

2. Kiberdeviancia

Kiss Tibor

2.1. A normák változása a kibertérben

A norma alapja az érték, ami elsősorban valaminek azt a tulajdonságát jelöli, ami az egyén és a társadalom többsége számára kiemelkedő fontosságú. Az értékek nem függetlenek az adott társadalom kultúrájától, ugyanakkor közmegegyezésen alapuló, közös tudás eredményeként megjelenő, elvont manifesztációkként jellemezhetők. Az értékek kulturális alapelvekként kifejezik, hogy egy társadalomban mit tartanak jónak, rossznak, kívánatosnak vagy elítélendőnek mindamellett, hogy számos formában és módon válnak láthatóvá. Lehetnek elvek, eszmék, attitűdöket tükröző érzelmek, ideálok, trendek alapjai, állhatnak különböző magatartásminták, együttélési formák fókuszában, kifejeződhetnek kézzel fogható tárgyakban (FEHÉR–LAPPINTS 1999, 29.; ANDORKA 2006, 569.). Az értékek akkor válnak társadalmivá, amikor a túlnyomó többség érdekéhez vagy szükségletéhez kötődve is értékként jelennek meg. Az ilyen módon közösségé váló értékek felminősítése idővel a társadalom minden tagja részéről kötelezővé válik, vagyis normává emelkedik (ROSTA 2007, 22.). A normák a társadalom többsége által jelentős értékekből eredeztethető magatartási szabályok, amelyek követése és betartása a társadalom minden tagja részéről kötelező, megszegésük formális vagy informális szankcióval jár. A normák összességéként kialakuló normarendszer kiépítése a társadalom stabil működésének alapvető feltétele, az együttélés biztosítója, a közösség integritásának garanciája. Kijelöli a társadalom tagja számára a normális működési határokat, előírja azokat a cselekvésmódokat, amelyekhez az egyén viselkedési mintáit igazítani tudja, és a társadalom normakövető és normatartó tagjaként élhet. A legtöbb társadalomban a normák különböző szinteken pozicionáltak attól függően, hogy mennyire fontos és meghatározó értékeken alapulnak. Ebből az okból a normaképződést tárgyaló szociológiai irodalmakban a magatartási szabályokat jogi normák, erkölcsi normák és szokásnormák mentén tagolják. Míg a jogi normák megsértése jogszabályokban deklarált szankciókkal jár (például a bűncselekmények szankciói), az erkölcsi normák és a szokásnormák társadalmi rosszállást, informális elítélést, kiközösítést eredményezhetnek (például az illemszabályok megsértése). A szociálpszichológia képviselői a társas normák cselekvésmeghatározó erejének magyarázatában a leíró és az előíró normák funkcióját különösképp kihangsúlyozzák. A leíró társas normák a közösség tagjainak cselekvés-, érzés- és gondolkodásmódját prezentálják, vagyis azt, hogy a csoport tagjai valójában milyen értékek mentén működnek. Az előíró normák összessége pedig azt fejezi ki, hogy egy közösség tagjainak hogy kell gondolkodnia, éreznie és cselekednie, milyen normákat kell képviselnie. Mindkét társas norma közmegegyezésen alapul, gyakran a leíró normák előíró, társas normákká alakulnak át, vagyis amit a közösség többsége



tesz, azt később mindenkitől elvárt magatartásmintaként kell képviselnie. Akkor, amikor az egyén érzés-, cselekvés- és gondolkodásmódját csoportnormákhoz igazítja, valójában a leíró és előíró normák betartására törekszik, így a társadalom konform tagjaként viselkedik (SMITH–MACKIE–CLAYPOOL 2016, 497–498.). A kibertér és az annak esszenciális részét képező internetes hálózat számos emberi cselekvésforma megjelenésének terepe, ezért sokan úgy vélik, hogy az ember a kibertérben is a szocializációja során internalizált és interiorizált értékek és normák betartásával működik. Ezt a nézőpontot Peter N. Grabosky az *old wine in new bottles* kifejezéssel írta körül, amivel arra utalt, hogy a virtuális környezetben leképeződő, szokványostól eltérő magatartásmintázatok valójában hagyományos normasértések, csupán a környezet más. Szerinte az emberi motivációt az anonimitásra épülő interperszonális kapcsolatokat, a titkos működést, az ellenőrzésben felmerülő új kihívásokat, a földrajzi határok elmosódásával járó kiterjedt bűnözést sem lehet újnak tekinteni (GRABOSKY 2001, 243–249.). Grabosky gondolatmenete valójában a normasértésekre irányult, de a normákra éppúgy vonatkoztatható, vagyis a kibertérben megvalósított normasértés nem több, mint a hagyományos normahatárok átlépése. Ezzel szemben célszerű szem előtt tartani azokat a jelenségeket, amelyek a hagyományosan felfogott normákhoz és normasértésekhez képest eddig nem megszokott szerkezetben jelentek meg a kibertérben, ugyanakkor kezelésükre eszközbéli séma nem áll rendelkezésre (például a *cyberbullying*). A megváltozott magatartásformák mögött ma már olyan új tényezők állnak, amelyek könnyen láthatók, és a kibertér sajátosságaiban gyökereznek. Ezek a tényezők nem feltétlenül és közvetlenül vezetnek normasértő magatartásokhoz, de közvetett módon kapcsolódnak azokhoz:

