemben a társadalom érdektelensége észlelhető. A tanulás olyan közegben zajlik, amelyben a jogellenes cselekvés megerősítése éppúgy fontos, mint a normasértő magatartásokkal szembeni morális gátak kizárása, a deviáns magatartás elkövetésében való szövetkezés. A tanulás akkor a legsikeresebb, ha az ismeretek átszármaztatásában és a megerősítésben a szülő is részt vesz (Gunter 2011, 175–179.).

Egy másik megközelítés a cyberdevianciák tanulásának magyarázatában a *modelltanulás elmélete*. Albert Bandura amerikai pszichológus szerint az emberi agresszió tanulás útján alakul ki, vagyis tapasztalatokon, ismereteken, szokásokon és az érzelmi élet szakaszain át. Empirikus kutatásaihoz a pszichológiában már ismert *operáns kondicionálás* elméletét vette alapul. Eszerint egy viselkedésformát az egyén a külső környezet pozitív vagy negatív visszajelzését követően egészen addig ismétel, míg meg nem tanulja. Az operáns kondicionálás folyamatában a pozitív megerősítés jutalmat, a negatív büntetést jelent, vagyis a külső környezet megerősítése meghatározó az egyén későbbi viselkedésében. Bandura szerint az agresszív viselkedés pozitív megerősítés útján tanulható leginkább, sőt így válhat személyes tulajdonságaink részévé. A pozitív megerősítés történhet a családban a szülők részéről, az iskolában a pedagógus helytelen pedagógiai módszere nyomán, kortársközösségben, baráti társaságban, esetleg erőszakos bandákban az erőszak elismerésével. Bandura a tanuláselméleteken belül kiemeli a *modelltanulást* vagy *utánzásos tanulást* (Bandura 1978). Az egyén megfigyeli és modellként látja az előtte zajló agresszív viselkedési mintákat, az azokhoz kapcsolódó pozitív megerősítést, és behelyettesíti magát a modell szerepébe, majd azokat utánozza, végül más környezetben is alkalmazza (Bandura 1965; Szabó 2016, 91.; Hárdi 2010, 73.). A virtuális tér alkalmas az elméletben levezetett magatartásformáló modelltanulásra, ami nem feltétlenül jelenti a negatív minták átvételét (lásd például viselkedési, öltözködési trendek átvétele).

A deviáns viselkedésformák modelltanulás útján való átszármaztatásának többféle formája létezik. Ezek közül talán a legmarkánsabbak az erőszakos cselekvéseket közvetítő internetes tartalmak *scriptjeinek* terjesztése, másolása, tanítása, illetve az online jelzőmozzanatok hatásai. Az online történt események sokak számára mintaértékűek, a felhasználó azokkal azonosul. Egyes kutatások eredményei szerint az erőszakos pornófilmek jelenetei *(scriptjei)* épülnek be a leggyorsabban az egyén viselkedési mintái közé. A szexuális aktusok erőszakos elemekkel vegyített jelenetei olyan modellek, amelyek destruktívabb formái perverz fantáziálásokban, internetes gyermek-felnőtt kapcsolatokban és fizikai cselekvésekben is megjelenhetnek (Gonsalves 2010, 16.). A scriptek modellként kezelése illeszkedik Bandura modelltanulás-elméletéhez, ami akkor optimális, ha közben az utánzó viselkedést jutalmazással erősítik (Bandura 1965). A pornóesemények olyan explicit tartalmak, amelyek önmagukban kívánatos viselkedést mutatnak be – ha csak a szereplők filmbéli reakcióit vesszük alapul –, ami pozitív jelentéstartalmat generál a felhasználóban. Ha a tartalomban észlelhető erőszak a felhasználó agresszív érzelmeivel szinkronban áll, vagy szexuális késztetéseit nem tudja megkülönböztetni agresszív feszültségeitől, akkor agresszivitását nagyobb eséllyel vegyíti a szexualitással, és az erőszakos pornójeleneteket valós kapcsolataiban is alkalmazni fogja.

A cybertérben megnyilvánuló szexuális erőszak további meghatározó magyarázata a szocializáció során kialakult sztereotípiák és a cybertérben észlelt erőszakos tartalmak kapcsolódása. Az erőszakos szexuális devianciákhoz kapcsolódó meghatározó sztereotípia a *nemi erőszak mítosza,* amely szerint az ilyen bánásmódot maguk az áldozatok, legtöbbször a nők igénylik. A nemi erőszak mítosza pont azokat a hiedelmeket oldja fel, amelyek a nemi erőszak elleni védelmet garantálják (BURT 1980). Az elmélet középpontjában álló nemierőszak-mítoszt a korábban már említett internetes pornográf scriptek erősítik fel, amelyek az internetes perverzió és az internetes szexuális erőszak formáinak mozgatórugói (MALAMUT–CHECK 1985; GONSALVES 2010). Az a felhasználó, akinek a hiedelmei közt szerepel a nők elleni erőszak alkalmazásának hasznossága és helyessége, valós kapcsolataiban is nagyobb eséllyel alkalmazza a scriptekből tanult erőszakos technikákat. Az erőszakos pornójeleneteknek ekképp komoly cselekvésmeghatározó erejük van, főleg az agresszív felhasználók körében (FISHER–BARAK 2001).

Az internetes pornófilmekhez hasonlóan a modelltanulás lényeges elemei az erőszakos viselkedést kiváltó agresszív jelzőmozzanatok. Ezeket hagyományos színtéren a fegyverek látványa vagy más emberi viselkedésből fakadó ingerek testesítik meg. A szociálpszichológusok szerint nagyobb eséllyel lesz valaki agresszív, ha a közelében erőszakot szimbolizáló tárgyak vannak, vagy ilyen ingereket észlel (SMITH–MACKIE–CLAYPOOL 2016). A számítógépes játékokban az ellenség elpusztítása helyes viselkedés, mint ahogy az online szélsőséges közösségekben az ellenséges megnyilvánulásokra ösztönző tartalmak sem elítélendők. Mindkét ingerforrás erőszakos magatartásra ösztönző jelzőmozzanatként értelmezhető, és ha a felhasználónak nincsenek mozgósítható belső vagy külső kontrolleszközei, nagyobb eséllyel gyakorolja a látott sémákat az egyes élethelyzetekben. Az erőszakos jelzőmozzanatok hatását sokan vizsgálták, egyes kutatások szerint a fantázia szülte erőszakos filmek és tartalmak képesek az egyén agresszióinak pozitív levezetésére azzal, hogy a felhasználó a meglévő feszültségeit a jelenetekkel párhuzamosan vezeti le. Az agresszió levezetésének elméletét taglaló Seymour Feshbach által felállított katarziselméletet (más néven *Feshbach-hipotézist*) sok kritika érte, és legalább annyi kutatás bizonyította, hogy ilyen tartalmak a legtöbbször nemhogy csökkentik, hanem növelik az agressziót. Abban viszont a kritikusok is egyetértettek, hogy a hipotézis nem mindenkor cáfolható, ugyanis az agresszió levezetése függ az erőszakos tartalmak nézőinek lelkivilágától továbbá, hogy az erőszakos műsor mennyire adaptálható a valós események folyamatába, és milyen mértékben illeszthető a valóságban alkalmazott konfliktuskezelésbe (VETRÓ 2010, 406–407.). Az erőszakos tartalmak és jelzőmozzanatok olyan kockázati tényezőként értelmezhetők, amelyek a felhasználó tartós és időleges diszpozícióitól (bizonytalanság, befolyásolhatóság, tapasztalatlanság) a tartalmak erőszakos jeleneteinek alkalmazhatóságával, szereplőinek mintaértékével állnak szoros összefüggésben (VETRÓ 2010, 408.).

2.6.5. Az internetes trendek mint a normasértés aktorai

A differenciális asszociáció elmélete és a modelltanulás elmélete megvalósulásának feltételei közül a cybertérben zajló interakciókra egységesen jellemző az *utánzás.* Gabriel Tarde francia kriminológus, szociológus 1895-ben alkotott társadalomtudományi elmélete szerint a társadalom a találmány és az utánzás tengelyében működik. A társadalomnak van

egy olyan szűk (elit) rétege, amelynek tagjai az új dolgokat feltalálják, és van a hiszékeny és befolyásolható többség (a nagy tömeg), akik az új dolgokat utánozzák. Minden, ami a társadalomban működik, egy szűk réteg által feltalált dolog, amely utánzás útján válik társadalmivá. Ahhoz, hogy valaki kreatív feltaláló legyen, fel kell emelkednie a tömegből az elit szűk közösségébe, el kell szakadnia attól a társadalomtól, amelynek tagjai kollektív hallucinációban szenvednek és hipnotizálhatók (Némedi 2005, 28.).

Az utánzás egyes tevékenységek, magatartási és viselkedési módok aktív megismétlése, a tanulás alapvető szükségessége, a kultúra terjedésének és fenntartásának alapvető feltétele (Fehér–Lappints 1999, 110.). Elemi elvárás, hogy a közösség tagja a normalitás keretein belül a társadalom többsége által normálisnak tartott viselkedési mintákat utánozza.

A virtuális teret bárki saját elképzelései szerint megtöltheti tartalommal, a világban zajló legapróbb események és trendek villámgyorsan eljuttathatók a felhasználók otthonaiba, megállíthatatlanul terjednek. A könyvek elmélyült olvasása, az elvont gondolkodás sokak számára már a múlté, sokkal inkább a rövid szövegek felületes átfutása, a mennyiségi hírfogyasztás a népszerű, aminek hozadéka, hogy a felhasználók jelentős része a megalapozott ismeretek gyűjtögetése helyett, forrásellenőrzés nélkül, reflexszerűen elfogadja a látott tartalmakat. A bővülő és frissülő információbázisok épp a felületes és mennyiségi hírfogyasztás igényét elégítik ki, és közben formálják a felhasználók többségének attitűdjeit, hiedelmeit, mítoszait és érzelmeit. Mindez merőben megváltoztatja az értékről és értékesről való gondolkodást és véleményformálást (Fábry 2013). A cselekvéseket közvetítő trendek követhetetlenül gyakran változnak, így mindig lesznek olyan lemaradók, akik a trendek dinamikus változásait értékválságnak vagy értékzavarnak élik meg, és lesznek, akik számára a normálistól eltérő magatartásminták követendő trendekké válnak – mint például a szexuális tartalmak posztolása, küldése és fogadása. A szexting a web 2.0-es kommunikáció kialakulásával vált igazán dinamikussá, népszerűsége az elmúlt tizenöt év intenzív virtuális működésének köszönhető, amelyet a társas oldalakon való önmegvalósítás határtalan szabadsága lendített fel. A *trendek akkor nevezhetők kockázatosnak, ha eszközeivé válnak valamely normasértő magatartásnak,* mint ahogy a szexting a cyberbullying és a zsarolás bevált eszköze. A trendek arra is alkalmasak, hogy a deviáns cselekvők a megfelelési kényszert használják fel a felhasználók megtévesztésére, befolyásolására.

A fiatal felhasználók körében a cybertérben megjelenő trendek utánzása – ha hallgatólagosan is, de – részben a kortársközösség nyomásgyakorlásának eredménye. A követendő trendek fókuszában álló tárgyak vagy cselekvések rövid idő alatt egy egész generáció szimbólumává emelkedhetnek, elérendő célként fogalmazódhatnak meg (például a veszélyes offline cselekvések teljesítése, vagyis a bátorságpróba).

A Blue Whale (Kék Bálna) egy orosz nyelvű online kezdeményezés volt 2017 elején, amelyen keresztül 10–14 éves fiatalokat környékeztek meg azzal a céllal, hogy önkárosító és öngyilkos késztetéseket ébresszenek bennük. Az online közösség lényege az volt, hogy a hozzá csatlakozó tinédzserek 50 napon keresztül feladatokat kaptak, az utolsó 10 napban pedig éjjel is felkeltette őket egy adminisztrátor azért, hogy gondolkodjanak el a halálról. A feladatok között szerepelt, hogy egy kékbálna-tetoválást kellett csináltatniuk, majd az utolsó reggel öngyilkosságot kellett elkövetniük. Arra az esetre, ha bárki megpróbált volna kiszállni a körből, az adminisztrátor bosszúval fenyegette a felhasználókat.

Azonban a trendeknek való megfeleléshez az erőforrások nem minden esetben állnak rendelkezésre, vagyis a kortársak megbecsülésének, elismerésének megszerzése veszélybe

kerülhet. A célok eléréséhez szükséges eszközök hiánya feszültséget és frusztrációt keletkeztet, ezért alkalmas és legitim eszközök híján olyan utakat választanak a résztvevők, amelyek életveszélyesek vagy jogellenesek. Az online interakciókban felfedezhetők a Robert K. Merton nevéhez fűződő *feszültségelmélet* elemei. A szociológus a 20. század elején az amerikai társadalmat helyezte vizsgálódásainak középpontjába a deviáns viselkedések okainak magyarázatait kutatva. Nézete szerint a feszültségelméletet alapvetően a kulturális struktúra két tényezője magyarázza. Az egyik a *kulturálisan meghatározott, közvetített célok és értékek,* amelyeket a társadalom minden tagja jogos célkitűzésnek tart, és elérésük szükségességében egyetértés van (család, a házasság, a munkahely, autó, a stabil anyagi egzisztencia). A kulturális struktúra másik tényezője a célok *elérését biztosító törvényes, legitim eszközök rendszere* (tanulás, kapcsolatok, képességek és lehetőségek). Merton szerint akkor működik egy társadalom harmonikusan, ha a kulturális célok és eszközök elfogadása között nincs nagy eltérés: a társadalom tagjai a kulturális célokról és azok elérésének törvényes és intézményes módjairól nagyjából hasonlóan vélekednek, elfogadják azokat. Abban az esetben, ha az elvárt és a vágyott kulturális célok elérésére nincs megfelelő intézményes eszköz és mód, a célok és eszközök közt ellentét keletkezik (MERTON 2002, 214–217.). Ha a kulturális és a társadalmi struktúra közt nincs összhang, vagyis a kulturális struktúra elvárásait (célok és eszközök) a társadalmi struktúra kizárja (alacsony státusz), akkor *anomikus állapot* alakul ki (MERTON 2002, 246.). Merton a deviáns magatartásokat öt alkalmazkodási modell mentén írta le, mint a *konformizmus,* az *újítás,* a *ritualizmus,* a *visszahúzódás* és a *lázadás* (MERTON 2002, 222–238.).

Merton a 20. század első felében alkotott elméletét az Amerikai Egyesült Államok akkori társadalomstruktúrájához, valamint a korabeli tömegkommunikációs technikákhoz (rádió, televízió) illesztette, ezért teljességében nem adaptálható a cybertársadalom működésére, de egyes elemei – a trendkövetésre irányuló nyomás hatásain felül – kirajzolódnak az internetes reklámok által felerősödő, kényszeres fogyasztói magatartás-mintázatokban.[38] Az elérhetetlen elérhetőségének illúziójában a gyanútlan internetező kényszeres fogyasztóvá válhat, anyagi vagy képességbeli hiányosságai azonban elérhetetlenné teszik a vágyott célt. Az értékesnek tartott tárgyak, szolgáltatások megszerzésének vágyát felerősítik az olyan új normasértő cselekvések, mint a bérkommentelés, aukciós csalások folyamatában a vásárló véleményét alakító cinkos együttműködés vagy a reklámbannerek túlzott és nem kívánt megjelenését biztosító technikai műveletek. Az újdonságok olyan értékként jelennek meg, amelyet a felhasználók jogos célkitűzésként értelmeznek, vagyis egy elérhető „amerikai álomként". A világhálón megjelenő információbázisok gyártói és szerkesztői, a kortárscsoportok vélemény- és trendformálói, a tartalomszolgáltatók – ha nem is mindig közvetett módon, de – *cselekvést meghatározó hatalommal* rendelkeznek, és képesek hozzájárulni a mertoni alkalmazkodás egyes modelljeinek megformálódásához, ezáltal a deviáns magatartásformák megvalósulásához.

Az internet fejlődésével a vásárlás, a reklámozás sajátos, kifejezetten az internet architektúrájára jellemző formái is megjelentek. Ennek egyik megjelenési formája, hogy egyre speciálisabb, közvetlenül a fogyasztó igényeit kielégítő termékeket reklámoznak. A reklám középpontjába a termék helyett a vásárló kerül. A jó reklám és a jó termék a vásárló igényeit

[38] A felhasználók észrevétlen meggyőzésének eszközei az új dolgok vásárlására ösztönző reklámok, amelyek akkor is megjelennek a felhasználók előtt, amikor épp más szándékkal szörfölnek az interneten.

már-már egyedül az adott személyre jellemző módon elégíti ki. Az információs társadalomban a tömeg helyébe az egyén, a tömeges igény helyébe az egyéni lép. Mind a reklám, mind az eladási technika szempontjából egyre nagyobb jelentősége lesz a bizalomnak. Az egyik ilyen, bizalmi alapú találmány a vásárlói közösség által működtetett rendszer (például eBay). Ebben a résztvevők – lakjanak bárhol is Földön – egymás számára értékelik a vásárlókat és az eladókat. A másik típus a Paypal fizetőszolgáltatás és az eBay aukciós portál integrált rendszere, amelyben egy-egy szolgáltató magával a bizalommal kereskedik, az eladó és a vevő között a tranzakció részleteit tekintve – megállapodásuk értelmében – felügyeletet gyakorol. A marketing új formája a *gerillamarketing,* amelynek lényege a figyelemfelhívás és a közösségihálózat-alapú terjedés, valamint a mindennapi életben való, gátlás nélküli jelenlét. Ezeket a reklámozási és eladási formákat nagymértékben támogatja a *big data* jelenség, azaz hogy az eladók részletes információkkal rendelkeznek a vevőkről.

2.6.6. Cyberdevianciák a racionálisdöntés- és a rutintevékenység-elméletekben

A *racionális döntés elmélete* Gray S. Becker közgazdasági Nobel-díjas nevéhez fűződik. Becker szerint az egyén cselekvéseit racionális döntésfolyamatok előzik meg, amelyek hátterében a döntést hozó azt mérlegeli, hogy miként tudja a számára legnagyobb szubjektív hasznot megszerezni a legkisebb költséggel. Gazdaságosnak és racionálisnak tartott cselekvéseit tudatosan választja, éppúgy, mint az alkalmazott eszközöket, módszereket és stratégiákat – vállalva a költségoldalon felmerülő kockázatokat (Korinek 2010, 132.). Becker közgazdasági elméletét Derek B. Cornish és Ronald V. Clarke vezette be a kriminológiába azzal, hogy az elmélet a bűnözés esetében is alkalmazható modellként. A bűnelkövető mérlegel a bűncselekmény előtt az elkövetéssel megszerezhető haszon, a ráfordított költségek és a kockázatok között. Abban az esetben, ha magasabb a haszon, mint a költség és a veszteség (befektetett munka, pszichés terhelés, lebukással járó büntetés), akkor a bűncselekmény elkövetése mellett, ha alacsonyabb, akkor ellene dönt. A deviáns magatartásokról való döntés sok más egyéni tényezővel függ össze, de az elmélet az egyén célorientáltságát és a maximális haszonra törekvését feltételezi (Podoletz 2016, 240–241.). A racionális döntés elmélete a vagyon elleni bűncselekmények magyarázataként közismert, de számos olyan további cselekvés folyamatára is ráilleszthető, ahol nem feltétlenül az anyagi haszonszerzés, hanem valami más előny megszerzése a cél. A deviáns magatartást megvalósító egyénnek az elkövetés mellett szóló döntése akkor a legvalószínűbb, ha a költségek közül a lebukás kockázatai (büntetés, szégyenérzet) elkerülhetők. A cyberdevianciákban a személyazonosság rejtve maradása (anonimitás és a titkosság) csökkenti a lebukás kockázatát, ezért a racionális döntés a normasértő logika része.

Az agresszió és az erőszak virtuális alakzatainak instrumentális mintázatai megközelíthetők a racionális döntés elméletének nézőpontjából, ugyanis az efféle cselekvések folyamatában az egyén mérlegeli a cselekvésekből származó hasznot és a költségeket. Ha a normasértő a költségeknél nagyobb haszonra tehet szert az agresszió alkalmazásával, nagyobb az esély arra, hogy ilyen eszközöket használ, és vállalja azok költségeit. A döntés a képességekkel is egyenesen arányban áll: ha a felhasználó képes az agresszióra és ezzel együtt az erőszak alkalmazására – mert adottságai mentén erre könnyedén lehetősége nyílik, és a haszna is meghaladja a költséget –, akkor nagy eséllyel folyamodik agresszív eszközökhöz (Smith–Mackie–Claypool 2016). Az instrumentális magatartások körébe a zsarolás, a csalás,

a zaklatás, a behálózás egységesen beletartozhat, valójában azokban az esetekben, amikor maga a normasértő szándékosan és tervezett módon cselekszik. A *haszon* maga a szükséglet kielégítése (egy tárgy megszerzése vagy az adott cselekvés megnyerése), a *képesség* a digitális tudás és az agresszív fellépés azonnali aktivizálásának képessége, a *kockázat* pedig a lebukás, amely az anonimitással vagy a virtuális identitás megváltoztatásával minimálisra redukálható. Ilyen lehet egy anonim felhasználó, aki zaklat vagy zsarol valakit olyan kompromittáló tartalmakkal, amelyeket a célszemély számítástechnikai rendszerének feltörését követően szerzett meg. A cyberzaklató a nyereséget, amely nem feltétlenül anyagi haszon, jövőbeli jutalomnak *(prospective rewards)* tekinti. Mindeközben az elkövetés kockázatait, „költségeit" (kontrollintézmények büntetése) az anonimitás csökkenti (PITTARO 2011, 290.). Racionális döntés előzi meg az internetes kereskedelmi tevékenységeket (kábítószer-kereskedelem, a fegyverkereskedelem vagy a gyermekekről készült pornográf felvételek adásvétele), ahol a hatékonyságot az óriási kereslet tartja fenn. A kínálati és keresleti oldalon állók mindegyikénél magasabb a haszon a lebukási kockázatnál, amit a rejtett működés és a szürkezónák nehéz elérhetősége garantál. A kínálati oldalon a haszonszerzési szükségletek, a keresleti oldalon a jogi normákat sértő és a társadalom által nem preferált szükségletek kielégítése a cél, ezért mindkét oldal érdeke a szürkezónák fenntartása.

Az egyén arról való döntése, hogy a normasértő magatartást a cybertérben vagy a hagyományos térben valósítja-e meg, kétségkívül racionális mérlegelési folyamat. Az anonimitás és a számítástechnikai tudás elegendő lehet ahhoz, hogy az elkövető ne a hagyományos tér magas kockázatait (a felismerhetőséget vagy a hátrahagyott materiális nyomot) válassza, így például a bankrablás helyett a bank információs rendszerének feltörését választja. Az online csalás során rövid idő alatt több felhasználó megtéveszthető, és az anonimitás okán sokkal kevesebb kockázattal jár. *A cybertérben az az egyén dönthet racionálisan a számítástechnikai rendszerek megértését feltételező cyberdevianciák megvalósításáról, aki rendelkezik ilyen kompetenciákkal.*

A cybertérben a deviáns magatartások haszonmaximalizálásra irányuló döntési mechanizmusát a tömegnyomás is befolyásolhatja, a reaktív agresszivitás esetén pedig a heves érzelmek téríthetik el az egyén észszerű döntését. Herbert Simon *korlátozott racionalitás* elnevezésű koncepciója szerint az észszerűtlennek tűnő magatartások hátterében számos tényező állhat, ezek közül a legjelentősebbek az információhiány, a nem látható kockázatokból eredő események és a döntési helyzet komplexitása (PODOLETZ 2016, 242). A cybertérben ezek leginkább a konfliktusos magatartások eredményei, így például a dühből eredő rágalmazás vagy más, önbecsülést sértő megnyilvánulások.

A *rutintevékenység-elmélet* Lawrence E. Cohen és Marcus Felson nevéhez fűződik (1979). Eszerint az egyén a normasértéseket napi rutintevékenységek által adandó alkalmak és lehetőségek során valósítja meg, három alapvető feltétel megléte esetén: az *elkövető,* vagyis aki deviáns módon cselekszik, a *célpont,* ami lehet tárgy vagy személy, és végül *a lehetőség,* vagyis az alkalom a normasértő magatartásra. Ha a hármas pillér valamelyike hiányzik, a bűncselekmény nem valósulhat meg. A deviáns magatartások a hétköznapok részei és hétköznapi emberek normasértései, akik a deviáns cselekvésre adandó alkalmat használják ki (KORINEK 2010, 141.). Cohen és Felson az elméletüket kiegészítették a potenciális elkövető jellemzőivel: ilyen az érték (az elkövetőt mindig valamilyen cél vezeti: az érték megszerzése miatt követi el tettét), a bűncselekmény tárgyának fizikai kiterjedése és súlya (könnyen megszerezhető és szállítható), a tárgy láthatósága, valamint elérhetősége *(value, inertia, visibility,*

accessibility – VIVA) (Cohen–Felson 1979), de kiegészítő elem még a bűncselekmény tárgyát vagy a potenciális sértettet védő személy, a fizikai vagy személyes őrző *(capable guardian)* (Choi 2008, 308.).

A rutintevékenység-elmélet szorosan kapcsolódik Travis Hirschi és Michael R. Gottfredson *csekélyönkontroll-elméletéhez.* A szerzőpáros szerint a bűncselekmények elkövetése szorosan összefügg az egyén gyenge önkontrolljával, tehát ha a normasértésre alkalom adódik, nem képes ellenállni a kísértésnek. A rutincselekvés és a csekély önkontroll elméletének közös metszete egy olyan személy, aki előtt az alkalom és a célpont is megjelenik, miközben a bűncselekmény elkövetésétől visszatartó belső ereje gyenge. Az önkontrolldeficit visszavezethető a családi szocializációs hiányosságokra, amelyek épp az ilyen alkalmakkal szembeni immunitás megerősítésében tölthetnek be alapvető szerepet. A csekély önkontroll továbbá olyan individuális gyökerekből származhat, mint a túlzott énközpontúság, a nárcisztikus személyiség, az antiszociális személyiség (Győry 2016, 185–190.). Az elmélet Hindelang, Gottfredson és Garofalo *életstílus-elméletével* is rokon, amely szerint a mindennapi cselekvések, mint amilyen a munkába járás vagy a szabadidő eltöltése, sértetté válási alkalmakat teremtenek (Győry 2016, 18.), és a sértetté válás kockázatát növelik az egyén társadalmi (például családban vagy közösségben betöltött) szerepével kapcsolatos aktivitások is.

A cyberdevianciákra vonatkoztatva a csekély önkontroll emlélete a szexuális ösztönkésztetéseknek való ellenállás gyengeségében (például a pornográfia vagy a cyberszex esetében), illetőleg agresszív magatartásban (például zaklatás, kényszerítés) nyilvánul meg. A rutintevékenység és a csekély önkontroll elmélete a számítástechnikai rendszerintegritás elleni magatartások okaira is rávilágít. *Az elkövetésre az alkalmat maga a felhasználó teremti meg azzal, hogy nem elég alapos az azonosító adatainak tárolásában, ezzel sebezhetővé válik, és az elkövetési alkalmat tálcán kínálja támadói számára.* Az „etikus hackerek" gyakran ezekre a sebezhetőségekre (alkalmakra) mutatnak rá, felhívják a tulajdonos figyelmét a támadhatóságra.

A *cyberbullying* magatartás-mintázatait a rutintevékenység-elmélet mentén vizsgáló kutatók szerint az elkövető a napi rutintevékenysége során fejti ki megfélemlítő megnyilvánulását, ha gyenge ellenállású felhasználóra talál a kortárscsoportban (Martinez-Prather–Vandiver 2014). Hasonlóan értelmezhető a cyberragadozókként ismert felhasználók cselekvésformája is, amikor a naiv, gyermekkorú a felhasználó a potenciális sértett, az alkalmat pedig a chatszobák és a nyilvános közösségi oldalak könnyű elérhetősége teremti meg. Az elmélet a szellemi termékek jogellenes használatára is érvényes, azzal a különbséggel, hogy abban a konformnak mondott felhasználók is nagyobb arányban vesznek részt. Napi rutinnak számító szörfölgetésük alkalmával töltenek le, küldenek el vagy terjesztenek szerzői jogvédett tartalmakat. A normasértésről való döntést ebben az esetben a normasértő felhasználók nagy tömegének részvétele is ösztönzi (Gunter 2011, 176.).

A rutintevékenység elméletét több, *szexuális bűnelkövetővel végzett vizsgálatban* is tesztelték. A vizsgálatokban a kutatók arra voltak kíváncsiak, hogy milyen összefüggés van a szexuális bűnelkövetők cselekményei és az internetes pornográf tartalmak látogatása és tárolása közt. Az eredmények szerint a szexuális abúzust elkövető bűnözők számos, gyermekekről szóló pornográf oldalt látogattak elkövetés előtt, illetve több ilyen tartalmat tároltak eszközeiken, amelyek a szexuális erőszakot és az ezzel összefüggő deviáns gondolatokat aktivizálták. A szexuális bűnelkövetők közül azok, akik az efféle tartalmak látogatására és internetes kapcsolatkötésre több lehetőséggel rendelkeztek, több esetben is

követtek el újabb bűncselekményt, mint azok, akik ilyen tartalmakkal nem kerültek kapcsolatba. A bűnelkövetők által internetes csatornákon kialakított, aktív felnőtt-gyermek kapcsolatok további bűncselekmények elkövetésére ösztönözték őket, szemben azokkal, akiknek nem volt ilyenre alkalmuk (ELLIOT et al. 2009; HAMILTON 2012, SETO–EKE 2005).

A rutincselekvés-elmélet *cybertérre adaptálhatóságáról* megoszlanak a vélemények. Leukfieldt és Yar metaanalízis keretében a 2008 és 2015 közötti időszakban írt, összesen tizenegy tanulmány eredményeit vetették össze, beleértve saját vizsgálatukat is (LEUKFELDT–YAR 2016). Az *alkalmas őrző* a cybertérben lehet technikai – tűzfal, vírusirtó, szűrőprogram, felhasználóazonosító, online beléptető alkalmazás – vagy személyes jellegű, mint például egy online közösségi oldalon a chatpartnerek vagy a jelen lévő, ámde nem mindig látható felhasználók, továbbá hálózati adminisztrátorok, moderátorok, kommentfelügyelők (Williams terminológiájával élve a „netizenek": WILLIAMS 2010). A tanulmányok, amelyek közül valamennyi önbevallásos adatgyűjtés volt, nem hoztak egymással összecsengő eredményeket. Ennek az lehet az oka, hogy különböző nagyságú és nem reprezentatív, jobbára kényelmi mintákat kérdeztek meg, a válaszolási arány igen csekély volt, és a tanulmányok többsége csupán egyetlen bűncselekmény előfordulását vizsgálta. Leukfeldt és Yar mindebből okulva már nagyobb mintát vett (n = 9161), és három kategóriába tartozó cselekményeket vizsgált.

- Az első kategória a high-tech bűncselekményeké (*hacking, malware* – számítástechnikai rendszerbe való jogellenes behatolás és a felhasználó számítógépébe kártékony program bejuttatása). A hacking esetén az életkor megnöveli az áldozattá válás esélyét. A kémprogrammal való fertőződés viszont inkább a nőket, a magasabb iskolai végzettségűeket és az állandó, fizetett állásban lévőket sújtja.
- A kibercsalások *(cyberfraud)* elszenvedése körében az identitáslopás *(identity theft)* mögött nem azonosítottak szignifikáns karaktereket: ez nem függött sem a sértett iskolai végzettségétől, sem a nemétől, sem pedig az életkorától. Ezzel szemben azok, akik alacsonyabb fokú iskolát végeztek, és nem rendelkeztek fizetett állással, inkább estek áldozatul fogyasztói csalásnak *(consumer fraud).* A szerzők azt gyanítják, hogy ennek a hátterében a kevésbé megbízható, a megrendelt áruért előre fizetést kikötő weboldalak állnak, amelyek jobban vonzzák a kevésbé tehetős felhasználókat. Az itt vásárolt termékek olcsók ugyan, de gyakran megesik, hogy soha nem érkeznek meg a megrendelőhöz. Ugyanakkor ebben a körben azonosítottak egy védelmi faktort is: azok az online vásárlók, akik tudatában voltak az ilyen vásárlások magas kockázatának, kevesebb visszaélést szenvedtek el – valószínűleg azért, mert gondoskodtak technikai és más védelmi intézkedések megtételéről (például a fizetési garancia). Esetükben tehát az alkalmas védelem faktora volt hatékonyabb.
- A harmadik csoport az interperszonális kiberbűncselekményeké *(interpersonal cybercrimes),* ami az online fenyegetést *(online threat)* és a zaklatást *(online stalking)* foglalja magában. Az első típus inkább a fiatalokat sújtja: minél fiatalabb az illető, annál inkább jellemző rá a kortársakkal való online kapcsolattartás, a közösségi oldalak és direkt online kommunikációs eszközök (amilyen a Skype, az MSN vagy az e-mail) gyakori használatával pedig megnövekednek a visszaélési alkalmak. Hasonló rizikónövelő a közösségi felületeken az ismerősök nagy száma, ami akár még védőfaktorként is működhetne, ám a kutatások szerint

ez a proaktív kiállás – megfelelő és célzatos képzés, továbbá tudatosságnövelés hiányában – nem jellemző a kortárs közösségekre (Agustina 2015; Choi 2008).

Ami azonban minden tanulmány szerint kockázatnövelő volt, az az online eltöltött idő tartama: az expanzív internethasználat megnöveli az áldozattá válás kockázatát, bármely vizsgált bűncselekménytípusról legyen is szó (Leukfeldt–Yar 2016, 279.). Nyitva maradó kérdés, hogy vajon az identitáslopás és a kártékonyszoftver-telepítés miért nem inkább a tehetősebb felhasználókat fenyegeti. A szerzők szerint ez a *harmadik generációs informatikai bűnözés* jellemzőivel függ össze, miszerint a hackerek ezekkel a módszerekkel rengeteg felhasználót céloznak meg, és arra törekednek, hogy automatizált támadások segítségével könnyűszerrel kis összegeket szerezzenek meg minél több sértettől (Parti–Kiss 2016).

Összefoglalva elmondható, hogy a bemutatott elméletek a cybertér viszonylatában alapvetően három formában jelennek meg:

- a *sebezhető rendszerekbe történő behatolás és jogtalan adatkezelés* formájában, amelynek a hacker nem képes ellenállni;
- *ahol szexuális késztetések törnek felszínre* (például online gyermekpornográfia), amikor a behálózható felhasználó körül nincs védelem (Pittaro 2011, 289.);
- az *impulzív, agresszív internetező esetén,* aki egy közösség tagjaként a napi rutinja során gyakorol nyomást a sebezhető áldozatra (cyberbullying).

Az elméletek az elkövetők magatartását, motivációit magyarázzák, ám a cybertérben az anonimitás megtévesztő érzete a felhasználókra is kihat, és éppen emiatt hajlamosak személyes adataikat könnyen kiadni vagy más meggondolatlan lépéseket tenni (Agustina 2015, 44.). Az önbevallásos latencia- és áldozatkutatások megállapításai szerint az áldozatok magatartása kockázati faktort képezhet a cyberdevianciákkal való érintettségben. Ezek közül a legkiemelkedőbb kockázatot *a gyakori és kiterjedt internethasználat* (függőség, „támadási felület"), *a nettapasztalatok teljes hiánya* (a kezdő internetezők hiszékenysége, zsarolhatósága) jelenti, de *a genderpszichológia* (nők mint speciális áldozati csoport) és *a fejlődéspszichológia* (kamaszok mint a kortárscsoporttól leginkább függő generáció) is azonosít vulnerábilis társadalmi csoportokat.

2.6.7. Címkézés és kommunikáció a cyberdevianciák kialakulásában

A cyberdevianciák igen gyakran a virtuális interakciókban létrejövő közvetlen kommunikáció mentén teljesednek ki, a közlő és a fogadó közti információáramlás folyamatában. A közvetlen kapcsolatban zajló információcsere végkimenetelét (cselekvések) a felek észlelési és értelmezési képessége, olykor már előzetesen meglévő kapcsolatai befolyásolják. Egy közölt tárgyi tartalom számos más kapcsolt üzenetet tartalmazhat, amelyet a vevő sokféle jelentéstartalommá formálhat. A címzett saját szimbólumai, sémái, diszpozíciói alapján dekódolja a fogadott tartalmakat, ami akkor helyes, ha egyezik a küldő által közölni akart információtartalommal (Schulz von Thun 1981). Ha attól eltérőként értelmezi, cselekvést formáló félreértések, konfliktusok generálódhatnak a két fél közt. A jelentéstartalom fogadó általi értelmezése egyáltalán nem magától értetődő. George Herbert Mead szerint az egyén észlelése és az arra adott reakció olyan folyamat, amelyben az egyén kiválasztja az észlelt

ingerre adható reakciót. Az inger, vagyis az észlelt dolog és a reakciók közt ugyanis eltérések lehetnek, ami abban nyilvánul meg, hogy az egyén a beérkező ingerekből (kódokból) egy jelentéstartalmat alakít ki, amelyet az észlelt dologgal kapcsolatos korábbi szimbólumsorozatokkal is összevet, majd az így kialakított jelentéstartalomra reagál. Nem biztos, hogy az észlelt dolog a reakció közvetlen kiváltója, sokkal inkább az a jelentéstartalom, amelyet az egyén az észlelt dologból a folyamat során kialakít (MEAD 1973).

Mead tézise nagyon fontos a kommunikáció helyes értelmezésében, ugyanis a megformált jelentéstartalom alapján történő cselekvés vagy válasz meghatározó a kommunikáció kimenetelében. A kommunikációs csatornákon generálódó konfliktusokból eredő agresszív megnyilvánulások gyakran a hibás kódolás és dekódolás műveletének hozadékai. Mivel a metakommunikációs jelek – a testbeszéd vagy a mimika – a kommunikácó szerves részei, helytelen dekódolás adódhat, ha az egyik fél nem látja a másikat. A metakommunikációs jelek olyan plusz adalékot társítanak a közölt verbális tartalomhoz, amely megváltoztatja a közölt információ jelentését, igazságtartalmát. A metakommunikációs jeleket a cybertér kommunikációs csatornái nem minden esetben képesek továbbítani. A cybertérben történő kommunikáció lehet olyan információáramlás, amelyben a küldő célja alapvetően a címzett lelki bántalmazása vagy manipulatív befolyásolása. A csalás vagy a behálózás manipulatív módszereinek alkalmazása esetén nem csupán rossz dekódolásról van szó, hanem *megtévesztő* információtartalmakról, vagyis a fogadó jól dekódol hamis információkat. A behálózás cselekvésláncolatában viszont olyan információk küldése történik, amelyek az egyik oldalról a fogadó fél szimbólumaihoz, értelmezési sémáihoz tervezettek (a küldő a fogadó szimbólumaival egyező kódokat küld), és épp azoknak a szükségleteknek a kielégítését vagy vágyaknak a teljesülését ígérik, amelyekre a fogadó vágyik. A behálózásban gyakran alkalmazott technika a *kommunikációs maszk* és a *hízelgő technika,* amelyek lehetővé teszik a nem kongruens elemeket tartalmazó kommunikációt, elfedik a közlő valós érzelmeit és szándékait (SCHULZ VON THUN 1981). A tartalmak hibás dekódolása vagy a manipulált tartalom helyes dekódolása a kollektív cselekvéseket is formálja, félelem- és pánikkeltésre alkalmas, normasértésre ösztönözhet.

Az egyén az egyértelmű és tiszta információkat nemcsak az előre beépített sémái alapján, hanem lelki zavarai, negatív önbecsülése miatt is sérelmesnek értelmezheti (WERNER–BUMPUS–ROCK 2009). Baumeister szerint például a reaktív agresszivitás egy kommunikációban akkor jelenik meg, ha valakinek az önbecsülését meghatározó önértékelését vagy valamely közösséghez tartozását éri fenyegetés. A becsmérlés (vagy a tiszteletlenség) épp ebbe a kategóriába tartozik, és gyakori eleme a konfliktusoknak. Az önértékelést fenyegető ingerek hatására az *alacsony* vagy éppen a *magas* önértékelésű felhasználók reagálhatnak agresszív töltetű válasszal. Ha a provokáció nagy nyilvánosság előtt zajlik – ami a cyberfórumokon evidens –, még erősebb feszültséget keletkeztet, ami ennél is intenzívebb magatartást eredményez. Az agresszív reakció viszont mindenkinél sokkal valószínűbb akkor, ha a kommunikációban a múlandóságra (élet-halál kérdések) vagy a világnézetre (vallás, politika vagy bármilyen más ideológia) utalóan történik fenyegetés (SMITH–MACKIE–CLAYPOOL 2016, 657.). Az internetes fórumokon jól megfigyelhető, hogy a világnézetre irányuló beszélgetés olykor valóban elmérgesedő vitába torkollik.

A kommunikációban keletkező érdekellentétek további oka, amikor az egyén nem képes a másik fél érdekeire koncentrálni. Beck *ellenséges leképezésnek* nevezi azt a jelenséget, amikor a felek nem mérik fel reálisan egymás érdekeit, csak a fenyegetést észlelik, és arra

reagálnak. Az ellenséges leképezés az egyén helytelen hiedelmeitől is függ, vagyis azoktól a téves gondolkodási mintáktól, amelyekben megmutatkozik mindaz, amit gondol a másik félről. A hiedelmek az egyén szocializációja során formálódnak, és meghatározzák, hogy ő maga mit vár el környezetétől, milyen státuszban helyezi el önmagát a társadalomban. A hiedelmek egy része az agresszív magatartás forgatókönyve és egyben a felületes értelmezés sémája. Egy végtelenül magas önbecsülésű felhasználónak például lehet olyan hiedelme, miszerint minden embernek tisztelnie kell őt, aki ezt nem teszi, annak meg kell bűnhődnie (Beck A. 1999). Az effajta hiedelmek a felsőbbrendűség különböző mintáiban is megmutatkoznak, és hosszan tartó gyűlöletet generálnak, ugyanakkor az antiszociális egyén személyiségének meghatározó elemei. A cybertérben zajló konfliktusok gyakran az ilyen hiedelmek által felkorbácsolt indulatok miatt léphetnek ki a hagyományos színtérre, ahol aztán súlyos erőszakként fejeződnek be. Konfliktusos, reaktív magatartás többnyire társas oldalakon, interaktív weboldalakon és kommunikációs csatornákon zajlik, némely esetben épp azért, mert a cél eléréséhez a nyilvánosság nélkülözhetetlen.

A cybertér interakcióiban zajló kommunikáció és információközlés sokféle magatartás meghatározója, köztük olyan *megbélyegző* interakcióké, amelyekben egyént vagy közösséget deviánsnak címkéznek. A *címkézéselmélet* több teoretikus nevéhez fűződik, úgymint George Herbert Mead, Howard S. Becker, Frank Tannenbaum, Harold Garfinkel, Emil Goffman és Edwin Lemert. Az elmélet többek közt abból a kérdésből indult ki, hogy a társadalomban egyes cselekvések miért normasértők, míg más magatartások nem. A válasz az, hogy egyes magatartások nem önmagukban deviánsak, hanem akkor, ha azt a társadalom, illetve a társadalmi kontrollintézmények deviánsnak minősítik. A normákat a hatalommal rendelkezők, a döntéshozók (morális felügyelők) szűk rétege szabja meg, ezzel együtt azt is, hogy hol vannak a társadalom normahatárai (Rosta 2007, 153.; Korinek 2010, 175–184.; Győry 2016, 169–175.). A teória szerint a deviáns magatartás társadalmi interakciókban keletkező társadalmi produktum, amely leginkább a hatalommal rendelkezők érdekeihez áll közel. Becker szerint a szabályok érvényesítése egy folyamat eredménye, amelyben a szabályalkotók ellentétes akarata áll egymással szemben. Hogy mikor melyik szabály lesz érvényes, az attól függ, hogy a szabályalkotó csoportok közti erőviszonyok hogyan alakulnak (Győry 2016, 171.). George Herbert Mead szerint az egyén vagy a közösség önmaga identitását, szerepét és cselekvéseit a társadalmi interakciókban mások által róla kialakított attitűdök mentén formálja, vagyis az „én" a társadalmi interakciókban fogalmazódik meg, és alakul „reaktív énné" (Mead 1973). Mead tétele a címkézéselmélet egyik alapköve abban a tekintetben, hogy az egyén a környezete és a társadalmi kontrollintézmények vele szemben kialakult és ismétlődő attitűdjei mentén értelmezi önmagát deviánsnak. A címkézési folyamat eredménye lehet az *elsődleges és másodlagos deviancia,* amelyeket Tannenbaum és Lemert különböztetett meg. Az egyén a társadalom által kevésbé elítélt normaszegését követően elindul ugyan a címkézés útján, de nem jut el a bűnözői szerepig, és nem is azonosul azzal – főként, ha cselekménye látens marad. Ha viszont normasértő szerepét egyre többen és többször hangsúlyozzák, az egyén ellenállását további normasértéssel fejezi ki, ami még több szabályszegést eredményez, végül már a hatóság is felelősségre vonja. A címkézés mélyül, az egyén önmagáról bűnözői önképet alakít ki. Ebben a fázisban már megfogalmazható a másodlagos deviancia, ami az egyén számára káros következményekkel jár: egyre több deviáns cselekedetet követ el, keresi a deviáns közösségeket, azonosul a bűnözői szereppel, és valóban elindul a bűnözői karrier útján (Rácz–Fokasz–Szügyi 2001, 121–143.).

A címkézés az intézményekben tovább zajlik, a gyanúsított a kihallgatástól a szabadon bocsátásig egyfajta lefokozási szertartáson megy keresztül, majd a társadalomba kilépve örökre megbélyegzett lesz (RÁCZ–FOKASZ–SZÜGYI 2001, 143.).

A címkézéselmélettel összefüggésben említendő a hackerkultúra, amelynek társadalmi megítélése a mai napig homályos. Évtizedekkel ezelőtt a hackerek olyan közösséget alkottak, amelyben a szabad információcserén alapuló szabályok egyértelműen kirajzolódtak, miközben a társadalmi hierarchiával való szembenállás és az ellenkultúra szellemiségének mozaikjai szabályrendszerük szerves része maradt. Az idők folyamán a magukat hackereknek nevező nagyközösségen belül létrejöttek kifejezetten normasértő egyénekből álló csoportok. E kis csoportok illegális tevékenysége, a rosszindulatú rendszerfeltörések azt eredményezték, hogy a hackereket általánosságban bűnelkövetőnek címkézték, tevékenységük a köztudatban deviáns magatartássá formálódott. A negatív társadalmi megbélyegzés felerősítésében a szakirodalom szerint a média, a politika és az igazságszolgáltatás prezentációjának volt és van a legnagyobb szerepe. Annak ellenére, hogy a „jó" hackerekre (*white hat,* vagyis fehérkalapos hackerek) a bűnelkövetésen kívül a technológia feletti politikai és vállalati önkényuralom elutasítása, tehát a hierarchikus rendszerbe való beilleszkedés nagyon is jellemző volt, követelték reputációjuk helyreállítását, és azoktól való megkülönböztetésüket, akik tudásukat normasértésekre használták (*black hat,* vagyis feketekapalos hackerek). A negatív sztereotípiák a követelések ellenére stabil hiedelmekké formálódtak. Emellett kialakult az a nézet is, hogy a hackerek olyan ellenállók, akik a virtuális hatalom megszerzésére törekednek, amelyet aztán saját céljaikra használnak (JORDAN–TAYLOR 1998). A hackertársadalom képviselői szerint a rendszerintegritást sértő magatartásokat egységesen hackercselekedetként hirdetők nem tudják és nem is akarják reálisan értékelni a cselekvések közti különbséget, és úgy tartják társadalomra veszélyesnek, hogy közben nem részletezik a normasértők valódi szándékát. A cybertérben zajló deviáns tevékenységek efféle általánosítása a negatív megbélyegzésen kívül a morális pánikkeltés elméletével is azonosítható.

A Stanley Cohen és Jock Young által leírt *morális pánik* elmélete szerint egy a többségtől eltérő társadalmi csoportot a hatalmi struktúra szereplői vagy más társadalmi közösség, a médiumok felerősítő hatását kiaknázva, a társadalmi rendre és értékekre veszélyesnek tüntetnek fel, ezzel velük szemben a társadalmi többség tagjaiban félelmet és gyűlöletet keltenek. Az elmélet kidolgozói szerint a veszélyhelyzet túldimenzionálásával pánikot keltenek a társadalmi többség tagjai közt, és ezzel együtt negatív attitűdöket formálnak a célkeresztben állókkal szemben (KORINEK 2010, 181.; GYŐRY 2016, 173.).

A morális pánikkeltés, a címkézés és a félelemkeltés az internetes hálózatokon működő online hírszolgáltatók működésében és a közösségi média platformjain közzétett információkban összpontosul, amelyek hatással vannak a felhasználók többségének attitűdjeire. A címkézés, a félelem- és pánikkeltés nem új jelenségek, egyes korszakokban a hatalomgyakorlás hatásos eszközei voltak, napjainkra viszont azoknak az internetes oldalaknak a működéséhez köthetők, amelyek a nézettségnövelést célzó tartalmakat gyártják. Az online hírszolgáltatók és a közösségi média erre irányuló tevékenysége röviden úgy foglalható össze, mint *olyan tartalomközléssel vagy aktív kommunikációval megvalósuló szándékos és céltudatos magatartás, amely félelemkeltésre, negatív attitűd formálására, agresszió generálására és konzerválására alkalmas. Közvetett módon kapcsolódhat az információs rendszerek megsértéséhez és a fizikai erőszakhoz.* Az online közösségi platformokon gyakran terjednek a felhasználóktól származó, megalapozatlan rémhírek (például gyermekrablásokról), amelyek a terjesztés és a terjedés

virtuális törvényszerűségeiből adódóan olykor bizarr felhasználói reakciókat eredményeznek és az offline környezetre is kiterjednek.

A korábban már hivatkozott Kék Bálna elnevezésű közösségről a világ számos országában jelent meg hír, s ez a bűnmegelőzési szakemberek szerint csak pánikot keltett, nélkülözve minden alapot. Valójában csak egyetlen embert tartóztattak le a közösség tagjai közül, aki súlyos bipoláris depresszióban szenvedett. Amellett, hogy a fiatalok közötti öngyilkossági ráta Oroszországban és a szovjet utódállamokban az egyik legnagyobb a világon – amit az 1990-es években bekövetkező gazdasági összeomlás, a társadalmi anómia, a válások és a diszfunkcionális családok nagy száma és a mentálhigiénés segítség *(helpline-ok)* hiánya együttesen magyaráz –, a kezdeményezés és az öngyilkosságok közötti kauzalitás bizonyítása is problematikus. Politikai elemzők mindemellett globális összeesküvést gyanítanak a háttérben, nevezetesen azt, hogy orosz bérkommentelők hozták létre a közösséget, akik a kezdeményezéssel kapcsolatos pánikkeltés nyomán akarják elérni, hogy a Kék Bálnával együtt az orosz politikai befolyás ellen tevékenykedő online közösségeket is ellehetetlenítse a nyomozó hatóság, amely egymás után veszi őrizetbe az ukrán nemzetiségű rendszeradminisztrátorokat (Khazov–Cassia 2017), és kapcsolja le ezzel párhuzamosan a hosztoló szervereket. Az elméletek között a másik oldalon napvilágot látott olyan információ is, amely a Kék Bálna mögött ukrán nacionalista mozgalmat sejt, mondván, az ukrán radikálisok valódi célja az oldallal, hogy anarchista tettekre aktivizálják a fiatalokat (Khazov–Cassia 2017). A pánikhangulatnak mindenesetre már megvan az eredménye: az orosz parlament egy új törvényt szavazott meg az öngyilkosságot támogató online közösségek betiltásának jogi lehetőségéről (IMMA 2017).

Az internetes félelemkeltés másik hasonló jelensége az online hírszolgáltatókhoz köthető eltúlzott bűnözésábrázolás. Az internetes médiumok pusztán a nagyobb nézettségért az erőszakos események túlhangsúlyozásával, rossz közbiztonsági állapotok közvetítésével a hatóságokkal szembeni bizalomhiányt mélyítik, és a társadalmi stigmatizációt erősítik; indirekt módon a bűnözés latenciáját növelik. A félelemkeltő információk készítőinek szándéka a befolyásolható felhasználók általi továbbítással és terjesztéssel már beteljesültnek tekinthető. Az attitűdformálás egyik iskolapéldája az a rendőrségi gyakorlat, amelyben a hatóság önmaga hatékonyságának népszerűsítése és a biztonságérzet növelése céljából a „renitens" személlyel szembeni sikeres intézkedését saját weboldalán közzéteszi név nélkül, de szűkebb környezete által felismerhető módon. Az online hírszolgáltatók azonnal átveszik és továbbítják a kriminális eseményt leíró hírt, amelyet főként az illetőt felismerő felhasználók a közösségi média csatornáin és platformjain még szélesebb körben terjesztenek. A hatóság, a hírszolgáltatók és a közösségi média egy olyan *virtuális láncolatot* alkotnak, amely pozitív szándékú hatósági célzattal a médiumokon keresztül a véleményalkotó felhasználók tömegében negatív kritikák táptalajául szolgáló információként jelenik meg. A terjedés „törvényszerűségei" és a terjesztők szabadon megalkotott kritikája mentén ezt a folyamatot *online címkézési láncolatnak vagy mechanizmusnak* nevezzük.

Az internetes címkézés, a félelem- és pánikkeltés – a bosszantó internetes trollkodástól a nagyobb közösségi zavart előidéző rémhírterjesztésig – közvetlenül hatással van a kapcsolatokra, az egyén és a közösség döntéseire és cselekvéseire. Ezek kiterjedt formája globális szinten lehet a gazdasági erőviszonyok átformálása (például vállalatok ellen intézett hackerműveletek részeként) vagy más hatalmi harc eszköze (például a választási eredmények befolyásolása a választói attitűd formálásával).

2.6.8. A kontrollelméletek jelentősége a cyberkörnyezetben

A *kontrollelméletek* arra adnak magyarázatot, hogy miért nem válik az egyén normasértővé, vagyis milyen tényezők hatnak rá, amelyek segítségével a társadalom konform tagja marad. A kontrollelméletek megalkotásában kiemelkedő a szerepe Walter C. Reckless *visszatartás-elméletének,* miszerint az egyént a normasértés elkövetésétől kétféle erő tartja vissza. Az egyik a *belső visszatartó erők* halmaza: a jó önismeret, az önuralom, az erős ego, a fejlett lelkiismeret, a frusztrációtűrő képesség és az erős felelősségérzet, a másik a *külső visszatartó erők* csoportja: a társadalmi szerep, az észszerű felelősségek és korlátok rendszere, az egyén lehetősége a státuszra, csoportkohézió, az egyénekkel és közösségekkel való azonosulás és a vágyak beteljesítésének alternatív útjai (ADLER–MÜLLER–LAUFER 2005, 235.). A belső visszatartó erők a normasértésre késztető belső hatások kontrollját, a külső erők a külső csábítások, a környezeti tényezők elleni védekezést, kontrollt erősítik. Reckless visszatartás-elmélete végső soron a kontrollt megtestesítő külső és belső erők meglétének, erejének és mozgósíthatóságának függvénye, amelyek az egyén szocializációs szakaszai során alakulnak ki az érzelmi és erkölcsi fejlődés részeként.

A kontrollelméletek másik ága Travis Hirschi eredményein alapul, és arra mutat rá, hogy az egyén négy tényező megléte esetén kisebb eséllyel válik normaszegővé. Az első ilyen tényező a *kötődés* a szülőkhöz, az iskolához, a tanárokhoz; ez elsősorban érzelmi alapú. Ha a kötelék megfelelően mély és minőségi kapcsolatokon alapul, kevés esély van a normasértő karrier beindulásához. Az *elkötelezettség* olyan társadalmi tevékenységekben való részvétel, amely az egyént a normakövető életvitelre ösztönzi. A *részvétel* különböző hasznos programokban való időtöltést jelent. A hasznos időtöltések, mint például az iskolán kívüli programok, előmozdítják az egyén fejlődését, miközben elvonják a destruktív időtöltéstől. A negyedik tényező *a hit,* ami az adott társadalom értékendjének elfogadását jelenti (ADLER–MÜLLER–LAUFER 2005, 233.).

A kontrollelméletek egy további megalapozója Albert J. Reiss, aki a társadalmi kontroll és a személyes kontroll közötti különbség felállításával azt fejezte ki, hogy a környezet csupán formális kényszer, önmagában nem hat teljességgel. A konform életvitel akkor válik igazán valósághűvé, ha a társadalmi kontroll intézményei és csoportjai által átszármaztatott premisszákat az egyén *internalizálja,* és ennek mentén él, vagyis a konformminták mély meggyőződés elemeivé válnak (GYŐRY 2016, 180.). A kontrollelméletek közül említendő még David Matza *sodródáselmélete,* amelynek lényege, hogy a fiatal a szabad akaratával dönt arról, hogy a deviáns utat választja-e, vagy konform marad. A döntési helyzet a társadalom által elfogadott normák és a szubkultúrák által képviselt normarendszer közötti választást jelenti, amelynek adott esetben a fiatal a tagja, és a deviáns magatartás a szabad választás eredménye (GYŐRY 2016, 179.).

Hogy teljes legyen a kép, Sigmund Freud *pszichoanalízis-elméletére* is szükséges utalnunk, amelyet több kritika ért, de logikája támogatja a cyberdevianciák súlyosabb formáinak megértését (cyberszex). Freud szerint az emberi pszichében zajló lelki folyamatoknak három tartománya létezik. Az első az *id,* amely a személyiség tudattalan része, a kielégülésre irányuló késztetéseket, primitív ösztönöket, alapvető *drive-okat* tartalmazza (szexuális késztetések). A másik az *ego,* amely a személyiséget uralja, annak tudatos része, és közvetítő szerepet tölt be az id és a szuperegó között (a kognitív folyamatok is idesorolhatók). A harmadik a *szuperegó* (felettes én), amely a szocializáció során átszármaztatott moralitást,

erkölcsi szabályokat, normákat és a kontrolláló gátlásokat tartalmazza, tudatalatti része a léleknek és ellenőrző szerepet tölt be személyiségben. Ha a három tartomány működése nincs egyensúlyban, akkor nagy az esély arra, hogy az egyén normasértéseket követ el. Normasértés akkor következik be, ha az elégtelen vagy helytelen szocializációban a szuperegó nem tartalmaz elég morális, erkölcsi szabályt és gátakat, vagy az ego a jutalmazás hiánya miatt alulszabályozott vagy éppenséggel a túlzott szigor miatt túlszabályozott. Az előbbi esetében az alacsony frusztrációtűrő képesség okozza az idből előtörő vágyak egészséges késleltetésének elmaradását (szexuális erőszak), az utóbbi a túlzott lelkiismeretességet, bűntudatot eredményezi, amiből ugyancsak normasértés következik azért, hogy a túlszabályozás miatt kialakuló bűntudat a normasértés utáni büntetéssel enyhüljön (Rosta 2007, 100.).

A cyberdevianciák okainak vizsgálatában ezért a *kötődést,* az *alternatív vágyak kielégítésének lehetőségét* és a *szabad döntést* helyezzük vizsgálódásunk középpontjába. Az ellenőrzés nélküli szabadidő a gyermekkorúak tekintetében épp arra ad lehetőséget, hogy az érintett ismeretlen felhasználókkal kössön kapcsolatot, és megtanulja a normasértő magatartások megvalósításának technikai műveleteit (például hogyan kell elkövetni rendszerfeltöréseket). Minél több időt tölt az illető a cybertérben, annál nagyobb eséllyel látogat destruktív virtuális csoportokat. A szülő-gyermek kapcsolat (kötődés) nem csupán az ellenőrzés kapcsán lényeges, hanem az érzelmi kapcsolat kialakításának szükségessége miatt is. Ha a családi kötelékben nincs pozitív érzelmi alapokra helyezett kapcsolat és minőségi időtöltés, a bizalom sem alakul ki, a hiányzó érzelmi támogatást a gyermek más közösségekben keresi – példának okáért egy hackerközösségben vagy egy radikális online csoportban. Miközben fizikailag ellenőrizhető körülmények között otthon marad, IT-eszközei által a „globális játszótérre" látogathat, ahol a virtuális közösségek anonimitás vagy hamis identitás mögé rejtőző tagjaival kontroll nélkül ismerkedhet. A cybertérben már nem működik a 20. század második felében érvényes „kulcsos gyermek" és a kortárscsoport kontrollfunkciója, ahol mindenki mindenkit ismert. A külső kontroll hiányának áthidalhatósága a pozitív érzelmi attitűdöket kialakító családi szocializációban keresendő, ahol a minőségi idő része az őszinte kommunikáció és az érzelmi jólét, amely az identitáskereső fiatalok részéről nem mindenkor adott (Modecki–Barber–Vernon 2013, 651–661.). Az internetező fiatal számára a fórumokon való részvétel épp azért előnyös, hogy része lehessen egy közösségnek, lehetősége nyíljon a kortárscsoportján belül státusz kialakítására, azonosulhasson ideológiákkal, és vágyainak beteljesüléséhez alternatív eszközöket és módokat találjon. Nem mindegy azonban, hogy mindezt egy normasértő vagy egy konform közösségben teszi. A sodródáselméletben megfogalmazott *szabad döntés* pont ebben a tekintetben lényeges. A káros internetes környezeti hatásokkal szemben kialakult immunitás fogalomkörébe beletartozik a normasértő magatartás kockázatainak felismerésére és a helyes döntésre való képesség, amihez nélkülözhetetlen az erkölcsi szabályok belső szabályokká alakítása. A belső védelmi bástyák kialakítása csak az egyik oldala a nevelési folyamatnak, a másik a tapasztalatszerzés, amelyhez a cybertérben való közlekedés szabadsága elengedhetetlen feltétel. A belső kontroll megerősítésének folyamatában fontos szerepet játszik a virtuális térre nevelés, amely elsődlegesen a szülő és a család kötelezettsége, majd a másodlagos és harmadlagos szocializációs színtér szereplőié. A virtuális térben működő fiatalok esetében a belső erők megformálása éppolyan fontos, mint a külső kontrolltényezők megerősítése, mivel előbb részese lehet egy virtuális közösségnek, mint egy offline társadalmi csoportnak.

A *kötődés* mellett meg kell említenünk a *vágyak beteljesítésének alternatív útjait* is. A gyermekkort követő serdülőkor olyan életszakasz, ahol a szexuális ösztönkésztetések levezetésének különféle próbálkozásai (például a maszturbáció) az egészséges szexuális fejlődés része (BUDA 2002, 110–112.). A cybertérben szörfölgető fiatal gyakran látogat felnőtt tartalmakat, ami a szexuális fantáziálásnak, illetve a szexuális késztetések kiélésének különböző alternatíváit teszi lehetővé. Ha nem rendelkezik megfelelő belső (recklessi) visszatartó erővel (frusztrációtűrő képesség), amely vágyait féken tartaná, nagy eséllyel sajátíthat el deviáns magatartásformákat (például *szexting, sextortion, cyberstalking*). A freudi pszichoanalízis-elméletben leírt ego diszfunkciója vagy a szuperegó morális, erkölcsi szabályoktól mentes állapota az idben kitörni vágyó késztetések gátlástalan érvényesülését idézheti elő, ami a cybertérben szexuális motivációra épülő erőszakos magatartásban végződhet. A szexuális devianciák okainak feltárására irányuló pszichológiai kutatások szerint a gyermekekkel létesített szexuális kapcsolatokban a felnőtt vagy fiatalkorú szereplők cselekvései részben a gyermekkori szexuális fejlődési rendellenességekben gyökereznek. Olyan gyermekkori történésekkel állnak kapcsolatban, amelyek negatív módon befolyásolják a felnőtt vagy fiatalkori szexuális életvitelt (YOUNG 2011, 57.). Ha a szocializációs szakaszban a szülők szexuális nevelése túlzottan korlátozza, tiltja, sőt bünteti a gyermek szexuális érdeklődését, a másneműekkel való játékot vagy a szexuális megnyilvánulások gyermekkori próbálkozásait, később a szexuális feszültség fantáziák nélkül keres levezetődést, vagy elfojtás alá kerül, és más formában kerül felszínre (BUDA 2002, 110.). A szexuális fejlődési rendellenesség felől közelítő perspektíva összhangban áll Marshall és Barbee integrált elméletével, amely szerint az erőszakoló felnőtt olyan abuzív, elhanyagoló környezetben nőtt fel, amelyre az intimitásszegénység és a szexizmus volt a jellemző. A negatív fejlődési élmény gyermekkorban internalizálódott, és felnőtt- vagy fiatalkorban abnormális magatartásmintákban manifesztálódik. Marshall és Barbee szerint a cselekvések abból is eredeztethetők, hogy a serdülőkorban a fiatal nem tanulja meg az agresszív és a szexuális impulzusok elkülönítését és helyes alkalmazását (VIRÁG–KULCSÁR–ROSTA 2016, 576.). A kontrollelméletekre épülő cyberkutatások némelyike arra is rámutat, hogy a konform felhasználók agresszív feszültségeinek levezetését szabályozó kontrolltényezők hatása elveszti erejét, és különböző normasértő magatartások formájában jelenik meg.

2.6.9. Az agresszív és a szexuális normasértések mintázatai a cybertérben

Az agresszív megnyilvánulások igen gyakran a *személyek közötti* érdek-összeütközésekkel és *belső* feszültségekkel hozhatók kapcsolatba. Az *intraperszonális* feszültségekből fakadó negatív érzelmek az önközpontú gondolkodás vagy a kognitív tévesztések külvilág számára is látható formái. Erre példa a depresszív állapotban vagy ellenséges hangulatban szörfölgető egyén viselkedése, amikor egy semleges tartalmat ellenségesnek értelmez, magára vonatkoztat. Ezzel szemben *az interperszonális* konfliktusokból adódó agresszív magatartások a felhasználók legszélesebb körét érintik, és különböző súlyúak – a kommunikációs szabályok legenyhébb megsértésétől (káromkodás) a jogsértő magatartásokig (lelki erőszak). Napjainkban egyre gyakrabban szembesülhetünk olyan virtuális bántalmazásokkal, amelyekben két ellentétes irányú agresszió együtthatása ismerhető fel. A támadó heteroagressziója, valamint a megtámadott önmaga ellen irányuló autoagressziója

egy irányba haladva, egymást felerősítve fejtik ki hatásukat. A cyberbullying öndestruktív magatartásban végződő esetei lehetnek ilyen erőhatások produktumai, amikor a depresszív lelkialkatú egyén a saját maga ellen irányuló agresszív késztetései és a külső agresszív támadások együttesével már nem tud megküzdeni, és a menekülést választja. Egy depresszív lelkialkatú internetező fiatalnak az őt megalázó, önbecsülését sértő támadás sokkal nagyobb nyomást jelent, mint egy egészséges önbecsülésű fiatalnak, aki énvédő mechanizmusait hatásosabban tudja mozgósítani.

Berkowitz (1989) szerint negatív érzelmek a mindennapi ingerek hatására keletkeznek, amelyeknek az egyén hosszabb-rövidebb ideig hordozója. Az ilyen mindennapos agresszív érzelmek *a düh, a harag, a gyűlölet, az irigység* és a *féltékenység,* amelyek különböző súlyú agresszív megnyilvánulások, köztük az erőszak előzményei (Hárdi 2010, 42–46.). A cybertérben felfedezhető agresszióérzelmek a féltékenységből közzétett intim videók, az irigységből posztolt lejáró szöveges tartalmak, a düh által ösztönzött heves viták, a gyűlöletkeltő közösségi interakciók erőszakos megnyilvánulások katalizátorai és a mindennapos kommunikáció részei. Olyan, általánosan jelen lévő feszültségek, amelyek nem feltétlenül kapcsolódnak személyiségzavarhoz vagy más, bonyolult patológiás kórképekhez. Tehát a legtöbb hétköznapi agresszív cselekvésforma inkább általános felhasználói attribútumhoz társítható, és nem determinált személyiségű internetezőkhöz. Mindenesetre a berkowitzi negatív érzelmek megfelelő kiindulási pontot jelentenek az agresszív vagy erőszakos magatartások hatásainak feltárásához.

Korábban utaltunk rá, hogy a mindennapi agresszív megnyilvánulások lehetnek instrumentális jellegűek, főként ha erőszakos magatartásként manifesztálódnak. Az *instrumentális agresszió* vagy *instrumentális erőszak* valaminek a megszerzésére, uralására szolgál, lehet a versengés vagy éppen vagyon elleni normasértések eszköze (Smith–Mackie–Claypool 2016, 652.). A korábban szintén tárgyalt *reaktív agresszió* viszont olyan érzelmi feszültség esetén lép fel, amely leginkább a konfliktusos cselekvések hátterében áll. Az *instrumentális* és a *reaktív* agresszió közt a legnagyobb különbség, hogy az előbbi esetében egy hosszabb tervezési és döntési folyamat áll, míg a másiknál ugyanez a szakasz jóval rövidebb. Ezért a cybertérben az instrumentális agresszióra jellemző, hogy a zsarolás és a zaklatás eszköze, míg a becsületcsorbító, trágár megnyilvánulások valójában reaktív cselekvések eredményei, és inkább hirtelen fellángolásból történnek. Mindkétfajta agresszió negatív érzelmek hatására keletkezik, azonban az instrumentális formája negatívabb társadalmi megítélésű eredménnyel jár, és alapja a szándékos károkozásnak is (Smith–Mackie–Claypool 2016, 653.). A cyberkörnyezetben észlelhető magatartások épp az agresszió instrumentális és reaktív formái mentén tipizálhatók a legpontosabban, ugyanis a normasértő szándékát pontosabban fejezik ki. Erich Fromm az *instrumentális* és a *reaktív agressziót* rossz és jó szándékú megnyilvánulásokként *malignus* és *benignus* kategóriába sorolta (Fromm 2001). A *benignus agresszió* csoportjába helyezte az *alkalmi agressziót,* amikor az egyénnek nem áll feltétlenül szándékában károkozás, és a *védekező agressziót,* amely nemcsak az emberek, hanem az állatok magatartásában is megnyilvánul közvetlen támadásra, fenyegetettségre. Végül a saját érdek- és önérvényesítés eszközének, de még *benignusnak* tartotta az *önérvényesítő agressziót.* A *malignus* kategóriába emelte a *bosszút,* amely a történelem folyamán a mai napig része egyes szubkultúráknak, a kegyetlenséget, brutalitást kifejező *szadizmust,* a kínzással, megalázással és fájdalom okozásával örömet és kielégülést nyújtó *mazochizmust.* A *malignus agresszió* csoportosításánál tárgyalja az *agresszív fantáziálást,* amikor valaki súlyos sérelmet

szenved egy konfliktusban, viszont abban a helyzetben nem, de álmaiban vagy képzeletében újból lejátssza a történéseket, és elképzeli a sérelem elkerülésére történő helyes viselkedést (FROMM 1974, 185–426.). Ha a cybertérben zajló negatív magatartásformák vizsgálatában csak a Fromm által megfogalmazott védekező agresszióból, a bosszúból vagy az agresszív fantáziálásból indulunk ki, már akkor is sokféle magatartás okaira tudnánk rámutatni a konfliktusos párbeszédtől a legnagyobb kárt okozó rendszerfeltörésekig. Példának okáért a bosszút gyakran helyezik a hackercselekmények és a cyberbullying hátterébe.

Az agresszió céltudatos és szándékos formájaként ismert fenyegetés vagy a rendszeres megfélemlítés olykor azért zajlik a cybertérben, mert a hagyományos környezetben külső akadályai (hatósági szabályozás, fizikai távolság, erőfölény) vagy belső gátjai vannak (félelem, komplexusok, kiközösítettség érzése, tehetetlenségérzés). Dollard és Miller *frusztráció-agresszió elmélete* szerint, ha az egyént szükségleteinek, céljainak elérésében megakadályozzák, belső érzelmi feszültségei keletkeznek, ami agresszív megnyilvánulásokban törhet ki. Nem mindegy, hogy milyen fontos célokról van szó, az akadályoztatás azok elérésének melyik fázisában és milyen gyakran történik, ugyanis ezek a szempontok az agresszió erejét illetően meghatározók. Dollard és Miller arra jut, hogy a frusztrációra elég gyakran agresszió a válasz, de nem minden esetben (BERKOWITZ 1989, 59–72.). A cyberdevianciák hátterében legalább annyi hétköznapi megnyilvánulást találunk, mint berkowitzi agresszív érzelmek esetén (BERKOWITZ 1989). Elég, ha egy csalódott egyetemista felhasználó posztjára utalunk, amelyben durva szavakkal szidja vagy fenyegeti a vizsgáztató bizottság tagjait, miután megbukott. A frusztráció kiváltó ingerei mindkét térben keletkezhetnek, ezek közül a legmarkánsabb a kiközösítés, az elutasítás, az önérvényesítés és az önkifejezés akadályozása vagy az internetes közösségek verbális provokációja.

Az agresszív érzelmekben gyökerező feszültségek okozta normasértésekre Robert Agnew amerikai szociológus *általános feszültségelmélete (general strain theory – GST)* is rávilágít. Az egyén bármely negatív életesemény hatására feszült helyzetbe kerülhet, aminek következményeként deviáns megoldási modelleket választhat. A feszültség adódhat a pozitív ingerek elvesztéséből (például szerelmi válság, barát halála), negatív ingerek hatására (például rosszindulatú fizikai vagy verbális támadás), a célok megakadályozásával vagy igazságtalansággal (például frusztrációt kiváltó ingerek). Agnew szerint a feszültség agresszív magatartásokhoz, erőszakos cselekményekhez és más bűncselekményekhez is vezethet mindazon felül, hogy a sebezhetőséget is növeli. A feszültségelmélet részben magyarázhatja a cyberdevianciákat, főként az agresszív motivációk által ösztönzötteket. Tudnunk kell azonban, hogy a belső és környezeti hatások nem minden esetben késztetik az egyént deviáns magatartásra (AGNEW 2001, 319–361.).

Az agresszió cybertérbeli megjelenéseit Leroy McFarlane és Paul Bocij cyberzaklatókra alkalmazott megfigyelései jól tükrözik. A *bosszúálló zaklatók (vindictive cyberstalker)* a legveszélyesebbek, ők avatkoznak bele a legerősebben a célszemély életébe a többi zaklatóhoz képest. A normasértés legsúlyosabb formáit követik el, a számítástechnikai rendszerintegritás elleni bűncselekményektől (például trójai programok telepítésével történő adatszerzés) a legsúlyosabb fizikai erőszakig. A cyberfenyegetés különféle módjait választják az e-mail-levelezőrendszerek és más információs rendszerek (mobiltelefon) felhasználásával, hogy még személyesebb legyen. Heterogén közösséget alkotnak, a pszichés zavarokban szenvedőktől a képzett számítástechnikai szakemberekig változatos tagsággal. A bosszúálló zaklatók körében sokan vannak magas társadalmi státuszú személyek,

akik a zaklatás mozzanatait a legnagyobb precizitással valósítják meg. A *szervezett vagy felkészült zaklatók (composed cyberstalker)* ezzel szemben kevésbé impulzívak, inkább megfontolt elkövetők, de a fenyegetés és a rendszeres zaklatás részükről is gyakori. Inkább instrumentális agresszió vagy erőszak jellemzi őket, és sokkal markánsabb korlátok között fejtik ki tevékenységüket, amely gyakran kötődik haszonszerzéshez vagy szexuális motivációhoz. A *bizalmas vagy intim zaklatók (intimate cyberstalker)* kétféle alcsoportra oszthatók. Vannak, akik a már létező viszonyra építve próbálnak kapcsolatot teremteni a célszeméllyel, miközben ennek más úton akadályai adódnak. Ilyen például, amikor a baráti kapcsolatokban az egyik fél részéről erős érzelmi kötődés alakul ki. A bizalmas vagy intim zaklatók másik alcsoportjába a látens érzelmek által ösztönzött zaklató személyiség sorolható, akit a sértett nem ismer. A zaklató téves észlelései révén (vagy egyoldalúan mély érzelmi kötődése folytán) rendszeresen, invazív módon közeledik a másik félhez (lásd erotománia). A *közösségi zaklatók (collective cyberstalker)* tevékenységét a cyberbullying jelenségével lehet a legjobban példázni, amikor egy közösség lép fel egy személlyel szemben. A bosszúálló zaklatókhoz hasonlóan az agresszió és az erőszak különféle formája ebben a csoportban is gyakori (Pittaro 2011, 286.).

Az egyénre irányuló veszélyek közül az agresszivitással együtt fellépő legnagyobb kockázatot a *szexuális ösztönkésztetésekből eredeztethető viselkedésformák* jelentik, amelyek gyakran a konform felhasználókhoz köthetők. Az internetes szexualitás okainak feltárását célzó vizsgálatok eredményei szerint a szexuális tartalmú oldalak látogatása és a szexuális fantáziák köré kialakuló közösségek működése olyan tényezőkkel áll szoros kapcsolatban, mint a *szexuális fantázia szárnyalásának szabadsága, az internetes működés korlátlansága, a szabad hozzáférhetőség, a megfizethetőség és az anonimitás.* A gyűjtőoldalakat és interaktív közösségeket épp ezekből a tényezőkből adódóan nemcsak szexuális és személyiségzavarban szenvedők látogatják, hanem azok a konform felhasználók is, akik ilyen módon a mindennapokban felgyülemlő feszültségeiket vezetik le (Cooper 1998). A konform felhasználók cybertérben mutatott szexuális viselkedésének megváltozására az Amerikai Egyesült Államok hatóságai által az ezredforduló időszakában letartóztatott, gyermekkorúakkal intim kapcsolatba került 22 felnőttel végzett átfogó kutatás eredményei mutattak rá. A vizsgálatot végző pszichológusok egy ötfázisú függőségi modellt állítottak fel, majd a láncolatba fűződő fázisokon keresztül levezették, hogy egy konform felhasználó miként juthat el a szexuális tartalmú oldalak véletlenszerű látogatásától a gyermek-felnőtt kapcsolatról való fantáziáláson át a *legszélsőségesebb kényszeres állapotba.*

A modell első fázisa a *felfedezés,* amelyben a felhasználók – gyakran egészen véletlenül – megtalálják azokat a webhelyeket, ahol pornográf tartalmakra (köztük gyermekeket ábrázoló tartalmakra), illetve szexuális töltetű beszélgetőfórumokra találnak. A felfedezés a konform felhasználóban egyfajta izgalmi feszültséget alakít ki, kíváncsivá teszi őt. A hétköznapitól eltérő élmények felerősítik a kalandvágyat, és további látogatásokra ösztönöznek. Egyre több visszatérés után a felhasználó átlép a *felderítés* fázisába, ahol kapcsolatokat keres és talál, immár aktív interakciókba kezd. A szexuális szokásokról folyó párbeszéd felszabadítja a mélyen nyugvó feszültségeit, egyre szabadabbá, könnyedebbé teszi, s így perverz, a szokványostól eltérő, gyermek-felnőtt kapcsolatokról szóló fantáziálásokba kezd. Az *eszkaláció* fázisában a szélsőséges fantáziálás nyújtotta élvezet és izgalom még több látogatásra és aktív részvételre készteti a felhasználót, aki hagyományos szokásait elhagyja, és szabadidejének nagy részét internetes kalandozásokra fordítja, rituális csevegésekbe

kezd, fantáziakapcsolatokat köt, önkielégítést végez, és lassan, de biztosan kialakul a függőség. A negyedik szakasz a felhasználó életvitelét befolyásoló *kényszer vagy kényszeresség* fázisa. A virtuális szexualitás és a köré fonódó fantáziavilág rendszeres és meghatározó része lesz a napi rutinnak, a kényszeres ragaszkodás megváltoztatja a valós társas kapcsolatokat, levezeti a feszültségeket, időlegesen feloldja a szorongásokat. A kényszer fázisában már rendszeres felnőtt-gyermek fantáziálásokon alapuló kapcsolatok szövődnek, de megvalósulhat a fizikai érintkezés is. Az ötödik fázis *a kétségbeesés vagy reménytelenség szakasza,* ahol a felhasználó ráismer saját addiktív állapotára. Tehetetlenségérzése mellett próbál menekülni függőségéből, törli a szolgáltatásokat, eltávolítja a számítástechnikai eszközöket, de gyakran sikertelenül (YOUNG 2011, 59–63.).