- *Új javak.* Az informatikai rendszerek és a rendszereken belül tárolt adatok új értéket jelentenek, 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 ezzel együtt 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 (YAR 2006, 11.). Az ilyen normák megsértésének következményeivel szemben megszilárdulni látszik egyfajta immunitás, amely először az egyén, majd a közösség attitűdjeiben jelenik meg, ami később általánossá válhat.
- *Anonimitás.* A virtuális tér lehetővé tette anonim akciók felszabadítják az egyént belső és külső kontrolljaitól. Míg a valós életben a személyes identitás felvállalása visszatart a szabályszegéstől, és támogatja a konform viselkedést, addig a kibertérben a hagyományos normák különböző szintjei a rugalmas erkölcs (*flexible morality* – MICHELET 2003) szellemében könnyebben átléphetők.
- *Kontrollhiány.* Az online hálózatot ellenőrző intézmények által kevésbé ellenőrzött, privát böngészésre alkalmas *darkweb* működése növeli a kibertérben megvalósuló normasértések látenciáját (YAR 2006, 9.).
- *Az offline normák eróziója.* Az anonimitás által támogatott kettős lét a digitális bennszülöttek szocializációjának része (PRENSKY 2001, 1–6.). Az efféle szocializációs

folyamatban a hagyományos normák nem mindegyike internalizálódik és automatizálódik, ami a valós életviszonyokban az eligazodás és alkalmazkodás nehézségeit okozza és termeli újra.

- *Online-offline normakompatibilitás.* Egyre gyakoribb, hogy az egyén a virtuális szabályokhoz illeszti viselkedésének mércéjét, majd onnét kilépve ugyanezt a mércét a valós térbe is átviszi, és fordítva (TURKLE 2000). Amennyiben a két mérce nem kompatibilis, a két szintér egymástól eltérő elvárási repertoárján alapuló normakompatibilitási feszültség keletkezhet, ami deviáns magatartásokhoz vezethet.
- *Destruktív e-trendek terjedése.* A fiatal felhasználók körében a kibertérben megjelenő trendek utánzása – ha hallgatólagosan is, de – részben a kortárs közösség nyomásgyakorlásának eredménye. A követendő trendek fókuszában álló tárgyak vagy cselekvések rövid idő alatt egy egész generáció szimbólumává emelkedhetnek, elérendő célként fogalmazódnak meg a generáció tagjaiban (például a veszélyes offline cselekvések teljesítése, vagyis a bátorságpróba). A világhálón megjelenő információbázisok gyártói és szerkesztői, a kortárs csoportok vélemény- és trendformálói, a tartalomszolgáltatók – ha nem is mindig közvetlen módon, de – cselekvést meghatározó hatalommal rendelkeznek, és képesek hozzájárulni a deviáns magatartásformák megvalósulásához.
- *A nyilvánosság megváltozása.* A nyilvánosság hagyományosan a közügyek intézésének a területe, élesen elhatárolva a magánszférától. 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 közszereplők esetében kifejezetten reklámeszköz a magánélet közüggé tétele. Azonban nemcsak a nyilvánosság előtt élők esetén merül fel a magán- és a nyilvános szféra közötti határ elmosódása. Minden olyan esetben, amikor magánügyek kerülnek nyilvánosságra, 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).
- *Digitális kompetencia.* A hagyományos deviáns viselkedések mintázataihoz képest a kibertérben leginkább az jöhet számításba normasértőként, aki alapvető digitális kompetenciával és az internet hálózatához elegendő hozzáféréssel rendelkezik. Ugyanez nem mondható el a kiberdevianciákat elszenvedőkről.
- *Az e-bizalom felértékelődése.* A bizalom az egyéni kötődések alapja és egyben a kereskedelmi tranzakciók (eBay) sikerének záloga (O'REGAN 2016). Az ügylet vagy a személyes kapcsolat megbízhatóságáról való tájékozódás az outputperifériákon keresztül sokkal korlátozottabb, ezért a bizalom marad a legfőbb garancia. Az online bizalomra hagyatkozás nemes alapja az együttműködésnek, és bár közvetett módon, de kapcsolódik a devianciákhoz, voltaképpen azok folyamatában egyfajta kockázati tényezőként tartható számon.

Valójában az új társadalmi tényezők cselekvésmódosító hatásai a mai napig arra motiválják a kibertér kutatóit, hogy megalkossák azt a fogalmi keretet, ami felismerési, értelmezési és eligazodási lehetőséget nyújt a hagyományos szintéren, a kibertérben, illetve az ezek kombinációiban megjelenő normasértések között, és ezzel kijelölik a kibertér és a fizikai

színtér határait. Kötetünk következő fejezetében a normasértő magatartások besorolhatósága érdekében a kiberdeviancia fogalmi meghatározására teszünk kísérletet.

2.2. Deviancia a kibertérben

A *deviancia* legelterjedtebb 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 et al. 1974; ROSTA 2007). A deviánsnak minősített egyén magatartásának veszélyességi fokát leginkább az fejezi ki, hogy a megsértett szabályokhoz milyen közösségi attitűdök kötődnek, vagyis mennyire fontos és meghatározó értékeken alapulnak. Mivel a deviancia köztudatban elterjedt fogalomköre magában foglal számos *eltérő*, de veszélytelen viselkedésformát vagy jelenséget, ezért célszerű kijelölni azokat a szempontokat, amelyek figyelembevételével kiemelhető és leszűkíthető a legnagyobb kockázatot jelentő deviációk csoportja. A deviánsnak tartott magatartások különböző definíciói között vannak olyan közös vonások, amelyek egységesen utalnak az univerzálisan károsnak ítélt magatartásformákra. Többek között

- a társadalom többsége negatív értékítéletét fejezi ki a deviánsnak minősített magatartásokkal szemben,
- az adott magatartás komplex reakciót vált ki mind a társadalom tagjaiból, mind a kontrollintézmények részéről,
- a deviáns viselkedésforma nem lehet túlsúlyban a konform magatartásformákhoz képest, és
- többnyire veszélyt jelent az egyénre és a közösségre, beleértve a deviáns személyt önmagát is (ön- és közveszélyesség) (GÖNCZÖL–KEREZSI 1993; ROSTA 2007; GIDDENS 2008).

A kriminológia képviselői a deviancia modern megfogalmazásában az ön- és közveszélyességet emelik ki fő szempontként, és a deviánsnak minősítést a kiváltott intézményes reakció meglétéhez kötik (GÖNCZÖL 2016, 115.). A deviáns jelenségek megítélése önmagában sem egyszerű, de az ön- és közveszélyes magatartásokkal szemben kialakuló különféle társadalmi viszonyulás ezt még bonyolultabbá teszi, például azzal, hogy „tűrt, még tolerált és már tiltott” magatartásokként – ha néha hallgatólagosan is, de – egymástól elkülöníti (GÖNCZÖL 2016, 115.). A meghatározást az is befolyásolja, hogy a társadalom mikor, milyen módon és eszközökkel reagál a negatív megnyilvánulásokra. Ennek hátterében markáns szerepet tölt be a már említett társadalmi toleranciaképesség, a tradíciók és a kultúra, valamint az adott társadalom kormányzatának törekvései és a deviancia kezelésére irányított valós erőfeszítései (például hogy milyen mértékű erőforrásokat fordít a társadalmi jelenség kezelésére) (GÖNCZÖL 2016, 116.). A deviancia kezelésében hozott kormányzati döntések jelentősen meghatározzák a devianciák alakulását pozitív és negatív irányban egyaránt. Voltaképpen ez azt jelenti, hogy a kormányzati intézkedések lehetnek a devianciákat mérséklők és a deviancia reprodukcióját vagy devianciaspirált generálók (GÖNCZÖL 2016, 116.). A modern megfogalmazás szerint tehát a deviancia „az átlagostól,