Az ötfázisú modell egy magyarázat a szexuális motivációra épülő internetes addikció kialakulására, mindamellett rámutat a magatartások mögött rejlő hétköznapi feszültségekből adódó kockázatokra. *A kutatás alanyainak egy része az interjúkban intimitáshiányra, párkapcsolati stresszre, munkahelyi frusztrációra, internetfüggőségre hivatkozott, és arra is kitért, hogy más szerektől – mint az alkohol és a kábítószer – is addiktív életvitelt kezdtek élni.* A kutatás lényeges eredménye, hogy a hétköznapi stressz levezetése vagy a rendszertelen szexuális élet folytán felerősödő késztetések a gyanútlan felhasználót is kényszeres látogatóvá tehetik, pontosabban az addikció kialakulását eredményezhetik. Az ötfázisú modell elméletéhez több hasonló kutatás is kapcsolódott, amelyekben a cyberszex interaktív folyamatában zajló kommunikációt specifikus kapcsolatnak értékelik, a résztvevőket fantáziafelhasználóknak definiálják. A kapcsolat specialitása a kutatók szerint abban áll, hogy a felhasználók szexuális fantáziája szabadon szárnyalhat, és ezt bátran megoszthatják másokkal, vagyis az internet olyan fantáziaeffektek szabad megjeleníthetőségének terepe, ahol az egyén mindennapi feszültségei és szorongásai oldódnak. A szexuális impulzivitás kontrollnélkülisége mélyen nyugvó ösztönkésztetéseket szabadít fel, ami állandó visszatérésre motiválja a résztvevőt, cselekvéseit kényszeressé teszi (DURKIN–BRYANT 1995). A virtuális környezetre irányuló további elméletek szerint az anonimitás lehetőségével a személyiség átformálódhat, és képes az offline működésétől eltérő nemi identitást *(gender swapping)* és magatartásformát felvenni, amivel átlépi morális határait *(flexible morality)* (TURKLE 2005; DURKIN–BRYANT 1995). A normasértés hátterében álló további sajátosság lehet a virtuális környezet személytelenségében kialakított *képernyőarc-effektus,* amely a valóságérzékelést és a gátlásokat elfedi, az egyént immunissá teszi tetteinek következményeivel szemben, miközben a védelem illúzióját teremti meg (PARTI 2009).

Az elméleti megközelítések a szexuális kalandozások okozati összefüggései közül az internetfüggőséget emelik ki, egyben mint az intenzív internetes szexuális élet következményét. Valamennyi függőségre és cyberszexre irányuló kutatási eredmény tartalmazza azt a megállapítást, hogy az a felhasználó, aki egyébként sok időt tölt az interneten, nagy eséllyel talál rá ösztönző oldalakra, és kerül még mélyebb függőségi helyzetbe. Az internetfüggő felhasználók köre heterogén, már ami a társadalmi státuszt és a kriminalitást illeti, ugyanis a szexuális témájú internetes csevegőoldalak kényszeres látogatói sokan magas társadalmi státuszú személyek, akik kiszorultak a rendszeres szexuális életből, az erotika és az intimitás világában elszigeteltek, ugyanakkor előéletüknek egyáltalán nem volt része a kriminalitás. A fantázia és az anonimitás által megváltozott normasértőt függősége mindezen túl nemcsak a szexuális megnyilvánulásokra, hanem más erőszakos magatartásokra is kapacitálja (YOUNG 2011).

A súlyosabb internetes szexuális devianciákat magyarázó elméletek némelyike azonban konzekvensen kitart amellett, hogy az effajta virtuális magatartásformák *személyiségzavarban vagy súlyosabb szexuális zavarban szenvedő felhasználókra,* vagy azokra jellemző, akiknek a *bűnözés az életük része volt* (Mitchell–Finkelhor–Wolak 2003). A cyberdevianciák pszichés betegségeken alapuló és gyakori epizódja a zaklató figyelemfelhívás, amely a tartalmak rendszeres és mániás küldözgetésében merül ki. A magatartás egyes formái mögött megbúvó okok egyike a *szerelmi téboly* (erotománia, más néven *Clérambault-szindróma*), ami a paranoia egyik megnyilvánulása. Az erotomániás zaklató abban a téveszmében él, hogy a másik személy (aki lehet magasabb társadalmi státuszú is) mély érzelmeket táplál iránta (Ozsváth 2011). A pszichiátriai szakirodalmak az erotomániát a normálistól eltérő túlzott szexualitással is azonosítják, amely önmagában magyarázat lehet a pornográf oldalak látogatására, a perverz fantáziálásokra és alapvetően a zaklató viselkedésre (Pléh–Boros 2010, 98.; Pittaro, 2011). Az erotomániából fakadó névtelen zaklatások az internetes zaklatások jelentős részét képezik, és legtöbbször ismert, sőt közismert személyek szerepelnek az áldozati oldalon. Az erotomániás zaklatók az esetek többségében az anonimitás álcája mögé bújnak, cselekvéseik kiterjedhetnek a számítástechnikai rendszerintegritás-sértésekre, például a kiszemelt célpont információs rendszereiben tárolt tartalmak megszerzésére is. A rendszerfeltörések már megfelelő súlyú cyberdevianciák (bűntettek) ahhoz, hogy az áldozat feljelentést tegyen, és a hatóságok segítségét kérje, de a hosszú megfigyelést igénylő nyomozás sem garantálja a sikert.

A szerelmi tébolyon kívül további pszichés betegség is szerepel a kriminális cyberdevianciák mögött, mint a társadalom és a kontrollintézmények azonnali reakcióját kiváltó pedofil felhasználók cselekvései. A cybertérben zajló pedofília úgy is definiálható, mint *a gyermekkorú felhasználókkal való szexuális kapcsolat létesítésének céljából, vagy azokkal kapcsolatos szexuális szükségletek kielégítéséért a cybertérben folytatott akciók vagy interakciók összessége.* A pedofília a szexuális vágy kielégítésének azon formája, amely nem tartozik a társadalmilag elfogadott magatartásminták közé. A pszichiátriai szakirodalom szerint a pedofil személy gyermekkorúakkal (serdületlen személyekkel) folytat szexuális tevékenységet, vagy ilyen tevékenységek látványa kelt benne szexuális késztetést, izgató fantáziát (Ozsváth 2011). A pedofília megnyilvánulásait a másik nemhez tartozó egyenrangú személy közelségétől való szorongáskeltő, fenyegető hatás is kiválthatja. A pedofil férfiak általában nem mernek közel kerülni szexuálisan érett partnerekhez, vagy ha mégis, szorongásuk folytán feszültté válnak, a szexuális aktus kudarcba fullad. Egyenrangú kapcsolatok elől menekülve csak a gyermekekkel szemben vállalják szükségleteiket, ami a kisebbségi komplexusok alóli feloldódást eredményezi, ezáltal a hatalmi fölényt sikeresen érvényesítik (Buda 2002, 197–198.). A cyberpedofília jelenségéhez illeszthető a parafília további három formája: a mások szexuális aktusait rejtőzködve figyelő maszturbációs tevékenység *(vojőrizmus),* a fizikai kapcsolatot helyettesítő és a fiatalok körében korábban népszerű „távszex" *(telefonszkatológia),* illetve a szexuális éretlenségben gyökerező nemiszervmutogatás, amely a szexting egyik formája lehet *(exhibicionizmus).* A pedofil felhasználók a cybertérben a gyermekekről készült pornográf képi anyagokat tartalmazó weboldalak és az internetes fantáziaközösségek rendszeres látogatói. Aktív gyermek-felnőtt kapcsolatok kialakítása céljából a behálózás technikáját, a zsarolás, a zaklatás módszerét alkalmazhatják, tartalmak készítésének, kereskedelmének szereplői lehetnek.

David Finkelhor szerint a pedofil személy gyermekkorúakkal szemben alkalmazott szexuális kizsákmányolásának négy előfeltétele van. Az első a *motiváció,* ami a szexuális szükségletek és a gyermeki jellemzők összeegyeztethetőségéből, a gyermekek iránt érzett szexuális izgalomból és az elfogadott egészséges szexuális élettel és azok szereplőivel szembeni gátlásokból alakul ki. A második a *belső gátak* leküzdésére való törekvés, ami valójában az elkövető gyermekekkel folytatott szexuális kapcsolatának kialakítását megelőző félelmeinek, szorongásainak és feszültségeinek elnyomását jelenti. A harmadik a *külső gátak* leküzdése, ami a fizikai kapcsolat útjába álló ismerős védőbástyákat, iskolai vagy más társadalmi kapcsolatok által megtestesülő kontrollközösségek elkerülését vagy kijátszását, a gyermek és a pedofil közötti fizikai akadályok elhárítását testesíti meg. A negyedik a *fizikai ellenállás leküzdése,* (a belső gátlások és a külső gátak megszűnését követően) a gyermek ellenállásának fizikai erőszakkal, manipulációval, meggyőzéssel vagy más befolyásoló technikával való megtörése, majd a szexuális kapcsolat beteljesítése (VIRÁG–KULCSÁR–ROSTA 2016, 575.).

Finkelhor elmélete a cyberpedofíliára is ráilleszthető azzal a különbséggel, hogy virtuális térben a pedofil és a gyermek között a közvetlen elérési út biztosított, vagyis átíveli a külső akadályokat, az anonimitás támogatásával csökkenti a lelepleződési kockázatokat. A cybertérben a fizikai ellenállás leküzdésére nem minden esetben van szükség, olykor elég a szexuális tartalmú kép, videó kikényszerítése és azok látványa a szexuális feszültségek levezetéséhez. A pedofil felhasználó kapcsolatszerzését és -működését a társas és a társkereső oldalak, az illegális szolgáltatásokhoz való hozzájutást biztosító weboldalak megkönnyítik.

2.6.10. Normasértő közösségek a cybertérben

A cybertérben szerveződő normasértő közösségek felépítésük, működésük, kiterjedésük és a deviáns magatartások súlyát tekintve számos szempont alapján csoportosíthatók. Fejezetünkben az extrém csoportok és a terrorszervezetek, a cyberbullying formációinak és az internetes közösségekből álló véleménynyilvánító csoportoknak a bemutatására és működésük egyfajta magyarázatára vállalkozunk.

2.6.10.1. Extrémista csoportok

A cyberkollektívák legveszélyesebb formációit kétségkívül a szélsőséges csoportok és a terrorszervezetek alkotják. Az efféle közösségek kialakítására az online toborzás a legpraktikusabb, amelynek folyamatában a belépő fél hosszú ideig megőrizheti anonimitását, és szabadon érvényesülhet. A szervezők nemzeti, vallási vagy más, identitással összefüggő elemeket jelenítenek meg a virtuális közösségbe tartozás előnyeiről, az egységességről, amelyet több csatornán és platformon érvényesítenek. A közösségi szellem olyan tagoknak is kedvez, akiket más csoportokból kiközösítettek, vagy akik máshol nem kapják meg a kellő érzelmi támogatást, és sikertelenek. Egyes extrémista csoportok a gyűlöletet helyezik ideológiájuk középpontjába, ezért olyan felhasználók szimpátiáját is kiváltják, *akiknek személyes beállítódásai között szerepel az erőszak.* A közösségek ideologizálásának módszerei az ellenségkép, a bűnbakképzés, a biztonság hiányának skandálása és más népcsoportok

kriminalizálása. A szerveződésekre jellemző, hogy köreikben a bizalom megnyerésével, az ellenséges attitűdök megerősítésével és az erőszakos fellépés mintáinak bemutatásával mozgósítható, erőszakos egyén formálódik (Kiss 2014, 82–92.). Mivel a hosszabb távra szerveződő homogén közösségek cselekvéseire a virtuális környezet csak egy új terep, ami nem változtatta meg a kialakulásuk okairól eddig összegyűjtött ismereteket, ezért képződésük gyökereit a hagyományos elméletek szerint mutatjuk be.

A szélsőségességet az erről szóló elméletek egy része az etnocentrizmusból, a sztereotipizálásból és az előítéletességből eredezteti. Kai Theodor Erikson szerint minden közösséget *határfenntartó* tulajdonsága tesz egyedivé. A határok azonban nemcsak a szó szoros értelemben vett földrajzi vonalakat jelentik, hanem olyan kulturális szférát, ahol a tagok létrehozzák közös normarendszerüket, kialakítják együttélésük szabályait, megformálják kultúrájukat (Erikson 1966). A közösség a tagjától azt várja el, hogy igazodjon a normáihoz, vegyen részt azok védelmében, konfrontálódjon a normahatárok átlépőivel. Az egyén így átveszi a közösség kultúrájának mintázatát, és ebben a cselekvéskörben működik tovább. A csoporttal való túlzott azonosulás *etnocentrizmushoz* vezethet, ami gyakran jár együtt a saját csoport kultúrájának felmagasztalásával és a másik közösség kultúrájának elutasításával. A csoport tagjainak egymás iránti pozitív érzelmei felerősödnek, kialakul a *„mi" tudat,* ami torzíthatja a *másik csoporthoz tartozók* észlelését, és elősegítheti többek között a „*mi"* és az „*ők"* közötti ellentét kialakulását. A közösség tagjaira a bajtársiasság, az összetartozás érzése, az eszméknek történő alárendelődés lesz jellemző. Az énközpontúságot és az egoizmust felváltja a csoportközpontúság, ami nem csupán a szolidaritást és a lojalitást jelenti, hanem a *másik közösséggel történő tartós szembehelyezkedést* is. Az egyén a csoportközpontúság jegyében arra is törekszik, hogy a csoporttársairól alkotott képet javítsa, másokat pedig ezzel együtt leértékeljen. A felmagasztalást és a leértékelést a csoport hiedelmei, eszmerendszere, ideológiái, a közös célok, jutalmak és vélemények egyöntetűsége támogatja, ami könnyen *csoportpolarizációhoz,* elköteleződéshez vezethet (Beck A. 1999, 197.).

Ha a közösség csupán saját csoportján belül folytat interakciókat, és csak a közösség tagjainak egységes álláspontjára támaszkodik, miközben nem vesz figyelembe más nézőpontokat, nem egyeztet másképp gondolkodó egyénekkel, akkor egységesen szélsőséges nézetek irányába sodródik. A közös álláspont ebben az esetben még értékesebb és érvényesebb lesz számukra, mint addig volt (Smith–Mackie–Claypool 2016, 674.). A közösségek a tagok gondolkodását és érzéseit összehangolják, és a másik csoporttal szemben megalkotják a sztereotípiákat. *Sztereotípiáról* akkor beszélhetünk, ha az észlelő a személyek észlelésekor a beérkező adatokat összehasonlítja a már meglévő *személysémáival* (amelyek vonatkozhatnak tulajdonságokra, külső jegyekre vagy akár egy embertípusra is), következésképpen az észlelő a reálistól eltérő, pontatlan kép alapján ítél vagy cselekszik. Csepeli György szerint a sztereotipizálás egy *megismerési térkép,* amely az empirikusan megalapozott igazságot ugyan nem nélkülözi, de szubjektív valószínűségi értékítéletekkel, oktulajdonításokkal átszőtt torzképet eredményezhet (Csepeli 1990, 24.). Beck szerint a sztereotipizálás más közösségekhez tartozók egységes jellemzőinek kiemelését jelenti (Beck 1999, 10.). Ahogy az egyén egy közösséget vallási, faji vagy más alapon körülhatárol, annak tagjait egyszerre egymással behelyettesíthetőnek is véli. Allport szerint a sztereotipizálás azt jelenti, hogy az emberi elme kategóriákban gondolkodik, és ha kialakította kategóriáit, azok a normális ítélet (előítélet) alapjait képezik (Allport 1977).

A cyberközösségekben uralkodó negatív sztereotípiák az egyén hagyományos kontextusban *már létező* és a virtuális közösségben *megalkotott* gondolkodási sémáinak összessége. Az előbbi esetben a virtuális körbe belépő egyén sztereotípiái megegyeznek azokkal, amelyeket a csoport többi tagja is működtet. Megalkotott sémák esetében a belépést követően a virtuális csoport hatására alakulnak ki vagy formálódnak a sztereotípiák. A sztereotipizálás az alapja a másikról kialakult helytelen megítélésnek és a negatív viszonyulásoknak (ALLPORT 1977, 281–282.). Ha a csoport tagja a sztereotipizáláson túl a másik közösség tagjával szemben negatív érzelmi attitűdöt alakít ki, akkor *negatív előítéletről* beszélünk, amelyhez gyakran kapcsolódik egy sémaszerűen felállított érvrendszer, amellyel az előítéletes ember folyton igazolhatja önmagát, alátámaszthatja cselekvésének helyességét, a másikról való (hamis) tudás megdönthetetlenségét. A negatív attitűdök által meghatározott online csoport tagjának szemében saját közössége mindenható, nem képes rosszat cselekedni, ellentétben a másikkal, amelynek mozzanatai minden esetben rosszak. Az előítéletesség Gordon Alport által felvázolt fokozatai a *szóbeli megnyilvánulásoktól* az *elkerülésen,* a *hátrányos megkülönböztetésen* és a *testi erőszakon* keresztül szélsőséges esetben az adott csoport *kiirtásáig* terjed (ALLPORT 1977, 47–61.).

A cyberkörnyezetben előforduló előítéletes magatartások ráilleszthetők az alporti előítéletesség-fokozatokra. A verbális sértegetés és a legkegyetlenebb erőszakos cselekvés mozgatórugójaként is értelmezhető előítéletesség akkor válik igazán veszélyessé, amikor a negatív érzelmek szavakban kifejezve cselekvést formáló és mozgósító erővé válnak (CSEPELI 1990, 24.). Ha a polarizált közösségekben zajló interakció megkeményedik és előítéletességgel társul (például rasszizmus), akkor a csoport szélsőséges szerveződésként működik tovább. A szélsőséges viszonyban álló közösségek nagyságuk és összetételük szerint a családi kis csoporttól különböző etnikai közösségeken és nemzetiségi csoportokon át az államhatalommal rendelkező nemzetekig terjedhetnek. A szélsőséges közösségre jellemző a bosszúállás (lásd: Anonymus hackerközösség). Nem minden esetben az áll bosszút, aki sérelmet szenvedett, és nem minden esetben az szenvedi el a bosszú eredményét, aki a sérelmet közvetlenül okozta. Az ilyen agresszív cselekvést *vikariáló bosszúnak* nevezik (SMITH–MACKIE–CLAYPOOL 2016, 678.).

A szélsőséges polarizált csoportokra jellemző, hogy a feszültség elnyomja a józan gondolkodás képességét, ezért a reaktív agresszió és erőszak nyer teret cselekvéseikben. Ebben a helyzetben a berkowitzi agresszióérzelmek és a Dollard–Miller-féle frusztráció-agresszió elmélet gyakran érvényesül (BERKOWITZ 1989). A csoporttagok beszűkült gondolkodása kizárólag az előítéletekre támaszkodik. A csoportok közti konfrontáció során az egyénben nem csupán a saját magára irányuló veszély tudatosul, hanem a csoportra ható fenyegetettség is, így cselekvését eszerint alakítja. A csoport érdekében fellépő egyén destruktív cselekvését követő belső morális nyomást a csoportjutalom (például bátorítás, ösztönzés, dicséret) ellensúlyozza, és helyes cselekvésként erősíti meg, vagyis az *operáns kondicionálás* is része a közösség működésének. A negatív torzítás azon kívül is az egyén személyiségének része lehet, hogy ennek tudatában lenne, és hatna rá a csoport ereje. Ha egy másik ember nem a közösség attribútumait hordozza, személyes értékítélettel, hiedelmekkel összeegyeztethetetlen (például eltérő bőrszín, testi jellemzők, nyelv, vallás), nagyon gyorsan a „jó" vagy a „rossz" kategóriák egyikébe kerülhet, vagyis az automatikus negatív értékelés funkciója érvényesül, ami minden ember személyiségeleme. A jó vagy rossz kategóriába sorolást néhányan dualisztikus gondolkodásnak tekintik, mások

a depressziós, szorongó, paranoiás betegek jellemzőjeként említik (Beck A. 1999, 209.). Milton Rokeach amerikai szociálpszichológus a vizsgálatainak eredményeiből azt szűrte le, hogy az előítéletes egyénekre egyfajta *zárt gondolkodás* jellemző (Beck A. 1999, 210.). Ez alapvetően merevséget, impulzív, azonnali véleménynyilvánításra való hajlamot, az ellentmondókkal szembeni intoleranciát, más emberekkel szembeni nehéz megértést, a valóság eltorzítását és eltúlzását foglalja magában. A zárt gondolkodású egyén markáns hiedelmekkel rendelkezik, gyakran magányos, jellemző rá a tehetetlenség és a problémamegoldásra való képtelenség.[39] A szélsőséges közösségek körében tekintélytisztelet uralkodik, és a csoport nyomására az ideológiák *merevvé* válnak. A zárt és merev gondolkodás nagyon szoros összefüggésben áll a vallási fanatizmussal, a kognitív torzítással és az extrémizmussal, ugyanakkor a csoporthatás olyan hosszan tartó, destruktív érzelem kialakítására és konzerválására is képes, mint a gyűlölet.

2.6.10.2. Terrorista csoportok

A gyűlölet további ellenséges attitűdök kialakítását generálja, ami a gyűlöletcsoportok és a terrorszervezetek működését támogatja, az egyént gátlástalan cselekvésekre ösztönzi. Az elvont ideológiák mentén megfogalmazott célok mindenek feletti tisztelete, a közösség eszmerendszerének elvakult követése a terrorszervezetek működésének alapja. A közösségek működése a technikai fejlődéssel és a globális hálózatosodással még inkább konzerválhatóvá, földrajzi meghatározhatósága pedig megfoghatatlanná válik. A szerveződések virtuális megjelenésének megakadályozása ma már egyre több társadalom elsődleges törekvése, amit nehezítenek a lokalizálhatatlan szerverek és a párhuzamos online-offline működés.

A terrorista sejtek különbözőképpen hasznosíthatják az internetet. Legkézenfekvőbb, hogy az online kommunikációs csatornákat – e-mail, online hirdetőtábla *(bulletin board)* – használják a szervezeten belüli kapcsolattartásra (Shelley 2003). Ennek előnyei, amilyen az anonimitás, a rejtve maradás és ezáltal a biztonság garantálása, itt is megjelennek. A terrorista csoportok az internetet előszeretettel használják adománygyűjtésre is, direkt vagy indirekt felhívás formájában. Az utóbbi online csalás formájában történik: jótékonysági szervezeteknek tulajdonított weboldalakon tesznek közzé számlaszámokat, amelyekre átutalva a pénz a nemlétező szervezetek helyett a terrorista sejt számlájára érkezik (Weimann 2004).

Az internet a szervezett bűnözői csoportok számára a belső kapcsolattartáson túl számos lehetőséget kínál, így például a propaganda terjesztésére, a nagyobb publicitás elérésére, valamint a támogatók és az önkéntes „katonák" toborzására. Az internet lehetővé teszi a világon mindenütt a potenciális utánpótlást biztosító, az önmegvalósítás lehetőségeit kereső tinédzserek gyors és olcsó elérését. A legutóbbi elemzések szerint a terrorista-extrémista csoportok könnyű prédái a nyugati világ fiataljai, akik egyszerű, egyértelmű, ugyanakkor szélsőséges üzeneteket, karizmatikus vezetőket keresnek (Reitman 2015). Farah Pandith,

[39] A cyberközösségek zárt csoportjaiban a tagok gyakran nem ismerik a csoportot létrehozó személyt, de egymást sem, és működésük közben sem lépnek egymással közvetlen kapcsolatba, hanem a csoportot összetartó ideológia mentén cselekszenek.

az Egyesült Államok Külkapcsolati Tanácsának ISIS-szakértője szerint az ISIS mára egy tinédzserek körében népszerű brandet alakított ki: „Az iszlám [olyan, mint a] punk rock, a fejsál szabaddá tesz, a szakáll pedig szexi" (TOLAN 2015).

2.6.10.3. Hacktivizmus és cyberhadviselés

A cybertérben szerveződött extrém csoportok magatartás-mintázatait sokan szoros összefüggésbe hozzák a hackelés politikai és ideológiai irányba való elmozdulásával. Történik ez annak ellenére, hogy a hackerek etikai szabályaikban politikai céloktól mentes működést követelnek meg egymástól. A számítástechnikai ismeretekben képzett szakemberek által kifejlesztett eszközöket (szoftvereket, kódokat) politikai, társadalmi aktivisták virtuális tiltakozásokra, ellenállásra használhatják az interneten és más információs rendszerekben (például virtuális blokádok, túlterheléses támadások, e-mail-bombák) (JORDAN–TAYLOR 2004). A hacktivizmus formái így váltak a társadalmakon belüli és a társadalmak közötti konfliktusok eszközeivé, amelyek segítségével kormányoldalakat blokkolnak, rendszereket befolyásolnak vagy csupán a kommunikáció megzavarását végzik. A hackerek szolgálatait a kisebb politikai befolyással rendelkező államok is felhasználják, mégpedig úgy, hogy a technológiailag fejlett államok internetdependenciáját használják ki. A cybertámadások kritikusinfrastruktúra-szervereket béníthatnak meg, amilyen a közlekedés, az áruszállítás, az energiaellátás vagy a telekommunikáció (SHARMA 2010). Ugyanezeket az eszközöket terrorszervezetek és a társadalmi-politikai rend ellen tiltakozó civil mozgalmak is felhasználhatják arra, hogy valamely politikai szereplőre nyomást gyakoroljanak (VERTON 2003). Államok hadseregei és nemzetbiztonsági szolgálatai támadnak meg hackingtechnikák eszközével valamely ellenséges államot, annak kormányzati szervereit, valamint állampolgárait. A *kiberhadviselésnek (cyberwarfare)* nevezett jelenség keretében számítástechnikai rendszereket állítanak le napokra, megbénítva ezzel a kormányzatot és a közigazgatást.

2010-ben emlékezetes hackertámadás volt az iráni nukleáris erőművek elleni Stuxnet akció, amelynek keretében az Amerikai Egyesült Államok és Izrael hadserege kártékony szoftvert jutatott be iráni szerverekbe. 2015-ben az Egyesült Államok titkosszolgálata, az NSA elismerte, hogy Kínában gyártott számítástechnikai eszközök kártékony szoftverrel való megfertőzésével sikerült bejutnia számos ország kormányzati szervereibe, ahol aztán a szoftvereket igény szerint élesítették, és a megfigyelést vagy a cybertámadást beindíthatták (GREENWALD 2015).

A hacktivista műveleteket idővel virtuális terrorizmusnak tekintették, ami nem áll messze az igazságtól, ugyanis a módszereket a terrorszervezetek is a céljaikhoz tudták illeszteni, hiszen a válogatás nélküli károkozás, a félelem és a rettegés kiváltása virtuális úton is megvalósulhat. A hacktivista módszerek alkalmazása ebben a kontextusban a legnagyobb támadás előidézésére lett képes. A terrorszervezetek virtuális cselekvésekkel kiemelkedően fontos infrastruktúrák működését biztosító kereskedelmi, hírközlési, pénzügyi rendszerek befolyásolására képesek mindazon felül, hogy a módszerek a haszonszerzést, az anonimitást, a toborzást, a szervezést, a tervezést, a koordinációt és a kooperációt is lehetővé teszik, továbbá a virtuális és fizikai erőszak támogatására, előkészítésére képesek.

2.6.10.4. Politikai töltetű civil demonstrációk

Az online platformok gyors és hatékony lehetőséget biztosítanak a hasonló érdeklődési körű felhasználók közösséggé formálására és megmozdulások szervezésére, beleértve a politikai töltetű, illetve a fennálló rezsim megdöntésére irányuló *demonstrációkat* is.

2005-ben Kínában nagy felháborodást keltett, hogy a japán kormány kiadott egy könyvet, amelyben a japán megszálló hadsereget Kína felszabadítójaként tüntette fel (Xiangwei 2005). A két ország közötti évszázados ellentétekhez járulnak hozzá még azok az erkölcsileg elítélendő akciók is, amelyek a két ország morális-kulturális eltéréseiből fakadnak. 2003-ban japán üzletemberek kínai hotelekben megrendezett orgiáitól voltak hangosak a kínai chatszobák, és az online kezdeményezést hamarosan tettek követték, amelyek során az emberek az utcára vonultak, és a japán üzleti befektetők kivonulását követelték. Kínában ez nem az első, de nem is az utolsó japánellenes megmozdulás, amely az online közösségi oldalakon szerveződött, és amelynek következményeként japán tulajdonosok üzleteit törték föl, és japánellenes tüntetések szerveződtek online – a helyi rendőri erők teljes tudomásával, sőt asszisztálásával (Huang 2012).

2.6.10.5. A cyberbullying jelenség

A cybertérben zajló közösségi zaklatást úgy lehetne összefoglalni, mint *olyan kép, videó, szöveg, gif, internetes mém, tartalmakkal vagy aktív kommunikációval megvalósított, negatív érzelmeken alapuló, rendszeresen ismétlődő károkozó magatartások összessége, amelyek a közösségtől az egyén ellen irányulnak, közvetett módon sérthetnek információs rendszereket, és pszichés erőszak előidézésére alkalmasak, de akár fizikai erőszak formájában is megnyilvánulhatnak.* Az effajta normasértések egyik leggyakoribb vetülete a fiatal korosztályba tartozó felhasználók körében előforduló cyberbullying. A cyberbullying hagyományos formáját az erről szóló kriminológiai irodalom a lelki, fizikai vagy anyagi kárt okozó erőszakos vagy más szándékos normasértések körébe sorolja, és iskolai környezetben, az iskolai élettel összefüggésben, az oktatási intézmény szereplői közt zajló direkt és indirekt agresszió valamelyikeként definiálja. A direkt agresszió nyílt támadásként manifesztálódik fizikai és pszichikai erőszak vagy más károkozó akció formájában, az indirekt agresszió pedig közvetett destruktív cselekvésként, amely inkább burkolt és közvetett módon a célkeresztben álló személy szociális környezetét érinti, és kapcsolatrendszerének lerombolását jelenti (Virág–Kulcsár–Rosta 2016, 587–589.). A cyberbullyingnak más tudományos megfogalmazások szerint három kötelező eleme van:

- ártó szándékú támadás, félelemkeltés, fenyegetés vagy kényszerítés;
- egyenlőtlen erőpozíciókon nyugszik;
- hosszabb időn keresztül rendszeresen ismétlődik (Olweus 1993; Olweus 1999; Farrington 1993).

A cyberbullying folyamatában az erőszak pszichikai formája érvényesül. Ennek ellenére az információs rendszerek megsértése és a jogosulatlan adatkezelés is egyfajta károkozásnak minősül, ami ha nem is kézzel fogható tárgy sérülését, megsemmisülését jelenti, de mégis ugyanazt a hatást éri el. A cybertér ugyanakkor a *korlátlan elérhetőséggel* a közösségi

nyomásgyakorlás lehetőségét és a sebezhetőséget, *nagyobb nyilvánossággal* az önbecsülésre gyakorolt nyomást, az *anonimitással* a destruktív cselekményekre ösztönzést támogatja, vagyis *katalizáló* szerepet tölt be a közösségi bántalmazás folyamatában. A cyberbullying jelenségéről egyes kutatások úgy számolnak be, hogy az csupán az iskolai erőszak egy virtuális térbe kiterjesztett alakzata és egy újabb eszköz a bántalmazók eszköztárában, de nem minősül markánsan elkülönülő új jelenségnek (WOLKE–LEE–GUY 2017). A kutatók ezirányú megállapítása lényeges abból a szempontból, hogy a közösségi erőszak virtuális és offline folyamata legtöbbször egy komplex láncolatba fűződik. A közösségi cselekvések színterein zajló eseményekben jól elkülöníthető, de egymást kiegészítő szerepek formálódnak az aktív bántalmazótól a bántalmazást támogatókon át a passzív szemlélőkig, akik a közösségi platformokon is hasonló státuszban maradnak, mint az azt megelőző vagy épp azt követő offline kontextusban. A bántalmazó magatartás oksági magyarázatai arra következtetnek, hogy a virtuális térben a közösségi erőszak az erőfölényhez való hozzáférésnek, a hatalmi egyensúly és a dominancia fenntartásának és érvényesítésének az eszköze. Mások szerint ez a motiváció a fiatal férfiakkal szemben a társadalmi elvárásként megfogalmazható kényszermaszkulinitásból *(forced masculinity)* eredeztethető, amelynek során a fiatal férfi az erőszakos viselkedésben látja a szerepelvárásnak való megfelelés lehetőségét (WOLKE–LEE–GUY 2017; YAR 2006, 31.).

A fiatalok virtuális térben tanúsított bántalmazó magatartását gyakran vezetik vissza az antiszociális személyiségzavarra, a szocializációs problémákra, az identitáskereső korszak morális mélypontjára, az érzelmi jólét hiányára, a túlzott agresszivitásra vagy egész egyszerűen az erőszak alkalmazásának lehetőségére, amelyben a bántalmazó kihasználja az adódó alkalmat erőfölénye érvényesítésére. A cyberbullying folyamatában a *passzív résztvevők* (néma szemlélők) fontos szerepet játszanak. Az erőszakos viselkedésre adott passzív közösségi reakció John Darley és Bibb Latané amerikai szociálpszichológusok elmélete szerint a *bystander-hatásnak* köszönhető (HUDSON–BRUCKMAN 2004). Ennek lényege, hogy ha egy negatív esemény (például erőszak) bekövetkezésének helyszínén minél több segíteni képes személy tartózkodik, annál kisebb az esély arra, hogy bárki a tömegből az áldozatnak segítséget nyújt, vagy a negatív történést elhárítja. A kutatók a bystander-hatás ellenőrzésére – főleg egyetemisták körében – számos kísérletet végeztek. Azt állították, hogy a közösség tagjait nem a megtorlástól való félelem és az apátia tartja távol a cselekvéstől, hanem a csoport tagjai gátolják egymást. Minden egyes személy megpróbálja értékelni a veszély forrásait, és ezzel egyidejűleg a többi résztvevő értelmezéseit, miközben senki nem reagál a történtekre. Ez a folyamat az egyéni próbálkozásokat, a helyzet azonnali megoldására vagy segítségnyújtásra irányuló pozitív reakciót és cselekvést lelassítja, sőt a cselekvésről való döntést blokkolhatja. A közösségben az egyén effajta viselkedéséhez Darley és Latané szerint négy mechanizmus járul hozzá:

- Az *öntudatosság,* amely az egyén attól a negatív megítélésétől való félelme, amelyet a lehetséges segítő cselekvéséről a közösség többi tagja kialakíthat.
- A *társadalmi jelek* mechanizmusa, ami mások tétlenségéből fakadó egyéni tétlenségbe torkollik, vagyis egymás tétlenségét mint társadalmi jeleket látva senki sem cselekszik.
- A *blokkolás* mechanizmusa több ember egy időben történő cselekvési szándéktól adódó visszalépését, cselekvési blokkolódást jelent.

- Végül az *átlátható felelősség* mechanizmusa arra mutat rá, hogy az egyéni felelősség a csoportban legyengül, és a cselekvés ennek okán elmarad. A négy mechanizmus aktivizálódásával a közösség tagja a negatív esemény helyszínén kívülálló szerepében tétlenül marad. A bystander hatás logikája a cyberbullying közösségi dinamikájában is értelmezhető, de leginkább a passzív résztvevők oldaláról. Ők azok, akik az agresszív vagy erőszakos normasértések elkövetőjének pszichés támogatói és tevékenységük abban destruktív, hogy nem tesznek semmit az áldozat védelmében, végignézik a bántalmazó önkényes műveleteit. (Hudson–Bruckman 2004, 168–171).

A közösségi erőszak dinamikájának megértését célzó kutatásokból az áldozati magatartás vizsgálatát sem felejtették ki. A klasszikus magyarázatok, mint az alacsony önértékelés, a depresszió, a konfliktuskezelési képesség alacsony foka, az ártalmakkal szembeni immunitás gyengesége mellett egy lényeges tényező az áldozatok többségénél kiemelhető, mégpedig a *kimaradástól való félelem (fear of missing out* – FOMO*).* A FOMO-jelenség értelmezésében a kortársközösségek tagjai a közösségben maradás alapvető feltételének tartják, hogy állandóan részesei legyenek a kortárscsoportban zajló információáramlásnak. A bent maradás iránti erős egyéni szükségletet más generációs elvárás is erősíti, amilyen a *trendkövetés,* amelyről már korábban írtunk. A folyamatos kapcsolatban maradásért az egyén mindent megtesz, még az ezzel együtt járó kellemetlenségeket is elviseli, példának okáért a közösségi nyomást. A FOMO-jelenség arra a központi kérdésre ad választ, hogy miért nem lép ki a bántalmazott abból a virtuális közegből, ahol őt támadás éri (Przybylski et al. 2013, 1844.).