az uralkodó normáktól, az elvárt és még tolerált magatartási formáktól eltérő olyan ön- és/ vagy közveszélyes magatartások halmaza, amely a többségi társadalom oly mértékű erkölcsi rosszsallását váltja ki, hogy a féken tartásukra – a szaktudományok fejlettségének és az uralkodó felfogásoknak megfelelő – intézményes reakciókat rendszeresít” (GÖNCZÖL 2016, 117.). Egyes jelenségeket a társadalom tagjai akkor is normalistól vagy megszokottól eltérőnek minősíthetnek, amikor egy olyan gyors lefolyású globális vagy társadalmi változás eredményei, amihez az adott közösség nem tud egyszerre alkalmazkodni. Az elmúlt évtizedekben az internet és a számítástechnikai eszközök globális forradalma pont ilyen jelenség volt. A technológia robbanásszerű fejlődése és a hálózatosodás kizökkentette a hagyományos kommunikációs környezetében élő egyént megszokott életmódjából, majd az innovációk társadalmi terjedésének következtében a digitális eszközökhöz való hozzáférés, valamint a digitális kompetenciákban mutatkozó különbségek mélyítették a társadalom egyes csoportjai között fennálló szakadékot. Ennek megfelelően még ma is megfigyelhető, hogy a korábbi predigitális generáció tagjai a technikai alapokra helyezkedő globális hálózatosodást gyakran erőn felülinek ítélik meg. Christopher Freeman a gyors lefolyású technológiai átalakulás társadalmi gazdasági folyamatokra gyakorolt hatását nem a normától való eltérésként, hanem technológiai paradigmaként fogalmazta meg, amelynek legfőbb jellegzetességét a technológia információra irányultságában, az új technológia mindent áthatóságában, a rendszerek és kapcsolatok hálózati logikát követő felépülésében, a rugalmas átalakulásban és a speciális technológiák integrációjában látta (CASTELLS 2005, 117–119.). Freeman okfejtése tisztább képet fest, ugyanis az új környezet kínálta lehetőségeket felismerő és azokhoz alkalmazkodni tudó társadalmakban ma már megkérdőjelezhetetlen, hogy a technikai fejlődés és az internetes hálózatosodás sokkal inkább a gazdasági, társadalmi, politikai fejlődés kulcsa, mintsem egy olyan jelenség, amely a normalistól eltérő. A devians viselkedés inkább a kibertérhez kapcsolódó egyéni és közösségi érdekek és értékek szükségszerű következményeként alakult ki és vált megfogalmazhatóvá és súlyozhatóvá. Ez utóbbi a kiberdevianciák területén azt jelenti, hogy vannak olyan normasértő faktorok, amelyekkel szemben inkább a közömbösség erősödik (túrt és tolerált), emellett léteznek olyanok is, amelyek időben és térben az állandó elítélés tárgyai. A durva, normaszegő magatartásmintákat és az enyhébb megítélésű elhajlásokat ennek okán egy szűkebb és egy tágabb fogalmi keretbe illesztve, a hagyományos deviancia fogalmi elemeinek figyelembevételével vázoltam fel. Eszerint az olyan cselekedet minősül kiberdevianciának,

- amely érinti a kibertérét;
- amely jogi normát sért vagy ön- és közveszélyes a kibertérben;
- amelyhez a társadalom többsége negatívan viszonyul;
- amely kiváltja a társadalmi többség és a kontrollintézmények negatív 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 kiberdeviancia szűkebb értelemben a kibertérben 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, vagy veszélyt jelent az egyénre és/vagy a közösségre.

A globális hálózat heterogén közösségeiben az értelmezés egy cseppet sem egyszerű. A legtöbb társadalomban a gyermekkorúakról készült pornográf felvételek terjesztése jogsértő, a rágalmozás vagy a becsületsértés azonban eltérő értelmezésű lehet. A fentiekben meghatározott szűkebb fogalom szerint a kibertérben elkövetett szabályszegő magatartás deviánsnak minősítése – bár nagyjából azonos feltételek szerint került megfogalmazásra – függ attól, hogy mely társadalom felhasználóinak körében került nyilvánosságra, és a deviáns magatartásokat megvalósító és elszenvető mely társadalom tagja. A kiberdeviancia tágabb fogalomköre a szűkebb fogalomkört is magában foglalja, de annál jóval több megnyilvánulásra kiterjed, és nemcsak a súlyosabb normasértésekhez áll közel. Ennek alapján kiberdevianciának az olyan cselekedetet nevezem,

- amely érinti a kibertérteret;
- amely valamely normát sért a kibertérben;
- amely kiváltja a társadalom többségének negatív értékítéletét;
- amely legalább 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 kiberdeviancia tágabb értelemben tehát a kibertérben 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 kiberdeviancia mindkét fogalma két feltételben tér el a hagyományos devianciafogalomtól, mégpedig a kibertérben való megvalósulás szükségességében és a digitális kompetencia meglétében.

2.3. A kiberdeviancia szintérmódozatai

Bármilyen kiberdevianciáról is legyen szó, hátterében emberi motivációk és célok fogalmazódnak meg, végső soron emberi cselekvések eredményei, mint ahogyan azok megítélése és szankcionálása is, ezért az internet hálózatában a számítástechnikai rendszerek és eszközök együttese eszközként és lehetőségként is számításba vehető. Kétségtelen, hogy a legtöbb kutatás a humán meghatározottságokból és a hagyományos környezetből indul ki, vagyis a virtuális teret az alanyokhoz viszonyítva mutatja be, viszont kevésbé fókuszál a környezet katalizáló szerepére. A kibertér normasértő cselekvéseket generáló sajátosságai a belépő felhasználók magatartásváltozásai mentén figyelhetők meg, vagyis azokban az esetekben, amikor az új környezet hatásai révén a felhasználóban gyengülnek azok a visszatartó erők, amelyek a mindennapi feszültségek felszabadításában a hagyományos térben meggátolják (PARTI 2018). Az offline és az online tér közötti devianciaátjárásról szól