2.6.10.6. Az internetes mémek (i-mémek)

A közösségi normasértések további típusa valamely közfelháborodást vagy elégedetlenséget kiváltó eseményre, döntésre, cselekvésre történő tömeges reakció, azaz egy vélemény internetes mém formájában való kivetülése. *Az internetes mém a felhasználók által az információs technológia segítségével készített, internetes felületeken közzétett, felhasználói közvetítéssel terjedő videó-, kép-, hang- és írott tartalmak különböző változataiból, hiperhivatkozásokból, illetve ezek kombinációjából álló, gyakran változó jelentésű, általában rövid, pozitív vagy negatív üzenettartalmú, módosított vagy valós tényeket megjelenítő digitális információs egység* (Kiss–Parti 2016, 39.). Az internetes mémek természetét leginkább Richard Dawkins mémdiskurzusa magyarázza (Dawkins 2011). Dawkins „mémelméletében" a kultúra terjedése és az evolúció folyamata közti összefüggést vizsgálva arra a következtetésre jutott, hogy a gének másolódása és a gondolkodás elemeit alkotó kulturális egységek terjedése közt hasonlóságok fedezhetők fel. A mémek mint kulturális egységcsomagok a *replikátorok* segítségével, utánzással másolódnak és terjednek emberről emberre. A gének mutálódásához hasonlóan folyamatosan alakulnak, gyakran megváltozott formájukban másolódnak – ezzel gazdagítva és megőrizve a kultúrát. Dawkins a vallási tanok és ideológiák fennmaradását is a mémek működésének tulajdonította, és az evolúcióhoz hasonlóan terjedésükre automatikus folyamatként tekintett, amit később számos kritika ért. A memetika tudománya a mémeket továbbra is az emberi kultúra

szükséges részének tekinti azzal a felismeréssel, hogy terjedésüket maga az ember szabályozza, az nem autonóm folyamat eredménye.

A 20. század végén egyre szélesebb körben elterjedt internetes hálózat megteremtette a mémek új birodalmát, és életre keltette a dawkinsi elmélet tárgyának virtuális változatát, az internetes mémeket. Mivel az internetes információs egységek komplex információtartalma, terjedése, tárolhatósága a dawkinsi mémekéhez áll a legközelebb, ezért a köztudatba internetes mém elnevezéssel vonult be. Az internetes mémeket a közösségi önkifejezésre, illetve a közéleti reflexióra alkalmas funkciójuk tette igen széles körben népszerű közlési formává, ami a web 2.0 tartalmak előretörésével teljesedett ki a jelenleg tapasztalható formában. További sajátosságuk, hogy a nyelvi sokszínűség és a technikai környezet (megjeleníthetőség, terjeszthetőség, tárolhatóság) révén megőrizhetik a virtuális közösségek értékeit, szokásait, hagyományait vagy akár ideológiáit. Az internetes mém földrajzi határok nélkül bármit népszerűsíthet, lehet párbeszéd vagy konfliktus kifejezőeszköze, tartalmazhat társadalmi eseményhez kötődő vagy közéleti vonatkozású információt, de a tartalma nem feszítheti szét azokat a kereteket, amelyeket maga az internetes közösség neki tulajdonít. Kapacitását alapvetően a gyors közlésre alkalmas, közérthető, nagy tömegeket érintő lényegi információ mérete szabja meg, ezáltal válik lehetővé gyors terjedése. Az internetes mémek további sajátossága, hogy tömeges értékítéletet fejeznek ki, a közösségi véleménynyilvánítás eszközei, ezért terjedésük is nagyobb dinamizmust feltételez. Összetettségük révén sokszor felerősítik az értékítéletben rejlő sértő elemeket, így *arra is alkalmasak, hogy durva torzításokat, egyénre vagy közösségre vonatkozó valótlan tényeket és kifejezéseket közvetítsenek* (KISS–PARTI 2016, 9.). Ettől függetlenül az internetes mémek mégiscsak a szólás- és véleményszabadság leginkább védett eszközei, és káros mivoltuk csak abban a formában nyer értelmet, amennyiben az egyénnek vagy épp egy másik közösségnek való károkozásra irányulnak, vagyis *károkozó internetes mémekként* működnek (KISS–PARTI 2016, 9.). A károkozó internetes mémek által hordozott tartalmak hátterében az emberi méltóság megsértésének szándéka áll, és célkeresztjükben bármilyen természetes személy állhat, aki nem csak virtuális entitással (azaz nem csak kitalált internetes karakterrel) rendelkezik. Az effajta internetes mémekben azok a szövegtartalommal ellátott képek vagy karikatúrák jelennek meg, amelyek a sértett egyént vagy közösséget kínos kontextusban ábrázolják, és ebben a környezetben az érintett és a nyilvánosság számára is egyértelműen felismerhetők. Lényeges, hogy olyan azonosítható testi jellegzetességre (arc) vagy személyiségjegyekre, cselekedetekre utaljanak, amelyek felismerhetővé és azonosíthatóvá teszik az egyént. Negatív internetes mémek tartalmaként gyakran alkalmazzák a gifeket.

Az interneten megjelenő káros mémtartalmakhoz *nem kapcsolódik egyértelműen sem negatív társadalmi megítélés, sem pedig jogi felelősségre vonás*. A retorzió elmaradásának több oka lehet, amit részben a címzett passzivitásával, másrészt a tömeges internetes megjelenésből és az adatok rejtettségéből adódó *anonimitással* lehet magyarázni. Az internetes mémek káros hatásáról való közgondolkodás is idesorolható, vagyis a tartalmak büntetendő jellegéről, káros hatásáról való kollektív tudomás vagy tudatlanság. Ez azt jelenti, hogy a tömeg tisztában van-e a terjesztett tartalom sértő jellegével vagy sem. Ha nem, akkor a destruktív kollektív cselekvés miatt a felelősség az internetes mém készítőjére vagy legfeljebb első közzétevőjére redukálható. Ha igen, akkor egy olyan kollektív egyetértésen alapuló nyílt normasértésről van szó, amelynek negatív hatásával minden

résztvevő tisztában van. A további magyarázat a tartalom eltérő kulturális és büntetőjogi megítélése közti különbségben rejlik. Amíg például az Amerikai Egyesült Államok internetes platformjain közzétett internetes mém még viccesnek számít, addig ugyanaz más államokban elítélt, sőt büntetendő lehet. Noha egyes bűncselekmények tekintetében a bűnügyi együttműködésről szóló egyezmények tartalmazzák az államok hatóságainak közös fellépését, a jogi környezetek túlzott eltérősége kellő akadály az együttműködésre. Ha az államok büntetőjogi normái mégis egységesek lennének, még akkor is nehézségeket okozna a készítés pontos földrajzi helyének megállapítása és a készítő azonosítása.

Végül idetartozik még az internetszolgáltatók felelőssége, azaz a káros tartalmak tárolása, megjelenítése és terjesztése, technikai korlátozásának kötelezettsége. Vannak olyan internetes tartalmak, amelyek a devianciák *feketezónájába* sorolhatók, törlésük, vagy legalább elérhetőségük korlátozása a szolgáltatók részéről kötelező. Jelentős számban maradnak azonban olyan információs egységek, amelyek elérhetőségkorlátozása csak akkor történik meg, ha azt a sértett egyén vagy közösség kéri. Ebből arra lehet következtetni, hogy egyes internetes mémek az érintett döntése és nem a tartalmuk valódi üzenete miatt kerülnek normasértő vagy épp nem normasértő kategóriába. Ha egy i-mémre a sértett nem reagál, és ezáltal kikerül a hivatalosan szankcionálandó magatartások köréből, annak valójában még megmarad az önbecsülést sértő üzenete, vagyis normasértő jellege. Az online színtéren keringő sértő információkat tartalmazó mémek – hasonlóan egyes offline magatartásokhoz – közösségi reakciók internetes formáiként is értelmezhetők. A hálózatban terjedő, önbecsülést sértő tartalmak iskolapéldája a politikai szereplőket megjelenítő internetes mém, amely egy kevésbé népszerű politikai döntés vagy politikusi megnyilvánulás következményeként születik. Az ilyen információs egységek egyértelműen a döntést démonizálják, és a politikai közszereplő karakterisztikájára utalnak torzított, humoros, néha megalázó formában. A humor szintén központi eleme a mémnek; ilyenkor a mém a politikai döntések, a társadalmi disszonanciák, az egyes etnikai, vallási, kulturális vagy nemi identitást képviselő csoportokkal szembeni intolerancia társadalmi feldolgozásának az eszköze, vagyis a konfliktusok olyan instant megjelenési formája, amely alkalmat teremt társadalmi viták kibontakozására és lefolytatására (Kiss–Parti 2016).

A mémekkel történő kollektív cselekvésre vonatkozó kérdésekre első ránézésre Howard S. Becker kollektív normasértésről alkotott tézise adhat választ. Becker úgy fogalmazott, hogy az emberek, miközben együtt cselekednek, egymás tevékenységét figyelve hozzáigazítják önmaguk tevékenységét a többiekéhez, mint ahogy a többiek is igazodnak a kollektíva együttes cselekvéséhez. A közösség által elkövetett normasértés a közösség tagjainak interakcióin alapul, ami nem feltétlenül jelent személyes, szemtől szemben lezajló találkozást, de egy olyan „kommunikációt" igen, amely a tagok közti kölcsönhatást létrehozza, és lehet a kollektív elkövetésre való ösztönzés. Ahogy létezik kollektív együttműködés, úgy kollektív normasértés is, amelyben minden egyes tagnak részt kell vennie. Becker szerint a kollektív devianciának az adhat igazán teret, amikor a devianciát senki sem tekinti annak, ami. Mindezt azért teszik, mert túl nagy gonddal járna a deviáns magatartások elleni fellépés, vagy limitált erőforrás áll rendelkezésre ahhoz, hogy a deviáns egyéneket üldözzék vagy felelősségre vonják (Becker 1963, 19–72.). Becker gondolatait azzal kiegészítve lehet az internetes kollektív cselekvéshez igazítani, hogy a folyamatban pont a sértett döntése határozza meg az intézményi reakciót, azaz a törvényes eljárások megindítását, majd a kollektív magatartás normasértő jellegét.

A kollektív deviancia internetes környezetben való értelmezésénél felmerül a kérdés, hogy van-e különbség a kollektíva tagjainak egyéni hajlamai között, vagy együttműködésük hasonlóképp érvényesül, mint a Becker által felvázolt kollektív deviancia esetében (KISS–PARTI 2016).

Az online társadalom résztvevői egyenként különböző tagságot (pozíciót) töltenek be az cybertársadalomban. A tagság közösségi elfogadottsága, véleményformáló ereje az internetes aktivitástól és az egyén tulajdonságainak, tapasztalatainak, ismereteinek, attitűdjeinek, előítéletének, érzelmi és kulturális beállítódásának összességétől, azaz *egyéni diszpozícióitól* függ. Ha egy internetes mém népszerű, és terjedése dinamikus, akkor okkal feltételezhető, hogy kifejez egy olyan kollektív igazságot, amellyel az internetes közösség tagjai egyetértenek és azonosulnak. Ha ez így van, akkor a károkozó mém terjedése esetében is elmondható, hogy a közösség tagjai egyetértenek az aktuálisan terjesztett információs egység normasértő elemeivel, és egységesen követnek el egy-egy normasértést. Ahogy a hagyományos térben szervezett tüntetés esetében is az egyetértés nem minden résztvevő szempontjából jelenti ugyanazt attól függetlenül, hogy valamennyien részt vesznek a tüntetésen.

Mivel az internetes mémek az egyénekből álló kollektív cselekvés folytán terjednek, fontos, hogy az egyén milyen alternatívák alapján dönt a terjesztésükről. A döntésben meghatározó tényező a tartalom megfelelő értelmezése és az ezt követő reakció. Utaltunk már George Herbert Mead elméletére (1973), amely szerint az észlelt dolog és a reakciók között eltérések lehetnek. Ha Mead tézisét a negatív internetes mémek terjedésére ültetjük át, akkor úgy tűnhet, hogy a kollektíva tagjának terjesztésről kialakított döntése és célja az általa kreált jelentéstartalomtól függ, ami a szélsőséges ideológiákat valló terjesztők között a közös negatív sztereotípiák mentén történik. A heterogén csoportokban a hasonló jelentéstartalom olyan közös sémákból ered, amelyek a csoport tagjainak eltérő gondolkodásától függetlenül mindenkiben megvannak. Lehet úgy is fogalmazni, hogy a heterogén csoportokban a káros internetes mémek terjesztése a csoport valamilyen fontos értékrendszerét sértő ingerre adott válasz, és nem egy kialakult negatív sémarendszerből képzett egységes jelentéstartalomra történő reakció (KISS–PARTI 2016).

Az internetes mémek terjedésének természete Durkheim társadalmi tényekről írott gondolataival is társítható. A szociológus *társadalmi áramlatoknak* nevezte a kollektíva azon megmozdulásait, amelyek a lelkesedés, fölháborodás és a szánalom érzelmi hullámain keletkeznek, és nem az egyéni tudatból fakadnak, de az egyént mégis magukkal sodorják. A közösség ereje egy olyan csoportnyomás, amelynek az egyén nem bír ellenállni (NÉMEDI 2005, 39.). Az internetes mém a durkheimi értelmezés szerint a véleményáramlatok olyan kifejezőeszköze, amely mindig a kollektíva által fontosnak tartott vélemények, kritikák, trendek irányába tereli az egyént. A negatív internetes mémeket terjesztő kollektívák között ezért differenciálódás figyelhető meg, ha a készítését és nyilvánosságra hozatalát megalapozó okokat és az egységek célkeresztjében álló közösségeket együtt vizsgáljuk.

Vannak olyan információs egységek, amelyek egy homogén társadalmi csoport irányából egy másik társadalmi csoport irányába haladnak sértő célzattal, vagyis ezek a két csoport között kialakult negatív viszonyulás virtuális leképeződései. Az effajta i-mémek iránymutatást adhatnak arról, hogy egy kisebbséget vagy valamely más meghatározottsággal rendelkező közösséget milyen előítéletek, sztereotípiák lengenek körül. A társadalmi csoportok közt terjedő internetes mém egyik iskolapéldája a homoszexuális közösségről készült vagy az etnikai kisebbségeket karikírozó információs egység. Nehéz lenne elképzelni, hogy

a hagyományos színtéren már létező közösségek nemzeti, etnikai vonatkozású viszonyulásai előbb-utóbb ne képeződjenek le valamilyen formában a cybertérben is. Természetesen mindezt nemcsak az i-mémek testesíthetik meg, de egy közösség kulturális különbségeit, etnocentrizmusát, előítéleteit és negatív érzelmeinek különféle formáit épp a vizuális és verbális megjelenítés komplex alakzata képes optimálisan kifejezni (Kiss–Parti 2016).

A másik kategóriába a nagyobb, heterogén összetételű tömeg irányából a hatalmi struktúra felső fokán álló döntéshozók felé irányuló negatív internetes mémek tartoznak. Ezek többnyire többségi véleménynyilvánítások, de mindenképp valamilyen inger hatására megjelenő, reaktív, tömeges cselekvés termékei, amelyeket egy heterogén kollektíva vesz körül (Kiss–Parti 2016).

A kollektív terjesztés résztvevői egységesek abban az értelemben, ami a kollektív normasértést mint célt és a közös fellépést illeti, de különbözők abban, ami az egyén reakciót kiváltó hatáshoz való viszonyulását illeti. A negatív tartalmú internetes mém terjedésének dinamikája és iránya magában hordozza a terjesztésében szerepet vállaló közösség morális határait, előítéleteit, sztereotípiáit, tartalmazza az egyén és a közösség kulturális beállítódását és lelkiállapotát. Annak megállapítása, hogy egy társadalomban az internetes mém információtartalma normasértő-e vagy sem, sokkal inkább a készítésében és a terjesztésében részt vevők, illetve a megcélzott egyén vagy közösség értékítélete határozza meg, semmint a tartalmakat szabályozó, illetve az egyént és a közösség jogait védő jogi normák (Kiss–Parti 2016).

2.7. A cyberdevianciák pozitív funkciói

Már több mint egy évszázada elfogadott tézis, hogy a devianciának a társadalomra nézve nem csupán negatív hatásai vannak. A deviancia olyan megszokottól való elhajlásként is értelmezhető, amely egy társadalom működésének rigiditását feloldva a fejlődés irányába mutat, megerősíti és tudatosítja a társadalmi szabályokat, kijelöli a normarendszer határait, kihangsúlyozza a kontrollintézmények működésének hiányosságait, vagyis pozitív funkciókkal rendelkezik. Emile Durkheim a 19. század végén arról írt, hogy a bűnözés minden társadalom része, és ha az elfogadott magatartásmintákhoz képest nincs túlsúlyban, normális jelenségként definiálható (Gönczöl–Kerezsi 1993, 10.). A cybertér olyan új környezet, amelyben a devianciák korábbi és új formái is megjelennek, ezért a pozitív funkciók meghatározása több szempontból is érdekes lehet.

A virtuális tér önmagában eltér a hagyományostól: azzal, hogy korlátozottabb megnyilvánulási lehetőségeket kínál, képes a deviáns magatartások konzerválására, szabályozhatóságában és a normasértések definiálhatóságában pedig jóval nagyobb kihívást jelent. A cybertérben kirajzolódó súlyos normasértéseknek viszont megvan az a pozitív tulajdonságuk, hogy közvetlenül nem kell tartani fizikai kivetüléseiktől. Pozitív funkcióik a motivációkkal együtt járó feszültségek levezetésének lehetőségében ragadhatók meg. Gyakran tapasztalható, hogy a negatív érzelmek, mint a frusztráció, a harag, a düh, a bosszú vagy a gyűlölet egy internetes posztolással, egy heves vitával, elektronikus levelezésben vagy cyberközösségek belső interakcióiban levezetődnek, további megnyilvánulásra már nem kerül sor, vagy ha mégis, annak csak enyhébb formájára lehet számítani. A megnyilvánulások legsúlyosabb formája ennek ellenére maradhat a pszichés erőszak szintjén,

de fizikai formáira sokkal kisebb az esély. Ugyanez elmondható a szexuális feszültségek levezetésével kapcsolatosan is. A pornográf oldalak látogatásával vagy a nehezen elérhető weboldalakon zajló interaktív fórumokon számos olyan szexuális feszültség enyhítésére van lehetőség, amely akár fizikai abúzus formájában is megjelenhetne. A szexuális szükségletek kielégítésének anonim lehetőségei például azoknak kedveznek, akik elszigetelten élnek, párkapcsolatok kialakításában sikertelenebbek, szexuális életük nem teljes. Ők a tartalmak használatán felül virtuális kapcsolatokat is kialakíthatnak, ahol anonimitásba burkolózva szexuális fantáziájukat érvényesíthetik. Természetesen mindvégig szem előtt kell tartani, hogy a pornográf tartalmakban gyakran valós emberek szerepelnek, akik valahol, valamikor valóságos kiszolgáltatott, megalázott helyzetbe kerültek. A fiatalkorúak szexuális fejlődésének, szexuális érdeklődésének szakaszában meghatározó az online szexualitást közvetítő platformok szerepe – ami akkor optimális, ha az efféle oldalak vagy platformok nem tartalmaznak erőszakos forgatókönyveket.

Az internetes mémekkel történő kollektív véleménynyilvánításnak akkor van igazán pozitív szerepe, amikor egy társadalmi felháborodás eszköze. Arról ugyan még nem végeztek kellő mélységű és számú kutatást, hogy az internetes mémek pontosan milyen súlyos és tömeges megmozdulás megelőzésében dominánsak, de arra minden bizonnyal lehet következtetni, hogy a kritikai véleményformálás azonnalisága egy biztonságiszelep-funkciót képez a kollektív érzelmi vihar kezelésében.

A szabad tartalommegosztással olyan emberi megnyilvánulások látnak napvilágot, amelyek annak ellenére, hogy normasértők, a közösség egy része előtt negatív mintaként szolgálnak. A negatív tartalommegosztásra történő felhasználói reakció kifejezetten fontos az adott magatartásról alkotott egyéni attitűdformálásban, vagyis egy káros tartalomra adott nagyszámú negatív reakció formálhatja a tartalmat szemlélő egyén értékítéletét.

A cybertér sokféle deviáns közösség szerveződésének optimális színtere, de emellett olyan multikulturális közösségek kialakulását is lehetővé teszi, ahol a többségi társadalmi normáktól eltérő szemléletű egyén érvényesülése, kötődése biztosított, a szubkultúra egyénre gyakorolt pozitív hatása kifejeződik. A véleménynyilvánítás szabadsága mindenkit megillet, de ha normasértő (önbecsülést sértő, becsületcsorbító), akkor előnyösebb, ha a negatív sztereotípiákból és előítéletekből fakadó feszültségek levezetése hasonló attitűdökkel rendelkező felhasználók között egy zárt, virtuális közösségben marad. Erre a virtuális színtér számos alternatív lehetőséget kínál, ami nemcsak a csatornák és rendszerek rendelkezésre állásában, hanem a szimbólumok különféle megjelenítési lehetőségében is megmutatkozik (például címerkészítés grafikus eszközökkel).

A cybertérnek vannak olyan tulajdonságai, amelyek a konform felhasználókat is káros cselekvésekre ösztönzik, és ezek csak az egyén védendő értékkel kapcsolatos attitűdváltozásainak okait feltáró vizsgálattal deríthetők fel. A normasértések gyakran rávilágítanak arra is, hogy melyek a szabályozatlan szürke foltok. A cyberdevianciák további pozitívuma, hogy képesek prognosztizálni, mely normasértésekkel szemben kezd megváltozni a társadalom rosszalló megítélése, vagyis a deviánsnak számító cselekvések közül melyek azok, amelyeket az új környezetben már egyfajta közöny leng körül (például személyiségi jogok megsértése képek engedély nélküli közzétételével).

Az aktív online lét addiktív életmódot eredményezhet, de ebben az életmódban mindenképp lehetőséget biztosít arra, hogy a dinamikus társas életből kiszorult felhasználók rátaláljanak önmagukra egy új identitás megformálásával. A szegényes szociális kapcsola-

tokból fakadó destruktív állapot a valós identitás újraértelmezésével, a vágyott képernyőarc megformálásával feloldható, esély egy virtuális közösségi kapcsolatrendszer kialakítására.

A cyberdevianciák a multikulturális cybertársadalom viszonyrendszerének rendezésére alkalmas szabályozási eszközök (jogszabályok, társadalmi kontroll) megalkotását és a meglévők folyamatos finomhangolását is szükségessé teszik. A modern kontrolleszközök többféle igényt elégítenek ki, és a multikulturális közösségek harmonikus együttműködésének esélyét teremtik meg.

Vákát oldal

3. A cybertér szabályozása

3.1. Az információ és az ember

Arisztotelész *Metafizikája* szerint az ember tudásra született: „Az emberekben természettől fogva megvan az a vágy, hogy megismerjék a látható dolgok okait" (Arisztotelész, Met. I, 2.). A modern korban már nem bölcsek tanítanak minket, nem előre megszűrt és magyarázott információkat kapunk készen, hanem magunknak kell rátalálnunk az adatok miriádjában a számunkra releváns adattöredékre, továbbá nekünk kell eldöntenünk, mennyire megbízható a talált információ, amely nem önmagában, hanem az információ kiválasztásának, rendszerezésének és validálásának a képességével együtt jelenti a tudást (Cherry 1978, 244.). Az információelmélet a 20. század közepén keletkezett; gondolkodói szerint nem az információ szemantikája, tartalma a lényeges, irreleváns tehát, hogy épp igaz, hamis, fontos vagy haszontalan. Ehelyett az információ kvantitatív elemzése kerül előtérbe, illetve az, hogy az egyes rendszerek alkalmasak-e az információ befogadására, rögzítésére, átvitelére, kódolására és dekódolására. Az információelmélet nemcsak a matematikával és a kommunikációtudománnyal összefüggésben fejlődött, hanem az információ kódolására, rögzítésére és átvitelére alkalmas gépek megjelenésével is (Shannon–Weaver 1949).

Az információ szociokulturális kontextusban viszont nem az átvitelt vagy a hordozhatóságot, hanem az információ emberi értelmezésének képességét jelenti – azaz maga a jel, illetve annak kontextusa a lényeg (Capurro–Hjørland 2003). Ebben az értelmezésben az információ emberi jelenség, amely lehetséges cselekvésekben manifesztálódik (Machlup 1983). Az információ az egyén társadalmi realitásának dimenziója, amely hidat képez az egyén és a külvilág között, vagy másképpen: az egyén és az érdeklődésének tárgya között (Ledermann 2016, 5,12.). Az ember számára érdeklődésre számot tartó dolgoknak értéke van, így arra törekszünk, hogy azt a jog eszközével védjük és szabályozzuk.

A fent bemutatott elméletek mind leképezhetők a mai (digitális) információs társadalomra, de szociotechnológiai dimenzióban az információnak, ha lehet, még komplexebb jelentősége van. Az információs társadalomban az információ a biztonságot és a mindennapok élésének képességét jelenti. Gondoljunk csak az okoseszközökre vagy az okosházak okosberendezéseire, amelyek mind információt közvetítenek az egyén számára. A kritikus infrastruktúrákat számítógépek irányítják. A viselkedésünket számítástechnikai algoritmusok figyelik, amelyek viselkedésünkből tanulnak. Ha elveszítjük valamelyik végtagunkat, kaphatunk egy másikat, amely megtanítja az agyunknak a saját használatát. Az információhoz jutás és annak sebessége gazdasági, kormányzati és politikai szinten befolyásolja az életünket. A tőzsdék online működnek, és a világgazdaság vagy a politika apró változása azonnal visszatükröződik az árfolyamokon. Az ember nélküli repülő tárgyak, a drónok segítségével kifürkészhető és lerombolható valamely távoli objektum. A számítástechnika lehetővé tette a hatalmas adatbázisok létrehozását és összekapcsolhatóságát. A kommu-

nikáció eszközeinek fejlődése megváltoztatta kulturális normáinkat és a viselkedésünket (BELL 2001). Az információ mindenütt jelenlevőségére, könnyű (olcsó) elérhetőségére vezethető vissza a fogalom összekapcsolása különböző jelenségekkel, mint például információs társadalom, információs gazdaság, információs kor (Z. KARVALICS 2007; FUCHS 2008; CASTELLS 2010).

Az információ sokkal több, mint csupán mozgatórugó; árucikké, önmagában vett értékké alakult. A posztmodern információs társadalomban az információkezelők, az információmenedzsmentet végző dolgozók, azaz a programozók, az informatikusok válnak a vezető társadalmi réteggé. Az online közösségi portálokon való gyakori jelenlét könnyű népszerűséget hozhat, ami mindenki számára karnyújtásnyira közel hozza a vágyott tizenöt perc hírnevet. A legutóbbi politikai fejlemények azt mutatják, hogy az online kommunikáció, ha átgondolt koncepció rejlik mögötte, átváltható társadalmi, politikai és gazdasági tőkévé (HILTON 2016).

Az információs korban a jog szerepe is átértékelődik. Nem egyszerűen arról van szó, hogy a jog sokkal lassabban reagál a társadalmi változásokra, mint a technikai fejlődés egy alacsonyabb fokán. Az információs korban új védendő jogtárgyak és értékek jelennek meg, amilyenek például a digitális szerzői jogok vagy az információhoz való jog. A magánélet védelme új értelmezést nyer, és az információt hordozó technikai tér, a cybertér is szabályozásra szorul. A cybertér egy megváltozott szociokulturális közeg, ahol a viselkedés megváltozásának lehetünk tanúi. A változás önmaga a normától való eltérés, azaz a deviancia. A változás katalizátora a technikai fejlődés, amely új viselkedési és szociokulturális sémákat generál.

E fejezetben arra teszünk kísérletet, hogy átfogó képet nyújtsunk az internet szabályozásának konstrukcióiról, az ön- és a központi szabályozás szereplőiről és legfontosabb nemzetközi dokumentumairól. Habár a fejezetben a központi, állami szabályozás produktumaival is foglalkozunk, nem szeretnénk elveszni a jogi keretek sűrűjében, ezért szándékosan nem foglalkozunk az Európai Unió Kiberbiztonsági Stratégiájával és az Európai Biztonság Tervével (Cybersecurity Strategy of the European Union 2013; European Agenda on Security 2015),[40] azok bemutatása meghaladná a tartalmi kereteket.

3.2. Az internet szabályozói

1966-ban egy nyugalmazott brit őrnagy, Paddy Roy Bates beleszeretett egy kicsiny, elhagyatott betontalapzaton álló toronyba az Északi-tengeren. A torony a második világháború alatt lőtoronyként szolgált, innen lőtték a britek a partjaik felé tartó német pilóták gépeit. 1966-ban a tornyot Bates megvette, elnevezte Sealand Hercegségnek, és kinyilvánította függetlenségét az Egyesült Királyságtól, amely a háború után nem tartott igényt a rozsdásodó tákolmányra. Sealandnak színes a története, de senki nem gondolta volna, hogy 1999-ben az internet történelmébe is beírja magát. Ebben az évben adott engedélyt ugyanis Bates egy fiatalember, Ryan Lackey számára arra, hogy a szigetre költözzön, és ott megalapítsa saját cégét, a HavenCo-t. A HavenCo szerverekkel rakta tele a sziget egyetlen épületét,

[40] Az Európai Unió kiberbiztonsági stratégiájáról lásd: https://ec.europa.eu/digital-single-market/en/cybersecurity (A letöltés dátuma: 2018. 05. 15.)

amelyek mikrohullámmal és műhold segítségével kapcsolódtak az internethez (Markoff 2000). Lackey egy cyberpunk novellából vett ötlettől vezérelve internetszolgáltatást ajánlott mindenki számára, aki ki akart kerülni az állam vagy az igazságszolgáltatás látóköréből. Potenciális kliensei között voltak pornográfiaterjesztők, adócsalók, onlineszerencsejáték-szervezők vagy éppen csak függetlenségre szomjazók, a társadalomból kivonulni vágyók. A HavenCo hirdetése szerint ez volt „a világon az első és egyetlen hely, ahol úgy üzletelhetsz, hogy nem leskelődnek a vállad fölött" (Grimmelmann 2012). Lackey hiú ábrándokat kergetett, a HavenCo az 1990-es évek végén bekövetkező internetforradalom apoteózisa maradt, hiszen éppen a fizikai határok védelmével kecsegtetett, aminek az internet korában elveszett a jelentősége. A kormányok hamarosan kiterjesztették fennhatóságukat az offshore internetszolgáltatókra (Goldsmith–Wu 2006, 66.).

Habár kezdetben az internetet, illetve a cyberteret jogon kívüli területnek tekintették, mára számos, sikeres és kevésbé sikeres kísérlet született a szabályozására, illetve a fizikai világ szabályainak a cybertérre való kiterjesztésére.

Technikai, gazdasági, üzleti és jogi komplexitása miatt az internet kibogozhatatlan szövevénynek tűnik. Nemzetközi szervezetek, nemzeti kormányok, tudományos kutatók, cégek és technológiai fejlesztők mind a közös megegyezés kialakításán dolgoznak arra vonatkozóan, ki és hogyan szabályozhatja, illetve védheti meg a cyberteret. Habár széles az egyetértés abban, hogy a kormányok egyedül, a magánszektor (azaz a vállalatok) és a civil társadalom közreműködése nélkül nem képesek szabályozni a cyberteret mint „közjót" *(public good),* amelyből mindenki részesedhet (Benedek 2008, 32.), az továbbra is vitás, hogy mennyiben szükséges bevonódniuk a szabályozásba a magánszereplőknek, és hogy a szabályozás eredményességéhez az iparnak inkább motivációra vagy kötelező erejű szabályokra van-e szüksége.

Az *állami szabályozás felülről jövő (top-down)* kezdeményezést jelent, amely kötelező erejű a gazdasági szereplőkre. Az államok a cyberteret is érintő, illetve ott szerveződő támadások megjelenésével kezdték el megalkotni saját jogszabályaikat a nemzetbiztonság és az állampolgáraik védelmére. A *gazdasági szereplők* a maguk által kifejlesztett, a piaci mozgásokhoz idomuló, *alulról jövő (bottom-up)* rendelkezései – kiegészülve a civil szerveződések által hozzáadott értékekkel – viszont úgy tűnik, inkább biztosítják az internet decentralizált felépítéséhez illeszkedő, többszereplős rendszert, amely hosszú távon szavatolni képes a rendszer biztonságát és a szolgáltatások minőségét. A szabályozási politika kialakítására eddig nem született egységes és egyértelmű válasz. A tanulmányok azonban abban egyetértenek, hogy rendszerezett és valamennyi szereplő bevonásával járó, *ex ante* megoldást kell találni a cyberteret fenyegető incidensek megelőzése érdekében, aminek jóval nagyobb a jelentősége, mint az állam által a bűnözés és a nemzetbiztonságot fenyegető veszélyek új formáira adandó, *ex post* válaszoknak. A másik oldalon nem elegendő kizárólagosan a piac és a magánszféra szereplőire bízni a szabályok kialakítását, hiszen a magánszereplők érdekei különbözők lehetnek, és tevékenységi körük szabja meg a beavatkozás mélységét. A magánszektor nagyon jó az incidenskezelésben és -megelőzésben, de a piac és az állam biztonságos működéséhez az elkövetett visszaélések szankcionálására, ezzel való fenyegetésre is szükség van. Ez utóbbi – a jogszabályok megalkotása, a nyomozások lefolytatása, az igazságszolgáltatás, a védelem és a garanciák eszközeinek lefektetése – a mindenkori hatalom, a kormányok hatáskörébe tartozik (áttekintését lásd: Tropina–Callanan 2015). Az önszabályozó szervezetek bevonásával kialakított többsze-

replős döntéshozatali és menedzsmentmodell további előnye, hogy a technikai fejlődéssel óhatatlanul előálló változásokhoz minden érdekelt bevonásával igazodik. Az önszabályozás ilyen módon elmozdítja a fókuszt a cyberbűnözés és az arra való reaktív fellépés felől a hosszabb távra tervező cyberbiztonság felé, amelyben a proaktív, megelőző szemlélet jut inkább szerephez (17. táblázat).

17. táblázat

Az internet szabályozásának szereplői. Önszabályozó és központi szabályozó szervek

	Önszabályozás (self-regulation)	**Államok, kormányok által lefektetett szabályok, központi szabályozás (central regulation)**
Szereplők	• vállalatok, magánszektor, ipari szereplők, független szakértők, akadémia, kutatók, civil szervezetek és szerveződések	• közigazgatási és kormányzó szervek, a közszektor szereplői, föderális szervek (például Európai Unió)
Jellemzők	• proaktív, megelőző szerep *(ex ante);* • az informatikai és kommunikációs (IKT) hálózatok résztvevőinek önkéntes és evolucionális (a technikai és piaci fejlődés és igények folyamatában kifejlődő) szabályai.	• reagáló, szankcionáló szerep *(ex post);* • kötelező erejű szabályok, amelyek vonatkozhatnak valamely piaci megegyezés magánszektor általi kialakítására (például az Európai Unió NIS-irányelve, 2016) is.
Eszközök, funkciók	• káros és ártalmas tartalmak bejelentése, szűrése, monitorozása; • minőségbiztosítás; • etikai kódexek kidolgozása és érvényesítése; • tanácsadás; • incidenskezelés; • tudatosságnövelés; • információmegosztás; • a válaszadás annál hosszabb időt vesz igénybe, minél több a szereplő.	• jogalkotás; • nyomozás; • igazságszolgáltatás; • szabályegységesítés; • jogi garanciák (panasz- és fellebbezési lehetőségek) lefektetése; • azonnali válaszadás (jogszabályok módosítása, elfogadása).

Forrás: Parti Katalin szerkesztése

Számos példát találhatunk arra, hogy a szabályozás csak akkor sikeres, ha az imént bemutatott két terület, a *köz- és a magánszféra együttműködik (self-regulation + central regulation = co-regulation / guided regulation).* Mivel a cybertér nem ismer határokat, a szabályozás nemcsak nemzeti, hanem regionális és nemzetközi szinten is létrejöhet.

3.3. A központi szabályozás példái

3.3.1. Az Európai Unió 2000/31/EK irányelve az elektronikus kereskedelemről

2000 után a világ és az Európai Unió az önszabályozást promotáló kezdeményezések felé mozdult el (TROPINA–CALLANAN 2015, 86.); a két legfontosabb dokumentum az Európai Unió elektronikus kereskedelmi irányelve és az Európa Tanács számítástechnikai bűnözésről szóló egyezménye.

Az Európai Unió 2000/31/EK irányelve az elektronikus kereskedelemről[41] világosan kimondja és részletezi a közvetítő szolgáltatók felelősségét:[42] meghatározza az egyszerű továbbítás körébe tartozó szolgáltatásokat *(mere conduit)*, a *caching* definícióját, a *tárhelyszolgáltatók* felhasználók jogsértései esetére való mentességét, ezzel párhuzamosan az értesítési-eltávolítási eljárás mibenlétét, valamint azt, hogy a szolgáltatók nem kötelezhetők arra, hogy a felhasználóik online adatforgalmát monitorozzák, hiszen jogellenes tevékenységek megfigyelése nem feladatuk.

3.3.2. Az Európa Tanács számítástechnikai bűnözésről szóló egyezménye

Az Európa Tanács számítástechnikai bűnözésről szóló egyezménye[43] nemcsak a számítástechnikai/informatikai bűnüldözéssel kapcsolatos kihívásokat fogalmazza meg – nevesítve és csoportosítva a bűncselekménytípusokat –, hanem meghatározza az internetszolgáltatók felelősségét az általuk továbbított és tárolt felhasználói adatok bűnüldözés céljára való valós idejű megőrzésére és átadására. Ilyenként eleddig az egyetlen átfogó nemzetközi dokumentum. Az egyezmény deklarálja a szolgáltatók nyomozó hatósággal való együttműködését a bizonyítékok megszerzése, átadása és rögzítése terén. Meghatározza a köz- és a magánszektor együttműködésének kereteit és a nyomozó hatóságok nemzetközi együttműködésének alapjait. Az első dokumentum, amely a szolgáltató által kezelt adatok körében elhatárolja a forgalmi *(traffic data)* és a tartalmi *(content data)* adatokat, hiszen az utóbbiakra szigorúbb adatvédelmi rendelkezések vonatkoznak. A forgalmi adatok tárolásának ideje és miként je, valamint az átadásukra vonatkozó szabályok, beleértve az adatok átadására és lefoglalására irányuló jogsegély alkalmazását is, a mai napig élénk vita tárgyát képezik. Különösen az egyezménynek arra a kitételére vonatkozóan vannak viták, hogy a nyomozó hatóságok egy másik országban tárolt adatot közvetlenül, tehát a jogsegélykérelmi eljárás megindításával egy időben is beszerezhetnek, ha ahhoz az adat kezelője – a szolgáltató – hozzájárul. A 29. cikk szerinti Adatvédelmi Munkacsoport (Working Party 29 – WP29) véleménye szerint azonban mindenkor szükség van

[41] Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól (elektronikus kereskedelemről szóló irányelv). Európai Közösségek Hivatalos Lapja L 178/1, 2000.07.17.

[42] Elektronikus kereskedelemről szóló irányelv, 4. szakasz, 12–15. cikk.

[43] Az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezménye, ETS. No. 185. Magyarországon kihirdette a 2004. évi LXXIX. törvény.

a szolgáltatás helye szerinti hatóság kifejezett hozzájárulására – habár a hozzájáruló nyilatkozat hivatalos kibocsátása történhet akár utólag, az adatok rögzítése és átadása után.[44]

3.3.3. Az Európai Unió 2006/24/EK adatmegőrzési irányelvének tündöklése és bukása

Az Európai Unió 2006/24/EK adatmegőrzésről szóló irányelvének[45] mögöttes gondolata az volt, hogy a telekommunikációs szolgáltatók rendszere által kezelt, feldolgozott adatok megfelelően legyenek kategorizálva (például forgalmi vagy meta- és tartalmi adatok), és az adatok megőrzésére és kiadására vonatkozó időre egységes keretek szolgáljanak az Európai Unión belül. A felhasználói adatokat a nemzeti szolgáltatók már addig is kiadták a nyomozó hatóságok számára, de az államhatárokat felülíró cyberbűncselekmények esetén sokszor vált szükségessé külföldi szolgáltató megkeresése, aki viszont joggal hivatkozhatott arra, hogy az adatokat az országa jogszabályai szerint (már) nem tárolja. Ezért az Európai Unió szükségesnek látta az adatmegőrzési szabályokat legalább keretjelleggel egységesíteni a tagállamokban. A szabályozás szerint a tagállamok 6–24 hónapig terjedő időintervallumban határozhatták meg a telekommunikációs adatok megőrzési idejét – Magyarországon ez az idő jelenleg is 6–12 hónap.[46] Az irányelv értelmében a bűnüldözési és nemzetbiztonsági szervek, *bírói engedéllyel,* olyan adatok kiadását kérhették a szolgáltatóktól, mint az IP-cím, az e-mail-fiók használatának, a telefonhívásoknak, illetve a szöveges üzenetek küldésének és fogadásának időpontjai.

Az Európai Unió Bírósága (Curia) 2014. április 8-án azonban megsemmisítette az irányelvet, válaszul a Digital Rights Ireland (DRI) ügyekben hozott döntésekre.[47] A Curia érvei között szerepelt, hogy az irányelv túlságosan nagy mozgásteret hagyott a tagállamoknak az adatok felhasználásának célját és a megőrzési időintervallumot tekintve, így azok nem biztosítottak átláthatóságot (CHRISTOU 2016, 95.). Az adatok tömeges, célhoz nem kötött megőrzésére kötelező előírás ugyanakkor elősegítheti egy megfigyelésre épülő társadalom kialakulását, ami szembemegy a magánélet védelméhez fűződő alapvető emberi jogokkal, azaz nem áll arányban az Emberi Jogok Európai Egyezménye (EJEE) 7–8. cikkelyében meghatározott jogokkal, amelyek a törvényi rendelkezés nélküli büntetéskiszabás tilalmát és a magán- és családi élet tiszteletben tartásához fűződő jogot deklarálják (WOODS 2016). Mindemellett számos tagállam inkonzisztenciával küszködött az irányelv átültetése során – az alkotmánybíróságok sorra nyilvánították alkotmányellenessé az átültető jogszabályokat (EFF 2011a; TASZ 2015). Az európai adatvédelmi biztos azzal érvelt,

---

[44] Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime. 5 December 2013.

[45] Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Európai Unió Hivatalos Lapja, L 105/54. 2006.4.13.

[46] 2003. évi C. törvény az elektronikus hírközlésről. A bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettségre vonatkozó rendelkezéseket lásd: 159/A. § (3) bekezdés.

[47] Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, Court of Justice of the European Union Press Release No 54/14 Luxembourg, 8 April 2014.

hogy az Európai Bizottság az irányelv elfogadása óta nem bizonyította, hogy az szükséges és arányos rendelkezéseket tartalmazna, így az a lisszaboni szerződésben elfogadott Európai Alapjogi Charta értelmében jogellenes helyzetet teremt (EFF 2011b). Így amikor Edward Snowden nyilvánosságra hozta az Amerikai Nemzetbiztonsági Szolgálat (NSA) által a PRISM-program keretében való, tömeges, cél nélküli adatgyűjtés gyakorlatát, a kifogásolható amerikai rutin kritikái összecsengtek az európai adatmegőrzési irányelvet érő kritikákkal, amelyek a biztonság és a magánélet egyensúlyát hiányolták (CHRISTOU 2016, 97.).

3.3.4. Az Európai Unió információs rendszerek biztonságáról szóló 2016/1148 irányelve (NIS-irányelv)

Az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Európai Unióban egységesen magas szintjét biztosító intézkedésekről (Információs rendszerek biztonsága irányelv, a továbbiakban: NIS-irányelv)[48] a központi szabályozás legutóbbi példája, amely az önszabályozó szervezeteket kötelezi arra, hogy igazodjanak egy általuk kialakított, de a nemzeti hatóságok által felügyelt standardhoz. 2018-tól minden létfontosságú rendszerelemnek (kritikus infrastruktúra – víz- és közműszolgáltatás, energiaellátás, telekommunikációs és informatikai szolgáltatás) egységesen magas szintű informatikai biztonsági állapotot kell biztosítania.

A NIS-irányelv szigorú együttműködési szabályokat ír elő a kritikusinfrastruktúra-szolgáltatók és az információs társadalom szolgáltatói (általánosan az internetszolgáltatók) számára Európa-szerte. A cél „a hálózati és információs rendszerek egységesen magas szintű biztonságának" megvalósítása az Európai Unióban.[49] A szolgáltatókra ezen túl szigorú jelentési és információmegosztó kötelezettséget ró, amelyet a számítógépes biztonsági eseményekre reagáló csoportok hálózata (Computer Security Incident Response Team Network – CSIRT Network) számára kell teljesíteniük.[50] Habár az irányelv kezdeti tervezési szakaszában voltak viták az Európai Parlament és a Tanács között arról, hogy milyen szolgáltatókat érintsen a jelentési és informálási kötelezettség, a végleges változatba bekerültek a felhőszolgáltatók és a közösségihálózat-szolgáltatók, a nemzeti doménnévregiszterek és a webfelület-szolgáltatók is mint digtálisinfrastruktúra-szolgáltatók.[51]

A NIS-irányelv szerint a felelősséget nemcsak az információs rendszerbe jogellenesen behatoló, illetve az adatok integritását megsértő viseli az adatvesztésért, de a szabályok értelmében felelősséggel tartozik a meghackeléséért maga az adatkezelő is. A tagállamok által kötelezően létrehozott, illetve kijelölt felügyelő szerv (Magyarországon a Nemzeti Adatvédemi és Információszabadság Hatóság – NAIH) szankciót[52] szabhat ki az adat kezelőjére

[48] Európai Unió Hivatalos Lapja L 194/1, 2016.07.19.

[49] NIS-irányelv, 1. cikk (1) bekezdés.

[50] NIS-irányelv, 10. cikk.

[51] A NIS-irányelv a digitálisinfrastruktúra-szolgáltatók közé sorolja az IXP-ket, a DNS-szolgáltatókat és a TLD-névnyilvántartókat (NIS-irányelv, II. melléklet). Az IXP *(internet exchange point)* funkciója a hálózatok összekapcsolása, ők magunk nem biztosítanak internet-hozzáférést. Ilyenek például a felhőszolgáltatások, az online keresőprogramok és az online közösségi felületek üzemeltetői. A DNS-szolgáltató az internetes doménnevek helyi, illetve regionális elosztásáért felel. A TLD a legfelső szintű domén alatti internetes doménnevek regisztrációját irányítja és működteti.

[52] NIS-irányelv, 21. cikk.

olyan esetekben, amikor az adatvesztés azért következhetett be, mert az adatkezelő nem tett meg minden szükséges és tőle elvárható intézkedést az adatok biztonsága és a rendszer védelme érdekében. Tehát az Európai Unió felelőssé teszi az adatok jogszerű *kezelőjét* is azért, hogyha az nem működtette a NIS-irányelvben meghatározott,[53] magas szintű biztonsági előírások szerint a rendszerét, amely így feltörhetővé vált, és alkalmat adott az adatok jogellenes megszerzésére és kiszivárogtatására. Ez egy eleddig nem tapasztalt, forradalmi újítás az informatikai biztonság terén (CHRISTOU 2016, 132.). De ez még nem minden: ha az Európai Unió állampolgárainak adatai szivárognak ki egy másik, unión kívüli ország szolgáltatóján keresztül, akkor az uniós állampolgárt ért veszteség miatt a külföldi szolgáltató az Európai Unió (illetve az adott állam polgárának) joghatósága szerint felel.[54] Ha ezek a szigorított uniós adatvédelmi rendelkezések hatályba lépnek,[55] akkor várhatóan érdemben javul majd az uniós állampolgárok adatait kezelő szolgáltatók IT-biztonsága is.

A NIS-irányelv azzal, hogy önkéntes – de kötelező – bejelentési és informálási kötelezettséget ró a digitális szolgáltatók széles körére, amelyet a tagállamoknak egy standard információs network keretében kell létesíteniük, fenntartaniuk és felügyelniük, a magánszektort kötelezi arra, hogy nemzeti és nemzetközi szinten működjenek együtt a felülről jövő szabályozás végrehajtásában (ROBINSON et al. 2013; ITIC 2013). A kritikák középpontjában egyfelől az áll, hogy a digitális szolgáltatók teljes körére kiterjed a biztonsági standardnak megfelelés és a jelentéstétel kötelezettsége, amelyre eddig nem vonatkozott állami szabályozás. Másfelől önellentmondó az előírás, amely „önkéntes" jelentéstételi és együttműködési kötelezettséget ró a digitális szolgáltatókra. Harmadrészt azzal, hogy az államok dönthetik el, hogy nemzeti szinten mely digitális szolgáltatók tartozzanak jelentéstételi kötelezettséggel, elvész a szándékolt egységesítés, és fennáll mind a túl-, mind pedig az alulszabályozás veszélye.

A kritikáktól eltekintve azonban nem kétséges, hogy az Európai Unióban a felülről jövő, az állam általi szabályozás *(co-regulation)* legújabb és eddigi legteljesebb példáját láthatjuk az információs rendszerek biztonsága terén (TROPINA–CALLANAN 2015, 19.). Fontos hangsúlyozni, hogy az Európai Unió csak keretjellegű, minimális elvárásokat határoz meg az irányelvben, amelyen belül a tagállamok még szigorúbb és részletesebb rendelkezéseket hozhatnak. Ennek alapján például Németország a telekommunikációs szolgáltatókról szóló törvényben az incidensjelentési kötelezettségen felül azt is elvárja a szolgáltatóktól, hogy értesítsék a felhasználókat a rendszer elleni támadásokról (például *malware-ekről*), és – számukra is elérhető módon – azt is hozzák tudomásukra, hogyan állíthatják helyre a rendszerük működését (KUSCHEWSKY 2014).

[53] NIS-irányelv, 16. cikk.

[54] NIS-irányelv, 18. cikk.

[55] A tagállamok belső jogba való átültetésének határideje 2018. május.

3.4. Az önszabályozás példái – nemzetközi kitekintés

3.4.1. A szektorok közötti együttműködés

Vannak a világon az önszabályozást szorgalmazó, a piaci szolgáltatókat saját szabályok megalkotására motiváló megoldások is az információbiztonság terén, mint amilyen az Amerikai Egyesült Államokban a *Kiberbiztonság irányelv és végrehajtási rendelkezései* (Cybersecurity Directive and Executive Order 2014).[56] Az Egyesült Államokban számos törekvés látott napvilágot a felülről jövő szabályozás bevezetésére – az egységesítés égisze alatt[57] –, a hatályos szabályozás mégis elveti a központi regulációt, és a megvalósuló forma a piaci szereplőket incentívákkal motiváló önszabályozásnak tekinthető. Az cyberbűnözés elleni fellépésben a magánszféra szereplőit sikeresen mozgósító egyik jó példa Hollandiáé, ahol az incidensbejelentésre rendelkezésre áll a nemzeti rendőrségen belül egy külön egység, és a cybertér biztonságával kapcsolatos bűncselekmények nyomozására a rendőrség szervezetén belül egy további osztály. A kormány számítástechnikaivészhelyzet-reagáló csoportot (Computer Emergency Response Team – CERT) üzemeltet, emellett a kritikus infrastruktúrákat működtető ipari szereplők is közreműködnek a nemzeti cyberbiztonság megteremtésében: trendelemzést végeznek, bejelentéseket továbbítanak a rendőrségnek, monitoroznak, tudásbázisként biztosítják a szakmai továbbképzéseket, lakossági felvilágosítást, figyelmeztetéseket adnak ki, és közreműködnek a bűnmegelőzésben. 2012-ben Hollandia felállított egy nemzeti, köz- és magán-együttműködésen alapuló (Public Private Partnership – PPP) cyberbiztonsági központot (National Cyber Security Center – NCSC), amely a különböző szereplők és szintek (köz- és magánszféra) közötti koordinációért felelős (Den Tekk 2012).

Egy másik, a köz- és magánszektor együttműködésére gondot fordító állam Ausztrália, ahol a kormány létrehozta a helyi CERT-vel (AusCERT) és a Trusted Information Sharing Network for Critical Infrastructure Protectionnel (TISN) együttműködő cyberbiztonság operációs központját (Cybersecurity Operations Centre – COC). A TISN hálózatán keresztül osztják meg a CERT-n keresztül beérkező incidensek híreit három kritikus szektorral – a bankokkal, a telekommunikációs szektorral és a víz- és energiaellátást biztosító szektorral (Parliament of Australia 2010). További példával szolgál Svájc, ahol az incidensbejelentés és -elemzés a Swiss Reporting and Analysis Centre for Information Assurance (MELANI) keretében történik, amely az üzleti és privát felhasználók és a kritikus infrastruktúrák elleni támadások védelmét biztosítja (Tropina–Callanan 2015, 26.). Hasonló az Egyesült Királyságban a Centre for the Protection of National Infrastructure (CPNI), amely a nemzetbiztonsági szerveket látja el tanácsokkal úgy, hogy közben a rendőrség terrorelhárító központjával (National Counter Terrorism Security Office, NCTSO) és a magánszektorral (National Counter Terrorism Security Advisor Network) is kapcsolata van. Ausztriában a „Cybersecurity ICT – Risk Assessment of the Austrian Power Sector" egy az ipari szektorból kinőtt kezdeményezés, ma már a nemzeti felügyeleti hatóság részvételével működő, alulról építkező önkéntes szerveződés. A projekt alapcélja kockázatfel-

[56] Az elnök egyik végrehajtási rendelkezését lásd: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 11, 2017.

[57] Protecting Cyberspace as a National Asset Act of 2010; Cybersecurity Act of 2010; Cybersecurity Act of 2012.

mérések végzése volt, de ma már a gázellátás szektorát is magában foglalja, javaslatcsomagokat ad ki, és nemzetközi téren is kapcsolatokat ápol. Belgiumban 2014-ben indult három szektort – az akadémiát, az ipart és a szabályozó hatóságokat – felölelő kezdeményezés (TROPINA–CALLANAN 2015, 26.).

Az első komplex, az internet önszabályozásáról publikált ajánlást a Bertelsmann Alapítvány adta ki 1999-ben (MACHILL–WALTERMANN 1999). Hitvallásuk szerint olyan sok káros és ártalmas tartalom található az interneten, hogy azok kiszűrését, valamint a tartalom szabályozását egy piaci vagy állami szereplő sem végezheti egyedül. Artikulálta az önszabályozás szükségességét és annak elveit is: csak a piaci szereplők technikai tudásával és az állam jurisdikciós kapacitásával lehetséges egy olyan átfogó rendszerben gondolkodni, amely lehetővé teszi a jogsértések üldözését és végső soron az internet biztonságosabbá tételét. Ebben a körben – a javaslatok szerint – a tartalomszolgáltatóknak tartalomcímkézési és -szűrési kötelezettséget kell ellátniuk (a minőségbiztosítás keretében), a felhasználók számára bejelentőhelyeket *(hotline)* kell létesíteni (felhasználói szintű visszacsatolási mechanizmus), az államoknak és az államok fölötti döntéshozóknak (Európai Unió) pedig meg kell teremteniük a piaci szereplőkkel való együttműködés jogi alapjait. A Bertelsmann Alapítvány fennállása során eddig 12 javaslatcsomagot bocsátott ki, többek között az internet mindennapi életvitelt megváltoztató erejéről, a tartalomszolgáltatók etikai kódexeinek szükségességéről, az internet szűrési technikáiról és azok hatásosságáról, a nemzetközi együttműködésről, a hotline-ok tevékenységéről, valamint a képzés és a továbbképzés fontosságáról.[58]

3.4.2. A magánszféra szereplői

Az internetszolgáltatókat nemzetközi platformon összefogó ISPA (Internet Service Providers Association) a legelső és legfontosabb feltétele volt annak, hogy a szabályalkotók valóban kommunikálhassanak a szolgáltatókkal (TROPINA–CALLANAN 2015, 78.). A különböző földrészek szolgáltatókat összefogó szervezetei között az EuroISPA, az internetszolgáltatók páneurópai szervezete[59] a legnagyobb a világon: több mint 2 300 szolgáltatót tömörít az Európai Unió és az Európai Szabadkereskedelmi Társulás (European Free Trade Association – EFTA) tagállamaiból. 1997-ben alapították azért, hogy az Európai Unió jogalkotási-konzultációs folyamatában képviselje a szolgáltatók érdekeit, összegyűjtse az egyes országokból származó jó gyakorlatokat és más országokban is gondoskodjon azok adaptálásáról és implementálásáról (az ISPA szervezetek teljes felsorolását lásd: TROPINA –CALLANAN 2015, 78.).

Az ICANN (Internet Corporation for Assigned Names and Numbers) az internetdomének kiosztásáért felelős nonprofit szervezet, amelyet az internet kommercializálásának idején, 1998-ban bízott meg az Egyesült Államok kormánya által felügyelt Nemzeti Tudományos Alapítvány (National Science Foundation – NSF), illetve az alapítvány által koordinált Nemzeti Tudományos Alapítvány Hálózat (National Science Foundation Network – NSFNET) az internetdoménnevek hozzárendelésével. Az ICANN felügyeletével osztják le az Internet

[58] Bertelsmann Alapítvány honlapja: www.bfna.org (A letöltés dátuma: 2018. 05. 15.)
[59] EuroISPA honlapja: www.euroispa.org (A letöltés dátuma: 2018. 05. 15.)

Assigned Numbers Authority (IANA) által vezetett internetes doménnévregiszterből az összes domént (Domain Name System – DNS) az egész világon. A szervezet alulról építkező, konszenzuson alapuló, többszereplős döntéshozó modell,[60] amelynek működése felett 2016 márciusában formálisan is megszűnt az Egyesült Államok ellenőrzési joga (Farrell 2016).

Az INHOPE-ot (Internet Hotline Providers in Europe Association) az Európai Bizottság Daphne Programjának keretében állították fel 1997-ben.[61] Az Internetes Forródrótok Nemzetközi Szervezeteként olyan, nemzeti szinten működő hotline-okat tömörít, ahová bárki akár névtelenül bejelenthet online megjelenő káros vagy ártalmas tartalmakat.[62] Magyarországon a Nemzeti Média és Hírközlési Hatóság által működtetett hotline a szervezetnek 2012 óta tagja. Az INHOPE ernyőszervezete gondoskodik arról, hogy a bejelentések ne maradjanak válasz nélkül, és a valóban illegális tartalmak a megfelelő bűnüldöző hatósághoz kerüljenek felderítés és nyomozás céljából. A szervezet a beérkező bejelentések között előszűrést végez, és annak eredményét szükség esetén a hatóságoknak (partnerszervezetek) továbbítja. A partnerszervezetek között a nyomozó hatóságokon (Europol, Interpol, Combating Online Child Abuse Virtual Taskforce) kívül megtalálhatók a piaci szereplők, az internetszolgáltatók és a vezető közösségi oldalak szolgáltatói (például Google, Facebook, Twitter, Microsoft) is. Az INHOPE közvetlen kapcsolatot alakít ki a tartalomhosztoló szolgáltatókkal, akiknek rövid úton – még a nyomozás megindulása előtt – ideiglenes tartalomeltávolítási kérelmet küldhet.

Az Európai Bizottság *Biztonságosabb Internet Programjának* (1999–2013) sikerét követve, a bizottság 2013-ban létrehozta a *Better Internet for Kids* (BIK) projektet.[63] A BIK az INHOPE-pal stratégiai partnerségben működik, és a gyermekek és fiatalok számára biztonságos online tartalmak fejlesztését, a képzést és a tudatosítást tűzte ki célul. A program (korábban InSafe) keretében az Európai Unió valamennyi tagállamában biztonságosabb internetközpontok (Safer Internet Centres – SIC) létesültek, amelyeknek tagja egy hotline, egy helpline, egy tudatosító center és egy ifjúsági panel.[64] Utóbbi keretében a megszólított fiatalok közvetlenül részt vehetnek a nekik szóló tartalmak kialakításában.

A hosszú távú, megelőző jellegű stratégiának fontos szereplői a tudatosságnövelésben részt vevő vállalatok és civil szerveződések is. A telekommunikációs vállalatok tevékenységi körébe tartozik mára a lakosságot és főként a fiatalokat célzó, a biztonságos internethasználatra szoktató, felvilágosító, illetve a felhasználókat technikai eszközökkel (például szűrőszoftverek, tartalombejelentési lehetőségek) ellátó *vállalati szegmens* létrehozása, amely tevékenységét társadalmi felelősségvállalás keretében végzi.[65]

---

[60] ICANN honlapja: www.icann.org/resources/pages/welcome-2012-02-25-en (A letöltés dátuma: 2018. 05. 15.)

[61] INHOPE honlapja: www.inhope.org/gns/who-we-are/Ourhistory.aspx. (A letöltés dátuma: 2018. 05. 15.)

[62] Az ártalmas (illegális) és a káros (káros pszichológiai következmények kockázatát magában hordozó, de jogszerű) tartalmak elhatárolását lásd az Európai Unió Safer Internet Akciótervében: Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.

[63] Better Internet for Kids (BIK) holnapja: www.betterinternetforkids.eu/ (A letöltés dátuma: 2018. 05. 15.)

[64] Magyarországon a Biztonságosabb Internet Központot a Nemzetközi Gyermekmentő Szolgálat vezeti, a hotline feladatokat az NMHH keretében működő internethotline.hu, a helpline feladatokat a Kék Vonal Alapítvány, a tudatosságnövelő és ifjúsági panel feladatokat pedig maga a Nemzetközi Gyermekmentő Szolgálat látja el.

[65] Magyarországon ilyen például a Telenor által kiadott Biztonságos Internet Oktatócsomag (hipersuli.hu), vagy a Magyar Telekom Internetbiztonság szoftvere, de említhetnénk ehelyütt az ugyancsak a Telekom vállalatból kinőtt és önállóvá vált Digitális Tudás Akadémiát (Elérhető: http://digipedia.hu A letöltés dátuma: 2018. 05. 15.)

3.5. A big data jelenség – jogok a cybertérben

Az előző alfejezetben szemléltetett szigorú trend, amely az internet felülről irányított, egységes szabályozásának kialakítását célozza, annak a folyamatnak a hatására indult meg, amelynek keretén belül egyre több adatot teszünk közzé magunkról. A szolgáltatók felhőben *(cloud)* tárolják az adatainkat, amelyet az állambiztonság is igénybe vesz a tájékozódáshoz a veszélyek felmérésekor. Edward Snowden 2013-ban nyilvánosságra hozta az Egyesült Államok Titkosszolgálata (NSA) által a terrorelhárítás és az állambiztonság szavatolása érdekében való, nem célzott adatgyűjtés tényét és a bírói engedély nélkül megfigyelt személyek listáját. Részben ennek is köszönhető, hogy az Európai Unióban az évtizedek óta tartó biztonság vs. magánszféra vita felizzott, és az Európai Unió megreformálta adatvédelmi szabályait. Ha eddig voltak is meg nem alapozott gyanúink arra, hogy a hatóságok túlságosan proaktívan élnek – és visszaélnek – a tömeges adatrögzítés technika nyújtotta lehetőségével, és hogy az internet szabályozásában részt vevő szervezetek nem az adatvédelmi előírásoknak megfelelően kezelik az adatainkat, a snowdeni reveláció(k)[66] (GREENWALD et al. 2013) után már bizonyosan nem fogunk ebben kételkedni.

3.5.1. A big data fogalma

A 21. század korai szakaszában talán a legfontosabb, ember-gép viszonyt meghatározó esemény személyes adataink digitalizálódása, amely egy sor megoldásra váró technikai és jogi kérdést vet fel. Napjainkban az *adatbázisok keletkezésének* és *folyamatos bővülésének* lehetünk tanúi. Az adatállomány gyorsan növekszik, köszönhetően annak, hogy az információérzékelő applikációkkal ellátott mobileszközök folyamatosan gyűjtik az adatokat – a távérzékelő berendezések a levegőből, másikak a szoftverek logjaiból, megint más eszközök a kamerákon, mikrofonokon, rádiófrekvenciás azonosítási rendszereken és vezeték nélküli érzékelő hálózatokon keresztül áthaladó adatokból táplálkoznak. Az adatoknak ebben a kakofóniájában David Wall szerint még azok sem kerülhetik el az online áldozattá válást, akik nem használják az internetet – habár ez napjaink digitalizált társadalmában egyre nehezebb –, hiszen számos személyes, forgalmi, kommunikációs és egyéb járulékos adatunk tárolódik olyan számítógépeken, amelyek hálózatba és az internetre kapcsolódnak (WALL 2011, xi).

A *big data* (szabad fordításban „nagy mennyiségű adat") azoknak az adatfájloknak a *terminus technicusa,* amelyek feldolgozására és elemzésére komplexitásuk miatt a hagyományos szoftverek nem képesek. A kihívások között szerepel az adatrögzítés és -tárolás, az elemzés, az adattárházak létrehozása, az adatbázisban való keresés, a megosztás és a transzfer, a vizualizáció, a lekérdezés és az információs titoktartás. A terminus gyakorta csupán a prediktív adatbevitelre, a felhasználó viselkedéselemzésére, illetve az olyan emelt szintű adatelemző módszerekre vonatkozik, amelyek értéke az adatbázisban és nem annak nagyságában rejlik. A tudományos kutatók, az üzleti életben tevékenykedő menedzserek,

[66] Snowden az információkat a Guardian és a Washington Post kiválasztott újságíróinak adta át azzal, hogy feldolgozott, kommentekkel ellátott, interpretált adatszettekben szükséges azokat a nagy nyilvánosság elé tárni az elkövetkező években.

a gyógyszerészek vagy a gyógyászat területén dolgozók, a hirdetéskezelők, továbbá a kormányok gyakorta ütköznek nehézségekbe az internetes keresés, a pénzügyek, az üzleti informatika, az adatbázisok elemzése és feldolgozása terén, hiszen a felsorolt területeken, ágazatokban manapság már ilyen óriási, többdimenziós adatbázisok állnak rendelkezésre.[67]

A big data azonban nemcsak az adatok nagy mennyiségére, hanem az adatok sokoldalú gyűjthetőségére és az általuk hordozott információ sokoldalú felhasználhatóságára is utal. Már a bigdata-evangelisták, az adatok hasznosíthatóságáról szóló első tudományos értekezések szerzői is előre jelezték az adatok döntéshozatalban játszott fontos szerepét. Neil M. Richards és Jonathan H. King olyan globális problémák megoldását várják a big datától, mint amilyen a fertőző betegségek, járványok terjedése, a kriminológiai trendek előrejelzése és válaszok kidolgozása, de előnyeként említik az olyan hétköznapi dolgokat is, amilyen a mindennapi élet biztonságosabbá vagy hatékonyabbá tétele (Richards–King 2013). A testre, illetve testbe építhető mikroelektronikai eszközök, szenzorok – amelyek lehetővé teszik például az alvás, a testsúlyszabályozás és egyéb élettani folyamatok megkönnyítését – idővel az egyént is adathalmazzá (*quantified self,* azaz „számszerűsített én") teszik.

Ebben a körben szükséges szót ejteni a dolgok internetéről (Internet of Things – IoT).[68] A dolgok internetének lényegét leginkább megragadó definíciót az Internet of Things Global Standards Initiative dolgozta ki. E szerint a fizikai kiterjedéssel rendelkező dolgok hálózata – elektromos, szenzoros csatlakozással felszerelve – lehetővé teszi, hogy a „dolgok" adatokat gyűjtsenek és cseréljenek egymás között, a hálózaton keresztül. Az okoseszközök – mint a testre vagy testbe szerelhető mikrocsipek, rádiófrekvenciás mikroeszközök – szenzorok segítségével kommunikálnak egymással a mozgásunkról, cselekvéseinkről, élettani mutatóinkról, életvitelünkről. Ezek az adatok önmagukban nem rendelkeznek információval, csak rendszerezve, kiválogatva, analizálva és standardizált módon feldolgozva (Mann 2015, 2.).

A big data exponenciális növekedése nemcsak a közvetlenül hasznosítható adatok, hanem a közvetetten hasznosítható, úgynevezett metaadatok növekedésének is köszönhető. *Közvetlenül hasznosítható adatoknak* nevezzük a felhasználóktól valamely szolgáltatásra való elektronikus regisztráció alkalmával kért adatokat, valamint a szolgáltatás teljesítéséhez, illetve az adatátviteli eszközök egymás közti kommunikációjához szükséges adatokat.[69] Ehhez képest *közvetetten hasznosuló adatok* a számítógépes algoritmusok által rendszerezett és elemzett olyan adatok, amelyek a mindennapi kommunikáció, a helyváltoztatás, a vásárlás révén tárolt geolokációs, banki és egyéb műveletek közben mint funkcionális melléktermékek állnak elő, amelyek nem szükségesek valamely szolgáltatás igénybevételéhez, de automatikusan tárolódnak. A közvetetten hasznosuló adatoknak köszönhetők a személyre szabott online hirdetések, az online közösségi oldalakon megjelenő, felhasználóknak címzett ajánlatok (viselkedésalapú hirdetés). A közvetetten hasznosuló adatok önmagukban nem, csak egymással összevetve, aggregálva, folyamatukban rendelkeznek információtartalommal (Delort 2015).

---

[67] Lásd a Wikipédia és a Webopedia szócikkeit.

[68] A dolgok internetéről átfogó képet nyújt a Cisco vállalat honlapja: www.cisco.com/ (A letöltés dátuma: 2018. 05. 15.)

[69] Lásd erről az OECD két kapcsolódó munkacsoportjának riportját: OECD Working Party on the Information Economy & OECD Working Party on Information Security and Privacy, Exploring the economics of personal data: A survey of methodologies for measuring monetary value, 2 April 2013, DSTI/ICCP/IE/REG(2011)2/FINAL.

A digitalizálódással következett be – és a technikai fejlődés nyomán szintén folyamatos – az adatok továbbítási sebességének növekedése, illetve az adatok összekapcsolhatósága (ROUVROY 2016, 8.). Az adatok expanziója, valamint összekapcsolhatósága mellett a harmadik, a technológiai fejlődéssel, a digitalizálódással előálló attribútum az *adatok sokoldalúsága.* A közintézmények és közszolgáltatók, a lakossági felméréseket végző statisztikai hivatalok, a rendőrség, a bíróságok és a szabálysértési nyilvántartások adatokat gyűjtenek rólunk, születési, házassági és halotti anyakönyvi regiszterek keletkeznek. Mindennapi életünk során óriási mennyiségű adathalmazt hagyunk magunk után: azzal, hogy utazunk, vásárolunk, fogyasztunk, kommunikálunk, blogot vezetünk, online csatornákon üzenetet váltunk vagy akár elhaladunk egy CCTV-kamera alatt.

3.5.2. A big data megjelenésével előálló problémák

1. Digitális nyomaink, azaz metaadataink (avagy közvetetten hasznosítható adataink) tárolását és a hatóságok számára történő rendelkezésre bocsátását az Európai Parlament és a Tanács 2006/24/EK adatmegőrzésről szóló, korábban részletesen tárgyalt irányelve (adatmegőrzési irányelv) szabályozta 2014-ig, amikor is a Curia a szabályozási dokumentumot megsemmisítette.[70]

Az a tény, hogy már nem áll rendelkezésre a direktíva, amely az uniós tagállamok között szabályozta az adatok készen tartásának idejét és az adatátadás körülményeit, nem jelenti azt, hogy a szolgáltatók szükség esetén ne adnák át a tárolt forgalmi adatokat a hatóságoknak. Az adatmegőrzési irányelv hatályon kívül helyezésével ugyan a szolgáltatók már nincsenek európai uniós szinten kötelezve arra, hogy a tagállamoknak nemzetbiztonsági vagy nyomozási célból adatokat adjanak át a felhasználókról, ám előállt egy olyan *ex lex* állapot, amelyben az adatok tárolási idejét és átadását, illetve a területükön bejegyzett szolgáltatók együttműködési kötelezettségeit immár teljes mértékben a tagállamok határozhatják meg. Ez egyfelől kiszolgáltatottá teszi a helyi szolgáltatókat (és a felhasználókat) a tagállamok által támasztott kötelezettségeknek, másfelől a külföldi szolgáltatók könnyűszerrel megtagadhatják valamely nemzeti nyomozó hatóság megkeresésének teljesítését azon az alapon, hogy (már) nincs meg a keresett adat.

2. Az adatbányászat (data mining) és a gépi automatikus tanulás (machine learning) főleg a felhasználói adatok és a magánélet védelme terén jelentenek megoldandó problémákat, de egy sor társadalmi vonatkozásuk is van.

Az Európa Tanács 1981-ben fogadta el a személyes adatok gépi felhasználása során az egyének védelméről szóló, 108. számú egyezményét (a továbbiakban *európai adatvédelmi egyezmény*), amely az adatvédelem tárgyában a mai napig az egyetlen kötelező erejű dokumentum az egész világon.[71] Az egyezmény célja „minden egyén számára […] biztosítani, hogy jogait és alapvető szabadságjogait, különösen a magánélethez való jogát tiszteletben tartsák személyes adatainak gépi feldolgozása során" (RÁTAI et al. 2010, 232.). Az európai adatvédelmi egyezmény 1981. évi elfogadása és 1985. évi hatálybalépése óta olyan mértékű

[70] Lásd: az Európai Bíróság (ECJ) 2014. április 8-án hozott, C-293/12 és C-594/12 összevont határozatát.

[71] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ETS. No. 108. Magyarországon 1998. február 1-jén lépett hatályba. Bővebben lásd: RÁTAI et al. 2010.

technológiai fejlődés (*digital turn,* azaz digitális fordulat, ROUVROY 2016, 37.) következett be, amely szükségessé tette az egyezmény teljes felülvizsgálatát és módosítását. Megoldásul az Európa Tanács 2016-ban protokollt terjesztett elő a személyi adatok automatikus feldolgozásának szabályozására, amely lefekteti a személyek alapvető védelmének feltételeit az automatikus adatfeldolgozás korában.[72]

3. A prediktív elemzés (predictive analytics) jó példái a kriminológiában a bűnözési trendek, az elkövetővé válás és a sértetté válás esélyeinek megjósolására vállalkozó rendőrségi kockázatbecslő algoritmusok (predictive policing).

A rendőrségi kockázatbecslő algoritmusok egy fajtája a *résztvevőalapú modellezés* (*agent-based modeling* – ABM):[73] olyan számítógépes szimulációs program, amely a bűnelkövetés és az áldozattá válás előrejelzésére szolgál. A programba betáplálják az áldozatok és az elkövetők összes jellemzőjét, így olyan ágenseket (szereplőket) alkotnak a bűnözés modellezésére, amelyben tipikus áldozati és elkövetői karakterek jelennek meg. Ha a rendszerbe betáplálják a környezeti kriminológia adatait is, akkor környezeti kriminológiai elméletek szerint előre jelezhető az egyes elkövetői és áldozati karakterek viselkedése (BIRKS et al. 2012).

A *reviktimizálódás (near repeat victimization, repeat victimization)* valamely személy, földrajzi hely, lakóhely, lakóingatlan, háztartás, közösség, cég, vállalkozás, jármű, illetve bármilyen dolog és a hozzá kapcsolódó személyek időben és térben megismételt sértetté válását jelenti. Az 1990-es és 2000-es években számos kísérlet született ezeknek a viktimizálódási hotspotoknak a felmérésére és a hozzájuk illeszkedő rendőri prevenciós programok kifejlesztésére (GROVE–FARRELL 2011). A korai empirikus kutatások jórészt a betöréses lopásra koncentráltak (TOWNSLEY et al. 2000, 2003; JOHNSON–BOWERS 2004). Azt találták, hogy a betöréses lopás helyszínéhez közel fekvő ingatlanok is ki vannak téve az azonos módon elkövetett bűncselekmény veszélyének. Míg a helyszíntől fizikailag és időben távolodva csökken az áldozattá válás veszélye, azaz az elkövetett típusbűncselekmény kevésbé terjed, és – a betegségekhez hasonlóan – kevésbé „ragályos". A Townsley és munkatársai által használt statisztikai becslőmodell szerint a kritikus táv 400 méter, az idő pedig egy hónap, amelyet átlépve térben és időben már jóval kisebb a hasonlóan elkövetett betörések kockázata. Minél hasonlóbbak az áldozat személyében vagy a károsult dolog felszereltségében, kinézetében, fekvésében rejlő jellemzők, annál biztosabb, hogy áldozatul esnek hasonló bűncselekménynek. A betöréses lopással összefüggésben a házak és lakóövezetek hasonlóságára figyeltek fel: ha betörés történt az egyik lakásban vagy házban, akkor pár napon belül a szomszédos nagyon hasonló ingatlan is áldozatul esett (TOWNSLEY et al. 2000, 2003). Jerry Ratcliffe, volt rendőrtiszt beszámolt arról, hogy a hasonló áldozatok elleni bűncselekmények száma is megbecsülhető.[74]

Egy másik statisztikai prediktív modell, a *bűnözés-előrejelző térképek modellje (crime predictive maps)* először a Brit Kriminológiai Társaság 2001-ben tartott konferenciáján

---

[72] Draft protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).

[73] *Agent-based modeling* / *individual-based modeling:* A résztvevők segítségével való modellezés vagy résztvevőalapú modellezés olyan számítástechnikai programvezérelt szimuláció, amely személyek, illetve közösségek, csoportok, szervezetek viselkedésének a vizsgált rendszerre való hatását jelzi előre. A játékelmélet, a komplex rendszerek, a számítástechnikai szociológia, a többágensű rendszerek és az evolúciós programozás elemeit vegyíti (Wikipédia).

[74] Lásd: www.jratcliffe.net (A letöltés dátuma: 2018. 05. 15.)

mutatkozott be (JOHNSON et al. 2007, 2009). A ProMap bűnözési térképére felviszik az adott bűncselekménytípus minden adatát, és azokat az újabb bűncselekmények adataival kiegészítve egy dinamikus térképet hoznak létre, mivel az újabb és újabb bűncselekmények mindig új kockázati megvilágításba helyezik az egyes lakóövezeteket. Minden hasonló körülmények között elkövetett bűncselekmény kockázatnövekedéshez, ugyanakkor minden újabb bűncselekmény nélkül eltelt nap kockázatcsökkenéshez vezet az adott helyen (MCLAUGHLIN et al. 2006). A ProMap lehetővé teszi a rendőri járőrözés és a rövid távú megelőző intézkedések operacionalizálását. Ilyen módon költségtakarékos, hiszen a nyomozó hatóság a bevett útvonalakról áttelepítheti a járőröket a nagyobb kockázati jellemzőkkel rendelkező lakóövezetekre (SHORT et al. 2008; MOHLER et al. 2011). Az Egyesült Királyságban a ProMap gyakorlati alkalmazásának példája a PredPol.[75]

Ken Pease és Andromachi Tseloni a rendőrség számára olyan statisztikai becslési programot fejlesztettek ki, amely az elkövetett bűncselekmények helyi, valamint az elkövetők és a sértettek demográfiai és személyi jellemzőiből kreált adatbázist[76] veszi alapul a sértetté válás, illetve a reviktimizáció megelőzéséhez (PEASE–TSELONI 2014). Ez a program az előzőkhöz képest összetettebb: mind a személyi jellemzőket (a sértettek személyes profilja: nem, életkor, családi státusz, gyermekek száma, képzettségi fok, munkahely, háztartás jellemzői; társadalmi réteg szerinti profil, különös tekintettel a szocioökonómiai státuszra), mind az életstílust (aktivitási skála, napi rutincselekvések), mind pedig a lakóhely jellegzetességeit (ház és lakókörnyék típusa, háztartások átlagos jövedelme) figyelembe veszi. Emellett az áldozattá vált alanyok adatbázisa az áldozattá nem váltak adataival is összevethető. A program tehát összetett kockázati elemzéseket végez. A rendőrség és az áldozatvédő szervezetek e kockázati faktorok nyomán csoportosíthatják és időzíthetik a megelőző intézkedéseket, hogy azok ne rutinszerűek legyenek, hanem a modell alapján a megfelelő időben és helyen a megfelelő személyi állomány teljesítsen szolgálatot, akiket képzettségük és gyakorlati tapasztalataik alkalmassá tesznek arra, hogy a megfelelő válaszokat adják a veszélyhelyzetekre, továbbá felkészültek az érintett társadalmi csoportok által támasztott kockázatok kezelésére (PEASE–TSELONI 2014, 34.).