az *EU Kids Online* című kutatás is, amelyben Livingstone, Haddon és Görzig kockázat-vándorlási hipotézisének (*risk migration hypothesis*) legfőbb mondanivalója, hogy az online kockázatvállalás nagyon szoros kapcsolatban áll a hagyományos környezetben tanúsított viselkedéssel és az életkorral (BARBOVSCHI et al. 2012, hivatkozik rá PARTI 2018). Az emberi cselekvések okai és megvalósulási színtereinek különböző kombinációi, röviden színtérmódozatai egyébként a korábban hivatkozott Grabosky diskurzusában használt hasonlat mentén is megragadhatók (*old wine in new bottles*). A térbeli mozgás (mobilizálódás) modellezése tehát időszerű és indokolt, ebben a normasértéseket logikus más-más szintéren zajló mozzanatokként és összefüggéseikben is vizsgálni. Az előbbi esetében a terekben külön-külön megvalósuló cselekvések eltérő súlya, különböző jogi és társadalmi megítélése, az utóbbi esetben a normasértő magatartás teljes hatása mérhető. A szinterek között mobilizálódó deviancia akkor nevezhető kiberdevianciának, ha a normasértés folyamata valamilyen módon érinti a virtuális teret. A folyamatban a deviancia logikailag négy különböző módon jelenhet meg:

1. *Eredmény- és színtérmódozat*. Ebben a típusban a normasértés a kibertérben kezdődik, ott zajlik, és ott is végződik, vagyis tisztán a kibertérben. Ebben a módzatban felerősödik az anonimitás, a titkos információáramlás, a kevésbé szabályozott szürke foltok működése és a digitális identitás szerepe, ugyanakkor a normasértők köre leszűkül azokra, akik digitális kompetenciával rendelkeznek. Mivel az eredmény- és színtérmódozat minden elemében érinti a kibertert – sőt, csak és kizárólag azt érinti –, ezért ebben a modellben helyezhetők el a kiberdeviancia új formái.
2. *Eredménymódzat*. A folyamat kiindulópontja a hagyományos tér, azonban a deviáns magatartások a virtuális „infrastruktúrákban” végződnek. Azaz olyan magatartásokról van szó, amelyek mind a rendszerintegritás elleni (például hagyományos szintéren való megtévesztéssel megszerzett adatokat követő rendszerfeltörés), mind a tartalommal vagy médiummal összefüggő deviáns magatartásformákat (például a párkapcsolati erőszak verbális, zaklató jellegű formája) magukban foglalják.
3. *Színtérmódzat*. A színtérmódzat az eredménymódzat fordítottjaként működik. Ebben az esetben is mind a valós, mind a virtuális teret érinti a normasértés, ezúttal viszont a kibertérben kezdődik a folyamat, ott is zajlik, de a valós térben fejeződik be. Ma már az sem újdonság, ha egy virtuális térben eszkalálódó konfliktus testi sértéssé fajul, vagy az internetes kábítószer-kereskedés megrendelője szemtől szemben veszi át a tiltott szereket. Ide köthető a prostitúciós szolgáltatások internetes reklámozása és még sok más folyamat, amely az offline térben zárul.
4. *Katalizáló módzat*. A hagyományos és a kibertér szoros kapcsolatát azok a normasértő magatartások fejezik ki igazán, amelyek történetük folyamatában átfogják a hagyományos és a virtuális teret. 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 folyamatában. Azaz a katalizáló módzat két alcsoportra osztható a kibertér és az offline tér katalizáló funkciója szerint:
 - Az első esetben a kibertér 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. Ennek modellezésére a napjainkban ciklikusan változó irányú *cyberbullying* szolgál példaként, ahol az online lejáratást offline kiközösítés követ, majd ennek folytatásaként újabb internetes nyomásgyakorlás következik egy folyamatban (valójában a *cyberbullying* mindkét módozatra igaz lehet).

A négy módozat a kibertér átjárhatóságának olyan értelmezési struktúráját adja, amivel az egyes cselekvések mögött rejlő érzelmi és morális diszpozíció is felfedhető, mindazonáltal kiküszöbölhető a szintereket átfogó cselekvések leegyszerűsített megítélése.