4. Az ok-okozatiság rejtve marad. A big data halmazában felgyűlt adattömeg kicsiny szegmensei ugyan önmagukban nem informálnak a felhasználókról, de leválogatott, feldolgozott és összepárosított formában igen. Az adatok a leválogatás előtt nem alkalmasak a személyazonosításra, de megfelelő algoritmus segítségével már profilokat alkothatunk – megtudhatjuk, milyen szokások jellemzik a felhasználókat, és előre jelezhetünk bizonyos felhasználói aktivitást, trendeket. Az algoritmusok működése azonban a nagy adatmennyiség miatt meglehetősen átláthatatlan: a számos különféle változó közül nehéz elkülöníteni azokat, amelyek hatására valójában bekövetkezett a jelzett változás.

Eric Winsberg a big databan rejlő eme tulajdonságot úgy nevezi, hogy nem az igazságot mutatja meg, csak annak egy operacionális szeletét (WINSBERG 2006). Az operacionális szeletek, amelyeket valamely algoritmus segítségével lehet előállítani, informálják az adatfeldolgozót a jövőbeli trendekről, mégpedig a múltban generált adatok elemzésével, így

[75] A Predpol gyakorlatáért lásd: www.predpol.com (A letöltés dátuma: 2018. 05. 15.)

[76] A Brit Bűncselekményi Felmérés (British Crime Survey) és az Egyesült Királyság cenzusának adatait használták fel az adatbázisok képzéséhez.

ez egy „algoritmikus racionalitás". Az *algoritmikus racionalitás* átláthatatlansága éppen az automatizmusban rejlik: feketedobozként a felhasználó ugyan nyomon követheti, milyen adat kerül a rendszerbe (mondjuk úgy, hogy regisztrál egy weboldalra), és ennek eredményét is láthatja (mondjuk egy személyre szabott ajánlat formájában), de azt már nem tudhatja, hogy a kettő között milyen elemzési-feldolgozási folyamatok zajlottak. Ez tehát nem a valóság egy tényleges szelete, azaz az „igazság", hanem csak egy algoritmikus valóság. A képet tovább bonyolítják a beépített tanulási képességgel rendelkező algoritmusok, amelyek a statisztikai valószínűségtől eltérő részleteket azonnal beépítik az elemzési folyamatba.

5. Az adatok újraazonosíthatósága – az anonimitás megszűnése. A Massachusetts Institute of Technology kutatóinak 2013-ban lefolytatott (DE MONTJOYE et al. 2013), majd 2015-ben megismételt (DE MONTJOYE 2015) kutatása szerint csupán négy darab, az interneten nyilvánosan elérhető adat elegendő arra, hogy egy névtelen metaadatgyűjteményből összeállítható legyen a kreditkártya-tranzakciókat végző személyek 90 százalékának profilja pusztán azzal, hogy három hónapon keresztül rögzítik a kreditkártya-tranzakciókat.

Az azonosításra felhasznált metaadatok között szándékosan nem használtak nevet, lakcímet, kreditkártya- és banki adatokat vagy bármilyen más, személyes adatot. Az *anonimitás* tehát ugyancsak a big datának köszönhetően a múlté, de legalábbis relatív, amennyiben csupán a hétköznapi teendőink közben hagyott digitális nyomok könnyen *újraazonosíthatóvá* tehetnek minket. Az újraazonosítás annál könnyebb, minél több a tranzakció, minél hosszabb ideig őrzik meg adatainkat – hiszen ez növeli az információ denzitását, sűrűségét. Az adatok szaporodása önmagában megnöveli az egyéni magatartás megjósolhatóságának esélyét.

A big data fent bemutatott tulajdonságai követhetetlenné, ellenőrizhetetlenné teszik a személyes adatok feldolgozását és felhasználását. Emiatt kiüresednek az olyan adatvédelmi rendelkezések, amelyek a feldolgozandó (kezelendő) adatok minimalizására,[77] célhoz kötött gyűjthetőségére és kezelhetőségére,[78] az adatkezelés és -feldolgozás átláthatóságára,[79] az adatmegőrzés idejének korlátozottságára,[80] valamint a különleges (egészségi állapottal, szexualitással, vallással, etnikummal, DNS-sel, biometrikus jellemzőkkel, büntető nyilvántartással, szabálysértésekkel, politikai preferenciával összefüggő) adatok gyűjtésének tilalmára[81] vonatkoznak (ROUVROY 2016). A 29. cikk szerinti Adatvédelmi Munkacsoport 2014-ben kiadott véleménye szerint az adatvédelem alapvető elvei a mai napig érvényesek, más kérdés, hogy további garanciákkal szükséges azokat kiegészíteni a felhasználók védelme érdekében.[82]

[77] Európai adatvédelmi egyezmény 5.4.c cikk.
[78] Európai adatvédelmi egyezmény 5.4.b cikk.
[79] Európai adatvédelmi egyezmény 5.4.a cikk.
[80] Európai adatvédelmi egyezmény 5.4.e cikk.
[81] Európai adatvédelmi egyezmény 6. cikk.
[82] Statement of the Article 29 Working Party on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU, 16 September 2014, 14/EN/WP 221.

3.5.3. A big data és a társadalmi szerződés

Berzsenyi Dániel *A közelítő tél* című versében[83] a maga számára teremtett szubjektív világot írta le. Ebbe az idealisztikus létbe néha – ha engedjük – beleszól a valóság, a „dialektikus metafizikai totalitás" (ZUBRECZKY 1969, 291.). Ilyenkor az ideális világ falán repedések keletkeznek, és a világról alkotott idealista, romantikus elképzeléseink közé kénytelenek vagyunk beengedni a kegyetlen valóságot. Berzsenyi nem volt egyedül ezzel a képpel; korának romantikus költői a panteizmus szűrőjén keresztül láttatták a természet elmúlását, benne az emberrel és minden lénnyel.

Antoinette Rouvroy belga filozófus szerint az internet megjelenésével a *társadalmi szerződésben* lefektetett alapelvek átalakuláson mennek keresztül; az eredeti alapelvek többé már nem szolgálhatnak viszonyítási pontokként (ROUVROY 2016, 15.). A digitalizáció, a programozott adatkezelés és kormányzás, a káresemények és bűncselekmények előrejelzése, a személyhez fűződő újabb bűnelkövetés kockázatának megbecslése *(risk assessment),* valamint a terrorcselekmények előrejelzése korában új társadalmi szerződés létrehozása szükséges. A korábban változatlannak, öröknek tekintett alapelveket a gyorsan változó technika lerombolta, és csak egyetlen horgonyt hagyott meg: mindennek a *vitathatóságát.*

A technikai fejlődésben *sorsszerűséget* fedezhetünk fel. Az ember által teremtett gép, a technikai újítás konstans, sőt gyorsuló ütemű fejlődésének lehetünk tanúi. Itt nincs pauza, amely megnyugvást hozhatna. Ez megmutatkozik a bűnelkövetők és a bűnüldözés, illetve az új formában megjelenő jogsértések és a jog versenyfutásában vagy akár az online közösségi portált elhagyni képtelen felhasználó belső feszültségében. Ha kilépünk a technikai fejlődés körforgásából, úgy azt kockáztatjuk, hogy az eddiginél jóval nagyobb lesz a lemaradásunk, felhasználóként pedig kimaradunk a közösségi történésekből – óhatatlanul kirekesztődünk. Kockáztatjuk, hogy pauzánk végzetes lesz, hogy nincs onnan visszaút.

Ezt a hasonlatot figyelhetjük meg a cybertérhez kötődő sajátos moralitásban, az erkölcsök és értékek átformálódásában, a morális határok áttevődésében. A versenyfutás megfigyelhető az állampolgár digitalizált lenyomatának megteremtődésében, adatai kiadásában és az azokról való rendelkezéssel kapcsolatos vesszőfutásban, a bűnelkövetés és a bűnüldözés (jogalkotás) macska-egér játékában, valamint a felhasználó és az online közösség dinamikájában.

3.5.4. A big data és az emberi jogok

A 20. században az emberi jogokat érintő olyan releváns technológiák keletkezésének lehettünk tanúi – jórészt a hadseregnek és a biztonságiparnak köszönhetően –, amilyen maga az internet, a kromoszómaelemzés, a biometrikus azonosítás, a közterületfigyelő-kamerák (CCTV), a mobiltelefon-kamerák, a lehallgató berendezések, az adatelemzés neurális hálózatai, a hangfelismerő rendszerek, hogy csak néhányat említsünk. A digitális eszközök miniatürizálása lehetővé tette, hogy a technológiai eszközök az emberi testbe is – a bőr alá vagy szervekbe, illetve azok helyére – beszerelhetők legyenek. A megfigyelés akár észre-

[83] „Minden csak jelenés; minden az ég alatt, Mint a kis nefelejcs, enyész." Berzsenyi Dániel: A közelítő tél. Lásd: *Berzsenyi Dániel válogatott versei* (2006). Válogatta: TARJÁN Tamás. Budapest, Holnap Kiadó.

vétlenül is lehetővé vált, a felhasználói adatokat kezelő adatbázisok összekapcsolása pedig hozzájárul az adatokkal való visszaéléshez.

A digitális társadalomban az ENSZ két dokumentumában, az *Emberi jogok egyetemes nyilatkozatában* (EJENY 1948), és a *polgári és politikai jogok nemzetközi egyezségokmányában* (PPJNE 1966), valamint az Európa Tanács Rómában kelt *Emberi jogok európai egyezményében* (római egyezmény – RE 1950) lefektetett legfontosabb emberi jogok kerülnek veszélybe, amilyen az *emberi szabadság* és *méltóság,* a *hátrányos megkülönböztetés tilalma,* a *gondolat- és véleménynyilvánítás szabadsága,* a *biztonsághoz való jog* és az *embertelen büntetés tilalma,* a *tisztességes tárgyaláshoz való jog* és az *ártatlanság vélelme,* a *fizikai és szellemi tulajdonhoz való jog,* a *magánélet és a család tiszteletben tartása,* az *élethez való jog* és a *haza ügyeiben való részvétel joga.*[84] A 18. táblázat tartalmazza az Európai Unió új adatvédelmi rendeletét is (Európai adatvédelmi rendelet, EU 2016/679) a magánélet tiszteletben tartásához való jog részeként.

18. táblázat

Emberi jogok, amelyek az adott infokommunikációs technológia használatával sérülhetnek

Emberi jog	Annak sérelmét okozó IKT
Az emberi szabadság és méltóság (EJENY 1. cikk; PPJNE 10. cikk; RE 3. cikk)	• elektronikus megfigyelés (elektronikus eszközök lehallgatása, CCTV) • DNS-elemzés • elektronikus személyi igazolvány • ez elkövetők elektronikus monitorozása
A hátrányos megkülönböztetés tilalma (EJENY 2. cikk; PPJNE 26. cikk; RE 14. cikk)	• rasszista és xenofób online tartalmak
A gondolat- és véleménynyilvánítás szabadsága (EJENY 18–19. cikk; PPJNE 18–19. cikk; RE 9–10. cikk)	• online kommunikáció megfigyelése, adatok cél nélküli rögzítése • központi tartalomszűrés és -blokkolás
• a biztonsághoz való jog • az embertelen büntetés tilalma • (EJENY 3. és 5. cikk; PPJNE 7. cikk; RE 3. és 5. cikk)	• az elkövetők elektronikus monitorozása • biometrikus azonosítás
• a tisztességes tárgyaláshoz való jog • az ártatlanság vélelme • a büntetés kiszabásának tilalma törvényi rendelkezés nélkül • (EJENY 11. cikk; PPJNE 9. és 14. cikk; RE 6–7. cikk)	• a „veszélyes” személyek monitorozása elektronikus eszközökkel (karperec, lábbilincs, bőr alá ültetett mikrocsip)

[84] A digitális jogokat tágan értelmezve az információhoz jutás szabadsága és a diszkrimináció tilalma körében a nemzetközi egyezmények sora kiegészíthető még az ENSZ Gazdasági, szociális és kulturális jogok nemzetközi egyezségokmányával (hatályba lépett 1976. január 3-án), amely lefekteti a munkához, az egészséges élethez és az ezekhez szükséges tájékozódáshoz és érdekképviselethez való jogokat.

Emberi jog	Annak sérelmét okozó IKT
A fizikai és szellemi tulajdonhoz való jog (EJENY 17. és 27.1. cikk)	• online szerzői művek engedély nélküli letöltése, felhasználása • számítástechnikai rendszerek integritásának megsértése bűncselekménye (hacking) • digitális kémkedés
• a magánélet és a család tiszteletben tartása • (EJENY 12. cikk; PPJNE 17. cikk; RE 8. cikk) • a felejtéshez való jog • (Európai adatvédelmi rendelet [2016/679] 17. cikk])	• elektronikus megfigyelés (elektronikus eszközök lehallgatása, CCTV) • az Európai Unió állampolgárai adatainak engedély nélküli kezelése, feldolgozása és továbbítása
Az élethez való jog (EJENY 3. cikk; PPJNE 6. cikk; RE 1. cikk)	• online szerveződő terrorcselekmények • halálbüntetés IKT bűncselekmény elkövetéséért
A haza ügyeiben részvételhez való jog (EJENY 21. cikk; PPJNE 25. cikk)	• elektronikus megfigyelés • szavazási tevékenység elektronikus megfigyelése

Forrás: SMITH 2011, 397. alapján Parti Katalin szerkesztése

3.5.4.1. A magánélethez való jog

Az Európa Tanács számítástechnikai bűnözésről szóló egyezményét érő kritikák egyik legerőteljesebbike az, amely szerint az adatok valós idejű gyűjtéséről és a tartalomra vonatkozó adatok kifürkészéséről – és a nyomozó hatóság számára átadásáról – szóló szakaszok (20–21. cikk) gyakorlatilag az állampolgári és emberi jogok megsértésére kötelezik az internetszolgáltatókat (SMITH 2011, 398.; TAYLOR 2001).

Az elektronikus személyazonosító igazolványok, az e-útlevelek, és az adatillesztő *(data matching)* technológiák esetében hasonló aggodalmak merülnek fel.

Hongkongban például bevezettek egy multifunkcionális személyazonosító okoskártyát, amely alapvető biometrikus adatokat (portré és ujjlenyomat) tartalmaz, gépjárművezetői engedélyként és könyvtári szolgáltatások igénybevételére is alkalmas (BENITEZ 2002). Az országba érkező menekültek azonosítására az Egyesült Királyság is bevezetett már ilyen okoskártyát (MCAULIFFE 2002).

A biometrikus okoskártyákkal kapcsolatos kételyek között megfogalmazódik, hogy azok lehetővé teszik az előzetes hozzájárulás, illetve cél nélküli adatgyűjtést és felhasználást (funkciók terjeszkedése, *function creep*). Lehetővé válik továbbá a kártyán gyűjtött adatok más adatbázisokkal való összekapcsolása, és a felhasználókról olyan összetett adatbázisok készülhetnek, amelyek a szisztematikus állami megfigyelés *(state surveillance)* alapjául szolgálhatnak (SMITH 2011, 399.).

3.5.4.2. A felejtés joga a digitális korban

A felejtés joga *(right to be forgotten)* talán a legalapvetőbb digitális alapjog, amely a magánélet tiszteletben tartásának jogából ered.

Az Európai Bíróság C-131/12 számú, 2014. május 13-án kihirdetett döntése[85] mondta ki először az európai uniós állampolgárok felejtéshez való jogát a digitális korban.

2010-ben egy spanyol állampolgár a nemzeti adatvédelmi hatósággal közösen nyújtott be panaszt az Európai Bírósághoz egy spanyol napilap, valamint a Google Spain és a Google vállalat ellen. Az állampolgár házát 1998-ban egy ellene irányuló hivatalos eljárás keretében, társadalombiztosítási adósságai behajtása érdekében végrehajtás alá vonták. A hirdetést a spanyol munkaügyi és társadalmi minisztérium online is közzétette. Az állampolgár az eljárás befejeződése után, 2010-ben kérte a Google-t, hogy távolítsa el a neve alatt megjelenő találati listából az eseményre mutató linket, hiszen az időközben relevanciáját vesztette, és egyébként a személyére nézve sérelmes. A Google a kérelem teljesítését megtagadta azzal, hogy a hivatalos közlést a minisztérium kérte hivatalos eljárásban. Az állampolgár panaszában előadta, hogy az ingatlana árverési hirdetményét a Google név szerinti keresési találati listája még évekkel az eljárás befejeződése után is feldobta, noha az eljárás ellene befejeződött. Így a keresőmotor-szolgáltató nemcsak irreleváns adatokat közölt róla, de alapvetően megsértette a magánélet tiszteletben tartásához fűződő jogát is. Kérelme, amelyet az Európai Bírósághoz nyújtott be, először is arra vonatkozott, hogy a hivatalos lap távolítsa el vagy anonimizálja az adott hirdetményt. Másodszor követelte a Google keresőmotortól, hogy a találati listából távolítsa el a neve és az esemény közötti linket.

A Curia döntése szerint minden embernek joga van ahhoz, hogy ne szerepeltesse életének minden mozzanatát az önéletrajzában, tehát mindenkinek saját joga eldönteni, hogy életének mely momentumait nem szeretné egy keresőmotor találati listájában látni. Ennek a rendelkezésnek vulnerábilis társadalmi csoportok esetében, illetve olyan bűncselekmények áldozatai esetében van nagy jelentősége, amelyek tipikusan családon belül fordulnak elő, és az áldozatok számára döntő jelentőségű, hogy adataik rejtve maradjanak, a reviktimizálódást elkerülendő (Google 2014).

A Curia döntése a következőkre terjedt ki:

- Az Európai Unió (adatvédelmi) rendelkezései abban az esetben is kötik az Európai Unióban digitális szolgáltatást nyújtót, ha a szolgáltató szervere külföldön, az Európai Unió joghatóságán kívül eső országban található.
- A keresőmotorok ellenőrzést gyakorolnak a személyes adatok fölött, ebben az értelemben adatkezelők. Éppen ezért a Google nem mentesül az adatkezelőket terhelő felelősség alól.
- A felhasználókat megilleti annak joga, hogy kérhessék a szolgáltatótól a nevük vagy más személyes adatuk és valamely egyéb adat közötti link eltávolítását. Ennek oka lehet, ha az eltávolítani kért információ nem helyes, nem teljes, irreleváns, vagy a tömeges adatfeldolgozás céljára szolgál. A bíróság szerint nem szabad döntést hozni az állampolgárok személyes adatai fölött a keresőmotor-szolgáltató gazdasági érdekei szerint.

[85] Court of Justice of the European Union Press Release No 70/14 Luxembourg, 13 May 2014 Judgement in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González.

A visszaélések napvilágra kerülése a közösségimédia-szolgáltatókat arra indította, hogy a felhasználók bizalmát visszaszerzendő egyfelől szigorítsák az adatvédelmi klauzulákat, másfelől nyomatékkal tegyenek eleget az eltávolítási kéréseknek. A Google például már a Curia hivatkozott döntése előtt is teljesítette a felhasználók személyes adatok eltávolítására vonatkozó kéréseit. A döntést követően azonban olyan tartalmakat is eltávolít már előzetes értesítés nélkül, amelyek gyermekkorúakkal való szexuális visszaélést ábrázolnak vagy erre utalnak. A személyes adatok közül a személyazonosításra alkalmas számokat (például társadalombiztosítási szám, adóazonosító szám, természetes személyek regisztrációs száma illetve személyiigazolvány-szám) távolítják el – a felhasználói feltételekben felsorolt államokban automatikusan, máshol külön kérésre –, továbbá a bankszámlaszámokat, a bank- és hitelkártyaszámokat, az aláírásokról készült képeket, valamint a beleegyezés nélkül feltöltött vagy megosztott, nyíltan szexuális jellegű képeket. A születési dátumot, a címeket és a telefonszámokat nem, de a neveket kérésre eltávolítják. Fontos kitétel, hogy az adott személyes adatot bár törlik, de a mögötte lévő tartalmat nem, így az más keresési feltételekkel továbbra is elérhető marad. Ha például egy újságíró közzéteszi oknyomozó riportját, a riport és a kapcsolódó anyagok mindvégig elérhetők maradnak, még miután a riportban hivatkozott személyek kérték is nevük keresési találatok közül való eltávolítását.[86]

A Curia azt is megállapította, hogy az Európai Unió 1995-ben hatályba lépett adatvédelmi irányelve[87] a technikai fejlődéssel elavulttá vált. Habár az 1995-ös irányelv már tartalmazta a felejtés jogát – miszerint a felhasználó kérhette az adat kezelőjétől adatai eltávolítását, ha nem volt már szükség rá gazdasági (számlázási) okokból –, ám az irányelv a felejtés jogát *expressis verbis* még nem nevesítette.

Az Európai Unió új adatvédelmi rendelete (a továbbiakban: adatvédelmi rendelet) a felejtés jogát a fent bemutatott ítélkezési gyakorlat és a szakmai viták eredményeképpen kikristályosodott formában tartalmazza.[88] Az adatvédelmi rendelet modernizálja az európai adatvédelmi jogot, és az információs kor technikai újításaira tekintettel számos állampolgári jogot deklarál. Megteremti az adatok egységes európai piacát, és a részletszabályok meghozatalában együttműködésre kötelezi a tagállamok jogalkotóit. Az adatvédelmi rendelet legfontosabb újításai a következők:[89]

- A felejtés joga csak üres frázis lenne, ha az európai állampolgárokat nem védené az Európán kívüli adatkezeléssel és -feldolgozással kapcsolatban. Tehát tekintet nélkül arra, hogy fizikailag hol, melyik – akár az Európai Unión kívüli – állam területén található az adatkezelő vagy -feldolgozó cég vagy keresőmotor-szolgáltató szervere, az európai fogyasztók számára kínált és folyósított szolgáltatásoknak az európai szabályoknak kell megfelelniük.[90]

---

[86] Részletes leírását lásd a Google Legal Help oldalán.

[87] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Európai Unió Hivatalos Lapja, L 281, 23/11/1995. 31–50.

[88] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Európai Unió Hivatalos Lapja, L 119/1.

[89] Európai adatvédelmi rendelet 17. cikk: Az adattörlés joga (a felejtéshez való jog).

[90] Európai adatvédelmi rendelet 3. cikk: Területi hatály.

- Hogy a felejtés joga teljes legyen, a bizonyítási terhet az új szabály megfordítja: immár nem az adatkezelésről információt kérelmező személyét, hanem az adatkezelőt terheli annak bizonyítása, hogy az érintettet az adatkezelés köréről azért nem tájékoztatja, mert a kérelem megalapozatlan vagy túlzó jellegű.[91]
- Az adatvédelmi rendelet a nemzeti adatvédelmi hatóságokat (felügyeleti hatóságokat) teszi felelőssé az iránt, hogy gondoskodjanak róla: az adatkezelő eltávolítja, törli vagy hozzáférhetetlenné teszi a felhasználó adatait, amennyiben ő külön kérelmezi. Abban az esetben, ha az adatkezelő a felszólításnak nem tesz eleget, a hatóság korrekciós hatáskörében szankciókkal élhet az adatkezelő ellen.[92]
- Az európai adatvédelmi rendelet kötelezi a tagállamokat a *felejtés jogának* a *szólás- és véleményszabadság jogával* való összhangba hozására, beleértve a sajtó és a média céljára való adatfeldolgozást is. A nemzeti jognak garantálnia kell, hogy a felejtés joga épp olyan magas szintű állampolgári jog legyen, mint a szólásszabadság.[93]

3.5.4.3. A szólásszabadság és a média

A felejtés joga sem a Curia, sem pedig az új európai adatvédelmi rendelet szerint nem abszolút jog.[94] Erre tekintettel minden ügyben egyedileg kell vizsgálni, hogy a személyes adatok tárolása a tárolás vagy feldolgozás eredeti céljához képest szükségtelenné vagy okafogyottá vált-e. Tisztességes egyensúlyt kell kialakítani az internetfelhasználók és az adatkezelés alatt álló személy alapvető jogai között. Az adatkezelőt kötő szabályok ugyanakkor nemcsak az online, hanem az offline szférában is kötöttséget jelentenek. Ez az egyensúly függ az információ természetétől, az adott személy életére gyakorolt hatásától, valamint az információ nyilvánosságához fűződő közösségi érdektől. Az információ relevanciáját az adott személy számára meghatározhatja annak frissessége, naprakészsége is. Bizonyos információk elveszíthetik relevanciájukat az idő múlásával, így az adott személy érdekeinek védelme szempontjából már nem lényegesek. Az adat eltávolítására érkezett kérelmet mindig a személy érdekei, valamint a szólás- és sajtószabadság fényében kell mérlegelni.

Ehelyütt kell szólni a rasszista és idegengyűlölő tartalmak és a szólásszabadság konfliktusáról nemzetközi színtéren. A számítástechnikai bűnözésről szóló egyezmény 2003-ban kelt kiegészítő jegyzőkönyve az ilyen internetes tartalmak büntetendővé nyilvánításának és üldözésének célját és a részes államok együttműködési kötelezettségét fekteti le.[95] Az egységes szabályozási törekvés ellenére az államok belső jogában eltérések tapasz-

---

[91] Európai adatvédelmi rendelet 12. cikk: Az átlátható tájékoztatás joga.

[92] Európai adatvédelmi rendelet 58. cikk (2) bekezdés.

[93] Európai adatvédelmi rendelet Preambulum (153) bekezdés.

[94] Az abszolút jog olyan jog, amellyel szemben más jog érvényesülése nem mérlegelhető. Ilyen az emberi méltósághoz való jog, a vallás szabad megválasztása, az ártatlanság vélelme, a tisztességes eljáráshoz való jog. Lásd: Európai adatvédelmi rendelet Preambulum (4) bekezdés.

[95] ETS. 189 Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of racist and xenophobic nature committed through computer systems. Strasbourg, 28.I.2003. (Magyar nyelven az Országgyűlési Könyvtárban nyomtatott példányban áll rendelkezésre.)

talhatók. Anakronisztikus ellentét áll fenn például az Egyesült Államok és az Európai Unió felfogásában: míg előbbi alkotmányának első kiegészítése a szólásszabadságot elsődleges állampolgári jognak tekinti, amely még a rasszista-idegengyűlölő tartalmak megjelentetését is lehetővé teszi, addig az Európai Unió szigorúan tilalmazza azokat, akár a szólásszabadság rovására. Az Egyesült Államok csak abban az esetben függeszti fel a szólásszabadság jogát, hogyha az ilyen tartalmak azonosítható módon valamely személy vagy személyek elleni bűncselekmény elkövetésére szólítanak fel (WENDEL 2004). A szólásszabadság és az (online) gyűlöletkeltő tartalmak tilalmának konfliktusát az amerikai jogban például a cyberbullying-esetekben hozott ítéletek is szemléltetik (PONGÓ 2016). Az Európai Unióban a Tanács 2007. évi német elnöksége alatt született előterjesztés az információs rendszerben megjelenő gyűlöletkeltő tartalmak elleni egységes fellépésre. A Tanács ennek nyomán 2008-ban fogadta el kerethatározatát, amely biztosítja a természetes és a jogi személyek felelősségre vonását az Európai Unió egész területén.[96] Egyes elemzők szerint ez nemcsak az unió tagállamaiban elkövetett, hanem az Európai Unióban hatását kifejtő – tudniillik európai uniós állampolgárok által elérhető online portálokon megjelenő – rasszista és idegengyűlölő tartalmak esetében is eljárásra jogosít (SIEBER 2012).

Kevin Mitnick, a legendás hacker a számítástechnikai rendszerekbe való jogellenes behatolási tevékenysége miatt csaknem öt évet töltött börtönben, emellett jóvátételként 4 125 dollár büntetést kellett kifizetnie a károsultaknak. A börtönből 2001-ben három évre feltételesen helyezték szabadlábra, ezalatt csak a pártfogó felügyelő eseti, előzetes hozzájárulásával használhatott bármilyen számítástechnikai eszközt, beleértve a mobiltelefont, a szoftverprogramokat, bármilyen, számítástechnikai rendszerbe csatlakozó eszközt (például nyomtatót, modemet), illetve minden további olyat, amelynek segítségével számítástechnikai rendszerrel kapcsolat hozható létre. A foglalkozástól eltiltás részeként sem magánszemélyeknek, sem cégeknek nem adhatott tanácsot számítástechnikai ügyben.[97]

Mitnick az ítélettel szemben fellebbezést nyújtott be azzal, hogy a büntetés az elkövetett cselekmények súlyához képest aránytalanul korlátozza az alkotmány első kiegészítésében lefektetett szólásszabadsághoz való jogot. A bíróság azonban elutasította a fellebbezést, mondván: a számítástechnikai eszközök használata újabb elkövetési lehetőséget biztosítana. Mondhatjuk tehát, hogy a bíróság a büntetés céljának elérése és a visszaesés megelőzése érdekében az Egyesült Államokban is alappal korlátozhatja a szólásszabadságot.[98]

3.5.4.4. Az aránytalan és embertelen büntetés tilalma

Egyes országokban, amilyen például Kína, a *halálbüntetés* nemcsak hogy hatályban van, de számítástechnikai rendszerek elleni bűncselekmények elkövetőire is kiszabják.

A People's Daily Online 2000-ben adott hírt arról, hogy egy 36 éves hackert halálra ítéltek Kína Hangzhou tartományában, mert banki alkalmazottként banki papírok hamisításával és befizetések eltérítésével összesen 1,66 millió jüan (kb. 200 000 USD) összeget

[96] A Tanács 2008/913/IB kerethatározata (2008. november 28.) a rasszizmus és az idegengyűlölet egyes formái és megnyilvánulásai elleni, büntetőjogi eszközökkel történő küzdelemről. Európai Unió Hivatalos Lapja, L 328., 2008. 333–341.

[97] United States v. Kevin Mitnick, No. 97-50365, WL 255343 (9th Circ. Central Ca, May 14, 1998).

[98] United States v. Kevin Mitnick, 145 F.3d 1342 (9th Circ. Central Ca, May 20, 1998).

tulajdonított el különböző számlatulajdonosoktól (PEOPLE'S DAILY ONLINE 2000). Ez a gyakorlat nem egyedülálló: 1998-ban a kínai bíróságok egy hacker testvérpárt ítéltek halálra bankszámlák adatainak kifürkészése és 260 000 renminbi (21 500 GBP) leemelése miatt. Az egyik testvér szintén banki alkalmazott volt (GITTINGS 1998).

Az aránytalan és embertelen büntetés tilalmába ütközhet az *elkövetők elektronikus monitorozása* is. Az elektronikus eszközök testre szerelhetők (például láb- vagy karperecként) vagy bőr alatt helyezhetők el. Az ilyen mikrocsipek bőr alá helyezése, még ha az elkövető beleegyezik is a műveletbe és a megfigyelésébe, egyfelől invazív beavatkozás a magánéletbe, másfelől az eljárás hatékonysága is kérdéses (BRIGHT 2002). A mikrocsipek az illető fiziológiai és földrajzi állapotáról küldenek adatokat a nyomozó hatóság részére, például drogfüggő elkövetők vagy gyermekek elleni szexuális kizsákmányolást elkövetők esetén. Ezeknek az eszközöknek azonban egyfelől nem ismert az összes mellékhatása, másfelől pedig egyáltalán nem biztos, hogy releváns adatok származnak a megfigyelésből. Például a börtönbüntetését kitöltő szexuális elkövető átélhet szexuális izgalmat úgy is, hogy azzal nem veszélyezteti környezetét. Az elektronikus monitorozó berendezések használatát előzetesen sokszor nem evaluálják, így kérdéses, hogy hatékonyságuk arányban áll-e a kifejlesztésükkel és alkalmazásukkal járó anyagi ráfordítással (BLACK–SMITH 2003), nem beszélve a testi épséghez és integritáshoz fűződő jog sérelmével.

Ausztrália a terrorcselekmények megelőzésére tett proaktív intézkedési csomagja részeként, még az internet elterjedése előtt, 1995-ben törvénybe iktatta az elektronikus monitorozás lehetőségét (SMITH 2011, 405.). A jogszabály szentesíti konkrét terrorcselekményt el nem követő személyek megfigyelését is, hogyha azok részt vettek valamely terrorista csoport által szervezett tréningen, vagy ilyen tréninget tartottak, vagy kínálnak. Habár az elektronikus monitorozás – amely ugyancsak végrehajtható bőr alá ültethető microcsip segítségével – csak bírói ellenjegyzéssel rendelhető el, számos emberi jogi kérdést vet fel (BYRNES et al. 2005). Felmerül a hatékonyság kérdése is, hiszen nem tudhatjuk, hogy a megfigyelésnek ez a formája mennyire alkalmas a terrortámadások megelőzésére.

3.5.4.5. Megfigyelés és viszontfigyelés

A felülről jövő, valamely hatóság vagy központi szerv által történő megfigyelés *(surveillance)* technológiái a modern kori terrortámadások nyomán terjedtek el, céljuk az állampolgári biztonság, a közbiztonság garantálása. Ezzel szemben az alulról, az állampolgárok és a civil szervezetek általi megfigyelés, azaz viszontfigyelés (*sousveillance*: MANN et al. 2003) csak később, a 2010-es évek második felében kezdett terjedni. Ennek okaként említhetnénk Snowden mellett a Wikileaks kiszivárogtatási tevékenységét, amely nyomán számos, a hatalom általi túlkapásra, az állampolgári jogok csorbítására, de legalábbis annak potenciális lehetőségeire derült fény (GARRIDO 2015). Egy másik releváns példa az alulról jövő, a hatalmat gyakorló entitás feletti kontrollt biztosító megfigyelésre a testre szerelhető mikrokamerák megjelenése és használatuk elterjedése.

Egy ilyen, járókelők által mobiltelefonnal készített rövid videó volt az alapja annak a büntetőeljárásnak, amelyet Michael Slager dél-karolinai rendőrtiszt ellen folytattak az Egyesült Államokban. A rendőrtiszt ellen lőfegyver indokolatlan használata, valamint emberölés miatt indult büntetőeljárás, miután 2015 áprilisában egy rutinigazoltatást köve-

tően a személygépkocsiját elhagyó és menekülésnek induló állampolgárt, Walter Scottot lelőtte (TNYT 2015). A négy percnél is hosszabb videó látszólag hitelesen, azonban kontextusából kiragadva, egyoldalúan mutatja be az eseményt. A kamerával felszerelt mobileszközök tömeges elterjedése óta számos ügyben használtak fel bizonyítékul civilek által készített videót büntetőperben (BERMAN 2016).

David Lyon, a *megfigyelés társadalmának* kutatója arról ír, hogy a Snowden által kiszivárogtatott adattömeg elemzése egy eddig nem tapasztalt problémával szembesíti a tudományos közösséget és az adatvédő szervezeteket (LYON 2015). Egyfelől nem tudjuk, *milyen módszerrel válasszuk ki* az anyagok közül a relevánsakat. Másfelől nem tudjuk, hogy *milyen módszerrel elemezzük ezek lehetséges hatásait.* Harmadik problémaként *nem tudjuk bizonyítani,* hogy a titkosszolgálatok által gyűjtött adatok valóban *nem* szolgálják a terrorizmus elhárítását. Nem tudjuk, hogy a gyűjtött adatok felhasználásával milyen és mennyi fenyegető terrortámadást sikerült megelőzni. Végül nem vagyunk olyan elemző algoritmusok birtokában, amelyek segítségével megérthetnénk, hogy az elmúlt 40 év adatgyűjtése, amelyet az állam a polgárai kommunikációjának megfigyelésére használt, mennyire komplex, és *milyen visszaélések történtek a megfigyelések segítségével az állampolgárok ellen.* Habár a digitális kor előtt is volt megfigyelés, akkor még az állampolgárban nem tudatosult, hogy mennyi nyomot hagy maga után azzal, ha csupán kommunikál vagy helyet változtat (VLADECK 2014).

Az adatok tömegének elemzése és az állampolgári jogok sérelmének vizsgálata szempontjából releváns adatok kiválasztása, valamint az adatkezelés céljának ellenőrzése a big datával kapcsolatos problémákra vezet vissza. Moore törvénye szerint minden 18–24. hónapban megduplázódik az integrált áramkörök összetettsége (Moore törvényét Kurzweil dolgozta ki és terjesztette ki minden jövőbeli technológiára is). Ez az adatok egyre összetettebb elemzésének képességét is jelenti (ROUVROY 2016, 5.). Nielsen törvénye szerint minden 21. hónapban megduplázódik a kapcsolat sebessége, Kryder pedig 2005-ben azt jelezte előre, hogy a mágneslemezen tárolható adatok sűrűsége 13 havonta duplázódik meg.[99] Ha ehhez hozzávesszük, hogy azóta feltaláltak nagyobb tárolókapacitású adathordozókat is, amilyen például az SSD, egyértelműnek látszik, hogy a jóslat bevált.

3.5.5. Az internetszabályozás és az alapjogok kapcsolata

Az előzőekben bemutattuk az internet szabályozásában részt vevő szereplőket. Megmutattuk, hogy ez a szabályozás evolucionális folyamat, amely még ma sem ért véget – az új technológiák megjelenésével ez is folyamatos. Szóltunk a digitalizálódással potenciálisan sérülő emberi jogokról és arról, milyen új színezetet kapnak a hagyományos alapjogok a big data korában. Most tekintsük át, milyen szerepe van *az önszabályozás aktorainak a jogok formálásában!*

Az információs társadalommal összefüggő jogok interpretálásában, az alapjogok internetre „lefordításában" először is jelentős szerepe volt az ENSZ Internetszabályozó Munkacsoportjának (Working Group on Internet Governance – WGIG). A WGIG 2005-ben

[99] Moore, Kurzweil, Nielsen és Kryder törvényéről lásd: www.flydata.com/blog/moores-law-kryders-law/ (A letöltés dátuma: 2018. 05. 15.)

terjesztette elő az internet szabályozásának többszereplős modelljéről szóló ajánlását,[100] amely azonosítja az internet szabályozásával és az új technológiák fejlesztésével potenciálisan sérülő emberi jogokat. A WGIG tevékenységéből nőtt ki az Internetszabályozó Fórum (Internet Governance Forum – IGF), amely számos úgynevezett dinamikus koalíciót hozott létre azokból a piaci szereplőkből, amelyek saját (gazdasági) területüket alakítják. Idetartozik példának okáért a Magánélet, a Szólásszabadság, az Online Média Dinamikus Koalíciója, az Internet Alapjogainak Keretkoalíciója, a Nyelvi Diverzió, és a Társadalmi Nem és Internetszabályozás vagy a Távoli, Vidéki, Szétszóródó Közösségek Internetkapcsolatának Dinamikus Koalíciója.[101] A dinamikus koalíciók körében fogalmazódott meg az internetes jognyilatkozat (Internet Bill of Rights) gondolata, amelyet 2010-ben terjesztettek elő Vilniusban.[102] Ez a jognyilatkozat nem új jogokat fogalmaz meg, hanem a meglévő emberi alapjogokat értelmezi az információs társadalomban.

A *dinamikus koalíciók* által újraértelmezett jogok közül ehelyütt csupán egyet emelünk ki, a *diszkrimináció tilalmát.* A hátrányos megkülönböztetés tilalmát a korábban hivatkozott emberi jogi egyezmények deklarálják (lásd a 18. táblázatot). Azonban a jogok tartalma az információs korban átalakult. A dinamikus koalíciók a diszkrimináció tilalmát a tudáshoz való joggal kapcsolják össze. Abból indulnak ki, hogy a Földnek nem minden táján azonos az információs szabadság, már csak amiatt sem, mert a gazdasági peremvidéken lévő, harmadik világbeli régiókban az internetpenetráció csak töredéke a fejlett, első világbeli országokénak. Például míg Afrikában a teljes lakosság kevesebb mint egyharmada (27,7%), addig az európai lakosság (77,4%) és az észak-amerikai lakosság (88,1%) túlnyomó része rendelkezik interneteléréssel.[103] Az alacsony internetpenetrációval rendelkező országok lakossága kevesebb információ birtokában kevesebb munkalehetőséghez is jut, és kevésbé tudja érvényesíteni a jogait is – úgy dolgozóként, mint állampolgárként (Benedek 2008). Ezeknek a problémáknak a tárgyalására jött létre a Progresszív Kommunikáció Szövetség (Association for Progressive Communication – APC), amely szintén a piaci és civil szereplők összefogásának az eredménye.[104] Az APC az internetdiplomácia eszközeivel fejti ki tevékenységét: összehozza a gazdaság, a szakpolitika és a civil társadalom lokális szereplőit (például a szoftverfejlesztő cégeket, a közoktatási szakpolitikusokat és a csellengő fiatalokat összefogó helyi NGO-kat), és eléri, hogy a lokális problémák és igények ismeretében jól hasznosítható megoldások szülessenek.

Az APC egyik elemzője, David Souter 2017 tavaszán írt arról (Scouter 2017), hogy egy indiai kis faluban, Keralában egy halászközösség megélhetését mennyire fellendítette a mobilkommunikációs technológia. Az eredeti elemzést 2001-ben publikálta Robert Jehnsen társadalomkutató (Jehnsen 2007), aki 1997 és 2001 között gyűjtött empirikus adatokat a kis indiai falu mélyszegénységben élő halászairól. A jórészt még saját csónakkal sem rendelkező szegény halászok életében az hozta a fordulatot, amikor egy helyi telekommunikációs szolgáltató megfizethető áron kezdte kínálni a mobiltelefonokat. Pár telefonhívás

[100] *Tunis Agenda for the Information Society* (2005). WSIS-05/TUNIS/DOC/6 (Rev. 1)-E, 18 November. Elérhető: www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (A letöltés dátuma: 2018. 05. 15.)

[101] A dinamikus koalíciók teljes listáját lásd: www.intgovforum.org/cms/dynamiccoalitions (A letöltés dátuma: 2018. 05. 15.)

[102] Internet Bill of Rights: www.internetrightsandprinciples.org (A letöltés dátuma: 2018. 05. 15.)

[103] Internet World Stats: www.internetworldstats.com/stats.htm (A letöltés dátuma: 2018. 05. 15.)

[104] Association for Progressive Communication: www.apc.org/node/5677 (A letöltés dátuma: 2018. 05. 15.)

segítségével a halászok gyorsan felderítették, melyik szomszédos kis faluban van szükség éppen halra, és a kifogott árut a kereslet helyére szállították. A vizsgált időszakban az 1996-os minimális szintről 2001-re csaknem maximális szintet ért el a halászok által értékesített halzsákmány, akik a telefonok segítségével ki tudták játszani a nagyobb halforgalmazókat és disztribútorokat, és nem volt már szükségük közvetítő kereskedőkre sem. A halászok profitjának növekedésével a helyi lakosság életszínvonala is emelkedni kezdett.

De David Souter feladata nem kizárólag az, hogy hírt adjon a kis helyi sikerekről, és ezáltal másolhatóvá tegye azokat más közösségek számára. Souter és az APC elemzői híradásaikban provokatív kérdéseket tesznek fel, amelyek elgondolkodásra és párbeszédre késztetik a helyi IKT-ipart, a gazdaságot, a piaci szereplőket és a szakpolitikusokat. Az idézett esetben nemcsak fellendülésről volt szó, hanem a mobiltelefónia számos kritikus kérdést is felvetett. Például azt, hogy vajon hogyan reagál majd a piac ezekre a változásokra hosszú távon? Kivonulnak-e a nagykereskedők, vagy integrálni próbálják a kicsiket? Hogyan változott a halkínálat és a helyi ökoszisztéma? Lehetséges, hogy a halászok az okostelefónia más lehetőségével is élnek, vagy esetleg szonárt is használnak, aminek következményeként a halállomány lassan elapad, és ennek következtében a halászok is feladni kényszerülnek mesterségüket? Hol fognak akkor elhelyezkedni, hogyha a nagykereskedők már mind kivonultak a helyi piacról, és profilt váltottak? Hogyan fogja ez érinteni a lakosság fennmaradó részét? Hogyan éleszthető fel – vagy teremthető meg – az IKT, a piaci szereplők és a helyi lakosság együttműködése a helyi igényeknek megfelelően?

3.5.6. Jogok az információs társadalomban: Quo vadis?

Nem kétséges, hogy az információs társadalomban a legfontosabb emberi jog a felejtés joga. Székely Iván információstársadalom-kutató pamfletjében összehasonlítja az információ (összefoglalóan internet) előtti kor és az információ korának jellemzőit (SZÉKELY 2012). Míg korábban a felejtés volt az uralkodó szabály, addig az információs korban nem engedhetjük meg a felejtés luxusát. Több okból alakult ez így:

A felejtés pénzbe kerül. Korábban az információ rögzítése, tárolása és feldolgozása volt drága, ma viszont, amikor az információ lett a legnagyobb érték, már eleve az adatok végtelen tárolására tervezzük a jövőnket. Ebben a technikai környezetben az információ elfelejtése, törlése válik költségessé és luxussá.

Az információs rendszerek biztosítják a társadalmi kontrollt: az információs kor előtt a szabályok betartására valamely felső entitás – törvények, börtönőrök, állam, illetve bíróságok – ügyelt. Ez volt a *habeas corpus* kora, a boldog békeidő, amikor tudvalevő volt, ki a megfigyelő, és hol, milyen tevékenységünk közben figyelnek meg minket, ahogy az is, hol, mivel kapcsolatban, ki fogja felhasználni a megfigyelés eredményét. Az információs társadalomban a megfigyelés allegóriájává Jeremy Bentham Panoptikonja szolgál (BENTHAM 1995), amelyben a (központi) megfigyelést végző őr számára látható és ellenőrizhető a rabok celláikban végzett tevékenysége. Az információ korában a megfigyelő szerepét átvette a gép: azzal, hogy folyamatosan kapcsolatban vagyunk a digitális világgal, automatikusan jeleket küldünk magunkról – földrajzi helyünkről, munkánkkal, szabadidőnkkel vagy utazásunkkal kapcsolatos tevékenységeinkről. Szolgáltatásokat veszünk igénybe, kommuni-

kálunk – mindez hozzáadódik digitális lábnyomunkhoz. Az ember nem csupán hús és vér, hanem adatokból összeálló képződmény, *habeas data* (PAGALLO 2012, 339.), aki a rendszer használatával önként vállalja, hogy részt vesz az adatgyűjtés ubikvitális rendszerében, a megfigyelés társadalmában *(surveillance society),*[105] és ezzel saját maga megfigyelését vállalja. Foucault a jelenségre az 1970-as években a televíziónézéssel, illetve a börtönzárkákba szerelt tévékészülékek hatásával összefüggésben hívta fel a figyelmet, de a gépek, a használati tárgyak általi megfigyelés, a monitorozás az információs korban teljesedik ki (FOUCAULT 1990). Ez a kor panoptikon helyett inkább periptikonhoz (vagy kriptoptikonhoz) hasonlít, amelyben nem tudható, hogy ki, mikor, milyen eszközzel végzi a megfigyelésünket, mint ahogy az sem, hogy ki, mikor, milyen célból fogja felhasználni a rólunk gyűjtött adatokat (SZÉKELY 2012). Székely szerint azzal, hogy nem megengedett (illetve technikailag nem a rendszerbe beépített opció) a felejtés, a múlt börtönébe zárjuk magunkat – az információ tehát maga a kontroll eszköze (SZÉKELY 2012). A kontroll és a szabály pedig a társadalmi együttélés alapja, ami az információ korában teljesen digitálissá vált.

A digitalizációval lehetővé válik a *kockázati társadalom* (BECK U. 2003) magas szintű megvalósítása: a biztosítók számítástechnikai programok, algoritmusok segítségével statisztikai valószínűséggel számítják ki valamely baleset vagy biztosítási esemény bekövetkezésének valószínűségét. Ugyanez az előrejelzés jelenik meg a felhasználói viselkedéshez idomuló reklámokban (viselkedésalapú hirdetés). A nyomozó hatóság szoftverek segítségével időzíti és szervezi a bűnmegelőzési programjait, bekalkulálva a múltban történt eseményeket és a sértettek jellemzőit. A fogvatartási intézményekből szabaduló súlyos bűncselekmények elkövetői (például szexuális bűnelkövetők) visszaesésének prediktálására néhány ország bevezette a bűnismétlésikockázat-menedzsment rendszerét (ilyen például az Egyesült Királyságban a ViSOR,[106] az Egyesült Államokban pedig a NSOPW).[107] A bűnelkövetők rádiófrekvenciás (RFID) monitorozását számos európai uniós ország alkalmazza már a 2000-es évektől kezdve (THAN 2016). Mára a német parlament, a Bundestag elfogadta azt a törvényjavaslatot, amely lehetővé teszi azoknak a megfigyelését, akik bár bűncselekményt nem követtek el, de – a terrorizmus elleni harc égisze alatt – a titkosszolgálatok megfigyelése alatt állnak (DIE WELT 2017).

3.5.7. Merre tartunk hát?

Mind a szabályozás, mind pedig a technika adta lehetőségek összességében pozitív képet vetítenek előre. Az internet többszereplős szabályozási modellje megvalósulásának lehetünk tanúi, amelyben az államok, a magánszféra és a civil szereplők is közreműködnek, így biztosítva egymás törekvései fölött a fékek és ellensúlyok rendszerének dinamizmusát. A technológia pedig mindamellett, hogy elsősorban üzleti és nemzetbiztonsági érdekeket

[105] A megfigyelés társadalma a 21. században népszerű kutatási területté nőtte ki magát, lásd például a következő nemzetközi kutatócsoportok munkáját: Living in Surveillance Societies (LiSS), Surveillance Studies Network (SSN).

[106] Violent and Sex Offender Register, UK, Centre for Crime and Justice Studies. Elérhető: www.crimeandjustice.org.uk/publications/cjm/article/visor-violent-and-sex-offender-register (A letöltés dátuma: 2018. 05. 15.)

[107] National Sex Offender Public Website, U.S. Department of Justice. Elérhető: www.nsopw.gov/ (A letöltés dátuma: 2018. 05. 15.)

követ, magában hordozza azokat a lehetőségeket is, amelyek nyomán megvalósulhat a kérelmezett felejtés *(forgetting on demand)* társadalma.

A *magánéletbarát adatbányász* (privacy preserving data mining – PPDM) technikák a big data korában is lehetőséget nyújtanak arra, hogy az adat és az adatalany közötti linket titkosítsák úgy, hogy az ne legyen helyreállítható. Ilyen módon a felhasználó által valamilyen szolgáltatás igénybevételéhez felvitt digitális adatok nem használhatók fel más célra, csakis az adott szolgáltatásra (WANG et al. 2004). A PRIME (korábban PrimeLife) olyan szoftver, amely – ha PRIME-kompatibilis keresőmotorokon és digitális felületeken használják – minden weboldalról, közösségi oldalról és a keresőmotorok találati listáiból is eltávolíthatja a személyes adatainkat és képeinket[108] (FISHER-HÜBNER et al. 2013). A U-Prove egy olyan összetett titkosítási alkalmazás, amelynek segítségével bármilyen további információ bevitele nélkül azonosíthatjuk magunkat az interneten, és személyes adataink az autentikáció során sem válnak publikussá, azaz harmadik fél számára kereshetővé. Az alkalmazás privát fejlesztés, de a Microsoft megvásárolta és bizonyos csomagjai részévé tette (HOEPMANN 2014).

Mindezek a fejlemények azt sugallják: van remény arra, hogy az információs társadalom időről időre kitermeli a felejtéshez – és a magánéletéhez – ragaszkodó felhasználó számára a saját ellensúlyait.

Végül, de nem utolsósorban mind a bevezetés előtt, mind az alkalmazás folyamatában hatástanulmányokat szükséges készíteni arról, hogy az invazív elektronikus eszközök – amilyenek a megfigyelésre használt mikrocsipek és egyéb kamerák, adatlehallgató szoftverek – arányban állnak-e az általuk érintett emberi jogok korlátozásával, és beváltják-e a hozzájuk fűzött prevenciós reményeket.

[108] A PRIME projekt: http://primelife.ercim.eu (A letöltés dátuma: 2018. 05. 15.)

Felhasznált irodalom

Adler, Freda – Mueller, Gerhard O. W. – Laufer, William S. (2005): *Kriminológia.* Budapest, Osiris.

Agustina, José R. (2012): Analysing Sexting from a Criminological Perspective. Beyond child pornography issues: Sexting as a threshold for victimization. In Reich, Pauline C. ed.: *Cybercrime & Security.* West, Thomson Reuters, Vol. 4, 64–96.

Agustina, José R. (2015): Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology,* Vol. 9, No. 1. 35–54.

Allport, Gordon W. (1977): *Az előítélet.* Budapest, Gondolat.

Andorka Rudolf – Buda Béla – Cseh-Szombathy László szerk. (1974): *A deviáns viselkedés szociológiája.* Budapest, Gondolat.

Asch, Solomon E. (1980): A csoportnyomás hatása az ítéletek módosulására és eltorzulására. In Pataki Ferenc szerk.: *Csoportlélektan.* Budapest, Gondolat. 210–222.

Bandura, Albert (1978): The self system in reciprocal determinism. *American Psychologist,* Vol. 33, No. 4. 344–358.

Barabási Albert-László (2013): *Behálózva. A hálózatok új tudománya.* Budapest, Helikon.

Bard, Alexander – Söderqvist, Jan (2002): *Netocracy – the new power elite and life after capitalism.* London, Pearson Education.

Beck, Aaron T. (1999): *A gyűlölet fogságában.* Budapest, Háttér.

Bell, Daniel (1976): *The Coming of Post-Industrial Society.* New York, Basic Books.

Berzsenyi Dániel válogatott versei (2006). Válogatta: Tarján Tamás. Budapest, Holnap Kiadó.

Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk. (2016): *Kriminológia.* Budapest, Wolters Kluwer.

Buda Béla (2002): *Szexuális viselkedés.* Budapest, Animula.

Burt, Martha R. (1980): Cultural myths and supports for rape. *Journal of Personality and Social Psychology,* Vol. 38, No. 2. 217–230.

Campbell, Joseph W. (2015): *'Cyberporn' scare of 1995 demonstrates the early Web's corrective power.* Elérhető: https://1995blog.com/2015/07/01/the-cyberporn-scare-of-1995-demonstrating-the-early-webs-corrective-power/ (A letöltés dátuma: 2018. 05. 15.)

Castells, Manuel (2005): *A hálózati társadalom kialakulása.* Budapest, Gondolat–Infónia.

Castells, Manuel (2007): *Az évezred vége.* Budapest, Gondolat–Infónia.

Chiesa, Raul – Ducci, Stefania – Ciappi, Silvio (2009): *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking.* Boca Raton, CRC Press.

Choi, Kyung-Shick (2008): Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology,* Vol. 2, No. 1. 308–333.

Csepeli György (1997): *Szociálpszichológia.* Budapest, Osiris.

Csepeli György (2005): *A meghatározatlan állat.* Budapest, Jószöveg.

Csepeli György (2014): *Szociálpszichológia mindenkiben.* Budapest, Kossuth.

Csepeli György – Prazsák Gergő (2010): *Örök visszatérés? Társadalom az információs korban.* Budapest, Jószöveg.

CSEPELI György – PRAZSÁK Gergő (2013): *Információs társadalom 2.0. Elsődleges és másodlagos digitális egyenlőtlenségek*. Társadalominformatika, ELTE TáTK. Elérhető: http://tarsadalominformatika.elte.hu/tananyagok/informaciostarsadalo/ (A letöltés dátuma: 2018. 05. 15.)

CSERMELY Péter (2004): *A rejtett hálózatok ereje. Hogyan stabilizálják a világot a gyenge kapcsolatok?* Budapest, Vince.

DARWIN, Charles (1961): *Az ember származása és a nemi kiválasztás.* Budapest, Gondolat.

DAWKINS, Richard (2011): *Az önző gén.* Budapest, Kossuth.

DE MONTJOYE, Yves-Alexandre – HIDALGO, César A. – VERLEYSEN, Michel – BLONDEL, Vincent D. (2013): Unique in the crowd: The privacy bounds of human mobility. S*cientific Reports,* Vol 3.

DE MONTJOYE, Yves-Alexandre (2015): Unique in the shopping mall: On the re-identifiability of credit card metadata. *Science,* Vol. 347, No. 6221. 536–539.

DONALD, Merlin (2001): *Az emberi gondolkodás eredete.* Budapest, Osiris.

DRESSING, Harald – BAILER, Josef – ANDERS, Anne – WAGNER, Henriette – GALLAS, Christine (2014): Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking,* Vol. 17, No. 2. 61–67.

DUNBAR, Robin (1998): The Social Brain Hipothesis. *Evolutionary Anthropology,* Vol. 6, No. 5. 178–190.

DUNBAR, Robin (2006): Vannak-e korlátai az e-világnak? *Világosság,* 47. évf. 6–7. sz. 149–158.

ELIAS, Norbert (2004): *A civilizáció folyamata.* Budapest, Gondolat.

ELLIOT, Ian A. – BEECH, Anthony R. – MANDEVILLE-NORDEN, Rebecca – HAYES, Elizabeth (2009): Psychological profiles of Internet sexual offenders: Comparisons with contact sexual offenders. *Sexual Abuse: A Journal of Research and Treatment,* Vol. 21, No. 1. 76–92.

ENGLANDER, Elizabeth K. (2013): *Bullying and Cyberbullying: What Every Educator Needs to Know.* Cambridge, Harvard Education Press.

FÁBRY György (2013): Megváltoztatta az internet a gondolkodásomat. In VESZELSZKI Ágnes szerk.: *A világhálóba keveredett ember.* Budapest, ELTE Eötvös. 58–66.

FARRINGTON, David P. (1993): Understanding and preventing bullying. In TONRY, Michael ed.: *Crime and Justice.* Chicago, University of Chicago Press, Vol. 17, 381–458.

FÁZSI László – FÁZSI László Milán (2009): Megjegyzések a számítógépes bűncselekmények hatályos szabályozásához. *Rendészeti Szemle,* 57. évf. 5. sz. 3–11.

FEHÉR Irén – LAPPINTS Árpád (1999): *Pedagógiai fogalomtár.* Pécs, Comenius.

FEKETE Mariann (2018): *eIdő, avagy a szabadidő behálózása. Generációs kultúrafogyasztás a digitális korban.* Szeged, Belvedere Meridionale.

FISHER, William A. – BARAK, Azy (2001): Internet pornography: A social psychological perspective on Internet sexuality. *Journal of Sex Research,* Vol. 38, No. 4. 312–323.

FISHER-HÜBNER, Simone – ANGULO, Julio – PULLS, Tobias (2013): How can Cloud Users be Supported in Deciding on, Tracking and Controlling. How their Data are Used? In HANSEN, Marit – HOEPMAN, Jaap-Henk – LEENES, Ronald – WHITEHOUSE, Diane eds.: *Privacy and Identity Management for Emerging Services and Technologies.* Nijmegen, International Summer School, June 17–21. 77–92.

FÖTINGER, Christian S. – ZIEGLER, Wolfgang (2004): *Understanding a hacker's mind – a psychological insight into the hijacking of identities.* Austria, Donau Universität Krems–RSA Security. Elérhető: www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf (A letöltés dátuma: 2018. 05. 15.)

Fromm, Erich (2001): *A rombolás anatómiája.* Budapest, Háttér.
Furnell, Steven (2002): *Cybercrime: Vandalizing the Information Society.* London, Addison-Wesley.
Genoni, Paul – Merrick, Helen – Willson, Michele A. (2005): The use of the Internet to activate latent ties in scholary communities. *First Monday,* Vol. 10, No. 12.
Giddens, Anthony (2008): *Szociológia.* Második kiadás. Budapest, Osiris.
Gonsalves, Valerie M. (2010): *Exploring Online Sexually Explicit Material: What is the Relationship to Sexual Coercion? A Dissertation.* Lincoln, University of Nebraska.
Gönczöl Katalin – Kerezsi Klára szerk. (1993): *A deviancia szociológiája.* Budapest, T-Twins.
Grabosky, Peter N. (2001): Virtual criminality: Old wine in new bottles? *Social and Legal Studies,* Vol. 10, No. 2. 243–249.
Grabosky, Peter N. – Smith, Russel G. (2001): Digital Crime in the Twenty-first Century. *Journal of Information Ethics,* Vol. 10, No. 1. 8–26.
Griffin, Em (2003): *Bevezetés a kommunikációelméletbe.* Budapest, Harmat.
Grimmelmann, James (2012): Sealand, Havenco, and the rule of law. *University of Illinois Law Review,* Vol. 2012, No. 2. 405–485.
Gunter, Whitney D. (2011): Criminological Predictors of Digital Piracy: A Path Analysis. In Jaishankar, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press. 173–190.
Győry Csaba (2016): Kontrollelméletek. In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 177–192.
Habermas, Jürgen (1971): *A társadalmi nyilvánosság szerkezetváltozása.* Budapest, Gondolat.
Halder, Debarati – Jaishankar, Karuppannan (2011): Online social networking and women victims. In Jaishankar, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press. 305–307.
Hamilton, Melissa (2012): The Child Pornography Crusade and its Net-Widening Effect. *Cardozo Law Review,* Vol. 33, No. 4. 1679–1732.
Hampson, Noah C. N. (2012): Hacktivism: A new breed of protest in a networked world. *Boston College International and Comparative Law Review,* Vol. 35, No. 2. 511–542.
Hankiss, Elemér (1977): *Értékszociológiai kísérlet.* Budapest, Népművelési Intézet.
Hankiss, Elemér (2011): *Életstratégiák a bizonytalanság korában.* TEDX-előadás. Elérhető: www.youtube.com/watch?v=evw2qQRQziM&vl=hu (A letöltés dátuma: 2018. 05. 15.)
Hárdi István (2010): *Az agresszió világa.* Budapest, Medicina.
Heidegger, Martin (2003): Levél a humanizmusról. In Pongrácz Tibor szerk.: *Útjelzők.* Budapest, Osiris. 293–334.
Hinduja, Sameer – Patchin, Justin W. (2015): *Bullying Beyond the Schoolyard. Preventing and Responding to Cyberbullying.* 2nd ed. Thousand Oaks, SAGE.
Hoepman Jaap-Henk (2014): Privacy design strategies. In Cuppens-Boulahia, Nora – Cuppens, Frédéric – Jajodia, Sushil – El Kalam, Abou A. – Sans, Thierry eds.: *ICT Systems Security and Privacy Protection. 29th IFIP TC 11 International Security Conference Marrakech, Morocco, June 2–4, 2014.* Berlin–Heidelberg, Springer. 446–459.
Hudson, James M. – Bruckman, Amy S. (2004): The Bystander Effect: A Lens for Understanding Patterns of Participation. *The Journal of the Learning Sciences,* Vol. 13, No. 2. 165–195.
Inglehart, Ronald (1997): *Modernization and Postmodernization: Cultural, Economic, and Political Change in 43 Societies.* Princeton–New Jersey, Princeton University Press.

INGLEHART, Ronald (2003): *Human Values and Social Change: Findings from the Values Surveys.* Leiden–Boston, Brill.

INGLEHART, Ronald (2004): *Human Beliefs and Values: A Cross-cultural Sourcebook Based on the 1999-2002 Values Surveys.* México, Siglo XXI Editores.

JAISHANKAR, Karuppannan (2008): Space transition theory of cyber crimes. In SCHMALLEGER, Frank – PITTARO, Michael eds.: *Crimes of the Internet.* Upper Saddle River, Prentice Hall. 283–301.

JORDAN, Tim – TAYLOR, Paul A. (1998): A Sociology of Hackers. *The Sociological Review,* Vol. 46, No. 4. 757–780.

KHAZOV-CASSIA, Sergei (2017): Teen 'Suicide Games' Send Shudders Through Russian-Speaking World. *Radio Free Europe – Radio Liberty,* February 21. Elérhető: www.rferl.org/a/russia-teen-suicide-blue-whale-internet-social-media-game/28322884.html (A letöltés dátuma: 2018. 05. 15.)

KISS Tibor – PARTI Katalin (2016): A mém vajon mi? A mémekért való felelősség megállapíthatóságának kérdései és lehetőségei. *Infokommunikáció és Jog,* 66–67. sz. 39–47.

KISS Tibor (2013): Az internet és a társadalmi egyenlőtlenségek. *Információs Társadalom,* 13. évf. 3–4. sz. 97–99.

KISS Tibor (2014a): Áldozattá válás dimenziói az online színtéren. In FAZEKAS Marianna szerk.: *Jogi tanulmányok 2014.* Budapest, ELTE ÁJK. 382–393.

KISS Tibor (2014b): Gyűlölet-bűncselekmények és szélsőséges csoportok az információs társadalomban. In PRAZSÁK Gergő szerk.: *Nemzeti szempont.* Budapest, Aperion. 71–92.

KISS Tibor (2016): Internetes mémek mint káros információs egységek a tartalom-bűncselekmények körében. In FAZEKAS Marianna szerk.: *Jogi tanulmányok 2016.* Budapest, ELTE ÁJK. 350–360.

KLUCKHOHN, Clyde (1951): Values and value orientations in the theory of action. In PARSONS, Talcott – SHILS, Edward eds.: *Toward a General Theory of Action*. Cambridge, Harvard University Press. 388–433. Elérhető: https://archive.org/details/towardgeneralthe00pars (A letöltés dátuma: 2018. 05. 15.)

KORINEK László (2010): *Kriminológia I.* Budapest, Magyar Közlöny Lap- és Könyvkiadó.

KÜRTI Sándor (2002): Az informatikai bűnözés gyökerei. *Belügyi Szemle,* 50. évf. 11–12. sz. 10–26.

LAKATOS Krisztina – GERVAI Judit (2003): A korai kötődés neurobiológiai háttere. In PLÉH Csaba – KOVÁCS Gyula – GULYÁS Balázs szerk.: *Kognitív idegtudomány.* Budapest, Osiris. 326–342.

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

LICKIEWICZ, Jakub (2011): Cyber Crime Psychology – Proposal of an Offender Psychological Profile. *Problems of Forensic Sciences,* No. 87. 239–252.

MALAMUTH, Neil M. – CHECK, James V. P. (1985): The Effects of Aggressive Pornography on Beliefs in Rape Myths: Individual Differences. *Journal of Research in Personality,* Vol. 19, 299–320.

MARCUM, Catherine D. (2011): Adolescent online victimization and Constructs of Routine Activities theory. In JAISHANKAR, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press. 253–256.

MARTINEZ-PRATHER, Kathy – VANDIVER, Donna M. (2014): Sexting among Teenagers in the United States: A Retrospective Analysis of Identifying Motivating Factors, Potential Targets, and the Role of a Capable Guardian. *International Journal of Cyber Criminology,* Vol. 8, No. 1. 21–35.

MCCRAE, Robert R. – COSTA Jr., Paul T. (2004): A contemplated revision of the NEO Five-Factor Inventory. *Personality and Individual Differences,* Vol. 36, 587–596.

MCGUIRE, Michael (2007): *Hypercrime. The New Geometry of Harm (UCL).* New York, Routledge.

Mead, George H. (1973): *A pszichikum, az én és a társadalom.* Budapest, Gondolat.
Merton, Robert K. (2002): *Társadalomelmélet és társadalmi struktúra.* Budapest, Orisis.
Mitnick, Kevin D. – Simon, William L. (2003): *A legendás hacker – A megtévesztés művészete.* Budapest, Perfact.
Modecki, Kathryn L. – Barber, Bonnie L. – Vernon, Lynnette (2013): Mapping developmental precursors of cyber-aggression: Trajectories of risk predict perpetration and victimization. *Journal of Youth and Adolescence,* Vol. 42, No. 5. 651–661.
Mohler, Peter Ph. – Wohn, Kathrin (2005): Persönliche Wertorientierungen im European Social Survey. *ZUMA-Arbeitsbericht,* No. 1. 1–19.
Morgan, Lewis H. (1961): *Az ősi társadalom.* Budapest, Gondolat.
Moscovici, Serge – Faucheux, Claude (1972): Social Influence, Conformity Bias and the Study of Active Minorities. *Advances in experimental social psychology,* Vol. 6, 149–202.
Nagy Zoltán András (2009): *Bűncselekmények számítógépes környezetben.* Budapest, Ad Librum.
Nemeth, Charlan – Swedlung, Mark – Kanki Barbara (1980): A kisebbségi válaszok mintái és befolyásuk a többségre. In Pataki Ferenc szerk.: *Csoportlélektan.* Budapest, Gondolat. 223–235.
Negroponte, Nicholas (2002): *Digitális létezés.* Budapest, Typotex.
Nietzsche, Friedrich (1992): A nem-morálisan fölfogott igazságról és hazugságról. *Athenaeum,* 1. évf. 3. sz. 3–15.
Nyíri Kristóf (2007): Idő és kommunikáció. *Világosság,* 51. évf. 4. sz. 33–40.
Olweus, Dan (1993): *Bullying at School. What We Know and We Can Do.* Oxford, Wiley-Blackwell.
Olweus, Dan (1999): Az iskolai zaklatás. *Educatio,* 8. évf. 4. sz. 717–739.
Ozsváth Károly szerk. (2011): *Pszichiátriai lexikon.* Budapest, Oriold és Társai.
Parti Katalin – Kiss Tibor (2016): Informatikai bűnözés. In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 491–517.
Pease, Ken – Tseloni, Andromachi (2014): *Using Modeling to Predict and Prevent Victimization.* Springer e-Books.
Perrott, Kathryn (2016): 'Fake news' on social media influenced US election voters, experts say. *Australia News,* 14. November. Elérhető: www.abc.net.au/news/2016-11-14/fake-news-would-have-influenced-us-election-experts-say/8024660 (A letöltés dátuma: 2018. 05. 15.)
Petrovszkij, Artur V. (1980): A közösség szociálpszichológiai elméletéről. In Pataki Ferenc szerk.: *Csoportlélektan.* Budapest, Gondolat. 236–249.
Pittaro, Michael L. (2011): Cyber Stalking: Typology, Etiology, and Victims. In Jaishankar, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press. 277–296.
Platón (1984): Prótagorasz. In *Platón összes művei I.* Budapest, Európa. 173–266.
Pléh Csaba – Boross Ottilia (2010): *Pszichológiai lexikon. A pszichológia legfontosabb fogalmai magyar és angol nyelven.* Budapest, Akadémiai.
Podoletz Léna (2016): Környezeti kriminológia. In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 233–251.
Pongó, Tamás (2016): Anomalies in the US cyberbullying jurisprudence. *Masaryk University Journal of Law and Technology,* Vol. 10, No. 2. 148–169.
Polányi Mihály (1994). *Személyes tudás I.* Budapest, Atlantisz.
Poonia, Ajeet S. (2014): Cybercrimes: Challenges and it's classification. *International Journal of Emerging Trends & Technology in Computer Science,* Vol. 3, No. 6. 119–121.

PRAZSÁK Gergő (2014): Generációk és értékrendszerek: a tudás új útjai. *Információs Társadalom,* 14. évf. 2. sz. 6–23.

PRAZSÁK Gergő (2016): *Értékek és határhelyzetek.* Habilitációs értekezés kézirata. Budapest, Eötvös Loránd Tudományegyetem.

RÁCZ József – FOKASZ Nikosz – SZÜGYI Zoltán (2001): *Bevezetés a devianciák szociológiájába. Szabálykövetők és bajkeverők.* Budapest, Új Mandátum.

REITMAN, Janet (2015): *The children of ISIS. Why did three American kids from the suburbs of Chicago try to run away to the Islamic State, and should the Feds treat them as terrorrists?* Elérhető: www.rollingstone.com/culture/features/teenage-jihad-inside-the-world-of-american-kids-seduced-by-isis-20150325 (A letöltés dátuma: 2018. 05. 15.)

ROGERS, Carl (1961): *On Becoming a Person.* Boston, Houghton Mifflin.

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

ROKEACH, Milton (1973): *The Nature of Human Values.* New York, The Free Press.

ROSTA Andrea (2007): *A deviáns viselkedés szociológiája.* Budapest, Loisir.

SAGAN, Carl (1990): *Az éden sárkányai.* Budapest, Európa.

SAPIR, Edward (1961): *Culture, Language and Personality.* Selected Essays. Editor: MANDELBAUM, David G. Berkeley–Los Angeles, University of California Press.

SCHACHTER, Stanley (1981): Deviáció, elutasítás és kommunikáció. In CSEPELI György szerk.: *A kísérleti társadalomlélektan főárama.* Budapest, Gondolat. 288–308.

SCHULZ VON THUN, Friedemann (2012): *A kommunikáció zavarai és feloldásuk.* Budapest, Háttér.

SCHWARTZ, Shalom H. (2003): *A proposal for measuring value orientations across nations* [Chapter 7 in the Questionnaire Development Report of the European Social Survey]. Jerusalem, Hebrew University of Jerusalem.

SETO, Michael C. – EKE, Angela W. (2005): The Criminal Histories and Later Offending of Child Pornography Offenders. *Sexual Abuse: Journal of Research and Treatment,* Vol. 17, No. 2. 201–210.

SHANNON, Claude E. – WEAVER, Warren (1949): *The mathematical theory of communication.* Urbana and Chicago, University of Illionis Press. Elérhető: http://raley.english.ucsb.edu/wp-content/Engl800/Shannon-Weaver.pdf (A letöltés dátuma: 2018. 05. 15.)

SHELLEY, Louise I. (2003): Organized crime, terrorism and cybercrime. In BRYDEN, Alan – FLURI, Philipp eds.: *Security Sector Reform: Institutions, Society and Good Governance.* Baden-Baden, Nomos Verlag. 303–312.

SHERIF, Muzafer (1973): Normaképződés csoport-szituációban. In HUNYADY György szerk.: *Szociálpszichológia.* Budapest, Gondolat. 233–250.

SMITH, Eliot R. – MACKIE, Diane M. – CLAYPOOL, Heather M. (2016): *Szociálpszichológia.* Budapest, ELTE Eötvös.

SNELL, Patricia A. – ENGLANDER, Elizabeth K. (2010): Cyberbullying Victimization and Behaviors Among Girls: Applying Research Findings in the Field. *Journal of Social Sciences,* Vol. 6, No. 4. 510–514.

SULER, John (2004): The Online Disinhibition Effect. *Cyberpsychology and Behavior,* Vol. 7, No. 3. 321–326.

SUTHERLAND, Edwin H. – CRESSEY, Donald R. (1978): *Criminology.* Chicago, J. B. Lippincott.

Symantec Co. (2014): *Internet Security Threat Report.* Vol. 19. Elérhető: www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (A letöltés dátuma: 2018. 05. 15.)

Szabó Judit (2016): Biológiai és pszichológiai bűnözésmagyarázatok. In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 78–109.

Székely, Iván (2012): The right to forget, the right to be forgotten. In Gutwirth, Serge – Leenes, Ronald – De Hert, Paul – Poullet, Yves eds.: *European Data Protection: In Good Health?* Heidelberg, Springer. 347–363.

Szűcs Jenő (1983): *Vázlat Európa három történeti régiójáról.* Budapest, Magvető.

Tari Annamária (2011): *Z generáció.* Budapest, Tericum.

Terestyéni Tamás (2006): *Kommunikációelmélet.* Budapest, Akti–Typotex.

Tolan, Casey (2015): *How the fight against ISIS is being waged over teenagers' social media accounts.* Elérhető: http://fusion.kinja.com/how-the-fight-against-isis-is-being-waged-over-teenager-1793851919 (A letöltés dátuma: 2018. 05. 15.)

Tönnies, Ferdinand (2004): *Közösség és társadalom.* Budapest, Gondolat.

Turkle, Sherry (2005): *The Second Self: Computers and the Human Spirit.* Cambridge, MIT Press.

Valkenburg, Patti M. – Peter, Jochen (2011): Online communication among adolescents: An Integrated Model on its Attraction, Opportunities, and Risks. *Journal of Adolescent Health,* Vol. 48, No. 2. 121–127.

Varga Károly (1969): Magyar egyetemi hallgatók életfelfogása. Nemzetközi összehasonlítás. *Magyar Pszichológiai Szemle,* 26. évf. 3–4. sz. 360–375.

Váriné Szilágyi Ibolya (1987): *Az ember, a világ és az értékek világa.* Budapest, Gondolat.

Verton, Dan (2003): *Black ice: The invisible threat of cyber-terrorism.* Emeryville, McGraw-Hill–Osborne.

Vetró Ágnes (2010): Agresszió a képernyőn, a képernyő agresszivitása. In Hárdi István szerk.: *Az agresszió világa.* Budapest, Medicina. 401–428.

Vigh József – Gönczöl Katalin – Kiss György – Szabó Árpád (1973): *Erőszakos bűncselekmények és elkövetőik.* Budapest, Közgazdasági és Jogi könyvkiadó.

Virág György – Kulcsár Gabriella – Rosta Andrea (2016): Erőszakos bűnözés. In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 553–598.

Wall, David S. (1999): Cybercrimes: New Wine, No Bottles? In Davies, Pamela – Francis, Peter – Jupp, Victor eds.: *Invisible Crimes: Their Victims and Their Regulation.* London, Macmillan. 105–139.

Wang, Ke – Yu, Philip S. – Chakraborty, Sourav (2004): *Bottom-up generalization: A data mining solution to privacy protection.* Data Mining, ICDM '04. Fourth International Conference.

Weimann, Gabriel (2004): *www.terror.net. How Modern Terrorism Uses the Internet.* Special Report 116. Washington: United States Institute of Peace.

Whorf, Benjamin L. (1956): *Language, Thought and Reality. Selected Writings.* ed.: Carroll, John B. New York–London, MIT – J.Wilky – Chapman & Hall.

Wiener, Norbert (1967): *The Human Use of Human Beings.* New York, Avon.

Wittes, Benjamin – Poplin, Cody – Jurecic, Quinta – Spera, Clara (2016): *Sextortion: Cybersecurity, teenagers, and remote sexual assault.* Washington, The Brookings Institution.