2. táblázat

Az egyes magatartásformák színtérmódozatai

Magatartásmintázat	Eredmény- és színtér- módozat	Eredmény- módozat	Színtér- módozat	Katalizáló módozat	
				online	offline
Szexuális tartalmak szerepeltetése (<i>sexting</i>)	+	–	–	–	–
Heves párbeszéd (<i>flaming</i>)	+	–	–	–	–
Információs rendszerek megsértése	+	–	–	–	–
Behálózás (<i>grooming</i>)	+	–	+	+	–
Zaklatás	+	+	+	+	+
Zsarolás	+	+	+	+	+
Csalás	+	+	+	+	+
Kényszerítés	+	+	+	+	+
Extrémizmus, terrorizmus	+	+	+	+	+

Forrás: Kiss 2018

2.4. A kiberdevianciák motivációi

A hagyományos, társadalmi együttélésre veszélyes devianciák szűk fogalomkörébe olyan stabil magatartásminták tartoznak, mint az alkoholizmus, a kábítószer-fogyasztás, az öngyilkosság, az antiszociális viselkedést megalapozó mentális betegségek és a bűnözés (ROSTA 2007). Fizikai megjelenésüktől eltekintve igen gyorsan integrálódtak a kiberkörnyezetbe (például a 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, és gyakran arra is korlátozódnak. Ezek többnyire a *szexuális* ösztönkésztetésekből, az *agresszív* érzelmekből és a *haszon-szerzési* szükségletekből eredeztethetők, miközben a társadalom és kontrollintézményei jelentik megítélésük alapját.

2.4.1. Szexuális motiváció

A kibertérben a normasértő szexuális viselkedések valamennyi, az adott helyzetben részt vevő személy egységes akaratának hiányában, fizikai kapcsolat nélkülözésével vagy a fizikai érintkezés előkészítéseként, előzményeként zajlanak. 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, illetve az agresszív feszültségeknek (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, kortárs csoportokból álló baráti közösségek, a szemtől szemben történő észlelés és a személyi azonosítás lehetősége. Az anonimitás emellett a gátlások nélküli fantáziálásoknak és a parafiliák (például a pedofília) megjelenésének is melegágya lehet. A kibertérben megvalósuló szexuális motivációk által ösztönzött normasértő magatartások veszélyességük szerint három csoportba sorolhatók:

- a szexuális tartalmak a szexuális feszültség normasértő eredménnyel járó levezetését szolgálják (például a szexuális tartalmak küldése, fogadása, közzététele);
- a kibertérben zajló cselekvés bármely szintéren megvalósuló szexuális normasértés előzménye vagy előkészítő stádiuma (például a behálózás);
- a szexuális erőszak lenyomata vagy annak következményei a virtuális környezetben észlelhetők (például a zaklató jellegű magatartás vagy zsarolás).

A három viselkedésforma mindegyike valamilyen normasértést keletkeztet, és céljuk *a szexuális szükségletkielégítés vagy szexuális feszültséglevezetés*. Eltérés abban van, hogy más-más súlyú deviáns magatartásformák a részei a szexuális tartalmak küldésétől a behálózáson át az erőszak alkalmazásáig.

3. táblázat

A szexuális motivációkra épülő normasértések a kibertérben

Szexuális motivációk	• szexuális tartalmak szerepeltetésével való visszaélés (például <i>sexting</i>, szexuális témájú kommunikáció) • behálózás (<i>grooming</i>)
Szexuális motivációk agresszióval vagy erőszakkal összefonódva	• szexuális tartalmak szerepeltetésével történő visszaélés (például <i>sexting</i>, azaz a szexuális témájú kommunikáció bosszúból) • kibertérben történő szexuális zsarolás • kibertérben történő szexuális zaklatás

Forrás: KISS–PARTI–PRAZSÁK 2019

2.4.2. Haszonszerzési motiváció

A haszonszerzési szükségletek – ahogy a hagyományos térben is – markáns motivációként szerepelnek a kibervediancák háttérében. Nagyon gyakran kapcsolódnak az agresszív vagy erőszakos motivációkhoz, és kimondottan anyagi vagy más haszon elérésére irányulnak. A magatartást megelőzheti a behálózás szakasza, és eszköze lehet a szexuális tartalmak szerepeltetése (például a szexuális tartalmak szerepeltetése az interneten), főként zsarolás esetében. A haszonszerzési szükséglete körül felépített műveletekre különösképp jellemző a terek közötti mozgás, pontosabban amikor az elkövetés a kibertérben, az anyagi kár a hagyományos színtéren történik, és fordítva. A kibertérben a haszonszerző normasértések három csoportja különíthető el megvalósításuk módja és terepe szerint:

- haszonszerzés információs rendszerek elleni támadásokkal, technikai módszerek segítségével (például a szolgáltatás megtagadásával járó kibertámadások);
- az illegális kereskedelmi tevékenységek útján történő jogtalan haszonszerzés (például a kábítószerekkel vagy fegyverekkel való kereskedelmi tevékenység);
- az információs csatornákon át történő információközléssel vagy kommunikációval megvalósított haszonszerzési folyamat (például egy megtévesztő tartalom elküldése a levelezőrendszerben).

4. táblázat

Haszonszerzési motivációkra épülő normasértések a kibertérben

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 (<i>grooming</i>) • kibertérben megvalósuló csalás
Haszonszerzési motivációk agresszióval vagy erőszakkal összefonódva	• kibertérben történő zsarolás • kibertérben történő zaklatás

Forrás: KISS–PARTI–PRAZSÁK 2019

2.4.3. Agresszióra épülő motivációk

Az agresszió belső lelki tartományban rejtőző késztetésekhez, külső környezeti tényezők által alakított lelkiállapotokhoz köthető, támadó jellegű magatartás. Ellenséges belső rezdűletek, 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 az 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 kibertérben az agresszív megnyilvánulások széles palettájával találkozhatunk, ezek kifejeződhetnek

kép-, hang-, szöveg-, gif-, internetes mémes tartalmakban, kommunikációban zajló, heves párbeszédben. Az agresszív érzelmek – hasonlóan a hagyományos térhez – a kibertérben is a legsúlyosabb erőszakos normasértésekhez vezethetnek, azzal a különbséggel, hogy a hagyományos térhez képest az erőszak nem 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, amiről az agresszióelméletek széles irodalma ad különböző magyarázatokat. A virtuális környezetben megjelenő agresszív megnyilvánulások nem mindegyike eredményez jogi normát sértő cselekvéseket és pszichés erőszakot sem, ugyanakkor a legenyhébb formája is negatív hatással van a résztvevőkre. A kibertérben megnyilvánuló agresszió társadalomra való 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 kibertérben 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, kibertérben 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., hivatkozik rá: VIRÁG–KULCSÁR–ROSTA 2016, 554.). A kibertérben 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 vagyoni elleni normasértésekben. A kibererőszakra is érvényes az a megállapítás, hogy minden esetben agresszióból keletkezik, de az agresszió nem minden esetben válik erőszakos magatartássá (VIRÁG–KULCSÁR–ROSTA 2016, 555.). Ha ebből indulunk ki, akkor a kibertérben megnyilvánuló erőszak az egyén vagy közösség irányába ható agressziónak a virtuális tér „infrastrukturái” mentén megnyilvánuló tudatos, szándékos, károkozásra képes formája.

A kiberkörnyezetben az erőszakos magatartásmintázatok megvalósításuk szerint két csoportra oszthatók: amikor a *kényszerítés*, a *fenyegetés* alkalmazását követően a normasértés a *hagyományos térben végződik* (közvetett), és amikor a *kibertérben 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). A kibererőszak fogalmába tartozhat a zsarolószoftver (*ransomware*). A szoftvert az elkövető eljuttatja a kiszemelt felhasználó rendszerébe, ahol rendszerbénulást okoz. Amíg a felhasználó nem fizet „váltásdíjat”, a rendszere blokkolva marad (SYMANTEC 2015).

A kibererőszak két alapvető eleme valamelyik vagy mindegyik meglétéhez kötött, súlyosabb kiberdevianciákat eredményez, valamely normát sért, és a társadalom széles köre által elítélt. Az erőszak kiberkörnyezetben zajló mechanizmusa – hasonlóan az agresszióhoz – több jellemzővel bír:

- szándékos károkozásra vagy szükségletkielégítésre irányul, és agresszióból fakad (kényszerítéssel, fenyegetéssel megnyilvánuló agresszió);
- a kibertérben 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 kibertérben megnyilvánuló erőszak a fenti jellemzők szerint *minden olyan – nem fizikai formában megjelenő – kényszerítéssel, fenyegetéssel megvalósított agresszív cselekvés, ami 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 szintéren fejeződik be, csak akkor sorolható a kibererőszak fogalmi körébe, ha a kényszerítés, a fenyegetés valamelyike vagy mindegyike a kibertérben is megtörténik. A hagyományos térben erőszakos bűncselekményeknek minősített és a kibertérben 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 kibererőszak megfogalmazását viszont a pszichés erőszak feltételei – vagyis a kriminológiai fogalom – mentén határoztuk meg. Míg tehát a kibertérben megjelenő zaklatás a büntetőjog értelmezése szerint nem tartozik az erőszakos bűncselekmények körébe, addig kriminológiai értelemben annak minősíthető.¹

A virtuális térben az agresszió által motivált cselekvések oksági folyamatát és társadalomra való 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. A kényszerítés és fenyegetés által előidézett és a kibertérben manifesztálódó magatartások körét a 7. fejezetben részletesen tárgyaljuk.

¹ Btk. 222. §.

5. táblázat

Agresszióra és erőszakra épülő normasértések a kibertérben

Agresszióra épülő	• negatív érzelmeken alapuló párbeszéd (<i>flaming</i>) vagy negatív érzelmek által motivált tartalommegjelenítés • negatív érzelmek által motivált, önbecsülést sértő vagy becsületcsorbító kifejezés, tényközlés kommunikációban vagy tartalommegjelenítéssel (például a becsületsértés, rágalmozás) • egyén vagy közösség elleni, szándékos károkozó magatartás a 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 (kényszerítés, fenyegetés, megfélemlítés vagy félelemkeltés alapvető eleme)	• kibertérben történő zsarolás • kibertérben történő zaklatás • extrém csoportok kibertérben történő erőszakos működése • terrorszervezetek kibertérben történő erőszakos működése

Forrás: KISS–PARTI–PRAZSÁK 2019

2.5. A kiberbűnözés mint esszenciális kiberdeviancia

A kiberbűnözés létezése több mint húsz éve evidens jelenség, de a fogalmi meghatározására tett próbálkozások mégis csak az elmúlt tizenöt évben élénkültek fel, miután a web 2.0 által a normasértő magatartásmintázatok egyre szélesebb felhasználói réteget értek el, és egyre láthatóbbá váltak a globális hálózatokban. Ezt követően született meg néhány bűnözés-fogalmat felvonultató tanulmány, amelyek közül az egyik a már korábban említett Peter N. Grabosky nevéhez fűződő *old wine in new bottles*. Grabosky fogalommeghatározását követte Rutger Leukfeldt kiberbűnözésről szóló tanulmánya. Ebben arról írt, hogy a kibertérben megvalósuló bűncselekmények azok a cselekvésformák, amelyek az információs térrel, információs technológiával jelentős kapcsolatban állnak, illetve azok, amelyek nem kifejezetten az információs technológiát célozzák, de kötődnek ahhoz. Eszerint a *cyber-crime* átfogó kifejezése azokra a magatartásmintázatokra vonatkozik, amelyeknek feltétele az információs technológia igénybevétele. Leukfeldt ezen belül megkülönböztetett olyan devianciákat, amelyekben az információtechnológia egyben cél és eszköz, valamint olyanokat, amelyek megvalósításához az információtechnológia elengedhetetlen, de nem célpont (LEUKFELDT 2016, 214–215.; PARTI 2018). David S. Wall a kiberbűnözés kialakulásának folyamatát a számítógépes bűnözés evolúciójának nevezte, és olyan generációs korszakokra tagolta, amelyekben a globális internet generációról generációra egyre fontosabb szerepet töltött be (WALL 2008). A Wall által felvázolt modernkori harmadik generációs bűnözés olyan, a hálózat biztonsága elleni és a hálózatot mint médiumot az elkövetéshez felhasználó bűncselekmények összessége, amelyeknek elsődleges jellemzője az előre kifejlesztett számítástechnikai eszközök szervezett és elosztott formában, meghatározott munkavégzési rendben, automatizált módon való felhasználása valamely bűnözői csoportokkal vagy

bűnszervezetek hozzáadott tevékenysége nyomán, meghatározott cél elérésére (WALL 2008, 55–56.). Wall szerint a harmadik generációs bűnözés jellemzője a nemzetköziség, a gyorsaság, a magas látencia, valamint az intellektuális jelleg (PARTI–KISS 2016, 463–495.).

6. táblázat

A számítógépes bűnözés evolúciója

Első generációs bűnözés	A bűncselekményekhez a számítógépeket használták eszközként, az internetről csak információkat gyűjtöttek a bűncselekmények elkövetéséhez.
Második generációs bűnözés (hibridek korszaka)	Amikor az internetet már felhasználták egyes rendszerekbe való jogellenes bejutáshoz, de ennek nagyságrendje minimális volt.
Harmadik generációs bűnözés	A bűncselekmények elkövetésének folyamatában az internet globális hálózata nélkülözhetetlen (például automatizált eszközökkel történő bűnelkövetés).

Forrás: WALL 2008

Parti Katalin definíciója még ennél is logikusabb. Szerinte az informatikai bűnözés (kiberbűnözés) a számítástechnikai bűnözés (*computer 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 (PARTI–KISS 2016, 491.). Parti fogalomhasználatában a számítástechnikai bűnözés a számítástechnikai rendszerek és hálózat integritását sérti (például a rendszerekbe való illetéktelen behatolás), az internetes bűnözésnél az internet az elkövetés terepeként szolgál (például hamis weboldalak segítségével banki adatok kicsalása). 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 a számítógéppel vagy számítógépes hálózatban folytatott kettős könyvelés), nem tartoznak a modern informatikai bűncselekmények kategóriájába (PARTI–KISS 2016, 492.).