Wittgenstein, Ludwig (2004): *Logikai-filozófiai értekezés.* Budapest, Atlantisz.

Wolke, Dieter – Lee, Kirsty – Guy, Alexa (2017): Cyberbullying: a storm in a teacup? *European Child and Adolescent Psychiatry,* Vol. 26, No. 8. 899–908.

World Bank (2016): *World Development Report 2016: Digital Dividends.* Washington. Elérhető: http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf (A letöltés dátuma: 2018. 05. 15.)

YAR, Majid (2006): *Cybercrime and Society.* London, SAGE.

YAR, Majid (2016): Online Crime. In *Oxford Research Encyclopedia of Criminology.* Oxford, Oxford University Press.

YAR, Majid (2005). Computer hacking: Just another case of juvenile delinquency? *Howard Journal of Criminal Justice,* Vol. 44, No. 4. 387–399.

YOUNG, Kimberly (2011): Virtual Sex Offenders. A Clinical Perspective. In JAISHANKAR, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press. 53–64.

Z. KARVALICS László (2015): Mesterséges intelligencia – a diskurzusok újratervezésének kora. *Információs Társadalom,* 15. évf. 4. sz. 7–41.

Ajánlott irodalom

Adam, Alison (2002): Cyberstalking and Internet pornography: Gender and the gaze. *Ethics and Information Technology,* Vol. 4, No. 2. 133–142.

Agnew, Robert (2001): Building on the foundation general strain theory: Specifying the types of strain most likely to lead to crime and deliquency. *Journal of Research in Crime and Delinquency,* Vol. 38, No. 4. 319–361.

Anderson, Benedict (2006): *Elképzelt közösségek.* Budapest, L'Harmattan.

Andorka Rudolf (2006): *Bevezetés a szociológiába.* Budapest, Osiris.

B. Bernát István – Pais Károlyné – Rétfalvi György – Szilágyi Erzsébet – Turi László (2012): *Média, Kultúra, Kommunikáció.* Budapest, Libri.

Bales, Robert F. (1950): *Interaction Process Analysis.* Cambridge, Addison-Wesley.

Ball, Kirstie – Daniel, Elizabeth – Dibb, Sally – Meadows, Maureen (2010): Democracy, surveillance and „knowing what's good for you": the private sector origins of profiling and the birth of „Citizen Relationship Management. In Haggerty, Kevin D. – Samatas, Minas eds.: *Surveillance and Democracy.* New York, Routledge–Glasshouse. 111–126.

Balogh Zsolt György (1998): *Jogi informatika.* Budapest–Pécs, Dialóg Campus.

Bandura, Albert (1965): Influence of models' reinforcement contingencies on the acquisition of imitative responses. *Journal of Personality and Social Psychology,* Vol. 1, No. 6. 589–595.

Bányász Péter (2016): A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle*, 1. sz. 61–81.

Bányász Péter (2016): Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Csengeri János – Krajnc Zoltán szerk.: *Humánvédelem – békeműveleti és vészhelyzet-kezelési eljárások fejlesztése.* Budapest, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar. 643–673.

Beck, Ulrich (2003): *A kockázat-társadalom – Út egy másik modernitásba.* Budapest, Századvég Politikai Iskola Alapítvány.

Becker, Howard S. (1963): *Outsiders in the sociology of deviance.* New York, Free Press.

Bell, David (2001): An Introduction to Cybercultures. London–New York, Routledge.

Benedek, Wolfgang – Bauer, Veronika – Kettemann, Matthias C. eds. (2008): *Internet Governance and the Information Society. Global Perspectives and European Dimensions.* Utrecht, Eleven International Publishing.

Benedek, Wolfgang (2008): Internet governance and human rights. In Benedek, Wolfgang – Bauer, Veronika – Kettemann, Matthias C. eds.: *Internet Governance and the Information Society. Global Perspectives and European Dimensions.* Utrecht, Eleven International Publishing, 31–50.

Benitez, Mary A. (2002): ID card contract awarded. *South China Morning Post,* 27. February. 2.

Bentham, Jeremy (1995): Panopticon or the inspection-house. In Bozovic, Miran ed.: *The Panopticon Writings.* London, Verso. 29–95.

Berger, Peter L. – Luckmann, Thomas (1998): *A valóság társadalmi felépítése.* Budapest, Jószöveg.

BERKOWITZ, Leonard (1989): Frustration-Aggression Hypothesis: Examination and Reformulation. *Psychological Bulletin,* Vol. 106, No. 1. 59–73.

BERMAN, Mark (2016): Mistrial declared in case of South Carolina officer who shot Walter Scott after traffic stop. *Washington Post,* 5. December. Elérhető: www.washingtonpost.com/news/post-nation/wp/2016/12/05/mistrial-declared-in-case-of-south-carolina-officer-who-shot-walter-scott-after-traffic-stop/?tid=a_inl&utm_term=.99625d13b6df (A letöltés dátuma: 2018. 05. 15.)

BIRKS, Daniel – TOWNSLEY, Michael – STEWART, Anna (2012): Generative explanations of crime: Using simulation to test criminological theory. *Criminology,* Vol. 50, No. 1. 221–254.

BLACK, Matt – SMITH, Russell (2003): Electronic monitoring in the criminal justice system. *Trends & Issues in Crime and Criminal Justice,* No. 254. Elérhető: https://aic.gov.au/publications/tandi/tandi254 (A letöltés dátuma: 2018. 05. 15.)

BLAYA, Catherine – FARTOUKH, Michael (2016): Digital Uses, Victimization and Online Aggression: A Comparative Study Between Primary School and Lower Secondary School Students in France. *European Journal on Criminal Policy and Research,* Vol. 22, No. 2. 285–300.

BOSSLER, Adam M. – HOLT, Thomas J. (2010): The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice,* Vol. 38, No. 3. 227–236.

BOSSLER, Adam M. – HOLT, Thomas J. (2014): Further examining officer perceptions and support for online community policing. In MARCUM, Catherine D. – HIGGINS, George E. eds.: *Social Networking as a Criminal Enterprise.* Boca Raton–London–New York, CRC Press. 167–196.

BRENNER, Susan W. (2014): *Cyberthreats and the Decline of the Nation-State.* New York, Routledge.

BRIGHT, Martin (2002): Surgical tags plan for sex offenders. *The Guardian*, 17. November 2002. Elérhető: www.theguardian.com/society/2002/nov/17/childrensservices.crime (A letöltés dátuma: 2018. 05. 15.)

BYRNES, Andrew – CHARLESWORTH, Hilary – MCKINNON, Gabrielle (2005): *Human rights implications of the Anti-Terrorism Bill 2005.* Report prepared at the request of Jon Stanhope, MLA, Chief Minister of the ACT.

CAPURRO, Rafael – HJØRLAND, Birger (2003): The concept of information. *Annual Review of Information Science and Technology,* Vol. 37, No. 1. 343–411.

CASTELLS, Manuel (2010): *The Information Age: Economy, Society and Culture. Vol. 1: The Rise of the Network.* 2nd ed. Oxford, Wiley–Blackwell.

CHERRY, Colin E. (1978): *On Human Communication: A Review, a Survey and a Criticism.* 3rd ed. Cambridge, MIT Press.

CHESTER, Jeff (2012): Cookie wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era. In GUTWIRTH, Serge – LEENES, Ronald – DE HERT, Paul – POULLET, Yves eds.: *European Data Protection: In Good Health?* Heidelberg, Springer. 53–78.

Chinese hacker sentenced to death for embezzlement (2000). *People's Daily Online,* 13 June. Elérhető: http://en.people.cn/english/200006/13/eng20000613_42866.html (A letöltés dátuma: 2018. 05. 15.)

CHOMSKY, Noam (1986): *Knowledge of Language.* New York, Praeger.

CHRISTOU, George (2016): *Cybersecurity in the European Union. Resilience and Adaptability in governance Policy.* London, Palgrave and Macmillan

CITRON, Keats D. (2009): Cyber civil rights. *Boston University Law Review,* Vol. 89, No. 1. 61–125.

COHEN, Lawrence E. – FELSON, Marcus (1979): Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociology Review,* Vol. 44, No. 4. 588–608.

Cooper, Al (1998): Sexuality and the Internet: Surfing into the New Millennium. *CyberPsychology and Behavior,* Vol. 1, No. 2. 187–194.

Cornelius, Kai – Hermann, Dieter eds. (2011): *Virtual Worlds and Criminality.* Heidelberg, Springer.

Cornelius, Kai (2011): Responsibility under criminal law in virtual worlds. In Cornelius, Kai – Hermann, Dieter eds.: *Virtual Worlds and Criminality.* Heidelberg, Springer. 95–120.

Csepeli György (1990): *...és nem is kell hozzá zsidó. Az antiszemitizmus társadalom-lélektana.* Budapest, Kozmosz.

Csepeli György – Örkény Antal (2002): *Gyűlölet és politika.* Budapest, Friedrich Elbert Alapítvány.

Csepeli György – Prazsák Gergő (2009): Új technológiák – kommunikációs rétegződés – társadalmi státusz. *Információs Társadalom,* 9. évf. 2. sz. 80–91.

Csepeli György – Prazsák Gergő (2010): *Örök visszatérés: Társadalom az információs korban.* Budapest, Jószöveg.

CSI/FBI (2003): *Computer Crime and Security Survey.* San Francisco, Computer Security Institute.

Day, Jones (2013): *The cybersecurity debate: voluntary versus mandatory cooperation between the private sector and the federal government. A review of attempts at cybersecurity legislation and the Obama administration's administrative actions.* Elérhető: https://goo.gl/qc5LZA (A letöltés dátuma: 2018. 05. 15.)

Delort, Pierre (2015): *Le Big Data.* PUF, Collection: 'Que sais-je?' Elérhető: www.puf.com/content/Le_Big_Data (A letöltés dátuma: 2018. 05. 15.)

Den Tek, Klaas (2012): *The Netherlands bundles knowledge about cyber crime.* RNW. Elérhető: www.rnw.org/archive/netherlands-bundles-knowledge-about-cyber-crime (A letöltés dátuma: 2018. 05. 15.)

Dowland, Paul S. – Furnell, Steven M. – Illingworth, Helen M. – Reynolds, Paul L. (1999): Computer Crime and Abuse: A Survey of Public Attitudes and Awareness. *Computers & Security,* Vol. 18, No. 6. 715–726.

Durkin, Keith F. – Bryant, Clifton D. (1995): Log on to sex: Notes on the carnal computer and erotic cyberspace as an emerging research frontier. *Deviant Behavior,* Vol. 16, No. 3 179–200.

Eichenwald, Kurt (1998): Reuters subsidiary target of U.S. inquiry into theft data from Bloomberg. *Computers and Security,* Vol. 17, No. 2. 157.

Electronic Frontier Foundation (EFF) (2011a): *Mandatory Data Retention – European Union.* Elérhető: www.eff.org/issues/mandatory-data-retention/eu (A letöltés dátuma: 2018. 05. 15.)

Electronic Frontier Foundation (EFF) (2011b): *Mandatory Data Retention.* Elérhető: www.eff.org/issues/mandatory-data-retention (A letöltés dátuma: 2018. 05. 15.)

Erikson, Kai Th. (1966): *Wayward Puritans: A Study in the Sociology of Deviance.* New York, John Wiley & Sons.

Farrell, Maria (2016): Quietly, symbolically, US control of the internet was just ended. *The Guardian,* 14. March 2016. Elérhető: www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana?CMP=share_btn_tw (A letöltés dátuma: 2018. 05. 15.)

Foucault, Michael (1990): *Felügyelet és büntetés: A börtön története.* Budapest, Gondolat.

Fuchs, Christian (2008): *Internet and Society. Social Theory in the Information Age.* [Routledge Research in Information Technology and Society Series, No. 8.] New York, Routledge.

Garland, David (2001): *The Culture of Control.* Oxford, Oxford University Press.

Garrido, Miguelángel V. (2015): Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden. *Surveillance & Society,* Vol. 13, No. 2. 153–167.

GEHLEN, Arnold (1976): *Az ember természete és helye a világban.* Budapest, Gondolat.

GELLNER, Ernest (1983): *Nations and Nationalism.* Oxford, Blackwell.

Germany approves electronic ankle bracelets to monitor extremists (2017). Die Welt, 1 February 2017. Elérhető: www.dw.com/en/germany-approves-electronic-ankle-bracelets-to-monitor-extremists/a-37365188 (A letöltés dátuma: 2018. 05. 15.)

GITTINGS, John (1998): China sentences bank computer hackers to death. *The Guardian,* 30. December. Elérhető: www.theguardian.com/world/1998/dec/30/johngittings1 (A letöltés dátuma: 2018. 05. 15.)

GOLDSMITH, Jack – WU, Tim (2006): *Who Controls the Internet? Illusions of a Borderless World.* Oxford, Oxford University Press.

GOLDSTEIN, Sara E. (2015): Adolescents' Disclosure and Secrecy About Peer Behavior: Links with Cyber Aggression, Relational Aggression, and Overt Aggression. *Journal of Child and Family Studies,* Vol. 25, No. 5. 1430–1440.

Google: Who would want the right to be forgotten? (2014). *BBC News Magazine,* 14 May. Elérhető: www.bbc.com/news/magazine-27396981 (A letöltés dátuma: 2018. 05. 15.)

GOSSETT, Jennifer L. – BYRNE, Sarah (2002): "Click Here". A Content Analysis of Internet Rape Sites. *Gender and Society,* Vol. 16, No. 5. 689–709.

GOTTFREDSON, Michael R. – HIRSCHI, Travis (1990): *A General Theory of Crime.* Stanford, Stanford University Press.

GREENWALD, Glenn – MACASKILL, Even – POITRAS, Laura (2013): Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian,* 11. June. Elérhető: www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (A letöltés dátuma: 2018. 05. 15.)

GREENWALD, Glenn (2015): NSA claims Iran learned from Western cyberattacks. *The Intercept,* February 10. Elérhető: https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/ (A letöltés dátuma: 2018. 05. 15.)

GROVE, Louise – FARRELL, Graham (2011): *Repeat victimization.* Oxford Bibliographies, 29. June. Elérhető: www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0119.xml (A letöltés dátuma: 2018. 05. 15.)

HAGGERTY, Kevin D. – SAMATAS, Minas (2010): Introduction: surveillance and democracy: an unsettled relationship. In HAGGERTY, Kevin D. – SAMATAS, Minas eds.: *Surveillance and Democracy.* New York, Routledge–Glasshouse. 1–16.

HAGGERTY, Kevin D. – SAMATAS, Minas eds. (2010): *Surveillance and Democracy.* New York, Routledge–Glasshouse.

HALDER, Debarati – JAISHANKAR, Karuppannan (2008): Cyber crimes against women in India: Problems, perspectives and solutions. *TMS Academic Journal,* Vol. 3, No. 1. 48–62.

HARTMANN, Tilo (2011): Is virtual violence a morally problematic behaviour? In CORNELIUS, Kai – HERMANN, Dieter eds.: *Virtual Worlds and Criminality.* Heidelberg, Springer. 31–44.

HILTON, Nick (2016): How social media won the day for the Donald. *The Spectator,* 19. November. Elérhető: https://blogs.spectator.co.uk/2016/11/social-media-won-day-donald/# (A letöltés dátuma: 2018. 05. 15.)

HINDELANG, Michael J. – GOTTFREDSON, Michael R. – GAROFALO, James (1978): *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization.* Cambridge, Ballinger.

HOLT, Thomas J. – BOSSLER, Adam M. – FITZGERALD, Sarah (2013): Examining state and local law enforcement perceptions of computer crime. In HOLT, Thomas J. ed.: *Crime On-line. Correlates,*

Causes, and Context. 2nd ed. Durham, Carolina Academic Press. 219–244.

Holt, Thomas J. (2013). Crime on-line: Correlates, causes, and context. In Holt, Thomas J. ed.: *Crime On-line. Correlates, Causes, and Context.* 2nd ed. Durham, Carolina Academic Press. 3–26.

Horkheimer, Max (1976): Hagyományos és kritikai elmélet. In Papp Zsolt szerk.: *Tény, érték, ideológia. A pozitivizmus-vita a német szociológiában.* Budapest, Gondolat. 43–116.

Huang, Sandra (2012): How China's Mainstream Media Ignored the Anti-Japanese Riots. *The Atlantic International,* 26. September. Elérhető: www.theatlantic.com/international/archive/2012/09/how-chinas-mainstream-media-ignored-the-anti-japanese-riots/262879/ (A letöltés dátuma: 2018. 05. 15.)

Hwang, Jae Yeon – Choi, Jung-Seok – Gwak, Ah Reum – Jung, Dawn – Choi, Sam-Wook – Lee, Jaewon – Lee, Jun-Young – Jung, Hee Yeon – Kim, Dai Jin (2014): Shared psychological characteristics that are linked to aggression between patients with Internet addiction and those with alcohol dependence. *Annals of General Psychiatry,* Vol. 13.

The International Massmedia Agency (IMMA) (2017): Why Russian suicide game spread around the world. *The International Mass Media Agency,* 27. April. Elérhető: https://intmassmedia.com/2017/04/27/why-russian-suicide-game-spread-around-the-world/ (A letöltés dátuma: 2018. 05. 15.)

Information Technology Industry Council (ITIC) (2013): *ITI Position Paper on the Proposed "Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union", June 24, 2013.* Elérhető: www.itic.org/dotAsset/a748f2f7-7d73-4d62-8ea0-b5ad35e3af27.pdf (A letöltés dátuma: 2018. 05. 15.)

Inglehart, Ronald – Norris, Pippa (2012): *Sacred and Secular. Religion and Politics Worldwide.* Cambridge, Cambridge University Press.

Jaishankar, Karuppannan (2011): *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press.

Jakobson, Roman (1969): *Hang, jel, vers.* Budapest, Gondolat.

Jehnsen, Robert (2007): The digital provide: Information (technology), market performance, and welfare in the South Indian fisheries sector. *Quarterly Journal of Economics,* Vol. 122, No. 3. 879–924.

Johnson, Shane D. – Birks, Daniel J. – McLaughlin, Lindsay – Bowers, Kate J. – Pease, Ken (2007): *Prospective crime mapping in operational context.* Online Report 19/07. London, Home Office.

Johnson, Shane D. – Bowers, Kate J. (2004): The stability of space-time clusters of burglary. *British Journal of Criminology,* Vol. 44, No. 1. 55–65.

Jordan, Tim – Taylor, Paul A. (2004): *Hacktivism and Cyberwars.* London–New York, Routledge.

Klimmt, Christoph (2011): Virtual worlds as a regulatory challenge: A user perspective. In Cornelius, Kai – Hermann, Dieter eds.: *Virtual Worlds and Criminality.* Heidelberg, Springer. 1–18.

Kroeber, Alfred L. – Kluckhohn, Clyde – Untereiner, Wayne (1952): *Culture: A Critical Review of Concepts and Definitions.* New York, Vintage.

Krug, Etienne G. – Dahlberg, Linda L. – Mercy, James A. – Zwi, Anthony B. – Lozan, Rafael (2002): *World report on violence and health.* Geneva, World Health Organization. 1–254.

Kuschewsky, Monika (2014): Germany. New cybersecurity law draft proposed by interior ministry. In Bloomberg BNA: *World Data Protection Report,* Vol. 14, No. 9, September 2014. Elérhető: https://goo.gl/j6nGQU (A letöltés dátuma: 2018. 05. 15.)

LEDERMANN, Eli (2016): *Infocrime. Protecting Information Through Criminal Law.* Northampton, Edward Elgar Publishing.

LEUKFELDT, Rutger E. – LAVORGNA, Anita – KLEEMANS, Edward R. (2017): Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal of Criminal Policy and Research,* Vol. 23, No. 3. 287–300.

LEUKFELDT, Rutger E. – YAR, Majid (2016): Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behaviour,* Vol. 37, No. 3. 263–280.

LORENZ, Konrad (2013): *Agresszió.* Budapest, Helikon.

LYON, David (2010): Identification, surveillance and democracy. In HAGGERTY, Kevin D. – SAMATAS, Minas eds.: *Surveillance and Democracy.* New York, Routledge–Glasshouse. 34–50.

LYON, David (2015): *Surveillance After Snowden.* Malden, Polity Press.

LYON, David (2015): The Snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society,* Vol. 13, No. 2. 139–152.

MACHILL, Marchel – WALTERMANN, Jensen (1999): *Self-Regulation of Internet Content.* Gütersloh, Bertelsmann Foundation.

MACHLUP, Fritz (1983): Semantic quirks in studies of information. In MACHLUP, Fritz – MANSFIELD, Una eds.: *The Study of Information.* New York, Wiley. 641–660.

MANN, Jason (2015): *The Internet of Things: Opportunities and Applications across Industries.* SAS White Paper. Portland, International Institute for Analytics.

MANN, Steve – NOLAN, Jason – WELLMANN, Barry (2003): Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society,* Vol. 3, No. 1. 331–355.

MARKOFF, John (2000): *Rebel Outpost on the Fringes of Cyberspace.* The New York Times, 4. June. Elérhető: www.nytimes.com/2000/06/04/world/rebel-outpost-on-the-fringes-of-cyberspace.html?mcubz=2 (A letöltés 2018. 05. 15.)

MARX, Karl (1955): *A tőke. A politikai gazdaságtan bírálata.* Budapest, Szikra.

MAYO, Elton (1946): *The human problems of an industrial civilization.* 2nd Edition. Boston, Harvard University.

MCAULIFFE, Wendy (2002): Asylum seekers get first UK biometric ID cards, ZDNet Australia. ZDNet, 5. February. Elérhető: www.zdnet.com/article/asylum-seekers-get-uks-first-biometric-id-cards/ (A letöltés dátuma: 2018. 05.15.)

MCGRATH, Michael G. – CASEY, Eoghan (2002): Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. *Journal of the American Academy of Psychiatry and the Law,* Vol. 30, No. 1. 81–94.

MCLAUGHLIN, Lindsay – JOHNSON, Shane D. – BOWERS, Kate J. – BIRKS, Daniel – PEASE, Ken (2006): Police perceptions of the long- and short-term spatial distribution of residential burglary. *International Journal of Police Science & Management,* Vol. 9. 99–111.

MCLUHAN, Marshall (2012): *Médiamasszázs. Egy rakás hatás.* Budapest, Typotex.

MIFSUD BONNICI, Jeanne P. (2008): *Self-regulation in Cyberspace.* Information Security and Law Series Vol. 1. The Hague: TMC Asser Press.

MITCHELL, Kimberly J. – FINKELHOR, David – WOLAK, Janis (2003). The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact, and Prevention. *Youth & Society,* Vol. 34, No. 3. 330–358.

MITNICK, Kevin D. – SIMON, William L. (2012): *A legkeresettebb hacker.* Budapest, HVG.

Mitrou, Lilian (2010): The impact of communications data retention on fundamental rights and democracy – the case of the EU Data retention Directive. In Haggerty, Kevin D. – Samatas, Minas eds.: *Surveillance and Democracy.* New York, Routledge–Glasshouse. 127–147.

Mohler, George O. – Short, Martin B. – Brantingham, Jeffrey P. – Schoenberg, Frederic P. – Tita, George E. (2011): Self-exciting point process modeling of crime. *Journal of the American Statistical Association,* Vol. 106, No. 493. 100–108.

Moore, Henry T. (1981): A többségi és a szakértői vélemény befolyásának összehasonlító vizsgálata. In Csepeli György szerk.: *A kísérleti társadalomlélektan fő árama.* Budapest, Gondolat. 66–70.

Némedi Dénes (2005): *Klasszikus szociológia.* Budapest, Napvilág.

Nietzsche, Friedrich (2000): *Túl jón és rosszon.* Budapest, Műszaki Könyvkiadó.

Orue, Izaskun – Andershed, Henrik (2015): The Youth Psychopathic Traits Inventory-Short Version in Spanish Adolescents – Factor Structure, Reliability, and Relation with Aggression, Bullying, and Cyber Bullying. *Journal of Psychopathology Behavioral Assessment,* Vol. 37, No. 4. 563–575.

Pagallo, Ugo (2012): On the principle of privacy by design, and its limits: Technology, ethics and the rule of law. In Gutwirth, Serge – Leenes, Ronald – De Hert, Paul – Poullet, Yves eds.: *European Data Protection: In Good Health?* Heidelberg, Springer. 331–346.

Parliament of Australia (2010): *Hackers, fraudsters and botnets: tackling the problem of cyber crime, the report of inquiry into cyber crime.* Canberra, National Library of Australia. Elérhető: http://trove.nla.gov.au/work/37494558 (A letöltés dátuma: 2018. 05. 15.)

Parsons, Talcot (1967): *Sociological Theory and Modern Society.* New York, Free Press.

Parti Katalin – Schmidt Andrea – Néray Bálint – Virág György (2014): Cyberbullying – Az online zaklatás volumenének iskolai felmérése és mentorképzés Magyarországon. *Ügyészek Lapja,* 21. évf. 3–4. sz. 47–58.

Parti Katalin (2009): *Gyermekpornográfia az interneten.* Miskolc, Bíbor Kiadó.

Pew Research Center (2017): *Social Media Fact Sheet.* Pew Research Center, Internet & Technology. Elérhető: www.pewinternet.org/fact-sheet/social-media/ (A letöltés dátuma: 2018. 05. 15.)

Prazsák Gergő (2017): *Értékek és határhelyzetek.* Habilitációs értekezés, ELTE TáTK.

Procter, Rob – Crump, Jeremy – Karstedt, Susanne – Voss, Alex – Cantijoch, Marta (2013): Reading the riots: What were the police doing on Twitter? *Policing and Society,* Vol. 23, No. 4. 413–436.

Proudman, Charlotte R. (2014): Revenge porn: Why isn't enough being done to stop it? July 3. *The Independent,* 3 July. Elérhető: www.independent.ie/life/revenge-porn-why-isnt-enough-being-done-to-stop-it-30404049.html (A letöltés dátuma: 2018. 05. 15.)

Przybylski, Andrew K. – Murayama, Kou – DeHaan, Cody R. – Gladwell, Valerie (2013): Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior,* Vol. 29, No. 4. 1841–1848.

Rátai, Balázs – Homoki, Péter – Polyák, Gábor (2010): *Cyber Law in Hungary.* The Netherlands, Kluwer Law International BV.

Richards, Neil M. – King, Jonathan H. (2013): Three paradoxes of big data. *Stanford Law Review Online,* Vol. 66, No. 41.

Robinson, Neil – Horvath, Veronika – Cave, Jonathan – Roosendaal, Arnold P. – Klaver, Marieke (2013): *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts.* European Parliament, Policy Department A: Economic and Scientific Policy. Elérhető: www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf (A letöltés dátuma: 2018. 05. 15.)

ROSENBERG, Richard S. (2001): Controlling access to the Internet: The role of filtering. *Ethics and Information Technology,* Vol. 3, No. 1. 35–54.

ROUVROY, Antoinette (2016): *"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data.* Strasbourg, Council of Europe.

RUNIONS, Kevin C. (2013): Toward a Conceptual Model of Motive and Self-Control in Cyber-Aggression: Rage, Revenge, Reward, and Recreation. *Journal of Youth and Adolescence,* Vol. 42, No. 5. 751–771.

RUSSINOVICH, Mark (2015): *Tolvaj kód.* Budapest, Szak.

SCHWARTZ, Shalom H. (1992): Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. *Advances in Experimental Social Psychology,* Vol. 25. 1–65.

SEIGFRIED-SPELLAR, Kathryn C. – LOVELY, Richard W. – ROGER, Markus K. (2011): Self-Reported Internet Child Pornography Consumers. In JAISHANKAR, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* Boca Raton, CRC Press. 65–77.

SHARMA, Amit (2010): Cyber wars: A paradigm shift from means to ends. *Strategic Analysis,* Vol. 34, No. 1. 62–73.

SHIM, Jae W. – LEE, Seungwhan – PAUL, Bryant (2007): Who responds to unsolicited sexually explicit materials on the Internet? The role of individual differences. *CyberPsychology and Behavior,* Vol. 10, No. 1. 71–79.

SHORT, Martin B. – D'ORSOGNA, Maria R. – PASOUR, Virginia B. – TITA, George E. – BRANTINGHAM, Jeffrey P. – BERTOZZI, Andrea L. – CHAYES, Lincoln B. (2008): A statistical model of criminal behaviour. *Mathematical Models and Methods in Applied Sciences,* Vol. 18, No. 1. 1249–1267.

SIEBER, Ulrich (2012): *Straftaten und Strafverfolgung im Internet – Gutachten C zum 69. Deutschen Juristentag.* München, C.H. Beck.

SIMMEL, Georg (1973): A nagyváros és a szellemi élet. In BEREND T. Iván – HUSZÁR Tibor – KULCSÁR Kálmán szerk.: *Válogatott társadalomelméleti tanulmányok.* Ford.: BERÉNYI Gábor. Budapest, Gondolat. 543–560.

SMITH, Russel G. (2011): Human Rights Infringement in the Digital Age. In JAISHANKAR, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior.* New York, CRC Press. 393–410.

SOLLITTO, Marlo (2016): *Your Parent Could Be a Victim of Identity Theft and Not Know It.* Elérhető: www.agingcare.com/articles/elderly-identity-theft-victims-frauds-scams-cons-139206.htm (A letöltés dátuma: 2018. 05. 15.)

SONTA, Lisa M. – CLEMANS, Katherine H. – GRABER, Julia A. – LYNDON, Sarah T. (2011): Traditional and Cyber Aggressors and Victims: A Comparison of Psychosocial Characteristics. *Journal of Youth and Adolescence,* Vol. 40, No. 4. 392–404.

SOUTER, David (2017): 'Inside the information society: What's happened to the price of fish?' *Association for Progressive Communication* [APC], 8 May. Elérhető: www.apc.org/en/blog/inside-information-society-whats-happened-price-fi (A letöltés dátuma: 2018. 05. 15.)

Suqian's "Internet Propaganda Team" (2005): The practical aspects of directing Internet opinion. *Nanfang Weekend,* 22 May

TAJFEL, Henri – WILKES, Aisha L. (1963): Classification and Quantitative Judgement. *British Journal of Psychology,* Vol. 54, No. 2. 101–114.

Társaság a Szabadságjogokért (TASZ) (2015): *Call for Amicus Briefs in Case Against Hungary's Data Retention Law.* Elérhető: https://tasz.hu/en/data-protection/call-amicus-briefs-case-against-hungarys-data-retention-law

Taylor, Frederick W. (1911): *The Principles of Scientific Management.* New York–London, Harper & Brothers.

Taylor, Greg (2001): The Council of Europe's Convention on Cybercrime in Australia: A civil liberties perspective. *Cyber Law Resources,* 30. Elérhető: www.austlii.edu.au/au/other/CyberLRes/2001/30/ (A letöltés dátuma: 2018. 05. 15.)

Taylor, Paul (2001): Hacktivism: in search of lost ethics? In Wall David S. ed.: *Crime and the Internet.* London–New York, Routledge. 59–73.

Than Alexandra (2017): *Elektronikus mozgáskövető eszköz alkalmazása a büntető igazságszolgáltatás során Magyarországon és Európában.* PhD értekezés. Pécs, Pécsi Tudományegyetem ÁJK. Elérhető: http://ajk.pte.hu/files/file/doktori-iskola/than-alexandra/than-alexandra-muhelyvita-ertekezes.pdf (A letöltés dátuma: 2018. 05. 15.)

The New York Times (2015): Video Shows Fatal Police Shooting. Race in America. *The New York Times,* 7 April. Elérhető: www.nytimes.com/video/us/100000003615939/video-shows-fatal-police-shooting.html (A letöltés dátuma: 2018. 05. 15.)

Townsley, Michael – Homel, Ross – Chaseling, Janet (2000): Repeat burglary victimisation: Spatial and temporal patterns. *Australian and New Zealand Journal of Criminology,* Vol. 33, No. 1. 37–63.

Townsley, Michael – Homel, Ross – Chaseling, Janet (2003): Infectious burglaries: A test of the near repeat hypothesis. *British Journal of Criminology,* Vol. 43, No. 3. 615–633.

Townsley, Michael – Johnson, Shane D. – Ratcliffe, Jerry H. (2008): Space-time dynamics of insurgent activity in Iraq. *Security Journal,* Vol. 21, No. 3. 139–146.

Tropina, Tatiana – Callanan, Cormac (2015): *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security.* Heidelberg, SpringerBriefs in Cybersecurity.

Turgeman-Goldschmidt, Orly (2011): Identity construction among hackers. In Jaishankar, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, CRC Press. 31–52.

Turgeman-Goldschmidt, Orly (2017): Police detained administrators of "blue whale" suicide groups in social networks. *112 UA International News,* 25 February. Elérhető: http://112.international/ukraine-top-news/police-detained-administrators-of-blue-whale-suicide-groups-in-social-networks-14489.html (A letöltés dátuma: 2018. 05. 15.)

Van Laer, Jeroen – Van Aelst, Peter (2010): Cyber-protest and civil society: the Internet and action. In Jewkes, Yvonne – Yar, Majid eds.: *Handbook of Internet Crime.* Portland, Willan Publishing. 230–254.

Varga Árpád (2014): *Számítástechnikai bűnözés és elkövetők – A bűnelkövetés okainak és jellemzőinek vizsgálata.* OTDK dolgozat, kézirat. Budapest, ELTE ÁJK.

Vladeck, Stephen I. (2014): Big Data Before and After Snowden. *Journal of National Security Law & Policy,* Vol. 7, No. 2. 333–341.

Wall, David S. – Williams, Michael L. (2014): Introduction. In Wall, David S. – Williams, Michael L. eds.: *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing.* London, Routledge. 1–4.

Wall, David S. (2008): Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology,* Vol. 22, No. 1–2. 45–63.

Wall, David S. (2010): *Policing cybercrimes: Responding to the transnational challenges of cybercrime.* Hanover, Dartmouth College, Institute for Security, Technology and Society.

WALL, David S. (2011): Foreword. In JAISHANKAR, Karuppannan ed.: *Cyber Criminology. Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, CRC Press. xi

WEBER, Max (1987): *Gazdaság és társadalom.* Budapest, KJK.

WEBER, Rolf H. (2015): *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles.* Berlin, Springer.

WENDEL, Bradley W. (2004): The banality of evil and the First Amendment. *Michigan Law Review,* Vol. 102, No. 6. 1404–1422.

WERNER, Nicole E. – BUMPUS, Matthew F. – ROCK, Daquarii (2010): Involvement in Internet Aggression During Early Adolescence. *Journal of Youth and Adolescence,* Vol. 39, No. 6. 607–619.

WHITE, Ralph K. – LIPPITT, Ronald (1969): A vezető viselkedése és a tagság reakciója háromféle „társadalmi klímában". In PATAKI Ferenc szerk.: *Csoportlélektan.* Budapest, Gondolat. 315–345.

WHITSON, Jennifer R. (2010): Surveillance and Democracy in the Digital Enclosure. In HAGGERTY, Kevin D. – SAMATAS, Minas eds.: *Surveillance and Democracy.* New York, Routledge–Glasshouse. 231–246.

WIKSTRÖM, Per Olof (2006): Individuals, settings, and acts of crime: Situational mechanisms and the explanation of crime. In WIKSTRÖM, Per Olof – SAMPSON, Robert J. eds.: *The Explanation of Crime.* Cambridge: Cambridge University Press.

WILLIAMS, Kipling D. – FORGAS, Joseph P. – VON HIPPEL, William (2006): *A társas kirekesztés pszichológiája.* Budapest, Kairosz.

WILLIAMS, Michael L. – EDWARDS, Adam – HOUSLEY, William – BURNAP, Peter – RANA, Omer – AVIS, Nick – MORGAN, Jeffrey – SLOAN, Luke (2014): Policing cyber-neighbourhoods: Tension monitoring and social media networks. In WALL, David S. – WILLIAMS, Michael L. eds.: *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing.* London, Routledge. 53–73.

WILLIAMS, Michael L. (2001): The language of cybercrime. In WALL, David S. ed.: Crime and the Internet. London–New York, Routledge. 152–166.

WILLIAMS, Michael L. (2010): The virtual neighbourhood watch: Netizens in action. In JEWKES, Yvonne – YAR, Majid eds.: *Handbook of Internet Crime.* Portland, Willan Publishing. 562–581.

WINSBERG, Eric (2006): Models of success versus the success of models: Reliability without truth. *Synthese,* Vol. 152, No. 1. 1–19.

WOODS, Lorna (2016): Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber). *EU Law Analysis Blogspot,* 21. December. Elérhető: http://eulawanalysis.blogspot.de/2016/12/data-retention-and-national-law-ecj.html (A letöltés dátuma: 2018. 05. 15.)

XIANGWEI, Wang (2005): *Escalating outcry poses threat to Japanese trade, investments.* Elérhető: www.scmp.com/article/495334/escalating-outcry-poses-threat-japanese-trade-investments (A letöltés dátuma: 2018. 05. 15.)

YAKINTHOU, Christalla – CROESER, Sky (2016): Transforming Tunisia: Transitional justice and Internet governance in a post-revolutionary society. *International Journal of Transitional Justice,* Vol. 10, No. 2. 230–249.

Z. KARVALICS László (2004): *Bevezetés az információtörténelembe.* Budapest, Gondolat–Infónia.

Z. KARVALICS László (2007): Az információs társadalom – mi az? Egy kifejezés jelentéstörténete és fogalomkörnyezete. In PINTÉR Róbert szerk.: *Az információs társadalom. Az elmélettől a politikai gyakorlatig.* Budapest, Gondolat–Új mandátum. 29–46.

ZUBRECZKY György (1969): Berzsenyi Dániel: A közelítő tél. *Irodalomtörténeti Közlemények,* 73. évf. 2–3. sz. 290–295.

Név- és tárgymutató

F

G

H

I

J

K

N

O

P

A Dialóg Campus Kiadó a Nemzeti Közszolgálati Egyetem könyvkiadója.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó
www.dialogcampus.hu
www.uni-nke.hu
1083 Budapest, Ludovika tér 2.
Telefon: 06 (30) 426 61 16
E-mail: kiado@uni-nke.hu

A kiadásért felel: Petró Ildikó ügyvezető
Felelős szerkesztő: Dalloul Zaynab
Olvasószerkesztő: Szarvas Melinda
Korrektor: Bíró Csilla
Tördelőszerkesztő: Gyapjas Anikó
Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Simon László vezérigazgató

ISBN 978-615-5945-34-2 (nyomtatott)
ISBN 978-615-5945-35-9 (elektronikus)

Ha Sherlock Holmes ma élne, barátjával és segítőtársával, Watsonnal biztosan elolvastatná ezt a könyvet. A kötetben foglaltak ismerete nélkül nem lehet felvenni a siker reményében a harcot a bűnnel, amelynek elkövetői és áldozatai ma már a virtuális valóságban is jelen vannak. A szerzők meggyőzően mutatják be, hogy ugyanazok az emberek, akik a valóságos térben követik el a jogi és az erkölcsi normákat áthágó tetteiket, a cybertérben már merőben más bűnelkövetési eszközökkel, kockázatokkal és lehetőségekkel találkoznak. Ezt a művet érdemes tanulmányoznia annak, akit érdekel a szemünk előtt kibontakozó virtuális tér kriminológiája és patológiája, amelyeknek a feltérképezése jelentősen hozzájárulhat a cyberdeviancia által okozott károk mérsékléséhez és megelőzéséhez.

A kiadvány a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó közszolgálat-fejlesztés”
című projekt keretében jelent meg.

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE