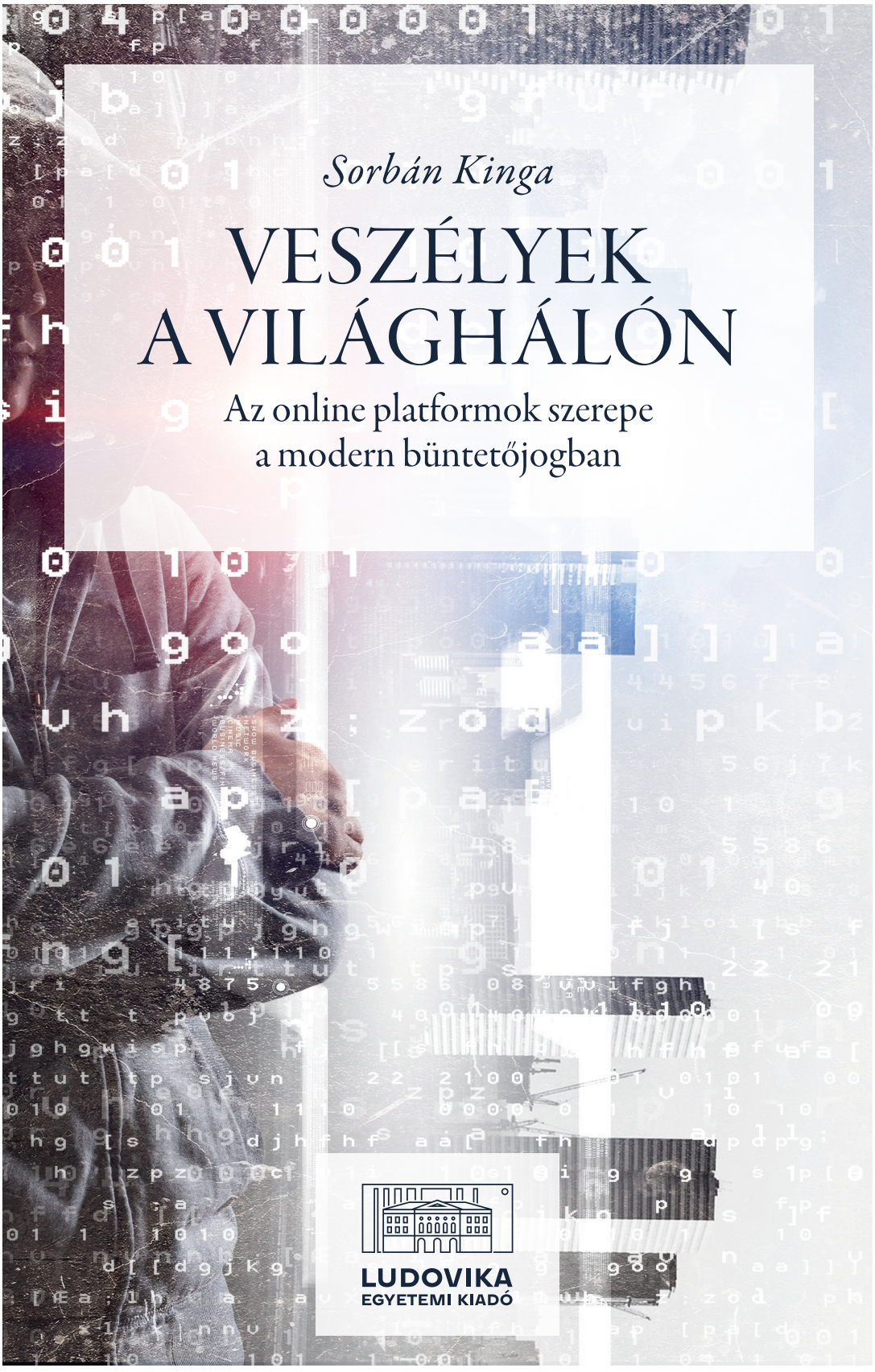


Sorbán Kinga

VESZÉLYEK A VILÁGHÁLÓN

Az online platformok szerepe a modern büntetőjogban

LUDOVIKA
EGYETEMI KIADÓ

Sorbán Kinga

Veszélyek a világhálón

Sorbán Kinga

Veszélyek a világhálón

Az online platformok szerepe a modern büntetőjogban

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2024

A mű az NMHH-val kötött, EM-1/1/2022. számú együttműködési megállapodásban részletezett feladatok végrehajtása céljából készült.

Szakmai lektor
Mezei Kitti

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztők: Karácsony Fanni, Inzsöl Kata
Olvasószerkesztők: Fülöp Éva, Szabó Ilse
Korrektor: Bujdosó Hajnalka
Tördelőszerkesztő: Tihanyi József

DOI: https://doi.org/10.36250/01201

ISBN 978-963-653-100-3 (nyomtatott)
ISBN 978-963-653-101-0 (elektronikus PDF)
ISBN 978-963-653-102-7 (ePub)

Tartalom

I. Bevezető gondolatok 7
A kötet szerkezeti felépítése 15

II. Fogalmi alapok 19
Informatikai alapfogalmak 19
Az internet architektúrája és rétegei 24
Az informatikai bűnözéssel kapcsolatos fogalmak – bűncselekmények számítógépes környezetben 26
Az online tér szereplői 33

III. Az informatikai bűnözés nemzetközi környezete 57
Az informatikai bűnözés rövid története – avagy hogyan lett a számítógép napjaink egyik legnagyobb nemzetközi bűnüldözési kihívása? 58
Az informatikai bűncselekmények nemzetközi jogi forrásai 65
Az informatikai bűncselekmények elleni fellépés európai dimenziói 72
Az informatikai bűncselekmények elleni fellépés az Egyesült Királyságban, Franciaországban és Németországban 111
Informatikai bűncselekmények az Egyesült Államokban 131

IV. Az informatikai bűncselekmények Magyarországon 149
Az informatikai bűncselekmények magyarországi története 149
Az informatikai bűncselekmények szabályozása a magyar jogban 154
Tisztán informatikai bűncselekmények 156
Információs rendszer és adatok elleni bűncselekmények 157

Az információs rendszerrel kapcsolatos bűncselekmények 185
Tartalom-bűncselekmények 215

V. Online fenyegetések a büntetőjog határán 261
A szexuális tartalmakkal kapcsolatos visszaélések 262
A cyberbullying ezer arca 281
A valótlan közlés, a hamis hír (fake news) és a félretájékoztatás (disinformation) mint büntetőjogi probléma 295
Gyilkosság és erőszak a kibertérben 306
Online terror – az internet terrorista célú használatának szankcionálása 317

VI. Az informatikai bűncselekmények nyomozásának egyes kérdései 331
A digitális bizonyíték fogalma és forrásai 332
A digitális bizonyítékok megszerzése és megőrzése 341
Speciális eszközök a malware-ek felderítésében 347
Speciális eszközök a határokon átnyúló kiberbűncselekmények nyomozásában 354

VII. Az internetes közvetítő szolgáltatók szerepe és felelőssége a kiberbűncselekmények felderítésében és nyomozásában 369
A büntetőeljárás egyéb szereplőinek helyzete az új Be. rendelkezéseinek tükrében, a közvetítő szolgáltatók büntetőeljárásbeli pozíciója 371
Az internetes közvetítő szolgáltatók részvétele az egyes kényszerintézkedések végrehajtásában 372
Az internetes közvetítő szolgáltatók felelőssége harmadik személyek jogellenes tartalmaiért 388
A társadalmi felelősségvállalás és a platformok magánszabályozásának szerepe a tartalom-bűncselekmények elleni fellépésben 397
Az online platformok által alkalmazott mesterségesintelligencia-alapú tartalommoderálás szabályozási kérdései 413

VIII. Pro futuro – adalékok egy jövőbeli szabályozási koncepcióhoz 431
A büntető anyagi jog reformja 433
A büntetőeljárás-jog reformja 435

Felhasznált források és irodalom 441

I. Bevezető gondolatok

Az internet mint a számítógépeket összekapcsoló globális hálózat az 1990-es évekbeli kommercializálódása óta szerves része a mindennapjainknak. Ma már sem a magánéletünket, sem a munkavégzést nem tudjuk elképzelni az internet és az ezerféle összekapcsolt eszköz nélkül. Nem túlzás azt állítani, hogy az internet kinyitotta a világot: a szórakoztatás, tájékozódás és a tájékoztatás, a vásárlás és a kapcsolattartás új dimenzióit tárta fel a nap 24 órájában elérhető, valós idejű kapcsolatot biztosító, az egész bolygót behálózó rendszer. Számtalan előnye mellett azonban a világháló szélesre tárta a kaput a bűnözés számára is.

Régi bűncselekmények jelentek meg új formákban (például az online zaklatás), és újfajta magatartásokról vált nyilvánvalóvá, hogy kriminalizálásukra a társadalom védelme miatt szükség van (például az információs rendszer vagy adat megsértése esetében). Az online jogsértések folyamatosan jelentkező nagy kihívások elé állítják a jogalkotókat és a jogalkalmazókat egyaránt. Ahogy Koltay András is felhívja rá a figyelmet,[1] az internetes jogsértő cselekmények egy részét, például a gyűlöletbeszédet ma is olyan törvények kezelik, amelyeket nem kifejezetten az online környezetre alkottak. Az internetes jogsértéseket tehát a jogalkalmazók igyekeznek a meglévő tényállások keretei közé szorítani, amennyiben ez lehetséges. A már létező szabályok azonban nem minden esetben alkalmazhatók az online környezetben, folyamatosan jelennek meg olyan új magatartások, amelyek nem illeszkednek egyik tényállás keretei közé sem (tipikusan ilyen a köznyelvben bosszúpornónak nevezett jelenség, amely

[1] Koltay 2019b: 98.

a korábbi partnerek által, a sértett hozzájárulása nélkül közzétett szexuális felvételeket takarja). A büntetőjogban a *nullum crimen sine lege* alapelvéből következően kizárt az analógia alkalmazása, a jogalkalmazó számára tehát nem adott a lehetőség, hogy a különböző cselekmények releváns tényállási elemeit összeválogatva jogot alakítson.

A dinamikusan fejlődő technológia és a változó magatartások folyamatos megújulásra sarkallják a szabályozást, ami egy komoly jogpolitikai dilemmát is felvet: ha a jog rugalmasan alkalmazkodik a gyorsan változó életviszonyokhoz, képlékennyé válik, ami a jogbiztonság szempontjából nemkívánatos. Ha viszont nem szabályoz időben egy jelenséget, akkor nem tesz eleget intézményes védelmi kötelezettségének. A dilemma nem csak a büntetőjog megújulásával összefüggésben merült fel, az 1980-ban leírt *Collingridge-dilemma* szerint a szabályozási probléma az, hogy egy új technológia hatásait nem lehetséges pontosan megbecsülni addig, amíg az teljesen ki nem fejlődött és nem vált széles körben alkalmazottá, viszont ha az adott technológia már elterjedt, nehéz szabályozás útján kezelni a problémáit és változást indukálni.[2] A Collingridge-dilemmát erősíti a Larry Downes által 2009-ben megfogalmazott fejlődés üteméből eredő probléma, az úgynevezett *pacing problem,* amely a fő nehézséget abban ragadja meg, hogy a technológia exponenciális ütemben változik, de a társadalmi, gazdasági és jogi rendszerek csak korlátozottan.[3]

A büntetőjogra vetítve e dilemmákat az elhamarkodott szabályozás folyamatosan változó magatartások esetében azzal a következménnyel is járhat, hogy mire az új magatartási szabályt elfogadják, és az alkalmazhatóvá válik, a jogalkotás indokául szolgáló cselekmény már rég nem releváns, „kiment a divatból", vagy éppen egészen új módon valósul meg. Az internethasználat kezdeti időszakában gyakoriak voltak az úgynevezett betárcsázós csalások, illetve a gépidőlopás, a széles sávú internet kereskedelmi szolgáltatássá válásával azonban ezek a magatartások teljesen eltűntek. Alapvető fontosságú tehát annak meghatározása, hogy szükséges-e, és ha igen, mikor az újfajta ártalmas magatartásokat szankcionálni, és mikor elégséges a már meglévő szabályok egyszerű adaptálása az új életviszonyokhoz. Egyesek, például Dobrocsi Szilvia és Domokos Andrea egyenesen azt a kérdést teszik fel, hogy szükség van-e „digitális büntető törvénykönyvre"?[4]

Az ártalmas online jelenségek elleni fellépés kirakósának a büntetőjog azonban csak egy darabkája. Az újonnan megalkotott szabályok nem üres térbe érkeznek, és a már meglévő szabályok sem steril környezetben léteznek, a büntető anyagi és eljárásjogra így

[2] Collingridge 1982.
[3] Downes 2009.
[4] Dobrocsi–Domokos 2018: 50.

több más jogág szabályai is hatással vannak. A büntetőjog, ahogyan az Alkotmánybíróság 30/1992. (V. 26.) határozata is megfogalmazza, a „jogrendszer egészének szankciós záróköve", vagyis „a jogi felelősségi rendszerben az *ultima ratio*". A technológia által megteremtett új, ártalmas magatartások kriminalizálását ennek megfelelően szigorú mérce alkalmazásával kell vizsgálni az alkotmányos célok és értékek mindenkori szem előtt tartása mellett. Az új internetes magatartások büntetőjogi fenyegetettségének meghatározása előtt tehát számításba kell venni, hogy milyen más jogágak szankciói jöhetnek szóba. Online tartalomközlések esetén felhívhatók a polgári jog személyiségvédelemmel kapcsolatos szabályai (a képmáshoz való jog vagy a személyes adatok védelméhez való jog), vagy a médiajog tartalomkorlátozással összefüggő rendelkezései (például a pornográf tartalmak korlátozása a kiskorúak védelme érdekében).

Mivel a tartalomközlések büntetőjogi fenyegetettsége minden esetben érinti a szólásszabadsághoz való jogot, az újonnan megjelenő ártalmas közlések kriminalizálásának szükségességéről szóló állásfoglaláshoz tárgyalni szükséges a szóláskorlátozás alapjogi aspektusait. Lehetnek ugyanis olyan esetek, ahol a véleménynyilvánítás szabadságához való jog védelme erősebb társadalmi érdek, mint a sérelmes tartalomközlések kriminalizálása. A szólásszabadsághoz való jogot érintő újfajta ártalmas online tartalomközlések esetén a kötet rámutat arra, hogy mikor korlátozható a véleménynyilvánítás szabadsága a büntetőjog eszközeivel. Mivel a büntető törvénykönyvben már szereplő, a szólásszabadság jogát korlátozó tényállások esetében az Alkotmánybíróság, az Európai Unió Bírósága (EUB), valamint az Emberi Jogok Európai Bírósága (EJEB) már mélyrehatóan elemezték a korlátozhatóság lehetséges eseteit, a rendelkezésre álló bírósági esetjog bemutatása elengedhetetlen ahhoz, hogy az újfajta közlések esetében megfelelően vonhassuk meg a véleménynyilvánítás büntetőjogi eszközökkel való korlátozhatóságának határait.

Nem mehetünk el szó nélkül a magánszabályozás jelentősége mellett sem, mivel egyes online szolgáltatók (így a videómegosztóplatform-szolgáltatók vagy a közösségimédia-platformok) felhasználási feltételeikben maguk is megfogalmaznak tilalmakat és korlátozásokat, befolyásolva a platformokat használó jogalanyok, a felhasználók magatartását. Az online közvetítő szolgáltatók szabályzatai által tiltott tartalmak köre nem teljesen esik egybe a büntetőjogi szankcióval fenyegetett tartalmak körével, ami a védelmi szintek között disszonanciát eredményez. Ha átolvassuk néhány szolgáltató közösségi iránymutatásait, láthatjuk, hogy a tiltott tartalmak nem mindegyike jogsértő (például a Meta és az ahhoz tartozó Facebook és Instagram a meztelenség minden formáját tiltják), vannak ellenben olyan tartalmak, amelyek terjesztése nem ütközik a platform felhasználási feltételeibe, közzétételük mégis bűncselekménynek

minősül, aminek oka részben a jogrendszerek különbözősége és az, hogy az amerikai óriásvállalatok a szólásszabadsághoz való jogot kiemelten kezelik, részben pedig a platformimmunitás. A szabályozás egyik nagy kérdése, hogy a platformok magánszabályozása képes-e nyomást gyakorolni a szuverén nemzeti jogalkotóra és befolyásolni a nemzeti szabályokat, akár a büntetendővé nyilvánított magatartások körét. A kötet összeveti az uniós és a magyar szabályokat a platformok által bevezetett szabályrendszerrel annak érdekében, hogy feltárja az esetleges ellentéteket, szürkezónákat.

Az előbbiekben leírtak vélhetően jól érzékeltetik, hogy az online tér egyes cselekményei nem vizsgálhatók pusztán egy jogág szemüvegén keresztül. Ha csak az anyagi büntetőjog lencséjén keresztül tekintenénk az online tér jogellenes és ártalmas magatartásaira, könnyen elveszhetnek fontos összefüggések, amelyek a jövőbeli szabályozás szempontjából értékesek lehetnek. Éppen ezért jelen kiadvány – noha magára főként büntetőjogi írásként tekint – nem szorítkozik csupán a büntető anyagi jog szabályainak ismertetésére és elemzésére, hanem teljes képet rajzol a vizsgált magatartásokról és az egyes jogágak metszéspontjában eredő dilemmákról.

A tárgyalt téma szempontjából nem csak a különböző tiltást megfogalmazó anyagi jogi normáknak van jelentőségük, nem szabad megfeledkeznünk arról, hogy a büntetőjog célja a társadalom védelme, a generális és speciális prevenció. E célok megvalósítását szolgálja a büntetőeljárás, amelynek célja az elkövető felelősségre vonása. Ezt a célt az internet több tekintetben is megnehezíti. Az online kommunikáció lehet anonim és titkosítható, ami megnehezíti az informatikai bűncselekmények elkövetőinek azonosítását és a cselekmény felderítését. Az internetes bűnözés globális jelenség, amely nincs tekintettel az országhatárokra, ez pedig a sikeres felelősségre vonás akadálya lehet. Az Európai Unió és az Európa Tanács a tagállami büntetőjogi szabályokat ugyan közelítették egymáshoz – az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (a továbbiakban: Cybercrime Egyezmény)[5] meghatározza és büntetni rendeli az informatikai bűncselekmények jelentős részét –, az egyes országok eltérő jogi hagyományainak és kultúrájának következtében azonban még napjainkban is előfordulnak jelentős különbségek. Markánsabban vannak jelen ezek a különbségek harmadik országok vonatkozásában. Az Egyesült Államok a véleménynyilvánítás szabadságát az európai jogrendszereknél, köztük a magyarnál is, fokozottabban védi. Nem számít bűncselekménynek például

[5] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

a rágalmazás, a becsületsértés, sem pedig a holokauszttagadás. Ezek a különbségek megnehezítik a nemzetközi jogérvényesítést, hiszen azért a közlésért, amelyet egy magyar felhasználó felháborítónak és sértőnek talál, egy amerikai felhasználó lehet, hogy semmilyen formában nem vonható felelősségre.

Az ilyen akadályok nemcsak az eljárásokra hatnak, hanem az azok alapját képező anyagi jogi szabályokra is hatást gyakorolhatnak, mivel kérdéses, hogy érdemes-e fenntartani az online környezetben alkalmazhatatlanná váló nemzeti szabályokat. Különösen igaz ez az olyan cselekmények esetében, amelyek dekriminalizálása már az online jogérvényesítés akadályaitól függetlenül is felmerült a magyar jogi gondolkodásban. Ilyen a rágalmazás és a becsületsértés, amelynek a dekriminalizálását Sajó András már 2005-ben is sürgette.[6]

Ennek ellentettje is felmerülhet problémaként, amikor nemzetközi jogi kötelezettségtől függetlenül egy más országban alkalmazott szabályozási megoldás elfogadására vagy átvételére kényszerül a magyar jog. Mivel az online kommunikáció piacvezető vállalatai többségükben a Szilícium-völgyben telepedtek le, az Egyesült Államok befolyása merülhet fel, amely az online platformokra irányadó szabályokon keresztül gyakorol hatást több más ország jogrendszerére. Az ilyen szabályok azonban a magyar jogban alapvetően idegenek lesznek, és mivel az egyes jogintézmények nem, vagy csak részben feleltethetők meg egymásnak, nem illeszkednek a hosszú idő alatt kimunkált dogmatikai rendszerbe.

Az eltérő szabályozási környezet mellett a felelősségre vonásnak egyéb akadályai is lehetnek. Az informatikai bűnözés olyan terület, amelynek a kezeléséhez a legtöbb esetben különleges szakértelem, határokon átnyúló kooperáció és hatalmas erőforrások szükségesek, amelyeket egyetlen nemzeti szerv sem képes önmagában biztosítani, egyes piaci szereplők azonban igen. Az internetes bűncselekmények nem valósíthatók meg egy vagy több közvetítő szolgáltatás használata nélkül, e szolgáltatók tevékenysége valójában átszövi az elkövetést, mivel a szolgáltatás lényegében a közeg, amelyben a cselekmény megvalósul. Az információs rendszerekbe betörő hackereknek is szükségük van internetkapcsolatra, amelyet az egyszerű hozzáférés-szolgáltatók *(mere conduit),* közismertebb nevükön internetszolgáltatók biztosítanak. Komplexebb a helyzet a tartalomközléssel megvalósuló bűncselekmények esetében, ahol az elkövetés jellemző helye a közösségi média (például Facebook) vagy valamilyen videómegosztóplatform-szolgáltatás (például YouTube), ahol a tárhelyszolgáltatóknak

6 Sajó 2005: 3–6.

(hosting service provider) lehet nagy szerepe a jogsértések felismerésében és megszüntetésében. Ebből kiindulva a kötet külön hangsúllyal tárgyalja, hogy az egyes cselekmények esetében az online közvetítő szolgáltatók mely pontokon és hogyan tudnak beavatkozni a jogsértés megszüntetése érdekében.

Felismerve e szolgáltatók különleges pozícióját, több jogrendszer igénybe veszi vagy kifejezetten előírja segítségüket a nyomozásban, valamint az egyes tartalommal kapcsolatos kényszerintézkedések végrehajtásában. A büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) több segítő, támogató jellegű kötelezettséget telepít az egyes internetes közvetítő szolgáltatások nyújtóira. Az egyszerű hozzáférés-szolgáltatók (internetszolgáltatók) kötelesek közreműködni az olyan leplezett eszközök alkalmazásában, mint az online kommunikáció lehallgatása, vagy az elektronikus adatokhoz való hozzáférés ideiglenes vagy végleges megakadályozása (weblapok blokkolása), a tárhelyszolgáltatók pedig kötelezhetők a tartalmak eltávolítására, de akár a jogsértéssel gyanúsított felhasználó IP-címének a kiadására is. Több olyan online térben megvalósuló bűncselekmény létezik, amelynek a kezelése a szolgáltató bevonása nélkül kivitelezhetetlen volna, az igazságszolgáltatási rendszer tehát képtelen elkerülni, hogy az eljárások során erőteljesen támaszkodjon az említett piaci szereplőkre. E szereplőknek azonban a büntetőeljárásbeli helyzete nem pontosan tisztázott, a Be. ugyanis nem határoz meg külön eljárásjogi pozíciót a közvetítő szolgáltatók számára. A sikeres kooperáció érdekében elengedhetetlen az állami és magánszereplők viszonyrendszerének konkretizálása nemcsak magyar, hanem nemzetközi szinten is. Noha sok olyan eljárási cselekmény van, amelyben a nyomozó hatóságok segítséget várnak piaci szereplőktől, az eljárások során a vállalatok nem mellérendelt pozícióban működnek, hanem alárendelt helyzetben vannak, ahol az állam a szabályozó, a szolgáltató pedig a szabályozott jogalany. Ez a szabályozotti pozíció különösen érdekes azokban az esetekben, amelyekben egyébként a piaci szereplő van erőfölényben, mert például a kezelésében találhatók a bizonyításhoz elengedhetetlen adatok, vagy mert külföldön letelepedett szolgáltató, amelyre a magyar joghatóság nem terjed ki. Nem elhagyható feladata tehát jelen kiadványnak az állam és a nyomozásban közreműködő piaci szereplők közötti viszonyrendszer feltérképezése, hiszen ez kulcsfontosságú eleme a sikeres eljárások lefolytatásának.

A közvetítő szolgáltatóknak nemcsak a szerepe, de a felelőssége sem pontosan rendezett. Az internetes kommunikáció tömegessé válásának hajnalán a jogrendszerek immunitást biztosítottak a közvetítő szolgáltatást nyújtó szolgáltatóknak, vagyis nem kellett viselniük a felelősséget a harmadik személyek által, a szolgáltatásuk felhasználásával elkövetett jogsértésekért. A felelősség e szolgáltatók vonatkozásában

nem kimondottan büntetőjogi felelősségként jelenik meg, hanem jogágakon átívelő általános felelősségként. Ilyen immunitást biztosít az amerikai Communications Decency Act (CDA) 230. §-a, és hasonló korlátozott felelősségi rendszert vezetett be Európában az Európai Parlament és a Tanács a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól szóló 2000/31/EK irányelve (a továbbiakban: Eker. irányelv) is.

A paradigma hátterében az áll, hogy ezek a szolgáltatók valójában csak közvetítő szerepet töltenek be az egyének közötti kommunikációs folyamatban, így nincsenek hatással arra, hogy ki, milyen információt hoz nyilvánosságra, vagy terjeszt. Ez a feltevés azonban napjainkban megdőlni látszik, mivel egyes szolgáltatók (például a közösségimédia-platformok) a passzív szolgáltatói szerepük helyett elkezdtek aktív szerepet vállalni a kommunikációs folyamat alakításában – elég csak a Donald Trump korábbi amerikai elnök és a Twitter tartalommoderálása közötti feszültségre gondolni. Mivel a platformok az információk rendszerezése, szűrése révén maguk is hatással vannak a terjesztés folyamatára, úgy helyes, ha a felelősségük is ehhez a kvázi kurátori szerephez igazodik. Európában és az Egyesült Államokban is egyre gyakrabban jelennek meg a szabályozási diskurzusokban olyan elképzelések, amelyek a platformok fokozott felelősségét, illetve felelősség alóli teljes mentesülésének megszüntetését propagálják.[7]

Adott tehát egy olyan szolgáltatói kör, amely bizonyos esetekben felelőssé tehető a szolgáltatásban megjelenő tartalmakért és az azon keresztül átvitt információért, a büntetőeljárás során mégis a nyomozó hatóság munkáját támogató, partneri szerepet várunk tőlük. Könnyű belátni, hogy előállhat olyan helyzet, amelyben a közvetítő szolgáltató érdeke nem a nyomozó hatóságok érdekeivel, hanem az elkövetők érdekeivel egyezik (például ha bírságtól, szankciótól, üzleti hírének a romlásától tart). A szolgáltatók felelősségi rendszerét tehát úgy szükséges kialakítani, hogy a közvetítő szolgáltató érdeke azonos legyen a nyomozó hatóság érdekével, vagyis hogy ne származhasson kára abból, ha segíti az eljárást. El kell helyeznünk tehát ezeknek a szolgáltatóknak a tartalomközlésekkel kapcsolatos tevékenységét a magyar és nemzetközi jogalkotási térben. A közvetítő szolgáltatók szabályozásban, végrehajtásban és büntetőeljárásban betöltött sokszínű szerepköre nyilvánvalóvá teszi, hogy a tradicionális szabályozási megoldások – ha nincsenek is teljesen kudarcra ítélve – nem lehetnek hatékonyak egy olyan szolgáltatási környezetben, amely jellegét tekintve globálisan nyújtott szolgáltatásokra épül.

7 Lásd Ződi Zsolt elemzését az Eker. irányelv és a CDA 230 válságáról (Ződi 2023: 73–98).

Muszáj szót ejteni azokról a felforgató technológiákról is, amelyeknek néhány éve még nem sok jelentőséget tulajdonítottunk, ma azonban már nagy hatással vannak mind az iparra, mind a nemzetközi jogalkotásra. E körben érdemes említeni a mesterséges intelligenciát, amely ugyanúgy segítheti a bűnelkövetőket, mint a bűncselekmények felderítésében és megakadályozásában részt vevő szerveket. Említést tehetünk az úgynevezett sötét webről is, amelyről bonyolult titkosításra épülő architektúrájánál fogva még ma is nagyon keveset tudunk, ugyanakkor napjainkra az online feketegazdaság egyik fő működési terepévé nőtte ki magát.

Jelen kötet azt tűzte ki célul, hogy ráirányítsa a figyelmet a virtuális tér modern devianciáira, és szisztematikusan, a joggyakorlatból kölcsönzött példák segítségül hívásával áttekintő rendszerezést nyújtson az interneten előforduló jogsértő, valamint a jogellenesség mezsgyéjén egyensúlyozó ártalmas magatartásokról. A kötet centrumában az internetet használó egyén áll, az átlagpolgár, aki gyanútlanul használja az internet infrastruktúráját munkavégzésre, szórakozásra, vagy akár csak a mindennapi életvitelhez szükséges szolgáltatások beszerzése érdekében. Bizonyára többen feltették már maguknak a kérdést, sokan közülük talán egy-egy rosszabb élményen átesve, hogy milyen veszélyeket rejthet magában a virtuális tér. E kötet ezen veszélyek világába kívánja elkalauzolni az olvasót, így a teljességre törekedve kívánja bemutatni mindazokat az ártalmakat, amelyekkel felhasználóként bármikor szembesülhetünk. Az átlagos felhasználó középpontba helyezése némiképp szűkítően hat a kötetben tárgyalt témákra, hiszen a hangsúly azokon a deliktumokon lesz, amelyekkel szinte bárki találkozhat. Azokat a cselekményeket, amelyeknek a tipikus sértettjei az államok vagy jogi személyek – például bankok vagy nagy cégek –, csak értintőlegesen tárgyalja. Kimaradnak tehát az ismertetésből az olyan cselekmények, mint a pénzmosás és a közérdekű adattal visszaélés.

Bár az online térben előforduló ártalmas cselekmények részletes ismertetésével sötét kép tárul az olvasó elé napjaink internetes kultúrájáról, a kötetnek nem célja, hogy bárkit elriasszon e technológia használatától. Éppen ellenkezőleg: jómagam azt vallom, hogy csak akkor tudunk hatékonyan fellépni az internet káros jelenségeivel szemben, ha jól ismerjük azokat, és felkészülten nézünk szembe a modern világ e kihívásával. Noha jelen kiadvány elsősorban joggal foglalkozó célközönség számára íródott, remélhetőleg más tudományterületek informatikai bűnözés iránt érdeklődő művelői is haszonnal tudják majd forgatni.

A kötet szerkezeti felépítése

Jelen kötet összesen nyolc részből áll.

A bevezető gondolatokat követően a II. rész a tárgyalt téma fogalmi alapjainak lefektetésére törekszik, amire több okból is szükség van. Egyrészt, az informatikai bűncselekmények igen speciálisak abból a szempontból, hogy azok helyes értékeléséhez nem elegendő pusztán a jogi szakzsargon ismerete. Ahhoz, hogy kellő mértékben tudjuk érzékeltetni a vizsgált problémák súlyát, illetve be tudjuk mutatni a tárgyalt szabályok hátterét és alkalmazását, elengedhetetlen az alapvető informatikai ismeretek átadása, szükség van bizonyos mértékű informatikai háttérre. Másrészt, a kötet nemzetközi szabályozási trendekre erőteljesen támaszkodó jellege miatt nem hagyhatjuk figyelmen kívül azt a tényt, hogy az informatikai bűnözéssel kapcsolatos fogalmak nem egységesek. Már a kötet tág értelemben vett tárgya, az informatikai bűnözés sem általános tartalommal használt fogalom, a képet pedig színesíti, hogy több hasonló, részben azonos tartalommal használt kifejezést is találunk a jelenség leírására (például számítógépes bűnözés, csúcstechnológiás bűnözés, kiberbűnözés). Ezen okokból mindenképpen szükség van a terminológiai alapok lefektetésére. Harmadrészt, a technológia és a szolgáltatók szabályozása során számtalan olyan fogalom keletkezett, amelyet a magyar jogrendszer is átvett és használ, a szabályozott szolgáltatótípusok bemutatásával így szintén e rész foglalkozik.

A III. rész külön tárgyalja az informatikai bűnözés nemzetközi, európai és amerikai történetét, illusztrálva a fejlődés dinamikáját, és rámutatva arra, hogy milyen gyorsan változnak a digitális technológiák. Mivel a magyar jog mellett az informatikai bűnözéssel több nemzetközi egyezmény és uniós jogforrás foglalkozik, e rész a téma szempontjából releváns nemzetközi instrumentumokat is bemutatja. Mivel a kötetben szereplő technológiai vállalatok nagy részének anyaországa az Egyesült Államok, az amerikai jogi gondolkodás pedig gyakran a szolgáltatók tevékenységén (például a szólásszabadsághoz való viszonyulásukon) is erőteljesen érződik, ez a rész betekintést nyújt az informatikai bűncselekmények angolszász szabályozásába. Az amerikai szabályok mellett jelen rész mutatja be a brit, a francia és a német szabályokat is.

A nemzetközi szabályozási környezet ismertetését követően a kötet rátér a hazai szabályok ismertetésére. A kötet külön részt szentel (IV. rész) az informatikai bűncselekményekkel kapcsolatos anyagi jogi szabályoknak, amely során felhívja a figyelmet arra, hogy a magyar jog szerint bűncselekményeknek minősülő deliktumokat egyes jelentős platformok hogyan kezelik, rámutat azokra a visszásságokra, amelyek a gyakorlatban

felmerülnek. A következő, V. rész tárgyalja azokat a cselekményeket, amelyek a magyar jog alapján nem minősülnek bűncselekménynek, vagy nem egyértelmű, hogy azokat pontosan melyik tényállás alá lehetne rendelni, s ennélfogva jelenleg a büntetőjog határterületén helyezkednek el.

A VI. rész a büntetőeljárás szemszögéből nézve mutatja be a platformok tevékenységeit, rámutatva a platformok büntetőeljárásbeli kötelezettségeire és lehetőségeire, felhívva a figyelmet azokra az ellentmondásokra, amelyek a platformok kötelezettségei és harmadik személyek tevékenységéért viselt felelőssége között fennállnak. Ezt követően esik szó azokról a jogon túli szabályozási megoldásokról, amelyek manapság gyakran jelennek meg az internetes ökoszisztémában (VII. rész). A platformok magánszabályozása, az ön- és társszabályozási rendelkezések nemcsak új szabályok, új eljárások megjelenését jelenti, hanem együtt jár végrehajtási jellegű szerepkörrel is: saját szabályainak megalkotásával és végrehajtásával a platform gyakorlatilag rendészeti szerepet gyakorol saját rendszerén belül. Ez a rész tárgyalja azt is, hogy az államoknak milyen lehetőségeik vannak szabályozni, illetve kontrollálni a platformok magatartását.

Az utolsó, VIII. rész azokat a területeket gyűjti csokorba, ahol elkerülhetetlen a reform. A kötet egyes részeiben leírtak alapján olyan átfogó szabályozási koncepciót kívánok felépíteni, amely a területet szabályozó nemzetközi jogi és uniós normákra figyelemmel jövőálló megoldásokat kínál az informatikai bűncselekményekkel kapcsolatos kihívásokra. E részben a büntető anyagi jogi szabályok között egyrészt olyan cselekmények pönalizálására teszek javaslatot, amelyek jelenleg nem, vagy nem a megfelelő helyen szerepelnek a büntető törvénykönyvben, másrészt bizonyos cselekmények dekriminalizálása mellett érvelek. Ez utóbbiak esetében ugyan van olyan büntető törvénykönyvi tényállás, amelynek az elemei ráillenek a tanúsított magatartásra, az elkövetés körülményei, célzata, illetve a társadalomban megváltozott életviszonyok azonban többé nem indokolják a büntetőjogi szankcióval fenyegetésüket.

A VIII. rész a büntetőeljárás-jogi rendelkezések reformját is tárgyalja. Mivel az informatikai bűncselekmények esetében az elkövetéssel gyakran több ország érintett, a büntetőeljárások egyre inkább a nemzetközi térben folynak. A büntetőeljárások sikere ennek megfelelően nem kizárólag a felderítésben és a nyomozásban részt vevő hatóságok felkészültségén és műszaki hozzáértésén múlik, hanem az országok közötti együttműködés gyorsaságán és hatékonyságán. Ahogyan látni fogjuk ezt a területet, legyen szó akár a virtuális térben keletkezett bizonyítékok megőrzéséről és átadásáról vagy a jogsértő információk eltávolításáról a hálózatról, egyre

inkább szupranacionális szinten szabályozott. A fő kihívást ez esetben tehát nem is a szabályok megalkotása jelenti, hanem azok eredményes integrálása a hazai jogrendszerbe. Végül a záró rész a közvetítő szolgáltatónak minősülő online platformok szabályozásával kapcsolatban is igyekszik hasznos adalékokkal szolgálni a jogalkalmazás számára. Az online platformok mint az információáramlás kapuőrei fontos szerepet töltenek be az informatikai bűncselekmények, főként a tartalomközléssel megvalósított kiberbűncselekmények elleni fellépésben, tevékenységük tehát a jogalkalmazó számára semmiképp sem közömbös.

Vákát oldal

II. Fogalmi alapok

Informatikai alapfogalmak

Az egyetemisták körében városi legenda, hogy a jogászok gyengék matematikából. A műszaki és a humán tudományok alapvetően eltérő készségeket feltételeznek, ezért a műszaki folyamatok leírása a jog nyelvével nem mindig egyszerű feladat. Nehézsége ellenére a jognak mégis neki kell veselkednie ennek a feladatnak, hiszen Szathmáry Zoltán is leírja, hogy „a számítástechnikai bűncselekmények dogmatikáját kizárólag az informatika és a jogi informatika önálló fogalmi alapjaiból kiindulva lehet felépíteni", a büntetőjog tradicionális kategóriáival kell leírni „elektromágneses impulzusokat".[8]

Ha meg akarjuk határozni, mit is jelent pontosan az informatikai bűnözés, nem árt először néhány számítástechnikai alapfogalmat tisztázni. Egyes bűncselekmények minősítése szempontjából ugyanis nem mindegy, mit tekintünk számítógépnek, információs rendszernek, programnak, valamint adatnak.

Az informatika önálló tudományág, amely az információk, adatok rögzítésével, kezelésével, rendszerezésével, továbbításával foglalkozik. Tekintettel arra, hogy a fenti tevékenységek tárgya legtöbbször a számítógép által feldolgozott adat, illetve azok támogatására egyre inkább számítógépet alkalmaznak, az informatika mindinkább az információtudomány, a matematika és az elektronika elegye. Az első fogalomalkotási kísérlet hazánkban a Központi Statisztikai Hivatalhoz (KSH) köthető, amely 1984-ben úgy határozta meg az informatikát, mint az a tudományág, amely „az információ

[8] Szathmáry 2012: 169.

áramlásának különböző módozataival, feldolgozásának és hasznosításának módszereivel, a termelékenységi és hatékonyságra gyakorolt hatásaival, megfigyelési és ellenőrzési célokra való felhasználásával és végezetül a társadalmi-gazdasági fejlődést és társadalmat alakító szerepével foglalkozik".[9] Balogh Zsolt György szerint az informatika „olyan tudomány, amely a számítógépekkel támogatott információs rendszerek strukturális és dinamikus változásaival foglalkozik, annak érdekében, hogy e rendszerek működését optimálissá tegye".[10] Az informatikával rokon fogalom a számítástechnika, amely az automatizált adatfeldolgozás eszközeivel és azok különböző területen való használatával foglalkozó elméleti és alkalmazott műszaki tudomány, tulajdonképpen az informatika egy részterülete.

Maga a számítógép szűkebb értelemben olyan elektronikus információfeldolgozó gép, amely információk (adatok és programok) tárolására alkalmas memóriával rendelkezik, az adatok feldolgozásához programra van szüksége, és saját tevékenységét, működését vezérli, azaz programozott működésű. Ebben az értelmezésben tehát egy okostelefon ugyanúgy számítógép, mint egy laptop vagy asztali PC, nem számítógép viszont a számológép, hiszen nem tudja tárolni a kiszámolt adatokat. A számítógépek körét mindezzel együtt sem lehet taxatív módon meghatározni, hiszen folyamatosan bővül azon eszközök száma, amelyekre a fenti fogalom már teljes mértékben ráillik, és már helytálló őket bevonni a számítógépek körébe. Számítógép nemcsak a PC, a laptop és az okostelefon, hanem a táblagép, az okosóra és az okosszemüveg, de a játékkonzol (Playstation, Xbox vagy a Nintendo Switch) is. Siegler Eszter 1997-ben megjelent tanulmányában[11] a fogalmi meghatározásoknál külföldi példához nyúl, méghozzá Texas állam büntető törvénykönyvének definícióihoz. Eszerint a számítógép olyan elektronikus eszköz, amely valamilyen logikai, számtani vagy memóriafunkciót lát el, elektronikus vagy mágneses impulzusok útján. Számítógép alatt érti továbbá az egymással hírközlés vagy a működés megvalósításának céljával összekapcsolt kettő vagy több számítógépes hálózatot, illetőleg minden, a komputerhez kapcsolódó vagy azzal összekapcsolt input-output, tároló és kommunikációs eszköz, berendezés összességét. Az előbbiekben ismertetett definícióknak ismétlődő eleme a programra, az információra, illetve az adatra való utalás.

Program az adatok rendezett halmaza, olyan kódolt utasítások vagy állítások formájában, amelyek számítógép útján történő végrehajtása adatok továbbítását vagy valamely speciális működés megvalósulását eredményezi. Láthatjuk tehát, hogy végső

[9] Noszkay 1999: 8–9.
[10] Balogh 1998: 21.
[11] Siegler 1997: 736–742.

soron minden esetben az adat fogalmához jutunk, amely olyannyira alapvető eleme az információtechnológiának és az online kommunikációs folyamatoknak, hogy egyesek szerint a 21. században az adat az új olaj.[12]

Az adat: valamilyen számokkal leírható formába öntött jel, információ, ismeret, tény, fogalom vagy utasítás, amely számítógép segítségével továbbítható, tárolható, feldolgozható, rögzíthető. Az adaton belül jól elkülöníthetünk információkat és ismereteket, amelyek az adat nyers fogalmához képest többlettel rendelkeznek. Előbbi alatt olyan adatokat érünk, amelyek valamilyen magatartás-befolyásolási képességgel rendelkező többletet közvetítenek a befogadó számára, utóbbi alatt olyan adatokat értünk, amelyek tapasztalatokból erednek.

A nemzetközi szervezetek viszonylag hamar felismerték a szupranacionális fellépés szükségességét, kiemelve azt a körülményt, amely szerint az információs rendszerek elleni támadás komolyan veszélyezteti az információs társadalom megvalósítását. Az Európai Tanács Miniszteri Bizottsága a 80-as évek vége óta foglalkozik a számítógépes hálózatokkal kapcsolatos bűnözéssel, így az előbbiekben bemutatott informatikai szakkifejezések jogi alkalmazása is korán megkezdődött. A következőkben azt tekintem át, hogy az ismertetett, alapvetően műszaki definíciókat a jog hogyan transzformálta a maga nyelvére. Az R (89) 9. számú ajánlás irányelveket tartalmaz a fogalmak egységesítése érdekében, aminek oka, hogy a belső jogi tényállások megfogalmazásakor olyan terminológiával kell operálnia a jogalkotónak, amely megfelel mind az informatika, mind a jogtudomány elvárásainak. 1992-ben a Gazdasági Együttműködési és Fejlesztési Szervezet (a továbbiakban: OECD) ajánlást fogadott el, amelyet az akkori 24 tagállama adaptált. Ez a dokumentum már meghatároz bizonyos alapfogalmakat, mint az adat, információ, információs rendszer, elismerve, hogy anélkül, hogy azonos fogalmakat azonos vagy közel azonos tartalommal töltenének fel a különböző országok, az együttműködés lehetetlenné válna. A 2001-ben született Cybercrime Egyezmény értelmező rendelkezései között már helyet kapnak konkrét fogalommeghatározások is, mint a „számítástechnikai rendszer" és „számítástechnikai adat" fogalma. A nemzetközi dokumentumok szövegezése speciális értelmezési gondokat vethet fel. Parti Katalin rávilágít bizonyos problémákra, amelyek a fogalmak tagországok nyelvére történő transzformálása során merültek fel. „Az angolban a »*computer system*« és a »*computer data*« szóösszetételben megjelenő computer előtag jelenthet számítógépest vagy számítógéppel kapcsolatost, ami az egyezmény által védett jogtárgyak körét tekintve nem indifferens. Ha ugyanis számítógéppel kapcsolatos adatokról van szó, az magában

12 Bhageshpur 2019.

foglalja nemcsak az adott számítástechnikai rendszerben tárolt adatokat, hanem azokat a külső adathordozókat is, amelyekre az adatok számítástechnikai eszközök útján kerültek, például CD, pendrive."[13] Véleményem szerint ebben a helyzetben a tágabb értelmezés a helyes, hiszen az adathordozókra kerülő adatot is számítógép állította elő, azok megtekintése, felhasználása szintén olyan tevékenység, amely nagyrészt számítógéphez kötött. Ráadásul napjainkban egyre gyakrabban szervezzük ki az adattárolást igen népszerű felhőtárhely-szolgáltatásokba, amelyek esetében a hozzáférés és a feltöltés helye egyértelműen elválik a tárolási helytől.

A fogalmak közül az „adat" definíciójának jogászi értelmezése a legnehezebben megragadható. A Cybercrime Egyezmény szerint „számítástechnikai adat" „az információknak, tényeknek, fogalmaknak minden olyan formában való megjelenése, mely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja".[14] Parti Katalin az egyezmény fogalmi rendszerének tekintetében további kritikaként említi meg azt, hogy az egyezmény kimondatlanul új tulajdoni formának tekinti az adatot azzal, hogy bünteti az adat jogellenes megismerését, abban való károkozást például törléssel. Parti az alábbi módon érvel:

> „[A]z adat, mint dolog alapvetően nem büntetőjogi, hanem polgári jogi kategória, ahol az adat fizikai megjelenését lehetővé tévő adathordozó anyaga minősül dolognak. […] Ugyanez áll a számítógépes programra is, amelynek […] a védelmét a kontinentális jogrendszerek (így a hazai jog is) szintén régtől fogva – a szerzői jogok megsértésének kriminalizálása óta – garantálják. Az írott, egységes fogalmi alapokon nyugvó kontinentális jogrendszerekben a számítástechnikai adathordozó által tárolt, használt vagy előállított adat védelme csak a már meglévő vagyontárgy károsítását, eltulajdonítását, jogtalan használatát stb. szankcionáló tényállások speciális cselekménye lesz, és ezzel külön tényállásban történő kriminalizálása nem szükséges."[15]

Az adat fogalmának és tartalmának problematikáját jól szemlélteti Blutman László, Karsai Krisztina és Katona Tibor közös tanulmánya, amely a lopás törvényi tényállásának egy eleme, a dolog fogalma köré építi fel az „adat" definícióját. A tanulmány azzal a kérdéssel foglalkozik, hogy miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya. 2007-ben született meg az első szabálysértési ügyben hozott végzés, amely jogerősen megállapította, hogy a *wardriving* – azaz olyan vezeték nélküli

[13] Parti 2007: 123–137.
[14] Cybercrime Egyezmény 1. cikk b).
[15] Parti 2007: 123–137.

internethálózatok felkutatása, amelyek jelszóval nem védettek, vagyis amelyekre bárki csatlakozhat – lopásnak minősül. A konkrét tényállásban a terhelt az utcán laptopjával rákapcsolódott a sértett *wireless* internetkapcsolatára, kb. 3,8 megabájtnyi adatforgalmat bonyolítva rajta, és mivel a sértett nem rendelkezett korlátlan letöltéssel, ezért az illegális adatforgalom mennyiségére vetítve 9 forint kára származott. „Az eljáró hatóságok szerint lopással realizálódott a tulajdon elleni szabálysértés, méghozzá akként, hogy az eljárás alá vont személy idegen dolognak minősíthető adatmennyiséget szerzett meg, jogtalan eltulajdonítási szándékkal."[16] A kérdés ebben az esetben az, hogy az adat, illetve adatáramlás idegen dolognak minősülhet-e. A törvényi megfogalmazás szerint dolog csak olyan ingó tárgy lehet, amelynek pénzben kifejezhető forgalmi értéke van. Azonban a régi Btk.[17] 333. §-ában előfordult a dolog fogalmának kiterjesztése a villamos és gazdaságilag hasznosítható más energiára is, rezonálva egyébként a polgári jogi szabályokra, amelyek a dologra vonatkozó szabályok alkalmazását rendelik a pénzre, az értékpapírra és a dolog módjára hasznosítható természeti erőkre.[18] Kérdés tehát, hogy ennek a szabálynak az analógiájára dolognak tekinthető-e az adatfolyam. A szerzők erre a kérdésre nemleges választ adnak, egyrészt azért, mert az adatfolyam nem energia, másrészt a *nullum crimen sine lege* elvet alapul véve az energia fogalmát csakis szűken lehetne értelmezni, a kiterjesztő értelmezés olyan analógia, amely a büntetőjogban nem megengedett. A szerzők utalnak arra, hogy kézzelfogható igény lenne az ilyen cselekmények elítélendő voltának elismerésére, hiszen „lényegében élősködő jellegű magatartás, amelyben a mást ellenszolgáltatás fejében illető javakat, s pénzben kifejezett értékkel bíró lehetőségeket harmadik személy használja ki, veszi igénybe úgy, hogy ezért semmiféle ellentételezést nem nyújt".[19]

A hazai jogirodalom és ezen belül a büntetőjog-irodalom is az adat többféle fogalmát ismeri, így éles különbséget tesz az adatvédelem és adatbiztonság között.

Szathmáry Zoltán az adatbiztonság szempontjából vizsgálja az „adat" fogalmát, amely a következőképp alakul: „Adatbiztonság vonatkozásában minden testet öltött információt, kódolt közleményt adatnak tekintünk, az adat az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája."[20] Támadás alapvetően az információt hordozó adatot érheti, amelyhez gazdasági és személyes értékek is fűződhetnek. „Az adat megvédése érdekében minden esetben

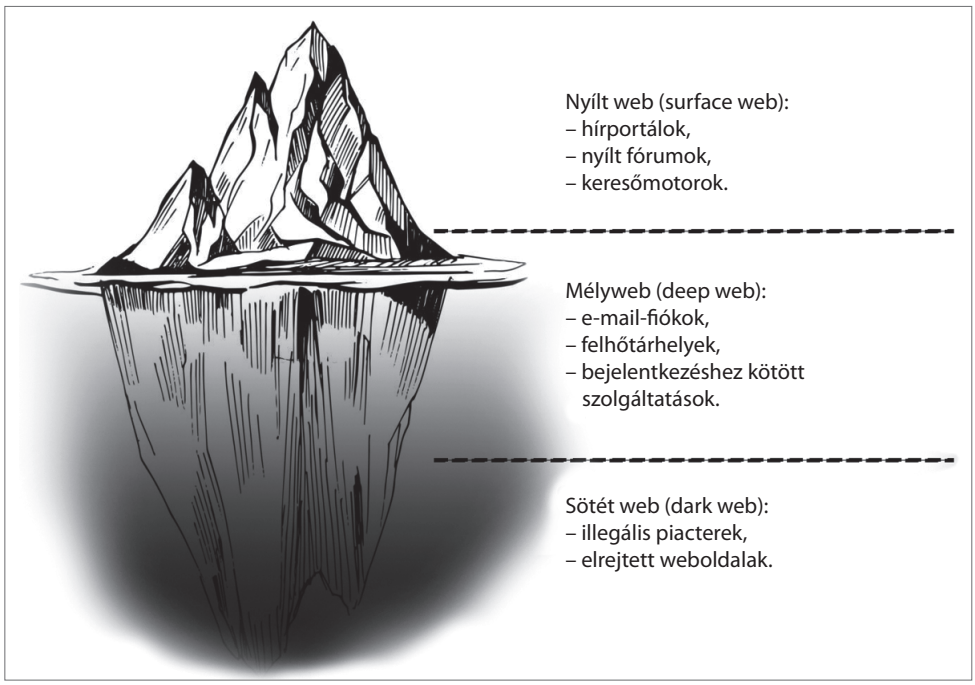
16 Blutman–Karsai–Katona 2008: 6.
17 1978. évi IV. törvény a Büntető Törvénykönyvről.
18 Lásd Ptk. 5:14 [A dolog].
19 Blutman–Karsai–Katona 2008: 15.
20 Szathmáry 2011: 162.

céltudatos, tervszerű emberi magatartás szükséges, amely a kívánt emberi magatartásokat előírások formájában rögzíti."[21] Ebben az értelemben a biztonság az információs és informatikai rendszerekben olyan előírások betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességet erősítik. Szathmáry ezt követően azt a környezetet jellemzi, ahol az adat elhelyezkedik. Az adatra irányuló támadások ugyanis rendszerint nem közvetlenül, hanem az adatot körülvevő rendszerelemeken keresztül történnek, ilyen például a hardverrendszer, szoftver, hálózati rendszerek, adathordozók. Ez alapján „számítástechnikai rendszer" minden olyan önálló eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelyek, illetőleg amelyeknek egy vagy több eleme program végrehajtásával adatok automatikus feldolgozását biztosítja.

Az internet architektúrája és rétegei

Az internet topológiáját egy jéghegyhez szokás hasonlítani.[22] A jéghegy csúcsa a nyílt internet, vagy felszíni web *(surface web),* ahol a tartalmak és weboldalak találhatók, amelyeket az ismert nagy keresőmotorok (Google, Bing) indexelni tudnak, azaz bárki számára hozzáférhetők. A nyílt interneten található információk azonban csak a töredékét képezik az internet adattartalmának. Az internet topológiájának második szintje a mélyweb *(deep web),* ahol a nem indexált oldalak találhatók. Ezeket általában nem találjuk meg egyszerű kereséssel, a hozzáférés pedig korlátozott, regisztrációt és jelszót igényel. Ilyenek az online adatbázisok, az e-mail-fiókok, a közösségi platformokon létrehozott felhasználói fiókok, a fizetési falak mögött lévő szolgáltatások, mint az online videotékák, de a munkahelyi intranetek is. Az online infrastruktúra legalsó rétege – egyes értelmezések szerint a mélyweb egy külön része – a sötét web *(dark web),* amelyen keresztül szintén nem indexált tartalmak érhetők el, a hozzáférés további feltétele pedig speciális anonimizáló webböngésző, amely a kapcsolatot proxyszerverek hálózatán irányítja át. A titkosítás miatt a sötét web felhasználói nehezen lenyomozhatók, ami a *dark web*et az online feketegazdaság fő platformjává teszi. A *dark web*hez való hozzáférést lehetővé tévő böngészők, például a TOR, valójában nem illegális tevékenységek megkönnyítésére jöttek létre, hanem az amerikai haditengerészet fejlesztette annak érdekében, hogy a külföldi műveletekben részt vevő katonák anonim módon tudjanak kommunikálni.

[21] Szathmáry 2011: 162.
[22] Nelson 2017.



1. ábra: *Az internet topológiája*
Forrás: A szerző saját szerkesztése

Az ártalmas, illetve az illegális tartalmak elleni fellépés során alkalmazható megoldások akkor lehetnek hatékonyak, ha képesek igazodni a terjesztési mód sajátosságaihoz. A nyílt weben terjesztett tartalmak esetében igénybe vehetők a hagyományos eszközök, a büntetőjogi normát sértő tartalmak esetében például az elkövető földrajzi helyének beazonosítása és kötelezése a tartalom eltávolítására, ezek sikertelensége esetén pedig a tárhelyszolgáltató, illetve a hozzáférés-szolgáltató kötelezése az elektronikus adat ideiglenes vagy végleges hozzáférhetetlenné tételére (illetve nemzetközi környezetben az ezzel egyenértékű intézkedés megtételére). Egyéb, nem büntetőjogi normát sértő esetekben pedig rendelkezésre áll a médiajog vagy a polgári jog eszközrendszere. A sötét weben elhelyezett tartalmak esetében ellenben már az elkövető kilétének felderítése is komoly nehézségekbe ütközik, ahogyan az sem ismert, hogy ki lenne az elektronikus adat ideiglenes eltávolításának kötelezettje. Az internetszolgáltatókat ezekben az esetekben lehetetlen bevonni a hozzáférés megakadályozásába, hiszen a proxyszerverek láncolatának igénybevétele miatt a szóban forgó weboldalak a szolgáltató számára csak aránytalanul nagy ráfordítás esetén válnak láthatóvá és blokkolhatóvá.

Az informatikai bűnözéssel kapcsolatos fogalmak – bűncselekmények számítógépes környezetben

Ez idáig sem a gyakorlat, sem a jogalkotás nem dolgozott ki egységes terminológiát az informatikai bűncselekmény fogalmának meghatározására, sőt még a témával foglalkozó egyetemi jegyzet is arról tesz említést, hogy nem alakult ki általánosan elfogadott fogalomrendszer e bűncselekményi kör leírására.[23] A szakirodalomban számtalan fogalom kering az információtechnikai elemet tartalmazó bűncselekményekkel kapcsolatban, a legtöbb szerző azonban nem azonos tartalommal használja az egyes kifejezéseket. Noha a témával hatalmas mennyiségű külföldi és egyre bővülő magyar szakirodalom is foglalkozik, az informatikai bűncselekményekkel kapcsolatban felmerülő fogalmak a mai napig meglehetősen tisztázatlanok, az egyes kifejezések elhatárolása pedig nem mutat egységes képet. A terminológiai káosz mellett az is problémát jelent, hogy az információtechnológiai elemet tartalmazó cselekmények köre gyorsabban változik, mint ahogyan arra a jogalkalmazás reagálni tudna: egyes bűncselekmények egyszerűen elavulnak, mások elkövetése az új technikák elérhetővé válása miatt átalakul. E részben a következő terminusok jelentését és egymáshoz való viszonyát tárgyalom: „számítógépes bűncselekmény", „számítógéppel kapcsolatos bűncselekmény", „informatikai bűncselekmény", „kiberbűncselekmény", „digitális bűncselekmény", „e-bűncselekmény", „csúcstechnológiás bűncselekmény".

A számítógépes bűncselekmény fogalma (computer crime)

Az egyik legkorábban megjelent fogalom az információtechnológiai bűncselekmények meghatározására a számítógépes bűncselekmény, azaz a *computer crime* fogalma. A számítógépes bűncselekmény egy „olyan gyűjtőkategória, amely több bűnözési ág területét érinti".[24] Parker, Nycum és Aura 1973-as meghatározása szerint „számítógépes bűncselekmény minden olyan törvénysértő cselekedet, amelynek elkövetéséhez, nyomozásához és bírósági vizsgálatához elengedhetetlen a számítástechnika speciális ismerete".[25] A meghatározás nagyon széles értelemben használja a számítógépes bűncselekmény fogalmát, és nemcsak az elkövetés mozzanatát, hanem a nyomozást és a bírósági vizsgálatot is bevonja az értékelendő szempontok közé. Napjainkban

[23] Simon 2012: 9.
[24] Balogh 1998: 259.
[25] Parker–Nycum–Aura 1973: 12.

ez a meghatározás már annyira általános, hogy relevanciáját veszítette, hiszen szinte nincsen olyan büntetőeljárás, amelyben nem jelenik meg semmilyen információtechnológiai elem. Példának okáért említsük azt az esetet, amikor a nyomozó hatóság egy autólopás esetén az utcán elhelyezett kamera felvételeit használja bizonyítékként, vagy számítógépes nyilvántartásban néz utána az ellopott autó adatainak. Noha a nyomozó hatóság nagymértékben támaszkodik a technológia vívmányaira, mégsem lenne helyes magát a deliktumot informatikai bűncselekményként kezelni.

A 2000-es években ennél szűkebb definiálási kísérletek jelentek meg a szakirodalomban, amelyek az információs rendszer tárgy- és eszközfunkcióját – illetve ezek valamelyikét – tették meg a számítógépes bűncselekmények fő ismérvének. A magyar szakirodalomban Szabó Imre úgy határozza meg a számítástechnikai bűncselekményeket, mint „azok a deliktumok, melyek egy számítógépes rendszerrel vagy számítástechnikai adattal kapcsolatba hozhatók, akár úgy, hogy az elkövetés eszközeként jelennek meg, vagy pedig a bűncselekmény elkövetési tárgyát képezik”.[26] Hasonló álláspontot képvisel az idegen nyelvű szakirodalomban Marjie T. Britz, aki a számítógépes bűncselekményeket általános fogalomként használja, és minden olyan bűncselekményt idesorol, amelyet számítógép használatával követtek el.[27] A számítógépes bűncselekmény fogalmát kiterjesztően értelmezi, így ideérti azokat a cselekményeket, ahol az információs rendszer vagy adat az elkövetés tárgya, és azokat is, amelyekben az információs rendszer az elkövetés eszköze. Hasonlóan értelmezi a számítógépes bűncselekmény fogalmát Eoghan Casey,[28] aki egzakt definícióval nem szolgál, de könyvében jelzi, hogy a számítógépes bűncselekmény kategória nem vonatkoztatható minden olyan cselekményre, amelyben információtechnológiai elem kap szerepet, kizárólag azokra, amelyek szorosabb kapcsolatot mutatnak a számítógépes környezettel, tehát amelyekben a számítógép a bűncselekmény eszköze vagy tárgya.

A legszorosabb értelmezés szerint ellenben csak azok a bűncselekmények minősülnek számítógépes bűncselekményeknek, amelyek a számítógépes rendszer, illetve adatok ellen irányulnak. Erre az álláspontra helyezkedett például Fázsi László és Fázsi László Milán, akik szerint a számítógépes bűncselekmények azok a cselekmények, amelyek kifejezetten a számítógépes rendszer, a programok, illetőleg a számítógépes adatok ellen irányulnak, vagyis ahol ezek az eszközök elkövetési tárgyak.[29]

[26] Szabó 2008: 547.
[27] Britz 2013: 6.
[28] Casey 2012: 37.
[29] Fázsi–Fázsi 2009: 3–11.

A fenti terminológiai káoszból adódóan a számítógépes bűncselekmény fogalom önálló alkalmazása félreértésekre adhat okot, ezért indokolt azt valamilyen egyértelműsítő jelző kíséretében használni. A szoros értelemben vett számítógépes bűncselekményeket – tehát ahol a számítógépes rendszer az elkövetési tárgy – a gyakorlatban szokás tisztán számítógépes bűncselekményeknek, szűk értelemben vett számítógépes bűncselekményeknek *(cybercrime im engeren Sinne)*[30] vagy számítógépfüggő bűncselekményeknek *(cyber-dependent crimes)*[31] is nevezni, ami arra utal, hogy ezeknek a cselekményeknek az offline formában történő megvalósítása kizárt, azok csak információtechnológiai környezetben értelmezhetők. Ebbe a csoportba tartozik a jogellenes belépés, az információs rendszer védelmét biztosító technikai intézkedés kijátszása, illetve az információs rendszer és adatok elleni bűncselekmények.

Számítógéppel kapcsolatos bűncselekmény (computer related crime)

A számítógéppel kapcsolatos bűcselekmények fogalmát kétféleképpen szokták meghatározni. A tágabb értelmezéshez a Britz által meghatározott fogalmat vesszük irányadónak,[32] amely szerint számítógéppel kapcsolatos minden olyan bűncselekmény, amelyben a számítógép bármilyen módon, akár közvetetten is, jelen volt. A tág értelmezés szerinti számítógéppel kapcsolatos bűncselekményeket ezért szokás számítógép által lehetővé tett bűncselekményeknek *(cyber-enabled crimes),*[33] illetve tág értelemben vett számítógépes bűncselekményeknek *(cybercrime im weiteren Sinne)*[34] is nevezni. Az elkövetésben betöltött funkció alapján három nagyobb csoportra bonthatjuk a számítógéppel kapcsolatos bűncselekményeket: az első, amelyben a technológia a cselekmény elkövetési tárgya, a második, amelyben az elkövetés eszköze, a harmadik pedig az az eset, amelyben a technológia jelen van ugyan, de csak mellékes elemként, amely legfeljebb elektronikus bizonyítékok forrása lehet. Jó példa erre az, amikor emberrablásnál az elkövetők e-mailben követelnek váltságdíjat. Látjuk, hogy itt magából a cselekményből, vagyis a személyi szabadság megsértéséből csak nagyon hosszú logikai láncon keresztül lehet arra a következtetésre jutni, hogy számítógépes bűncselekmény történt. A számítógéppel kapcsolatos bűncselekmény kategóriáját

30 Bundeskriminalamt [é. n.].
31 The Crown Prosecution Service 2019.
32 Britz 2013: 6.
33 The Crown Prosecution Service 2019.
34 Bundeskriminalamt [é. n.].

Britzcel azonosan határozza meg Casey is.[35] A számítógéppel kapcsolatos bűncselekmények nem kötődnek kizárólagosan a virtuális térhez, ugyanúgy elkövethetők a való/fizikai világban is. Az idetartozó cselekmények rendkívül színes képet mutatnak – lehetnek tartalommal kapcsolatos bűncselekmények, mint a szerzőijog-sértések vagy a gyermekpornográfia, illetve egy adott személy vagy csoport sérelmére elkövetett cselekmények (gyűlöletkeltés, zaklatás, rágalmazás, becsületsértés).

A teljesség kedvéért szólni kell arról is, hogy ennél létezik egy szűkebb meghatározás, amely csak azokat a cselekményeket sorolja a számítógéppel kapcsolatos bűncselekmények közé, ahol a számítógép az elkövetés eszköze, vagyis ahol a számítógép nem feltétele az elkövetésnek, hanem egy azt megkönnyítő eszköz, illetve közvetítő csatorna. A magyar jogirodalom jellemzően e szűkebb értelmezés pártján áll, Siegler Eszter ugyan megkülönbözteti a számítógépes bűncselekmények és a számítógéppel kapcsolatos bűncselekmények fogalmait, de jóval szűkebben értelmezi őket, mint külföldi kollégái.[36] Siegler számítógéppel kapcsolatos bűncselekmények alatt kizárólag azokat a cselekményeket érti, amelyeknél a számítógép az elkövetés eszköze vagy elkövetési tárgy, a számítógépes bűncselekmény fogalmát pedig szűkítően, kizárólag azokra a deliktumokra alkalmazza, amelyek kifejezetten számítógépes rendszer és adatok ellen irányulnak (tehát ahol a számítógépes rendszer elkövetési tárgyként van jelen). Jelen kötetben a számítógéppel kapcsolatos bűncselekményeket tekintem szélesebb kategóriának, amelybe beletartoznak egyrészt a szűk értelemben vett számítógépes bűncselekmények, másrészt a számítógép által lehetővé tett bűncselekmények (lásd 2. ábra).

Informatikai bűncselekmény, információs rendszerrel kapcsolatos bűncselekmény

Az informatikai bűncselekmény ugyan nem új keletű fogalom, Nagy Zoltán András már 1991-ben használta,[37] Magyarországon mégis csak akkor terjedt el, amikor a jelenleg is hatályos Btk.[38] lecserélte a számítógép fogalmát – nagyon helyesen – az információs rendszerére. A számítógépes bűncselekmény fogalma kikopott a szóhasználatból, átadva helyét az informatikai bűncselekmény, információs rendszerrel kapcsolatos bűncselekmény, illetve a későbbiekben tárgyalt kiberbűncselekmény fogalmaknak.

35 Casey 2012: 37.
36 Siegler 1997: 736–742.
37 Nagy 1991: 21–26.
38 2012. évi C. törvény a Büntető Törvénykönyvről.

A Btk. megújult fogalomhasználatának hátterében az áll, hogy a köznyelvi számítógép-fogalom az eszközöknek viszonylag szűk körére, a személyi számítógépekre értendő, ugyanakkor a tárgyalt bűncselekmények tárgyai, illetve eszközei lehetnek az olyan információtechnológiai eszközök is, mint a táblagépek, az okostelefonok, a nyomtatók vagy az adattovábbítást és a kapcsolatfelvételt biztosító műszaki berendezések (például a hálózati forgalmat irányító routerek). Az információs rendszer kifejezés magában foglal minden, az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezést vagy az egymással kapcsolatban lévő ilyen berendezések összességét, tehát a végpontokat és a hálózatot egyaránt. A Btk. az információs rendszer fogalmat a korábbi számítástechnikai rendszer fogalommal azonos tartalommal definiálja, ezért a számítógéppel és az információs rendszerrel kapcsolatos bűncselekmény fogalmak lényegében szinonimaként értelmezhetők, jelen kötet ezért felváltva alkalmazza őket.

Pusztán utalásszinten említendő, hogy az informatika és a számítástechnika kifejezések jelentéstartalma nem teljesen azonos, ez a különbség azonban jogi szempontból elhanyagolható.

Kiberbűncselekmény (cybercrime)

Napjainkban igen divatos, mégis nehézkesen értelmezhető kifejezés a kiberbűncselekmény. Sokan az informatikai bűncselekmény, illetve a számítógépes bűncselekmény fogalmával szinonim értelemben használják a fogalmat, amely az angolszász *cybercrime* kifejezés nyomán honosodott meg a magyar nyelvben. A másik értelmezés szerint azonban a kiberbűncselekmény kizárólag azokra a számítógépes bűncselekményekre vonatkozik, amelyekben valamilyen módon megjelenik az információs rendszereket összekötő hálózat (például az internet). Britz a kifejezést azokra a deliktumokra használja, amelyeket a hálózatban az internet felhasználásával követtek el. Röviden Casey is utal arra, hogy a kiberbűncselekmény kategória a számítógépes hálózatot érintő cselekményekre értendő.[39] Susan W. Brenner ugyan nem nevesíti közvetlenül a hálózatot mint az elkövetés eszközét, a kiberbűncselekmény lényegének meghatározásakor kiemeli, hogy ezeknél a cselekményeknél a kibertér (a számítógépeket összekötő virtuális közeg) válik a cselekmény elkövetésének eszközévé vagy tárgyává.[40] A Cybercrime Egyezmény is a *cybercrime* kifejezést használja, a fogalom normajellegű

[39] Casey 2012: 37.
[40] Brenner 2010: 39.

definíciójának megalkotásával azonban adós maradt. Noha az egyezmény preambuluma több esetben kiemeli a számítógépes hálózatok szerepét a modern bűnözésben, az egyezmény által felsorolt bűncselekmények elkövetése – bár jellemzően valóban hálózaton keresztül valósul meg – nem elképzelhetetlen offline környezetben sem, így kijelenthetjük, hogy ezen a területen is szükség lenne a fogalmak tisztázására és esetleges újragondolására. A fogalom tisztázatlanságának problémájára remekül rávilágít az Egyesült Nemzetek Szervezete (ENSZ) 2013-ban készült átfogó tanulmánya,[41] amelynek hátteréül egy kiterjedt kérdőíves kutatás szolgált. A tanulmány szerint a felmérésben részt vevő országok kevesebb mint 5%-a használja a *cybercrime* kifejezést, inkább a számítógépes bűncselekmény, az elektronikus bűncselekmény és a csúcstechnológiás bűncselekmény fogalmak elterjedtebbek. A fogalmat még azok az országok sem határozták meg, amelyek egyébként jogszabályi szinten is alkalmazzák a kiberbűncselekmény kifejezést, a tanulmány szerint az elemzett jogforrások definiálás helyett csupán utaltak a jogszabályban meghatározott bűncselekmények körére.

Digitális bűncselekmény, e-bűncselekmény és csúcstechnológiás bűncselekmény (digital crime, e-crime, high-tech crime)

Számos kevésbé elterjedt fogalom is létezik, amelyekkel a gyakorlat, illetve a szakirodalom az információtechnológiai elemet tartalmazó bűncselekményeket vagy azok egyes elemeit írja le. Ezek a fogalmak a digitális bűncselekmény, az e-bűncselekmény, illetve a csúcstechnológiás bűncselekmény.

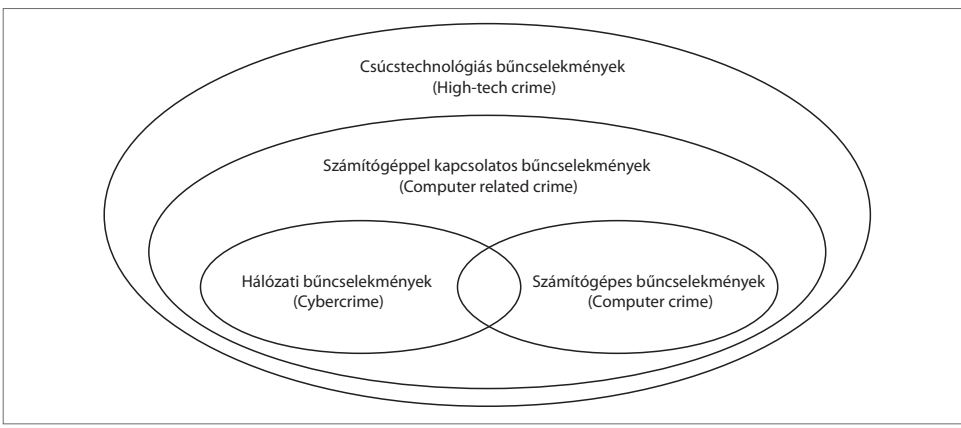
Britz a digitális bűncselekmény fogalmát alkalmazza azokra a cselekményekre, amelyek az elektronikusan tárolt adatokhoz kapcsolódnak, tehát amelyekben az adatokhoz való jogosulatlan hozzáférés, adatok jogosulatlan terjesztése, megváltoztatása, törlése történik, akár hálózaton keresztül, akár offline formában. Ennél tágabb értelemben, de ugyancsak a digitális bűncselekmény fogalmat használja Ambrus István. Ambrus a digitális bűncselekmény fogalma alatt az összes digitális eszköz és technológia révén, illetve azok ellen elkövethető deliktumot érti. Ez a fogalom a cselekmények igen széles körét lefedi, lehetőséget biztosítva arra, hogy olyan újfajta büntetőjogilag releváns magatartások is a vizsgálat tárgyai lehessenek, mint az önvezető autókkal, elektromos rollerekkel vagy akár a drónokkal megvalósított jogsértések.[42] Az *e-crime*

41 UNODC 2013.
42 Ambrus 2021: 81.

fogalommal főleg az Egyesült Királyságban találkozhatunk, ahol a rendőrfőnökök egyesületének (Association of Chief Police Officers) *e-crime*-stratégiája úgy definiálja, mint a hálózatba kötött számítógépek vagy az internet használata bűncselekmények elkövetésére vagy a bűncselekmény elkövetésének megkönnyítésére.[43] Az *e-crime* tehát lényegében a kiberbűncselekménnyel azonos fogalom.

Jóval nehezebb dolgunk van a csúcstechnológiás bűncselekmények *(high-tech crime)* fogalmának definiálásával, erre ugyanis nem találhatunk meghatározást a szakirodalomban. Azt, hogy mégis bevett és használatban lévő kifejezésről van szó, mutatja, hogy az Europol honlapja is külön kategóriaként nevesíti ezeket a cselekményeket,[44] illetve a Budapesti Rendőr-főkapitányság szervezetén belül sokáig működött az úgynevezett Pénzhamisítási és Csúcstechnológiai Bűnözés Elleni Osztály. (A szervezeti egység elnevezése azóta Kiberbűnözés Elleni Osztályra módosult.[45]) A csúcstechnológiás bűncselekmény kategóriába tartozik minden olyan offline vagy online környezetben elkövetett cselekmény, amelyben az elkövetés eszköze vagy az elkövetés tárgya a tudomány mai állása szerint a technológia élvonalába tartozik. Ez tehát a legtágabb fogalom, tartalma viszont meglehetősen relatív, hiszen a tudomány és a technológia folyamatos fejlődésben, változásban van, időszakosan változik, mit tekintünk csúcstechnológiának.

Az előbbiekben részletesen ismertetett fogalmak egymáshoz való viszonyát a 2. ábra szerint tudjuk a legjobban érzékeltetni.



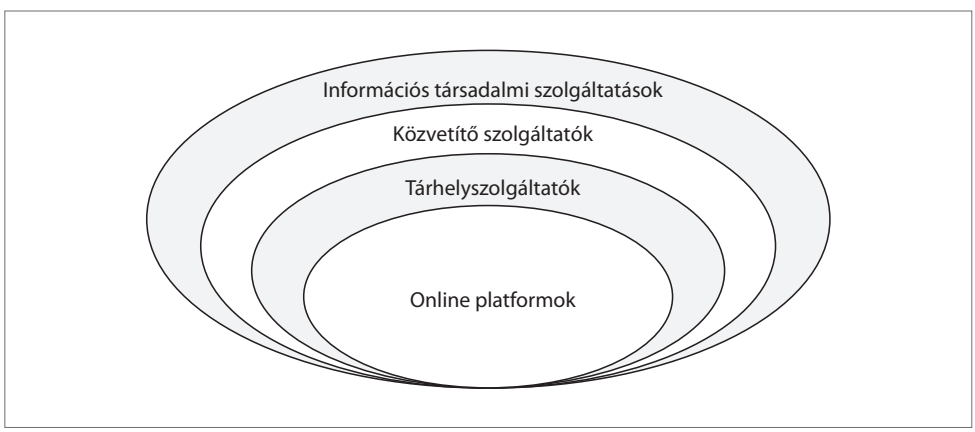
2. ábra: *Az információtechnológiai környezetben elkövetett bűncselekmények*

Forrás: Sorbán 2018: 374.

43 Home Affairs Committee 2013.
44 Europol 2023.
45 Budapesti Rendőr-főkapitányság 2023.

Az online tér szereplői

Az online térben számos piaci szereplő és magánszemély mozog. Talán ma már nem túlzás azt állítani, hogy az online tér leképezi környezetünket, sőt hozzátesz, hiszen képes bizonyos jelenségek hatását felnagyítani, és vannak olyan szolgáltatások, amelyek csak az online világban értelmezhetők (például a közösségimédia-platformok). Az internet világának vannak olyan szereplői, amelyek létrejötte az internet infrastruktúrájának sajátosságai miatt következhetett be. Ezek azok a szolgáltatások, amelyek biztosítják az internetnek mint hálózatos erőforrásnak a zavartalan működését, amelyek segítik a felhasználót az online térben történő eligazodásban, vagy amelyek csak virtuális közegben értelmezhetők (például a videómegosztóplatform-szolgáltatások). Sokféleségük miatt ezeket a szolgáltatásokat nehezen lehetne úgy csoportosítani, hogy ne legyenek átfedések az egyes halmazok között, ennek ellenére a csoportképzést nem tekintem hasztalannak. Az eltérő szolgáltatói funkciókból ugyanis az következik, hogy egy uniformizált szabályozás, amely mindenfajta online szolgáltatást egy kalap alá vesz, szükségszerűen keretjellegű és túlegyszerűsítő, vagyis nem alkalmas arra, hogy megfelelően kezelje az egyes szolgáltatások különbözőségéből eredő problémás helyzeteket, sem arra, hogy a sokféleségükből adódó lehetőségeket kiaknázza. Ezek a szereplők mind különbözőképpen gyakorolnak hatást az internet architektúrájára, illetve az abban zajló kommunikációs folyamatokra, ezért a piaci értéklánc eltérő pontjain eltérőképpen képesek beavatkozni, s így hézagmentes védelmet biztosítani a felhasználóknak. Az online tér szolgáltatóinak egymáshoz való viszonyát a 3. ábra szemléleti.



3. ábra: *Az információs társadalommal összefüggő szolgáltatások csoportosítása*
Forrás: A szerző saját szerkesztése

Az online tér szereplőire az Európai Unióban használt ernyőfogalom az információs társadalommal összefüggő szolgáltatás fogalma. Amint azt a későbbi részekben látni fogjuk, az egyes szolgáltatástípusok szabályozásánál az uniós normák újra és újra visszautalnak az információs társadalommal összefüggő szolgáltatások meghatározására, úgy indokolt tehát, hogy a jelen kötet is ezt a fogalmat tekintse origónak.

Információs társadalommal összefüggő szolgáltatás

Az online tér szolgáltatói azok a piaci szereplők, amelyek az Eker. irányelv által szabályozott információs társadalommal összefüggő szolgáltatást nyújtanak. Az információs társadalom szolgáltatásának fogalmát a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról szóló 2015/1535. irányelv határozza meg,[46] amely idesorol minden, általában térítés ellenében, távolról, elektronikus úton, a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatást. Ez a definíció elég tágan jelöli ki a kereteket, így az online tér legtöbb szolgáltatását magában foglalja.

Bár a hivatkozott irányelv sem zárt, sem nyílt taxációval nem határozza meg, hogy milyen szolgáltatások minősülhetnek az információs társadalom szolgáltatásainak, az EUB ítélkezési gyakorlata nagymértékben hozzájárult az e körbe tartozó szolgáltatások tipizálásához. Rendszerint az információs társadalom szolgáltatásainak minősülnek a közvetítő szolgáltatások, így a szálláshely-közvetítő szolgáltatások, illetve a személyszállítást közvetítő szolgáltatások.

Az információs társadalommal összefüggő szolgáltatás irányelvi definíciójából az is következik, hogy vannak olyan szolgáltatások, amelyek akkor sem tekinthetők az információs társadalommal összefüggő szolgáltatásnak, ha a szolgáltatásnyújtás online elemet tartalmaz. Az irányelv I. melléklete tájékoztató jelleggel felsorolja azokat a szolgáltatásokat, amelyek nem minősülnek információs társadalommal összefüggő szolgáltatásoknak. Ilyenek a nem távolról, azaz az ügyfél fizikai jelenlétében elektronikus eszközökkel nyújtott szolgáltatások, mint az orvosi diagnosztikai vizsgálatok, egy katalógus megtekintése egy üzlethelyiségben, repülőjegy-foglalás az utazási

[46] Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról.

irodában, valamint a játékteremben rendelkezésre bocsátott elektronikus játékok.[47] A lista korántsem teljes, Graeme B. Dinwoodie kiemeli, hogy például az internetkávézók sem minősülnek információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatóknak, mivel a szolgáltatásnyújtás nem távolról, hanem a felek közvetlen jelenlétével történik.[48]

Az előbbiekben ismertetett fogalom egyik kulcseleme, hogy a szolgáltatás nyújtása, vagyis az adatok továbbítása a felhasználó egyedi kérelmére történik. A hagyományos televíziós szolgáltatás, a rádiós műsorszolgáltatás és a teletext ennél fogva szintén nem minősül az információs társadalom szolgáltatásának,[49] akkor sem, ha azt a felhasználó az interneten keresztül veszi igénybe, hiszen a televízióban a szolgáltató meghatározott műsorrend alapján, a néző egyéni kezdeményezésétől függetlenül sugározza a tartalmakat.

A nem kereskedelmi jelleggel nyújtott szolgáltatások, mint a magánweboldalak szintén nem tartoznak az információs társadalommal összefüggő szolgáltatások közé.

Az információs társadalom egyes szolgáltatásait az Eker. irányelv és más EU-s normák külön nevesítik. Az Eker. irányelv a közvetítő szolgáltatókra tartalmaz részletes szabályokat, az AVMS irányelv[50] a lekérhető audiovizuális médiaszolgáltatások és a videómegosztóplatform-szolgáltatások részletszabályait rendezi, a digitális szolgáltatásokról szóló rendelet (a továbbiakban: DSA)[51] pedig az online platformokat szabályozza. A kötet az információs társadalommal összefüggő szolgáltatások közül ezekkel a közvetítő szolgáltatókkal foglalkozik részletesebben, abból az okból, hogy ezek azok a szereplők, amelyek az online szolgáltatási tér frontvonalában működnek, a tartalomközléssel megvalósított bűncselekmények pedig többnyire ezeken a platformokon történnek.

47 Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról I. melléklet 1. pont.

48 Dinwoodie 2017: 6.

49 Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról I. melléklet 3. pont.

50 Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv).

51 Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról.

Az elektronikusan nyújtott pénzügyi szolgáltatások az információs társadalom szolgáltatásaiként szintén az Eker. irányelv hatálya alá tartoznak, az irányelv hozzájárul az online módon nyújtott szolgáltatások pénzügyi kereteinek megteremtéséhez.[52] A 2015/1535. irányelv[53] az információs társadalom szolgáltatásaiként nyújtott pénzügyi szolgáltatásoknak az alábbi típusait különbözteti meg:

- befektetési szolgáltatások,
- biztosítási és viszontbiztosítási műveletek,
- banki szolgáltatások,
- nyugdíjalapokkal kapcsolatos műveletek,
- határidős vagy opciós ügyletekkel kapcsolatos szolgáltatások.

A pénzügyi szolgáltatásokkal kapcsolatba hozható deliktumok jelentős hányadát képezik a bank- és pénzügyi rendszert érintő informatikai bűncselekményeknek. Ahogyan a bevezető részben már említettem, ezekkel a cselekményekkel nem foglalkozom. Ennek egyik oka az, hogy a pénzügyi szolgáltatók, annak ellenére, hogy a tágabban értelmezett információs társadalommal összefüggő szolgáltatások nyújtóinak csoportjába sorolhatók, nem közvetítő szolgáltatók, így az ő tevékenységük az informatikai bűncselekmények vonatkozásában már kívül esik a kötet keretein. A másik ok az, hogy a pénzügyi rendszerre számos speciális szabály vonatkozik mind uniós, mind nemzeti szinten, ezért a szektort érintő bűnözés ismertetése már egy önálló kötet témája lehetne. Ahol az átlagos internethasználó találkozhat pénzügyi jellegű bűncselekményekkel, ott ezekről röviden említést teszek.

A közvetítő szolgáltatók (intermediary service providers)

A közvetítő szolgáltatóknak fontos szerep jut az internetes adatáramlásban, mivel ők az online térnek azok a szereplői, amelyek lényegében összekapcsolják a keresletet és a kínálatot, a fogyasztót a szolgáltatóval. Az OECD úgy határozza meg az internetes közvetítő szolgáltatókat, mint azok a szolgáltatók, amelyek harmadik személyek által

[52] Eker. irányelv (27) preambulumbekezdés.

[53] Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról.

biztosított tartalmakhoz, termékekhez és szolgáltatásokhoz hozzáférést biztosítanak, azokat tárolják, továbbítják és indexálják, továbbá azok a szolgáltatók, amelyek internetalapú szolgáltatást kínálnak harmadik személyeknek.[54]

Az EUB több esetben is vizsgálta azt, hogy mely szolgáltatók minősíthetők információs társadalommal összefüggő szolgáltatást nyújtó közvetítő szolgáltatónak. A fentiekben ismertetett négy feltétel (díjazás ellenében, távolról, az igénybe vevő egyedi kérelmére nyújtott szolgáltatás) teljesülése mellett az információs társadalommal összefüggő közvetítő szolgáltatóvá minősítésnek további feltételei is megállapíthatók. Ilyen további feltételek rajzolódnak ki az EUB esetjogából az összetett szolgáltatások esetében. Az EUB esetjoga szerint az összetett szolgáltatások minősítésekor döntő jelentősége van annak, hogy a vizsgált szolgáltatásrész elválasztható-e a szolgáltatás többi funkciójától, jelentősnek tekinthető-e a szolgáltatás többi eleméhez képest. Abban az esetben, amikor egy-egy technológiai megoldás egy átfogó szolgáltatás szerves része, nem beszélhetünk különálló információs társadalommal összefüggő szolgáltatásról.

A személyszállítási közvetítő szolgáltatások kapcsán az EUB három ügy – az Asociación Profesional Elite Taxi,[55] az Uber France[56] és a Star Taxi App[57] ügyek – kapcsán is értelmezte az elválaszthatóság követelményét, azonban eltérő következtetésekre jutott a vizsgált szolgáltatásokat illetően.

A felsorolt ügyek közül kettő is az Uber elnevezésű, a személyszállítási tevékenységek piacát felforgató applikációval állt összefüggésben. Az Uber applikáció lényege, hogy nem hivatásos sofőröket kapcsol össze utasokkal. Mivel a sofőrök nem hivatásos taxiszolgáltatást nyújtanak, kedvezőbb tarifákért dolgoznak, a szolgáltatásra pedig nem alkalmazhatók azok a szigorúbb és részletesebb szabályok, amelyek a közlekedési szolgáltatásokat hivatásszerűen nyújtókra vonatkoznak.

Az Asociación Profesional Elite Taxi, valamint az Uber France ügyekben a bíróság úgy határozott, hogy az Uber által nyújtott szolgáltatás átfogó jellegű, így abban a közvetítői funkció csupán az egyik részelem szerepét tölti be, vagyis közlekedés területén nyújtott szolgáltatásnak, nem pedig információs társadalommal összefüggő közvetítő szolgáltatásnak minősül.

54 OECD 2010.
55 C-434/15, az Asociación Profesional Elite Taxi ügyben hozott 2017. december 20-i ítélet.
56 C-320/16, az Uber France ügyben hozott 2018. április 10-i ítélet.
57 C-62/19, a Star Taxi App SRL ügyben hozott 2020. december 3-i ítélet.

C-434/15. sz. Asociación Profesional Elite Taxi ügy

Az Elite Taxi nevű taxitársaság 2014-ben keresetet terjesztett elő az Uber Systems Spain ellen a spanyol barcelonai 3. számú kereskedelmi bíróságnál, amelyben kérte a társaság eltiltását a szolgáltatásának – állítólagosan tisztességtelen módon, a megfelelő hatósági engedély hiányában – folytatott nyújtásától. A spanyol bíróság azért fordult előzetes döntéshozatal iránti kérelemmel az EUB-hoz, mert megítélése szerint az, hogy a spanyol jog hatósági engedélyhez kötheti-e az Uber tevékenységét, attól függ, hogy az információs társadalommal összefüggő szolgáltatásnak vagy közlekedési szolgáltatásnak minősül.

Az EUB azt állapította meg, hogy az Uber szolgáltatása nem merül ki csupán egy közvetítő szolgáltatásban, noha kétségtelen, hogy szolgáltatásának van ilyen része. A sofőrök és az utasok összekapcsolását lehetővé tévő applikáció egy átfogó szolgáltatás része. A szolgáltatáshoz hozzá tartozik az is, hogy az Uber befolyást gyakorol a sofőrök által nyújtott szolgáltatásra, megállapítja és beszedi a fuvardíjat, továbbá ellenőrzést gyakorol a gépjárművek és a sofőrjeik fölött. Mindezekből az következik, hogy az Uber nem közvetítő szolgáltatást, hanem közlekedési szolgáltatást nyújt.

Ugyanezen érvelést alkalmazta az EUB a franciaországi Uberrel kapcsolatos döntésében is.

C-320/16. sz. Uber France ügy

Franciaországban a saját gépjárművüket használó nem hivatásos sofőrök és potenciális utasaik összekapcsolását végző Uber Pop szolgáltatás nyújtóját a lille-i általános hatáskörű bíróság a francia büntető törvénykönyvre hivatkozva elmarasztalta megtévesztő kereskedelmi gyakorlat folytatása miatt. Az eljárás tárgyát képezte továbbá a cégnek a taxis foglalkozás gyakorlásában való közreműködése is, mivel a francia jog alapján a kevesebb mint tíz férőhellyel rendelkező gépjárművel díjfizetés ellenében történő személyszállítás, mint taxiszolgáltatás, engedélyköteles tevékenység, ilyennel viszont az Uber France nem rendelkezett. A bíróság előtt folyó eljárásban kérdésként merült fel, hogy az Uber France által kínált szolgáltatást információs társadalommal összefüggő szolgáltatásnak vagy közlekedés terén nyújtott szolgáltatásnak kell-e tekinteni. Igenlő válasz esetén a francia jogalkotónak előzetesen be kellett volna jelentenie a szolgáltatásra vonatkozó szabályozást az Európai Bizottságnak. Ilyen bejelentés azonban nem volt, ami a jogszabály magánszemélyekkel szemben való alkalmazhatatlanságát vonja maga után, amennyiben a szolgáltatás valóban információs társadalommal összefüggő szolgáltatás.

Az EUB úgy határozott, hogy az olyan szolgáltatás, amelynek célja, hogy okostelefonos alkalmazás segítségével a saját gépjárművüket használó sofőröket és városon belüli helyváltoztatást igénylő személyeket díjazás ellenében kapcsoljon össze, önmagában megfelel ugyan az információs társadalommal összefüggő szolgáltatások fogalmi elemeinek, a szolgáltatás egészét vizsgálva viszont mégsem minősül közvetítő szolgáltatásnak. Érvelésében rávilágított arra, hogy ezt a fajta közvetítői tevékenységet akkor lehet a személyek mozgatásának fizikai cselekményét magába foglaló szolgáltatástól elkülönülten kezelni, ha az elválasztható a fő szolgáltatástól. Az Uber szolgáltatása azonban egy átfogó szolgáltatás egyik része, a szolgáltatás domináns eleme pedig közlekedési területen nyújtott szolgáltatás, amely magában foglalja a fuvardíj megállapítását, annak beszedését, a gépjárművek, valamint a sofőrök minőségellenőrzését is.

Ellentétes kimenetelű lett viszont a román Star Taxi App ügyében hozott ítélet, ahol szintén egy személyszállítási szolgáltatást vizsgált az EUB.

C-62/19. sz. Star Taxi App SRL ügy

A Star Taxi App SRL ügyben egy taxiszolgáltatás igénybevevőit és taxisofőröket közvetlenül, applikáción keresztül összekapcsoló társaságot az illetékes román hatóságok 4500 RON (kb. 925) euró összegű bírsággal sújtottak a diszpécserszolgáltatókra vonatkozó szabályok megsértéséért. A román jogban a taxiszolgáltatást nyújtó személyszállítók kötelesek taxidiszpécseri szolgáltatást igénybe venni; ezek végzése szintén engedélyköteles tevékenység. 2008-ban Bukarest főváros közgyűlése a diszpécseri tevékenységre vonatkozó szabályokat kiterjesztette bizonyos informatikai szolgáltatásokra is, számukra engedélyeztetési kötelezettséget írva elő, amelynek a Star Taxi App SRL nem tett eleget.

Az EUB úgy találta, hogy a szolgáltatás az információs társadalommal összefüggő szolgáltatások négy kritériumának megfelel, így továbblépett annak vizsgálatára, hogy az taxisokat és az utasokat összekötő applikáció biztosítása a későbbi, személyszállítási szolgáltatástól elkülönült szolgáltatásnak minősül-e.

Szemben az Uber France, illetve az Asociación Profesional Elite Taxi ügyek eredményével az EUB a Star Taxi Appot közvetítői információs társadalommal összefüggő szolgáltatásnak minősítette. Kimondta, hogy a vizsgált szolgáltatás nem tekinthető egy átfogó szolgáltatás részének, hiszen a célközönséget elsősorban olyan személyek jelentik, akik a tevékenységet már korábban is végezték (hivatásos taxisofőrök), és akik számára a nyújtott szolgáltatás csak az ügyfélkör építésének az egyik módozatát jelenti. Fontos szempontnak tekintette azt is, hogy nem

az applikációt kínáló fél választotta ki a sofőröket, határozta meg a fuvardíjat, illetve minőségi követelményeket sem támasztott, tevékenysége az utasok és a sofőrök összekapcsolására, tehát kizárólag közvetítésre szorítkozott.

Az ügyek alapján a nyújtott szolgáltatások közötti különbségeket a következőkben ragadhatjuk meg: míg az Uber összetett szolgáltatást nyújtott, amelyben befolyást gyakorolt a sofőrök személyére, a gépjárművekre és a fuvardíjakra, a Star Taxi App csupán összekapcsolta a város egyik pontjáról a másikra igyekvő személyeket az applikációba regisztrált és annak használatáért díjat fizető taxisofőrökkel. Míg az Uber esetében az applikáción keresztül nem hivatásos sofőrök szolgáltatásait lehetett igénybe venni, a Star Taxi App csak az egyébként is hatósági engedéllyel rendelkező hivatásos taxisofőrök szolgáltatásaihoz biztosított hozzáférést.

Az egyes szolgáltatásrészek elválaszthatóságának vizsgálatára építette az EUB a szálláshely-közvetítő szolgáltatásokkal kapcsolatos érvelését is. Az Airbnb Ireland ügyben[58] a Bíróság úgy határozott, hogy a bérbeadókat és albérlőket összekapcsoló elektronikus platform megfelel az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatók fogalmának, és közvetítő szolgáltatónak minősíthető, mivel a platformon nyújtott szolgáltatás elválasztható az ingatlanügylettől. A két szolgáltatás az EUB álláspontja szerint azért választható el egymástól, mert az online kínált szolgáltatásrész nem a szálláshely-szolgáltatás azonnali megvalósítására irányult, hanem arra, hogy a platform a szállást kereső személyek által megadott kritériumok szerint rendszerezett listát állítson össze, és ezáltal megkönnyítse a jövőbeli ügyletekkel kapcsolatos szerződések megkötését.

C-390/18. sz. Airbnb Ireland UC ügy

Az Airbnb Ireland UC ügy alapját az képezte, hogy a francia hivatásos szálláshely-szolgáltatásért és idegenforgalmi szolgáltatásokért felelős egyesület (AHTOP) feljelentést tett az Airbnb ellen, mivel a cég úgy kezelt ingatlan- és üzletivagyon-közvetítői és -kezelői tevékenység érdekében pénzeszközöket, hogy nem rendelkezett a francia jogszabályok által megkövetelt illetékes kereskedelmi és iparkamara által kiállított, szakmához tartozást igazoló kártyával. Az AHTOP arra hivatkozott, hogy az Airbnb tevékenysége nem merül ki csupán abban, hogy elektronikus platformot szolgáltat szállásadó és szálláskereső személyek összekapcsolása érdekében, hanem olyan kiegészítő szolgáltatásokat is nyújt, amelyek az ingatlanközvetítői tevékenységre jellemzők.

58 C-390/18, az Airbnb Ireland ügyben hozott 2019. december 19-i ítélet.

Ennélfogva az Airbnb tevékenységét nem lehet leszűkíteni a közvetítői szolgáltatás nyújtására, hanem azt átfogó szolgáltatás egyik elemének kell tekinteni.
Az EUB ezzel éppen ellentétes álláspontra helyezkedett, amikor kimondta, hogy az Airbnb által nyújtott közvetítő szolgáltatás „nem tekinthető egy olyan átfogó szolgáltatás szerves részének, amelynek fő eleme a szálláshely-szolgáltatás". Érvelésében a bíróság kifejtette, hogy az Airbnb szolgáltatásai, nevezetesen az, hogy aggregálja a szálláshely-ajánlatokat, az ajánlatok közötti keresésre, azok összehasonlítására biztosít lehetőséget, önmagában is jelentős szolgáltatások, amelyek nem tekinthetők járulékosnak. Kiemelte a bíróság azt is, hogy az Airbnb nem gyakorolt döntő befolyást a platformján hirdetett szálláshely-szolgáltatások feltételeire, így a bérleti díjak meghatározására sem.
Mindezekre tekintettel az EUB megállapította, hogy „információs társadalommal összefüggő szolgáltatásnak" kell minősíteni azt a közvetítői szolgáltatást, amelynek a célja, hogy egy elektronikus platformon keresztül díjazás ellenében összekapcsolja a potenciális bérlőket a rövid távú elszállásolást kínáló hivatásos és magánszemély bérbeadókkal, és e közvetítői szolgáltatás mellett bizonyos járulékos szolgáltatások nyújtására is sor kerül.

A közvetítői szolgáltatói tevékenység azonban nem korlátozódik a szolgáltatások nyújtói és igénybe vevői közötti kapcsolatok kiépítését biztosító szolgáltatókra, hanem ennél jóval összetettebb képet mutat. Egyes közvetítő szolgáltatói típusokat az Eker. irányelv külön is nevesít, ezek:

- egyszerű átviteli szolgáltató *(mere conduit),*
- gyorsítótárolás *(cache),*
- tárhelyszolgáltatás *(hosting).*

A magyar jog a közvetítő szolgáltatóknak két további típusát is ismeri: a keresőszolgáltatásokat és az alkalmazásszolgáltatásokat.

Egyszerű átviteli szolgáltatások (mere conduit)

Az Eker. irányelv szerinti egyszerű átviteli szolgáltatást nyújtó szolgáltató olyan szolgáltatást nyújt, amely információnak hírközlő hálózaton keresztül történő továbbításából vagy hírközlő hálózathoz való hozzáférés biztosításából áll. Ilyen szolgáltatók az internetszolgáltatók, amelyek fő tevékenysége olyan fizikai infrastruktúra üzemeltetése, amelyen megvalósulhat az adatok áramlása. Az internetszolgáltatók tevékenysége főként műszaki jellegű, idetartozik a kapcsolódáshoz szükséges eszközök

(modemek, szerverek, routerek, switchek) telepítése és karbantartása, az IP-címek kiosztása, illetve a gerinchálózattal folyamatos kapcsolat biztosítása. Az internetszolgáltatók fő feladata tehát az adatcsomagok folyamatos forgalmának megvalósítása. Az adatátvitelt nem ők kezdeményezik, az információ címzettjét nem ők választják meg, és nem módosítják az átvitt információt, ezért sokszor a postai szolgáltatásokhoz hasonlítják őket. Az alkalmazott technológia jellegéből fakadóan előfordulhat, hogy ezek a szolgáltatók az átvitel és a hozzáférés biztosítása érdekében automatikusan, átmenetileg tárolnak információkat, ez azonban nem jelenti azt, hogy hatással vannak a közlések tartalmára és terjedésére. A DSA, bővítve a listát, e csoportba sorolja még a vezeték nélküli hozzáférési pontokat, a virtuális magánhálózatokat (VPN), a DNS-szolgáltatásokat, illetve legfelső szintű doménnév-szolgáltatásokat, valamint a hangátviteli és személyközi hírközlési szolgáltatásokat is.[59]

Gyorsítótárolás (cache)

A gyorsítótárolás egy átmeneti információtárolás, amelynek a célja a későbbi hozzáférés gyorsítása. Internetes környezetben ez annyit tesz, hogy a böngésző, illetve az internetszolgáltató rögzít bizonyos adatokat, így, ha a felhasználó azokat ismételten későbbi időpontban meg akarja tekinteni, nincs szükség azok újbóli lehívására. A gyorsítótárolás tehát olyan automatikus, közbenső és átmeneti tárolás, amely azzal a kizárólagos céllal történik, hogy az információ későbbi továbbítását a szolgáltatás igénybe vevői számára, azok kérésére, hatékonyabbá tegye.

Tárhelyszolgáltatás (hosting service)

A közvetítő szolgáltatók közül a tárhelyszolgáltatókról folyik a legélénkebb szabályozási diskurzus. Tárhelyszolgáltatók azok a szolgáltatók, amelyek szervereiken harmadik személyek által rendelkezésre bocsátott információknak, gyakran audiovizuális tartalmaknak biztosítanak helyet. A tárhelyszolgáltatás az Eker. irányelv megalkotásakor még szinte kizárólag passzív tevékenységet végző szolgáltatókra terjedt ki, mint a szerverhosting. Az ilyen típusú szolgáltatók többnyire csak tárhelyet biztosítanak a felhasználók számára, ám abba már nem avatkoznak bele, hogy a felhasználó

[59] DSA (29) preambulumbekezdés.

miként hasznosítja a rendelkezésére álló helyet, ahogy arra sincsen különösebb ráhatásuk, hogy a tárolt tartalom eljut-e, és ha igen, milyen módon harmadik személyek szélesebb köréhez.

Nem mindegyik tárhelyszolgáltató tevékenysége irányul legitim szolgáltatás nyújtására. Különösen a szerzői jogi jogsértésekkel összefüggésben szokott felmerülni a warez és a torrentszerverek üzemeltetőinek büntetőjogi felelősségre vonása. A warez az összefoglaló elnevezése azoknak a technológiáknak, amelyek segítségével szerzői jogvédelem alá eső műveket juttatnak el a nyilvánossághoz jogsértő módon, ez lényegében az internetes kalózkodás technológiája. A warez számtalan formában megvalósítható, az egyik legkorábbi és legelterjedtebb technika az FTP-szerverek üzemeltetése vagy bérlése, amelyre szerzői művek is feltölthetők. Az FTP-szerverhez való hozzáférés általában díjfizetéshez kötött, népszerű például az, hogy az üzemeltetők emelt díjas sms fejében biztosítanak hozzáférést a tárhelyükhöz. A warez másik népszerű formája a torrenttechnológia felhasználásán alapul. A torrent valójában egy *peer-to-peer* alapú decentralizált hálózat, ahol a felhasználók nem egy meghatározott forrásból töltenek le jogvédett tartalmakat, hanem egymástól. Ebben a konstrukcióban a tárhely üzemeltetője valójában nem a szerzői jogi védelemben részesülő műveket tárolja a szerverén, hanem csak azokat a fájlokat, amelyek a művek elérési helyére mutatnak (vagyis úgynevezett trackerként működnek). A tárhelyszolgáltatók szerepe és felelőssége ebből következően többféleképpen is alakulhat: amennyiben a tárhely üzemeltetője maga nyújt warezszolgáltatást, illegitim szolgáltatásról beszélünk, amennyiben viszont a tárhelyszolgáltató csak bérbeadja szerverét, nincs tudomása arról, hogy a szolgáltatás igénybe vevői arra milyen tartalmakat töltenek fel. Felelősség szempontjából érdekes kérdéseket vet fel a torrent, ahol a tracker üzemeltetője valójában nem tárol semmilyen jogsértő tartalmat, hanem csak arra mutat rá, hogy hol találhatóak meg azok.

Egyes tárhelyszolgáltatók tevékenysége mára eltávolodott az egyszerű tárolástól, amely passzív tevékenység. Bizonyos szolgáltatók a tárhely szolgáltatásán túl kiegészítő, kényelmi és közösségi funkciókat (például a tartalmak feltöltését megkönnyítő interfész, a tartalmak megosztása más felhasználókkal, a tartalom közzététele a szolgáltató által biztosított felületen, a kommentelés lehetősége) is beépítettek a szolgáltatásukba. A legnépszerűbb példákra szorítkozva, ezek közé a szolgáltatók közé tartoznak a közösségimédia-platformok és a videómegosztó platformok is. Mivel ezek a szolgáltatások a tárhelyszolgáltatók csoportján belül egy jól elhatárolható alkategóriát képeznek, az európai uniós szabályozás ezeket az úgynevezett online platform fogalma alá rendezte.

Az online platformok (online platforms)

A közvetítő szolgáltatók kapcsán szólni kell két másik fogalomról is, amelyek sűrűn előfordulnak uniós szakpolitikai dokumentumokban: ezek az online platform, valamint a kapuőr szolgáltató fogalmai. Az Európai Bizottság közleménye[60] az online, vagyis digitális platformokat lényegében a közvetítő szolgáltatókkal azonosítja, anélkül azonban, hogy magát a fogalmat megmagyarázná. A Bizottság közleménye az online platformok közé sorolja az online áruházakat, a videómegosztókat, keresőket, a közösségi médiát és a távközlési rendszereket is. Az Európai Bizottság 2015. szeptember és 2016. január között nyilvános konzultációt tartott a platformok, online közvetítők, adatok és felhőszolgáltatások szabályozási kérdéseiről.[61] A nyilvános konzultáció egyik fő megállapítása, hogy az online platform fogalma túl széles, bevezetése és használata pedig csak további szabályozást eredményezne, ami tovább bonyolítaná az amúgy is komplex szabályozási környezetet.[62] A nyilvános konzultáció válaszadói úgy találták, hogy az online platform és a közvetítő szolgáltató fogalmai között amúgy is nagy átfedés van, ezért szükségtelen és indokolatlan újabb fogalommal gazdagítani az online szolgáltatások szabályozási hátterét. Az Európai Bizottság digitális szolgáltatásokról szóló rendelete, a DSA úgy határozza meg az online platformokat, mint „olyan tárhelyszolgáltató, amely a szolgáltatás igénybe vevőjének kérésére információkat tárol és nyilvánosan terjeszt".[63] Amellett, hogy a Bizottság egyértelműen a tárhelyszolgáltatók csoportján belül helyezi el az online platformokat, két következtetést vonhatunk le a definícióból.

Az egyik, hogy a rendelet a létező definícióknál szűkebben határozza meg az online platform fogalmát. Az OECD által alkotott meghatározás a Bizottság nyilvános konzultációt megelőző definíciójához hasonlóan igen tág. Eszerint az online platformok olyan digitális szolgáltatások, amelyek célja az egymással internetes szolgáltatáson keresztül kapcsolatba lépő, két vagy több különböző, de egymástól függő felhasználói csoport (akár cégek, akár magánszemélyek) közötti interakció megkönnyítése.[64]

60 A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Online platformok és a digitális egységes piac. Lehetőség és kihívás Európa számára.

61 Gawer 2014.

62 Gawer 2014.

63 DSA 3. cikk i) pont.

64 OECD 2019.

A másik levonható következtetés, hogy a DSA-ban felvázolt definíció máshova helyezi a hangsúlyt: az OECD fogalommeghatározásával ellentétben nem a felhasználói csoportok összekapcsolását, hanem az információ nyilvános terjesztését helyezi a középpontba. A nyilvános terjesztés a DSA fogalmi rendszerében azt takarja, hogy a hozzáférhetővé tett információ potenciálisan korlátlan számú személy számára válik elérhetővé. Kizárja tehát azokat a szolgáltatásokat, amelyek egy webhely vagy online platform infrastrukturális hátterét biztosítják (például webtárhely vagy felhőszolgáltatások), az alkalmazásboltok (Apple Store vagy Google Play), a fizetési szolgáltatók (PayPal), illetve az azonnali üzenetküldő szolgáltatások (WhatsApp, Viber), ahol a felhasználói csoportok létrehozása nem meríti ki a nyilvánosság követelményét. Tovább szűkíti az online platformok által lefedett szolgáltatások körét a rendelet, amikor arról is rendelkezik, hogy ha az információk nyilvános terjesztése csupán egy másik szolgáltatás jelentéktelen és kizárólag kiegészítő eleme, amely – objektív technikai okokból – nem használható a másik, fő szolgáltatás nélkül, akkor e szolgáltatásokat nem kell online platformnak tekinteni.[65] Ilyennek tekinti az online újságok által biztosított hozzászólási lehetőséget.

Az online platformok csoportján belül a DSA még példálózó jelleggel sem sorolja fel azokat a szolgáltatástípusokat, amelyekre a szabályozás hatálya kiterjed. Az új szabályok tartalmából azonban arra következtethetünk, hogy az alábbi néhány szolgáltatástípus mindenképp a rendelet hatálya alá fog tartozni: közösségimédia-szolgáltatás, videómegosztóplatform-szolgáltatás, online piacterek, szállásközvetítő, illetve fuvarközvetítő oldalak.

Közösségimédia-platformok (social media platforms)

A közösségimédia-platformok definiálására a szakirodalom több kísérletet is tett. Aleksandra Gebicka és Andreas Heinemann úgy határozták meg a *social media* platformokat, mint olyan internetes szolgáltatásokat, amelyek lehetővé teszik az egyének számára, hogy nyilvános vagy részben nyilvános profilt hozzanak létre egy fórumon, meghatározzák azoknak a felhasználóknak a körét, akikkel kapcsolatban állnak, továbbá megtekintsék a saját maguk és a mások által kialakított kapcsolatokat a rendszerben.[66] További cél az interakció lehetősége felhasználók és/vagy szolgáltatók

[65] DSA (14) preambulumbekezdés.
[66] Gebicka–Heinemann 2014.

között különböző hálózati kapcsolatokon keresztül.[67] Tarleton Gillespie szerint a közösségimédia-platformok azzal a tulajdonságukkal írhatók le a legjobban, hogy interfészt, illetve megjelenési felületet biztosítanak az online tér számos szereplője, illetve cselekményeik számára.[68] A Facebook és a WhatsApp összeolvadásáról szóló döntésében az Európai Bizottság úgy határozta meg ezeket a platformokat, mint olyan szolgáltatásokat, amelyek lehetővé teszik a felhasználók számára, hogy kapcsolódhassanak, megosszanak tartalmakat, kommunikáljanak, és kifejezzék magukat online vagy mobilapplikáción keresztül.[69]

A szakirodalmi definiálási kísérletek és a bizottsági fogalomalkotás ellenére a közösségimédia-platform fogalma még egyetlen uniós normaszövegben sem jelent meg. Noha mindennapi életünk során szinte mindennap találkozunk valamilyen közösségi felülettel, ha fel kellene sorolnunk, milyen szolgáltatások tartoznak ebbe a körbe, bajban lennénk. Ennek részben az az oka, hogy a szolgáltatási környezet dinamikusan változik, és napról napra jelennek meg újfajta szolgáltatások, másrészt pedig az, hogy az információs társadalom szolgáltatásai gyakran összetett jellegűek. Az a platform tehát, amelyik rendelkezik közösségi funkcióval, például a tartalmak megosztásának és kommentelésének lehetőségével, gyakran számos más lehetőséget is kínál a felhasználók számára, sőt az is előfordulhat, hogy a szolgáltatás fő funkciója nem közösségi platform biztosítása, a közösségi elem csupán járulékos eleme a kínált szolgáltatásnak.

A közösségi médiát elsősorban azért szeretjük a hagyományos médiával rokonítani, mert a közösségimédia-platformok általában műsorszámoknak és felhasználók által generált tartalmaknak biztosítanak megjelenési felületet, elősegítik azok eljutását a nyilvánossághoz, így tevékenységükkel összefüggésben számos olyan kérdés felmerül, amelyet korábban a televízió, a rádió és a sajtó vonatkozásában kellett megválaszolnia a jogalkotásnak és a jogalkalmazásnak. Klein Tamás is rámutat, hogy a közösségi platformok napjainkban olyan tömegkommunikációs eszközök, amelyeket a felhasználók jelentős része használ tájékozódásra, a társadalmi folyamatokra vonatkozó információk beszerzésére.[70] A közösségimédia-platformok – noha nagy számban találhatók rajtuk audiovizuális tartalmak – nem minősülnek médiaszolgáltatásnak, mivel nyújtóik nem végeznek a hagyományos médiaszolgáltatások nyújtóihoz

[67] Fehér 2016.
[68] Gillespie 2010.
[69] Commission Decision of 03/10/2014 declaring a concentration to be compatible with the common market (Case No COMP/M.7217 – Facebook / WhatsApp) according to Council Regulation (EC) No 139/2004.
[70] Klein 2018a: 32.

hasonlóan szerkesztői tevékenységet. Ugyan klasszikus szerkesztői tevékenységet nem látnak el, a *social media* platformok nem nevezhetők a kommunikációs folyamat passzív szereplőinek. A platformok főként automatizált eszközök, algoritmusok révén szűrik a tartalmakat, rangsorolnak, javaslatokat tesznek olyan tartalmakra, amelyek a felhasználót érdekelhetik, egyedi lekérdezésre pedig találati listát állítanak össze. Ezen túlmenően saját szabályrendszert, például a Facebooknál közösségi alapelveket alkotnak, ezzel befolyásolják a felhasználóik magatartását. A meghatározott szabályokat ki is kényszerítik, a saját maguk által észlelt vagy a felhasználók által bejelentett normaszegést szankcionálják, például tartalmakat törölnek, korhatárossá tesznek, vagy felhasználókat tiltanak. Bartóki-Gönczy Balázs is kiemeli, hogy a konvergencia hatására egyre nehezebb eldönteni, hogy egy online közvetítő gyakorol-e tényleges ellenőrzést a tartalom felett, amelynek következében már médiumnak minősül, vagy továbbra is a technikai közvetítők között kell számontartani.[71] A szabályozási dilemma mellett arra is indokolt rávilágítani, hogy ezekre a platformokra nem kizárólag médiajogi szabályok vonatkoznak, hanem általában meg kell felelniük az adatvédelmi, fogyasztóvédelmi és szerzői jogi rendelkezéseknek is.

A 2018-as AVMS irányelv[72] az audiovizuális tartalmaknak felületet biztosító közösségimédia-platformokra részben ezen okok miatt terjeszti ki a hatályát, részben pedig amiatt, mert ugyanazért a közönségért és ugyanazon bevételekért versengenek, mint az audiovizuális médiaszolgáltatások.[73] Ezek a *social media* platformok kapuőrökként funkcionálnak, mivel képesek tényleges kontrollt gyakorolni az információáramlás felett: annak ellenére, hogy az audiovizuális médiaszolgáltatásokkal szemben követelményként támasztott szerkesztői felelősséget eredményező tevékenységet nem végeznek, befolyásolni tudják az információ megjelenítését, így egyes tartalmak hatását felerősítik, másokét pedig elnyomják. Szembetűnő a különbség továbbá a tartalomgyártás és tartalomterjesztés módjában. Míg a tradicionális médiában a tartalom egy csatornán (a szerkesztőn keresztül) jut el a közönség tagjaihoz, a közösségi média esetében mindenki egyszerre fogyasztó és tartalom-előállító. Eltér egymástól a néző és a tartalom-előállító kapcsolata is. A hagyományos médiában a kommunikáció alapvetően egyirányú, a közvetlen fogyasztói visszacsatolásnak viszonylag kevés szerep jut,

71 Bartóki-Gönczy – Pogácsás 2019: 719–756.

72 Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról.

73 2018-as AVMS irányelv (4) preambulumbekezdés.

míg a közösségi média elsősorban a felhasználói – sokszor moderálatlan – interakcióra épül. Szintén a tradicionális médiára jellemző szerkesztési tevékenységből adódik, hogy a médiaszolgáltatásokra többnyire a professzionális tartalom-előállítók által gyártott tartalmak bemutatása a jellemző. A közösségi platformokon a professzionális médiaszolgáltatók által előállított tartalmak mellett, hangsúlyosan vannak jelen a felhasználók által előállított tartalmak *(user generated content)* is.

Videómegosztók (video-sharing platforms)

A videómegosztók ugyan az Eker. irányelv szerinti tárhelyszolgáltatónak és a DSA szerinti online platformnak minősülnek, de a legtöbb ilyen szolgáltató tevékenysége meglehetősen túlmutat a klasszikus tárolási tevékenységen, és rokonságot mutat a médiaszolgáltatási tevékenységekkel. Ebből kifolyólag a videómegosztókra vonatkozó részletszabályok végül – vitatható módon – az AVMS irányelvben kaptak helyet. A videómegosztó azonban ezen irányelv rendszerén belül is fekete báránynak számít, hiszen annak ellenére, hogy a szabályai az audiovizuális médiaszolgáltatásokat szabályozó rendelkezések között helyezkednek el, maga nem számít médiaszolgáltatásnak. A szabályozási koncepció az irányelv (4) preambulumbekezdése szerint annak mentén alakult, hogy a videómegosztók fő profilja az audiovizuális műsorszámok és felhasználó által előállított videók tárolása és közönséghez való eljuttatása, tartalomszolgáltatással való szoros kapcsolatuk révén pedig célszerűbb a rájuk vonatkozó szabályokat az audiovizuális médiaszolgáltatásokra vonatkozó szabályok mellett szerepeltetni.

Az irányelvi meghatározás szerint a videómegosztóplatform-szolgáltatás:

> „[A]z Európai Unió működéséről szóló szerződés 56. és 57. cikkében meghatározott olyan szolgáltatás, amelynek, vagy amely egy elválasztható részének vagy egy alapvető funkciójának elsődleges célja, hogy tájékoztatás, szórakoztatás vagy oktatás céljából a 2002/21/EK irányelv 2. cikkének a) pontja értelmében vett elektronikus hírközlő hálózatokon keresztül olyan műsorszámokat, felhasználó által létrehozott videókat, vagy mindkettőt juttasson el a közönséghez, amelyekért a videómegosztó platform szolgáltatója nem tartozik szerkesztői felelősséggel, és amelyeket a videómegosztó platform szolgáltatója rendszerez például automatikus eszközökkel vagy algoritmusokkal, különösen megjelenítés, címkézés és sorba rendezés révén."[74]

74 AVMS 1. cikk (1) bekezdés aa) pont.

A definíció igen általános jellegű, nem könnyű értelmezni; bizonyos elemek interpretálása így teljes mértékben a tagállamokra van bízva. Határokon átnyúló jelleggel nyújtott szolgáltatások esetében kifejezetten problémát jelenthet, ha az egyes tagállamok eltérően értelmezik a fogalom egyes elemeit. Problémakezelés szempontjából kimondottan nem szerencsés, ha az egyik tagállam videómegosztóként tekint egy olyan szolgáltatásra, amelyre egy másik nem. Az eltérő besorolásból fakadó gondok nemcsak a kisebb platformokkal kapcsolatban merülhetnek fel, hanem még a nagy, globális platformok esetében sem mindig egyértelmű, hogy videómegosztónak minősülnek-e. Az AVMS irányelvben szereplő fogalom egyik említett hiányossága, hogy nem határolja el egyértelműen a videómegosztóplatform-szolgáltatásokat a többi hasonló jellegű, audiovizuális tartalmat szolgáltató információs társadalommal összefüggő szolgáltatástól, így a közösségimédia-szolgáltatásoktól sem. Sőt, inkább összemossa a különböző szolgáltatási kategóriákat, amikor akként rendelkezik, hogy azok a közösségimédia-platformok is videómegosztónak minősülnek, amelyek megfelelnek az irányelvben támasztott fogalmi elemeknek. Az elhatárolás azért is problémás, mert a *social media* platformoknak nincs általánosan elfogadott definíciójuk.[75] A két szolgáltatásfajta között vélhetően nem is lehet éles határvonalat húzni, hiszen mind a videómegosztók, mind a közösségi platformok multifunkciós szolgáltatások, amelyekben jelen vannak audiovizuális tartalmak feltöltését és megosztását lehetővé tévő, valamint közösségi funkciók egyaránt, a különbség inkább az egyes szolgáltatási elemek hangsúlyosságában nyilvánul meg. Míg például a YouTube esetében a kommentelést lehetővé tévő közösségi funkció inkább kiegészítő jellegű, a Facebook esetében a megosztott tartalmakra való reagálást lehetővé tévő felület a szolgáltatás alapvető eleme. A Facebook esetében viszont az audiovizuális tartalmak megosztásának lehetősége képez másodlagos funkciót, hiszen lehetőség van számos más tartalmat – szöveget, képet, eseményt – is megosztani. Az ír médiahatóság, a BAI a komplex, multifunkciós szolgáltatások vizsgálatára kidolgozott egy módszertant,[76] amelynek alapja a videómegosztáshoz kapcsolódó valamennyi szóba jöhető funkció azonosítása. A videómegosztáshoz kapcsolódó funkciókat a BAI két csoportra osztotta, központi funkcióra *(core function)*, valamint másodlagos funkciókra *(ancillary functions)*. Előbbi olyan alapvető elem (felhasználók által feltöltött audiovizuális tartalmakhoz biztosít hozzáférést), amelynek a megléte esetén az ír hatóságnak mérlegelés nélkül videómegosztónak kellene nyilvánítania az adott szolgáltatást, míg a másodlagos

[75] Koltay 2019b: 1.
[76] Broadcasting Authority of Ireland 2019.

funkciók (életkor-ellenőrzés, tartalomajánlások, értesítések, bejelentkezési lehetőség, felhasználási feltételek) jelenléte esetén a minősítés mindig mérlegelés eredménye.

Az azonosítást megkönnyítendő, egy szolgáltatás nemcsak akkor minősíthető videómegosztónak, ha a szolgáltatás teljes egésze felel meg az irányelvi definíciónak, hanem akkor is, ha a fogalmi elemek csak a szolgáltatás valamely különválasztható részére vagy alapvető funkciójára igazak. Azt, hogy mi minősül egy szolgáltatás különválasztható részének vagy alapvető funkciójának, esetről esetre lehet csak eldönteni az adott szolgáltatás sajátosságait figyelembe véve. A jogalkalmazási gyakorlat közelítése érdekében a 2018-as AVMS irányelv a Kapcsolattartó Bizottság (Contact Committee) feladatává teszi az olyan ajánlások kidolgozását, amelyek segítséget nyújtanak a tagállamoknak e két kritérium értelmezéséhez.[77]

Az EUB esetjoga ad némi iránymutatást arra nézve, hogy mit érthetünk egy szolgáltatás különválasztható része alatt, mivel ez a szövegrész a New Media Online ügyben[78] levont következtetések nyomán került be mind az audiovizuális médiaszolgáltatás, mind a videómegosztóplatform-szolgáltatás fogalmába.

C-347/14. sz. New Media Online GmbH kontra Bundeskommunikationssenat és Der Bundeskanzler. A Verwaltungsgerichtshof ügy

A *Tiroler Tageszeitung* online hírportál a szöveges tartalmú cikkek mellett számos audiovizuális tartalmat is kínált a fogyasztóknak. Az oldalon a videókkal alapvetően kétféleképpen találkozhattak a felhasználók: előfordultak a hosszabb, szöveges cikkekbe beágyazott, az írások tartalmát kiegészítő, illusztráló videók, ezenfelül azonban a hírportál üzemeltetője egy aldoménen egy külön videószekciót is létrehozott, kimondottan az audiovizuális tartalmak számára. Az ügyben az a kérdés merült fel, hogy a portálnak ez a külön videók számára létrehozott aloldala a szolgáltatás különválasztható részének minősül-e. Az EUB erre a kérdésre igenlő választ adott, így egyértelművé téve, hogy az ehhez hasonló videószekciók lekérhető szolgáltatásoknak minősíthetők.

A testület kimondta, hogy az egyes szolgáltatásrészek besorolásának annak vizsgálatához kell kapcsolódnia, hogy az adott szolgáltatás önálló tartalommal és funkcióval rendelkezik-e, és nem csak olyan kiegészítés, amely különösen az audiovizuális és szöveges kínálat közötti összefüggésből fakadóan elválaszthatatlan az utóbbi tevékenységtől.

77 2018-as AVMS irányelv (52) preambulumbekezdés.

78 C-347/14, a New Media Online GmbH kontra Bundeskommunikationssenat és Der Bundeskanzler. A Verwaltungsgerichtshof ügyben hozott 2015. február 21-i ítélet.

A cikkekbe ágyazott rövid videók például olyan elválaszthatatlan kiegészítő elemet képviselnek, amely nem indokolja a sajtóterméktől elkülönülő, önálló médiaszolgáltatásként való nyilvántartásba vételt. Az EUB által megfogalmazott különválaszthatósági teszt nemcsak az online sajtótermékek és a lekérhető szolgáltatások elválasztására szolgálhat, hanem alkalmazható egyéb szolgáltatások megítélése esetén is, így a Facebook esetében például a platform önálló aloldalon működtetett Facebook Watch funkciója minősülhet a szolgáltatás különválasztható részének.

Vélhetően a gyakorlatban nehezebb lesz az „alapvető funkció" szövegrész tartalmának a megállapítása. Kizárólag azokban az esetekben lehet megállapítani, hogy az audiovizuális kínálat alapvető funkcióját képezi a szolgáltatásnak, amikor a szolgáltatás több részből áll, ugyanakkor az egyes részei nem különíthetők el egymástól, mert például egy hírfolyamot jelenítenek meg a felhasználóknak, amelyen vegyesen jelennek meg audiovizuális, állóképes és szöveges tartalmak. Az Európai Bizottság 2020-ban egy közleményben értelmezte az alapvető funkció kritériumát, és tizenhárom olyan mutatót határozott meg, amelyek orientálják a jogalkalmazót a funkció jelentőségének meghatározásában:[79]

1. a szolgáltatás szerkezete és felépítése,
2. az audiovizuális tartalom önálló jellege,
3. audiovizuális tartalomra szabott konkrét funkciók,
4. a mód, ahogy a szolgáltató pozicionálja magát a piacon,
5. a platformon elérhető audiovizuális tartalom mennyisége,
6. a platformon lévő audiovizuális tartalom használata,
7. az audiovizuális tartalom hatóköre,
8. kereskedelmi kommunikáció jelenléte,
9. a felhasználók tevékenységének nyomon követése,
10. az audiovizuális tartalom fogyasztását ösztönző egyedi jellemzők,
11. a felhasználók interakciójának ösztönzése,
12. tartalomajánló rendszerek működtetése,
13. teljesítmény nyomon követése.

Részben ugyan szubjektív szempont, de támpontot nyújthat az, hogy a szolgáltató milyen mértékben törekszik a videómegosztási funkció népszerűsítésére. A szolgáltató honlapjának szerkezete, a menüpontok elrendezése, a videókat tartalmazó rész

[79] A Bizottság közleménye: Iránymutatások az audiovizuális médiaszolgáltatásokról szóló irányelv értelmében a „videomegosztóplatform-szolgáltatás" fogalommeghatározásában szereplő alapvető funkció kritériumának gyakorlati alkalmazására vonatkozóan.

vizuális kiemelése indikátorai lehetnek a szolgáltatásrész jelentőségének. Amennyiben a szolgáltató nagy hangsúlyt fektet az audiovizuális tartalomkínálatra, valószínű, hogy a honlapjának vagy a szolgáltatás elérésére használt interfésznek a kialakítása megkönnyíti az audiovizuális tartalmakhoz való eljutást (audiovizuális tartalomra szabott konkrét funkciók), a platformon használt keresőfunkció pedig szintén az audiovizuális tartalmak könnyű kereshetőségére szabott. Az ilyen platformok a felhasználók számára megkönnyítik a videók feltöltését is azáltal, hogy hangsúlyos helyre pozicionálják a feltöltés gombot, illetve olyan szolgáltatáselemeket tartalmaznak, mint az automatikus lejátszás, élő közvetítés. Indikátora a funkció jelentőségének az is, hogy a szolgáltató ösztönzi-e a tartalmak fogyasztását, például azzal, hogy a felhasználói felületen a hírfolyamokban ajánlásokat, javaslatokat tesz audiovizuális tartalmakra. Csekély jelentőségre utal azonban, ha az audiovizuális tartalmak jelen vannak ugyan, de nem hangsúlyos helyen szerepelnek, hanem például cikkekbe ágyazottan.

Önálló az audiovizuális tartalom jellege, ha azokat „információs, szórakoztató vagy oktatási értéküknél fogva" osztják meg és fogyasztják. Nem önállóak ellenben azok a videók, amelyeket egy gazdasági szolgáltatás népszerűsítése vagy termék értékesítése miatt osztanak meg. Egyes online piacterek, mint például az Amazon, lehetővé teszik a termékek véleményezését rövid videók feltöltésével, más szolgáltatók pedig az értékesítést végző felhasználóknak teszik lehetővé, hogy videóban mutassák be a kínált terméket. Ezekben az esetekben a videómegosztás az értékesítés megkönnyítését szolgálja csupán, vagyis a felhasználó által generált tartalom hasznos, de nem szükségszerű eleme a szolgáltatásnak, amelynek a végső célja termékek online adásvételének biztosítása.

Fontos jellemző a szolgáltató önmagáról alkotott felfogása is, illetve az a kép, amelyet a saját szolgáltatásáról a felhasználó felé közvetít. A videómegosztó jelleg hangsúlyosságára lehet következtetni, ha a szolgáltató az adott szolgáltatást úgy forgalmazza vagy reklámozza, hogy felhívja a potenciális felhasználók figyelmét az audiovizuális tartalmak jelentőségére.

Az alapvető funkció kritériumának egyik meghatározó jellemzője, hogy a szóban forgó funkció nem lehet „csupán kiegészítő jellegű" vagy „csekély része" a szolgáltatásnak. Egy funkció akkor minősíthető csekélynek a teljes szolgáltatás egyes részelemei között, ha „mennyiségi és/vagy minőségi megfontolások alapján úgy tűnik, hogy jelentéktelen szerepet játszik a szolgáltatás általános gazdaságosságában". Nem elhanyagolhatók tehát a mennyiségi szempontok sem, hiszen a videómegosztó funkció jelentőségének egyik indikátora lehet a feltöltött tartalmak egyéb tartalmakhoz viszonyított aránya is.

Nem elhanyagolható, de nehezen mérhető, szubjektív szempont a felhasználók percepciója, hiszen egy szolgáltatásrész fontosságát az is jelzi, hogy a szolgáltatást ténylegesen igénybe vevő személyek miként vélekednek róla (például alapvető lehet egy funkció, ha annak hiányában a felhasználók nem látogatnák a platformot). Azok a szolgáltatók, amelyek hangsúlyosnak tekintik az audiovizuális kínálatukat, mérhetik annak hatékonyságát, ami alapulhat az egyes videók nézettségén, az aktív felhasználók számán, a látogatottságon, de a feltöltött tartalmak számán is.

Ehhez szorosan kapcsolódik az a szempont, hogy a szolgáltató kínálatában található audiovizuális tartalmak milyen széles réteg elérésére alkalmasak. Az úgynevezett virális, azaz robbanásszerűen népszerűvé váló tartalmak jelenléte a platformon arra utalhat, hogy a funkció jelentős, hiszen a platform felhasználóinak számottevő részét meg tudja szólítani.

Annak eldöntésében, hogy a videómegosztás alapvető funkciója-e egy szolgáltatásnak, mindenképp indokolt figyelembe venni azt, hogy az adott funkció milyen kereskedelmi értéket képvisel a szolgáltató számára. Az AVMS irányelv alapvetően a gazdasági szolgáltatóként nyújtott médiaszolgáltatásokat és videómegosztókat szabályozza, ezért nem elhanyagolható tényező, hogy a szolgáltatónak származik-e haszna a funkció működtetéséből, és ha igen, az mennyire jelentős eleme az üzletpolitikájának, milyen mértékben befolyásolja a szolgáltató piaci helyzetét. Egy funkció gazdasági jellegét mutathatja például az, hogy a szolgáltatónak származik-e bevétele a működtetéséből. A bevétel jelen esetben tágan értelmezendő, hiszen az származhat akár a felhasználóktól (például prémiumszolgáltatások, előfizetéses konstrukciók esetén) vagy hirdetési bevételekből. Azok a szolgáltatók, amelyek maguk helyeznek el kereskedelmi kommunikációt a videók környezetébe, és ezáltal bevéltelt realizálnak (vagyis monetizálják a tartalmakat), valószínűleg jelentős elemként tekintenek e funkcióra.

Nemcsak az jelzi a funkció fontosságát, ha a platform hirdetésekből szerez bevételt, hanem az is, ha a hálózat „másik oldaláról", a tartalomfogyasztó felhasználótól szed díjat a szolgáltatás használatáért. A szolgáltatás lehet havidíjas, az egyes tartalmak megtekintéséért díjat kérő *(pay-per-view),* illetve a díj kivetése megvalósulhat prémium- vagy VIP-csomagok révén is, ahol a felhasználó lényegében azért fizet, hogy reklámmentesen tekinthesse meg a szolgáltató tartalmait. A bizottsági közlemény azonban felhívja a figyelmet arra, hogy a vizsgált funkció alapvető jellegűnek minősítéséhez nem szükséges, hogy „alapvető kereskedelmi jelentőséggel" bírjon, mert ez olyan szűkítő értelmezést jelentene, ami hátrányosan befolyásolhatná a felhasználók védelmét egyes szolgáltatások esetében.

Az is a funkció jelentőségét mutatja, ha a szolgáltató ösztönzi a felhasználók egymás közötti interakcióját a tartalmakkal összefüggésben. Ez megvalósulhat például kommentszekció létrehozásában, vagy abban, hogy a felhasználók az élő videóhoz valós időben tudnak hozzászólni.

Jelzi a funkció jelentőségét az is, ha a szolgáltató összetett tartalomajánló rendszereket működtet. Az ajánló, javaslattevő rendszerek napjainkban bonyolult és költséges mesterségesintelligencia-alapú algoritmusok, amelyek kifejlesztése a szolgáltatók K+F-költéseiben jelentős tételt tesz ki. Ezek az algoritmusok a felhasználók véleményén túl számtalan szempontot figyelembe tudnak venni, így azt, hogy a felhasználó végignézi-e a tartalmat, használja-e a „tetszik" gombot, beleteker-e a videóba.

A szolgáltatás végső céljának meghatározása is fontos szempontja lehet a döntéshozatalnak, mivel egy funkciót lényegében akkor tekinthetünk alapvetőnek, ha az nélkülözhetetlen a szolgáltatás végső céljának eléréséhez.

Egyéb közvetítő szolgáltatók

Az Eker. irányelvben felsorolt közvetítő szolgáltatók listája nem zárt. Nemzetközi szakpolitikai dokumentumok és a magyar Ekertv.[80] is többféle közvetítő szolgáltatót nevesít, mint az uniós norma. Az OECD a közvetítő szolgáltatók közé sorolja még a keresőmotorokat és oldalakat, az internetes fizetési rendszereket, valamint azokat az online részvételen alapuló hálózatokat *(participative networking platform),* amelyek nem maguk gyártják, illetve választják meg a szolgáltatásukban megjelenő tartalmat.[81] Az Európa Tanács Miniszteri Bizottságának ajánlása szintén a közvetítők közé sorolja a keresőmotorokat, továbbá a kereskedelmi jellegű tranzakciókat (köztük az online fizetést) lehetővé tévő szolgáltatásokat és az aggregátorokat.[82] Az online keresőprogram a DSA 3. cikkének j) pontja szerint is közvetítő szolgáltatás. Ez azonban ellentmond az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló 2019/1150/EU rendeletnek, amely a keresőmotorokat nem sorolja ebbe a körbe. A digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU)

80 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

81 OECD 2010: 9.

82 Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries 4. pont.

2020/1828 irányelv módosításáról szóló 2022/1925/EU rendelet, a DMA erre a 2019-es rendeletre visszautalva szintén külön kategóriába sorolja az online keresőmotorokat. Az Ekertv. Magyarországon a keresőmotorokat és az alkalmazásszolgáltatókat szintén a közvetítő szolgáltatók közé sorolja. A keresőmotorok alapvető szerepet töltenek be a felhasználók információhoz juttatásában, mivel ezek a szolgáltatók teszik lehetővé, hogy a felhasználók eligazodjanak az interneten, megtaláljanak információkat, és hozzáférjenek azokhoz. Az Ekertv. 2. §-ának l) pont ld) alpontja szerint az információk megtalálását elősegítő segédeszközöket biztosítanak az igénybe vevő számára. Alkalmazásszolgáltató az a szolgáltató, amely elektronikus hírközlő hálózat felhasználásával valamilyen szoftverhez vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen több felhasználó számára, időben korlátozott vagy korlátlan módon, havi vagy használatalapú ellenszolgáltatás fejében vagy ingyenes formában.[83]

[83] Ekertv. 2. § l) pont le) alpont.

Vákát oldal

III. Az informatikai bűnözés nemzetközi környezete

A közelmúltban még azon folyt a vita, hogy ki kell-e terjeszteni a jog uralmát a virtuális térre, vagy hagyni kell ezt a területet úgynevezett „jog nélküli zónaként" működni. Ma már kétség sem fér hozzá, hogy a digitális világban ugyanúgy szükség van szabályokra, mint a fizikai világban, ám ez az állítás sokszor még megválaszolásra váró kérdésekhez vezet. Elsőként például ahhoz, hogy amennyiben hatékonyan szeretnénk szabályozni a digitális világot, pontosan milyen szabályokra van szükségünk? Ugyanazokat a szabályokat kell-e alkalmazni, mint a materiális világban, vagy olyan rendszert kell kialakítani, amely a virtuális tér sajátosságaira van szabva? Kérdés továbbá az is, hogy egy adott ügyben melyik ország szabályai alkalmazandók. Mivel az internet egy globális hálózat, amely a világ összes számítógépét összeköti, a nemzeti határok jelenléte csekély jelentőségű. Vannak ugyan olyan országok (például Kína), ahol a kormány korlátozza az állampolgárok hozzáférését a világhálóhoz, illetve bizonyos tartalmakhoz, azonban a demokratikus országokban az internet alapvetően nyíltan működik, annak ellenére is, hogy egyre fokozódó nyomásgyakorlást figyelhetünk meg a szuverének részéről egyes közösségimédia-platformok vonatkozásában. Könnyen előfordulhat tehát, hogy a bűncselekmény elkövetője nem azonos országban, de még csak nem is azonos kontinensen tartózkodik, mint a bűncselekmény sértettje. Sőt az sem szükségszerű, hogy a bűncselekménynek csak egy sértettje legyen, az elkövető egyszerre akár több ezer, különböző országokban tartózkodó sértett sérelmére is elkövetheti a bűncselekményt. Több elkövető esetén sem biztos, hogy mindegyikük azonos országban tartózkodik. Problémát jelenthet az is, ha a sértett országában az adott

cselekményt a büntetőjog szankcionálni rendeli, az elkövető országában azonban nem. Az elektronikusan tárolt adatok illékony és könnyen megváltoztatható természetéből adódóan számos kérdést vet fel az is, hogy a nyomozó hatóságok hogyan szerezhetik meg az úgynevezett digitális bizonyítékokat, illetve milyen intézkedéseket tehetnek az ilyen típusú bizonyítékok megszerzése érdekében.

Az államok viszonylag hamar felismerték, hogy ezen deliktumok esetében a pusztán nemzeti szintű szabályozás nem elég, és a hatékony fellépés érdekében nemzetközi összefogásra van szükség, amelynek keretében tisztázni kell az informatikai bűncselekményekhez kapcsolódó fogalmakat, joghatósági kérdéseket, illetve tényállásokat. Szükségessé vált ezenfelül egy olyan szupranacionális szervezetrendszer kialakítása, amely hatékonyan képes koordinálni a tagállamok hatóságainak együttműködését, és biztosítja az információáramlást az egyes országok között. A kötet jelen részének egyik célja, hogy bemutassa, hogyan vált a számítógép és a világháló napjaink egyik legnagyobb bűnüldözési kihívásává. Az informatikai bűncselekmények történetének bemutatása elengedhetetlen ahhoz, hogy megértsük, hogyan és miért alakult ki az a sokszínű szabályozási rendszer, amely az információs társadalom deliktumait jellemzi. A jelen rész második célkitűzése, hogy a történeti megalapozást követően megvizsgálja, hogy a számítógéppel kapcsolatos jogsértésekre milyen szabályozói válaszok érkeztek, és bemutassa azokat a fontosabb nemzetközi normákat, amelyek a területet átszövik.

Az informatikai bűnözés rövid története – avagy hogyan lett a számítógép napjaink egyik legnagyobb nemzetközi bűnüldözési kihívása?

Az informatikai bűnözés csaknem egyidős az informatikai eszközökkel. Ahogyan az új technológiák esetében az eszközök sorozatgyártása megkezdődött, a gyártószalagról lekerült termékek pedig tömegtermékekké váltak, úgy kezdték el a bűnelkövetők is elsajátítani használatukat és kiaknázni a bennük rejlő potenciált. A számítógépek és az internet elérhetősége és anonimitása a bűnelkövetőknek ugyanúgy kedvez, ahogyan az átlagpolgároknak, és az információs technológiák széles körű elterjedtsége és könnyű kezelése miatt nagyon sok bűncselekmény könnyebben és gyorsabban megvalósítható a kibertérben, mint a fizikai világban; valamint megjelentek új, kifejezetten az információs rendszerek integritását sértő deliktumok is. Egyes cselekmények, például az információs rendszerek elleni támadások folyamatosan idomulnak

a technológiai környezet változásaihoz, a megvalósítás módja tehát a technológiával párhuzamosan folyamatosan fejlődik. Korábban a számítógépes rendszerek elleni támadások esetében népszerű volt a gépidőlopás, a számítógép rendszeridejének manipulációja, a vezetékes telefonhálózatok percdíjainak manipulálása. Ezek a cselekmények a széles sávú és korlátlan internet-hozzáférés, a mobiltechnológia és a *voice over internet protocol* (VOIP) elterjedésével szinte teljesen megszűntek, megjelentek azonban másfaja jogellenes cselekmények, például a személyazonosság-lopások közösségi platformokon, a személyes adatokkal való tömeges visszaélések. Egy ilyen dinamikus fejlődéssel nem könnyű a szabályozásnak lépés tartania. Bizonyos szempontból azonban elmondhatjuk, hogy nincs új a nap alatt, az elkövetési módszerek ugyan változnak, az elkövetők technikája és a használt eszközök kifinomultabbá válnak, az előző évezred informatikai bűncselekményei és a kortárs cselekmények sokszor azonos alapokon nyugodnak. Az informatikai bűnözéssel kapcsolatos rövid, történeti áttekintés ezeket az alapokat kívánja megvilágítani, hiszen a jogi szabályozásnak kellően absztraktnak kell lennie ahhoz, hogy tartósan alkalmas legyen egyes életviszonyok szabályozására.

Az informatikai bűnözés története az Egyesült Államokban

Az 1960-as évek a technológia fejlődése szempontjából azért jelentősek, mert ekkortájt jelentek meg a tranzisztoralapú számítógépes rendszerek, amelyek lényegesen olcsóbbak és kisebb méretűek voltak a korábbi társaiknál, amelyek teljes termeket töltöttek meg. Bár számítógépek és az internet elődje, az ARPANET is léteztek már 1962-ben, a 60-as, 70-es években a számítógép még nem számított tömegterméknek, és a katonai felhasználásán túl főleg a bankszektorban és a felsőoktatásban, egyetemi kutatóműhelyekben alkalmazták. A számítógép-használat első korszakában még gyakrabban fordultak elő a számítógép mint hardver ellen elkövetett, fizikai kárt okozó, rongálásszerű cselekmények. Az új technológiában az emberek egymástól való elidegenedésének eszközét látó, az innovációra a kultúra elnyomásának eszközeként tekintő, az ipari forradalom ludditáihoz hasonló géprombolók és a nagy anyagi károkozással a figyelem középpontjába kerülő politikai aktivisták egyaránt a hardver megrongálásában találták meg álláspontjuk nyomatékosításának eszközét. A számítógépes szabotázs egyik legkorábban dokumentált esete mégis egy magányos éjszakai biztonsági őrhöz, Alberthez[84] köthető, akinek nem volt tudomása arról, hogy

[84] Kabay 2008: 7.

milyen nagy értékű a berendezés és a benne található adat, mindössze arra a figyelemre vágyott, amelyet a számítógép kijavítására érkező technikusoktól kapott.

A későbbi, számítógépekkel kapcsolatos bűncselekmények már korántsem voltak annyira ártó szándéktól mentesek, mint Albert rongálása. A 70-es években kezdtek el igazán elterjedni a számítógépekkel és adatokkal kapcsolatos visszaélések, a csalások megvalósításának új lehetőségeit teremtette meg az információs környezet névtelensége és arctalansága, amely szinte megágyazott a manipulációknak. A számítógépekkel kapcsolatos cselekmények nagy része a gépesített telefonhálózatok azon gyengeségeit használta ki, amelyekről közvetlenül automatizált kapcsolással lehetett hívást indítani a világ szinte bármely részére. A hálózatok gyenge pontjait kihasználó csalók (*phreaker*ek) többnyire ingyenes távolsági hívásokat kezdeményeztek. Ebben az időszakban jelentek meg az első *malware*-ek, az ARPANET-en 1971-ben jelent meg az első számítógépes vírus, a Creeper.[85] Az új jelenségre reagáló, akkor még csak állami szintű törvények is megszülettek, az amerikai szakirodalom az 1978-as floridai számítógépes bűnözésről szóló törvényt (Florida Computer Crimes Act, 1978) tartja számon az első informatikai bűnözést kezelni kívánó jogszabályként.

Az 1980-as években a személyi számítógép már gyakran megtalálható eszköz volt a munkahelyeken és a háztartásokban egyaránt, a tömeges elterjedés a kezdeti felhasználói tudatlansággal kiegészülve kiváló terepet jelentett a bűnelkövetőknek, megjelentek az első kortárs számítógépes vírusok és a hackerek. Az USA-ban először 1981-ben ítéltek el jogerősen egy hackert számítógépes bűncselekmény miatt, a kiszabott büntetés közmunka és próbaidő volt.[86] Az elkövető Ian Murphy (felhasználónevén Captain Zap), három tettestársával az AT&T telekommunikációs cég számítógépes rendszerébe törtek be, ahol átállították a rendszer belső óráit. A cselekmény motívuma az volt, hogy abban az időben a percdíjak jelentősen függtek a napszaktól, az éjszakai hívások pedig jóval olcsóbbak voltak. Az Egyesült Államokban szabadságvesztés büntetést számítógépes bűncselekmény miatt először 1983-ban szabtak ki. A *malware*-ek kezdetben fertőzött adathordozókkal, például floppylemezekkel terjedtek, mint az 1981-es Elk Cloner, vagy az 1986-os Brain boot sector vírus. Az azonos érdeklődésű, többnyire fiatalokból álló hackerek elkezdték kialakítani saját közösségeiket. Az egyik ilyen csoport volt az 1984-ben alakult Legion of Doom, amely még hackereknek szóló szaklapot is megjelentetett, ezzel segítve a számítógépek és programozás iránt érdeklődő fiatalok fejlődését.

[85] Hill–Marion 2016: 23.
[86] Hill–Marion 2016: 24.

Az 1990-es években elterjedt a *world wide web,* mint globális hálózat, így az immár hálózatba kapcsolt számítógépek ellen elkövetett bűncselekmények száma emelkedett, hiszen az elkövetőknek már nem kellett fizikailag jelen lenniük vagy adathordozót juttatniuk a számítógépbe ahhoz, hogy megfertőzzék azt, hanem mindez távolról is lehetségessé vált. Az első számítógépes vírus, amelynek nagy közéleti visszhangja lett, az 1988-as Morris féreg *(worm)* volt, amelyre több szervezet a számítógépek hálózatról való lekapcsolásával reagált.[87] A technológia széles körű használatának köszönhetően exponenciális ütemben növekedett az online gazdaság, így a cselekményekkel okozható kár többé nem néhány kósza távolsági hívás díja volt, hanem akár dollármilliós nagyságrendűre is rúghatott. 1999-ben az online elterjedt Melissa vírus 500 millió dolláros kárt okozott, készítőjét, David Smitht pedig öt év szabadságvesztés büntetésre ítélte a bíróság. A felhasználók és az üzleti érdekeiket védő gazdasági társaságok egyre jobban kezdtek tudatában lenni az új technológia által hordozott kockázatnak, az üzleti szférában előtérbe került az informatikai biztonság kérdése, és 1984–1987 között megjelentek az első vírusirtó szoftverek. Mivel a számítógép elleni ártó szándékkal elkövetett cselekmények egy globális hálózaton valósultak meg, az országhatárok is megszűntek, ami hamar megteremtette egyrészről a bűnügyi és igazságügyi együttműködés iránti igényt, másrészt a kiberbűncselekményekkel kapcsolatos anyagi jogi és eljárási szabályok közelítésére való törekvés iránti igényt. Az anyagi haszonszerzési céllal elkövetett kibertámadások mellett megjelentek az ideológiai, politikai indíttatású hackertámadások, hiszen az érintettek nagy száma, a viszonylag gyorsan okozható hatalmas károk kiválóan alkalmassá tették ezeket a cselekményeket arra, hogy az elkövetők a figyelem középpontjába és az újságok címlapjaira kerüljenek. 1996-ban egy fehér felsőbbrendűséget hirdető csoport egy tagja feltörte egy massachusettsi internetszolgáltató rendszerét, és arra használta a hálózatot, hogy a szolgáltató nevében rasszista üzeneteket küldjön szét.[88] Az átviteli rendszerek fejlődésével nőtt az átvitel sebessége, a felhasználói eszközök pedig egyre kedvezőbb áron, egyre növekvő tárkapacitással álltak rendelkezésre, ami a tartalommal kapcsolatos deliktumok (gyermekpornográfia, szerzői jogsértések) elterjedésének kedvezett.[89]

A 2000-es években jelentek meg és váltak igen gyorsan népszerűvé a közösségi oldalak, újabb felületet teremtve a kiberbűncselekményeknek. A közösségi hálóval és a tartalmak közvetlen közzétételének lehetőségével párhuzamosan megjelentek a világhálón az ember személyét és emberi méltóságát sértő cselekmények.

87 Kabay 2008: 29.
88 Hill–Marion 2016: 31.
89 Gercke 2011: 34.

Hamar egyértelművé vált, hogy a kibertérben megjelent közlések hatásukat tekintve ugyanolyanok, mint az élőszóban tett kijelentések, sőt jelentőségüket felerősíti, hogy a szó ugyan elszáll, de az internetre feltöltött tartalmak megmaradnak, és gyakorlatilag korlátlanul visszakereshetők bármikor bárki által. A magánjellegű üzenetváltások ugyanúgy hatnak az egyénekre, a bántó, sértő kifejezések éle nem tompul attól, hogy e-mail- vagy chatüzenetben érkeznek a címzetthez. Kialakult a *cyberbullying* jelensége, amelyre a jogalkotás annak ellenére sem tudott hatékonyan reagálni, hogy 2008-ban halálos áldozatot is követelt, amikor egy Megan Meier nevű tinédzser a folyamatos online zaklatás hatására öngyilkos lett. Az internethasználatra alkalmas mobil eszközök elterjedésével új sebezhető készülékek jelentek meg a kibertérben.

Az Egyesült Államokban először 1984-ben született olyan szövetségi törvény, amelyben kifejezetten informatikai bűncselekményekkel kapcsolatos rendelkezéseket is találunk, ez az 1984. évi átfogó bűnüldözési törvény (Comprehensive Crime Control Act, 1984). Az úgynevezett „hackertörvényt" azonban számtalan kritika érte, Marjie T. Britz szerint[90] például a jogszabály azért sem bizonyult hatékonynak, mivel a nyelvezete kétértelmű volt, ezenfelül túl nagy hangsúlyt fektetett a pénzügyi jellegű információkra. A rendelkezéseket 1986-ban módosította a számítógépes csalásról és számítógépes visszaélésekről szóló törvény (Computer Fraud and Abuse Act, 1986), amelynek a megalkotása óta több rendelkezése is módosult. A módosítások között említést érdemel az 1996. évi nemzeti információs infrastruktúra védelméről szóló törvény (National Information Infrastructure Protection Act, 1996), amely több ponton módosította elődjét, és megalkotására Marjie T. Britz szerint[91] azért volt szükség, mert az 1986-os törvény csak a hackerek, illetve az olyan egyének felelősségre vonása kapcsán volt alkalmazható, akik jogosulatlanul léptek be vagy jogosultságukat túllépve bent maradtak egy számítógépes rendszerben. Nem fedte le azonban az olyan egyéb bűncselekményeket, amelyeket számítógép felhasználásával követtek el, illetve amelyek számítástechnikai eszközökkel álltak kapcsolatban. A nemzeti információs infrastruktúra védelméről szóló törvény kiegészítette az 1986-os hackertörvényt olyan új tényállásokkal, amelyek a számítógépekhez kapcsolódó informatikai bűncselekményeknek jóval szélesebb körét fedik le.

Az informatikai bűncselekmények kapcsán említést kell tennünk a gyermekpornográfia elleni fellépéssel kapcsolatban született törvényekről is. A gyermekpornográfia ugyan nem tisztán informatikai jellegű bűncselekmény, de

90 Britz 2013: 191.
91 Britz 2013: 193.

az elkövetésében (gyermekpornográf anyagok elkészítése, tárolása, terjesztése) az internet kvázi anonim jellegének köszönhetően ma már domináns az információtechnológiai elem. Az Egyesült Államokban az első gyermekpornográfia kérdésével foglalkozó törvény az 1977. évi, a gyermekek szexuális kizsákmányolástól való védelméről szóló törvény volt, ez azonban még nem tartalmazott semmilyen technológiára utaló elemet. Az 1996. évi, gyermekpornográfiától való védelemről szóló törvény (Child Pornography Prevention Act – CPPA, 1996) azonban kiterjesztette a tilalmat azokra a képekre is, amelyeket digitálisan módosítottak, és ezáltal válnak gyermekpornográfiának minősülő anyagokká. Marjie T. Britz leírja,[92] hogy ez a rendelkezés sok vitát váltott ki, a Legfelsőbb Bíróság pedig később alkotmányellenessé nyilvánította azt. Az Ashcroft vs. Free Speech Coalition ügyben[93] a bíróság kimondta, hogy a gyermekpornográfia fogalma, amennyiben magában foglalja az olyan anyagokat, amelyekről úgy tűnik, hogy valódi gyermekeket ábrázolnak, alkotmánysértő. A döntésben a bíróság kifejtette, hogy az igazi gyermekeket ábrázoló pornográf anyagok betilthatók, mivel valódi gyermekek válnak áldozattá. A virtuális gyermekpornográfia azonban nem büntethető, mivel véleménynyilvánításnak minősül, és az ilyen anyagok megalkotása semmilyen emberi lénynek nem okoz sérelmet. Az Ashcroft-döntést követően fogadta el a kongresszus a gyermekek kizsákmányolása elleni büntetőeljárás-jogi intézkedésekről és egyéb eszközökről szóló törvényt 2003-ban (Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today [PROTECT], 2003).

1998-ban fogadták el a személyazonosság-lopás és személyazonosság-másolás elleni fellépésről szóló törvényt (Identity Theft and Assumption Deterrence Act [ITADA], 1998), amely az első olyan törvény, amely bűncselekménnyé nyilvánítja egy másik személy személyazonosságával való visszaélést. Részben a személyazonossággal kapcsolatos visszaéléseket szabályozza a 2003-ban elfogadott tisztességes és pontos hitelügyletekről szóló törvény (Fair and Accurate Credit Transactions Act [FACTA], 2003), amely olyan fogyasztóvédelmi rendelkezéseket tartalmaz, amelyek lehetővé teszik a személyazonosság-csalás, illetve -lopás hatékony bejelentését. 2004-ben a kongresszus elfogadta a személyazonosság-lopás büntetési tételének növeléséről szóló törvényt (Identity Theft Penalty Enhancement Act, 2004), amely növeli azoknak a személyazonosság-lopásoknak a büntetési tételét, amelyeket egy másik bűncselekmény elkövetése céljából hajtottak végre. A törvény továbbá kötelezővé teszi a szabadságvesztés büntetést az olyan bizalmi pozícióban lévő alkalmazottaknak,

92 Britz 2013: 194.
93 Casey 2012: 97.

illetve egyéneknek a vonatkozásában, akik személyazonosság-lopás elkövetése céljából adatokat loptak. 2008-ban vezették be a személyazonosság-lopással kapcsolatos rendelkezések végrehajtásáról és a kárpótlásról szóló törvényt (Identity Theft Enforcement and Restitution Act, 2008), amely kiterjesztette azoknak a tevékenységeknek a körét, amelyek személyazonosság-lopásnak minősülnek, további olyan intézkedéseket vezetett be, amelyek elősegítik az áldozatoktól ellopott vagyon visszaszerzését.

Az informatikai bűncselekmények európai története

A számítógépekkel kapcsolatos bűncselekményekkel sokáig csak a gazdasági bűncselekmények körében foglalkoztak. Az Európa Tanács 81(12) számú, gazdasági bűncselekményekről szóló ajánlása azt javasolja, hogy a tagországok rendeljék büntetni az olyan számítógépes rendszerekkel kapcsolatos cselekményeket, mint az adatlopások, a manipuláció és a titoksértés. Az ideológiai, haszonszerzési motivációval bíró hackerek Európában is viszonylag korán kialakították saját közösségeiket. 1981-ben Hamburgban alakult a Chaos Computer Club, amely a nyugatnémet posta sebezhetőségét kihasználva nagy összeget utalt át tagjainak bankszámláira. A pénzt egyébként később hiánytalanul visszaadták, az akcióval mindössze arra kívánták felhívni a figyelmet, hogy a német kormány kiberbiztonsági intézkedései nem megfelelők.[94]

1990-ben az Egyült Királyságban született meg a számítógépes visszaélésekről szóló törvény (Computer Abuse Act, 1990), az első olyan törvény, amely a számítógépbe történő jogosulatlan belépést büntetni rendelte. A jogszabály ellenére a hackerek kora nem áldozott le a szigetországban, a korszak egyik nagy sajtónyilvánosságot kapó rendszerfeltörését éppen egy brit, Data Stream felhasználónéven dolgozó hacker követte el. A brit tinédzser, aki az elkövetéskor mindössze 16 éves volt, betört az amerikai Griffiss légierőbázis, a NASA, valamint a Koreai Atomenergia Kutató Intézet rendszerébe. A cselekmény nemcsak a kritikus rendszerek és intézmények sebezhetőségére hívta fel a figyelmet, hanem arra is, hogy az online térben az országhatárok vajmi kevés jelentőséggel bírnak, így a szoros nemzetközi együttműködés elkerülhetetlen a területen. A 90-es évek megsokszorozódott incidenseire a reakció egy nemzetközi egyezmény volt. A G8-ak együttműködésének eredményeként született meg 2001-ben a számítástechnikai bűnözésről szóló egyezmény, amely jelentős lépés a számítógépes bűncselekmények egységes kriminalizálása felé. Az egyezményt, noha a maga nemében

94 Hill–Marion 2016: 33.

mérföldkőnek számít, több kritika is érte. Nagy Zoltán például kiemeli, hogy igen kevesen írták alá, ami azt jelentheti, hogy „az államok vagy nem veszik komolyan ezeket a bűncselekményeket, vagy nem kívánnak szembemenni bizonyos gazdasági, netán bűnözői körök érdekeivel”.[95]

Az informatikai bűncselekmények nemzetközi jogi forrásai

A nemzetközi szabályok kialakításának e körben különös jelentősége van, hiszen a számítógépes hálózatok és az internet határon átnyúló jellegűek, így könnyűszerrel lehet elkövetni különböző országokban ezzel kapcsolatos bűncselekményeket. A szabályozási eltérések csökkentése jogharmonizáció és a szabályok közelítése által szintén kulcsfontosságú, hiszen a jogrendszerek közötti eltérések ez esetben az elkövetőknek kedveznek, kialakulhatnak olyan informatikai paradicsomok, ahol nagyon enyhén büntetik a cselekmények elkövetőit, illetve a lebukás esélye is csekély. Bayer Judit szerint a nemzetközi egyezményekkel azért érdemes foglalkozni, mert megalkotásukat Magyarországon jogalkotás is követte, a jogalkotó folyamatosan próbál reagálni a gyors technológiai változásokra, és igyekszik a tényállásokat ehhez igazítani.[96]

Egyesült Nemzetek Szervezete (ENSZ)

Az ENSZ kiberbűncselekményekkel kapcsolatos tevékenységének számos ága van. A szervezet több fontos lépést tett az informatikai bűncselekmények által támasztott kihívások leküzdése érdekében, több nemzetközi egyezményt hozott létre, és több olyan dokumentumot bocsátott ki, amelyek még ma is állami jogszabályok alapját képezik. Ezek közül az alábbiak a legfontosabbak:

- a Gyermek jogairól szóló, New Yorkban, 1989. november 20-án kelt Egyezmény;
- az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről (1994);
- az ENSZ Közgyűlésének 55/63. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról;

[95] Nagy 2018: 475.
[96] Bayer 2003: 98–126.

- az ENSZ Közgyűlésének 56/121. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról;
- az ENSZ Közgyűlésének 60/177. számú és 64/211. számú határozatai;
- az ENSZ Közgyűlésének 65/230. számú határozata.

Az ENSZ Gyermekjogi Egyezménye

A gyermekjogi egyezményt 1989-ben fogadták el, Magyarországon pedig az 1991. évi LXIV. törvénnyel hirdették ki. Az egyezményben foglaltak fő célja a gyermekek védelme, amely kiterjed az online térrel összefüggésbe hozható cselekmények elleni fellépésre is. Az Egyezmény 34. cikke kifejezetten felhívja a részes államokat arra, hogy védjék meg a gyermekeket a nemi kizsákmányolás és a nemi erőszak minden formájától, amelybe beletartozik a gyermekpornográfia elleni küzdelem is. A gyermekjogi egyezményt kiegészíti három fakultatív jegyzőkönyv, amelyek közül az egyik a gyermekek kereskedelmi célú szexuális kizsákmányolásával foglalkozik. A fakultatív jegyzőkönyvet hazánkban a 2009. évi CLXI., a gyermekek eladásáról, a gyermekprostitúcióról és a gyermekpornográfiáról szóló, a Gyermek jogairól szóló egyezményhez fűzött Fakultatív Jegyzőkönyv megerősítéséről és kihirdetéséről szóló törvénnyel hirdették ki.

A fakultatív jegyzőkönyv lefekteti a gyermekek kizsákmányolásának fogalmi alapjait, és meghatározza a „gyermekpornográfia", valamint a „gyermekprostitúció" fogalmait. A fakultatív jegyzőkönyv 3. cikke kötelezettséget teremt a részes államok számára, a gyermekpornográfia előállításával és terjesztésével kapcsolatos cselekmények kriminalizálására.

Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről

Az ENSZ informatikai bűncselekményekkel kapcsolatos fellépésének alapját az ENSZ Közgyűlésének 45/121. számú határozata képezi. E határozat alapján az ENSZ 1994-ben kiadott egy kézikönyvet a számítógépes bűncselekmények megelőzéséről és kezeléséről. A dokumentum a maga idejében megteremtette a kiindulási alapját az informatikai bűncselekmények elleni összehangolt fellépésnek, noha ma már szinte teljesen elavultnak számít. A korabeli szabályrendszer még kizárólag a számítógépre *(computer)*

koncentrál, és nem veszi figyelembe azokat az információtechnológiai eszközöket, amelyek szintén szerepet játszanak a bűnözésben. A dokumentum még nem tesz különbséget a számítógépes bűncselekmények *(computer crime)* és a számítógéppel kapcsolatos bűncselekmények *(computer-related crime)* között, ezért a számítógépes deliktumokat együtt szabályozza. A két fogalom elválására csak később, az információtechnológiai elemet tartalmazó büntetendő cselekmények diverzifikálódása eredményeként került sor. A kézikönyv felsorolja a számítógépes bűncselekmények leggyakoribb típusait, amelyek a következők:

1. a számítógép manipulációjával elkövetett csalás *(fraud by computer manipulation),*
2. számítógépes hamisítás *(computer forgery),*
3. károkozás számítógépes adatokban vagy programokban, illetve a számítógépes adatok vagy programok megváltoztatása *(damage to or modifications of computer data or programs),*
4. jogosulatlan hozzáférés számítógépes rendszerekhez és szolgáltatásokhoz *(unauthorised access to computer systems and service),*
5. jogi védelem alá eső számítógépes programok jogosulatlan reprodukálása *(unauthorised reproduction of legally protected computer programs).*

A felsorolt cselekmények egy része változatlanul, más része pedig modernizált formájában ma is a büntetőszabályozás része.

Az ENSZ Közgyűlésének 55/63. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

2000-ben a Közgyűlés elfogadott egy újabb határozatot, amelyben már nem pusztán a számítógépről esik szó, hanem annál szélesebb körről, az információs technológiával való visszaélésről. A határozat szerint a részes államoknak a jogalkotásuk és gyakorlatuk révén biztosítaniuk kell, hogy ne jöjjenek létre olyan menedékek, védett zónák *(safe haven),* amelyek óvják azokat, akik visszaélnek a technológiákkal. A határozat, felismervén a kooperáció fontosságát, nagy hangsúlyt helyez a nemzetközi együttműködés erősítésére, és több intézkedéssel támogatja azt. Ezek:

1. Az információs technológiákkal való nemzetközi jellegű visszaélések esetében a nyomozó hatóságok együttműködésének, különösen a nyomozás és a vádemelés koordinációja az érintett államok között.

2. Az információmegosztás támogatása a bűncselekményekhez használt információs technológiákat érintő problémákkal kapcsolatban.
3. Közös támogatási rezsimek kialakítása, amelyek célja az információs technológiákkal való visszaélések időszerű kivizsgálásának és a keletkezett bizonyítékok összegyűjtésének és cseréjének biztosítása.

A közös célok elérése érdekében a Közgyűlés számos olyan intézkedést azonosított, amelyek segítenek az információs technológiákkal való visszaélések megelőzésében. Az intézkedések a következők:

1. A nyomozó hatóságok személyzetét ki kell képezni és felszereléssel kell ellátni az információs technológiákkal való visszaélések elleni hatékonyabb fellépés érdekében.
2. A jogrendszereknek védeniük kell az adatok és számítógépes rendszerek bizalmasságát, integritását és hozzáférhetőségét a jogosulatlan megkárosítással szemben, és biztosítaniuk kell, hogy a visszaéléseket büntetni rendeljék.
3. A jogrendszereknek lehetővé kell tenniük a bűnügyi nyomozásokkal kapcsolatos elektronikus adatok megőrzését, és az ezekhez való gyors hozzáférést.
4. A nyilvánosság figyelmét fel kell hívni az információs technológiákkal való visszaélések megelőzésének és üldözésének szükségességére.
5. Az új információs technológiákat a megvalósíthatóság keretein belül úgy kell tervezni, hogy megkönnyítsék a visszaélések megelőzését és felderítését, az elkövetők azonosítását és a bizonyítékok összegyűjtését.

A határozat azonban az információtechnológiával való visszaélések elleni fellépést célzó intézkedések támogatása mellett felismeri azt is, hogy egyes állami intézkedések szükségszerűen korlátoznak bizonyos alapjogokat. Ezért kifejezetten rendelkezik arról, hogy az információs technológiákkal való visszaélések elleni küzdelem olyan megoldások kifejlesztését igényli, amelyek számba veszik mind a személyes szabadságjogok és a magánélet védelmét, mind a kormányzat cselekvési lehetőségeinek megőrzését a visszaélések elleni küzdelemben.

Az ENSZ Közgyűlésének 56/121. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

2002-ben az ENSZ Közgyűlése újabb határozatot fogadott el ugyanebben a tárgyban. A határozatban az ENSZ sürgeti a tagállamok közötti együttműködés erősítését, ugyanakkor felismeri, hogy problémákat okozhatnak az államok közötti különbségek az információs technológiákhoz való hozzáférésben és azok felhasználásában. Felhívja a tagállamokat arra, hogy az információs technológiákkal való visszaélések visszaszorítására koncentráló nemzeti jogszabályok, politikák és gyakorlat kialakításakor vegyék figyelembe a nemzetközi és regionális szervezetek munkáját és eredményeit.

Az ENSZ Közgyűlésének 60/177. számú és 64/211. számú határozatai

Az ENSZ Közgyűlése a 11. bangkoki kongresszusa után fogadta el a 60/177. számú határozatot, amelyben a nemzetközi együttműködés erősítésére mint a megelőzés fontos eszközére hívja fel a figyelmet. 2010-ben fogadták a Közgyűlés 64/211. számú határozatát, amely egyszerre foglalkozik a kiberbűnözés és a kiberbiztonság kérdéseivel. Mindkét területtel összefüggésben javasolja az állami szervek és hatóságok szervezetének és működésének felülvizsgálatát, amelyhez egy önértékelési rendszert is rendelkezésre bocsát. A jogszabályok és a szervezetrendszer felülvizsgálatának igényét az információtechnológiával összefüggő bűncselekmények rohamos fejlődése teremtette meg, amelynek következtében az ENSZ korábban megalkotott dokumentumai gyorsan elavulnak.

Az ENSZ Közgyűlésének 65/230. számú határozata[97]

Az ENSZ Közgyűlésének 65/230. számú határozata felhívta a részes államokat a salvadori deklarációval[98] összhangban egy nyílt végű kormányközi szakértői csoport létrehozására, amelynek feladata a kiberbűncselekmények és az azokra adott tagállami válaszok átfogó vizsgálata.[99] A szakértői csoport feladata a jó gyakorlatok megosztása,

97 Az ENSZ Közgyűlésének 65/230. számú határozata a bűnmegelőzésről és büntető igazságszolgáltatásról szóló tizenkettedik ENSZ Kongresszusról.

98 United Nations 2010.

99 9. pont.

valamint a tájékoztatásnyújtás a nemzetközi és nemzeti jogszabályokról.[100] Az ajánláshoz fűzött melléklet elismeri a magán- és az állami szektor közötti partnerség fontosságát a bűncselekmények elleni fellépésben és a megelőzésben,[101] és kimondottan felhívja a magánszféra szereplőit arra, hogy támogassák a gyermekek interneten történő szexuális kizsákmányolása elleni küzdelmet.[102] Az ajánlásnak megfelelően létrejött a kiberbűnözéssel foglalkozó globális program (*Global Programme on Cybercrime*[103]).

Interpol

Az Interpol célja, hogy globálisan koordinálja az információtechnológiai elemet tartalmazó bűncselekmények (vagy ahogyan a szervezet honlapja nevezi őket: digitális bűncselekmények) felderítését és megelőzését. Ennek érdekében felállította a Digital Crime Centre-t, amely kutatás-fejlesztési tevékenységet lát el. Az Interpol jelenleg három területen működik, ezek:

1. Harmonizáció: a kiberbűncselekmények elleni hatékony fellépés alapvető eleme a hatékony bűnüldözés, az Interpol azonban felismerte, hogy az összes érintett szektort – privát, akadémiai, közintézmények – be kell vonni a kibertér biztonságossá tételébe. Ennek érdekében arra törekszik, hogy összehangolja a különböző szektorok munkáját, illetve elősegíti, hogy megosszák egymással a tapasztalataikat.
2. Kapacitásbővítés: az Interpol szerint biztosítani kell, hogy a rendőrség tartsa a tempót a technológiai fejlődéssel, és rendelkezzen a szükséges szakértelemmel, hogy megfelelően tudják kezelni a folyamatosan változó digitális bűncselekményeket mind nemzeti, mind nemzetközi szinten.
3. Operatív és forenzikus tevékenység: az Interpol támogatja a tagországokat, az informatikai elemet tartalmazó nyomozásokat, valamint segíti a közös műveletek koordinációját. Ennek érdekében működteti a Cyber Fusion Centre-t, amely segítséget nyújt az Interpol tagországainak a nyomozás minden szakaszában, valamint a kártékony internetes tevékenységet valós időben vizsgálja és elemzi. Emellett igazságügyi szakértői labort *(Digital Forensics Laboratory)* működtet.

[100] 10. pont.
[101] Melléklet 34. pont.
[102] 40. pont.
[103] UNODC [é. n.].

Fontos eleme az Interpol munkájának az a képi adatbázis, amely a gyermekek szexuális kizsákmányolását ábrázoló felvételeket tartalmaz. Az adatbázis célja az áldozatok azonosítása, valamint a felderítés gyorsítása. Az Interpol állandóan működő kapcsolattartási pontot is üzemeltet, amely szintén a nemzetközi együttműködés gyorsítását szolgálja.

OECD

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) 1983 és 1985 között *ad hoc* bizottságot hozott létre a számítógépes bűnözés körébe tartozó bűncselekmények rendszerezése céljából. A bizottság munkájának eredményeként 1985-ben jelentés készült, amely három részre tagolható: a) általános alapelvek; b) rendőri és igazságszolgáltatási alapelvek; c) azon irányelvek, amelyek betartásával garantálható az alapvető etikai szabályok védelme, illetve amelyekkel javítható az egyes felhasználók védelme. Az 1985-ös ajánlást követően az OECD rendszeresen foglalkozott az informatikai bűncselekmények egyes aspektusaival, és az évek során több dokumentumot is kibocsátott. 2005-ben adták ki az OECD jelentését a spamek fejlődő országokra gyakorolt hatásáról,[104] míg 2008-ban az online személyiséglopásról szóló dokumentum,[105] 2009-ben pedig a kártékony szoftverekről szóló jelentés[106] látott napvilágot. 2008-ban Szöulban a Miniszteri Bizottság elfogadta az internetes gazdaság jövőjéről szóló deklarációt, amelyben felhívta a szervezetet, hogy vizsgálja meg, mi az internet egyes szereplőinek – köztük a közvetítő szolgáltatóknak – a szerepe az olyan közérdekű célok elérésében, mint a biztonsági fenyegetések elleni küzdelem. Az OECD a vizsgálat eredményeit 2011-ben megjelent tanulmányában összegezte.[107] A tanulmányban szó esik az internetes közvetítő szolgáltatók globális információáramlásban betöltött szerepéről, az internetszolgáltatók és a *malware*-ek kapcsolatáról, a jogellenes tartalmakról és a gyermekek számára nem megfelelő tartalmakról, az illegális szerencsejátékról, a szerzői jogsértésekről, továbbá az illegális árukat és szolgáltatásokat kínáló piacterekről.

Az OECD kiemelten foglalkozik a gyermekek online térben való védelmével. A szervezet 2012-ben tett közzé egy jelentést[108] azokról a kockázatokról, amelyek

104 OECD 2005.
105 OECD 2009a.
106 OECD 2009b.
107 OECD 2011a.
108 OECD 2011b.

a gyermekeket érintik, illetve azokról a szakpolitikákról, amelyek a védelmüket szolgálják. A jelentés alapján az OECD ugyanebben az évben egy ajánlást is megfogalmazott.[109]

Az informatikai bűncselekmények elleni fellépés európai dimenziói

Az informatikai bűncselekmények elleni európai fellépés fő irányvonalait az Európai Unió, valamint az Európa Tanács határozzák meg. A következőkben részletesen is áttekintem az általuk megalkotott joganyagot.

Európa Tanács

Az Európa Tanács egy regionális nemzetközi szervezet, amely kormányközi együttműködés keretében jött létre. A szervezet jelenleg 46 tagot számlál. Az Európa Tanács mindig különös figyelmet fordított az új technológiákkal összefüggő szabályozási kérdésekre. A szervezet már 1976-ban kiemelte,[110] hogy a számítógéppel kapcsolatos bűncselekmények nemzetközi természetűek, ezért ennek megfelelően kell őket kezelni, noha ekkor a szervezet még nem tekintette önálló kategóriának ezeket a cselekményeket, hanem a gazdasági bűncselekmények részeként kezelte őket.

A Miniszteri Bizottság R (89) 9 számú ajánlása a számítógéppel kapcsolatos bűnözésről

Az Európa Tanács Miniszteri Bizottsága 1985-ben egy szakértői bizottság felállításáról döntött, amelynek a feladata a számítógépes bűncselekmények *(computer crime)* jogi vonatkozásainak vizsgálata volt. A kutatás eredményei nyomán a Miniszteri Bizottság ajánlást adott ki a számítógéppel kapcsolatos bűncselekményekkel *(computer related crimes)* kapcsolatban,[111] amelyben elemezte azokat a büntető anyagi jogi rendelkezéseket, amelyek az elektronikus bűncselekmények elleni harchoz – beleértve a számítógépes csalást és hamisítást – szükségesek. Az ajánlás hangsúlyosan szól

109 OECD 2012.

110 Twelfth Conference of Directors of Criminological Research Institute.

111 Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems.

az ilyen cselekmények határokon átnyúló természetéről, emiatt pedig szorgalmazza a jogszabályok és a gyakorlat harmonizációját.[112] A nemzeti jogalkotás egységesítésének elősegítése érdekében az ajánlás melléklete konkrét modelljogszabályt is felvázol. A dokumentum összesen tizenkét tényállást különböztet meg, amelyeket két csoportra oszt: az első egy úgynevezett „minimumlista", amely nyolc tényállást, a második egy opcionális lista, amely négy tényállást tartalmaz.

A minimumlista elemei a következők:

1. Számítógéppel kapcsolatos csalás *(computer-related fraud):* Aki azzal a szándékkal, hogy a maga vagy más személy számára jogtalan gazdasági előnyhöz jusson, számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, illetőleg hozzáférhetetlenné tesz, vagy az adatfeldolgozást bármilyen egyéb módon befolyásolja, úgy, hogy azok hatással vannak az adatfeldolgozás eredményére, ezáltal más személynek gazdasági vagy birtokbeli kárt okoz, számítógéppel kapcsolatos csalást követ el.
2. Számítógépes hamisítás *(computer forgery):* Aki a nemzeti jog által meghatározott módon vagy körülmények között számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, illetőleg hozzáférhetetlenné tesz, vagy az adatfeldolgozást bármilyen egyéb módon befolyásolja, úgy, hogy az megfelel a hamisítás bűntettének, amennyiben az ilyen típusú bűncselekmények hagyományos tárgyára tekintettel követte el, számítógépes hamisítást követ el.
3. Károkozás számítógépes adatokban és programokban *(damage to computer data or programs):* Aki számítógépes adatot vagy programokat jogtalanul töröl, károsít, eltérít vagy hozzáférhetetlenné tesz, kárt okoz.
4. Számítógépes szabotázs *(computer sabotage):* Aki azzal a szándékkal, hogy egy számítógép vagy telekommunikációs rendszer működését gátolja, számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl vagy hozzáférhetetlenné tesz, a számítógépes rendszer működését befolyásolja, számítógépes szabotázst követ el.
5. Jogosulatlan hozzáférés *(unauthorised access):* Aki egy számítógépes rendszerbe vagy számítógépes hálózatba jogtalanul, a biztonsági intézkedéseket kijátszva belép, jogosulatlan hozzáférést követ el.

[112] Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems 15b. cikk.

6. Jogosulatlan lehallgatás *(unauthorised interception):* Jogosulatlan lehallgatás olyan kommunikációtechnikai módszerrel, amely számítógépes rendszer vagy hálózat útján valósul meg.
7. Védett számítógépes programok jogellenes reprodukálása *(unauthorised reproduction of a protected computer program):* Aki egy jog által védett számítógépes programot jogtalanul reprodukál, terjeszt vagy a nyilvánosság számára hozzáférhetővé tesz, bűncselekményt követ el.
8. Topográfiák jogosulatlan reprodukálása *(unauthorised reproduction of a topography):* Aki egy jog által védett félvezető termék topográfiáját jogtalanul reprodukálja, vagy a félvezető terméket reprodukálás céljából jogtalanul hasznosítja, importálja, vagy jogtalanul félvezető terméket gyárt topográfia használatával, bűncselekményt követ el.

Az opcionális lista elemei pedig az alábbiak:

1. Számítógépes adatok vagy programok megváltoztatása *(alteration of computer data or computer programs):* Aki a számítógépes adatokat vagy programokat jogtalanul megváltoztatja, bűncselekményt követ el.
2. Számítógépes kémkedés *(computer espionage):* Aki kereskedelmi vagy üzleti titkot jogtalanul, illetve jogi felhatalmazás nélkül, helytelen eszközökkel megszerez, közzétesz, átruház vagy felhasznál, azzal a szándékkal, hogy a titok jogosultjának gazdasági veszteséget okozzon, illetőleg magának vagy másnak jogtalan gazdasági előnyt szerezzen, bűncselekményt követ el.
3. Számítógép jogosulatlan használata *(unauthorised use of a computer):* Aki a számítógépes rendszert vagy hálózatot jogosulatlanul oly módon használja, hogy
   – elfogadja a jelentős kockázatát annak, hogy a rendszer használatára jogosult személynek kára keletkezik, vagy a rendszerben, illetve annak működésében kár keletkezik;
   – szándéka arra irányul, hogy a rendszer használatára jogosult személynek kára keletkezzen, vagy a rendszerben, illetve annak működésében kár keletkezzen;
   – a rendszer használatára jogosult személynek kára keletkezik, vagy a rendszerben, illetve annak működésében kár keletkezik, bűncselekményt követ el.
4. Védett program jogosulatlan használata *(unauthorised use of a computer program):* Aki jog által védett és jogtalanul reprodukált számítógépes programot jogtalanul használ azzal a szándékkal, hogy magának vagy másnak jogtalan gazdasági előnyt szerezzen, vagy a jog tulajdonosának kárt okozzon, bűncselekményt követ el.

Noha az ajánlás kétségtelenül nagy újítást hozott a maga idejében, hamar meghaladottá vált, és számos kritika érte. Siegler Eszter szerint[113] a minimum- és fakultatív lista nem jó, mert a felvázolt tényállások között sok átfedés van, illetve hiányzik a számítógéppel kapcsolatos bűncselekmények fő típusainak éles elhatárolása, és ez a szabályozást kiszámíthatatlanná, áttekinthetetlenné teszi. Egyetértve az előbbiekkel, szükséges rávilágítani arra, hogy az ajánlásban szereplő tényállásokat csak nagy vonalakban sikerült felvázolni, a pontatlan megfogalmazások pedig nem feltétlenül a nemzeti jogszabályok közeledéséhez, hanem éppen az ellentétek szaporodásához vezetnek. A számítógépes adatok vagy programok megváltoztatása címszó alatt például csak annyit ír az ajánlás, hogy aki számítógépes adatokat vagy programokat megváltoztat, bűncselekményt követ el, azonban nem rendelkezik arról, hogy a megváltoztatás csak szándékosan történhet, vagy akár gondatlanságból is, így a részes államok jogalkotóira van bízva ennek meghatározása.

A Miniszteri Bizottság R (95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról

1995-ben a Miniszteri Bizottság újabb ajánlást fogadott el, amelyben nem az anyagi jogi szabályokra, hanem az eljárásjogra fókuszált. Az ajánlás hét pontban foglalja össze azokat a problémákat, amelyek a büntetőeljárás során felmerülhetnek, amennyiben informatikai bűncselekményekről van szó. Noha az ajánlás 1995-ben született, a felsorolt problémák még napjainkban is megfigyelhetők.

1. Átvizsgálás és lefoglalás *(search and seizure):* A számítógépes rendszerek átvizsgálásának, valamint a bennük tárolt adatok lefoglalásának és az átvitel közben keletkező adatok lehallgatásának szabályozását világosan el kell határolni, vagyis ezeket az intézkedéseket jogilag egyértelműen kell felvázolni, és konzekvensen kell alkalmazni. A büntetőeljárási jogoknak lehetővé kell tenniük azt, hogy a nyomozó hatóságok átvizsgálják a számítógépes rendszereket, és lefoglalják az adatokat hasonló feltételek mellett, mint a tradicionális házkutatás és lefoglalás esetében. A rendszerért felelős személyt tájékoztatni kell a rendszer átvizsgálásáról és a lefoglalt adatok típusáról. Azoknak a jogorvoslatoknak, amelyek alkalmazhatók az általános házkutatás és lefoglalás esetében, ugyanúgy alkalmazhatónak kell lenniük a számítógépes rendszerek átvizsgálása

[113] Siegler 1997: 736–742.

és a bennük tárolt adatok lefoglalása esetében. Az átvizsgálás végrehajtása során a nyomozó hatóságoknak megfelelő biztosítékok mellett rendelkezniük kell azzal a jogosítvánnyal, hogy kiterjesszék a keresést egyéb joghatóságuk alá tartozó számítógépes rendszerekre, amelyek hálózaton keresztül vannak összekapcsolva, illetve lefoglalják a bennük található adatokat, amennyiben azonnali intézkedésre van szükség. A hálózati eszközökön található adatok lefoglalása napjainkban a felhőszolgáltatásokban tárolt adatok kapcsán szokott felmerülni. Ahol az automatikusan feldogozott adat megfelel egy tradicionális dokumentumnak, a büntetőeljárás-jog dokumentumok átvizsgálásával és lefoglalásával kapcsolatos szabályainak ezekre is ki kell terjednie.

2. Megfigyelés *(technical surveillance):* Az információtechnológia és a telekommunikáció konvergenciája miatt a bűnügyi nyomozások során alkalmazott technikai intézkedéseket (például telekommunikáció lehallgatása) felül kell vizsgálni, és ahol szükséges, módosítani kell, az alkalmazhatóságuk biztosítása végett. Ez a rész tárgyalja azokat a problémákat, amelyek a megfigyeléssel, lehallgatással és forgalmi adatok összegyűjtésével kapcsolatosak, különös figyelmet fordítva a jelenlegi szabályok felülvizsgálatának kérdésére.
3. A nyomozó hatóságokkal való együttműködés kötelezettsége *(obligations to co-operate with the investigating authorities):* A legtöbb jogrendszer megengedi, hogy a nyomozó hatóságok utasítsanak bizonyos személyeket a birtokukban lévő tárgyak átadására, amennyiben azokra a bizonyítás során szükség van. Ennek mintájára rendelkezéseket kell hozni arra is, hogy utasíthassák ezeket a személyeket arra, hogy a birtokukban lévő információs rendszerben tárolt adatokat a szükséges formában átadják a nyomozó hatóságnak. A nyomozó hatóságoknak rendelkezniük kell azzal a jogosítvánnyal, hogy utasítsák azokat a személyeket, akiknek adataik vannak az információs rendszerben, hogy átadják az információs rendszerhez, valamint a benne tárolt adatokhoz való hozzáféréshez szükséges összes információt (például felhasználói fiókokhoz tartozó azonosítókat, jelszavakat). A büntetőeljárási jognak azt is biztosítania kell, hogy hasonló utasítást lehessen adni olyan személyeknek is, akiknek ugyan nincsenek saját adataik a rendszerben, ám információval rendelkeznek az információs rendszer működéséről vagy azokról az intézkedésekről, amelyeket a benne tárolt adatok védelmében alkalmaztak (például rendszergazdák). A telekommunikációs szolgáltatásokat nyilvános vagy magánhálózatokon kínáló szolgáltatókra speciális kötelezettségeket kell telepíteni, hogy olyan információkat adjanak át, amelyekkel azonosítható a felhasználó, amennyiben

a nyomozó hatóság erre utasítja őket. Ez az ajánlás tulajdonképpen a később széles körben alkalmazottá vált adatmegőrzés és a tárolt adatok átadásának alapjait teremti meg. Az adatmegőrzéssel és azok átadásával kapcsolatos problémakör napjainkban továbbra is aktuális, egyre gyakrabban merül fel ugyanis az, hogy a tárhelyszolgáltatók, tartalomközléssel megvalósuló bűncselekmények esetén a közösségimédia-szolgáltatók rendelkeznek adatokkal, amelyek nyomozási értékkel bíró információt hordozhatnak.

4. Elektronikus bizonyítékok *(electronic evidence):* El kell ismerni a közös igényt az elektronikus bizonyítékok oly módon történő összegyűjtésére, megőrzésére és bemutatására, amely a legjobban biztosítja és tükrözi integritásukat és hitelességüket mind a nemzeti büntetőeljárásban, mind a nemzetközi együttműködésben. Ezért azokat az eljárásokat és technikai módszereket, amelyek az elektronikus bizonyítékok kezelésére vonatkoznak, tovább kell fejleszteni oly módon, amely biztosítja az államok közötti kompatibilitást.
5. Titkosítás használata *(use of encryption):* Olyan intézkedéseket kell tenni, amelyek minimalizálják a bűncselekmények nyomozásakor a kriptográfia használatának negatív hatásait, anélkül, hogy a feltétlenül szükségesnél jobban korlátoznák a titkosításra használt technológiák legitim felhasználását.
6. Kutatás, statisztika, képzés *(research, statistics and training):* Tovább kell vinni az informatikai bűncselekményekről rendelkezésre álló adatok elemzését, beleértve a *modus operandi* és a műszaki szempontok vizsgálatát. Meg kell fontolni az ilyen speciális szakértelmet igénylő bűncselekmények vizsgálatára egy speciális szakosított egység létrehozását.
7. Nemzetközi együttműködés *(international co-operation):* Az átvizsgálás jogának kiterjesztését más számítógépes rendszerekre azokban az esetekben is alkalmazni kell, amikor a rendszer más ország joghatósága alá tartozik, amennyiben azonnali intézkedésre van szükség. Annak érdekében, hogy elkerülhető legyen az állami szuverenitás, illetve a nemzetközi jog megsértése, az ilyen kiterjesztett átvizsgálásra és lefoglalásra egyértelmű jogi szabályokat kell létrehozni. Elérhetőnek kell lennie olyan gyorsított és megfelelő eljárásoknak, valamint egy összekötő rendszernek, amelyek alapján a nyomozó hatóságok igényelhetik, hogy a külföldi hatóságok gyűjtsék össze a bizonyítékokat. A megkeresett hatóságoknak felhatalmazással kell rendelkezniük a telekommunikációval kapcsolatos forgalmi adatok megosztására, a telekommunikáció lehallgatására, illetve a forrásának azonosítására. E célból a jelenlegi kölcsönös jogsegély eszközeit ki kell egészíteni.

A számítástechnikai bűnözésről szóló egyezmény és a kiegészítő jegyzőkönyvek[114]

Az Európa Tanács számítástechnikai bűnözésről szóló egyezményét (Cybercrime Egyezmény) 2001-ben fogadták el Budapesten, 2011 júliusáig 47 állam írta alá, és 31 ratifikálta. Az Egyezményhez később két kiegészítő jegyzőkönyvet fűztek, az első a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló,[115] a második pedig a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról szóló[116] kiegészítő jegyzőkönyv. Az egyezmény azon felül, hogy dogmatikailag letisztultan csoportosítja a bűncselekményeket, definiálja a számítógépes környezetben megjelenő technikai fogalmakat, és mind a mai napig az alapkövét képezi a területen folyó jogalkotásnak.

Az értelmező rendelkezések körében az egyezmény több alapfogalmat definiál, úgymint számítástechnikai rendszer *(computer system),* számítástechnikai adat *(computer data),* szolgáltató *(service provider),* illetve forgalmazási adat *(traffic data),* viszont a kiberbűncselekmény *(cybercrime)* fogalmának meghatározásával adós marad. Az egyezmény értelmezésekor zavaró lehet, hogy az új Btk. hatálybalépése óta a magyar büntetőjog már nem használja sem a számítástechnikai rendszer, sem a számítógépes/számítástechnikai bűncselekmény fogalmát, hiszen azokat a valamivel tágabb, információs rendszer, illetve informatikai/információs bűncselekmények fogalmakra cserélte. Az egyezmény és a magyar büntető törvénykönyv a számítástechnikai rendszer, valamint az információs rendszer fogalmakat nagyrészt ugyanazzal a tartalommal töltötte ki. Ha vetünk egy pillantást a Btk. kommentárjára,[117] kiderül, hogy a magyar jog az információs rendszer fogalma alatt nemcsak számítástechnikai, hanem telekommunikációs eszközöket is ért, az információs rendszer fogalma tehát elvben hazánkban tágabb, mint a számítógépes rendszeré. A nemzetközi egyezményekben azonban többnyire nincsen ilyen megkülönböztetés, így ezeket a fogalmakat jelen kötet is váltakozva használja. Emellett szól az az érv is, hogy manapság azonban

[114] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

[115] A számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv.

[116] A számítástechnikai bűnözésről szóló egyezményhez csatolt, a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról szóló második kiegészítő jegyzőkönyv.

[117] Szomora 2019c: 1049–1083.

a számítástechnikai eszközök és a telekommunikációs eszközök nem határolhatóak el élesen egymástól, példaként említve egy okostelefont, amely egyszerre telefon és miniatűr számítógép.

Az egyezmény második része a büntető anyagi jogi szabályokkal foglalkozik, és négy csoportra osztja a bűncselekményeket. Az első csoportot képezik a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények, amelyek mindegyikét tartalmazza a magyar Btk. is. Ebbe a csoportba az alábbi bűncselekmények tartoznak:

- jogosulatlan belépés,
- jogosulatlan kifürkészés,
- számítástechnikai adat megsértése,
- számítástechnikai rendszer megsértése,
- eszközökkel való visszaélés.

A második csoportba a számítógéppel kapcsolatos bűncselekmények tartoznak, amelyek az alábbiak:

- számítógéppel kapcsolatos hamisítás,
- számítógéppel kapcsolatos csalás.

Ezen a ponton az egyezmény némiképp eltér attól a csoportosítástól, amely a magyar jogirodalomban megszokott. Hazánkban ugyanis általában az informatikai bűncselekményeket két csoportra szokás osztani: tisztán informatikai jellegű bűncselekményekre, illetve a hagyományos, számítógéppel elkövetett bűncselekményre. Előbbi csoportba azok a deliktumok tartoznak, amelyeknek az elkövetési tárgya az információs rendszer, a hálózat, illetve a bennük tárolt adat, utóbbi csoportba pedig azok a bűncselekmények tartoznak, amelyeknél a számítógép az elkövetés eszköze, így ez a csoport nagyon színes képet mutat. A nálunk meghonosodott csoportosításból némiképp kilóg az információs rendszer felhasználásával elkövetett csalás bűntette, hiszen ezt a tisztán informatikai bűncselekmények közé sorolják, azonban nem jellemző rá az informatikai bűncselekmények összes tulajdonsága. Az információs rendszer felhasználásával elkövetett csalások tekintetében az elkövetés tárgya nem a számítógép, az elkövető cselekménye sem a rendszer működésében, sem az abban tárolt adatokban nem okoz kárt, és nem akadályozza azok megfelelő működését sem. A harmadik cím a számítástechnikai adatok tartalmával kapcsolatos bűncselekményekről, a negyedik pedig a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekményekről szól. Előbbi kategóriába a gyermekpornográfiával kapcsolatos bűncselekmények tartoznak.

Az egyezmény első kiegészítő jegyzőkönyve kriminalizálja a rasszista és faji megkülönböztetést, a bántalmazást, valamint a népirtás és az emberiesség elleni bűncselekmények tagadását, következményeinek minimalizálását, elfogadását, illetve támogatását. E magatartásokat azért egy kiegészítő jegyzőkönyv formájában kellett hozzákapcsolni az Egyezményhez, mert 2001-ben nem sikerült egyetértésre jutni a nevezett deliktumok tartalmáról. Különösen a gyűlöletbeszéd jellegű cselekmények esetében bizonyult jelentősnek az eltérés az egyes országok szabályozása között, a kulturális és szabályozási különbségek miatt ugyanis a védendő tulajdonságok listájában nehezen sikerült megállapodni. A kompromisszumként elfogadott végleges szöveg csak fajon, bőrszínen, leszármazáson vagy a nemzeti, etnikai hovatartozáson, illetve szűk körben a valláson alapuló rasszizmussal és idegengyűlölettel összefüggő magatartásokat kriminalizálja, egyéb védett tulajdonságokról mint a nem, a szexuális hovatartozás vagy a fogyatékosság nem rendelkezik. A kiegészítő jegyzőkönyvet végül csak 35 ország ratifikálta.[118]

Az anyagi jogi szabályokat ért kritikán felül az egyezmény rendszertani szempontból is kifogásolható, a csoportképzés ugyanis nem egyértelmű. A gyermekpornográfia és szerzői jogok megsértése deliktumok külön szerepeltetése a tartalommal kapcsolatos bűncselekményektől például szükségszerűtlen, és legfeljebb csak a cselekmények nagyobb tárgyi súlyával indokolható. A tisztán informatikai bűncselekmények csoportja nem szorul átalakításra, az információs rendszerrel kapcsolatos bűncselekmények esetében azonban célszerűnek tartanám a kategórián belüli bűncselekmények áttekinthetőbb tagolását. Az információs rendszerrel kapcsolatos bűncselekmény jó összefoglaló elnevezés lehet azokra a deliktumokra, amelyeknél a számítógép csak az elkövetés eszköze, azonban úgy vélem, ezen a kategórián belül további alegységekre van szükség, hogy ezt a nagyon sokszínű bűncselekményhalmazt némiképp rendszerezni lehessen. Az Egyezmény egyik nagy hibájának tartom, hogy nem fogja át teljeskörűen azokat a magatartásokat, amelyeket manapság jellemzően információs rendszer felhasználásával követnek el. Az egyezmény nem vesz figyelembe olyan új trendeket, mint a *cyberbullying* (internetes zaklatás), *sextortion,* valamint a személyazonosság-lopás *(identity-theft),* a botnetek elterjedése, az internet terrorista célú használata, pedig ezek tipikusan olyan cselekmények, ahol a számítógépes hálózat, illetve az internet kulcsszerepet játszik. Ennek feltehetően az az oka, hogy egy nemzetközi egyezmény

[118] A 189. szerződés aláírásának és ratifikálásának jegyzékét az Európa Tanács vezeti. Lásd Council of Europe: Chart of signatures and ratifications of Treaty 189.

kiegészítése és módosítása körülményes és hosszadalmas feladat, ezért nem várható el tőle, hogy alkalmazkodjon az ilyen folyamatosan változó és bővülő magatartásokhoz.

Az Egyezmény harmadik része az eljárási szabályokat, negyedik része pedig a nemzetközi együttműködés szabályait tartalmazza. Az eljárási szabályok a magyar jogrendszerben is megtalálhatók, ilyen a tárolt elektronikus adat gyors megőrzése, amely a Be.-ben a lefoglalás szabályai között, az elektronikus adat lefoglalása és a megőrzésére kötelezés címen szerepel, illetve a közlésre kötelezés, amelyre az adatszerző tevékenység körében az adatkérés teljesítésére vonatkozó szabályok vonatkoznak. Nem ismeri viszont a magyar jogrendszer a házkutatás kiterjesztését más rendszerre. Az Egyezmény alapján ugyanis, ha a nyomozó hatóság alappal feltételezheti, hogy a keresett adatok egy része más információs rendszerben található, és ezek az adatok a kiinduló rendszer számára hozzáférhetők, akkor a hatóság haladéktalanul kiterjesztheti az átvizsgálást vagy a más hasonló módon történő hozzáférést a másik rendszerre is. Ilyen lehet például egy felhő vagy egy FTP-szerver. Érdekes kérdés viszont, hogy mi a teendő abban az esetben, ha a felhasználó a számítógépén keresztül hozzáfér egy olyan FTP-szerverhez, amelyben jogsértő tartalmakat (például gyermekpornográfiát) találnak. Ebben az esetben ugyanis az adathordozó, vagyis a szerver egy teljesen más helyen található, és a felhasználó számítógépétől függetlenül működik és elérhető. Az adathordozó lefoglalása csak abban az esetben lehetséges, amennyiben a nyomozó hatóság a házkutatást erre a helyszínre fizikailag is kiterjeszti. Problémát okozhatnak továbbá az olyan új technológiák, amelyekre az Egyezmény elfogadásakor még nem gondoltak, így a VOIP, amely a távközlés olyan formája, ahol a beszélgetés nem hagyományos telefonhálózaton, hanem az interneten vagy más adathálózaton folyik. VOIP használata esetén a hívó fél tartózkodási helye az IP-cím alapján határozható meg, a felhasználó nem köteles a hagyományos számgazdálkodás szerinti azonosítókat használni (például egy Skype-felhasználónév akár betűkből is állhat). Ugyanakkor az úgynevezett *vocoder*ral adattá alakított hangot továbbító partner elrejtheti az IP-címét akár VPN vagy TOR használatával.

A Cybercrime Egyezmény eljárási rendelkezéseit egészíti ki a második, 2022-ben elfogadott kiegészítő jegyzőkönyv. E kiegészítő jegyzőkönyv már reagál arra a trendre, amely a közvetítő szolgáltatások aktív, eljárást segítő szerepét várja el. A büntetőeljárás szempontjából releváns adatok gyors megszerzését elősegítendő, a kiegészítő jegyzőkönyv olyan eljárási szabályokat vezet be, amelyek lehetővé teszik az egyes szolgáltatók közvetlen megkeresését, ahelyett, hogy végig kelljen járni a nemzetközi jogsegély bonyolult és hosszadalmas útját. A 6. cikk alapján a részes államoknak lehetőséget kell biztosítaniuk doménregisztrációs adatok,

a 7. cikk alapján előfizetői adatok közvetlen beszerzésére. A kiegészítő jegyzőkönyv nagyobb hangsúlyt helyez a hatóságok közötti együttműködésre is: a részes államok hatóságainak el kell ismerniük egymás adatkérésre és adatmegőrzésre vonatkozó határozatait, biztosítaniuk kell a közös nyomozócsoportokban való részvételt, illetve a sürgős jogsegélykérelmek teljesítését.

Az Európa Tanács terrorizmus megelőzéséről szóló, Varsóban, 2005. május 16-án kelt Egyezménye

Az Európa Tanács terrorizmus megelőzéséről szóló egyezményét hazánkban a 2011. évi II. törvény[119] hirdette ki. Az egyezmény célja a terrorizmus megelőzése, valamint az azzal járó negatív hatások csökkentése.[120] Az egyezmény a terrorcselekmény fogalmát nem határozza meg, hanem azt a nemzetközi jogra bízza. Az egyezmény a terrorizmus elleni fellépés terén különös jelentőséget tulajdonít a polgárok tájékoztatásának, a szakemberek képzésének, valamint a nemzetközi együttműködés javításának,[121] amelynek kulcselemei az információcsere, a jó gyakorlatok megosztása, a képzés, továbbá a „más megelőző jellegű közös erőfeszítések" megtétele.[122] Az egyezmény előírja a részes államok számára bizonyos cselekmények kriminalizálását, ezek: terrorcselekmény elkövetésére való nyilvános izgatás, terroristák toborzása, terroristák kiképzése.

Terrorcselekmény elkövetésére való nyilvános izgatás alatt kell érteni valamely üzenet terjesztését, vagy egyéb módon a nyilvánosság számára hozzáférhetővé tételét, azzal a szándékkal, hogy terrorcselekmény elkövetésére uszítson, ha ez a magatartás – akár a terrorcselekmény közvetlen támogatásával, akár anélkül – annak veszélyével jár, hogy egy vagy több ilyen bűncselekményt követhetnek el.[123] Terroristák toborzása alatt kell érteni más személyeknek terrorcselekmény elkövetésére vagy abban való részvételre, illetve ilyen jellegű társasághoz vagy csoporthoz való csatlakozásra való felhívását azzal a szándékkal, hogy a társaság vagy csoport által elkövetett egy vagy

[119] 2011. évi II. törvény az Európa Tanács terrorizmus megelőzéséről szóló, Varsóban, 2005. május 16-án kelt Egyezménye kihirdetéséről.
[120] 2. cikk.
[121] 3. cikk.
[122] 4. cikk.
[123] 5. cikk.

több terrorcselekmény kivitelezéséhez hozzájáruljon.[124] Terroristák kiképzése alatt kell érteni a robbanóanyagok, lőfegyverek vagy más fegyverek, mérgező vagy veszélyes anyagok készítésére vagy használatára, vagy más különleges módszerek vagy technikák alkalmazására vonatkozó oktatás nyújtását terrorcselekmény elkövetése vagy abban való részvétel céljából, tudatában annak, hogy az átadott szakismeretet e célokra kívánják felhasználni.[125] A kriminalizálandó cselekmények meghatározásán túl az egyezmény eljárásjogi szabályokat is megfogalmaz. Ilyen rendelkezés a kötelező nyomozás előírása arra az esetre, ha valamelyik részes ország arról értesül, hogy területén terrorista bűncselekményt elkövető személy tartózkodik, a kiadatásra vagy büntetőeljárás megindítására kötelezés, illetve a hatóságok közötti információcsere előírása hivatalos megkeresés hiányában is.

Az egyezményhez később kiegészítő jegyzőkönyv is készült, amelyet Magyarországon a 2018. évi XXI. törvény[126] hirdetett ki. A kiegészítő jegyzőkönyv újabb büntetendővé nyilvánítandó cselekményeket fogalmaz meg, ezek:

a) terrorcselekmény céljára szolgáló társaságban vagy csoportban való részvétel,
b) terrorista kiképzésben való részvétel,
c) terrorcselekmény elkövetése céljából külföldre utazás, illetve
d) ennek finanszírozása vagy
e) megszervezése vagy egyéb módon történő elősegítése.

A felsorolt cselekmények közül természetesen nem mindegyik számít informatikai bűncselekménynek.

Az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és szexuális zaklatás elleni védelméről szóló Egyezménye (a Lanzarote Egyezmény)

A New York-i gyermekjogi egyezmény mellett egy másik jelentős nemzetközi jogi dokumentum is foglalkozik a gyermekek szexuális kizsákmányolásával, hiszen 2007-ben az Európa Tanács is elfogadott egy egyezményt a gyermekek jogairól. Az egyezmény fő célja, hogy elősegítse a gyermekek szexuális kizsákmányolása elleni büntető jogszabályok harmonizációját. Magyarországon a gyermekek szexuális kizsákmányolás

[124] 6. cikk.
[125] 7. cikk.
[126] 2018. évi XXI. törvény az Európa Tanács terrorizmus megelőzéséről szóló Egyezménye Kiegészítő Jegyzőkönyvének kihirdetéséről.

és szexuális zaklatás elleni védelméről szóló ET egyezményt a 2015. évi XCII. törvény[127] hirdette ki. Az egyezmény rendszerében a gyermek 18 éven aluli személyt jelent. A gyermek és a nagykorú fogalmakat az egyezmény elválasztja egymástól, tekintettel arra, hogy a nagykorúság elérése az egyes országokban más és más életkorhoz kötött. Gyermek tehát minden 18 éven aluli személy függetlenül attól, hogy saját országában elérte-e a nagykorúságot. Ez az egyezmény is kiemelt figyelmet fordít a tudatosságfejlesztésre – amely jelenti egyrészt a gyermekekkel foglalkozó személyek képzését, a gyermekek oktatását, valamint a figyelemfelhívó kampányok szervezését –, illetve a nemzetközi együttműködésre és a magánszektorral való együttműködésre. Az egyezmény büntető anyagi jogi tényállásokat is meghatároz, amelyeket a részes államoknak át kell ültetniük a jogrendszerükbe. Az egyezmény egyike azoknak, amelyek nem kimondottan kiberbűncselekményekkel foglalkoznak, ám horizontális szabályaik között megtalálhatók azok a deliktumok is, amelyek az online térben követhetők el.

Az egyezmény alapján kriminalizálandó a gyermekek szexuális zaklatása (18. cikk), amely

a) szexuális cselekmény folytatása olyan gyermekkel, aki a nemzeti jog vonatkozó rendelkezései szerint nem érte el a szexuális cselekmény tekintetében a nagykorúságot;

b) szexuális cselekmény folytatása gyermekkel
- kényszer, erőszak vagy fenyegetés alkalmazásával; vagy
- elismert bizalmi helyzettel, tekintéllyel vagy a gyermek befolyásolásával történő visszaéléssel, ideértve a családon belüli eseteket is; vagy
- a gyermek különösen veszélyeztetett helyzetével történő visszaéléssel, nevezetesen a testi vagy szellemi fogyatékossága vagy függőségi helyzete miatt.

Büntetendő a gyermek prostitúcióra toborzása vagy gyermek prostitúcióban való részvételre rávétele, prostitúcióra kényszerítése vagy ilyen célú kihasználása vagy más módon történő kizsákmányolása, továbbá a gyermekprostitúció igénybevétele is (19. cikk).

A kriminalizálandó cselekmények közé tartoznak a gyermekpornográfiával összefüggő magatartások (20. cikk), pontosabban a gyermekpornográfia előállítása, felkínálása, hozzáférhetővé tétele, terjesztése, továbbadása, beszerzése saját célra vagy más személy részére, birtoklása, illetve az információs és kommunikációs

[127] 2015. évi XCII. törvény az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és szexuális zaklatás elleni védelméről szóló Egyezménye kihirdetéséről, valamint ezzel összefüggésben egyes törvények módosításáról.

technológiákon keresztül tudatos hozzáférés a gyermekpornográfiához. A magyar jog az előbbiekben felsorolt magtartások közül a gyermekpornográfiához való hozzáférést nem nevesíti külön, a megszerzés aktusa elméletben a hozzáférést is lefedi. Az egyezmény a gyermekpornográfia fogalmát a magyar meghatározástól eltérően fogalmazza meg. Az egyezményben ugyanis a gyermekpornográfia kifejezés „minden olyan anyagot jelent, amely vizuálisan ábrázol egy valós vagy színlelt, egyértelműen szexuális cselekményben részt vevő gyermeket, vagy egy gyermek nemi szerveinek elsődlegesen szexuális célú ábrázolását".[128] A magyar pornográfiafogalomnak emellett az is központi eleme, hogy a felvételnek kimondottan a nemi vágy felkeltését kell szolgálnia. Ilyen szűkítő kitételt a Lanzarote Egyezmény meghatározása nem tartalmaz.

Európai Unió

Az Európai Unió számos jogi eszközt dolgozott ki az informatikai bűncselekmények tekintetében, ám ezeknek az intézkedéseknek az a hátrányuk, hogy csak az Unió 27 tagállamára kötelezők. Az Európai Unió működéséről szóló szerződés (EUMSZ)[129] 83. cikkének (1) bekezdése szerint az Európai Parlament és a Tanács szabályozási minimumokat állapíthat meg bűncselekményi tényállások és büntetési tételek meghatározására vonatkozóan egyes különösen súlyos bűncselekmények esetében. Az ilyen, különösen súlyosnak minősülő bűncselekményi kategóriák a következők: terrorizmus, emberkereskedelem és a nők és gyermekek szexuális kizsákmányolása, tiltott kábítószer-kereskedelem, tiltott fegyverkereskedelem, pénzmosás, korrupció, pénz és egyéb fizetőeszközök hamisítása, számítógépes bűnözés és szervezett bűnözés. Az alábbi uniós jogi aktusok tartalmaznak az informatikai bűncselekményekkel kapcsolatos rendelkezéseket:

- az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Eker. irányelv);
- az Európai Parlament és a Tanács 2006/24/EK irányelve 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;

[128] 2015. évi XCII. törvény 20. cikk 2.

[129] Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata 2012/C 326/01.

- az Európai Parlament és a Tanács 2011/92/EU irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról;
- az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról;
- az Európai Parlament és a Tanács (EU) 2019/713 irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról;
- az Európai Parlament és a Tanács 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről;
- az Európai Parlament és a Tanács 2021/1232 rendelete a 2002/58/EK irányelv bizonyos rendelkezéseitől a technológiáknak a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatók által a gyermekek online szexuális bántalmazása elleni küzdelem céljából a személyes és egyéb adatok kezelésére történő használata tekintetében való ideiglenes eltérésről;
- az Európai Parlament és a Tanács 2022/2065 rendelete a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet).

A kiberbűncselekmények elleni fellépés jogi hátterével kapcsolatban szólni érdemes az Európai Parlament és a Tanács a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló rendelettervezetéről is, amelyet ugyan jelen kötet lezárásáig nem fogadott el az uniós jogalkotó, mégis alapvető jelentősége van a tárgyalt deliktumok felderítése esetében.

Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól[130]

Az Eker. irányelv alapvetően nem büntetőjogi jellegű dokumentum, mégis érdemes megemlíteni, mivel az irányelv által szabályozott tárgykörök „a számítógépes

[130] Eker. irányelv.

hálózatokon keresztül végzett gazdasági tevékenységek széles skáláját ölelik fel",[131] ebből kifolyólag az irányelv néhány olyan rendelkezést is tartalmaz – például a közvetítő szolgáltatók felelősségének szabályozása –, amelyek az informatikai bűncselekmények esetében is relevánsak.

A közvetítő szolgáltatók felelőssége a magyar jogirodalomban is gyakran tárgyalt téma,[132] amely az internetes közvetítő szolgáltatók körének bővülésével egyre nagyobb jelentőségre tesz szert. Mivel a kötet központi témája a közvetítő szolgáltatók felelősségének kérdése, az Eker. irányelv szabályaira több ponton is utalok.

Az internetes közvetítő szolgáltatók Eker. irányelv szerinti tipizálásáról a kötet második részében részletesen esett szó, ezért ezek újbóli ismertetésétől eltekintek.

Az irányelv bizonyos feltételek teljesülése esetén mentesíti a közvetítő szolgáltatókat, hiszen a tevékenységük többnyire csak egyszerű továbbításra, illetve adattárolásra korlátozódik, a tárolt információ tartalmáról, így jogsértő voltáról nem feltétlenül van tudomásuk, és a tartalomszolgáltatókkal ellentétben nem rendelkeznek szerkesztői felelősséggel sem. A mentesülés egyik feltétele azonban, hogy amint a közvetítő szolgáltató észleli a jogsértő adatokat, köteles azokat haladéktalanul eltávolítani.

Az Európai Parlament és a Tanács 2006/24/EK irányelve 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

Az adatmegőrzési irányelvről annak ellenére is érdemes pár szót ejteni, hogy az Európai Unió Bírósága 2014. április 8. napján az Európai Unió Alapjogi Chartájával való ütközése miatt részben érvénytelennek nyilvánította.

Az irányelv megalkotásának mozgatórugója az volt, hogy

> „a bűncselekmények megelőzése, kivizsgálása, felderítése és üldözése érdekében az adatok megőrzését előíró nemzeti rendelkezések közötti jogi és technikai különbségek akadályokat jelentenek az elektronikus hírközlés belső piaca számára, mivel a szolgáltatások nyújtóira eltérő követelmények vonatkoznak a megőrzendő forgalmi és helymeghatározó adatok típusait, valamint a megőrzés feltételeit és idejét illetően".

131 Eker. irányelv (18) preambulumbekezdés.
132 Lásd például Szabó 2014.

Az irányelv szerint a tagállamoknak az alábbi adatkategóriák megőrzését kellett biztosítaniuk:

1. a közlés forrásának megtalálásához és azonosításához szükséges adatok,
2. a közlés címzettjének azonosításához szükséges adatok;
3. a közlés napjának, időpontjának és időtartamának megállapításához szükséges adatok;
4. a közlés típusának megállapításához szükséges adatok;
5. a felhasználók (feltételezett) kommunikációs berendezésének azonosításához szükséges adatok;
6. mobil kommunikációs eszköz helyének megállapításához szükséges adatok.

Az irányelv alapján a közlés tartalmát felfedő adat nem őrizhető meg.

A magyar szabályokat az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) 159/A. §-a rögzítette, bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettség cím alatt, teljes mértékben megfelelve az irányelv előírásainak.

Az EUB a C-293/12. és C-549/12. számú Digital Rights Ireland, valamint Seitlinger és társai egyesített ügyekben hozott ítéletben[133] azért nyilvánította érvénytelennek az irányelvet, mert az irányelv széles körű és súlyos beavatkozást jelent a magánélet tiszteletben tartásához és a személyes adatok védelméhez való alapvető jogba. A bíróság álláspontja szerint

> „ezen adatok együttesen véve igen pontos következtetések levonását tehetik lehetővé azon személyek magánélete vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében".

A bíróság azt is aggályosnak találta, hogy az irányelv általános jelleggel állapít meg szabályokat, és nem alkalmaz semmilyen megkülönböztetést, korlátozást vagy kivételt, így tehát olyan személyek adatait is megőrzik, akik nem állnak büntetőeljárással kapcsolatban. Az irányelv nem rendelkezik arról sem, hogy az adatok későbbi felhasználásának egyes pontosan körülhatárolt súlyos bűncselekmények megelőzése

133 C-293/12 és C-594/12, a Digital Rights Ireland Ltd. kontra Írország és Kärntner Landesregierung kontra Michael Seitlinger és társai egyesített ügyekben hozott 2014. április 8-i ítélet.

és felderítése vagy ezekkel kapcsolatos büntetőeljárások céljára kell korlátozódnia, ezért fennáll a lehetősége a személyes adatok visszaélésszerű felhasználásának.

A TASZ jogvédő szervezet álláspontja szerint

> „a kérdés különös súlyát az adja, hogy a jelenlegi 9 millió 358 ezer mobiltelefon-előfizető, és a 3,3 millió vezetékes telefon-előfizető nagyjából lefedi a teljes magyar társadalmat. […] Nem képzelhető el egy jogállamban olyan nemzetbiztonsági, bűnüldözési, bűnmegelőzési, honvédelmi vagy közrenddel kapcsolatos cél, amelynek megvalósításához gyakorlatilag a teljes lakosság kommunikációs és mozgási adatait évekre visszamenően tárolni szükséges."[134]

Az Európai Parlament és a Tanács 2011/93/EU irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról

A gyermekek szexuális kizsákmányolásával kapcsolatos fellépés az EU normáiban is megjelenik. A 2004/68/IB tanácsi kerethatározatot felváltó irányelv már tekintettel van arra a sajnálatos trendre, hogy a gyermekek szexuális kizsákmányolását nagyon megkönnyíti az új technológiák és az internet széles körben való elterjedése és rendelkezésre állása [(3) preambulumbekezdés].

Az irányelv, hasonlóan az egyéb nemzetközi dokumentumokhoz, minden 18 évesnél fiatalabb személyre gyermekként tekint.[135]

Az irányelv gyermekpornográfia-fogalma minden olyan anyagra kiterjed, amely: vizuálisan ábrázolja a kifejezetten szexuális magatartást tanúsító vagy ilyen magatartást színlelő gyermeket, gyermeknek tűnő személyt; vagy gyermek, gyermeknek tűnő személy nemi szerveit mutatja be, elsődlegesen szexuális céllal, továbbá kiterjed a kifejezetten szexuális magatartást tanúsító gyermek, illetve gyermek nemi szerveinek valósághű, elsősorban szexuális céllal bemutató képeire.[136] Az irányelv rendszerében gyermekpornográf felvételnek minősülnek a nem valós kiskorút ábrázoló felvételek is, tehát „az olyan, elsődlegesen szexuális célú, valósághű képek is, amelyek kifejezetten szexuális jellegű magatartást tanúsító, vagy ilyen magatartást tanúsítóként ábrázolt

134 Földes 2007.
135 2. cikk a) pont.
136 2. cikk c) pont.

gyermekeket ábrázolnak".[137] Pornográf előadás az irányelv szerint a fentiek többek között információs és kommunikációs technológiák révén történő, közönségnek szóló, élő bemutatása.[138]

Az irányelv a gyermekek szexuális bántalmazásával kapcsolatban több magatartásformát is büntetni rendel, amelyek között találhatóak a gyermekpornográfiával összefüggő tényállások is. Az irányelv büntetni rendeli a szexuális bántalmazással kapcsolatos cselekményeket, így a gyermek arra kényszerítését, hogy szexuális tevékenység vagy bántalmazás tanúja legyen[139] (akkor is, ha abban nem vesz részt), a beleegyezési korhatárt el nem ért gyermekkel folytatott szexuális tevékenységet.[140] Az irányelv előírja, hogy a tagállamok szigorúbban büntessék azt, amikor a gyermekkel valaki úgy folytat szexuális tevékenységet, hogy bizalmi, hatalmi helyzettel vagy befolyással él vissza, a gyermek különösen kiszolgáltatott helyzetével – így szellemi vagy testi fogyatékosságával, eltartotti helyzetével – él vissza, valamint a kényszer, erőszak vagy fenyegetés alkalmazását.[141]

Az irányelv a gyermekek szexuális kizsákmányolásával kapcsolatos eseteket is büntetni rendeli, így büntetendő a gyermek pornográf előadáson való részvételre való késztetése vagy toborzása,[142] amelyek súlyosabban minősülnek, ha ehhez kényszert vagy erőszakot alkalmaznak.[143] Büntetendő a gyermek részvételével folytatott pornográf előadáson való tudatos részvétel.[144] A tagállamoknak kriminalizálniuk kell a gyermekprostitúcióra való késztetést vagy toborzást is,[145] amelyek szintén súlyosabban minősülnek, ha kényszerítés vagy erőszak alkalmazásával történtek.[146]

A gyermekpornográfiával összefüggésben az irányelv az alábbi magatartásokat rendeli büntetni: gyermekpornográfia készítése,[147] megszerzése, birtoklása,[148] megosztása, terjesztése vagy továbbítása,[149] felajánlása, nyújtása vagy annak hozzáférhetővé

137 (13) preambulumbekezdés.
138 2. cikk e) pont.
139 3. cikk (2) és (3) bekezdés.
140 3. cikk (4) bekezdés.
141 3. cikk (5) bekezdés.
142 4. cikk (2) bekezdés.
143 4. cikk (3) bekezdés.
144 4. cikk (4) bekezdés.
145 4. cikk (5) bekezdés.
146 4. cikk (6) bekezdés.
147 5. cikk (6) bekezdés.
148 5. cikk (2) bekezdés.
149 5. cikk (3) bekezdés.

tétele,[150] továbbá a gyermekpornográfiához való, informatikai és kommunikációs technológia útján történő tudatos hozzáférés.[151] Az irányelv rendelkezik arról, hogy ezek a cselekmények jogellenesen elkövetett szándékos magatartások esetén büntetendők. Az irányelv normaszövege a gyermekpornográf felvétel vonatkozásában a „jogellenes" kifejezést is használja, utalva arra, hogy nem minden meztelen gyermeket ábrázoló felvételt tekint gyermekpornográfiának. A tagállamoknak lehetőségük van arra, hogy orvosi, tudományos vagy hasonló célokat szolgáló, pornográf anyagokkal kapcsolatos magtartásokat ne büntessenek, továbbá lehetővé teszi, hogy a hatóságok a büntetőeljárás lefolytatása vagy bűncselekmények megelőzése vagy felderítése céljából jogszerűen birtokolhassanak ilyen felvételeket.[152] Az irányelv arról is rendelkezik, hogy a gyermekpornográf felvétellel való visszaéléssel összefüggő magtartások csak szándékosan követhetők el. A szándékosság az irányelv értelmezésében azt jelenti, hogy az adott személynek szándékában áll olyan oldalra látogatni, ahol tudja, hogy ilyen jellegű alkotások lelhetők fel.[153] Az irányelv tehát nem rendeli szankcionálni azt, aki véletlenül téved ilyen weboldalra, sem azt, aki egy weboldalon található hirdetés formájában vagy számítógépes vírus következtében találkozik ilyen felvételekkel.

Az irányelv elismeri, hogy az infokommunikációs technológiák és az internet, így a közösségimédia-platformok, azonnali üzenetküldő alkalmazások, fórumok, chatszobák megkönnyítik azt, hogy az elkövetők kapcsolatba kerüljenek potenciális áldozataikkal, ezért a szexuális kizsákmányolás körében büntetni rendeli a gyermekkel való, szexuális céllal történő kapcsolatfelvételt *(grooming)* is.[154] Az irányelv rámutat arra, hogy ennek a cselekménynek a figyelembevétele azért is különösen fontos, mert az internet névtelenséget biztosít a felhasználók számára, akik elrejthetik valós identitásukat, így valótlan életkor, fénykép megadásával tőrbe csalva áldozataikat.[155]

Az irányelv speciális kötelezettségeket fogalmaz meg a tagállamok számára a gyermekpornográfiát tartalmazó weboldalakkal összefüggésben, ugyanis biztosítaniuk kell a területükön üzemeltetett, gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak azonnali eltávolítását.[156] Az irányelv tekintettel van arra a tényre is, hogy a weboldalak lekapcsolása nem minden esetben kivitelezhető, főleg, ha azok

150 5. cikk (4) bekezdés.
151 5. cikk (3) bekezdés.
152 (17) preambulumbekezdés.
153 (18) preambulumbekezdés.
154 (12) preambulumbekezdés és 6. cikk.
155 (19) preambulumbekezdés.
156 25. cikk (1) bekezdés.

olyan szervereken vannak elhelyezve, amelyek nem az EU területén találhatók.[157] Ennélfogva a tagállamoknak lehetőségük van a területükön található, internetfelhasználókat célzó weboldalakhoz való hozzáférés meggátolására, azaz az egyes weboldalak blokkolására.[158]

Főként az angolszász jogban merül fel a gyermekpornográfia – illetve általában a pornográfia – és a szólásszabadság kapcsolata. Az egyes közlésfajtákat kriminalizáló büntetőjogi tényállások jellegüknél fogva korlátozzák a szólásszabadságot. Erre reflektálva az irányelv rendezi a véleménynyilvánítás szabadsága és a gyermekpornográfia kapcsolatát, amikor kimondja, hogy a „gyermekpornográfia olyan különleges típusú tartalom, amely nem tekinthető véleménynyilvánításnak".[159]

Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

2005 februárjában az Európai Unió Tanácsa elfogadta az információs rendszerek elleni támadásról szóló kerethatározatot.[160] Mindenekelőtt a büntető anyagi jog harmonizációját emeli ki, de precíz definíciókat is alkot, célja a komputerbűnözéssel kapcsolatos fogalmak megalkotása és nemzetközi szintű egységesítése, noha a kerethatározat fogalmai megegyeznek a korábban említett Cybercrime Egyezményben foglaltakkal. Ebben a kerethatározatban a korábban használatos számítógépes rendszer fogalom helyett már az információs rendszer *(information system)* fogalom jelenik meg. Az egyes fogalmak összevetésekor megfigyelhető, hogy annak ellenére, hogy a megjelölés különbözik (információs rendszer – számítógépes rendszer), a fogalmak tartalma gyakorlatilag megegyezik. Ez nemcsak nemzetközi viszonylatban igaz, hanem ahogyan arra már korábban utaltunk, az új Btk. hatálybalépésekor a korábbi számítógépes rendszer kifejezés gyakorlatilag csak új elnevezést kapott. A kerethatározat, tekintettel a dinamikusan változó információtechnológiai környezetre, hamar elavulttá vált. A kerethatározat hibája volt például, hogy a jogi felelősség formájának megválasztását gyakorlatilag a tagállamokra bízta, amikor kimondta, hogy a nevezett

[157] (47) preambulumbekezdés.
[158] 25. cikk (2) bekezdés.
[159] (46) preambulumbekezdés.
[160] A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról.

cselekmények legalább a jelentősebb esetekben minősüljenek bűncselekménynek. A gyakorlatban ez azt jelentette, hogy a tagállamoknak nem volt kötelességük büntetőjogi szankcióval fenyegetni a felsorolt cselekményeket. A kerethatározat adós maradt a jelentősebb esetek kritériumainak meghatározásával is, tovább bővítve a tagállamok szabad mozgásterét. A kerethatározat leszűkítette az üldözendő magatartások körét három magatartásra: az információs rendszerbe való jogellenes belépés, a rendszer jogellenes megzavarása és az adatokhoz való jogellenes hozzáférés.

A kerethatározatot 2013-ban felváltotta az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv, amely már figyelemmel van arra, hogy növekvő veszélyt jelentenek az információs rendszerek elleni támadások, amelyekben nagy szerepe van a szervezett bűnözésnek, továbbá a terrorszervezeteknek. Az irányelv kiemelt figyelmet fordít a kritikus infrastruktúrák – azon eszközök, rendszerek, illetve azok részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok, az egészségügy, a biztonság, a védelem, valamint az emberek gazdasági és szociális jólétének fenntartásához[161] – részét képező információs rendszerek védelmére.[162]

Fontos változás a 2005/222/IB kerethatározathoz képest, hogy különös figyelmet fordít az úgynevezett botnetekre[163] és a személyazonossághoz kapcsolódó bűncselekményekre,[164] valamint súlyosabb szankciókat helyez kilátásba abban az esetben, ha az informatikai bűncselekményt bűnszervezetben követik el,[165] ezenfelül előírja, hogy a büntetőeljárás során figyelembe kell venni azt a körülményt, ha a bűncselekményt az elkövető alkalmazotti minőségben követi el.[166]

Az irányelv felhívja a figyelmet a tagállamok közötti együttműködés, valamint a tagállamok és a magánszektor szereplői közötti együttműködés fontosságára. A szolgáltatókkal szemben megfogalmazott fontos elvárás, hogy azok őrizzék meg a potenciális bizonyítékokat, illetve iktassák ki a fertőzött vagy jogellenes célra használt információs rendszereket.[167]

Az irányelv minimumszabályokat fektet le a kriminalizálandó tevékenységekkel kapcsolatban, és alapvetően négyféle cselekmény büntetendővé nyilvánítását írja elő a tagállamok számára:

161 (4) preambulumbekezdés.
162 (3) preambulumbekezdés.
163 (5) preambulumbekezdés.
164 (14) preambulumbekezdés.
165 (13) preambulumbekezdés.
166 (18) preambulumbekezdés.
167 (23) preambulumbekezdés.

1. az információs rendszerekhez való jogellenes hozzáférés,
2. az információs rendszert érintő jogellenes beavatkozás,
3. az adatot érintő jogellenes beavatkozás,
4. jogellenes adatszerzés.

A tagállamok legalább a súlyosabb esetekben kötelesek büntetni azt, ha valaki információs rendszerhez vagy annak egy részéhez szándékosan és jogosulatlanul hozzáfér, akkor, ha a bűncselekményt valamely biztonsági intézkedés megsértésével követték el.[168] Az irányelvben nevesített bűncselekmények csak jogsértő szándékkal követhetők el, tehát ha az elkövetőnek nincs tudomása arról, hogy hozzáférése jogosulatlan, vagy kimondottan azzal bízták meg, hogy tesztelje az információs rendszer védelmét (például etikus hacker), nem büntethető.[169] A tagállamoknak legalább a súlyosabb esetekben büntetniük kell azt is, ha valaki az információs rendszer működését számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, vagy ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén súlyosan akadályozza. A súlyos akadályozás többnyire kártékony számítógépes szoftverek (*malware*-ek) rendszerbe juttatásával valósul meg, és idetartozik a botnethálózatok kiépítése, valamint a túlterheléses támadások folytatása is. A botnetek létrehozása az irányelv fogalomrendszerében az a tevékenység, „amellyel célzott informatikai támadások révén jelentős számú számítógép felett veszik át a távvezérelt irányítást oly módon, hogy rosszindulatú számítástechnikai programokkal fertőzik meg őket".[170]

Az irányelv nemcsak magát az információs rendszert védi a jogosulatlan műveletektől, hanem az abban található adatot is. Ennélfogva a tagállamoknak legalább a súlyosabb esetekben büntetniük kell az adatok szándékos és jogosulatlan törlését, megrongálását, minőségi rontását, megváltoztatását vagy elrejtését, vagy az ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tételét.[171] Az irányelv az adatokkal végzett jogosulatlan műveleteken túl külön kriminalizálni rendeli a jogosulatlan adatszerzést. Az irányelvi megfogalmazás szerint a tagállamoknak legalább a súlyosabb esetekben büntetniük kell az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs

168 3. cikk.
169 (17) preambulumbekezdés.
170 (5) preambulumbekezdés.
171 5. cikk.

rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő, szándékos és jogosulatlan megszerzését.

A felsorolásszerű megfogalmazás joggal veti fel a kérdést, hogy a magyar Btk. dogmatikai rendszerében hogyan helyezhetők el ezek a megatartások. A magyar Btk. szabályai közül az irányelv jogellenes adatszerzést szabályozó cikkéhez kapcsolódhat az adatok jogosulatlan kifürkészésének, magántitok, levéltitok megsértésének a kérdése, valamint a manapság oly népszerű személyazonosság-lopás *(identity theft)* kérdése.

Végig kell gondolnunk, hogy a személyazonossághoz kapcsolódó bűncselekmények, például a személyazonosság-lopás hol helyezhetők el a magyar büntetőkódexben. A személyazonosság-lopás kétlépcsős folyamat. Első lépésként az elkövető eltulajdonítja a személyes adatokat (például személyiigazolvány-számot, tajszámot), majd következő lépésként ezek birtokában önmagát a sértettnek kiadva visszaélést követ el. A visszaélés több formában megjelenhet, például bűncselekmény elkövetése, egészségügyi, illetve egyéb szolgáltatások igénybevétele stb. Véleményem szerint nem szükséges külön tényállást létrehozni az ilyen típusú bűncselekményeknek, hiszen azok beilleszthetők a már létező tényállások közé. Az első lépcső, azaz a személyes adatok megszerzése többféle tényállás megvalósításával is megtörténhet. A tiltott adatszerzés egyik esete, amikor valaki „személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti". A Btk. kommentárja szerint a kifürkészés „olyan magatartás, amely a közlemény tartalmának az elektronikus hírközlő hálózat útján történő továbbítása során való megismerésére irányul. Ez gyakorlatilag bármilyen technológiával történő lehallgatást jelent."[172] Információs rendszerek tekintetében megvalósítható például billentyűleütés-rögzítő programokkal *(keylogger),* vagy adathalász tevékenységgel *(phishing).*

Az adat megszerzése után következik a második lépcsőfok, azaz annak visszaélésszerű felhasználása. A felhasználásra a személyes adattal visszaélés vétségének szabályai vonatkoznak. A Btk. 219. §-a így szól: „[a]ki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel". Az adatkezelés fogalmát az információs önrendelkezési jogról

[172] Szomora 2019b.

és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) a következőképpen határozza meg:

> „az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése" (3. § 10. pont).

A fentiek alapján a személyazonosság-lopás minden esete tényállásszerű, hiszen vagy haszonszerzési célzattal követik el (például egészségügyi ellátások, egyéb szolgáltatások igénybevétele), vagy oly módon, hogy az a sértettnek jelentős érdeksérelmet okoz (például bűncselekmény elkövetése esetén a következmények viselése, jó hírnév, méltóság sérelme).

A személyazonosság-lopást el kell határolnunk az információs rendszer felhasználásával elkövetett csalástól, hiszen mindkét esetben haszonszerzési célzattal történik a cselekmény, és mindkét esetben adatkezelés történik. Az elhatárolás egyik szempontja, hogy az információs rendszer felhasználásával elkövetett csalás esetében az elkövetés tárgya az információs rendszer, míg a személyes adattal való visszaélésnek nincs elkövetési tárgya. Személyazonosság-lopás esetében a felhasználás pillanatában az adat már kikerült az információs rendszerből, az elkövető tudomására jutott, az adattal való visszaélés pedig nem szükségszerűen valósul meg információs rendszer útján. További szempont, hogy az információs rendszer felhasználásával elkövetett bűncselekmény eredmény-bűncselekmény, ezért minden esetben kár keletkezik. Az információs rendszer felhasználásával elkövetett csalás bármely információs rendszerben tárolt adatra elkövethető, míg a személyes adattal visszaélés kizárólag személyes adatokra.

Az Európai Parlament és a Tanács 2019/713 irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról

2001-ben a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló kerethatározat az információs társadalom egyik újonnan megjelenő

problémájára igyekezett megoldást találni. Ebben az időszakban kezdett el Európában elterjedni a készpénz-helyettesítő fizetési eszközök, bankkártyák, utazási csekkek használata, ezért a kerethatározat kötelezettséget írt elő a tagállamok számára, hogy bizonyos deliktumok esetében harmonizálják büntetőjogi szabályaikat.

A kerethatározat fogalommeghatározásai meglehetősen hiányosak voltak, hiszen a dokumentum mindössze két fogalmat definiált, a „fizetőeszköz", valamint a „jogi személy" fogalmát. A határozat szóhasználata meglehetősen esetlen volt, hiszen a „fizetőeszköz" fogalmát úgy határozta meg, hogy kivonta alóla az úgynevezett törvényes fizetőeszközöket (bankjegyeket, érméket), vagyis a készpénzt, valamint példálózó felsorolással határozta meg a készpénz-helyettesítő fizetési eszközöket.

> „»[F]izetőeszköz« a törvényes fizetőeszközök (bankjegyek és érmék) kivételével minden olyan materiális eszköz, amely különleges természeténél fogva önállóan vagy más (fizető)eszközzel együtt birtokosát vagy használóját képessé teszi pénz vagy pénzbeli érték átruházására; ilyen például a hitelkártya, az eurocsekk-kártya, a pénzügyi intézmények által kibocsátott más kártyák, az utazási csekkek, az eurocsekkek és más csekkek és váltók, amelyek a hamisítás vagy a jogosulatlan felhasználás ellen például kivitelezésük, kódolásuk vagy a rajtuk lévő aláírás folytán védettek."[173]

A kerethatározatot 2019-ben váltotta fel a 2019/713 irányelv, amely igyekszik számításba venni, hogy az innováció következtében új fizetési technológiák jelentek meg, és a hagyományos csalások mellett az információs rendszer felhasználásával elkövetett csalások is egyre nagyobb hangsúllyal vannak jelen a bűnözésben.

Az irányelv a kerethatározattal szemben már nem a fizetőeszköz, hanem a készpénz-helyettesítő fizetési eszköz fogalmát adja meg, és idesorol minden olyan immateriális vagy materiális védett készüléket, tárgyat vagy rögzített adatot és ezek kombinációját, amely önállóan, illetve egy eljárás vagy eljárások alkalmazásával lehetővé teszi, hogy birtokosa vagy felhasználója pénzt vagy pénzbeli értéket utaljon át, többek között digitális csereeszközök révén.[174] Az irányelv nemcsak a materiális világban megjelenő fizetési eszközöket, például bankkártyákat szabályozza, hanem

[173] A Tanács 2001/413/IB kerethatározata a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről, 1. cikk a) pont.

[174] Az Európai Parlament és a Tanács (EU) 2019/713 irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról, 2. cikk a) pont.

rendelkezéseket tartalmaz a virtuális fizetési eszközökre is. A virtuális fizetési eszközök, mint a kriptovaluták (például bitcoin) egyre nagyobb szerephez jutnak a virtuális gazdaságban, újdonság jellegük miatt azonban még kevésbé szabályozottak, mint a pénzforgalomban régebben szerepet játszó technológiák. Az irányelv fogalommeghatározása szerint a virtuális fizetőeszköz „olyan digitális értékmegjelenítő, amelyet nem központi bank vagy hatóság bocsát ki vagy garantál, nem feltétlenül kapcsolódik törvényes fizetőeszközhöz, és nem minősül pénznemnek vagy pénznek, de amelyet természetes vagy jogi személyek csereeszközként elfogadnak, és amely elektronikusan átutalható, tárolható és értékesíthető".[175] Mivel a virtuális fizetőeszközök nem kapcsolódnak szorosan államokhoz, kibocsátásuk könnyebb, felhasználásuk pedig kevésbé nyomon követhető, ami a feketegazdaság ideális fizetőeszközeivé teszi őket.

A dokumentum három csoportját határozza meg a fizetési eszközökkel kapcsolatos bűncselekményeknek, ezek:

1. Materiális készpénz-helyettesítő fizetési eszközök csalárd felhasználásával kapcsolatos bűncselekmények, így az eszköz ellopása, eltulajdonítása, hamisítása vagy meghamisítása, csalárd felhasználás érdekében történő beszerzése.
2. Immateriális készpénz-helyettesítő fizetési eszközök csalárd felhasználásával kapcsolatos bűncselekmények. Megjegyzendő továbbá, hogy az irányelv nemcsak a materiális eszközöket (csekkek, váltók, hitelkártyák és más kártyák) részesíti védelemben, hanem magát az elektronikus pénzt, amely „készpénz átvétele, illetőleg számlapénz átutalása ellenében kibocsátott elektronikus pénzeszközön tárolt pénzérték" is.
3. Információs rendszerrel kapcsolatos csalás, amely jelentheti az információs rendszer működésének jogosulatlan akadályozását vagy a működésébe való jogosulatlan beavatkozást, illetve adatok jogosulatlan bevitelét, módosítását, törlését, továbbítását vagy hozzáférhetetlenné tételét.

Figyelemre méltó, hogy az irányelv szerint az információs rendszerrel kapcsolatos csalás körében elkövetett deliktumok esetében követelmény a cselekmény célzatossága, vagyis az, hogy az elkövető vagy harmadik személy jogellenesen hasznot szerezzen.

[175] 2. cikk d) pont.

Az Európai Parlament és a Tanács 2021/1232 rendelete a 2002/58/EK irányelv bizonyos rendelkezéseitől a technológiáknak a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatók által a gyermekek online szexuális bántalmazása elleni küzdelem céljából a személyes és egyéb adatok kezelésére történő használata tekintetében való ideiglenes eltérésről

Érdekes eleme az európai szabályozási rendszernek a 2021/1232 rendelet, amely a hírközlési adatvédelmi irányelv egyes rendelkezéseitől enged eltéréseket.[176] A rendelet célja, hogy a számfüggetlen személyközi hírközlési szolgáltatások (például chatszolgáltatások, mint a Facebook Messenger, a WhatsApp vagy a Discord, illetve az e-mail-szolgáltatások) esetében lehetővé tegye, hogy a szolgáltatók felderítési tevékenységet végezzenek, amennyiben felmerül a gyanúja a gyermekek online szexuális bántalmazásának. A rendelet adatvédelmi szempontból is különleges, hiszen a gyermekek elleni szexuális bűncselekmények elleni fellépést mint bűnüldözési érdeket előbbrevalónak tekinti az adatvédelemnél, így a felhasználók magánéletének és magánjellegű kommunikációjának védelménél.

A hírközlési adatvédelmi irányelvnek a közlések és az azokra vonatkozó fogalmi adatok titkosságát biztosító (5. cikk), valamint a forgalmi adatok szükségtelenül hosszú ideig való tárolását tiltó, azok törlését megengedő (6. cikk) rendelkezéseit a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatók a 2021/1232 rendelet értelmében figyelmen kívül hagyhatják. Erre akkor van lehetőségük, ha a gyermekek online szexuális bántalmazását ábrázoló anyagot derítenek fel. Az ilyen tartalmak felderítése során a szolgáltatóknak olyan technológiát kell alkalmazniuk, amely a legkisebb sérelmet okozza,[177] biztosítaniuk kell, hogy csak a legszükségesebb adatokat szerezzék be,[178] és hogy a használt rendszerek átessenek adatvédelmi hatásvizsgálaton,[179] és kellően megbízhatóak legyenek (vagyis minél alacsonyabb hibaszázalékkal szűrjék ki a szóban forgó tartalmakat).[180] A szolgáltatóknak az alkalmazott technológiát minden esetben emberi felügyelettel kell kiegészíteniük,[181] és ha olyan tartalmat

176 Az Európai Parlament és a Tanács 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv").
177 3. cikk (1) b).
178 3. cikk (1) a).
179 3. cikk (1) c).
180 3. cikk (1) e).
181 3. cikk (1) g).

derítenek fel, amely valószínűsíthetően gyermekek szexuális bántalmazását ábrázolja, azt haladéktalanul jelezniük kell a bűnüldöző hatóságok felé.[182]

E rendelet ideiglenes jogi aktus, érvényessége 2024. augusztus 3. napján megszűnt volna. Az uniós jogalkotóknak azonban nem sikerült megállapodni a gyermekek szexuális kizsákmányolásáról szóló végleges rendelet szövegéről, így a Tanács és a Parlament megállapodott az ideiglenes rendelet időbeli hatályának 20 hónappal, 2026. március 3-ig való meghosszabbításáról. Mivel az elmúlt években több olyan uniós jogalkotási folyamat zajlott, amely az adatvédelmet, illetve az online jogellenes tartalmakat érintette, a végleges szabályozási keret megszületéséig tartó átmeneti időszakra az uniós jogalkotó biztosítani akarta a gyermekek kellő védelmét. Mivel ideiglenes szabályokról van szó, a szolgáltatók számára a rendeletben javasolt technikai megoldások alkalmazása nem kötelező, hanem önkéntes. A végleges szabályozási keret elfogadását követően egy új rendelet fogja szabályozni a titkos vagy titkosított kommunikáció felderítését, amelyet már az általános adatvédelmi rendelet (GDPR) és a DSA rendelkezéseire figyelemmel fogad el az EU. A gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról szóló rendeletet várhatóan 2024-ben fogadják el az uniós döntéshozók, ez már állandó és kötelező jelleggel fogja szabályozni a szolgáltatók – és nem csak a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatók – kötelezettségeit.

Az Európai Parlament és a Tanács 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről

Az online terjesztett terrorista tartalmakkal szembeni fellépés gondolata abból a felismerésből fakad, hogy az internet terrorista célú használata egyre nagyobb szerepet játszik a több ember életét követelő, tényleges terrorcselekmények elkövetésében. Az Európai Bizottság a rendelet tervezetének indokolásában felhívta a figyelmet arra, hogy az internetes tárhelyszolgáltatásokban tárolt terrorista tartalmak „lényeges szerepet játszottak a radikalizálódás és az úgynevezett »magányos farkasok« által elkövetett támadások tekintetében".[183] Az iparág számára javasolt intézkedések mellett

[182] 3 cikk (1) h).

[183] Javaslat: az Európai Parlament és a Tanács rendelete az online terrorista tartalom terjesztésének megelőzéséről. Az Európai Bizottság hozzájárulása a 2018. szeptember 19–20-i salzburgi vezetői üléshez. 1.

az Európai Tanács felhívta a figyelmet arra, hogy a platformszolgáltatók tevékenységén túl uniós szinten is szükség van megfelelő jogalkotási intézkedésekre.

Az EU viszonylag friss rendeletének célja egy olyan hatékony eszközrendszer megalkotása, amelynek segítségével eredményesen eltávolíthatók a terrorista tartalmak az online platformokról. A terrorista tartalmak körét a rendelet tágan határozza meg, idesorolja a terrorista bűncselekmények elkövetésére vagy elkövetésében való közreműködésre felbujtást és felhívást, terrorista csoportban részvételre buzdítást, a terrorizmust dicsőítő, például terrortámadásokat bemutató anyagokat,[184] illetve az olyan oktatóanyagokat is, amelyek célja, hogy segítséget nyújtsanak terrorcselekmények elkövetéséhez (például bombakészítés bemutatása, célpontok kiválasztásának technikái).

A rendelet kiegészíti az audiovizuális médiaszolgáltatásokról szóló irányelvet, hatálya azonban nemcsak a videómegosztóknak minősülő tárhelyszolgáltatásokra terjed ki, hanem annál szélesebb körre, a képes és szöveges tartalmak számára tárhelyet biztosító szolgáltatókra, így a közösségimédia-platformokra is vonatkozik.

A rendelet tervezetének az indokolásában az Európai Bizottság szól a rendeletnek az Eker. irányelv szerinti felelősségi rendszerével való összhangjáról. Generális értelemben a rendelet nem kívánja felülírni az Eker. irányelv korábban már ismertetett felelősségkorlátozó rendelkezéseit,[185] és megerősíti, hogy a terrorista tartalmak üldözésével kapcsolatos proaktív magatartás nem vezethet az általános nyomonkövetési kötelezettség tilalmának feloldásához.[186] Bizonyos fokú gondossági kötelezettséget azonban megállapít, és előírja a szolgáltatók számára, hogy megfelelő, észszerű és arányos intézkedéseket hozzanak a terrorista tartalom terjesztése és a felhasználók terrorista tartalmaktól való védelme érdekében.[187] A rendelet elismeri, hogy a terrorizmus esetében vannak olyan különösen súlyos kockázatok, ahol kivételesen el lehet térni az általános nyomon követés tilalmától, tehát korlátozott esetben, de megteremti annak a lehetőségét, hogy a szolgáltatókat előzetes tartalomszűrésre lehessen kötelezni.

Az Eker. irányelvnek és az AVMS irányelvnek is sarokköve a származási ország elve – vagyis annak deklarálása, hogy a szolgáltatók felett az a tagállam gyakorol joghatóságot, amelyben a szolgáltató letelepedettnek minősül. Audiovizuális médiaszolgáltatások, valamint a közvetítő szolgáltatók esetében a letelepedési helyet összetett

184 (11) preambulumbekezdés.
185 (5) preambulumbekezdés.
186 (6) preambulumbekezdés.
187 3. cikk.

szempontrendszer alapján lehet megállapítani, a videómegosztókat például abban az országban is letelepedettnek lehet tekinteni, amelyben a szolgáltató anyavállalattal, leányvállalattal rendelkezik. A rendelet az uniós joghatóság megállapítását nem köti letelepedéshez. A rendelet hatálya letelepedéstől függetlenül minden olyan szolgáltatóra kiterjed, amelynek a szolgáltatása az Unióban elérhető.

A rendelet a terrorista tartalmakkal kapcsolatos hatékony fellépés zálogát azok eltávolításában látja, ezért előírja, hogy minden tagállamnak kell rendelkeznie olyan kompetens hatósággal, amely eltávolítási végzéssel kötelezheti a tárhelyszolgáltatókat a tartalomtörlésre vagy a szóban forgó tartalom hozzáférhetetlenné tételére. A szolgáltatóknak gyorsított eljárásban kell a végzést elintézniük, annak kézhezvételétől számítva egy órájuk van a tartalom eltávolítására, illetve hozzáférhetetlenné tételére.[188] Az eltávolítással érintett tartalmak esetében a szolgáltatót megőrzési kötelezettség is terheli,[189] ami azt biztosítja, hogy a bizonyítéknak minősülő információk ne vesszenek el. A terrorista tartalomnak minősített információkkal szembeni reaktív fellépés mellett a tárhelyszolgáltatóknak proaktív intézkedésekkel is elő kell segíteniük azt, hogy az ilyen tartalmak ne jelenhessenek meg a szolgáltatásukban, vagy ha megjelennek, akkor azok az eltávolításuk előtt kevés felhasználót érjenek el. A rendelet szól arról, hogy a tárhelyszolgáltatóknak olyan technikai eszközöket kell beépíteniük a szolgáltatásukba, amelyek révén azonosíthatók, bejelenthetők a vélhetően terrorista tartalmak,[190] ezenfelül tudatosságnövelő anyagokat is meg kell osztaniuk a felhasználóikkal.[191]

Az Európai Parlament és a Tanács 2022/2065 rendelete a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet)

2022 őszén jelent meg az EU Hivatalos Lapjában a digitális szolgáltatásokról szóló rendelet, amely az e-kereskedelmi irányelv szabályait több ponton kíbővítve szabályozza az internetes közvetítő szolgáltatók tevékenységét.

188 3. cikk (3).
189 6. cikk.
190 5. cikk (2) a)–b).
191 5. cikk (2) c).

A DSA egyik említésre érdemes újítása, hogy a közvetítő szolgáltatások kategóriáján belül létrehozza az online platformok kategóriáját. Az online tér szereplőiről szóló fejezetben az online platformokról már esett szó részletesen, így e helyütt a DSA idevágó részeit nem ismételem.

A DSA lépcsőzetes szabályozási rendszert épít ki, a rendszer legalsó lépcsőfokán a minden közvetítő szolgáltatóra vonatkozó szabályok állnak. Ezt egészítik ki második lépcsőben a tárhelyszolgáltatókra, köztük az online platformokra vonatkozó szabályok, majd harmadik lépcsőben azok a szabályok, amelyek csak az online platformokra vonatkoznak. A negyedik és egyben utolsó lépcsőfokon azok a szabályok helyezkednek el, amelyek csak az úgynevezett online óriásplatformokra vonatkoznak.

Az összes közvetítő szolgáltatóra vonatkozó szabályok elsősorban a tagállami hatóságok és a szolgáltatók, valamint a felhasználók és a szolgáltatók közötti hatékony kommunikációra, a tájékoztatásra és a kapcsolattartásra helyezik a hangsúlyt. Ennek előmozdítása érdekében az EU-n belül letelepedett szolgáltatóknak kapcsolattartási pontokat kell kijelölniük, az EU-ban letelepedési hellyel ugyan nem rendelkező, de ott szolgáltatást nyújtó szolgáltatóknak pedig jogi képviselőt kell megjelölniük. A felhasználókat a szolgáltatóknak a szerződési feltételekben kell tájékoztatniuk a szolgáltatáshasználat korlátairól, például a tartalommoderálásról, illetve átláthatósági jelentésekben kell beszámolniuk tevékenységükről.

A DSA nagy hangsúlyt fektet a jogellenes tartalmak elleni fellépésre, a tárhelyszolgáltatókra vonatkozó szabályrendszertől indulva a szolgáltatókra a jogellenes tartalmak elleni fellépéssel kapcsolatos kötelezettségeket is telepít. Annak, hogy a DSA először a tárhelyszolgáltatók esetében szól a jogellenes tartalmak elleni fellépésről, az az oka, hogy a harmadik személyek tartalmai számára tárhelyet biztosító platformok esetében jóval nagyobb az illegális tartalmak előfordulásának kockázata, mint a többi közvetítő szolgáltató esetében. Noha viszonylag részletes szabályokat fogalmaz meg a rendelet a tartalmak elleni fellépésre, azt, hogy mely tartalmak minősülnek jogellenesnek, még csak példálózva sem rögzíti. Ernyőmeghatározásként a fogalommeghatározásokat tartalmazó 3. cikkben mindössze azt fogalmazza meg, hogy jogellenes minden olyan információ, amely nem felel meg az uniós jognak, vagy bármely tagállam jogának. E megfogalmazásból, de a (2) preambulumbekezdésből is kitűnik, hogy a jogellenes információk csoportját a rendelet nem kívánja a büntetőjogi normát sértő tartalmakra korlátozni. Idetartoznak azok az információk is, amelyek fogyasztóvédelmi szabályokat, szerzői jogi szabályokat, illetve közigazgatási jellegű szabályokat (élő állat szabálytalan értékesítése) sértenek. A fogalommeghatározásból az is kitűnik, hogy a jogellenesség

megállapításakor nemcsak az uniós jog által szankcionált cselekményeket lehet jogellenes információközlésként figyelembe venni, hanem a tagállami jogrendszerekben meghatározott normasértő információközléseket is.

A tárhelyszolgáltatók és az online platformok elsődleges kötelezettsége, hogy olyan bejelentési mechanizmusokat működtessenek, amelyek segítségével bejelenthetők a jogellenesnek vélt tartalmak, akár magánszemélyek, akár szervezetek által. Amennyiben akár bejelentés alapján, akár más forrásból a szolgáltatóban gyanú ébred, hogy valamely személy életét vagy biztonságát fenyegető bűncselekmény történt, van folyamatban vagy előkészületben, azt haladéktalanul jeleznie kell az érintett bűnüldözési vagy igazságügyi hatóság számára. Ha a szolgáltató nem tudja megállapítani az érintett bűnüldözési vagy igazságügyi hatóságot, lehetősége van a saját letelepedési helye szerinti tagállamban is megtenni ezt a jelzést.

Eljárási oldalon jelentős újítása a DSA-nak a jogellenes tartalmak elleni fellépésre vonatkozó, valamint az információszolgáltatásra vonatkozó végzések kibocsátásának lehetősége. A tagállamok igazságügyi vagy közigazgatási hatóságainak lehetőségük van arra, hogy a jogellenes tartalom elleni fellépésre felszólító végzést küldjenek közvetlenül a közvetítő szolgáltatónak. A végzések tartalmi követelményeit a rendelet részletesen szabályozza, e helyütt csak annyit emelnék ki, hogy a végzést kibocsátó hatóságnak indokolnia kell, hogy miért tekinti jogellenesnek a szóban forgó információt (akár uniós, akár nemzeti jog rendelkezésének megjelölésével). Az információszolgáltatásra vonatkozó végzések azt a célt szolgálják, hogy a tagállamok igazságügyi vagy közigazgatási hatóságai a szolgáltatások igénybe vevőiről, felhasználóiról információt kérhessenek, ha ezt bűnüldözési érdek, például az elkövetők azonosítása indokolja. A szolgáltatók mellett a végzést kibocsátó hatóságoknak a végzést meg kell küldeniük a saját országuk digitális szolgáltatási koordinátorának is.

A digitális szolgáltatási koordinátorok a közvetítő szolgáltatók felügyeletét ellátó hatóságok. E digitális szolgáltatási koordinátorok hatásköre meglehetősen széles, és olyan elemeket is magában foglal, amelyek korábban kifejezetten büntetőeljárási környezetben jelentek meg, például adatkérés, lefoglalás, ezen belül a DSA rendelkezéseit be nem tartó szolgáltatókat szankcionálhatják. A koordinátoroknak ezenfelül a tagállamok közötti információáramlás segítésében van nagy szerepük. Az említett végzéseket például a digitális szolgáltatási koordinátoroknak meg kell osztaniuk a többi tagállam koordinátorával is, valamint figyelemmel kell kísérniük azok elintézését.

Javaslat: az Európai Parlament és a Tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról

2016 tavaszán a brüsszeli terrortámadást[192] követően az európai bel- és igazságügyi miniszterek közös nyilatkozatot adtak ki, amelyben szorgalmazták az elektronikus bizonyítékokhoz való hozzáférés gyorsítását, valamint a közös nyomozócsoportok alakítását a bizonyítékok eredményesebb összegyűjtése és megőrzése szempontjából.[193] Ennek folyományaként a Tanács következtetéseket fogadott el a kibertérben gyakorolt büntető igazságszolgáltatás javításáról, majd 2018-ban felkérte a Bizottságot, hogy nyújtson be jogalkotási javaslatot az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférés közös, uniós szabályainak megteremtése érdekében. 2018-ban a Bizottság nyilvánosságra hozta a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló javaslatát.[194] A javaslat indokolásának már az első mondata is a közösségi média, valamint az azonnali üzenetküldő alkalmazások fontosságát hangsúlyozza,[195] rámutatva arra, hogy ezek a szolgáltatások a bűncselekmények elkövetői számára is megkönnyítik az online kommunikációt, néhány cselekmény (például a tartalomközléssel megvalósuló deliktumok) számára pedig olyan elkövetési helyet biztosítanak, ahol a nagy nyilvánosság érhető el. A javaslat indokolása kimondottan felhívja a figyelmet arra, hogy az online deliktumokkal összefüggő bizonyítékok igen gyakran internetes közvetítő szolgáltatóknál találhatók, azok illékony természetére figyelemmel pedig fontos, hogy a határokon átnyúló megkeresések gyorsan és hatékonyan legyenek elintézve. A rendelettervezet fő újításai tehát a más joghatósági területen található szolgáltatók által tárolt vagy birtokolt elektronikus bizonyítékok biztosítását és összegyűjtését megkönnyítő, közlésre kötelező európai határozat, valamint a megőrzésre kötelező európai határozat intézményeinek bevezetése. Mindkét határozatot tagállami igazságügyi hatóságnak kell kibocsátania, kötelezettjük pedig közvetlenül – tehát a joghatósággal rendelkező tagállam bevonása nélkül – az elektronikus hírközlési

192 Rankin–Henley 2016.

193 *Az Európai Unió bel- és igazságügyi minisztereinek, valamint az uniós intézmények képviselőinek közös nyilatkozata a 2016. március 22-i brüsszeli terrorista merényletek kapcsán* 2016.

194 Javaslat: Az Európai Parlament és a Tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról.

195 1. A javaslat háttere – A javaslat indokai és céljai.

szolgáltatók, közösségi oldalak, online piacterek szolgáltatói, egyéb tárhelyszolgáltatók és az IP-címhez, illetve a doménnév-nyilvántartásokhoz hasonló internetes infrastruktúra szolgáltatói.

A szolgáltató a rendelettervezet értelmezésében háromféle szolgáltatástípust takar. Jelenti egyrészt az Európai Elektronikus Hírközlési Kódexről szóló irányelv szerinti elektronikus hírközlési szolgáltatásokat,[196] így az internethozzáférés-szolgáltatásokat, a személyközi hírközlési szolgáltatásokat, valamint a jelátvitelből álló szolgáltatásokat (például műsorterjesztésre használt átviteli szolgáltatások). A kötelezettséggel terhelt szolgáltatók közé tartoznak a 2015/1535. európai parlamenti és tanácsi irányelv által szabályozott információs társadalommal összefüggő szolgáltatások[197] közül azok, amelyek esetében az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásoknak, beleértve a közösségi oldalakat, a felhasználóik közötti ügyleteket megkönnyítő online piactereket és egyéb tárhelyszolgáltatókat.[198] Az irányelv hatálya alatt álló szolgáltatók harmadik csoportjába pedig az internetes doménnév-szolgáltatók és IP-cím-szolgáltatók tartoznak. A rendelettervezet által nevesített szolgáltatói kör több ponton is átfedést mutat a már korábban ismertetett Eker. irányelv által szabályozott szolgáltatókkal. A kötet szempontjából a legfontosabb, hogy az E-bizonyításról szóló javaslat szintén telepít kötelezettségeket azokra a tárhelyszolgáltatókra (közösségimédia-platformokra, videómegosztó platformokra, online piacterekre), amelyeket az Eker. irányelv is szabályoz.

A közlésre kötelező európai határozat esetében a más tagállamban letelepedett szolgáltatót egy tagállam arra kötelezheti, hogy elektronikus bizonyítékokat közöljön,[199] míg a megőrzésre kötelező európai határozat esetében a kötelezettség címzettjének csupán adatmegőrzési kötelezettsége lenne.[200] Az Eker. irányelv által részletesen szabályozott szolgáltatói felelősség kérdése ugyanis az E-bizonyíték rendelettervezet javaslatainak fényében is vizsgálandó. A tárhelyszolgáltatók esetében a szolgáltató harmadik személyek tartalmaiért viselt felelősségét az keletkezteti, ha a jogsértő tartalmakról való tudomásszerzést követően nem intézkednek haladéktalanul azok eltávolításáról. A bármely tagállamból érkező európai határozat, amennyiben az tartalommal

196 2. cikk (3) a) pont.

197 A 2015/1535 irányelv 1. cikk (1) b) pontja szerint „szolgáltatás": az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás.

198 2. cikk (3) b) pont.

199 2. cikk (1).

200 2. cikk (2).

kapcsolatos, megalapozhatja a szolgáltató tudomásszerzését. A megőrzésre kötelező európai határozat esetében pedig az Ekertv. felelősségkizáró rendelkezéseivel való összhang a szolgáltatók részéről azt kívánja meg, hogy az adatok megőrzéséről olyan formában gondoskodjanak, hogy közben a kérdéses tartalom ne legyen hozzáférhető a felhasználók számára, amelyet megvalósíthatnak ideiglenes eltávolítással vagy a hozzáférés ideiglenes megakadályozásával.

Mindkét európai határozat az elektronikus bizonyítékok meghatározott körére vonatkozik. A rendelettervezet értelmezése szerint az elektronikus bizonyíték olyan elektronikus formában tárolt bizonyíték, amely a tárolt előfizetői adatokból, hozzáférési adatokból, tranzakciós adatokból és tartalmi adatokból áll.[201] Az előfizetői adatok egyik csoportját a személyazonosító adatok, úgymint a megadott név, születési idő, postai vagy földrajzi cím, számlázási és fizetési adatok, telefonszám vagy e-mail-cím,[202] másik csoportját pedig a szolgáltatás típusára és tartalmára vonatkozó adatok – beleértve a szolgáltatásnyújtás technikai paramétereit, a felhasználó számára biztosított interfészeket azonosító adatokat is – képezik.[203] Nem tartoznak azonban az előfizetői adatok közé a felhasználó által megadott vagy a felhasználó kérésére létrehozott jelszavak és más, a jelszó helyett használt hitelesítési eszközök. A hozzáférési adatok körébe főként azok a szolgáltatás használatával összefüggésbe hozható adatok tartoznak, amelyek lehetővé teszik a felhasználó azonosítását, így: használat dátuma és időpontja, a szolgáltatásba való belépés és kilépés időpontja, az internet-hozzáférési szolgáltató által a szolgáltatás felhasználója részére kiosztott IP-cím, a használt interfész azonosítója és a felhasználóazonosító, valamint az ezekkel összefüggő elektronikus hírközlési metaadatok.[204] Tranzakciós adatokon olyan adatokat értünk, amelyek a szolgáltatás használata során a szolgáltatónál keletkeznek, például az üzenetek vagy más típusú interakciók forrásai, címzettjei, a felhasználó által használt készülék fellelhetőségére vonatkozó adatok, dátum, időpont, időtartam, méret, útvonal, formátum, a használt protokoll és a tömörítés típusa.[205] Tartalmi adat pedig minden, az előbbiekben felsoroltakon túli digitális formátumban tárolt adat, így bármilyen szöveg, hang, kép, audiovizuális tartalom ebbe a körbe tartozhat.[206]

201 2. cikk (6).
202 (7) a) pont.
203 (7) b) pont.
204 (8).
205 (9).
206 (10).

Fontos rendelkezései a javaslatnak azok a szakaszok, amelyek azt határozzák meg, hogy milyen esetekben van lehetőség az egyes adatok közlésére vagy megőrzésére kötelező európai határozat kibocsátására. Előfizetői vagy hozzáférési adatok közlésére vonatkozó határozat kibocsátható bármilyen bűncselekmény vonatkozásában.[207] Korlátozottabban kötelezhetők a tranzakciós vagy tartalomra vonatkozó adatok közlésére a szolgáltatók, hiszen a rendelettervezet szerint csak meghatározott esetekben lesz lehetőség határozat kibocsátására. A tranzakciós vagy tartalomra vonatkozó adatok közlésére csak azon bűncselekmények vonatkozásában kötelezhető a szolgáltató, amelyek büntetési tételének felső határa a kibocsátó államban legalább három év szabadságvesztés,[208] vagy amennyiben az eljárás tárgya az alábbi információs rendszer felhasználásával elkövetett cselekmények valamelyike:

- A 2001/413/IB tanácsi kerethatározat szerinti fizetési eszközök csalárd felhasználása, az azzal kapcsolatos bűncselekmény előkészülete, illetve a jogellenes haszon szerzése céljából pénzbeli érték vagy virtuális fizetési eszköz átutalása, amennyiben az információs rendszer működésének akadályozása vagy működésébe való jogosulatlan beavatkozás, vagy számítógépes adatok bevitele, módosítása, törlése, továbbítása vagy hozzáférhetetlenné tétele révén valósul meg.
- A 2011/92/EU európai parlamenti és tanácsi irányelv szerinti szexuális bántalmazással, kizsákmányolással, gyermekpornográfiával kapcsolatos bűncselekmények, a gyermekkel való, szexuális céllal történő kapcsolatfelvétel, illetve az ezekkel kapcsolatos felbujtás, bűnsegély, továbbá ezek kísérlete.
- A 2013/40/EU európai parlamenti és tanácsi irányelv szerinti információs rendszerekhez való jogellenes hozzáférés, rendszert vagy adatot érintő jogellenes beavatkozás, jogellenes adatszerzés, továbbá ezeknek a cselekményeknek az elkövetéséhez eszköz biztosítása, illetve az ezekkel kapcsolatos felbujtás, bűnsegély, továbbá ezek kísérlete.

Lehetőség van a tranzakciós vagy tartalomra vonatkozó adatok közlésére kötelezésre a 2017/541 európai parlamenti és tanácsi irányelv szerinti terrorista bűncselekmények és terrorista csoporthoz kapcsolódó bűncselekmények, terrorista tevékenységekhez kapcsolódó bűncselekmények esetében is.

Az adatok megőrzésére kötelező európai határozat kibocsátására bármelyik adatfajta vonatkozásában bármelyik bűncselekmény esetében lehetőség van. Feltétele azonban

[207] 5. cikk (3).
[208] 5. cikk (4) a).

a határozat kibocsátásának az, hogy az érintett adatok eltávolításának, törlésének vagy megváltoztatásának megakadályozása céljából szükséges és a védendő érdekkel arányos legyen.

A rendelettervezet által szabályozni kívánt határozattípusok végrehajtásának módszeréről is részletesen szól a javaslat. A határozatot speciális tanúsítványok – közlésre kötelezés esetében közlésre kötelező európai határozatra vonatkozó tanúsítvány (KKEHT), megőrzésre kötelezés esetében megőrzésre kötelező európai határozatra vonatkozó tanúsítvány (MKEHT) – révén kell megküldeni a címzetteknek.[209] A címzettnek a KKEHT-ban feltüntetett kibocsátó hatóságnak vagy bűnüldöző hatóságoknak, legkésőbb az átvételtől számított 10 napon belül meg kell küldenie a kért adatokat,[210] míg a MKEHT esetében a címzettnek indokolatlan késedelem nélkül gondoskodnia kell a kért adatok megőrzéséről.[211] A büntetőeljárás sikerét és az elkövető elszökésének, elrejtőzésének veszélyét minimalizáló garanciális rendelkezés, hogy a kibocsátó hatóság felhívására a szolgáltatóknak tartózkodniuk kell azon személy tájékoztatásától, akinek az adatait kérik.[212]

A rendelettervezet rendelkezik arról is, hogy milyen szankciók alkalmazhatók azokkal a szolgáltatókkal szemben, akik nem tesznek eleget az adattovábbítási, illetve megőrzési kötelezettségüknek. A tagállamoknak – a nemzeti jogukban előírt büntetőjogi szankciókon túl – lehetőségük van hatékony, arányos és visszatartó erejű pénzbeli szankciókat alkalmazni a szolgáltatókkal szemben.[213]

Javaslat: az Európai Parlament és a Tanács rendelete a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról

A 2021/1232/EU rendelet szabályai a 3.2.6. pontban írtaknak megfelelően nem kötelezőek, és csak ideiglenes jellegűek. Mivel a szabályok csak 2026 márciusáig alkalmazhatók, az Európai Uniónak gondoskodnia kell azokról az új szabályokról, amelyek a gyermekek megfelelő online védelmének biztosítására hivatottak, átfogó

209 8. cikk (1).
210 9. cikk (1).
211 10. cikk (1).
212 11. cikk (1).
213 13. cikk.

és kötelező jelleggel szabályozzák az online szolgáltatók kötelezettségeit a gyermekek szexuális bántalmazását ábrázoló tartalmak vonatkozásában.

A rendelettervezet az információs társadalommal összefüggő szolgáltatásokat nyújtó szolgáltatókra különleges kötelezettségeket telepítene. Az információs társadalom szolgáltatásai közül értelemszerűen itt a tárhelyszolgáltatók, azokon belül az online platformok a kötelezettségek fő címzettjei, hiszen általában az ő rendszereikben van jelen nagyobb számban ellenőrizetlen felhasználói tartalom. A tárhelyszolgáltatóknak és a személyközi hírközlési szolgáltatásokat nyújtó szolgáltatóknak kockázatértékelést kell végezniük,[214] amelynek során figyelembe kell venniük azokat az azonosított eseteket, amikor szolgáltatásukat korábban gyermekek szexuális bántalmazására használták, a szabályzatok megfelelőségét, a szolgáltatás kialakítását és működését, valamint a felhasználók általános viselkedését. A kockázatértékelés során a szolgáltatóknak különös figyelmet kell fordítaniuk arra, hogy a gyermekek használhatják-e, és ha igen, akkor hogyan a szolgáltatást, és meg kell vizsgálniuk, hogy a kiskorú felhasználókkal hogyan lehet kapcsolatba lépni a szolgáltatás használata során. A feltárt kockázatokhoz mérten a szolgáltatóknak kockázatcsökkentő intézkedéseket kell életbe léptetniük,[215] ami lehet a tartalommoderálás vagy az ajánlórendszerek finomhangolása, a döntéshozatali folyamatok, belső eljárások, határidők, szerződési feltételek felülvizsgálata. Az elvégzett kockázatértékelés eredményéről a szolgáltatóknak három hónapon belül tájékoztatniuk kell a saját tagállamuk koordináló hatóságát.[216]

A rendelettervezet az alkalmazásboltok (szoftveralkalmazás-áruházak) számára azt írná elő, hogy az alkalmazás- és szoftverfejlesztőkkel közösen vizsgálják meg, hogy fennáll-e az esélye annak, hogy az alkalmazást gyermekekkel való kapcsolatfelvételre használják,[217] és intézkedéseket hozzanak annak érdekében, hogy a megakadályozzák, hogy a gyermekek hozzáférjenek az ilyen alkalmazásokhoz.[218]

Az anyagi jogi rendelkezések mellett a rendelettervezet eljárási jellegű szabályokat is megfogalmaz, amiatt, hogy eredményesebbé tegye az EU országai közötti együttműködést. Eljárási típusú rendelkezése a felderítést elrendelő határozat, amely alapján a tagállami hatóságok felhívhatják a tárhelyszolgáltatókat és a személyközi hírközlési szolgáltatást nyújtó szolgáltatókat arra, hogy bizonyos, a gyermekek szexuális bántalmazásával összefüggő eseteket vizsgáljanak ki. Az EU-n belüli bűnügyi együttműködés

214 3. cikk (1).
215 4. cikk.
216 5. cikk.
217 6. cikk (1) a).
218 6. cikk (1) b).

keretében lehetőség van arra is, hogy egy tagállam felkérjen egy másik tagállamot arra, hogy bocsásson ki a területén letelepedett tárhelyszolgáltatóval szemben felderítést elrendelő határozatot.[219] Eljárási jellegű szabály vonatkozik az eltávolítást elrendelő határozatokra is, amelyet a joghatósággal rendelkező tagállam igazságügyi vagy más hatóságai bocsáthatnak ki a szolgáltató részére.

Az informatikai bűncselekmények elleni fellépés az Egyesült Királyságban, Franciaországban és Németországban

A nemzetközi és uniós normák ugyan egy használható keretet kölcsönöznek az informatikai bűncselekmények elleni fellépésnek, de az egyes országoknak megvannak a maguk megküzdési stratégiái és részletszabályai, amelyekkel eredményesebbé tehetik az online térben előforduló deliktumok elleni küzdelmet. Az irányelvi szintű uniós szabályok esetében a tagállamoknak átültetési kötelezettségük is van, vagyis az irányelvi előírások valamilyen formában biztosan megjelennek a belső jogrendszerek szabályai között. A kötet jelen részében három olyan európai ország szabályozását mutatom be, amelyek az internetszabályozás úttörői között szerepelnek, ezek az Egyesült Királyság, Franciaország és Németország. Ezen országok szabályai gyakran mintaként szolgálnak más országoknak, sőt előfordul, hogy egyes megoldások még az uniós jogalkotókat is megihletik – például a német tartalom-bűncselekmények elleni fellépésről szóló NetzDG,[220] amelynek a megoldásai több helyütt visszaköszönnek a DSA rendelettervezetben.

Egyesült Királyság

Az Egyesült Királyság vezető szerepet tölt be a digitális világ alakításában. Az internet széles körű elterjedése és a folyamatosan fejlődő digitális gazdaság azonban veszélyeket is hozott magával. A brit Belügyminisztérium *(Home Office)* által 2010-ben megjelentetett Kiberbűnözési Stratégia *(Cyber Crime Strategy)*[221] szerint az Egyesült Királyság internetes piaca az egyik legnagyobb Európában.

[219] 7. cikk.
[220] Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352).
[221] Home Office 2010.

A brit jogrendszer két fajtáját különbözteti meg az informatikai bűncselekményeknek: a számítógépfüggő bűncselekményeket *(cyber-dependent crimes),*[222] valamint a számítógép által lehetővé tett bűncselekményeket *(cyber enabled crimes).*[223] A számítógépfüggő bűncselekmények közé azok a deliktumok tartoznak, amelyeket új technológiákkal követnek el, és az elkövetés kizárólag számítógéppel történhet. Az ebbe a csoportba tartozó cselekmények esetében mind az elkövetés eszköze, mind annak tárgya az információs rendszer. Ilyen az információs rendszer vagy adat megsértésével kapcsolatos összes cselekmény, így a kártékony programok terjesztése, a hackelés, adatokkal való visszaélés.

A számítógép által lehetővé tett cselekmények közé azok a hagyományos bűncselekmények tartoznak, amelyek elkövetésében új dimenziót nyitott a számítógép és az internet. Ezek a cselekmények korábban az offline világban is léteztek (például a szerzői jogsértés, vagy a csalás), az infokommunikációs technológia azonban nagyságrendi növekedést hozott elkövetésükben. Ezeket a cselekményeket az alábbiak szerint több kategóriába lehet sorolni:

- gazdasági bűncselekmények, ideértve a csalást, a szellemi tulajdonnal kapcsolatos bűncselekményeket;
- az illegális termékek adásvételére létrehozott online piacterek működtetését,
- az ártó szándékú, illetve sértő kommunikációt, ideértve a közösségi médiában közzétett jogsértő közléseket, a *cyberbullying*ot, a *mobbing*ot;
- a kimondottan egyéneket támadó cselekményeket, így a hozzájárulás nélkül közzétett szexuális felvételeket, a zaklatást, zsarolást;
- a gyermekek elleni online térben megvalósuló szexuális bűncselekményeket, például a gyermekek szexuális bántalmazása, a behálózás *(grooming),* illetve a gyermekpornográfia;
- az extrém pornográfia, obszcén közlések és tiltott felvételek;
- terrorizmussal kapcsolatos bűncselekmények.

Az Egyesült Királyság jogrendszerének egyik sajátossága, hogy nincs egységes szerkezetbe foglalt büntető törvénykönyve. Az egyes bűncselekmények vagy bűncselekménycsoportok külön törvényekben találhatók meg, amelyek anyagi és eljárásjogi szabályokat egyaránt tartalmaznak, illetve vannak olyan deliktumok, amelyeket teljes mértékben a *common law,* a bírói gyakorlat szabályoz. A 20. századtól már egyértelmű

[222] McGuire–Dowling 2013a.
[223] McGuire–Dowling 2013b.

a hajlandóság a bűncselekmények kodifikálására – részben amiatt is, hogy amíg az Egyesült Királyság az Európai Unió tagja volt, számos jogforrás átültetésének kellett eleget tennie –, ezért az informatikai bűncselekmények, illetve ezen deliktumokkal foglalkozó rendelkezések több törvényben is megjelennek.

A számítógépfüggő bűncselekmények (cyber-dependent crimes)

A számítógépfüggő (avagy tisztán informatikai) bűncselekmények olyan deliktumok, amelyeket csak számítógéppel, számítógépes hálózattal vagy egyéb infokommunikációs technológia felhasználásával lehet elkövetni. A számítógépfüggő bűncselekményeket további két csoportra lehet osztani:[224]

- a számítógépes hálózatokba való jogszerűtlen behatolások, valamint
- a számítógép működését megzavaró, teljesítményét csökkentő támadások (*malware,* DDOS-támadások) csoportjára.

A számítógépes rendszerek elleni bűncselekményekről és támadásokról szól az 1990-ben elfogadott számítógépes visszaélésekről szóló törvény (Computer Misuse Act, 1990), amely a szűk értelemben vett informatikai bűncselekményeket szabályozza. A törvény konzekvensen a „számítógép" fogalmat használja, azonban nem határozza meg, hogy mit ért ez alatt, így az értelmezést nyitva hagyja, hogy ebbe a körbe lehessen sorolni a technológiai fejlődés során létrejövő újfajta eszközöket is. Iránymutatásul szolgálhatnak azonban a DPP v. McKeown, valamint a DPP v. Jones ügyek,[225] amelyek úgy határozták meg a számítógépet, mint információ tárolására, feldolgozására és kinyerésére szolgáló eszközt. Ez a megfogalmazás magában foglalhatja a hagyományos asztali számítógépek mellett már a táblagépeket, de akár az okostelefonokat is.

A törvény a számítógépes bűncselekmények körében összesen öt tényállást különböztet meg.

- Jogosulatlan hozzáférés számítógépen tárolt adatokhoz (hackelés):
  „A person is guilty of an offence if
  (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

[224] The Crown Prosecution Service 2019.
[225] DPP v. Mcmahon 1984 ILRM 461 és DPP v. Jones [1997] 2 Cr App R 155 HL.

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case."

- Jogosulatlan hozzáférés további bűncselekmények elkövetésének vagy elősegítésének szándékával:

  „A person is guilty of an offence under this section if he commits an offence under section 1 above («the unauthorised access offence») with intent

  (a) to commit an offence to which this section applies; or

  (b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence."

- Illetéktelen cselekmények, amelyeket a számítógép működése akadályozásának szándékával követtek el, valamint azok a gondatlanságból elkövetett cselekmények, amelyek akadályozzák a számítógép működését:

  „(1) A person is guilty of an offence if

  (a) he does any unauthorised act in relation to a computer;

  (b) at the time when he does the act he knows that it is unauthorised; and

  (c) either subsection (2) or subsection (3) below applies.

  (2) This subsection applies if the person intends by doing the act

  (a) to impair the operation of any computer;

  (b) to prevent or hinder access to any program or data held in any computer; or

  (c) to impair the operation of any such program or the reliability of any such data; or

  (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

  (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) to (c) of subsection (2) above."

- Komoly kárt okozó vagy komoly kár bekövetkezésének kockázatával járó illetéktelen cselekmények:

  „(1) A person is guilty of an offence if

  (a) the person does any unauthorised act in relation to a computer;

  (b) at the time of doing the act the person knows that it is unauthorised;

  (c) the act causes, or creates a significant risk of, serious damage of a material kind; and

  (d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused."

- Komoly kárnak az olyan anyagi jellegű kár minősül, amely károsítja az emberek jólétét, a környezetet, bármely ország gazdaságát, illetve nemzetbiztonságát:
  „(2) Damage is of a «material kind» for the purposes of this section if it is
  (a) damage to human welfare in any place;
  (b) damage to the environment of any place;
  (c) damage to the economy of any country; or
  (d) damage to the national security of any country."
- Az előzőekben meghatározott bűncselekmények elkövetéséhez vagy elkövetésének elősegítéséhez használt tárgyak készítése, átalakítása, forgalomba hozatala, illetve a forgalomba hozatal felkínálása.

A számítógép által lehetővé tett bűncselekmények (cyber-enabled crimes)

A számítógép által lehetővé tett bűncselekmények tradicionális deliktumok, a számítógépfüggő bűncselekményekkel ellentétben ezeket infokommunikációs technológiák felhasználása nélkül is el lehet követni.

Külön törvény szabályozza a kommunikáció jogellenes lehallgatásának, vagyis a tiltott adatszerzésnek a kriminalizálását. A nyomozati hatáskörökről szóló törvény (Investigatory Powers Act, 2016) tiltja a nyilvános vagy magán-telekommunikációs hálózatokon vagy nyilvános postai szolgáltatáson keresztül zajló kommunikáció szándékos lehallgatását. A személyes adatokkal való visszaélésekhez kapcsolódó cselekményeket a brit adatvédelmi törvény (Data Protection Act, 2018) szabályozza. Eszerint büntetendő a személyes adatok hozzájárulás nélkül történő szándékos és gondatlan megszerzése és nyilvánosságra hozatala, személyes adatok nyilvánosságra hozatalának megrendelése, a hozzájárulás nélkül nyilvánosságra hozott vagy visszatartott személyes adatok adásvétele.

A kibertérben megvalósított csalást rendeli büntetni a csalásról szóló törvény (Fraud Act, 2006), amely az online visszaélésszerű cselekményekkel foglalkozik. A törvény büntetni rendeli azt is, amikor valaki hamis közösségimédia-profilt vagy felhasználói fiókot hoz létre, amennyiben ezzel a cselekménnyel hasznot szerzett. Az információs rendszerekkel elkövetett hamisítás jellegű cselekményeket általánosságban a hamisításról szóló törvény (Forgery and Counterfeiting Act, 1981) rendeli büntetni, a védjegyekkel és árujelzőkkel kapcsolatos hamisítási cselekményeket ellenben a védjegytörvény (Trade Marks Act, 1994).

A zenék, filmek és egyéb szerzői jog által védett művek kalózkodása esetében a szerzői jogról, használati mintákról és a szabadalmakról szóló törvény (Copyright Designs and Patents Act, 1988) rendelkezései alkalmazandók. Az internet és az egyre nagyobb elérhető sávszélesség az online kalózkodásnak kedvezett a leginkább. A szerzői jogi jogosultak bánatára ma már gyorsan, kiváló minőségben és különösebb előképzettség nélkül lehet letölteni tartalmakat az internetről. A szerzői jogvédett alkotásokkal kapcsolatos magatartások sokféleképpen megvalósulhatnak:

- fájlcserélő technológiák alkalmazásával;
- szerzői jog által védett művek weboldalakon vagy a közösségi médiában való engedély nélküli közzétételével;
- sportmérkőzések vagy koncertek élő, engedély nélküli közvetítésével (streaming);
- szerzői jog által védett művek feltöltése tárhelyszolgáltatásra és engedély nélküli hozzáférés biztosításával.

A rosszindulatú kommunikációról szóló törvény (Malicious Communications Act, 1988) rendeli büntetni azt, ha valaki gyötrelem vagy szorongás kiváltása érdekében küld illetlen vagy súlyosan sértő üzeneteket másnak, valamint azt, ha valaki fenyegetést vagy hamis információt küld (amennyiben tudatában van az állítás hamisságának).[226] A kommunikációról szóló törvény (Communications Act, 2003) büntetni rendeli, ha valaki nyilvános elektronikus hírközlési hálózaton súlyosan sértő vagy illetlen, obszcén vagy fenyegető üzeneteket vagy tartalmakat küld. Ez a szakasz rendeli büntetni azt is, ha valaki hamis üzeneteket küld azzal a szándékkal, hogy másokat bosszantson, kellemetlenséget vagy szükségtelen szorongást okozzon.[227] A büntető igazságszolgáltatásról és bíróságokról szóló törvény (Criminal Justice and Courts Act, 2015) rendeli büntetni azt az esetet, amikor valaki magántermészetű szexuális fényképeket vagy filmeket tesz közzé valamelyik szereplő hozzájárulása nélkül, amennyiben a célja, hogy gyötrelmet okozzon a felvétel szereplőjének.[228]

A gyermekek szexuális bántalmazásával összefüggő cselekményeket és a gyermekpornográfiát tartalmazó felvételekkel kapcsolatos cselekményeket a szexuális bűncselekményekről szóló törvény (Sexual Offences Act, 2003), a gyermekekkel való fajtalankodásról szóló törvény (Indecency with Children Act, 1960), valamint a gyermekvédelmi törvény (Protection of Children Act, 1978) kriminalizálják. Az obszcén

[226] Computer Misuse Act Section 1.
[227] Computer Misuse Act Section 127.
[228] Computer Misuse Act Section 33.

közlések, valamint az obszcénnak minősülő extrém pornográfia az obszcén közlésekről szóló törvény (Obscene Publications Act, 1959) szerint szabályozottak.

A brit ügyészek számára közzétett útmutató szerint[229] a közlések vizsgálatakor az alábbiakat indokolt figyelembe venni:

- a kommunikáció fenyegető jellegű-e (fenyeget-e személy elleni erőszakkal vagy vagyonban okozott kárral),
- kimondottan egy egyént vagy egyének csoportját célozza-e,
- sért-e bírósági határozatban megítélt dolgot vagy törvényi rendelkezést,
- erősen sértő, trágár, obszcén vagy hamis-e.

Ezen szempontok alapján ebbe a körbe tartozik az online zaklatás, illetve a *cyberbullying,* a személyazonosság-lopás, illetve a szexuális motiváltságú cselekedetek, úgymint a hozzájárulás nélkül közzétett szexuális felvételek, a zsarolás, a gyermekpornográfiával való visszaélések, illetve a gyermekek „behálózása" *(grooming),* az obszcén tartalmak, így az obszcenitás mértékét elérő extrém szexuális felvételek. Az Egyesült Királyság büntetőkódexe (Criminal Justice and Courts Act, 2015) 2015 óta rendelkezik arról, hogy a magántermészetű fénykép- és videófelvételek közzététele azzal a szándékkal, hogy a közlő másnak szenvedést okozzon *(intent to cause distress),* szabadságvesztéssel büntethető. Rosalind Setterfield rámutat,[230] hogy ezek a szabályok azonban csak Angliára és Walesre irányadók, lehetőség van viszont más jogszabályok alapján fellépni azokkal szemben, akik hozzájárulás nélkül tesznek közzé más személyeket ábrázoló szexuális felvételeket. Nevezetesen:

- a rosszindulatú kommunikációról szóló törvény és a kommunikációról szóló törvény alapján, amelyek egyaránt tartalmaznak a súlyosan sértő *(grossly offensive)* közlések visszaszorítását célzó rendelkezéseket;
- a zaklatástól való védelemről szóló törvény (The Protection from Harassment Act, 1997) alkalmazható, ha az elkövető tevékenysége rendszeres;
- a gyermekvédelmi törvény (Protection of Children Act, 1978) alkalmazható, ha a sértett még nem volt nagykorú.

A terrorizmusról szóló törvény (Terrorism Act, 2000) is felsorol jó néhány olyan tartalomközléssel megvalósítható bűncselekményt, amelyek elkövetése nagyrészt az online térbe tevődött át. Ilyen a terrorszervezet támogatására való felhívás, az ilyen szervezetet

229 The Crown Prosecution Service 2019.
230 Setterfield 2019.

támogató vélemény vagy meggyőződés kifejtése, a szervezet tagjai számára találkozó szervezése, nyilvános adománygyűjtés, oktatóanyagok, képzések megszervezése terrorcselekmények, fegyverhasználat kapcsán, vagy a terrorcselekmény elkövetésére uszítás, az ilyen cselekmény előkészítése, vagy az azzal történő fenyegetés.

Tartalommoderálás az online platformokon: úton az Online Safety Act elfogadása felé

Mindenképpen érdemes néhány szóra egy 2023 végén elfogadott törvény, az Online Safety Act is, amellyel a brit jogalkotó célja, hogy biztonságosabbá tegye az online világot a felhasználók számára. A jogszabály előzménye, az online ártalmakról szóló fehér könyv (Online Harms White Paper) kormányzati prioritásként határozta meg az internetes ökoszisztéma biztonságosabbá tételét és a platformokba vetett állampolgári bizalom helyreállítását.[231] A fehér könyv megjelenését nem sokkal már törvényjavaslat, az Európa-szerte elhíresült Online Safety Bill követte. Az Online Safety Act maga nem büntető jellegű jogi norma, hanem alapvetően az online platformok jogellenes és ártalmas tartalmakkal kapcsolatos kötelezettségeit és felelősségét igyekszik rendezni. A törvény az online platformoknak valójában csak két típusát szabályozza, a felhasználók közötti szolgáltatást *(user-to-user service),* valamint a keresőszolgáltatást *(search service)* nyújtó szolgáltatókat. Előbbi csoportba tartozna minden internetes szolgáltatás, amelyen a felhasználók más felhasználók által készített, feltöltött vagy megosztott tartalmakkal találkozhatnak, lényegében tehát a közösségi média és a videómegosztó platformok. A törvény az említett szolgáltatások nyújtói esetében különleges gondossági kötelezettségeket *(duty of care)* fogalmaz meg, amelyeknek azok a szolgáltatók kötelesek eleget tenni, amelyeknek jelentős számú brit felhasználójuk van, brit felhasználókat céloznak a szolgáltatásukkal, illetve amelyek hozzáférhetők az Egyesült Királyságban. Ezeknek a gondossági kötelezettségeknek a törvény szerint három fő területen kell eleget tenniük a szolgáltatóknak:

- a felhasználók védelme a jogellenes tartalmaktól;
- a gyermekek védelme érdekében hozott kiegészítő intézkedések;
- a felhasználók védelme az ártalmas, de nem jogellenes tartalmaktól.

231 Consultation outcome – Online Harms White Paper 2020.

Látható, hogy az online tér ártalmas tartalmait a javaslat három különálló csoportra bontja. Az Online Safety Act új és eddig büntetőjogi szankcióval nem sújtható cselekményeket is kriminalizálni rendel. Büntetendővé nyilvánítja az önbántalmazásra rábírást, a szexuális tartalmak kéretlen küldését *(cyberflashing),* valótlan információk küldését károkozási céllal, a fenyegető kommunikációt, az intim felvételekkel visszaélést, valamint az epilepsziás roham kiváltását célzó mozgóképek küldését *(epilepsy trolling).*

Fontos megemlíteni, hogy a törvény nemcsak a bűncselekményt megvalósító tartalmak elleni fellépést szabályozza, hanem külön rendelkezései vannak a gyermekekre ártalmas tartalmakról, valamint a mindenkire ártalmas, de nem jogellenes tartalmakról. Ezeknek a tartalmaknak a köréről nem találunk taxatív felsorolást a jogszabályban. Az Online Safety Act szabályai arról rendelkeznek, hogy a platformszolgáltatóknak fel kell lépniük az olyan tartalmakkal szemben is, amelyek büntetőjogi normát ugyan nem sértenek, mégis károsak a felhasználók – különösen a kiskorúak – számára. Ilyenek a veszélyes magatartásokra buzdító tartalmak, mint a különböző internetes kihívások, a táplálkozási zavarokat népszerűsítő vagy éppen az önkárosításra felhívó tartalmak. A tartalomszabályozásban a bűncselekményt megvalósító és az ártalmas/káros tartalmak megkülönböztetése nem unikális, a későbbiekben is látni fogjuk, hogy vannak más tagállamok is, amelyek használnak hasonló elhatárolást. Nem egyedi az sem, hogy az online platformokat terhelő kötelezettségek megállapításánál, a gazdasági szempontú, a belső piac eredményes működését előmozdító rendelkezések között megjelennek alapvetően deliktuális tőről fakadó, jogellenes cselekedetekre reagáló rendelkezések.

A szolgáltatókat a jogellenes, valamint az ártalmas tartalmakkal kapcsolatban alapvetően kétféle gondossági kötelezettség terhelné. Egyrészt kockázatértékelést *(risk assessment)* kell végezniük, másrészt olyan biztonsági intézkedéseket *(safety measures)* kell meghozniuk, amelyek biztosítják, hogy a jogellenes tartalmakat minél hamarabb eltávolítják, minél kevesebb felhasználó találkozik velük, illetve nem kerülnek újra fel a szolgáltatásba. A jogszabály kritikusai szerint mindez kellő szükségességi-arányossági tesztek bevezetése nélkül a szólásszabadság indokolatlan korlátozásához vezethet.[232]

[232] Trengove et al. 2022.

Franciaország

Franciaország kontinentális jogrendszerének szabályozási struktúrája már közelebb áll ahhoz, amit hazánkban is megszokhattunk. Franciaország 2006-ban ratfikálta a budapesti Cybercrime Egyezményt, így annak szabályai természetszerűleg a francia jogban is megjelennek. Az informatikai bűncselekményekkel kapcsolatos anyagi jogi szabályokat elsősorban a büntető törvénykönyv, a Code pénal[233] rendelkezései között kell keresnünk. A tisztán informatikai bűncselekményeket a francia jogalkotó a tulajdon elleni bűncselekmények között helyezte el. A törvény 323-1 szakasza az információs rendszerhez való jogosulatlan belépést, illetve az abban való bent maradást rendeli büntetni, méghozzá két évig terjedő szabadságvesztés büntetéssel vagy hatvanezer eurós pénzbüntetéssel.[234] Szigorúbban minősül a cselekmény, amennyiben az a rendszerben tárolt adatok törlésével, megváltoztatásával, illetve a rendszer működésének megváltoztatásával jár, ez esetben az elkövető három évig terjedő szabadságvesztés büntetéssel, illetve százezer euró pénzbüntetéssel néz szembe.[235] A törvényben egy sajátos minősített eset is megjelenik, amelyben a védett jogi tárgy egyrészt az állami rendszerek megbízható működéséhez, másrészt pedig a személyes adatok védelméhez fűződő érdek. Amennyiben az előzőekben leírt cselekményeket olyan állami rendszer ellen követik el, amely személyes adatok automatizált kezelését végzi, a büntetés öt évig terjedő szabadságvesztés és százötvenezer eurós pénzbüntetés.[236] A magyar joggal ellentétben, amely az információs rendszer és adat elleni bűncselekmény címszó alatt rendeli büntetni mind a rendszerrel, mind az abban tárolt adatokkal kapcsolatos visszaéléseket, a francia jog külön szakaszt rendel az információs rendszer, illetve az abban tárolt adat megzavarásának. Az információs rendszer működésének megzavarását a Code pénal 323-2 szakasza szabályozza, eszerint aki akadályozza vagy megzavarja a rendszer működését, öt évig terjedő szabadságvesztéssel és százötvenezer eurós

233 A törvénykönyv III., vagyon elleni bűncselekményekről szóló könyve tartalmazza a szűk értelemben vett informatikai bűncselekményeket, míg a magánéletet sértő cselekmények a személyek elleni bűncselekményeket szabályozó II. könyvben helyezkednek el.

234 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

235 Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

236 Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

pénzbüntetéssel szankcionálható. A személyes adatok kezelésére használt rendszerek működésének megzavarása ez esetben is súlyosabban minősül. A 323-3 szakasz rendezi az adatvisszaélésekkel kapcsolatos cselekményeket: aki szándékosan információs rendszerbe adatot visz be, onnan adatot von ki, adatot változtat meg, másol, továbbít, töröl, szintén öt évig terjedő szabadságvesztéssel és százötvenezer eurós pénzbüntetéssel sújtható.

Az olyan informatikai bűncselekményeket, ahol az elkövetés eszköze a számítógép, elszórtan találjuk meg a Code pénal rendelkezései között.

A jogosulatlan kifürkészés (levéltitok megsértése, tiltott adatszerzés) a személyiségi jogokat sértő bűncselekményeket szabályozó VI. fejezetben kapott helyet. Eszerint, aki rosszhiszeműen elektronikus hírközlő hálózaton keresztül küldött, továbbított vagy fogadott levelezést megszerez, eltérít, felhasznál vagy nyilvánosságra hoz, illetve olyan technikai eszközt használ, amely ezeket lehetővé teszi, egy évig terjedő szabadságvesztéssel és negyvenötezer eurós pénzbírsággal sújtható.[237] Franciaországban ez a cselekmény súlyosabban minősül, ha azt házastárs vagy élettárs sérelmére, illetve párkapcsolaton belül követik el, ebben az esetben a kiszabható büntetés két év szabadságvesztés és hatvanezer euró.[238]

Részletesen és modern szemlélettel szabályozza a francia jog a gyermekpornográfiával kapcsolatos cselekményeket is. A Code pénal 227-3 szerint hét év szabadságvesztéssel és százezer eurós pénzbüntetéssel büntetendő a kiskorúakat ábrázoló pornográf felvételek terjesztési céllal történő készítése és továbbítása.[239] A törvényszöveg szóhasználata mindenképpen mélyebb elemzést indokol, mivel olybá tűnik, hogy a gyermekekről készült pornográf felvételek csak akkor minősülnek büntetendőnek, amennyiben

[237] Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.

[238] Lorsqu'ils sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, ces faits sont punis d'une peine de deux ans d'emprisonnement et de 60 000 euros d'amende.

[239] Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.

azok terjesztési, továbbközlési céllal készülnek. A francia jogalkotó ezzel az olyan fiatalokat értintő tevékenységek dekriminalizálását valósította meg, mint a szexuális tartalmú üzenetek egymásnak való küldözgetése, a szexting. Fontos kiemelni, hogy a beleegyezési korhatár – ami Franciaországban 15 év – alatti gyermekekről készült felvételeknek a tartása ugyanúgy bűncselekmény, mint Magyarországon,[240] hiszen az ezt az életkort el nem érő gyermekekkel szemben él az a vélelem, hogy még nem kellően érettek a szexualitáshoz, így ahhoz sem, hogy az őket ábrázoló felvételekkel kapcsolatos tájékozott döntéseket meghozzák. A francia jog a tekintetben is újító természetű, hogy a behálózást *(grooming)* kifejezetten büntetni rendeli. Az a felnőtt tehát, aki arra törekszik rábírni kiskorúakat, hogy azok pornográf felvételeket, képeket, videókat küldjenek, komoly szankciókkal – hét év szabadságvesztéssel és százezer eurós pénzbüntetéssel – nézhet szembe, a cselekmény ráadásul súlyosabban minősül, ha a behálózni kívánt kiskorú a 15. életévét nem töltötte be.[241]

Franciaország az első európai országok egyike, amely a szexuális felvételek hozzájárulás nélküli közzétételét különálló tényállásban büntetni rendeli. A 2016-ban elfogadott digitális köztársaságról szóló törvény[242] értelmében két év szabadságvesztéssel, illetve hatvanezer eurós pénzbüntetéssel néz szembe, aki mások személyiségi jogait megsértve szexuális felvételeket tesz közzé. A rendelkezés beiktatására azért volt szükség, mert ugyanebben az évben a francia legfelsőbb bíróság a Code pénal magánélethez való jog megsértését kriminalizáló rendelkezését vizsgálva arra a megállapításra jutott, hogy a köznyelvben bosszúpornóként emlegetett jelenség nem büntetendő, amennyiben a hozzájárulás csak a közzététel esetében hiányzik, maga a szexuális felvétel azonban az abban részt vevők hozzájárulásával készült.[243] A digitális köztársaságról szóló jogszabály rendelkezése a közzétételt abban az esetben is büntethetővé nyilvánítja, ha a felvétel előállítása konszenzuson alapult.

Nem minden jogszabály-módosítás jár azonban sikerrel a tartalomszabályozás területén. 2020 májusában elfogadtak egy törvényt az internetes gyűlölködő

240 Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.

241 Le fait pour un majeur de solliciter auprès d'un mineur la diffusion ou la transmission d'images, vidéos ou représentations à caractère pornographique dudit mineur est puni de sept ans d'emprisonnement et de 100 000 euros d'amende.
Les peines sont portées à dix ans d'emprisonnement et à 150 000 euros d'amende lorsque les faits ont été commis à l'encontre d'un mineur de quinze ans. Elles sont portées à dix ans d'emprisonnement et à un million d'euros d'amende lorsque les faits ont été commis en bande organisée.

242 LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique.

243 Cour de cassation, criminelle, Chambre criminelle, 16 mars 2016, 15-82.676.

tartalmakról.[244] A törvény nyilvánvalóan jogellenes tartalmak, így a gyűlöletbeszéd, a terrorista tartalmak, illetve a gyermekpornográfia elleni erőteljesebb fellépésre kötelezte volna az online platformokat, 24 órán belüli eltávolítási kötelezettséget vezetve be. A rövid határidő elmulasztása esetén a törvény legfeljebb kétszázezer euró pénzbírság kiszabását tette lehetővé. Az előterjesztője után lex Aviának nevezett jogszabály egyes részeit a francia alkotmánybíróság hatályon kívül helyezte.[245] A francia alkotmánybíróság szerint a törvény megfogalmazása nem állta ki a szükségességi-arányossági teszt próbáját, mivel az egynapos határidő nem biztosít kellő időt a panaszolt tartalmak esetében a megfelelő vizsgálat lefolytatására. A szolgáltatók a szankcióktól tartva olyan tartalmakat is eltávolíthatnak, amelyeket nem indokolt, sőt amelyek a demokratikus diskurzus szempontjából értékes véleményeknek minősülhetnek, mindez pedig végső soron a véleménynyilvánítás szabadságához való jog csorbulását eredményezi.

Németország

Németországban szintén két csoportra oszthatók az informatikai bűncselekmények. A német Bundeskriminalamt különbséget tesz a szűk értelemben vett kiberbűnözés *(Cybercrime im engeren Sinne),* valamint a tág értelemben vett kiberbűnözés *(Cybercrime im weiteren Sinne)* között.[246] Előbbi kategóriába a tisztán informatikai bűncselekmények tartoznak, amelyek tárgya az információs rendszer, illetve hálózat, az utóbbiba pedig azok a cselekmények, ahol az információs rendszer csak eszköz, azaz lehetővé teszi, megkönnyíti a bűncselekmény elkövetését.

Szűk értelemben vett kiberbűnözés (Cybercrime im engeren Sinne)

Tisztán informatikai bűncselekmény a német jogban a jogosulatlan hozzáférés *(ausspähen von Daten),* a kifürkészés *(abfangen von Daten),* a lopott adatokkal való visszaélés *(Datenhehlerei),* az információs rendszerben tárolt adatok manipulálása *(Datenveränderung),* valamint az információs rendszer megsértése, a számítógépes szabotázs *(Computersabotage).* Az információs rendszerben tárolt adatok kettős természetét remekül illusztrálja a német büntető törvénykönyv (Strafgesetzbuch – Stgb.) rendszere,

[244] LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.
[245] Décision n° 2020-801 DC du 18 juin 2020.
[246] Bundeskriminalamt [é. n.].

amelyben a tisztán informatikai bűncselekményeket két külön fejezetben helyezték el. Egyes bűncselekményfajták az Stgb. 15., a magánélet és magánszféra megsértéséről szóló fejezetében szabályozottak, míg a többi tisztán informatikai bűncselekmény a büntetőjogi károkozásról szóló részben helyezkedik el. Az adat egyes cselekményfajtáknál a magánszféra részeként jelenik meg, integritásának védelme szorosan kapcsolódik a személyek magánszférájának, személyi autonómiájának védelméhez. Az adatokhoz való jogosulatlan hozzáférés, a kifürkészés, illetve a lopott adatokkal való jogosulatlan visszaélés esetében a védendő érdek a *privacy,* a magánszféra mint személyiségi jog, amelynek kapcsán Sólyom László is kiemelte, hogy a védelem független a tulajdonosi pozíciótól.[247] Az olyan cselekmények esetében, mint az információs rendszerben tárolt adatoknak vagy az információs rendszernek a megsértése, hangsúlyosabb az adat tulajdoni elem jellege, így az ebben okozott kár eltérő rendszertani elhelyezést tesz indokolttá.

A német jog érdekessége, hogy a számítógépbe való jogosulatlan belépést, a hackelést összekapcsolja az adatokhoz való hozzáféréssel, ehhez igazodva a cselekmény megnevezése is adatok kikémlelése. Az Stgb. 202a szakaszában szabályozott cselekmény, az információs rendszerbe a védelem megkerülésével történő belépés tehát csak akkor lesz tényállásszerű, ha az elkövető a belépéssel hozzáfér a rendszerben tárolt adatokhoz is:

> „Strafgesetzbuch § 202a Ausspähen von Daten
> (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

E megfogalmazásnak nyilvánvalóan kevés a relevanciája, hiszen nehezen képzelhető el olyan információs rendszer, amely nem tárol adatot. A törvényszöveg kapcsán kiemelendő az is, hogy abban puszta hozzáférésről van szó, az adatok tényleges megismerése (például fájlok megnyitása) vagy ellopása (a fájlok letöltése) nem szükséges elemek, ezek híján, a hozzáférés puszta absztrakt lehetőségével is megvalósul a bűncselekmény.

Az Stgb. 202b szakasza rendeli büntetni a kifürkészést, amely az adattovábbítás során, technikai eszközzel történő szándékos lehallgatást jelent:

247 Sólyom 1983: 17.

„202b Abfangen von Daten
Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist."

A német jog szerint az e cselekményekhez kapcsolódó előkészületi tevékenységek is büntetendők (Stgb. 202c), tilos tehát a jelszavak, biztonsági kódok, számítógépes programok előállítása, megszerzése, terjesztése, illetve az azokkal való kereskedelem is:

„(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,
herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft."

A törvény rendelkezik az jogosulatlanul megszerzett, ellopott adatokon végzett további műveletekről is: büntetendő, ha valaki egy feltört rendszerből a belépést követően adatokat megszerez, illetve ilyen adatokat terjeszt, vagy azokhoz hozzáférést biztosít:

„(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

A 303a szakaszban szabályozott adatmanipuláció esetében a törvény már az adat gazdasági jelentőséggel bíró kvázi dologi jellegére helyezi a hangsúlyt. Aki jogosulatlanul töröl, használhatatlanná tesz, megváltoztat, hozzáférhetetlenné tesz az információs rendszerben tárolt adatot, két évig tartó szabadságvesztéssel vagy pénzbüntetéssel néz szembe:

„§ 303a Datenveränderung
(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft."

A számítógépes szabotázs 303b szakaszban foglalt tényállása lényegében a magyar információs rendszer megzavarásával összefüggő, károkozó jellegű magatartásokat fogja össze. Idetartozik az adatmanipuláció, a károkozási célú kifürkészés, az adatfeldolgozó vagy adatátviteli rendszer megsemmisítése, megrongálása, használhatatlanná tétele:

„(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Tág értelemben vett kiberbűnözés (Cybercrime im weiteren Sinne)

Az információs rendszerhez kapcsolódó bűncselekményeket a német büntető törvénykönyvben is elszórtan találjuk meg, olyan deliktumokhoz kapcsolódóan, amelyek elsősorban a hagyományos környezetben terjedtek el, mielőtt áttevődtek az online közegbe.

A német jogrendszer a magyarhoz hasonlóan elválasztja a számítógépes csalást *(Computerbetrug)* a hagyományos csalástól. Az Stgb. 263a szakasza az adatokon végzett jogosulatlan műveletekkel történő károkozásról szól, vagyis arról az esetről, amikor az elkövető az információs rendszert „téveszti meg" valótlan, hamis vagy hamisított adatok betáplálásával, illetve adatok törlésével:

„§ 263a Computerbetrug
(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft."

Az információs rendszerrel kapcsolatos bűncselekmények között a német jogban is megtalálhatók a pornográf tartalmakkal kapcsolatos bűncselekmények, azzal, hogy Németország érzékelhetően szigorúbban bánik az online környezetben megjelenő szexuális jellegű tartalmakkal, mint mondjuk a magyar jog. Hazánkban a pornográf tartalmak nyilvánosságra hozatala nem valósít meg bűncselekményt, még akkor sem, ha ezekhez a tartalmakhoz kiskorúak is hozzáférnek. Magyarországon a kiskorúakra káros tartalmak közzététele legfeljebb médiajogi szabályt sért, így a tartalmat közzétevő felhasználókkal, médiaszolgáltatókkal szemben a médiaigazgatás eszközrendszerével lehetséges fellépni. A büntetőjogi tényállások közül esetleg a kiskorú veszélyeztetése jöhet szóba, ezt a deliktumot azonban csak a szülő, gondviselő vagy a gyermek felügyeletével megbízott személy követheti el, például azáltal, hogy pornográf felvételeket mutat, ad át az érintett gyermeknek. Németország a büntetőjog eszközrendszerével igyekszik elérni, hogy a kiskorúak kevesebb pornográf tartalommal találkozzanak a televízióban és az online környezetben. Az Stgb. 184 szakasza szerint, aki pornográf tartalmat 18 éven aluli személynek kínál, átad, vagy számára hozzáférhetővé tesz, illetve olyan nyilvános helyen tesz közzé vagy reklámoz pornográf tartalmat, ahol kiskorúak is láthatják (például kereskedelmi forgalomban vagy filmszínházban), egy évig terjedő szabadságvesztéssel vagy pénzbüntetéssel néz szembe.

„§ 184 Verbreitung pornographischer Inhalte

(1) Wer einen pornographischen Inhalt (§ 11 Absatz 3)

1. einer Person unter achtzehn Jahren anbietet, überläßt oder zugänglich macht,

2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, zugänglich macht,

3. im Einzelhandel außerhalb von Geschäftsräumen, in Kiosken oder anderen Verkaufsstellen, die der Kunde nicht zu betreten pflegt, im Versandhandel oder in gewerblichen Leihbüchereien oder Lesezirkeln einem anderen anbietet oder überläßt,

3a. im Wege gewerblicher Vermietung oder vergleichbarer gewerblicher Gewährung des Gebrauchs, ausgenommen in Ladengeschäften, die Personen unter achtzehn Jahren nicht zugänglich sind und von ihnen nicht eingesehen werden können, einem anderen anbietet oder überläßt,

4. im Wege des Versandhandels einzuführen unternimmt,

5. öffentlich an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, oder durch Verbreiten von Schriften außerhalb des Geschäftsverkehrs mit dem einschlägigen Handel anbietet oder bewirbt,

6. an einen anderen gelangen läßt, ohne von diesem hierzu aufgefordert zu sein,

7. in einer öffentlichen Filmvorführung gegen ein Entgelt zeigt, das ganz oder überwiegend für diese Vorführung verlangt wird,
8. herstellt, bezieht, liefert, vorrätig hält oder einzuführen unternimmt, um diesen im Sinne der Nummern 1 bis 7 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, oder
9. auszuführen unternimmt, um diesen im Ausland unter Verstoß gegen die dort geltenden Strafvorschriften zu verbreiten oder der Öffentlichkeit zugänglich zu machen oder eine solche Verwendung zu ermöglichen,
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."

Németországban az egyes pornográf műfajok között nemcsak a gyermekpornográfia fenyegetett büntetőjogi szankcióval, hanem a túlzottan erőszakos, bestialitást bemutató pornográfia, valamint az állatokkal való közösülést bemutató tartalmak is szankcionálandók:

„§ 184a Verbreitung gewalt- oder tierpornographischer Inhalte
Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer einen pornographischen Inhalt (§ 11 Absatz 3), der Gewalttätigkeiten oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand hat,
1. verbreitet oder der Öffentlichkeit zugänglich macht oder
2. herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen.
In den Fällen des Satzes 1 Nummer 1 ist der Versuch strafbar."

A kiskorúakat ábrázoló pornográf tartalmakat két kategóriára bontja a német büntető törvénykönyv. A gyermekpornográfiát *(kinderpornographischer Inhalte)* tiltó 184b szakasz rendeli büntetni a 14 év alatti gyermekeket ábrázoló szexuális tartalmak terjesztését, megszerzését, kínálását, készítését, illetve tartását:

„(1) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren wird bestraft, wer
1. einen kinderpornographischen Inhalt verbreitet oder der Öffentlichkeit zugänglich macht; kinderpornographisch ist ein pornographischer Inhalt (§ 11 Absatz 3), wenn er zum Gegenstand hat:
a) sexuelle Handlungen von, an oder vor einer Person unter vierzehn Jahren (Kind),
b) die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in aufreizend geschlechtsbetonter Körperhaltung oder

c) die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Kindes,
2. es unternimmt, einer anderen Person einen kinderpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zugänglich zu machen oder den Besitz daran zu verschaffen,
3. einen kinderpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, herstellt oder
4. einen kinderpornographischen Inhalt herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 oder der Nummer 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist."

A 184c szakasz vonatkozik az úgynevezett ifjúsági pornográfiára *(jugendpornographischer Inhalte),* amelynek a sértettje a 14. életévét már betöltött, de a 18. életévét még el nem ért kiskorú:

„(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer
1. einen jugendpornographischen Inhalt verbreitet oder der Öffentlichkeit zugänglich macht;
2. es unternimmt, einer anderen Person einen jugendpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zugänglich zu machen oder den Besitz daran zu verschaffen,
3. einen jugendpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, herstellt oder
4. einen jugendpornographischen Inhalt herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 oder 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist."

Az ilyen kiskorút ábrázoló felvételekkel kapcsolatos magatartások enyhébben szankcionálandók, figyelemmel arra, hogy a tinédzserek már rendelkeznek bizonyos fokú szexuális autonómiával, és gyakran önszántukból osztanak meg erotikus felvételeket, a pornográf tartalmak fogyasztóitól pedig nem feltétlenül várható el, hogy maguk becsüljék meg egy-egy felvétel szereplőjének az életkorát. Noha a cselekmény korántsem helyeslendő, nem indokolt a törvény teljes szigorával lesújtani az ilyen felvételeket tartókra, a társadalmi rosszallást ez esetben egy kisebb mértékű szankció is kifejezi.

Tartalommoderálás az online platformokon: a NetzDG

Németország igazán a NetzDG rövidítéssel illetett törvénnyel – amelynek teljes megnevezése *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*[248] – írta be magát az online tartalomszabályozás megkerülhetetlen szereplői közé. A törvény megalkotásához alapvetően a Németország és a közösségimédia-óriások, különösen a Facebook közösségi oldal közötti tartalommoderálási feszültség vezetett. Németország ugyanis sokáig nem értett egyet a Facebook és a Google gyűlöletbeszéd visszaszorítása érdekében tett intézkedéseivel, kritizálva azok hatékonyságát a német gyermekvédelmi hatóság, a Jugendschutz statisztikai adataira hivatkozva, amelyek azt mutatták, hogy az egyes szolgáltatók igen csekély hatékonysággal szűrik ki a gyűlöletbeszédet. A 2017-ben elfogadott törvény azokra a profitorientált közösségimédia-platformokra vonatkozik, amelyek Németországban legalább kétmillió felhasználóval rendelkeznek.

> „§ 1 Anwendungsbereich, Begriffsbestimmungen (1) Dieses Gesetz gilt für Telemediendiensteanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die dazu bestimmt sind, dass Nutzer beliebige Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen (soziale Netzwerke). Plattformen mit journalistisch-redaktionell gestalteten Angeboten, die vom Diensteanbieter selbst verantwortet werden, gelten nicht als soziale Netzwerke im Sinne dieses Gesetzes. Das Gleiche gilt für Plattformen, die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind.
> (2) Der Anbieter eines sozialen Netzwerks ist von den Pflichten nach den §§ 2 bis 3b und 5a befreit, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat."

A legproblémásabb tartalmaknak helyet adó, de rétegszolgáltatásnak minősülő közösségi platformokra tehát nem terjed ki a NetzDG hatálya. Szintén nem terjed ki a törvény hatálya a médiaszolgáltatásokra (mint a streaming), valamint a végpontok közötti kommunikációra építő azonnali üzenetküldő szolgáltatásokra. A NetzDG egyik legfontosabb újítása – ami egyébként az uniós jogalkotókat is inspirálta a DSA megszövegezésekor – az, hogy a közösségimédia-szolgáltatókat arra kötelezi, hogy a bűncselekménynek minősülő tartalmakat rövid határidővel távolítsák el. A nyilvánvalóan jogellenes tartalmak esetén 24 óra alatt kell intézkednie a szolgáltatónak, egyéb esetekben pedig legfeljebb 7 nap áll a rendelkezésére.

[248] Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352).

„(2) Das Verfahren muss gewährleisten, dass der Anbieter des sozialen Netzwerks […]
2. einen offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt; dies gilt nicht, wenn das soziale Netzwerk mit der zuständigen Strafverfolgungsbehörde einen längeren Zeitraum für die Löschung oder Sperrung des offensichtlich rechtswidrigen Inhalts vereinbart hat,
3. jeden rechtswidrigen Inhalt unverzüglich, in der Regel innerhalb von sieben Tagen nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt."

A jogellenes tartalmak *(rechtswidrigen Inhalt)* körét a NetzDG az Stgb. egyes szakaszaira utalással határozza meg, a jogellenesség tehát tulajdonképpen büntetőjogi szankcióval fenyegetettséget jelent. A német törvény alapvetően arra hivatott, hogy a Németország területén szolgáltatást nyújtó platformokat rászorítsa a nemzeti szabályok alkalmazására, és szigorú bírságokat (ötvenmillió euró) helyez kilátásba arra az esetre, ha a platformok elmulasztanak eleget tenni moderálási kötelezettségüknek. A szolgáltatókat ezenfelül kötelezettség terheli, hogy külön átláthatósági jelentéseket fogadjanak el a NetzDG alkalmazásáról, továbbá olyan kapcsolattartó pontokat kell felállítaniuk, ahol a német bűnüldöző szervek és a platform közötti gyors információcsere megvalósulhat.

Informatikai bűncselekmények az Egyesült Államokban

Az Egyesült Államok, mint az internet és az informatikai bűncselekmények őshazája, az elsők között ismerte fel azt, hogy az információtechnológiai eszközök fejlődése és a széles rétegek számára való elérhetősége a számtalan lehetőség mellett veszélyforrásokat is rejt magában. A kötet tárgya szempontjából az Egyesült Államok szabályrendszerének azért is nagy jelentősége van, mert a legtöbb vizsgált online platform a Szilícium-völgyből érkezett Európába. Működésüket, felhasználási feltételeiket és moderálási elveiket gyakran az amerikai jogi tradíció hatja át, cselekedeteik mozgatórugói pedig az európai jogi gondolkodáson „szocializált" jogalkalmazónak idegenek lehetnek. Amikor például a platformok tartalommoderálása és a szólásszabadság biztosítása közötti feszültségről beszélünk, figyelemmel kell lennünk arra, hogy ez az alapjog az Egyesült Államokban jóval hangsúlyosabb szerepet tölt be, mint a kontinentális jogrendszerekben, ahol szabadabban korlátozható.

Az informatikai elemet tartalmazó bűncselekmények csoportosítása

Az amerikai jogban megjelenő informatikai elemet tartalmazó bűncselekményeket többféleképpen lehet csoportosítani. Az egyik ilyen csoportosítás a számítógép bűncselekményben játszott egyes szerepeit veszi alapul. Eoghan Casey[249] a számítógép lehetséges szerepeinek vizsgálatakor egy Donn Parker által összeállított csoportosításra hivatkozik, amely szerint:

- *A számítógép fizikai valójában az elkövetés tárgya:* ez a helyzet azoknak a bűncselekményeknek az esetében, amikor a számítógép fizikai komponensére követik el a bűncselekményt, például ellopják vagy megrongálják azt. Az informatikai elem ezekben a bűncselekményekben valójában csak esetleges, így ezek a deliktumok nem számítanak számítógépes bűncselekményeknek.
- *A számítógépes környezet az elkövetés tárgya:* a számítógépes környezet az elkövetés tárgya azokban az esetekben, amikor az adott bűncselekményt számítógépes rendszerre, programra vagy számítógépben tárolt adatra követik el. Ezek a bűncselekmények a klasszikus számítógépes bűncselekmények, például a hackelés, a számítógép megfertőzése kártékony programokkal *(malware)* stb.
- *A számítógépes környezet a bűncselekmény eszköze:* a számítógépes környezet a bűncselekmény eszköze, amikor az elkövető olyan bűncselekményt követ el információtechnológiai környezetben, amely egyébként számítógép felhasználása nélkül is elkövethető lett volna. Ebbe a körbe tartoznak a tartalommal kapcsolatos bűncselekmények, mint a gyermekpornográfia, illetve a szerzői jog megsértésével kapcsolatos bűncselekmények.
- *A számítógép lehet az elkövetés szimbóluma:* ez utóbbi esetben a számítógépnek nem kell feltétlenül jelen lennie a bűncselekmény elkövetése során, az elkövető csupán arra hivatkozik. A szerző egy olyan csalást hoz fel példaként, amelyben az elkövető a megtévesztés során arra hivatkozott, hogy hozzáférése van bizonyos speciális számítógépes programhoz.

A számítógép bűncselekményben játszott szerepei azonban nem, illetve csak részben szolgálhatnak alapot az informatikai bűncselekmények tényleges csoportosításához. Ha a számítógépek bűncselekményekben játszott szerepeit vennénk alapul az informatikai bűncselekmények csoportosításakor, akkor könnyen azt találnánk, hogy a világ összes bűncselekménye informatikai bűncselekménynek minősül. E tekintetben fontosnak

[249] Casey 2012: 40.

tartom hangsúlyozni, hogy meg kell egymástól különböztetni az információtechnikai elemet tartalmazó bűncselekményeket a szűkebb értelemben vett informatikai bűncselekményektől. Az előbbi csoportosítás utolsó eleme, amely szerint a számítógép az elkövetés szimbóluma, nem olyan ismérv, amely alapján egy bűncselekményt informatikai bűncselekménynek lehetne minősíteni (noha kétségtelen, hogy megjelenik információtechnikai elem). A számítógépre, illetve a számítógépes programra való hivatkozás itt csupán igen távoli jelleggel vonható összefüggésbe a tényleges információtechnológiai környezettel.

Marjie T. Britz[250] egy történeti jellegű csoportosítást használ, s ez alapján két kategóriába sorolja az informatikai elemet tartalmazó bűncselekményeket.

- *Tradicionális számítógépes bűncselekmények:* A tradicionális számítógépes bűncselekmények azok, amelyek a fejlettebb infokommunikációs eszközök szélesebb rétegek számára való elérhetővé válásával egy időben jelentek meg. Tradicionális számítógépes bűncselekménynek számít a hackelés, a *phreaking,* az alkatrészlopások, valamint a szellemi tulajdon megsértésével kapcsolatos korai bűncselekmények.
- *Kortárs számítógépes bűncselekmények:* A kortárs számítógépes bűncselekmények megjelenését Britz az internet széles körben való elterjedésének tulajdonítja. A kortárs számítógépes bűncselekmények között hat alkategóriát különböztet meg, ezek:
  - beavatkozás a számítógép jogszerű működésébe: DDOS-támadások, kártékony programok (vírusok, férgek) használata, kiberterrorizmus;
  - információlopás és szerzői jogsértés: ipari kémkedés, személyazonosság-lopás, személyazonosság-csalás;
  - tiltott anyagok terjesztése: gyermekpornográfia, tiltott szerencsejáték, rasszista tartalmak;
  - fenyegető kommunikáció: zsarolás, zaklatás, *cyberbullying;*
  - csalás: aukciós csalás, hitelkártyacsalás stb.;
  - kiegészítő bűncselekmények: pénzmosás.

Britz felosztásával az a legfőbb probléma, hogy a technológia rendkívül gyors ütemű fejlődése miatt a határvonal a tradicionális és a kortárs informatikai bűncselekmények között egyre elmosódottabbá válik. A felosztás már a hackelés esetében is kérdéses, hiszen igaz, hogy a jelenség már az 1960-as években jelen volt az Egyesült Államokban,

[250] Britz 2013: 51.

a személyi számítógépek és mobil eszközök rohamos elterjedésével reneszánszát éli a cselekmény. Megjegyzendő továbbá, hogy a csoportosításnál olyan szempontokra lenne szükség, amelyek időtállók, és amennyiben lehetséges, technológiasemlegesek.

Susan W. Brenner szerint[251] az informatikai bűncselekmények három csoportba sorolhatók.

1. Az első csoportba azok a bűncselekmények tartoznak, amelyekben az információs rendszer az elkövetés tárgya (célpontja). Idetartozik a hackelés, a *malware*-ek, azaz a kártékony programok terjesztése és a DDOS- (vagyis a túlterheléses) támadás.
2. A második csoportba azok a bűncselekmények tartoznak, amelyekben a számítógép az elkövetés eszköze. Ebbe a kategóriába tartozik a számítógépes csalás, a zaklatás, a hamisítás, a terrorizmus, a tiltott szerencsejáték, a rágalmazás, a gyűlöletkeltés és a gyermekpornográfia.
3. A harmadik csoportba tartoznak azok a bűncselekmények, amelyekben a számítógép csak esetlegesen van jelen, vagyis nem a bűncselekmény tárgya, és nem is annak eszköze, azonban megkönnyíti az elkövetést, vagy értékes bizonyítékok találhatók rajta. A szerző Melanie McGuire esetét hozza példának, amelyben az elkövető egy internetes keresőszolgáltatást használt arra, hogy ismereteket szerezzen arról, „hogyan kell elkövetni egy gyilkosságot", és „hogyan lehet illegálisan lőfegyvert vásárolni".[252]

Mivel az utóbbi csoportosítás mutatja a legnagyobb mértékű hasonlóságot az európai – a kiberbűnözésről szóló egyezmény által felállított – rendszerrel, a továbbiakban e csoportosítás mentén mutatjuk be az Egyesült Államokban szabályozott informatikai bűncselekményeket.

Mivel az Egyesült Államokban szövetségi rendszer működik, az informatikai bűncselekmények szabályozása is kétszintű: a szövetségi informatikai büntetőjog egy egységes, mindent magába foglaló rendszer, a területi hatálya az Amerikai Egyesült Államok teljes területére kiterjed. Az állami informatikai büntetőjog azonban mindenhol eltérő, mind az 50 szövetségi állam (valamint a kolumbiai körzet) informatikai büntetőjoga csak az adott állam területén érvényes. Egyrészt terjedelmi okokból, másrészt azért, mert az egyes államok rendszerei között sokszor nagy az átfedés, kötetem kizárólag a szövetségi szintet tárgyalja.

[251] Brenner 2013: 39.
[252] Brenner 2013: 46.

Bűncselekmények, amelyekben az információs rendszer az elkövetés tárgya

A számítógép kétféle minőségében is lehet az elkövetés tárgya: egyrészt, mint a fizikai térben létező tárgy, másrészt, mint a virtuális térben létező program. Amennyiben a hardver, azaz a számítógép fizikai térben megjelenő komponense az elkövetés tárgya, nem beszélhetünk valódi informatikai bűncselekményről, hiszen az, hogy a cselekményt egy számítógép „ellen" követték el, még nem olyan különös tulajdonság, ami indokolná az adott deliktumra vonatkozó általános szabályoktól való megkülönböztetést. A rongálás például hazánkban sem minősül másképp akkor, ha az elkövetési tárgy egy számítógép, mint akkor, ha egy mosógép, az információtechnológiai jelleg kiemelése ilyen szempontból nem logikus, és nem is indokolt.

Informatikai bűncselekményről beszélhetünk ellenben azokban az esetekben, amelyekben az információs rendszer programkörnyezete az elkövetési tárgy, hiszen ezekben az esetekben megkülönböztető elem, hogy a cselekmény a virtuális térben valósul meg, és elkövetéséhez speciális szaktudás és eszközkészlet szükséges. Az információs rendszer az elkövetés tárgya az úgynevezett „hackelés" (információs rendszer megsértése), a *malware*-ek (kártékony programok) terjesztése, illetve a DDOS- (túlterheléses) támadások esetén.

Az informatikai bűncselekményeket szövetségi szinten több jogszabály is kezeli. Az első és a mai napig legjelentősebb a számítógépes csalásról és visszaélésről szóló törvény (Computer Fraud and Abuse Act – CFA, 1986), amelyet 1986-ban fogadott el a Kongresszus, és amely az Egyesült Államok Törvénykönyvének (United States Code – a továbbiakban: U.S. Code) 18. címe alatt jelenik meg. Az amerikai szövetségi jog e törvénnyel rendeli büntetni a jogosulatlan hozzáférést, a kártékony programok *(malware)* terjesztését, az elosztott túlterheléses támadások (DDOS) indítását, a jelszavak jogellenes kereskedelmét, valamint a számítógép felhasználását csalásra és zsarolásra. A törvény hatálya kizárólag a védett számítógépekre terjed ki, ennyiben tehát speciális a törvény által büntetni rendelt cselekmények elkövetési tárgya.[253] A védett számítógép *(protected computer)* olyan számítógépet jelent, amelyet:

- kizárólag pénzintézet vagy a szövetségi kormányzat használ;
- nem kizárólag ezek a szervezetek használnak, azonban a büntetni rendelt cselekmények az általuk történő használatot érintik;
- államközi vagy külföldi kereskedelemre vagy kommunikációra használnak.[254]

[253] 18 U.S. Code 1030(a).
[254] 18 U.S. Code 1030(e)(2).

A szövetségi jogszabály hatálya tehát az egyes államok határain belül maradó cselekményekre, illetve a magánszemélyek által használt számítógépek megsértésére nem terjed ki. Ezeket a cselekményeket azonban az állami jogrendszerek rendelik büntetni, a hackelés például az Egyesült Államok összes tagállamában büntetendő.[255]

Brenner felhívja a figyelmet arra is, hogy a CFA nemcsak büntetőjogi normákat tartalmazó törvény, hanem megteremti a polgári jogi igényérvényesítés lehetőségét is azáltal, hogy az a személy, akinek kára keletkezik, igényével felléphet az elkövetővel szemben.[256] A törvényt megalkotása óta több alkalommal módosították, az egyik legátfogóbb módosítása a 2008-as, amikor a személyazonosság-lopásról szóló törvény (Identity Theft and Restitution Act, 2008) több rendelkezését módosította.

Hackelés

Hackelésen, azaz a számítógépes rendszer megsértésén az amerikai szövetségi jog azt érti, ha valaki jogosulatlanul belép egy számítógépes rendszerbe (külsős hackelés – *outsider hacking*), illetve a jogosultsága kereteit meghaladva fér hozzá a rendszer egyes részeihez (belsős hackelés – *insider hacking*). Ez utóbbi eset típuspéldája a vállalat alkalmazottja, aki a rendszer azon részeihez, illetve a rendszerben tárolt olyan adatokhoz fér hozzá, amelyekre egyébként nem lenne jogosult. A szövetségi büntetőjog az egyszerű további motiváció nélküli belépést, illetve bent maradást, vagyis az úgynevezett „egyszerű hackelést" *(simple hacking)* nem, illetve csak bizonyos feltételek fennállása esetén kriminalizálja. Az Egyesült Államok tagállamai állami szinten rendelik büntetni az egyszerű hackelést. Susan W. Brenner kiemeli, hogy az egyszerű hackereket nem az motiválja, hogy adatlopást, szabotázst vagy bármilyen más hagyományos bűncselekményt kövessenek el,[257] amennyiben azonban adatokat másolnak vagy semmisítenek meg, rendszerint a cselekmény minősített esetét *(aggravated hacking)* hajtják végre.

A számítógéphez való jogosulatlan hozzáférésnek a következő eseteit rendeli büntetni az amerikai szövetségi jog:

a) Amikor valaki tudatosan, jogosultság nélkül vagy annak kereteit megsértve fér hozzá a számítógéphez, és abból olyan információ(ka)t szerez, amely vagy amelyek nyilvánosságra hozatalát jogszabály tiltja és amelyekről az elkövető

[255] Brenner 2001: 28–32.
[256] Brenner 2010: 88.
[257] Brenner 2010: 51.

úgy tudja, hogy az Egyesült Államok hátrányára vagy idegen ország előnyére használhatók, amennyiben ezeket szándékosan megtartja vagy jogosulatlan személynek átadja.[258]

b) Amikor valaki szándékosan, jogosultság nélkül vagy annak kereteit megsértve fér hozzá a számítógéphez, és olyan információt szerez, amely pénzintézettől, hitelkártya-vállalattól, fogyasztói ügynökségtől, szövetségi minisztériumtól vagy ügynökségtől, védett számítógépről származik.[259]

c) Amikor valaki szándékosan és jogosultság nélkül fér hozzá az Egyesült Államok szövetségi minisztériuma vagy ügynöksége által kizárólagosan használt számítógéphez, illetve olyan számítógéphez, amelyet nem kizárólagosan ezek a szervezetek használnak, de a tevékenység befolyásolja a számítógépnek az Egyesült Államok kormánya általi, illetve annak érdekében történő alkalmazását.[260]

d) Amikor valaki csalási szándékkal, jogosultság nélkül vagy annak kereteit megsértve fér hozzá számítógéphez, amennyiben a csalást megvalósítja, és bármilyen értékkel bíró vagyont szerez, kivéve, ha a szerzett vagyon csupán a számítógép használatát jelenti, és a használat értéke nem haladja meg az ötezer amerikai dollárt.[261] Ebben a cselekményben a számítógéphez való hozzáférés csupán szükséges előfeltétele a csalás megvalósításának, ezért a deliktumot részletesen a számítógépes csalás körében tárgyaljuk.

e) Büntetendő a hackelés abban az esetben is, ha a jogosulatlan hozzáférés program, információ, kód vagy parancs küldésével történik, amennyiben hozzáférésével az elkövető akár gondatlanul, akár szándékosan kárt okoz.[262] Mivel ezeknek a cselekményeknek a kártékony programkódok terjesztése az eszközcselekménye, részletesen később a *malware*-terjesztésnél tárgyaljuk őket.

Az egyszerű hackelést a fentiek alapján mindössze egy esetben rendeli büntetni szövetségi törvény, a c) pontban meghatározott esetben, amelyben az elkövető a védett számítógépek egyik meghatározott fajtájába, a kormányzati számítógépekbe lép be jogosulatlanul. Kormányzati számítógépek azok a számítógépek, amelyeket kizárólag az Egyesült Államok kormánya használ, illetve amelyeket az Egyesült Államok kormányának érdekében használnak, továbbá azok a számítógépek, amelyek nem állnak

258 18 U.S. Code 1030(a)(1).
259 18 U.S. Code 1030(a)(2).
260 18 U.S. Code 1030(a)(3).
261 18 U.S. Code 1030(a)(4).
262 18 U.S. Code 1030(a)(5).

ugyan az Egyesült Államok kormányának kizárólagos használatában, de a használatuk befolyásolja a kormányzat általi, illetve az annak érdekében végzett használatot. E cselekmény két kulcselemét indokolt bővebben is megvizsgálnunk. A hackelés ez esetben csak a már korábban tárgyalt „külsős hackelés" esetében minősül büntetendőnek, vagyis abban az esetben, amikor az elkövető nem rendelkezik jogosultságokkal a rendszer tekintetében. A fenti cselekmények tehát a „belsős" elkövető, vagyis a kormányzati alkalmazottak tekintetében nem minősülnek tényállásszerűnek. Az Egyesült Államok Szenátusának Igazságszolgáltatási Bizottsága[263] több alkalommal is értelmezte, hogy miért indokolt ezen tényállások tekintetében a külsős és a belsős hackelés megkülönböztetése. Ebben az esetben a jogalkotó szándékosan nem kriminalizálja azt, amikor egy alkalmazott csupán túllépi a jogosultsága kereteit a saját szervezetén belül.

> „Nem nehéz elképzelni egy olyan alkalmazottat, aki rendelkezik ugyan jogosultsággal egy minisztériumi számítógép tekintetében, azonban elolvas a minisztérium által kezelt olyan adatokat, amelyeket neki nem lenne szabad. Ez különösen igaz ott, ahol a kérdéses szervezetnek nincs egyértelmű módszere arra, hogy elhatárolja, mely személyek milyen adatokhoz jogosultak hozzáférni. A Bizottság ezért úgy hiszi, hogy a közigazgatási szankciók sokkal megfelelőbbek, mint a büntetőjogi szankció."[264]

Az e pontban felsorolt tényállások kulcseleme a szándékosság, vagyis az elkövetőnek tudatában kell lennie annak, hogy jogszerűtlenül fér hozzá egy információs rendszerhez. Brenner szerint a hackelés egyébként is olyan tevékenység, amely magas szintű hozzáértést igényel, így nem követhető el „véletlenül".[265]

Számítógépes kémkedés (computer espionage)

A fenti a) pontban nevesített eset valójában a számítógépes kémkedés *(computer espionage)* tényállása. A bűncselekmény jogi tárgya kettős, hiszen szerepet játszik egyrészt a honvédelemmel, a külkapcsolatokkal, valamint az atomenergiával kapcsolatos titkosnak minősülő adatok integritásához és titokban maradásához fűződő érdek, másrészt az Egyesült Államok állambiztonságához fűződő érdek. Az elkövetési tárgy szintén kettős jellegű, hiszen egyrészt maga a számítógép, másrészt a számítógépben tárolt honvédelmi vagy külkapcsolati okok miatt védettnek minősített információ,

[263] S.Rept. 99-432 7-8 (1986) és H.Rept. 99-612 11 (1986).
[264] Doyle 2014: 4.
[265] Brenner 2010: 3.

és az atomenergia-törvény által bizalmasnak minősített adat is elkövetési tárgyak. Az elkövetési tárgy kapcsán fel kell hívnunk arra a figyelmet, hogy a cselekmény csak akkor valósul meg, ha a számítógép valóban tartalmazza a fenti tényállásban meghatározott információkat, és az elkövető meg is szerzi ezeket. Az elkövetési magatartások több fordulattal is megvalósíthatók: a megszerzett információk közlésével, továbbításával, átadásával, ezeknek a kísérletével, illetve azáltal, ha az elkövető a megszerzett információkat visszatartja. Hasonló esetet szabályoz a fenti b) pont azzal a különbséggel, hogy abban csak a jogosulatlan információszerzés történik meg, az információ átadása, továbbítása nem.

Kártékony programok és kódok terjesztése

A *malware (malicious software)* az összefoglaló neve a rosszindulatú számítógépes programoknak. A rosszindulatú szoftverek közé tartoznak a trójai programok, vírusok, férgek, kémprogramok *(spyware),* illetve az agresszív reklámok *(adware).* A rosszindulatú számítógépes programok fajtái állandó változásban vannak, hiszen folyamatosan újabb és újabb típusok jelennek meg a piacon. Az Egyesült Államok büntetőjoga az európai, köztük a magyar gyakorlattól eltérően a kártékony programok készítését nem kriminalizálja, kizárólag azokat a magatartásokat rendeli büntetni, amelyek az ilyen programok felhasználásával hozhatók kapcsolatba. A CFA kártékony programokról szóló szakasza háromféle elkövetési magatartást rendel büntetni. Az első eset azt a magatartást rendeli büntetni, amikor valaki tudatosan olyan programot, információs kódot vagy parancsot továbbít, amellyel szándékosan kárt okoz a számítógépben.[266] Ez a szakasz vonatkozik a kártékony programok terjesztésére, ideértve a különféle számítógépes vírusokat, valamint az úgynevezett elosztott szolgáltatásmegtagadással járó támadásokat (*distributed denial of service attack* – DDOS), amelyek annyiban különlegesek a többi *malware*-terjesztést megvalósító cselekményhez képest, hogy ebben az esetben a fertőzött számítógép és a megtámadott számítógép különböznek.

Az e szakaszban szabályozott második eset a kártékony program felhasználásával elkövetett jogosulatlan hozzáférést rendeli büntetni, amelyben a belépésnek a szükségszerű előfeltétele a program vagy kód használata. A második eset tényállásszerűségének további feltétele a meghatározott eredmény bekövetkezése, vagyis az, hogy az elkövető hanyagságból, méghozzá eshetőleges szándékkal *(recklessly)* kárt

266 18 U.S. Code 1030 (a)(5) (A).

okozzon.[267] A harmadik eset alá pedig azok a cselekmények tartoznak, amelyeknél az elkövető a hackeléssel gondatlan módon *(negligently)* okoz kárt. Köznyelvi értelemben ez a szakasz azokra a magatartásokra vonatkozik, amelyeknél a jogosulatlan belépést a számítógép feltörése előzi meg.

Számítógépes csalás

A számítógépes csalás tényállása azt az esetet rendeli büntetni, amelyben az elkövető célzatos magatartásával – a cél a csalás elkövetése – lép be jogosulatlanul egy információs rendszerbe. A cselekmény az amerikai jogban eredmény-bűncselekménynek számít, hiszen a célzatos belépés csak akkor büntetendő, ha az elkövető bármilyen értékkel gazdagodik *(obtains anything of value).* Sem a törvény, sem az azt tárgyaló szakirodalom nem határozza meg, hogy mit ért az amerikai jog „érték" alatt, ebből arra következtethetünk, hogy az bármi – ingó, ingatlan dolog, vagyoni értékű jog, egyéb – lehet, amennyiben pénzbeli értéke kifejezhető. A büntethetőségnek e cselekmény esetében speciális küszöbe van, hiszen, amennyiben az elkövető csupán a számítógép használatának lehetőségével gazdagodik, amelynek a pénzben kifejezhető értéke nem éri el az 5 ezer dollárt, nem büntethető. Kizárja tehát a bűnösséget a törvény azokban az esetekben, amikor az elkövető csupán kis értékű gépidőt szerez. A United States v. Czubinski ügyben[268] a bíróság kimondta, hogy ebben az esetben többről van szó, mint egyszerű jogosulatlan hozzáférésről, vagyis a szerzett érték nem lehet pusztán a hozzáférés ténye. A kíváncsiság kielégítése, illetve a barátokról, ismerősökről, politikai ellenfelekről szóló információkhoz való hozzáférés, amennyiben az elkövetőnek nem célja azokat felhasználni vagy nyilvánosságra hozni, nem tekinthető gazdagodásnak. A szakasz érdekessége, hogy az elkövetéshez egyrészt szükséges a csalási célzat már a cselekmény megkezdésekor, másrészt az, hogy az elkövető a hozzáférése során végre is hajtsa a tervezett csalást. „Az »ezáltal végrehajtja a tervezett csalást« fordulat azért került a jogszabály szövegébe, hogy kizárja azokat az eseteket, amelyekben a számítógépet csupán nyilvántartási céllal használja az elkövető."[269]

A számítógépes csalás egyik speciális esete az Egyesült Államokban a jelszókereskedelem *(password trafficking).* Aki tudatosan és csalási szándékkal jelszavakkal vagy más hozzáférést biztosító eszközökkel kereskedik, bűncselekményt követ el, amennyiben

[267] 18 U.S. Code 1030 (a)(5) (A) bekezdés.
[268] United States v. Czubinski (1997) U.S. Court of Appeals for the First Circuit (106.F.3d 711).
[269] Doyle 2014: 52.

a cselekmény érinti az államközi vagy a nemzetközi kereskedelmet, vagy a számítógép, amelyhez hozzáférést biztosítanak, a szövetségi kormányzat által vagy annak érdekében használt.[270] Ez a tényállás a jelszavak és egyéb azonosítók ellopásának és nyilvánosságra hozatalának tömeges elterjedése miatt került be külön a szövetségi büntetőjogba, nem egy példa van ugyanis arra, hogy a felhasználóktól ellopott adatok tömegesen jelennek meg az interneten. Fel kell hívni a figyelmet azonban arra, hogy a szövetségi szabályok szerint az illegális jelszó-kereskedelem csak akkor tényállásszerű, ha ez a tevékenység hatással van a tagállamok közötti, illetve a külkereskedelemre, vagy ha az ellopott és kínált azonosító olyan számítógéphez tartozik, amelyet kormányzat használ, vagy a kormányzati működéssel kapcsolatos használatban van.

Bűncselekmények, amelyekben az információs rendszer az elkövetés eszköze

Rendkívül színes képet mutatnak azok a cselekmények, amelyekben a számítógép csupán az elkövetés eszközeként van jelen. Ebben a kategóriában megjelennek egyrészt azok az információval való visszaélés jellegű bűncselekmények, amelyeknél a hackelés eszközcselekményként van jelen (számítógépes kémkedés, minősített információkkal való visszaélés, csalás, tiltott jelszó-kereskedelem, illetve a számítógépes zsarolás egyik formája), valamint azok az igen változatos deliktumok, amelyek a számítógép tömeges elterjedése előtt is büntetendők voltak, a számítógép csak az elkövetés módszerén változtatott. Ez utóbbi kategóriába tartoznak az olyan nem tisztán informatikai jellegű bűncselekmények, mint a személyazonossággal való visszaélés, az internetes zaklatás és zsarolás, a gyermekpornográfia, a szerzői jogsértések. A tartalom-bűncselekmények egyes fajtáit külön szövetségi törvények szabályozzák.

Számítógépes zsarolás

A számítógépes csalásról és visszaélésről szóló törvény rendelkezik a zsarolás *(extortion)* szövetségi szintű kriminalizálásáról is. A meghatározott tényállás szerint bűntettet követ el az, aki pénz vagy az államközi, illetve nemzetközi kereskedelemben értékkel bíró dolog megszerzése céljából egy számítógép megrongálásával fenyeget, jogosulatlan

[270] 18 U.S. Code 1030(a)(6).

vagy a jogosultság kereteit meghaladó hozzáféréssel, információk megszerzésével vagy az információk bizalmasságának megsértésével fenyeget, illetve aki elősegíti az ilyen cselekmények végrehajtását.[271]

A jogszabály 1030 (a)(7) (B), valamint (C) pontjaiban nevesített tényállások 2008-ban az Igazságügyi Minisztérium ajánlását követően kerültek a törvénybe, annak érdekében, hogy az „azokat az eseteket is lefedje, amelyekben az elkövető már ellopta az információkat, és azzal fenyeget, hogy nyilvánosságra hozza őket".[272] Ezeknek az eseteknek jó példái a hazánkban is elterjedt úgynevezett zsarolóvírusok *(ransomware)*.

Zaklatás (stalking és harassment)

Az elektronikus hírközlő hálózatokon, pontosabban a telefonon keresztül történő zaklatást az USA szövetségi szinten szabályozta már 1934-ben. Az úgynevezett Telephone Harassment Statute világszinten is a legelső zaklatást szabályozó törvények között van. Noha az Egyesült Államok úttörő szerepet töltött be abban, hogy a zaklatásszerű háborgató magatartásokat szankcióval fenyegessék a fejlett jogrendszerek, a cselekmény szabályozásának további fejlődése már korántsem olyan példaértékű. Ambrus István és Ujvári Ákos megjegyzik, hogy az amerikai *stalking*- vagy *harassment*jogszabályok esetében az állami jogszabályok egymástól jelentősen eltérnek mind a tényállási elemek, mind a büntetési tételek tekintetében.[273] Egyes államokban például a zaklatás megvalósítható közvetett (családon, barátokon keresztül történő) kapcsolatteremtéssel is. Az egyes államok szabályozására részletesen nem térek ki, a kötet szempontjából annyi a releváns, hogy az amerikai gyakorlat nem ugyanazt érti zaklatáson, mint a kontinentális európai jogrendszerek, így például Magyarország. A közösségi média önmagát szabályozó közösségi iránymutatásai ezen amerikai látásmódot közvetítik, amikor tiltanak bizonyos zaklató jellegű felhasználói magatartásokat.

Az internet terjedése természetesen az amerikai kontinensen is jelentős hatással volt a zaklató jellegű magatartások morfológiájára. Az úgynevezett *cyberbullying*-jelenség körébe tartozó magatartások kriminalizálása szintén az USA-ban kezdődött, szövetségi szinten azonban nincs olyan törvény, amely pönalizálni rendelné az e körbe tartozó magatartásokat. A modern online közösségi térben betöltött jelentősége és újszerűsége

271 18 U.S. Code 1030(a)(7).
272 Doyle 2014: 64.
273 Ambrus–Ujvári 2016.

miatt jelen kötet külön fejezetet szentel a *cyberbullying* tárgyalásának, elöljáróban azonban annyit mindenképpen le kell már most szögeznünk, hogy a *cyberbullying* és a kibertérben megvalósított zaklatás (*cyberstalking* vagy *cyberharassment*) közé nem tehető egyenlőségjel. A *cyberbullying* mint jelenség részint magában foglalja ezen internetes zaklató magatartásokat, részint azonban olyan háborító magatartásokat is inkorporál, amelyek eltérnek a zaklatás klasszikus tartalmától. *Cyberbullying*ként minősíti az amerikai gyakorlat például az online kiközösítést *(outing),* amely a zaklató magatartás szöges ellentéte, hiszen nem kéretlen kapcsolatba lépés történik, hanem éppen egy vágyott kapcsolat megtagadása.

Személyazonosság-lopás (identity theft)

„Az amerikai szövetségi jog két személyazonosság-lopással kapcsolatos rendelkezést is tartalmaz: a U.S. Code 18. címének 1028(a)(7) szakasza határozza meg a személyazonosság-lopás alapesetét, a U.S. Code 18. címének 1028A szakasza pedig a minősített eseteit."[274] A személyazonosság-lopás alapesete szerint, aki egy másik személyhez kötődő azonosítót szándékosan és jogosultság nélkül átad, birtokol, használ, abból a célból, hogy szövetségi jogot, vagy állami, helyi jog szerinti bűncselekményt kövessen el, bűncselekményt követ el.[275] A rendelkezéssel kapcsolatban ki kell emelni, hogy az azonosítók jogtalan átadása, birtoklása és használata önmagában még nem minősül bűncselekménynek, két további feltétel együttes teljesülése is szükséges: az egyik feltétel, hogy az azonosítók jogtalan kezelése a (c) bekezdésben meghatározott esetekben (például akkor, amikor úgy tűnik, hogy azt az Egyesült Államok valamely hatósága állította ki) történjen, másrészt az, hogy a cselekmény a szövetségi vagy a tagállami büntetőjog szerint bűncselekménynek minősüljön. Az 1028A (a)(1) szakaszban található tényállások a személyazonosság-lopás minősített eseteit tartalmazzák. Az (1) bekezdés azokban az esetekben súlyosabban rendeli büntetni a személyazonosság-lopást, ha bizonyos bűncselekmények elkövetése során (többek között az állampolgársággal kapcsolatos, valamint lőfegyverek megszerzésével kapcsolatos esetekben), illetve azokkal összefüggésben történik, a (2) bekezdés pedig a terrorcselekmények vonatkozásában rendeli büntetni ugyanezt.

[274] Casey 2012: 94.
[275] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America).

Gyermekpornográfia

A Kongresszus a gyermekpornográfiát először 1977-ben a gyermekek szexuális kizsákmányolása elleni védelméről szóló törvényben (Protection of Children Against Sexual Exploitation Act, 1977) szabályozta, később a digitális technológiák egyre elterjedtebb használata, az internetes terjesztés és az úgynevezett virtuális gyermekpornográfia miatt szükséges volt a módosítása. 1996-ban fogadta el a Kongresszus a gyermekpornográfia elleni védelemről szóló törvényt (Child Pornography Prevention Act, 1996), amely az új technológiákra tekintettel szabályozza a jelenséget. 2003-ban fogadta el a Kongresszus azt a törvényt, amely az obszcén gyermekpornográfiát is büntetendővé nyilvánította (Prosecutional Remedies and Other Tools to End the Exploitation of Children Today Act – PROTECT, 2003).

A gyermekpornográfia az amerikai szövetségi törvény szerint[276] bármely olyan szexuálisan explicit tevékenységet bemutató vizuális ábrázolás, ideértve a fényképfelvételt, videót, képet, számítógépes vagy számítógéppel generált felvételt:

- amelynek az előállítása során kiskorú vett részt szexuálisan explicit tevékenységben;
- amely digitális, számítógépes vagy számítógéppel előállított felvétel, amely kiskorút vagy kiskorútól megkülönböztethetetlen személyt szexuális tevékenység közben ábrázol;
- amelyet úgy készítettek vagy módosítottak, hogy úgy tűnjön, hogy azonosítható kiskorú szexuális tevékenységben vesz részt.

A törvény tehát a gyermekpornográfia három fajtáját is ismeri, a valós helyzetben, valóban kiskorú személy részvételével készült felvételeket, a digitálisan előállított kiskorút ábrázoló felvételeket (ez az úgynevezett virtuális gyermekpornográfia), valamint a manipulált felvételeket, amelyeknek van ugyan valós alapja, a kiskorú szexuális tevékenységben való részvétele azonban módosítás eredménye.

A gyermekpornográf felvételekkel összefüggésben több magatartást is büntetni rendel az amerikai szövetségi törvény:

- Tilos a kiskorú biztatása, rábírása vagy szállítása azzal a szándékkal, hogy az olyan szexuálisan explicit tevékenységben vegyen részt, amelyről felvétel készül.
- Tilos a szülő vagy gondviselő által engedélyt adni arra, hogy a kiskorú szexuálisan explicit tevékenységben vegyen részt azzal a céllal, hogy arról felvétel készüljön.

276 18 U.S. Code 2256(8).

- Tilos szándékosan terjeszteni – például számítógéppel, e-mailben – az olyan felvételeket, amelyek gyermeket szexuális tevékenység közben ábrázolnak.
- Tilos szándékosan olyan felvételeket fogadni, amelyek gyermeket szexuális tevékenység közben ábrázolnak.
- Tilos a gyermekpornográfiát eladni vagy értékesítési céllal tartani.
- Tilos a gyermekpornográf felvételeket tartani vagy azokhoz megtekintés szándékával hozzáférni.

Az utóbbi elkövetési magatartás utolsó fordulata azokat a cselekményeket kívánja dekriminalizálni, amikor az elkövető nem szándékosan, hanem böngészés közben véletlenül találkozik gyermekpornográfiával (mert mondjuk véletlenül egy internetes hirdetésre kattint).

2003 óta büntetendő az obszcén gyermekpornográfia előállítása, fogadása, birtoklása és előállítása. Az obszcén gyermekpornográfia a szexuálisan explicit tevékenység ábrázolásán túl magában foglalja az olyan felvételeket is, amelyeken egy gyermek olyan tevékenységben vesz részt, amely erőszakos bestialitásnak, szadisztikus vagy mazochisztikus bántalmazásnak minősül, és nem rendelkezik irodalmi, művészeti, politikai vagy tudományos értékkel.[277]

Szerzői jogsértések

A szerzői jogsértések egy részét kriminalizálja a 2006-os szellemi alkotások elleni bűncselekmények üldözéséről szóló törvény (Prosecuting Intellectual Property Crimes, 2006).

A szerzői jogsértések nem mindegyike számít szövetségi szinten bűncselekménynek, a köznyelvben szoftverkalózkodásként nevezett jelenség azonban igen. Ahhoz, hogy egy mű szövetségi szinten védelemben részesüljön, eredetinek kell lennie, és megragadható kifejezési formában kell megjelennie. Az eredetiség ebben az értelemben nem feltétlenül jelent újdonságot, pusztán arra utal, hogy egyértelműen a szerzőtől származtatható legyen. A megragadható kifejezési forma Brenner szerint olyan formában való megjelenést jelent, amely kellően állandó vagy stabil ahhoz, hogy befogadhassák, reprodukálják vagy egyébként kommunikálják több alkalommal, mint egyetlen átmeneti periódus.[278]

277 18 U.S. Code 1466A.
278 Brenner 2010: 100.

Szövetségi szinten büntetendő, ha valaki szándékosan megsérti más szerzői jogát
- kereskedelmi előny vagy magánjellegű vagyoni gyarapodás elérése érdekében, vagy
- azáltal, hogy egy vagy több szerzői jogvédelem alá eső művet reprodukál vagy terjeszt, amennyiben azok kereskedelmi értéke az ezer dollárt meghaladja.[279]

A törvény külön tiltja az úgynevezett kiadás előtt megvalósuló kalózkodást *(pre-release piracy),* amely fő tényállási eleme, hogy az elkövető olyan szerzői művel kapcsolatban követi el a jogsértést számítógépen vagy számítógépes hálózaton történő hozzáférhetővé tétellel, amely a kereskedelmi forgalmazásra történő előkészítés alatt áll.

A bíróság a Capitol Record, Inc v. Thomas[280] ügyben vizsgálta a terjesztés *(distribution)*, illetve a számítógépes hálózaton történő hozzáférhetővé tétel *(making it available on a computer network)* közötti különbséget. A tárgyalt ügyben az alperest azért perelték, mert *peer-to-peer* alapú fájlmegosztón tett hozzáférhetővé zeneműveket. Az alperes azzal védekezett, hogy tevékenysége nem minősült terjesztésnek. A bíróság egyetértett az alperesi védekezéssel, amikor kimondta, hogy a terjesztés a szerzői jogvédelem alatt álló művek tényleges aktív továbbítását is magában foglalja, megvalósulásához nem elegendő, ha az elkövető csupán passzív módon hozzáférést biztosít azokhoz a saját számítógépén.

Gyűlöletbeszéd-szabályozás az Egyesült Államokban

Európában a gyűlöletbeszéd *(hate speech),* avagy a gyűlöletre uszítás az egyik legjelentősebb tartalom-bűncselekmény, amellyel még a Cybercrime Egyezmény kiegészítő jegyzőkönyve is foglalkozik. Az Egyesült Államok jogi gondolkodásában az első alkotmánykiegészítésben megjelenő véleménynyilvánítás az egyik legjelentősebb alapjog, amely csak kevés esetben korlátozható, így szigorú mércével kell vizsgálni a gyűlöletkeltésre alkalmas közléseket is. Az Egyesült Államok közvetlen és nyilvánvaló veszély doktrínája Európában sem ismeretlen, sőt az amerikai jog ezen vívmánya még a magyar Alkotmánybíróság gyakorlatában is felüti a fejét, ha a gyűlöletre uszító közlésekről esik szó. Az elv lényege az, hogy a közlések csak akkor korlátozhatók,

279 17 U.S. Code 506(a).

280 Capitol Records, Inc v. Thomas (2008) U.S. District Court for the District of Minnesota (2008 WL 4405282).

hogyha a tényleges, fizikai világban megvalósuló erőszakhoz vezethetnek, az erőszak távoli, absztrakt veszélye esetén azonban a véleménynyilvánításhoz való jog az erősebb.

A közvetlen és nyilvánvaló veszély *(clear and present danger)* fent említett doktrínája az Amerikai Egyesült Államokban már az I. világháború környékén megfogalmazódott. A Schenck v. United States[281] ügy alapját egy olyan ítélet képezte, amelyben a vádlottakat azért ítélték el, mert olyan szórólapokat terjesztettek, amelyekben arra ösztönözték az olvasókat, hogy tagadják meg a bevonulást a hadseregbe. A tevékenység az I. világháború idején a kémkedésről szóló törvény (Espionage Act, 1917) alapján bűncselekménynek minősült, a törvény büntetni rendelte azt, aki hamis tudósításokat és állításokat terjesztett azzal a szándékkal, hogy beavatkozzon a katonaság vagy a haditengerészet műveleteibe, azok sikerébe, vagy azzal a szándékkal, hogy az ellenség sikerét támogassa. Oliver Wendell Holmes bíró véleményében megállapította, hogy „minden esetben az a kérdés, hogy az adott szavakat olyan körülmények között használták-e és azok olyan természetűek-e, hogy megteremtik annak nyilvánvaló és közvetlen veszélyét, hogy tényleges kárt okoznak, amit a Kongresszusnak joga van megelőzni".[282]

A nyilvánvaló és közvetlen veszély elve később finomhangoláson esett át. Az Abrams v. United States ügyben[283] a Legfelsőbb Bíróság hatályában fenntartotta öt anarchista elítélését, amiért azok támadták az Egyesült Államok beavatkozását az oroszországi polgárháborúba. Holmes bíró az ügyben ellentétes véleményt fogalmazott meg, amelyben kifejtette, hogy a vitatott közléseket nem kell korlátozni, csak akkor, ha azok a kár bekövetkezésének közvetlen veszélyét teremtik meg, vagy erre mutató szándékkal tették közzé őket. Az uszítás korlátozásának jelenleg is alkalmazott mércéjét a Brandenburg v. Ohio[284] ügyben fektette le a Legfelsőbb Bíróság. Az ikonikus ítéletben a bíróság kimondta, hogy az első alkotmánykiegészítés védi az erőszak alkalmazásának, illetve a jogszabályok megsértésének támogatását, kivéve, ha az ilyen támogató magatartás szándéka közvetlen jogellenes cselekvésre való felbujtás, azonnali jogellenes cselekvésre uszít, vagy tényleges jogellenes cselekedeteket eredményez. Önmagában az erőszakalkalmazás szükségességének absztrakt tanítása nem ugyanaz, mint egy csoport felkészítése tényleges, erőszakos cselekedetek elkövetésére.

Az Egyesült Államokban nemcsak a közvetlen veszélyt jelentő, hanem a valós fenyegetések *(true threats)* esetében is elfogadott a véleménynyilvánítás szabadságának

281 Schenck v. United States, 249 U.S. 47 (1919).
282 Reményi–Koltay 2017: 447.
283 Abrams v. United States, 250 U.S. 616.
284 Brandenburg v. Ohio, 395 U.S. 444 (1969).

büntetőjogi eszközeivel való korlátozása. A valós fenyegetésekről szóló három legfontosabb elvi jellegű megállapítás a Watts v. United States[285] ügyben, a Virginia v. Black[286] ügyben, valamint az Elonis v. United States[287] ügyekben született.

A Watts-ügyben egy olyan közlésről kellett döntenie a bíróságnak, amelyben a vádlott egy vietnámi háborút ellenző kirohanásában azt mondta, hogy ha még egyszer géppuskát adnak a kezébe, az első ember, akivel szembe akar találkozni, Lyndon Baines Johnson.[288] A Bíróság azt állapította meg, hogy ez a nagy nyilvánosság előtt elhangzott politikai színezetű közlés nem minősül valós fenyegetésnek, hanem csak „politikai hiperbola", amely bár durván sértő volt, a közlő nem vonható érte felelősségre. Az ügyben a bíróság nem foglalkozott az elkövető tudattartalmával, vagyis azzal, hogy előre kellett volna-e látnia szavai hatását. A Virginia v. Black ügyben ellenben már foglalkoztak a szándék kérdésével. A Legfelsőbb Bíróság megállapította, hogy a fenyegetés akkor valós, ha a közlés célja, hogy az egyén vagy egyének csoportja elleni erőszak elkövetésének szándékát fejezze ki. Az Elonis v. United States ügy az államközi és a nemzetközi fenyegető kommunikáció kérdésével foglalkozott. Az ügyben Roberts bíró elutasította az ügyészségnek azt az érvelését, hogy a vádnak csak azt kell bizonyítania, hogy egy logikusan gondolkodó személy előre láthatná, hogy a közlése fenyegető hatással van a közönségre. Alito bíró párhuzamos véleményében kifejtette, hogy a valós fenyegetések nemcsak azért korlátozandók, mert erőszakos konfrontációra uszítanak, hanem azért is, mert komoly érzelmi stresszt okoznak a megfenyegetett személynek.

285 United States, 394 U.S. 705 (1969).
286 Virginia v. Black, 538 U.S. 343 (2003).
287 Elonis v. United States, 575 U.S. 723 (2015).
288 Az Amerikai Egyesült Államok elnöke 1963. november 22. és 1969. január 20. között.

IV. Az informatikai bűncselekmények Magyarországon

Az informatikai bűncselekmények magyarországi története

Az Egyesült Államokhoz képest Magyarországon viszonylag későn, csak az 1980-as évek környékén kezdtek el a számítógéppel mint büntetőjogi problémával foglalkozni. Az 1979-ben megjelent *Bevezetés a jogi informatikába* című kötet[289] már foglalkozik a számítógép igazságügyi alkalmazásának egyes kérdéseivel, noha elsősorban még nem a számítógéphez kötődő kriminalitást vizsgálja, hanem azt, hogy hogyan lehet a nyomozás során alkalmazni ezeket az eszközöket, továbbá azt, hogy a bűnügyi nyilvántartások adatait hogyan lehet megjeleníteni számítógépes környezetben. A kötet ugyanakkor egy napjainkban aktuális témával is foglalkozik, mégpedig a bűnözés prognózisával, kriminalitási táblák és trendszámítás útján. A bűnözés prognosztizálása manapság főként a mesterséges intelligencián alapuló prediktív rendészet kapcsán érdekes téma. A jogi informatikai szakirodalom sokáig hajlamos volt inkább az igazságügyi alkalmazás kapcsán szólni az információtechnológiai eszközökről, a Borsi Zoltán és J. M. Baturin által szerkesztett *Számítástechnika és a jog* című kötet,[290] a későbbi munkák között pedig Torma András *Jogi informatika* című kötete[291] is az adatbázisokra és a bűnügyi statisztika informatikai hátterére helyezi a hangsúlyt. Előbbi kötet a jogi informatika szakterületei között főként a rendőrségi, ügyészségi, illetve

[289] Aranyi–Koós–Dörnyei 1979.
[290] Borsi–Baturin 1989.
[291] Torma 1993.

bírósági informatikát tárgyalja, koncentrálva a számítógépes nyilvántartásokra (például POLINFO) és ügykezelésre. Utóbbi a jogi munka informatikai támogatásán túl olyan témákat is felvet, amelyek akár napjaink jogpolitikai diskurzusaiban is aktuálisak lennének, többek között szól a számítógépes jogalkotásról, a jogi következtetések modellezéséről, valamint arról, hogy miként lehet adaptálni a jogrendszert a társadalmi-gazdasági-technológiai fejlődés vívmányaihoz. A magyar büntetőjogi szakirodalomban Polt Péter az elsők között, 1983-as tanulmányában hívta fel a figyelmet arra, hogy a számítógépek megjelenése újfajta kriminalitást hozhat, amelyben a számítógép bűncselekmény tárgya és eszköze is lehet.[292] Az információtechnológia és a bűnözés kapcsolatával a 80-as évek végén kriminológiai szempontból aktívan foglalkozott Vavró István is, akinek az írásaiban már megjelenik a „komputerjog" mint önálló diszciplína, amelynek büntetőjogi vonatkozásai is vannak.[293] A témával foglalkozó irodalom, így Nagy Zoltán András[294] és Pusztai László[295] a számítógépes bűncselekményeknek mindössze négy típusát különböztették meg:

- számítógéppel való visszaélés,
- adatkikémlelés,
- szabotázs,
- gépidőlopás.

Ezek a cselekmények a büntető anyagi jogban soha nem jelentek meg mint kodifikált tényállások. A magyar büntető törvénykönyv kimondottan számítógépes bűnözéssel kapcsolatos tényállást egészen a 90-es évekig nem is tartalmazott (szemben például az USA-val, ahol már 1983-ban is szabadságvesztés büntetés járt egyes számítógépes bűncselekmények elkövetéséért). A korai magyar informatikai bűnözést szabályozó normák az informatikai bűnözésre sokáig nem különálló bűncselekményi kategóriaként tekintettek, így azok nem kaptak különálló szerkezeti egységet a Btk.-ban, hanem a gazdasági bűncselekmények közé ágyazottan jelentek meg. Tóth Mihály *Gazdasági bűnözés és bűncselekmények* című monográfiájában[296] ennek megfelelően részletesen szól a számítógépes bűncselekményekről is. Tagadhatatlan, hogy az informatikai bűncselekményeknek, különösen a korai tisztán informatikai bűncselekményeknek (például számítógépes csalás) igen jelentős gazdasági vonzatuk volt, hiszen az ilyen

[292] Polt 1983: 60–64.
[293] Vavró 1989: 367–379.
[294] Nagy 1991: 21–23.
[295] Pusztai 1989: 106–107.
[296] Tóth 2002.

típusú cselekmények többnyire anyagi károkozással jártak. A későbbiek során azonban megszaporodott az olyan cselekmények száma, amelyek motívuma nem az anyagi haszonszerzés, hanem egyéb személyes (például bosszú) vagy politikai (például hacktivizmus) indok. Az első ténylegesen számítógépes bűnözéssel kapcsolatos deliktum, amely megjelent a Btk.-ban, a számítógépes csalás volt, amely 1994-ben került a magyar jogba,[297] viszonylag későn ahhoz képest, hogy Pusztai László már 1989-ben csalásként minősítette azt, ha valaki úgy okoz kárt, hogy „az adatfeldolgozási folyamat eredményeit a program helytelen kialakításával, helytelen vagy hibás adatok felhasználásával vagy a feldolgozás folyamatára való egyéb jogtalan ráhatással befolyásolja".[298] A magyar számítógépes bűnözéssel kapcsolatos irodalom, különösen a kezdeti időszakban, sokat merített a német szabályozás tapasztalataiból. Pusztai László, a téma hazai kutatásának úttörője a német *Computerkriminalität* tanulmányozása után kezdett foglalkozni „a jog és a technika találkozása nyomán jelentkező"[299] problémákkal. A csalás jellegű bűncselekmény kriminalizálására azért kerülhetett az elsők között sor, mert a számítógép megtévesztésével, az adatmanipulációval nem volt elkövethető a hagyományos csalás, amelynek kulcseleme a személyek megtévesztése, tévedésben tartása. A számítógépes csalás kodifikációja korántsem oldott meg minden elhatárolási problémát: a korabeli ítélkezési gyakorlat számára nehézséget jelentett, hogy amikor a gép nem az elkövetés, hanem a leplezés eszköze volt, továbbra is hagyományos csalást kellett megállapítani, olykor pedig a számítógép mind az elkövetésnek, mind a leplezésnek az eszközéül szolgált.[300] Később, 1996-ban a tényállás kiegészült, az elkövetési tárgyak körébe vonva a távbeszélő-szolgáltatások körében működő számítástechnikai rendszereket.[301] Az internet megjelenésével nemcsak a számítógépes csalás, de a hagyományos csalásra irányult figyelem is megjelent számítógépes köntösben. Az informatikai bűncselekmények hazai fejlődéstörténete során a jogalkotó és a témával foglalkozó szakirodalom számára sosem volt kérdéses, hogy a jövőben újfajta elkövetési módszerek, eszközök és terek jelennek meg.[302] A 90-es évek végének egyik nagy port kavart ügye az Elender-ügy, amely világossá tette, hogy az informatikai bűncselekmények sürgős és átgondolt bővítésére van szükség. 1999 decemberében néhány fiatal

297 A számítógépes csalás tényállását az 1994. évi IX. törvény iktatta be a gazdasági bűncselekmények közé.

298 Pusztai 1989: 106–107.

299 Parti–Kiss 2014: 297.

300 Tóth 2006: 182.

301 Tóth 2006: 184.

302 Lásd Kürti 2002: 10–26.

az Elender Rt. honlapján keresztül belépett a cég rendszerébe, ahol egy úgynevezett *sniffer*-programmal naplózták az előfizetők és a szerver közötti adatforgalmat, rögzítve mintegy 1900 felhasználó nevét és a hozzájuk tartozó jelszót.[303] Később a cég honlapját is kicserélték egy saját weblapra, amelyen közzétették a megszerzett adatokat. A cég válaszul leállította a szervereit, ami miatt sok ezer ügyfél internet- és e-mail-szolgáltatása szünetelt.[304] Az elkövetők, akik közül volt, aki még a 16. életévét sem töltötte be az elkövetéskor, cselekményüket elismerték a bíróságon is hangoztatva, hogy „fullra bent voltak" a rendszerben. Bűncselekmény hiányában másodfokon jogerőssé vált felmentő ítélet született, hiszen a számítógépes rendszer megsértése akkoriban még nem szerepelt a magyar büntető törvénykönyvben, a vádiratban az ügyészség közérdekű üzem működése megzavarásának bűntettével vádolta az elkövetőket. Az informatikai bűncselekmények szabályozása a későbbiekben szorosan követte az európai szabályozás vívmányait, a Cybercrime Egyezmény elfogadását követően 2001-ben a Btk.-ban is megjelentek az egyezmény által büntetni rendelt tényállások, így a számítógépes rendszer és adat sérelmére elkövetett bűncselekmény. Ekkor már hazánkban sem volt ismeretlen jelenség az adathalászat *(phishing),* de ekkoriban jelentek meg az úgynevezett „nigériai levelek" is,[305] és a számítógépes vírusok terjedése is közismert volt.[306] Nagy kárt okoztak a betárcsázós csalások, ahol más telefonos (ADLS) kapcsolatát az elkövetők emelt díjas számok tárcsázására használták.[307] Ezek elkövetése a következőképp történt:

> „[A]z Interneten böngészők miközben bizonyos honlapokra látogatnak (tipikusan casino-, gambling-, sex oldalakra) egy program kúszik fel számítógépükre. Például az »I Accept«, »I Agree« opciót választva aktiválódik észrevétlenül a betárcsázós program. Ezek a »betárcsázós« programok bontják a normál kapcsolatot, ehelyett újat építenek fel, általában egy emelt díjas, tengerentúli vagy éppen műholdas számot tárcsáznak több száz forint/perc díjért."[308]

A csalásnak ez a formája már szinte teljesen eltűnt, hiszen a telefonos modemkapcsolatokat felváltották a széles sávú kábeles és optikai szálas internetkapcsolatok. A közösségi média magyarországi elterjedésével együtt hazánkban is megjelentek a közösségi

303 Az Elender-hekkelés ítélete és tanulságai 2003.
304 Felmentették az Elender-hackereket 2004.
305 Egyre több az internetes csalás 2004.
306 2003: az internet, informatika egy éve 2003.
307 Ingyenes program a tárcsázós csalás ellen 2004.
308 Nagy 2009: 147.

oldalakon népszerű csalások, köztük az az iWiW-es csalás, ahol az elkövetők valójában kattintásvadász módszerrel igyekeztek hirdetési bevételekből hasznot szerezni.[309]

Az adatokkal összefüggő visszaélések hamarabb a figyelem középpontjába kerültek, ahogyan erről Nagy Zoltán András is ír, hiszen az információtechnológiai eszközök elterjedése hazánkban is megteremtette az adatok digitalizálásának, tömeges kezelésének, tárolásának és gyors továbbításának a lehetőségét.[310] Irk Ferenc a 90-es évek végén ki is emelte, hogy az adatvédelem kérdéseinek harmadik generációs érdekként kiemelt figyelmet kell kapniuk a kriminálpolitikában és a rendvédelemben.[311] Vámos Tibor az adatokkal kapcsolatos bűnözés esetében úgynevezett „információs óceánról" ír, amelyen „kalózok hajóznak",[312] amellyel az adatoknak azt a tömegét törekedett leírni, amely az internetes adatáramlás felgyorsulása következtében megjelent a világhálón. A Német Szövetségi Köztársaságban viszonylag korán rendelték büntetni a számítógépes visszaélést és a komputerszabotázst, amely a számítógépes rendszerek, adatok megsértését, manipulálását jelentette – utóbbi esetben haszonszerzési célzattal. A komputerszabotázs önálló tényállása mellett Pusztai László azt az érvet hozta fel, hogy az adat, program nem minősül dolognak, így arra nem alkalmazható a rongálás vagy lopás tényállása. Parti Katalin is felhívja rá a figyelmet, hogy ezek a számítógépes visszaélések tették ki a 80-as években a számítógépes bűncselekmények több mint felét az NSZK-ban.[313]

A 2000-es években hazánkban is megjelentek a külföldön népszerű, szervezett bűnözői hálózatok által elkövetett informatikai bűncselekmények, köztük a szerzői művek kalózkodása. Az *Index* által az évszázad warezpereként jellemzett Coldfusion-ügyben[314] még 2017-re sem született jogerős ítélet, holott a 28 vádlottas warezügyet elindító razziára 2009-ben került sor. A vádlottak gazdasági társaságot alapítottak szerverhosting szolgáltatás nyújtására, szerverparkjukban azonban sms-warez oldalakat is működtettek, amelyekről emelt díjas sms fejében lehetett szerzői jog által védett tartalmakhoz jutni. Hasonló ügy miatt zajlott a GTS-Datanet szerverparkjában házkutatás, amely főként a nagyszabású rendőrségi akció során elkövetett szabálytalanságok miatt vált hírhedtté.[315] A Coldfusion-ügyhöz

309 IWiW-es csalás terjed a neten 2010.
310 Nagy 2009: 147.
311 Irk 1999: 22.
312 Vámos 2002: 6.
313 Parti–Kiss 2014: 298.
314 Huszonnyolc vádlott az évszázad magyar warezperében 2012.
315 Bodoky 2007.

képest a fő különbség az volt, hogy a GTS-Datanet nem vett részt a cselekmények elkövetésében, számos magánszemély és cég részére kínált tárhelyszolgáltatást, amelyek között akadtak olyan ügyfelek, akik jogellenes tevékenységre használták az általuk bérelt szervereket. A rendőrség több olyan szervert is lefoglalt, amely nem kapcsolódott a cselekmény elkövetéséhez, ezeket utólag, a szakértői vizsgálatot követően juttatták vissza a tulajdonoshoz. Az eset felhívta a figyelmet arra, hogy mennyire fontos, hogy a nyomozó hatóság már a lefoglalásoknál különleges szakértelmet, szaktanácsadót vegyen igénybe, amellyel kiküszöbölhetők a hasonló eljárási szabálysértések. Elméletibb síkon az eset nyomán előtérbe került a digitális bizonyíték forrásával kapcsolatos diskurzus, amely megkérdőjelezhetővé tette azt a korábbi gyakorlatot, hogy az adatot annak hordozójával együtt tárgyi bizonyítási eszközként foglalják le.

Az informatikai bűncselekmények szabályozása a magyar jogban

Az informatikai bűncselekményekkel szembeni fellépéssel foglalkozó szabályok elsődleges forrásai hazánkban a törvények. A Btk. az anyagi jogi szabályokat tartalmazza, ebben találhatók meg azok a magatartások, amelyeket a jogalkotó szankcionálni rendel. A magyar Btk. több címben is foglalkozik olyan bűncselekményekkel, amelyek valamilyen módon információs rendszerekhez kapcsolódnak. Merítve a korábbi, csoportosításokat ismertető fejezetből, jelen fejezet külön alcímek alatt tárgyalja azokat a bűncselekményeket, amelyeknél az információs rendszer az elkövetés tárgya (tisztán informatikai bűncselekmények), valamint azokat a cselekményeket, ahol az információs rendszer csak kisegítő jelleggel, járulékosan van jelen (információs rendszerrel kapcsolatos bűncselekmények). Az egyes deliktumok bemutatása az alábbi struktúrát követi: az egyes alfejezetek a büntető törvénykönyvi tényállásokat követik, és minden esetben a bemutatott cselekmény törvényi tényállásának részletes ismertetésével kezdődnek. A büntető anyagi szabályokat tartalmazó kódexen túl több olyan törvény van, amely az informatikai bűncselekmények elleni fellépésben releváns lehet. A Btk. az informatikai bűncselekményekkel összefüggésben több helyen csak keretdiszpozíciót fogalmaz meg, amelyet más jogszabály tölt ki tartalommal. A személyes adattal, illetve a közérdekű adattal való visszaélés esetében az alkalmazandó háttérjogszabályok az Infotv., valamint az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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 (a továbbiakban: GDPR). Ezek a jogszabályok lefektetik az adatkezeléssel és -feldolgozással kapcsolatos fontosabb fogalmakat és elveket. Keretjellegű tényállás található a Btk.-ban a szerzői és szomszédos jogok megsértésével összefüggő deliktumok esetében is, amelyeknél a szerzői jogról szóló 1999. évi LXXVI. törvény (a továbbiakban: Szjt.) rendelkezéseit kell figyelembe venni.

Amennyiben a tárgyalt cselekményhez kapcsolódik magyar bírósági gyakorlat, az egyes bírósági ítéletek jelentősebb megállapításai is helyt kapnak ezekben a részekben, hiszen a joggyakorlat az a mankó, amely segít feltárni a szabályozás esetleges gyenge pontjait és hiányosságait, továbbá amely a legjobban ábrázolja, hogy az absztrakt törvényi tényállások valójában milyen formában jelennek meg a társadalomban.

Mivel a kötet elsődleges célja az online közegben megjelenő cselekmények részletes elemzése, az alfejezetek arra törekednek, hogy hangsúlyozzák azokat a jellegzetességeket, amelyek az internetes elkövetéssel együtt járnak. Már ezen a ponton is fontos felhívni a figyelmet arra, hogy ezeknek az online jogsértéseknek egy részével nem találkozunk bírósági ítéletekben. Ez nem jelenti azt, hogy ezek a cselekmények ne lennének gyakorta előfordulók vagy tényállásszerűek, sokkal inkább azt, hogy bizonyos ügyek el sem jutnak a magyar bíróságokig, mert például a sértettek nem tesznek feljelentést, vagy az elkövetők nem Magyarországon tartózkodnak, a nemzetközi jogsegély pedig nem jár sikerrel.

Az informatikai bűncselekmények felderítésével, nyomozásával, a jogsértés megszüntetése vagy a bizonyítékok megszerzése érdekében alkalmazható kényszerintézkedésekkel kapcsolatos eljárási szabályokat a büntetőeljárási kódex, a Be. rendezi. Ezeket az eljárási szabályokat részletesen a következő fejezetek ismertetik. E helyütt csak jelezzük, hogy a büntetőeljárásról szóló törvényben is találunk olyan rendelkezéseket, ahol egy-egy intézkedés részletes szabályait más jogszabályok tartalmazzák. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.) rögzíti a közvetítő szolgáltatók esetén alkalmazandó értesítési-eltávolítási eljárás[316] részletszabályait, valamint a tárhelyszolgáltató általi ideiglenes hozzáférhetetlenné tétel eljárási szabályait.[317] Az elektronikus hírközlésről szóló 2003. évi C. törvény rendelkezik az elektronikus hírközlési szolgáltatóknak és a kereső- és gyorsítótár-szolgáltatóknak

316 Ekertv. 13. §.
317 Ekertv. 12/A. §.

a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisához (a továbbiakban: KEHTA) való kapcsolódásának és elektronikus kapcsolattartásának szabályairól, valamint arról, hogy a Nemzeti Média- és Hírközlési Hatóság (a továbbiakban: NMHH) hogyan működik közre az elektronikus adat ideiglenes és végleges hozzáférhetetlenné tételében. Szintén az Eht. rendezi az egyszerű adatátvitelt és hozzáférést biztosító közvetítő szolgáltatást végző elektronikus hírközlési szolgáltatók kötelezettségeit az elektronikus adat ideiglenes és végleges hozzáférhetetlenné tétele esetében.[318]

Tisztán informatikai bűncselekmények

A tisztán informatikai bűncselekményeket a Btk. két fejezetben, négy szakaszban tárgyalja. A XLIII. fejezet szól a tiltott adatszerzésről, valamint az információs rendszer elleni bűncselekményekről, így az információs rendszer vagy adat megsértéséről, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszásáról. A XXXVI., vagyon elleni bűncselekményekről szóló fejezetben kapott helyet az információs rendszer felhasználásával elkövetett csalás (375. §), amely lényegében az információs rendszer vagy adat megsértésének károkozással járó alakzata. A fenti rendelkezések 2004 óta képezik a magyar jog részét – Magyarország ekkor ratifikálta az Európa Tanács 2001. november 23-án Budapesten elfogadott, a számítástechnikai bűnözésről szóló egyezményét,[319] vagyis a Cybercrime Egyezményt, aminek alapján kötelezettséget vállalt arra, hogy megalkotja a megfelelő jogszabályokat az egyezményben meghatározott cselekmények kriminalizálása érdekében. A Btk. e szabályainak beiktatásával a magyar jogalkotó az uniós aktusok átültetésére vonatkozó kötelezettségének is eleget tett.

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról lényegében a Cybercrime Egyezménnyel azonos szabályokat fektet le. Az irányelv, sok egyéb európai uniós normához hasonlóan, a *minimumharmonizáció* elvét követi, vagyis a tagállamok annak szabályainál részletesebb, illetve szigorúbb szabályokat szabadon megállapíthatnak.

[318] Eht. 92/A. §.
[319] Az egyezményt Magyarországon a 2004. évi LXXIX. törvény hirdette ki.

A tipológia koherenciája szempontjából fontos a teljességre törekvés, ezért jelen fejezet minden tisztán informatikai vagy információs rendszerrel kapcsolatos deliktumot számba vesz, ám eltérő hangsúllyal kezel egyes cselekményeket. Mivel a kötet főként azokra a cselekményekre koncentrál, amelyekkel az informatikai eszközöket mindennapjaiban használó egyén találkozhat, különös figyelmet szentelek azoknak a cselekményeknek, amelyek az online térben is elkövethetők (kiberbűncselekmények). A tényállások ismertetésén túl a magyar bírósági gyakorlatból hozott példákkal illusztrálom az egyes cselekmények legjellemzőbb magyarországi elkövetési módszereit. Mivel e cselekmények nem feltétlenül jutnak el még a nyomozási szakba se, ismételten indokolt felhívni arra a figyelmet, hogy a II. részben ismertetett magánpiaci szereplők mind a megelőzés, mind a jogsértő állapotok megszüntetése terén sokat tehetnek. Erre reflektálva bemutatom a cselekmények üldözésének azon mozzanatait, ahol az internetes közvetítő szolgáltatók közreműködése igen fontos lehet. Az offline térre jellemző cselekményeket nem elemzem részletesen, abban az esetben sem, ha azoknak van információtechnológiai elemük, hiszen ezek esetében az internetes közvetítő szolgáltatók szerepének vizsgálata indokolatlan lenne. Tipikusan ilyen cselekmény a pénzhamisítás, a magánokirat-hamisítás vagy a közokirat-hamisítás, amelyek esetében az elkövetést gyakran nyomtatók, scannerek vagy akár képszerkesztő szoftverek teszik lehetővé. Kisebb hangsúllyal szerepelnek a fejezetben azok a cselekmények is, amelyeknek speciális jellegüknél fogva nem magánszemélyek a sértettjeik. Ilyenek a pénzügyi szektort érintő informatikai bűncselekmények, a készpénz-helyettesítő fizetőeszközzel való visszaélés. Noha a pénzügyi szektorban nagyon sok szolgáltatás nyújtása történik online, ezekre a szolgáltatásokra annyira speciális szabályok vonatkoznak, hogy kívül esnek a kötet keretein.

Információs rendszer és adatok elleni bűncselekmények

Az információs rendszer vagy adat megsértése tényállásáról a Btk. 423. §-a rendelkezik. Az e szakasz által kriminalizált elkövetési magatartások köznyelvi elnevezése általában sokkal beszédesebb – ezek a bekezdések szabályozzák a hackelést, a kártékony szoftverek, például vírusok terjesztését, a botnethálózatok kiépítését és a túlterheléses támadásokat.

423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint, vagy jelentős érdeksérelmet okoz.

(4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

A Btk. 423. §-a által szabályozott tényállás valójában háromféle elkövetési magatartással is megvalósítható, ezek:

- az információs rendszerbe történő jogosulatlan belépés [(1) bekezdés],
- a rendszer működésének akadályozása [(2) bekezdés a) pontja], valamint
- az információs rendszerben tárolt adatokkal végzett jogosulatlan műveletek [(2) bekezdés b) pontja].

E bekezdés szövegén látszik, hogy a technológiasemlegesség jegyében fogalmazták meg, így az alkalmazott technológiától és az elkövetés módszerétől függetlenül büntetendő minden olyan magatartás, amely a meghatározott eredményre vezet.

A 9/2012. számú büntető elvi döntés szerint „a védett jogi tárgy a számítástechnikai rendszerek működéséhez, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, valamint titokban maradásához fűződő érdek, és nem magának a számítógépnek vagy gépeknek a mechanikus védelme, erre ugyanis a rongálás törvényi tényállása nyújt büntetőjogi védelmet". A védett jogi tárgy jogosulatlan belépés és az információs rendszer működésének akadályozása esetén az elektronikus

adatfeldolgozó és adatátviteli rendszer integritása, biztonsága, míg az adatokkal való visszaélés esetében az adatok által megtestesített érték, érdek. A bűncselekmény elkövetési tárgya az információs rendszer, amelynek fogalmát a Btk. 459. szakasz (1) bekezdésének 15. pontja pontosan meghatározza. Eszerint: „információs rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége."

Az információs rendszer fogalma felöleli tehát az egyes berendezések összekapcsolása révén létrejött hálózatot, valamint az összes olyan egyéb berendezést, amely szerepet játszik a kapcsolat megteremtésében, fenntartásában és az adattovábbítás folyamatában. A berendezések közötti kapcsolat nem jelent feltétlenül fizikai összekapcsoltságot. Az információs rendszerek közötti összeköttetés létrejöhet elektronikus vagy optikai jeleket továbbító kábelek vagy vezetékek útján, valamint rádióhullámok, infravörös, illetőleg rövidhullámok segítségével, vagy műholdas sugárzás igénybevételével is.[320] A Btk.-ban megfogalmazott definíció nem terjed ki viszont a programra (szoftverre), amely a Cybercrime Egyezmény szerint adatnak minősül. A törvényi szakasz (5) bekezdése definiálja az adat fogalmát. A Btk.-ban meghatározott adatfogalom a Cybercrime Egyezménnyel összhangban az információs rendszer általi feldolgozásra alkalmas információk körébe sorolja a számítógépes szoftverelemeket, vagyis a programokat is.

Jogosulatlan belépés, bent maradás és a belépési jogosultság túllépése vagy kijátszása

Az I. alapeset, amely az (1) bekezdésben jelenik meg, a valamely hálózatba vagy számítógépbe történő jogosulatlan belépés, illetve jogosulatlan bent maradás. Nagy Zoltán András részletesen foglalkozik azzal, hogy mikor jogellenes a hálózatba való belépés vagy bent maradás.[321]

Ha a számítógépbe az elkövető nem jogosult belépni, és a számítógép olyan biztonsági mechanizmusokkal védett, amelyek csak meghatározott személyek számára engedélyeznek belépést, valamint ezek a mechanizmusok aktiválva is vannak az elkövetés idején, a belépés vagy bent maradás jogellenes. Jogosultság nélkül lép be a felhasználó abban az esetben is, ha nem a számára engedélyezett belépési ponton lép

320 Görgényi et al. 2020.
321 Nagy 2009: 283.

be (például a munkahelye helyett az otthonában), a számítógép vagy hálózat biztonsági rendszer megoldásait kihasználva lép be, illetőleg más felhasználó nevével, jelszavával lép be. A magatartás csak abban az esetben tényállásszerű, ha az információs rendszer védelmét szolgáló intézkedések megsértésével, kijátszásával történt. A jogszabály nem követeli meg, hogy a védelmet megvalósító biztonsági intézkedések műszaki-technikai jellegűek legyenek, azok elvileg lehetnek testi, személyi jellegűek is, ez esetben, ha az elkövető az előbbi adatokat erőszak vagy fenyegetés alkalmazásával szerzi meg, más bűncselekmény (kényszerítés, zsarolás) is megvalósulhat. A belépéshez szükséges adatok megszerzésének egyik elterjedt módszere, ahogyan arra Mezei Kitti is rámutat, a pszichológiai manipuláció, az úgynevezett *social engineering*.[322]

Hazai joggyakorlat

A magyar bírósági gyakorlat azt mutatja, hogy a jogosulatlan belépés kétféle élethelyzetben a leggyakoribb.

Az egyik a magánjellegű kapcsolatok megromlása miatti jogosulatlan belépés, amikor is a terhelt alapvetően erőszakos, kontrolláló attitűdjéből következik a cselekmény elkövetése. Sűrűn fordul elő olyan eset, amikor megromlott párkapcsolatot követően a megbántott, megcsalt fél zaklatásszerűen kíséri figyelemmel a sértett számítógépén folyó tevékenységeket, hozzáfér az e-mail- vagy közösségimédia-fiókokhoz, olvassa azok tartalmát. A kapcsolati erőszaknak és az azzal összefüggő cselekményeknek általános velejárója az is, hogy az elkövető úgy zárja el a sértettet a külvilágtól, ismerőseitől, hogy annak e-mail-fiókjait és közösségi oldalait saját kezelésébe vonja a jelszó jogosulatlan megváltoztatásával (Fővárosi Ítélőtábla, 5.Bf.300/2016/40).

A belépés jogosulatlanságát illetően érdekes kérdést vet fel az a helyzet, amikor a terhelt azzal védekezik, hogy belépése azért nem jogellenes, mert a sértett a jelszavait önként elmondta neki, netalán a szóban forgó fiókot a terhelt maga hozza létre a sértett részére, annak jelszavát ő generálta. A 15.B.718/2012/5. ügyben a bíróság álláspontja az volt, hogy a sértett postafiók létrehozására irányuló kérése nem tartalmaz felhatalmazást arra, hogy a vádlott a jelszó ismeretében bármikor belépjen.

A másik előfordulási köre a jogosulatlan belépésnek a munkakörrel összefüggésben elkövetett visszaélés. Ezeknél az elkövető gyakran rendelkezik valamilyen szintű belépési jogosultsággal, ám olyannal, amely az elvégzett műveletekre alapvetően nem jogosítja (például amikor a rendőrkapitányságon egy ügy előadója lezár egy folyamatban lévő ügyet, holott arra csak a rendőrkapitányság segédelőadójának lenne jogosultsága).

322 Mezei 2020a: 32.

A jogosulatlan belépést valósítja meg a hackerek tevékenysége is, akik informatikai ismeretek, módszerek segítségével lépnek be különféle rendszerekbe. Az összes ilyen módszert célszerűtlen lenne felsorolni, az információs rendszerek sokfélesége és összetettsége miatt pedig vélhetően lehetetlen volna mindenre teljes körű listát állítani, ezért az alábbiakban csak néhány fontosabb módszert emelünk ki. Népszerű módszerek a „puffertúlterhelés" *(buffer overflow)* vagy a „nyers erő" *(brute force)* módszer.

> A puffertúlterhelés „alapját programozási hiányosságok képezik, konkrétan a bevitt adatokat tároló pufferek mérete nem megfelelően meghatározott. Ha nincs rendesen kezelve az adatbevitel, a támadó túlírhatja a puffert, és a program adatterületén továbbírva a program visszatérési értékét egy tetszőleges helyre irányíthatja. Jellemzően olyanra, mely részére rendszergazdai jogosultságaival való élést tesz lehetővé, amennyiben a támadott program is ilyen jogokkal futott."[323]

A *brute force* módszer működésének lényege, hogy a rejtjelező rendszer ismeretében az összes lehetséges kulcsot kipróbálva határozza meg az alkalmazott jelszót, adatot. Népszerű a hamis WAP használata, amely során a hacker egy vezeték nélküli hozzáférési pontot *(wireless access point)* hoz létre egy legitim szolgáltató, például étterem vagy szálloda nevében, így csalva lépre az internetkapcsolatra vágyókat. Amint a gyanútlan sértett csatlakozik a hálózathoz, és megkezdi a forgalmazást, a forgalmazott adatok, köztük akár belépési nevek, jelszavak, az elkövetőhöz kerülnek. A webböngészők sérülékenységeit kihasználó sütilopások *(cookie theft)* is népszerű technikája a felhasználói adatok, jelszavak megszerzésének. A hackerek gyakran élnek olyan megtévesztő technikákkal is, mint az adathalászat *(phishing)* vagy a kattintáshalászat *(clickjacking)*.

Mezei Kitti említést tesz az alapvető felhasználói műveletekkel, illetve a rendszergazdáéhoz hasonló jogosultságokkal rendelkező *root level access* vagy *god level access* hozzáférésekről is.[324] Az információs rendszer feletti irányítás megszerzése gyakran úgy történik, hogy az elkövető rosszindulatú szoftvert juttat a célzott számítógépes rendszerbe, ezek azonban már olyan módszerek, amelyek a számítógép működését is akadályozzák, így a következő alapesetnek megfelelően ítélendők meg. A jogosulatlan belépés után végzett további műveletek jellemzően már a következő bekezdés valamelyik fordulatát valósítják meg.

[323] Varga 2003: 41.
[324] Mezei 2020a: 24.

Hazai joggyakorlat

Információs rendszer megsértése valósul meg akkor is, ha az elkövető nem a sértett hardware eszközén hajt végre jogosulatlan műveletet, hanem olyan informatikai szolgáltatással összefüggésben, amelyet a sértett használ. Ilyen szolgáltatás lehet az e-mail-fiók, a felhőtárhely-szolgáltatás, vagy akár a közösségimédia-fiók. A sértett Facebook fiókjának feltörése és a jelszó megváltoztatása tehát megvalósítja az információs rendszer megsértését (Szekszárdi Járásbíróság, Bpk.520/2021/2). Információs rendszernek minősül a mobiltelefon is, így a lopásból származó mobiltelefon képernyőzárának feloldása és a telefon gyári helyzetbe állítása szintén megvalósítja az információs rendszer megsértésének tényállását (Szekszárdi Járásbíróság, Bpk.362/2021/3).

Kritikája lehet a jogosulatlan belépést szabályozó szakasznak, hogy gyakorlatilag egy olyan cselekedetet rendel büntetni, amelynek társadalomra veszélyessége sok esetben igen csekélynek mondható. Főképp a fiatalok körében figyelhető meg az a tendencia, hogy azért törnek be rendszerekbe, hogy megmutassák, ők képesek rá, vagyis vannak annyira képzettek technikailag, hogy ki tudják játszani a rendszert védő mechanizmusokat, mindenféle ártó szándék nélkül.

Itt kell szólni azokról az esetekről is, amikor a rendszerbe való belépés nem károkozásra irányul, de még csak nem is öncélú fitogtatása az informatikai ismereteknek, hanem valójában segítségnyújtási céllal történik. Az úgynevezett etikus hacking olyan tevékenység, amelynek során a hacker azért tör be bizonyos rendszerekbe, hogy azok sebezhető pontjait feltárja, az információkat pedig megossza a rendszer üzemeltetőjével a hibák kijavítása és a komolyabb, rosszindulatú támadások megelőzése végett. Az etikus hackerek gyakran egy-egy cég alkalmazottaiként működnek, ez esetben a büntetőjogi felelősségük értelemszerűen fel sem merül, más esetekben azonban kívülállóként avatkoznak be a rendszer működésébe, ezt Szathmáry Zoltán kéretlen sérülékenységvizsgálatnak nevezi.[325] Noha e cselekmény önmagában véve tényállásszerűnek minősül, a társadalomra veszélyesség gyakorta hiányzik, sőt a sérülékenységek feltárása inkább a társadalom hasznára válik, amennyiben komolyabb károsodástól óvja meg az érintett cégeket és azok ügyfeleit. Mivel vékony a határmezsgye a bűncselekmény és a jó szándékú, de kéretlen sérülékenységvizsgálat között, a jelenség semmiképpen nem maradhat szabályozási anomáliaként, a jelenlegi Btk.-beli szabályozás azonban túl szigorú, és nem feltétlenül szolgál társadalmi érdeket. A rosszindulatú hackerek számára szolgálhat a kódex e passzusa elrettentésül, azonban a fiatal informatikusok

[325] Szathmáry 2020: 340–346.

jövőjének derékba törése már nyilvánvalóan túlmutat a jogalkotó eredeti szándékán. Meglátásom szerint a probléma kezelhető jogalkotás révén, valamint a joggyakorlat finomhangolásával is a már létező jogszabályi kereteken belül. A bírói gyakorlat azzal tudná elősegíteni a helyzet megoldását, ha a bűncselekmény tárgyi oldali elemeinek megvalósulásán túl hangsúlyt helyezne a motívumra és a célzatra, továbbá ha azonos elbánásban részesítené az azonos tőről fakadó cselekményeket. Figyelemre méltó Ambrus István meglátása is, aki a közérdekű bejelentésekről szóló 2013. évi CLCV törvényre hivatkozva közérdekű bejelentésként kategorizálja az egyes, kéretlen sérülékenységvizsgálattal összefüggő magatartásokat.[326] Álláspontja szerint az etikus hackerek bejelentése a feltárt problémáról a társadalom érdekét szolgáló, jogellenességet kizáró közérdekű bejelentésnek minősülhet. E minősítésnek azonban meg kell felelnie azoknak a feltételeknek, amelyek kimunkálása jelenleg is a joggyakorlatra vár, így például a hackerrel szembeni követelmény, hogy dokumentálja a cselekménye egyes lépéseit, haladéktalanul jelezze a feltárt sérülékenységet, és tevékenysége ne irányuljon haszonszerzésre.

A bírói gyakorlat azonban e tekintetben nem mondható egységesnek. Ambrus István két olyan nagy sajtóvisszhangú esetet is részletesen elemez,[327] amelyek Magyarországon történtek, és amelyek összevetése jól rámutat a joggyakorlat következetlenségeire.

Hazai joggyakorlat

Az első esetben a Magyar Telekom rendszerét törte fel egy fiatal főiskolás egy nyilvános felhasználói útmutatóban talált IP-cím segítségével, oda több alkalommal jogosulatlanul belépett, és felhasználói profilokat hozott létre. A hibát jelezte a cégnek, amely feljelentést tett. A szolnoki törvényszék 2019-ben helybenhagyta az I. fokú bíróság ítéletét (Szolnoki Törvényszék: Pénzbüntetésre ítélték első fokon a fiatal hackert 2019).

A második, BKK-botrányként elhíresült esetben egy 18 éves fiatal egy sebezhetőséget kihasználva 50 Ft-ért vásárolt bérletet, majd a hibát haladéktalanul jelezte az online jegykezelési rendszert üzemeltető cégnek. Ebben az ügyben az ügyészség 2017-ben megszüntette a nyomozást, mert közérdekű bejelentőnek minősítette a gyanúsítottat (Nyertünk, megszüntette a nyomozást az ügyészség a BKK-botrány etikus hackere ellen 2017).

326 Ambrus 2021: 87.
327 Ambrus 2021: 86.

A másik lehetőség az etikus hackerek tevékenységével kapcsolatos feszültségek feloldására a szabályozási út, vagyis az etikus hackerek tevékenységének expressis verbis dekriminalizálása. Mivel a kibertérben számtalan jogellenes belépés fordul elő, én a szabályozási választ tartom követendőnek, amely a joggyakorlat számára vezérfonalként szolgálva egységesen meghatározhatja a büntetőjogi felelősségre vonás alóli mentesülés szükséges feltételrendszerét is.

Belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével marad benn az elkövető, ha van ugyan valamilyen szintű jogosultsága a rendszer használatára, azonban e jogosultságát meghaladó műveleteket folytat, vagy a számára engedélyezett idő lejártával nem lép ki a rendszerből. A bűncselekmény befejezett, amint a tettes az első hozzáférési korlátot átlépte, és számára az adatok vagy az adatfeldolgozó rendszer további lépései nyitva állnak.[328]

Hazai joggyakorlat

Nem valósul meg tehát az információs rendszerrel vagy adattal visszaélés azokban az esetekben, amikor az elkövető ugyan visszaélésszerű műveletet hajt végre, ám jogosultsága keretein belül marad, és nem kell technikai intézkedést kijátszania. Ez az eset fordul elő, amikor rendőr hivatalos személy saját egyéni céljából és nem bűnüldözési érdekből hajt végre lekérdezéseket a rendőrségi informatikai rendszerekből (Kb.I.77/201/14.), amikor a könyvelő a célhozkötöttség megsértésével magáncélból lép be a NAV adatbázisaiba (Bhar.III.201/2015/4.), illetve amikor a közfeladatot ellátó egészségügyi dolgozó más személyek különleges adatairól (például egészségügyi állapotáról) ad ki tájékoztatást az érintett beleegyezése nélkül (1.Bf.356/2018/7). Nem minősül technikai intézkedés kijátszásának az az eset, amikor egy dolgozó más személy felhasználónevével és jelszavával lép be ugyan a rendszerbe, ám ezeket a belépési adatokat ismerte, mert azok tulajdonosa felhatalmazást adott a nevében történő műveletek végzésére. A gyakorlatban ez úgy fordulhat elő, hogy a munkahelyi vezető odaadja a titkárnőjének a belépési adatait, hogy az bizonyos feladatokat a nevében végezzen el (Fővárosi Törvényszék, 14.B.454/2016/62).
Ezekben az esetekben azt kell vizsgálni, hogy helye van-e más bűncselekmények megállapításának, például személyes adattal visszaélésnek vagy hivatali visszaélésnek. Személyes adatok megsértésének megállapítását alapozza meg például az, amikor a rendőr a rendőrségi nyilvántartásokban szereplő adatokat saját adathordozóira menti le. Ennélfogva a jogosultság kereteit túl nem lépő keresések végrehajtása jelentős érdeksérelem okozására, haszonszerzésre, hátrányokozásra vagy jogtalan előnyszerzésre irányuló célzat hiányában nem minősülnek bűncselekménynek.

328 Gelányi – Csepely-Knorr 2009: 201–207.

A Kúria az egyik ítéletében felhívta a figyelmet arra, hogy ahhoz, hogy a jogosultság keretein való túllépés bűncselekménynek minősüljön, szintén szükséges a rendszer védelmét biztosító technikai intézkedés megsértése vagy kijátszása, önmagában a jogosultság kereteinek túllépése „nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván" (BH2017.392).

Az információs rendszer működésének akadályozása

Az információs rendszer működésének megzavarása történhet akár hardvereszközök (például különböző jelzavarók), akár szoftvereszközök révén.

Hazai joggyakorlat

Hardvereszköz használatával elkövetett, az információs rendszer működését akadályozó cselekményre példa annak a tevékenysége, aki tehergépkocsi vezetőfülkéjébe olyan készüléket szerel, amely a jármű menetíró készülékét manipulálni tudja, például haladás során pihenőidőt mutat, vagy nem rögzíti a valós haladási sebességet (Szekszárdi Járásbíróság, Bpk.392/2021/3).
Hardvereszköz révén sértette meg a mobiltelefon mint információs rendszer integritását az a fogvatartott, aki a speciális büntetés-végrehajtási intézeti kapcsolattartásra rendszeresített mobiltelefonba olyan mikrokontrollerrel rendelkező SIM-adaptert szerelt, amely meghamisítja a telefon és a SIM-kártya közötti kapcsolatot, és kijátssza a szolgáltatói szoftveres korlátozást, amelynek célja, hogy csak a fogvatartotti nyilvántartó rendszer közbeiktatásával, ellenőrzött módon lehessen hívásokat bonyolítani (Debreceni Járásbíróság, 44.B.221/2020/65).

Az információs rendszer rendeltetésszerű működésének akadályozására a modern technológia állása szerint különösen alkalmasak a különféle kártékony programok, ezért a 423. §-ban szabályozott cselekmény két legtipikusabb elkövetési magatartása a *malware*–, illetve a botnettámadás. A régi Btk.[329] *Kommentár*ja a számítástechnikai rendszer megsértésének egyik eszközeként a számítógépes vírusokat említi.[330] A számítógépes vírus azonban csak egyike azoknak a kártékony programoknak *(malware),* amelyek alkalmasak a számítógép működésének kedvezőtlen befolyásolására. A kártékony programok közös jellemzője, hogy olyan szoftverek, amelyek akadályozzák

[329] 1978. évi IV. törvény a Büntető Törvénykönyvről.
[330] Varga 2004.

a számítógép működését, illetve korlátozzák a rendeltetésszerű használatát. A legismertebb *malware*-fajták az alábbiak.[331]

- Vírus *(virus):* vírusnak nevezzük azokat a szoftvereket, amelyek képesek a felhasználó tudta nélkül egyik számítógépről a másikra, vagy akár ugyanazon a gépen belül több helyre észrevétlenül reprodukálódni. Általában fertőzött program segítségével terjednek. A vírusok csoportosításának egyik lehetséges módszere a fertőzött alrendszerek, illetve programok szerinti csoportosítás. Ezek alapján megkülönböztethetjük az alábbi vírustípusokat:
  - Programvírusok *(file-infector virus):* a programvírusok bináris futtatható (például exe) fájlokba ágyazódnak. Népszerűek mostanában az úgynevezett zsarolóvírusok *(ransomware),* amelyek a rendszert megfertőzve állományokat titkosítanak, és csak akkor adják meg a feloldáshoz szükséges kódot, ha a felhasználó egy megadott számlaszámra váltságdíjat utalt. A zsarolóvírusok egyre gyakrabban jelennek meg Magyarországon is, ahol magánszemélyek mellett főként cégek, illetve kritikus infrastruktúrák (például kórházi rendszerek) válnak áldozatul.
  - Adatfájlokban lévő vírusok: idetartoznak a makrovírusok, valamint az érvénytelen fájlformátumot kihasználó vírusok. A makrovírusok olyan vírusok, amelyek a Microsoft Office programjaiba ágyazódva különböző kártékony hatásokat fejtenek ki. Az érvénytelen fájlformátumra épülő vírusok azoknak a programoknak a hibáit használják ki, amelyek egy-egy meghatározott fájlformátummal dolgoznak.
- Féreg *(worm):* a féreg olyan önmagában működő szoftver, amely képes önmagát reprodukálva egyik számítógépről a másikra terjedni. Abban különbözik a vírustól, hogy önmagában is működik és életképes, nem kapcsolódik egyéb szoftverekhez. Az önsokszorosításon kívül a féreg számtalan dologra programozható – ezek a másodlagos funkciók a *payload.*
- Trójai faló *(trojan horse):* trójai szoftvereknek nevezzük azokat a kártékony szoftvereket, amelyek magukat általában ártalmatlan vagy segítő célú szoftvernek álcázva települnek fel a számítógépre. Hasonlóan a számítógépes férgekhez, a rendszerbe kerülésüket követően számtalan dologra programozhatók, például a számítógépen található állományok titkosítására, zombiszámítógép

[331] A csoportosítás és a fogalommagyarázat a Nemzeti Kibervédelmi Intézet tudatosító anyagainak felhasználásával készült (Nemzeti Kibervédelmi Intézet 2023).

létrehozására, személyes adatok összegyűjtésére és elküldésére, a felhasználó webkamerájának használatára, az operációs rendszer távoli használatára stb.
- *Rootkit:* olyan szoftvereszközök, amelyek elrejtenek egyes folyamatokat vagy adatokat az operációs rendszerben, vagy hozzáférést tesznek lehetővé bizonyos alrendszerekhez vagy programokhoz.
- Hátsó ajtó *(backdoor):* olyan program, amely a felhasználó tudta nélkül távoli hozzáférést tesz lehetővé. Ezek a programok általában egy előre meghatározott TCP- vagy UDP-portot nyitnak, amelyre az elkövető rácsatlakozhat.
- Kémprogram *(spyware):* célja a számítógépről információ megszerzése. Lehet webalapú, mint egy káros weboldal, települhet is webről, de megeshet, hogy maga az ártani kívánó fél telepíti fel a gépre (például billentyűleütés-naplózó program *[keylogger],* amely megjegyzi az összes leütött billentyűt).
- Kéretlen reklám *(adware):* olyan szoftver, amely automatikusan reklámokat jelenít meg. Bár ez nem következik a definíciójából, általában negatív értelemben használják a jelzőt olyan programokra, amelyeket nem szívesen látunk a számítógépen. Ilyennek minősülhet akár legális szoftver is, mint például egy másik szoftverrel feltelepült böngészőeszköztár *(toolbar).*

Az előbbiekben felsorolt kártékony programok általában nem egymástól elhatárolhatóan működnek, az előbbi kategóriák a mai környezetben inkább az egyes programfunkciók leírására szolgálnak. Egy-egy kártevő több funkció ellátására is programozható, így valójában a modern *malware*-ek esetében a fentiek valamilyen csomagba szerkesztett változatát jelentik.

Hazai joggyakorlat

Kártékony szoftverek egyre gyakrabban jelennek meg Magyarországon is, az Országos Bírósági Hivatal adatbázisában rendelkezésre álló nyilvános információk azonban arra engednek következtetni, hogy ezek terjesztőivel szemben jogerős ítéletek ritkán születnek. Ennek hátterében számos ok állhat, részben az, hogy az elkövetők felett nem Magyarország rendelkezik joghatósággal, az eljárások bonyolultak és elhúzódnak, valamint az is, hogy kevés sértett tesz feljelentést, tartva az üzleti jó hírnevük csorbulásától. A 2017-ben futótűzként elterjedt WannaCry zsarolóvírus miatt az ORFK tájékoztatása szerint csak ketten tettek feljelentést (ORFK: Ketten tettek feljelentést a WannaCry miatt. *HVG,* 2017. június 16.).

A zsarolóvírus-támadások népszerű prédái a kórházak és az egészségügyi intézmények, amelyeknél az egyes fájlok (például kórlapok, leletek) titkosítása nemcsak az egészségügyi dolgozók munkáját nehezítheti meg, hanem extrém esetben emberéletet is követelhet. Magyarországon az első kórházi zsarolóvírus 2016-ban jelent meg a veszprémi Csolnoky Ferenc kórház rendszerében (Itt az első magyar kórházi zsarolóvírus. *Index,* 2016. április 8.).
2021 novemberében a magyarországi leányvállalattal is rendelkező Media Markt csoport jelentette, hogy zsarolóvírus-támadás áldozatává vált. A támadást magára vállaló Hive-csoport a titkosított fájlok feloldásáért 240 millió dollárt követelt a cégtől. A cég a vírusfertőzés időszakában nem tudta működtetni a webáruházait, és az áruvisszavétel is akadozva folyt.

A magyar jogrendszerben nem nevesítik külön, az európai büntetőjogi gondolkodásban azonban kiemelt figyelmet kapnak az úgynevezett botnethálózatok. A botnet a *robot* és a *network* szavak összekapcsolásából ered, és vírussal fertőzött számítógépek hálózatára utal, amelyeket az elkövető(k) távolról küldött utasítások sorozatán keresztül képes(ek) irányítani, ezáltal tömegesen felhasználni bűncselekmények elkövetéséhez. A botnettámadások jelentősége abban áll, hogy tipikusan nem az egyéni felhasználók, hanem kritikus infrastruktúrák, nagyvállalati rendszerek ellen irányulnak, és komoly károkat tudnak okozni. A botnet kifejezést európai uniós dokumentumban először 2006-ban említik. A spamekről szóló közleményében az Európai Bizottság a kéretlen üzenetek küldésére szolgáló eszközként jellemezte a botnethálózatokat. Tény, hogy a botnetek célja kéretlen üzenetek tömeges küldése is lehet, de nem ez a legkártékonyabb felhasználási módjuk. A 2007 májusában kiadott, a kiberbűncselekmények elleni fellépés általános megközelítéséről szóló közlemény már jóval nagyobb szerepet tulajdonított a botneteknek, és ezeket az infrastruktúrákat tette felelőssé az olyan átfogó, információs rendszerek elleni támadásokért, mint amilyen az észtországi kritikus infrastruktúrák elleni támadás volt 2007-ben.[332]

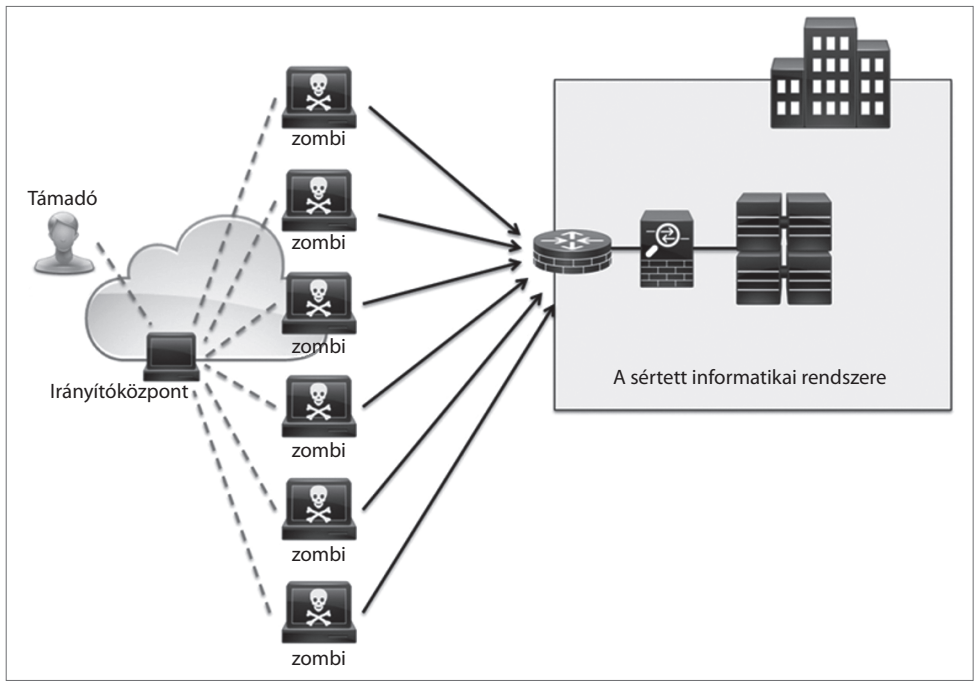
Az információs rendszerek elleni támadásokról szóló irányelv kiemelten foglalkozott a botnethálózatokkal szembeni fellépés kérdésével.[333] Ez az uniós norma már a célját is abban határozza meg, hogy „[büntetőjogi] szankciókat állapítson meg a botnetek létrehozására, vagyis azon cselekményre vonatkozóan, amellyel célzott informatikai támadások révén jelentős számú számítógép felett veszik át a távvezérelt irányítást oly módon, hogy rosszindulatú számítástechnikai programokkal fertőzik meg őket".[334]

[332] Az oroszok visszabombázzák Észtországot az online kőkorszakba 2007.
[333] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.
[334] Az Európai Parlament és a Tanács 2013/40/EU irányelve (1) preambulumbekezdés.

Az irányelv arról is rendelkezik, hogy az olyan támadások esetében, amelyek célja botnet létrehozása, vagy amelyeket botnet révén hajtanak végre, a tagállamok megállapíthatnak súlyosabb szankciót.[335] Ezt a szabályt a Btk. akképp ültette át, hogy az információs rendszer vagy adat megsértése bűntettének minősített esete valósul meg, ha a cselekmény jelentős számú információs rendszert érint.[336] A botnet számos funkciót elláthat, Nagy Zoltán és Mezei Kitti a következő botnetfunkciókat különbözteti meg: DDOS-támadások indítása, spamküldés, adathalászat, hálózatfigyelés, billentyűzetfigyelés, internetes reklámokhoz kapcsolódóan klikkelések begyűjtése.[337] Újabban a botnethálózatokat gyakran használják kriptovaluták (például bitcoin) bányászására.

A botnethálózatok funkciói közül talán az egyik leghírhedtebb a túlterheléses támadás *(denial of service attack – DOS).* A túlterheléses támadások esetében az elkövető azzal akadályozza a rendszer működését, hogy olyan adatmennyiséget zúdít a célrendszerre, amelyet az képtelen kezelni. A túlterheléses támadások manapság leggyakrabban úgynevezett elosztott túlterheléses támadással *(distributed denial of service attack – DDOS)* történnek, ami annyit jelent, hogy a megfertőzött zombiszámítógépek a megcélzott szervereknek folyamatosan kéréseket – adatcsomagokat – küldenek, és ha több ezer csomag érkezik egyszerre, a forgalmazás mértékét a támadott rendszer nem bírja el, és ez a rendszer teljes összeomlását eredményezheti. Ugyanakkor az információs rendszer működésének akadályozásához nem feltétel a célrendszer teljes megbénulása, ahogy Nagy és Mezei is kiemelik: a „funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik."[338] A cselekmény különösen súlyos lehet, hiszen a Btk. szerint a cselekmény minősített esetét követi el, aki a 423. §-ban szabályozott magatartásokat közérdekű üzem ellen követi el. Mivel bizonyos infrastruktúrák megbénításának a hátterében gazdasági érdek, de akár politikai figyelemfelhívás is állhat, a szervezett bűnözői körök ma már gazdasági szolgáltatásként kínálják DDOS-támadások lefolytatását, illetve az ilyen támadások lefolytatásához használható infrastrukúra bérbeadását. Mezei Kitti tanulmányában kifejti, hogy napjainkban „napi vagy havi díjjal átlagosan 5 $ és 1000 $ közötti áron" lehet szert tenni hasonló eszközökre.[339]

[335] Az Európai Parlament és a Tanács 2013/40/EU irányelve (13) preambulumbekezdés.
[336] Btk. 423. § (3) bekezdés.
[337] Nagy–Mezei 2017: 163–168.
[338] Nagy–Mezei 2017: 164.
[339] Mezei 2018: 70.



4. ábra: *Elosztott túlterheléses támadás*
Forrás: CISCO (2023): DDOS támadások felépítése; a szerző fordítása

Az elosztott túlterheléses támadások esetében érdemes röviden foglalkozni a tettesség kérdésével. A törvény *Kommentár*ja alapján a Btk. 423. § (2) bekezdése szerinti cselekmények elkövetője bárki lehet, azonban azok csak szándékosan valósíthatók meg.[340] Mivel a botnetek esetében a támadásban zombiként, távoli vezérléssel részt vevő rendszerek tulajdonosainak gyakran arról sincs tudomásuk, hogy a gépük vírusfertőzés áldozata, a támadással érintett információs rendszer tekintetében az akadályozási szándék egyértelműen kizárható. A szándék általában a mestergép tulajdonosa, a *botherder* oldalán jelenik meg, az ő cselekménye szándékos és egyben célzatos. Az elkövető ebben az esetben nemcsak a túlterheléses támadással célzott információs rendszer működését akadályozza, hanem az összes olyan információs rendszer működését is, amelyet megfertőzött, és távoli hozzáféréssel támadásra utasított.

340 Karsai 2019b: 989–996.

Az információs rendszerben tárolt adatok jogosulatlan megváltoztatása és törlése

A Btk. 423. § (2) bekezdésének b) pontjában található az elkövetési magatartások második köre, amely elektronikus adatok bevitelét, megváltoztatását, törlését és hozzáférhetetlenné tételét rendeli büntetni. Elkövető ebben az esetben bárki lehet. A tényállás szövegében a jogosulatlan jelző az eredményre utal, így elkövetheti a bűncselekményt az is, aki egyébként jogosult a rendszerbe belépni, ott az adatokon műveleteket végrehajtani, jogosultsága azonban nem terjed ki a rendszer működésének akadályozására. Adat törlése kapcsán az elkövető tudattartalma lényeges, ugyanis az akkor is megvalósul, ha az adatokat csak különleges szakértelemmel lehet visszaállítani. A törlés megvalósulhat a törlés funkcióval vagy a mágnesszalagok elektromágneses úton való törlésével, hozzáférhetetlenné tételen pedig az adatok elrejtését értjük például egy olyan fájlban, amely jelszóval védett vagy kódolt, de idetartozik az adathordozó elrejtése is.

A cselekmény az adatok megváltoztatásán túl megvalósítható új, valótlan adatok rögzítésével is. Ezekben az esetekben az adatbevitel más bűncselekményt is megvalósíthat (például sikkasztás), de az is előfordulhat, hogy az elkövető az adatbevitelt vagy -módosítást más jogellenes cselekmény leplezésére használja fel.

Az elhatárolási kérdések az adatmanipuláció esetében különösen érdekesek, hiszen kiemelt hangsúlyt kap az elkövető szándéka és az általa okozott kár. Előfordulhat, hogy az adatmanipuláció haszonszerzési célú, ez esetben információs rendszer felhasználásával elkövetett csalás valósul meg. Elképzelhető az is, hogy az adatok megváltoztatása valójában egy másik, jogellenes cselekmény leplezését (például sikkasztását) szolgálja, ez esetben az információs rendszerrel visszaélés halmazatban lesz megállapítható ezzel a cselekménnyel. A halmazat ugyanakkor látszólagos minden olyan esetben, ahol az egyik cselekmény nem hajtható végre az információs rendszerben tárolt adatok megváltoztatása nélkül. Ennélfogva közokirat-hamisítást kell megállapítani, ha az információs rendszerben található nyilvántartásban lévő rekord önmagában is közokiratnak számít (például gépjármű-vezetői jogosultság közhiteles nyilvántartásában kezelt adatok). Ekkor az információs rendszerben tárolt adatokkal kapcsolatos visszaélés a közokirat-hamisításba beolvad.[341]

[341] BH 2010.2.33: Legf. Bír. Bfv. II. 74/2008. I.

Hazai joggyakorlat

Az információs rendszerben tárolt adatok jogosulatlan megváltoztatása és törlése valósult meg, amikor az orvosírnoki munkakörben dolgozó vádlott egy kórházban az informatikai rendszerbe valótlan adatokat vitt be. A valótlan ambuláns kezelőlap adatait a munkaköri leírásban rögzített kötelességeinek megszegésével, az osztályvezető főorvos nevében hozta létre, annak tudta nélkül. A számítástechnikai rendszerbe bevitt egy hamis elszámolási nyilatkozatot is, így a rendszerben lévő adatok megbízhatóságához, hitelességéhez fűződő érdekek sérültek (Szombathelyi Törvényszék, B.448/2009/7). Ha a terhelt ugyanezt a cselekményt hasznonszerzési céllal követte volna el, akkor a cselekménye már információs rendszer felhasználásával elkövetett csalásnak minősülne. Jogosulatlanul változtat meg adatokat az egyetemen az a tanulmányi ügyintéző is, aki az egyetemi tanulmányi rendszerbe egyes hallgatók részére jogosulatlanul „jeles" érdemjegyet rögzít. Szintén csalás valósul meg abban az esetben, ha ezért a tevékenységéért ellenszolgáltatást fogad el a hallgatóktól.

Valótlan adatok rögzítésével valósul meg a cselekmény, amikor az elkövető, egy bank dolgozója az általa kezelt főkönyvi számláról létező, illetve fiktív ügyfelek számára ír jóvá összegeket, azért, hogy ezeket később, további műveletekkel a saját számlájára átvezesse (21.B.480/2019/20).

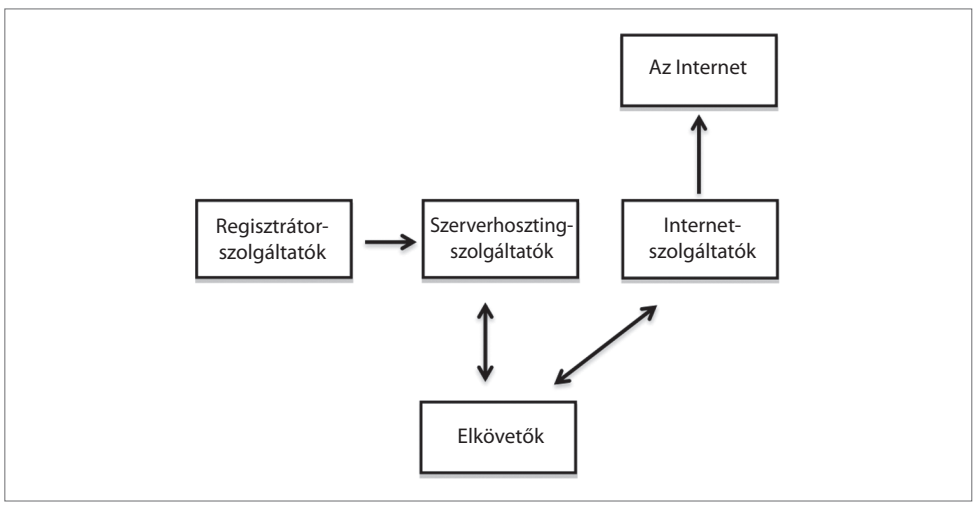
Az internetes közvetítő szolgáltatók szerepe a kártékony programok (malware) elleni fellépésben

Az OECD tanulmánya az internetes közvetítő szolgáltatóknak a közérdekű célok elérésében betöltött szerepéről[342] külön fejezetet szentel az internetszolgáltatók szerepének a kártékony programok elleni fellépésben. A tanulmány rámutat arra, hogy a felhasználók gyakran nem foglalkoznak eszközeik védelmével, és nem feltétlenül rendelkeznek a megfelelő készségekkel ahhoz, hogy megelőzzék a problémákat, vagy eltávolítsák a káros programokat, ha már megtörtént a gond.[343] Ha a felhasználó számítógépe vírusfertőzés révén egy botnethálózat tagjává vált, a fertőzés nagyobb kárt okozhat egy másik, megtámadott rendszernek, mint a fertőzött felhasználónak. Az OECD éppen ezért úgy látja, hogy az internetszolgáltatók bevonása a fertőzések megelőzésébe, felismerésébe, megszüntetésébe egyre inkább olyan módszernek tűnik, amely segíthet internalizálni a negatív externáliákat (vagyis azokat a költségeket,

342 OECD 2011a.
343 OECD 2011a: 112.

amelyek egy adott cselekvés miatt merülnek fel, harmadik személyek érdekkörében, akik nem felelnek a cselekvéshez vezető döntésért).[344] Az internetes közvetítő szolgáltatók szerepét a kártékony szoftverek terjedésében jól szemlélteti az 5. ábra.

Ebben a rendszerben több szolgáltatónak is kulcsfontosságú szerep jut az adatforgalmazásban. A regisztrációt végző szolgáltatók doménneveket osztanak ki a felhasználóknak, a tárhelyszolgáltatók szervereiken helyet biztosítanak harmadik személyek tartalmainak, a hozzáférés-szolgáltatók avagy internetszolgáltatók a hálózati infrastruktúrához való hozzáféréshez fizikai eszközöket (például modem) és virtuális eszközöket, azonosítókat (például IP-címet) biztosítanak. Jason H. Peterson az internetszolgáltatók funkcióját egyenesen egy szabályozói funkcióval azonosítja,[345] mivel ezek a szereplők képesek a felhasználók kapcsolódását szabályozni, a hozzáférést biztosítani, azt megakadályozni, előfizetési szerződéseikben pedig akár magatartási szabályokat is megfogalmazhatnak a hálózatuk használatára vonatkozóan. Az internetszolgáltatók megakadályozhatják a *malware*-ek terjedését azzal, hogy önkéntes alapon növelik a hálózatukra kapcsolt eszközök biztonságát, például azáltal, hogy jelzik a felhasználóknak, ha fertőzöttséget észlelnek, és tanácsot adnak az eltávolításra, adott esetben karanténba helyezik a fertőzött gépet.



5. ábra: *Az internetes közvetítő szolgáltatók szerepe a kártékony szoftverek terjedésében*
Forrás: Peterson 2014: 597

344 OECD 2011a.
345 Peterson 2014: 597.

Az internetszolgáltatók hasonló fellépésére holland és amerikai példa is ismert. Hollandiában az internetszolgáltók 2009-ben önszabályozás révén törekedtek kezelni a *malware*-fertőzött számítógépek és a botnetek problémáját.[346] Az önszabályozó rendszerhez tartozó 14 szolgáltató az információcsere mellett megállapodott abban is, hogy karanténba helyezik a fertőzött számítógépeket, és értesítik a felhasználóikat. Az Egyesült Államokban az American Council on Education v. FCC ügyben[347] a bíróság kimondta, hogy a bűnüldöző szervek számára nyújtott kommunikációs közreműködésről szóló törvény (Communications Assistance for Law Enforcement, 1994) lehetővé teszi, hogy az internetszolgáltatókat jobb és megbízhatóbb infrastruktúra biztosítására kötelezzék a nyomozó hatóságok által végzett megfigyelés érdekében. A Szövetségi Kommunikációs Bizottság (Federal Communication Commission) 2012-ben jóváhagyta a botnetek elleni küzdelemről szóló önszabályozási kódexet, amelyhez olyan szolgáltatók csatlakoztak, mint az AT&T, a Centurylink vagy a Comcast.[348] A vállalások között szerepel az azonosítás (a hálózaton folyó botnettevékenység azonosítása, adatgyűjtés annak működéséről), az értesítés (az érintett felhasználók tájékoztatása a fertőzés tényéről), valamint a segítségnyújtás a fertőzés megszüntetéséhez. Ennek ellenére Shachtman szerint[349] az internetszolgáltatók ritkán üldözik maguktól a büntetőjogba ütköző cselekményeket. Példaként egy amerikai tárhelyszolgáltató, a McColo esetét hozza, amely sokáig a világ spamküldő tevékenységének központjaként működött. Annak ellenére, hogy a McColónak hálózati hozzáférést biztosító szolgáltatók, a Global Crossing és a Hurricane Electric tudtak a tárhelyszolgáltató tevékenységéről, nem függesztették fel a szolgáltatás nyújtását, csak akkor, amikor annak *spam*- és *malware*-terjesztő tevékenységét a sajtó nyilvánosságra hozta.[350] Az internetszolgáltatók vonakodó magatartásának több indoka is van. Az egyik indok alapvetően üzleti jellegű, ugyanis a túl agresszív hálózat-ellenőrzés bevételcsökkenést eredményezhet,[351] hiszen a folyamatos ellenőrzés megnövekedett munka- és erőforrás-ráfordítással jár, ami költségigényes, másrészt a felhasználók magánéletébe történő beavatkozás miatt egyes fogyasztók elpártolhatnak a szolgáltatóktól. A hálózati adatáramlás megfigyelésére szolgáló mélyreható adatcsomag-elemzés *(deep packet inspection)* részletes információt ad a szolgáltatóknak a hálózati kommunikáció tartalmáról.

346 Evron 2009.
347 American Council on Education v. FCC, 451 F.3d 226, 233 (D.C. Cir. 2006).
348 The Communications Security, Reliability and Interoperability Council 2012.
349 Shachtman 2011.
350 Krebs 2008.
351 Peterson 2014: 599.

Az adatcsomag-elemzés a fejléc (címzés) adatainak vizsgálatán túl lehetővé teszi a tartalom elemzését is. Az elektronikus hírközlési szolgáltatók a kommunikáció tartalmát általában véve nem tárolják az átvitelhez szükséges időtartamnál tovább, és nem is ismerik. A kommunikáció tartalmának figyelemmel kísérése amellett, hogy elképesztő erőforrásokat emésztene fel, a felhasználók magánéletébe történő súlyos beavatkozásnak minősülne. Egyes országokban a közlés tartalmának internetszolgáltató általi megismerése még a szolgáltató büntetőjogi felelősségének kérdését is felveti. A NATO és az ENISA közös tanulmánya a német szövetségi büntető törvénykönyv szabályai mentén mutatja be az internetszolgáltatók felelősségének témáját, és arra a megállapításra jut, hogy az internetszolgáltatók csak *ad hoc* jelleggel vizsgálhatják az adatcsomagokat és a forgalmazási adatokat, amennyiben a telekommunikációs rendszerek hibáinak feltárása és kijavítása érdekében szükség van rá, máskülönben e tevékenységük tiltott adatszerzésnek minősül.[352] A magyar internetszolgáltatók is végezhetnek ilyen tevékenységet – a Telekom általános szerződési feltételei szerint „a [s]zolgáltató a tevékenysége során alkalmazott, a jelek továbbítását végző berendezéseinek adatait rendszeresen elemzi, valamint a hálózaton időszakos ellenőrzéseket végez a hálózat egysége és biztonságos működése érdekében".[353] A Btk. szintén ismeri a tiltott adatszerzés tényállását, a magyar jogban ez a cselekmény viszont célzatos, vagyis a büntetendőséghez a személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerésének célja szükséges, ami az internetszolgáltatók oldalán nem áll fenn, amennyiben céljuk a kártékony kódokat tartalmazó kommunikáció szűrése.

A hálózat „tisztán tartásának" vállalásával a szolgáltató közvetett felelősséget vállalna az azon folyó jogellenes tevékenység miatt is.[354] Ez a fajta felelősségvállalás nem éri meg a szolgáltatónak, kiváltképp amiatt, hogy mind az amerikai, mind az európai jogrendszerek széles körű felelősség alóli mentesülést tesznek lehetővé azokban az esetekben, amelyekben a szolgáltató passzív szereplője a kommunikációs folyamatnak. E passzív szerep megőrzése lényegében attól függ, hogy a szolgáltató ismeri-e a harmadik személyek által küldött adatcsomagok tartalmát. Ha tisztában van a felhasználó által küldött és fogadott adatcsomagok tartalmával, vagy vállalja, hogy a hálózat biztonságosabbá tétele esetében megismeri ezeket, akkor rá is telepíthető felelősség, amelynek a vállalása a szolgáltatók számára nem lenne sem célszerű, sem gazdaságos.

352 Vihul et al. 2012.
353 Telekom: Lakossági általános szerződési feltételek, 2/C melléklet.
354 Peterson 2014: 599.

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

424. § (1) Aki a 375. §-ban, a 422. § (1) bekezdés d) pontjában vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja,

vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntetőügyekben eljáró hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

(3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.

Ebben az esetben a védett jogi tárgy az elektronikus adatfeldolgozás és -átvitel integritása, biztonsága, amely magában foglalja az információs rendszert és annak működését, valamint a feldolgozásra rendelt adatok biztonságát. E bűncselekmény valójában „sui-generis előkészületi-bűnsegédi jellegű cselekmény”,[355] amely a korábbi szakaszok védelmét egészíti ki. A bűncselekmény elkövetési tárgya az elektronikus adatfeldolgozó és adatátviteli rendszer védelmi-biztonsági megoldásainak kijátszására alkalmas program, belépési kód, jelszó vagy egyéb adat, amely a védett rendszerbe történő jogszerű belépést biztosítja.

Az elkövetési magatartásoknak öt esetét nevesíti a törvény, ezek: készítés, megszerzés, forgalomba hozatal, kereskedés, valamint hozzáférhetővé tétel. Készítés például a program írása, vagy jelszó generálása. Megszerzésről beszélünk a program, jelszó hordozójának birtokbavétele esetén, azonban közömbös, hogy ez milyen módon valósult meg (ingyenesen, visszterhesen). Forgalomba hozatalról beszélünk abban az esetben, ha az elkövető több személy számára hozzáférhetővé teszi a programot. Ez megvalósulhat úgy is, hogy saját maga juttatja el a programot a felhasználóknak, illetve úgy is, hogy csak egyetlen személynek adja át abban a tudatban, hogy az másoknak is továbbadja.

[355] Karsai 2019b: 989–996.

A kereskedés minden olyan tevékenység, amely elősegíti a program eljuttatását a készítőtől a felhasználóig, ez magában foglalja a forgalomba hozatalt, ám annál tágabb körű. Hozzáférhetővé tétel a program, jelszó, adat eljuttatása, akár aktív magatartással, akár mulasztással, például warezoldalon megosztással. A (1) bekezdés b) pontjában meghatározott elkövetési magatartás a 423. §-ban meghatározott bűncselekményhez kapcsolódó bűnsegédi tevékenység, rendelkezésre bocsájtás, amely azt jelenti, hogy az érintett személy a tényállásban foglalt ismeretek birtokába jut. A bűncselekmény alanya az a) pont szerinti esetekben bárki lehet, a b) pont szerinti esetben viszont csak az a személy, aki a megfelelő gazdasági, műszaki, szervezési ismeretekkel rendelkezik. A régi Btk. kommentárja szerint ez önmagában még nem jelent speciális alanyt, mert: „bizonyos műszaki, számítástechnikai, szakmai ismeretek nem minősülnek olyan személyes qualifikáltságnak, amelyek a delictum proprium fogalmát megalapoznák."[356] A bűncselekmény csak szándékosan követhető el, mindemellett célzatos, hiszen az elkövető célja a 423. §-ban meghatározott bűncselekmény elkövetése.

A (2) bekezdés büntethetőséget megszüntető okról rendelkezik, vagyis ha valaki cselekményét a hatóság tudomására hozza, lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását, az nem büntethető.

Információs rendszer felhasználásával elkövetett csalás

375. § (1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy

b) a nagyobb kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy

b) a jelentős kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

356 Nagykommentár a Büntető Törvénykönyvről szóló 1978. évi IV. törvényhez, Btk. 300/E. §-ához – WK jogtár.

(4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha
a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy
b) a különösen nagy kárt okozó információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.
(5) Az (1)-(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.
(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.

A harmadik, tisztán informatikai bűncselekmények között tárgyalt cselekmény az információs rendszer felhasználásával elkövetett csalás tényállása. A régi Btk. még számítógépes csalás néven és a számítástechnikai rendszer és adatok megsértésének bűntettével együtt szabályozta ezt a deliktumot. Az új Btk. szakított ezzel a szabályozási megoldással, és a vagyoni érdekeket sértő deliktumok között helyezte el az információs rendszer felhasználásával elkövetett csalást, figyelemmel annak „csalásszerűségére". Az információs rendszer felhasználásával elkövetett csalás valójában egy vegyes deliktum, megtalálhatók benne az információs rendszer megsértésének egyes elemei (az adatokon végzett jogosulatlan műveletek) és a csalás egyes elemei (a manipuláció haszonszerzési célja). A cselekményt a hagyományos csalástól az határolja el, hogy a tévedésbe ejtés, illetve a tévedésben tartás mozzanata hiányzik. A jogosulatlan adatmanipuláció valójában az információs rendszert „téveszti meg", csak közvetett módon azt a személyt, aki az abban található adatok hitelességében bízva, azok alapján téves következtetésre jut. Az internetes közvetítő szolgáltatók szerepét érintő vizsgálatunk szempontjából fontos az információs rendszer felhasználásával elkövetett csalás elhatárolása az online környezetben elkövetett hagyományos csalástól. Míg előbbi cselekmény jellemzően vállalatok, hivatalok belső működését, esetleg az információs társadalommal összefüggő szolgáltatást nyújtó webshopokat érint, utóbbi sértettjei jellemzően magánszemélyek, sűrűn fordul elő internetes közvetítő szolgáltatók igénybevételével (a társkeresős csalások esetében például közösségi oldalak segítik a cselekmény elkövetését). A két cselekmény elhatárolásakor döntő szempont az információs rendszer szerepe az elkövetésben. Előfordulhat az a helyzet, hogy a számítógépet pusztán a leplezés eszközéül használták fel, s ennek érdekében történt az adatmanipuláció, ebben az esetben a hagyományos csalással van dolgunk. A másik fontos elhatárolási ismérv: a számítógépes csalás esetében hiányzik a tévedésbe ejtés, hiszen az elkövetés

számítógépen zajlik, adatmanipulációval, a gépet pedig e minőségéből adódóan nem lehet megtéveszteni. „Míg a csalásnál a megtévesztés tárgya az emberi szellem, addig a számítógépes csalásnál az adatfeldolgozási folyamat."[357]

E minőségből következik az, hogy az információs rendszer, illetve az információs rendszerben tárolt adat a bűncselekménynek a tárgya, és nem az eszköze. Ebben tehát a cselekmény hasonlít a korábbiakban tárgyalt információs rendszer és adatok elleni bűncselekményekhez, ez a szempont alapozza meg azt, hogy ezeket a cselekményeket is a tisztán informatikai bűncselekmények körében tárgyaljuk. Ha tehát az elkövető cselekménye az információs rendszer megfelelő működésébe nem avatkozik be, azt nem akadályozza, az abban lévő adatokkal nem végez visszaélésszerű műveleteket, az információs rendszer nem tekinthető elkövetési tárgynak. A leírtak fényében ugyanakkor a cselekmény büntető törvénykönyvi elnevezése meglehetősen megtévesztő, hiszen a törvényi tényállás címéből az következik, hogy az információs rendszer csalási célú felhasználása büntetendő, erről azonban nincs szó. Az információs rendszer felhasználása ugyanis csak akkor eredményezi a bűncselekmény megvalósulását, ha a használat a rendszerben végzett jogszerűtlen műveletek (adatmanipuláció, adatbevitel, adattörlés) révén történik.

Hazai joggyakorlat

Nem valósít meg tehát információs rendszerrel kapcsolatos csalást az, aki hamis átutalási megbízásokat személyesen visz be a bankfiókba. Ebben az esetben az átutalásokat a banki ügyintézők teljesítették, az átutalási megbízásokkal tehát a terhelt őket tévesztette meg, „a banki információs rendszer integritása, szabályszerű működése nem sérült" (Fővárosi Ítélőtábla, Bf.12/2021/11). Szintén nem információs rendszerrel kapcsolatos csalás valósult meg abban az esetben, amikor a terheltek internetes hirdetési oldalakon (Vatera, Jófogás) más hirdetők fiókjait feltörve és azokba belépve nem létező műszaki cikkeket és használati tárgyakat hirdettek meg eladásra. A terheltek a termékeket nem küldték el, és a vételárat sem utalták vissza a vásárlóknak. Mivel ebben az esetben a terheltek nem az információs rendszert, hanem közvetlenül a potenciális vevőket tévesztették meg, ennélfogva a károsodás is náluk, és nem az adattulajdonosnál állt be, így nincs helye az információs rendszer felhasználásával elkövetett csalás megállapításának. E cselekmény minősítése információs rendszer megsértése halmazatban hagyományos csalással (Székesfehérvári Törvényszék, 31.B.18/2019/72).

357 Nagykommentár a Büntető Törvénykönyvről szóló 1978. évi IV. törvényhez, Btk. 300/E. §-ához – WK jogtár.

Szintén hagyományos csalást állapított meg a bíróság 2017-ben egy fuvarszervező bűnszervezet ügyében. A bűncselekmény elkövetési módszere az volt, hogy a bűnszervezet tagjai fővállalkozóként fuvarszervező cégek által az interneten közzétett szállítmányozási munkákra jelentkeztek. A bűnszervezet álal alapított cégek a cégnyilvántartásban legálisan működő cégként jelentek meg, azonban a fuvarozáshoz megfelelő fuvareszközzel nem rendelkeztek, szándékukban nem állt a fuvart ténylegesen teljesíteni. A bűnszervezet tagjai a megrendelőkkel – egyes esetekben a megbízott képviselőjeként álnéven, más esetben mint a fuvareszköz sofőrje – telefonon tartottak kapcsolatot, akiknek nem valós információkat szolgáltattak a szállítmányok szállítás közbeni pozíciójáról, illetve minden egyéb olyan információról, amely a megrendelőket érintette. Ugyan a vádlottak internetes honlapokon szervezték tevékenységüket, a cselekményük nem tekinthető információs rendszer felhasználásával elkövetett csalásnak, hiszen nem a rendszerbe vittek be valótlan adatot, hanem valós személyeket tévesztettek meg fiktív fuvarozási tevékenységre vállalkozással (Debreceni Ítélőtábla, Bf.597/2017/76).

Amennyiben a terhelt cselekményei a rendszer rendeltetésszerű használata körében megengedett műveletek (például banki átutalás kezdeményezése az internetbankból), de a bűncselekménynek minősülő ügylet lebonyolítására szolgálnak (például alkalmasak arra, hogy a bank ügyintézőjét megtévesszék), az információs rendszer a cselekmény eszközévé válik. Ezek a cselekmények másként, többnyire hagyományos csalásként minősülnek, ebben pedig a bírói gyakorlat is következetesnek mutatkozik.

Hazai joggyakorlat

Információs rendszer felhasználásával elkövetett csalást valósít meg például az, aki bér- és munkaügyi előadói munkakörét kihasználva magának utal át bizonyos összegeket, majd az átutalások adatait törli (B.687/2012/11).

Az EBH2009.2033. I. szerint számítástechnikai rendszer és adatok elleni bűncselekményt valósít meg a főiskola számítástechnikai hálózatának felügyeletét ellátó informatikus, aki a hallgatók vizsgakötelezettségét és vizsgaeredményeit nyilvántartó számítástechnikai rendszerben levő adatok jogosulatlan megváltoztatásával – a vizsgát előírás ellenére nem tett hallgatóval kapcsolatban – olyan adatokat rögzít a rendszerben, amelyek szerint a hallgató a meghatározott tantárgyból eredményes vizsgát tett.

Az elkövetési magatartás az a) pontban lehet az adatok bevitele, megváltoztatása, törlése vagy hozzáférhetetlenné tétele, a b) pontban pedig az előbbieken felül az adatok

továbbítása és egyéb műveletek végrehajtása is, amennyiben azok a rendszer működését akadályozzák. Ausgusztinyi Krisztina a számítógépes csalás elkövetési magatartásainak három fő csoportját különbözteti meg,[358] ezek:

1. jogosulatlan műveletekkel anyagi haszonszerzés,
2. távbeszélő-szolgáltatások hamis igénybevétele,
3. a rendszer üzemének megzavarása vagy adatok lopása.

Hazai joggyakorlat

Abban az ügyben, ahol a terheltek egy bank internetes felületén hajtottak végre csalárd műveleteket oly módon, hogy a sértett pénzét eltulajdonították, nem valósult meg információs rendszer felhasználásával elkövetett csalás, hiszen a terheltek a számlacsomagnak, valamint az internetbanki szerződésben foglaltaknak megfelelően jártak el, magát a rendszert rendeltetésszerűen vették igénybe (BH 2017.8.252: Kúria Bfv. III. 1.291/2016).

Abban az ügyben, amelyben a terhelt jogszerűtlenül jutott az átutalás lebonyolításához szükséges elektronikus aláíráshoz, szintén nem valósult meg információs rendszer felhasználásával elkövetett csalás, hiszen a cselekménye a programot, az adatfeldolgozást magát nem befolyásolta, a rendszer rendeltetésszerű működésébe nem avatkozott be, a rendszer által megengedett műveletet végzett. A gép felhasználásával elkövetett visszaélést így a bíróság nem minősítette tényállásszerűnek (Fővárosi Ítélőtábla, Bf.392/2016/113).

Természetesen ezek a fő csoportok még tovább tagolhatók, konkrétabb magatartásformák szerint. A jogosulatlan műveletekkel való anyagi haszonszerzés körébe tartozik például a hamis banki átutalás, kettős számlázás, ügyfelek bejelentkezésének lemásolása és ezzel visszaélés.

Távbeszélő-szolgáltatások hamis igénybevétele lehet a telefonvonal lopása, hamis iratokkal történő rádiótelefon-vásárlás, telefonok klónozása, telefonkártyák ismételt feltöltése. Ezeknek manapság már nincs akkora jelentősége, szinte egyáltalán nem jellemző a telefonkártyák ismételt feltöltése. Kiegészítésképp mindenképpen idesorolnám még a telefonok kártyafüggetlenítésére irányuló feltörését, valamint a telefonok operációs rendszerének oly módon történő manipulációját, ami lehetővé teszi, hogy a készülékre a hivatalos alkalmazásboltot megkerülve is telepíthetők legyenek alkalmazások (Apple készülékek esetében e technika elnevezése *jailbreak*).

[358] Ausgusztinyi 2008: 66–79.

Hazai joggyakorlat

Egy ügyben az I. r. terhelt mobiltelefonokat újsághirdetésen keresztül vásárolt, majd ezek kártyafüggőségét, a SIM-LOCK-ját (kártyazárat) a II. r. terhelttel egy erre alkalmas számítógépes program segítségével feloldatta, s ezáltal a készülékek mind a Pannon GSM, mind a Westel szolgáltató cég kártyájával üzemeltethetők lettek. Az I. r. terhelt az általa megvásárolt kártyafüggő mobiltelefonokat azért alakította át kártyafüggetlenné, hogy azokat a kártyafüggő telefonoknál magasabb áron értékesítse, ezáltal tényleges haszonra tett szert. A kár ebben az esetben a telefontársaságot érte, mert a SIM-kártya manipulációja folytán a másik szolgáltató hálózatában annak szolgáltatásait a szerződési feltételeket megszegve úgy vették igénybe, hogy a szolgáltatás igénybevételének ellenértékét nem fizették meg.

A rendszer üzemének megzavarása főleg adatlopással, vírusok készítésével, terjesztésével, a számítógépes program megváltoztatásával valósul meg.

Az információs rendszer felhasználásával elkövetett csalás eredmény-bűncselekmény, ami azt jelenti, hogy a tényállásszerűséghez szükséges, hogy az adatmanipuláció következtében kár keletkezzen. Az elkövető oldalán a jogtalan haszon elérése a cél, ennek érdekében történik a megtévesztő magatartás tanúsítása, amely a sértett oldalán vagyoni kárt idéz elő. Az viszont már nem feltétel, hogy az elkövető hozzá is jusson a megszerezni kívánt haszonhoz, ahogyan az sem, hogy a haszon az elkövető oldalán realizálódjon.

Hazai joggyakorlat

A haszon kérdésével foglalkozott a Fővárosi Ítélőtábla a Bf.204/2015/13 ügyben. A tényállás szerint a banki hitelügyintézés szabályos menete az, hogy a hitelkérelmi lapról rögzítik a bank informatikai rendszerében a releváns adatokat, majd a fiókigazgató a hitelt engedélyezi. Ezt az engedélyt követi a hitelszerződés megkötése, a közjegyzői okirat készítése és az utalványozás. A terhelt annak ellenére, hogy tisztában volt a szabályos ügymenettel, a fiókvezetőt megkerülve, annak tudta nélkül, a rendszerben az adatok felvitelét követően engedélyezte a hitelek nyújtását, illetve kollégája kódjával utalványozta a hiteleket. A haszon ebben az esetben nem az elkövető oldalán jelentkezett, a jogtalan előnyszerzés azonban bekövetkezett, így az információs rendszer felhasználásával elkövetett csalás is megállapítható.

Hasonló eset megvalósult üzleti hitelkártya-igénylések ügyében is. Az ügy alapját a hitelkártya-kiadás képezte, amelyben az ügymenet első lépése a hitelbírálat volt. Erre a bank egy úgynevezett *scoring*alapú hitelminősítő rendszert alkalmazott, amely automatizáltan, kockázati

szempontból értékelte az igényléseket. Amennyiben az értékelés nem felelt meg a pénzintézet által meghatározott követelményeknek, úgy a hitelkérelmet el kellett utasítani, a terhelt azonban olyan valótlan gazdálkodási adatokat rögzített, amelyek a hiteligénylők vagyoni helyzetét a ténylegesnél jobbnak tüntették fel, ily módon azt a látszatot keltette, hogy azok hitelképesek. Ebben az ügyben azonban a terhelt az általa ily módon kötött hitelszerződések után jutalékban is részesült, tehát közvetett haszonszerző volt (Pécsi Ítélőtábla, Bf.31/2016/15).

Az EBH2005.419 kimondja, hogy a számítógépes csalás bűntettének alapeseténél a törvény nem állapít meg értékhatárt, így az bármilyen csekély mértékű kár okozása esetén megállapítható. A cselekmény tehát akár 1 forintos kár okozása esetében is megvalósul, az összegeknek legfeljebb a bűncselekmény minősítése kapcsán van jelentőségük, hiszen a minősített esetek, így a kiszabható szankció mértéke már a kár összegéhez igazodik.

A jogsértés alanya bárki lehet, a szakismeret és a tudás szinte közömbös. „A bűncselekmény csak szándékosan valósítható meg, azaz az elkövetőnek tisztában kell lennie azzal, hogy védett elektronikus adatfeldolgozási és átviteli folyamat titkosságát töri meg", illetve „az adatfeldolgozás céljára rendelt adatokat rongálja meg, a számítógépes rendszer működését akadályozza és ez számára kívánatos, ebbe belenyugszik".[359]

A 375. § (5) bekezdésével a jogalkotó az elektronikus készpénz-helyettesítő fizetési eszközökkel való visszaéléseket is információs rendszer felhasználásával elkövetett csalásként rendeli büntetni. Az e bekezdésben leírt tényállás jellemzői teljesen megyeznek az (1) bekezdésben leírtakkal, az elhatárolási szempont az elkövetési tárgy, amely ez esetben az elektronikus készpénz-helyettesítő fizetési eszköz. Ambrus István felhívja a figyelmet arra,[360] hogy e cselekmények szükségszerű eszközcselekménye a Btk. 393. § (1) bekezdésében szabályozott készpénz-helyettesítő eszköz megszerzése, vagy a készpénz-helyettesítő fizetési eszköz egyidejű elvételével elkövetett lopás [Btk. 370. § (1) b) pont be) alpont]. E két cselekmény anyagi halmazata az elektronikus készpénz-helyettesítő fizetési eszközök felhasználásával elkövetett csalással ennélfogva látszólagos. A bírósági gyakorlatból határozottan kitűnik, hogy ezek az informatikai bűncselekmények leggyakrabban előforduló esetei, hiszen az elkövetési lehetőségek nagyon széles skálán mozognak. Egy pénztárca ellopásánál szinte egészen biztos, hogy bankkártya is kerül a terhelthez, de rablás, kifosztás során sem elképzelhetetlen, hogy bankkártyák is vannak a „zsákmányban". Mivel kötetünk az online világban

[359] Nagy 2009: 288.
[360] Ambrus 2021: 90.

elkövetett jogsértésekre fókuszál, ezen a ponton mindenképpen hangsúlyozni kell, hogy a készépnz-helyettesítő eszköz fizikai jelenléte nem szükségszerű eleme a bűncselekmény megvalósulásának. A cselekmény megvalósításához elegendő, ha pusztán azokat a bankkártyaadatokat ismeri meg az elkövető, amelyekkel a visszaélés megvalósítható.

Hazai joggyakorlat

Egy 2021-es ügyben a terhelt ruházati márkabolt üzletvezetője volt, ő volt jogosult az ügyfelek által kezdeményezett bankkártya útján történő fizetések lebonyolítására az üzletben elhelyezett terminálon keresztül. Az üzlet és a terminált üzemeltető cég írásban úgy állapodtak meg, hogy kivételes esetben akár a bankkártya fizikai jelenléte nélkül, úgynevezett manuális tranzakcióval is volt lehetőség fizetésre. Ebben az esetben a bankkártyát a terminálon nem húzták le, hanem annak adatait kézzel vitték be a terminálba, amelyről bizonylatot állítottak ki. A terhelt a vásárlóktól és más forrásokból megszerzett bankkártyaadatokat arra használta, hogy visszaélésszerű fizetéseket kezdeményezzen, ezáltal valósítva meg az információs rendszer felhasználásával elkövetett csalást (Kúria, Bfv.744/2021/20).

Szintén információs rendszer felhasználásával elkövetett csalást valósított meg az a terhelt, aki egy általa létrehozott internetes honlapon virtuális kártya-elfogadóhelyet kívánt létesíteni. A honlapon 10, 20, és 50 euró összegű csomagokban forgalmazott internetes telefonszolgáltatásokat, amelyeket az ügyfelek bank-, illetve hitelkártyával is kiegyenlíthettek. A terhelt a honlap bank által történt jóváhagyását és a fizetési rendszer „élesítését" követően, a bank által elfogadott csomagok értékét jelentősen megemelve, az általa üzemeltetett honlapon 500-1000-2000-3000-4000-5000 euró összegű csomagokat hozott létre annak érdekében, hogy ismeretlen társai, a rendelkezésükre álló kártyaadatok jogosulatlan felhasználása révén minél rövidebb idő alatt, minél nagyobb összegű vásárlást tudjanak végrehajtani (Fővárosi Ítélőtábla, Bf.492/2013/19).

Ezeknek a cselekményeknek külön nevük is van: *card-not-present* csalás. A kártyaadatokkal (kártyaszám, CVC-kód stb.) való visszaélések tehát információs rendszer felhasználásával elkövetett csalásnak minősülnek.[361]

Bank- és hitelkártyaadatok megszerzésére számos lehetőség van. A fizikai térben ilyen lehetőség a bankkártya klónozása, illetve az úgynevezett *skimming,* amely során az ATM-be szerelnek olyan eszközt, amely rögzíti a bevitt kártyaadatokat és a beütött PIN-kódot. Az online térben a kártyaadatok gyűjtése nagyrészt adathalász-tartalmú e-mailek és weblapok felhasználásával valósul meg, a bűnelkövetők pedig a sötét

[361] Kondorosi 2014: 73–75.

weben akár vásárolhatnak is a jogszerűtlen módon megszerzett bankkártyaadatokból. Mind a fizikai, mind a virtuális visszaélésekre találunk példát a magyar bíróságok gyakorlatában is.

Hazai joggyakorlat

A *skimming* tipikus esete valósult meg 2016-ban, amikor az elkövetők leplezett technikai adatszerző egységet szereltek fel bankautomatákhoz (a bankfióki kapun vagy a készüléken elhelyezett kártyaolvasóra), amely képes megjegyezni a használt bankkártya egyedi adatait, továbbá egy mikrokamerát telepítettek a PIN-pad fölé, amely rögzíti a beütött biztonsági kódokat. Az elkövetők az adatokkal és kódokkal hamis bankkártyákat készítettek, s azokkal a banki ATM-ekből készpénzt kíséreltek meg felvenni. A készpénzfelvételhez további személyeket szerveztek be, a hamis bankkártyák felhasználása, a készpénzfelvétel volt a feladatuk (úgynevezett „casherek", avagy „lehúzók") (Fővárosi Ítélőtábla, Bf.136/2020/47).

Telefonos adathalászat valósult meg 2013-ban, amikor a terhelt magát internetes oldalak munkatársának adta ki, és az általa felhívott személyekkel közölte, hogy egy nyereményjáték keretében meghatározott összeget nyertek. A terhelt arról tájékoztatta a sértetteket, hogy a nyereményt majd átutalással kapják meg, amihez azonban meg kell adniuk bizonyos adatokat, így a bankkártyájuk számát, lejárati dátumát, CVC-kódját. Ezen adatok birtokában a sértettek bankkártyájának felhasználásával különböző internetes vásárlásokat tudott végrehajtani figyelemmel arra, hogy az internetes vásárlásokhoz a bankkártya fizikai jelenléte, valamint a hozzá tartozó PIN-kód ismerete nem volt szükséges (Kúria, Bfv.219/2020/10).

Az információs rendszerrel kapcsolatos bűncselekmények

Az informatikai bűncselekmények másik nagy kategóriája esetében az információs rendszerrel való kapcsolat már jóval lazább, mint a bűncselekmények előző csoportjában, ezekben az esetekben az információs rendszer jellemzően eszköze az elkövetésnek, megkönnyíti annak realizálását. „Közös jogi tárgy már elvontan nem határozható meg. A jogi tárgyat és a sértettek körét azon bűncselekmények határozzák meg, amelyek elkövetéséhez felhasználták a számítógépet" – írja Siegler Eszter.[362] Ezek a bűncselekmények elszórtan találhatók meg a Btk.-ban, a szabadság és az emberi méltóság elleni, nemi erkölcs elleni, a gazdaság, illetve vagyon elleni bűncselekmények

[362] Siegler 1997: 736.

között. Manapság már a legtöbb ember rendelkezik otthon számítógéppel és internetkapcsolattal. A világháló lehetőséget nyújt a másokkal való kapcsolattartásra, különféle tartalmak böngészésére és akár vásárlásra is, ugyanakkor van árnyoldala is: az átlagemberek számára is lehetőséget ad a különféle bűncselekmények elkövetésére. Mivel a számítógép felhasználói szintű kezelése külön szakértelmet nem igényel, ezeket a bűncselekményeket bárki elkövetheti, ellentétben például a speciális szakismereteket igénylő hackertámadásokkal. Sőt, az emberek gyakran tudatában sincsenek annak, hogy jogsértést követnek el például azáltal, hogy letöltik kedvenc filmjeiket, zenéiket, vagy másokat sértő állításokat tesznek egyes közösségimédia-platformokon. E fejezet tehát igen tág bűncselekményi kört fed le, itt mutatom be a számítógéppel kapcsolatos csalást és hamisítást, a személyes és közérdekű adattal visszaélést, valamint itt tárgyalom a tartalomhoz kapcsolódó és a szerzői jog megsértésével kapcsolatos bűncselekményeket is.

„Hagyományos" csalás

Ahogyan arra már korábban felhívtam a figyelmet, az online térben elkövetett „hagyományos" csalás nem azonos a Btk. 375. szakaszában megjelenő információs rendszer felhasználásával elkövetett csalással, az ilyen cselekményekre ugyanis a csalás Btk. 373. §-ban megjelenő rendelkezései irányadóak:

> 373. § (1) Aki jogtalan haszonszerzés végett mást tévedésbe ejt, vagy tévedésben tart, és ezzel kárt okoz, csalást követ el.
> (2) A büntetés vétség miatt két évig terjedő szabadságvesztés, ha
> a) a csalás kisebb kárt okoz, vagy
> b) a szabálysértési értékhatárt meg nem haladó kárt okozó csalást
> ba) bűnszövetségben,
> bb) közveszély színhelyén,
> bc) üzletszerűen,
> bd) jótékony célú adománygyűjtést színlelve
> követik el.
> (3) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha
> a) a csalás nagyobb kárt okoz, vagy
> b) a kisebb kárt okozó csalást a (2) bekezdés ba)-bc) pontjában meghatározott valamely módon követik el.

(4) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha
a) a csalás jelentős kárt okoz,
b) a nagyobb kárt okozó csalást a (2) bekezdés ba)-bc) pontjában meghatározott valamely módon követik el, vagy
c) a csalást a bűncselekmény felismerésére vagy elhárítására idős koránál vagy fogyatékosságánál fogva korlátozottan képes személy sérelmére követik el.
(5) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha
a) a csalás különösen nagy kárt okoz, vagy
b) a jelentős kárt okozó csalást a (2) bekezdés ba)-bc) pontjában meghatározott valamely módon követik el.
(6) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha
a) a csalás különösen jelentős kárt okoz, vagy
b) a különösen nagy kárt okozó csalást a (2) bekezdés ba)-bc) pontjában meghatározott valamely módon követik el.
(7) E § alkalmazása szempontjából kárnak kell tekinteni az igénybe vett szolgáltatás meg nem fizetett ellenértékét is.

A bűncselekmény elkövetési magatartását itt tágabban határozza meg a jogalkotó: tévedésbe ejtés. A hagyományos csalás számítógépes környezetben főleg a gyanútlan internetezők megtévesztése céljából történik. Tartalmában tehát ez a cselekmény nem különbözik az offline megvalósuló csalásoktól, specialitása mindössze annyi, hogy az elkövetés helyszíne a virtuális térbe tevődött át.

A szakirodalom a számítógéppel elkövetett csalás több fajtáját ismeri, ugyanakkor a cselekmény rendkívül változatos megvalósulási formái miatt kategorizálásuk nehézkes, több átfedéssel az egyes elemek között. Külföldi munkákban találkozhatunk ugyan különféle kategóriákkal, ezek azonban többnyire kriminológiai szempontú tipológiák, és nem a magyar büntető anyagi jog szabályrendszerét követik. Ezek a tipológiák többnyire a csalás ernyőfogalma alá vonják az összes olyan magatartást, amelynek központi eleme a megtévesztés révén történő, azaz csalárd haszonszerzés. Az ezekben a tipológiákban felsorolt csalásszerű magatartások a magyar Btk. több tényállását is lefedik, így csalásként jelenik meg bennük a pénzmosás, a készpénzhelyettesítő eszközökkel való visszaélés, a költségvetési csalás, a jóléti juttatásokkal kapcsolatos visszaélések (a köznyelvben adócsalás), EU-s pénzekkel való visszaélések, a fogyasztó jogait csorbító egyes visszaélések (például a versenytárs termékének csalárd utánzása, megtévesztő információ nyújtása). Michael Levi a sértettek szempontjából rendszerezi az információtechnológiai eszközökkel megvalósított csalárd

magatartásokat.[363] Eszerint a csalások sértettjei lehetnek magánszemélyek – köztük pénzügyi intézmények, nem pénzügyi szolgáltatást nyújtó jogi személyek, valamint természetes személyek –, továbbá közjogi jogalanyok – így országos szervek, helyi szervek, valamint nemzetközi szervezetek. A jogi személyekkel kapcsolatos csalások közé sorolja a csekkekkel kapcsolatos csalásokat, a hamisított termékek adásvételét, a pénzhamisítást, az adatmanipulációval elkövetett csalást, a biztosítási és a hitelezési csalást, a bankkártyacsalást, valamint a beszerzésekkel kapcsolatos csalárd magatartásokat. A természetes személyek sérelmére elkövethető csalástípusok Levi felosztásában az alábbiak:

- csalárd adománygyűjtés *(charity fraud),*
- értékesítési csalások *(scam),*
- hamis vagy hamisított termékek adásvétele,
- befektetési csalás,
- nyugdíj- vagy más járulékkal kapcsolatos csalás.

E lista kiegészíthető még a napjainkban igen népszerű társkeresőket kihasználó csalásokkal *(catfishing),* valamint a családi vészhelyzeteken nyerészkedő csalásokkal *(family emergency scam).* Magánszemélyként, az online térben mozogva többnyire az előbbiekben felsorolt cselekményekkel találkozhatunk, ezért úgy tűnik helyesnek, ha ezekről a cselekményekről bővebben is szólunk, néhány valóban megtörtént eset bemutatásával színesítve a leírtakat.

A leggyakrabban előforduló és talán a legváltozatosabb elkövetési magatartásokkal megvalósítható cselekmények az online értékesítési csalások, másnéven a *scam*ek. Ebbe a kategóriába sorolhatunk minden termékértékesítéssel vagy szolgáltatásnyújtással összefüggő magatartást, úgymint:

- szerencsejátékokkal kapcsolatos csalások *(gambling scam),*
- online aukciós csalások *(auction scam),*
- előfizetéses csalások *(subscription trap),*
- jegyértékesítési csalások *(ticketing scam).*

Nemcsak az online piacterek üzemeltetőinek, hanem az internet más közvetítő szolgáltatóinak a szerepe is növekszik az elektronikus kereskedelemben. A Facebooknak már van saját piactérfunkciója, ahol a felhasználók egymással kereskedhetnek, de az Instagramon is el lehet látni ármatricával a feltöltött képeket. Nagy Zoltán András

[363] Levi 2008: 391.

felhívja a figyelmet arra, hogy az online szolgáltatások, mint a Twitter vagy a Messenger, megkönnyítette a fogyasztók közötti (C2C) és a vállalatok és a fogyasztók közötti (B2C) kereskedelmet. Ezek a kereskedelmet elősegítő szolgáltatások alapvetően a decentralizált áru- és szolgáltatásforgalom számára biztosítanak keretet, az azokon belül zajló kereskedelem viszont ellenőrizetlenül zajlik, ami megnehezíti a fellépést.

A szerencsejátékokkal kapcsolatos csalásoknál a sértett behálózása gyakran történik böngészőben felugró ablakon keresztül. A böngészés közben a felugró ablakban megjelenik egy üzenet, amely arról tájékoztatja a potenciális áldozatot, hogy nagy értékű műszaki cikket, utazást nyert egy sorsoláson, amelyet bankkártyaadatok és más személyes adatok megadását követően tud átvenni. Természetesen a sértettek soha nem jutnak hozzá a nyereményükhöz. Nagy Zoltán kiemeli még a napjainkban népszerű, hasonló elkövetési sémájú holland lottót.[364] Ez esetben a felhasználó arról kap értesítést, hogy nyert a lottón, a nyereményét pedig nyereményadó befizetése után kapja meg. Ezek a csalástípusok gyakran fordulnak elő a közösségi médiával összefüggésben is. 2018-ban a Facebook-lottó csalássorozat segítségével több százezer dollárt szereztek bűnelkövetők, akik Mark Zuckerberg nevében kerestek meg embereket azzal a hírrel, hogy nagyobb összeget nyertek a Facebook-lottón.[365] A *New York Times* 2018-ban összesen 205 olyan Facebook-profilt talált, amely a Facebook vezérigazgatóját, Mark Zuckerberget személyesítette meg.[366]

Az értékesítési csalások között tartjuk nyilván az online aukciós csalásokat is.

Az aukciós csalás során számos megtévesztő magatartással idézhető elő kár. Az egyik legsűrűbben előforduló eset, amikor a vételár kifizetését követően az eladó eltűnik anélkül, hogy teljesített volna. Sűrűn előfordul az is, amikor a vevő rossz minőségű árut kap kézhez, illetve nem azt kapja, amit rendelt, esetleg hamis terméket postáznak a részére. Az online aukciós csalások további formája az, amikor egy beépített ismerős *(shill)* felsrófolja a vételárat, hogy a gyanútlan licitálók egy adott termékért a valós vételár többszörösét fizessék ki. „A shillek olyan ajánlattevők, akiknek nem áll érdekében az áru megvétele, amelyre ajánlatot tesznek, viszont azzal, hogy ajánlatot tesznek, emelik a termék tényleges eladási árát. Az online aukciókon az elkövetők hamis e-mail-címekről és hamis azonosítókról helyeznek el hamis ajánlatokat."[367]

Ebbe a bűncselekményi körbe tartoznak még az online kiskereskedelmi közvetett értékesítési csalások.

364 Nagy 2019: 154.
365 Nicas 2018.
366 Nicas 2018.
367 Szabó 2003: 301–324.

„A leggyakoribb módszer, hogy hivatalos aukciós oldalakra feltett hirdetésekkel az aukciós oldal tagját olyan oldalra irányítja egy linkkel tovább, amelyek már nem állnak a kiinduló aukciós oldal felügyelete alatt, így annak védelmi rendszerének felügyelete alatt sem. A másik módszer hasonló: a leendő áldozatoknak spamet küldenek, amelyben olyan weboldalra csalogatják a leendő áldozatokat, melyek hasonló termékeket kínálnak, mint az ismert aukciós oldalak."[368]

Hazai joggyakorlat

Az információs rendszer megsértése halmazatban a csalással fordult elő akkor, amikor a terheltek internetes hirdetési oldalakon (Vatera, Jófogás) más hirdetők fiókjait feltörve és azokba belépve nem létező műszaki cikkeket és használati tárgyakat hirdettek meg eladásra. A terheltek a termékeket nem küldték el, és a vételárat sem utalták vissza a vásárlóknak. Mivel ebben az esetben a terheltek nem az információs rendszert, hanem közvetlenül a potenciális vevőket tévesztették meg, ennélfogva a károsodás is náluk, és nem az adattulajdonosnál állt be, így nincs helye az információs rendszer felhasználásával elkövetett csalás megállapításának (Székesfehérvári Törvényszék, 31.B.18/2019/72).

Az előfizetéses csalás lényege annyi, hogy az elkövető a világhálón valamilyen szolgáltatást népszerűsít, és e szolgáltatásért cserébe rendszerint előre pénzt kér. Ezt természetesen fizetés esetén sem követi teljesítés, az elkövető a hozzá eljuttatott összeggel egyszerűen eltűnik.

Sűrűn fordulnak elő jegyértékesítési csalások *(ticketing scams)*. *Modus operandi*jukat tekintve ezek nem különböznek nagymértékben egy átlagos aukciós csalástól, jellegzetességük viszont, hogy a károsultak gyakran csak hosszabb idő elteltével jönnek rá arra, hogy átverték őket. E csalástípusnak az alapja, hogy az elkövetők különféle rendezvényekre (tipikusan koncertekre, fesztiválokra) kínálnak jegyeket, amelyekről kiderül, hogy érvénytelen jegyek, többször értékesítették ugyanazt a jegyet, de arra is van példa, hogy a rendezvény, amelyre belépőt kínálnak, még csak nem is létezik. A jegyeket magánszemélyek közösségi oldalakon is értékesíthetik, de vannak külön erre a célra létrejött jegyaggregáló oldalak, például a Viagogo.

368 Nagy 2009: 150.

Hazai joggyakorlat

Az egyik nagyobb másodlagos jegyértékesítő platform, a Viagogo ellen Magyarországon 2019-ben versenyfelügyeleti eljárás indult, amelynek eredményeként 2021-ben a GVH 472 milliós versenyfelügyeleti bírságot szabott ki. A fogyasztók az oldal ellen jellemzően amiatt tettek panaszt, hogy a weboldal nem tette egyértelművé, hogy a Viagogo csak közvetítő szerepet tölt be az értékesítésben (vagyis a jegyet valójában nem ő értékesíti), továbbá hogy sürgető üzenetekkel pszichés nyomás alá helyezte a felhasználókat. E platform ügyében büntetőeljárás is indult, de a magyar rendőrség 53 nyomozás megindítását követően végül csak egy esetben tett vádemelési javaslatot. Az *Index* hírportál értesülései szerint ennek hátterében sok esetben az állt, hogy az elkövető kiléte nem volt megállapítható (Kovács 2018).

Az online értékesítési csalások között tartja nyilván a szakirodalom a hamis, illetve hamisított termékek adásvételét, amely különösen olyan márkás termékek esetében fordul elő, amelyeket Kínában vagy más ázsiai országban hamisítanak. A felhasználó általában a valós piaci árhoz képest sokkal kedvezőbben juthat használt vagy új fogyasztási cikkekhez, amelyekről gyakran kiderül, hogy nem eredetiek. Néhány esetben ugyan feltűnik, hogy rossz minőségű replikáról van szó, más esetekben azonban a felhasználó részére küldött termék könnyen összetéveszthető a márka valós termékeivel. Ezeknek a csalástípusoknak a száma rendkívül megnőtt a Covid-19-világjárvány alatt, főként egészségügyi termékek vonatkozásában. Az interneten gombamód szaporodtak el a „covidbiztos" védőmaszkot, fertőzést megelőző gyógyszereket kínáló weboldalak és hirdetések.

Ki kell azonban emelni, hogy a magyar anyagi jog rendszerében ezek a magatartások nem csalásnak, hanem a Btk 417. §-ában szabályozott fogyasztók megtévesztése vétségének minősülnek. E tényállás központi eleme szintén a megtévesztés, az elkövető azonban egy áru értékesítője, aki az áru lényeges tulajdonsága tekintetében valótlan tényt állít.

Csalárd adománygyűjtésről beszélhetünk, ha az elkövetők jótékonysági célokra, nem létező alapítványok, szervezetek javára kérnek pénzt. Egyik legismertebb példája a „nigériai levelek" ügye. Számos gyanútlan felhasználó kapott olyan tartalmú e-mailt, amelyben egy magas rangú nigériai hivatalnok hozzátartozója kér segítséget, azt állítva, hogy apja halála után a családi vagyont zárolták, neki pedig nincs annyi pénze, hogy kifizesse azt a díjat, amellyel ezt a vagyont vissza tudná szerezni. Ezek után megadott egy nigériai bankszámlaszámot, és azt ígérte, mindenkit, aki őt támogatta, jelentős pénzösszeghez juttat.

Népszerűek manapság a romantikus csalások *(catfishing),* amelyek során az elkövető hamis személyazonosságot épít fel egy közösségi platformon azért, hogy kapcsolatot építsen valós személyekkel, akiktől aztán pénzt kér. Ezek általában kisebb összegek (például mobil-feltöltőkártya vásárlása, hogy a magát hősszerelmesnek kiadó elkövető tudjon csatlakozni az internetre), később azonban jelentősebb összegek is kicsalhatók a magányos sértettől. A Tinder nevű társkereső platformon 2021 elején lepleztek le[369] egy hálózatot, amelynek a tagjai magukat modelleknek, üzletasszonyoknak kiadva csábították befektetésre a sértetteket. A cselekmények áldozatainak kriptovalután alapuló befektetési lehetőséget ajánlottak, és a befektetés értékének nyomon követésére még egy külön weboldalt is létrehoztak.

Hazai joggyakorlat

A magyar ügyészség gyakorlatában 2020 és 2023 között több dokumentált esete volt az online társkeresős csalásoknak. Újszerű jellegük miatt jogerőssé vált bírósági ítéletek még nem jelentek meg a bírósági határozatok tárában a kötet lezárásáig. Kétmillió forint kárt okozott például az a kiskunfélegyházi férfi, akit magát jól menő vállalkozónak adva ki, társkereső felületeken személyes adatokat csalt ki áldozatától. E személyes adatokat felhasználva a terhelt nagy értékű ingóságokat vásárolt, és a nőhöz költözött, akitől a nála töltött időszak alatt folyamatosan kölcsönkért (2 millió forintot csalt ki a társkereső oldalon megismert nőtől – a Bács-Kiskun Megyei Főügyészség sajtóközleménye 2021).

Volt olyan terhelt, aki arra is rá tudta venni a társkereső oldalon megismert sértettek egyikét, hogy az a saját családi házát eladja, azzal hitegetve, hogy az összeget közös családi házra fordíthatják (Társkereső oldalakon megismert nőket csapott be egy férfi – a Komárom-Esztergom Vármegyei Főügyészség sajtóközleménye 2023).

Gyakran fordul elő olyan eset is, hogy betegségre hivatkozva, a gyógyszerek és a gyógykezelés finanszírozására kérnek kölcsön társkereső oldalakon keresztül.

Léteznek családi vészhelyzettel összefüggő csalások *(family emergency scam),* amikor bűnelkövetők találomra kiválasztott embereket keresnek meg azzal, hogy az egyik családtagjukat baleset érte, balesetet okozott, vagy más okból anyagi segítségre van szüksége. Magyarországon hasonló jellegű, de főként telefon segítségével elkövetett

369 Tinderen csábította el magyar áldozatát a bitcoincsaló 2021.

cselekmények az úgynevezett „unokázós csalások”,[370] amikor idős embereket keresnek meg azzal, hogy unokájuknak sürgős anyagi segítségre van szüksége.

A közvetítő szolgáltatók között különösen a közösségimédia-platformok, illetve az online aukciós platformok vannak kiemelt helyzetben ahhoz, hogy észleljék és eltávolítsák a jogsértéseket. Ahogy az előbbi esetek is mutatják, egy-egy platformszolgáltató sokszor olyan közeget biztosít a felhasználók számára, amelyben a csalók közvetlenül felvehetik a kapcsolatot a potenciális sértettekkel, termékeiket hirdethetik, illetve kereskedelmi tevékenységüket bonyolíthatják. Több szolgáltató is akad, amelyik felhasználási feltételeiben tilt bizonyos magatartásfajtákat annak érdekében, hogy elejét vegye a hasonló jogsértéseknek.

Csalások az online platformokon

A Meta közösségi alapelvei kimerítő felsorolásban írják le, hogy melyek azok a csalárd magatartások, amelyek tiltottak a Facebookon és az Instagramon. A platformokon más személy vagy szervezet kárára vagyoni vagy személyes előny megszerzése érdekében az alábbi tevékenységeket tilos folytatni:

- befektetési és pénzügyi csalások, különösen kölcsönnel, előlegfizetéssel, szerencsejátékkal kapcsolatos csalások, ponzi, piramisjáték és befektetési csalás;
- személyazonossággal összefüggő csalások, különösen a csalárd adománygyűjtés, romantikus csalás, nem létező vállalkozással elkövetett csalás;
- termékekkel, nyereményekkel kapcsolatos csalások, különösen támogatásokkal, juttatásokkal megvalósított csalások, spirituális csalások, biztosítási csalások;
- nem létező állásokkal, gyors jövedelemszerzéssel kecsegtető megtévesztések;
- adósságelengedéssel, hitelképesség-javítással kecsegtető megtévesztések.

A Facebook a csalásról és megtévesztésről szóló közösségi alapelvek között egy sor olyan magatartásról is szól, amelyek a magyar Btk. dogmatikai rendszerében csalárd jellegűek, de külön tényállásban helyezkednek el. A közösségi alapelvek ezen szabályairól a későbbiekben esik majd szó.

A Facebook a visszaélések megelőzése érdekében néhány olyan termékcsoport adásvételét is tiltja, amelyek egyébként legális áruknak minősülnek, könnyű azonban visszaélni velük. Korlátozottan lehet a platformon rendezvényekre (például koncertekre) szóló jegyeket és ajándékutalványokat, ajándékkártyákat árulni, hiszen a jegyüzérek nagyon könnyen hamisíthatják

370 Tolna Vármegyei Rendőr-főkapitányság 2015.

a jegyeket, aminek ténye a rendezvény időpontjáig pedig nem is feltétlenül derül ki. Az árukkal kapcsolatos visszaélések megelőzése érdekében a Facebook közösségi alapelvei jó néhány korlátozást tartalmaznak. Az illegális áruk és szolgáltatások kereskedelmét tiltja a platform, nem lehet tehát hamis pénzt, hamis vagy hamisított dokumentumokat (orvosi vényeket, diplomákat, okleveleket) eladásra kínálni.

A YouTube közösségi irányelvei a spam és megtévesztő gyakorlatok címszó alatt szólnak a csalás jellegű tevékenységekről. A közösségi irányelvek ebben a körben tiltják az olyan külső weboldalra mutató tartalmak elhelyezését a platformon, amelyek célja kártékony szoftverek terjesztése, félrevezető ígéreteken keresztül a felhasználók más oldalakra irányítása. A platform tiltja továbbá az olyan csalárd tartalmak elhelyezését, amelyek gyors pénzszerzési lehetőségeket, nagy értékű ajándékokat kínálnak valótlanul, illetve a piramisjáték jellegű tevékenységek folytatását. Tilos továbbá a megtekintések, követők, lájkok, illetve a csatornák forgalmát növelő botok eladásra kínálása.

Az X (korábbi Twitter) felhasználási feltételei igen szűkszavúan szólnak a platform által tiltott magatartásokról. Szabályzatukban például a csalás meg sem jelenik, a csalárd technikák közül egyedül a spamek terjesztésével, valamint a forgalmat generáló botok tilalmával foglalkoznak részletesebben. Ezek azonban, bár gazdasági szempontból etikátlan technikáknak minősülnek, büntetőjogi felelősséget nem vonnak maguk után.

A pénz- és bélyegforgalom biztonsága elleni bűncselekmények

Az informatikai bűncselekmények tipizálásának teljessége kedvéért röviden szólni kell a pénz- és bélyegforgalom biztonsága elleni bűncselekményekről, hiszen az elkövetés módszerei szinte minden esetben valamilyen információtechnológiai eszköz használatát feltételezik. Ezeket a cselekményeket nem tárgyalom részletekbe menően, mivel ha szerepel is internetes közvetítő szolgáltató a folyamatban, annyira speciális deliktumok, hogy külön kötetet lehetne szentelni vizsgálatuknak. Az előzőekben már arról is esett szó, hogy a pénzügyi közvetítő szolgáltatók az EU jogrendszerében is speciálisnak minősülnek, ezért az információs társadalommal összefüggő szolgáltatások között különös szabályok vonatkoznak rájuk. E cselekmények sértettjei ráadásul jellemzően nem magánszemélyek, így nem illeszkednek szorosan a kötet szerkezetébe.

A Btk. a pénz- és bélyegforgalom biztonsága elleni bűncselekmények között az alábbi deliktumokat szabályozza: pénzhamisítás, pénzhamisítás elősegítése, bélyeghamisítás, készpénz-helyettesítő fizetési eszköz hamisítása, készpénz-helyettesítő eszközzel visszaélés, készpénz-helyettesítő fizetési eszköz hamisításának elősegítése. Az alábbiakban ezeket a cselekményeket tekintem át.

Pénzhamisítás

389. § (1) Aki
a) pénzt forgalomba hozatal céljából utánoz vagy meghamisít,
b) hamis vagy meghamisított pénzt forgalomba hozatal céljából megszerez, az ország területére behoz, onnan kivisz, azon átszállít,
c) hamis vagy meghamisított pénzt forgalomba hoz,
bűntett miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés öt évtől tizenöt évig terjedő szabadságvesztés, ha a pénzhamisítást
a) különösen nagy vagy azt meghaladó értékű pénzre vagy
b) bűnszövetségben
követik el.

Pénzhamisítás elősegítése

390. § (1) Aki pénzhamisításhoz szükséges anyagot, eszközt, berendezést, gyártási tervet, műszaki leírást vagy számítástechnikai programot készít, átad, elfogad, megszerez, tart, az ország területére behoz, onnan kivisz, azon átszállít, vagy forgalomba hoz, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a pénzhamisítás elősegítését bűnszövetségben vagy üzletszerűen követik el.

Készpénz-helyettesítő fizetési eszköz hamisítása

392. § (1) Aki felhasználás céljából
a) készpénz-helyettesítő fizetési eszközt meghamisít,
b) hamis készpénz-helyettesítő fizetési eszközt készít, vagy
c) az elektronikus készpénz-helyettesítő fizetési eszközön tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket technikai eszközzel rögzíti,
vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) Aki készpénz-helyettesítő fizetési eszköz hamisítására irányuló előkészületet követ el, elzárással büntetendő.
(3) A külföldön kibocsátott készpénz-helyettesítő, illetve elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.

Készpénz-helyettesítő fizetési eszközzel visszaélés

393. § (1) Aki
a) egy vagy több olyan készpénz-helyettesítő fizetési eszközt, amely nem vagy nem kizárólag a sajátja, vagy amelynek a használatára nem vagy nem kizárólagosan jogosult, mástól, annak beleegyezése nélkül, jogtalanul elvesz vagy megszerez,
b) hamis vagy meghamisított, az a) pontban meghatározott módon elvett vagy megszerzett készpénz-helyettesítő fizetési eszközt, vagy az elektronikus készpénz-helyettesítő fizetési eszközön tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket átad, megszerez, az ország területére behoz, onnan kivisz, vagy azon átszállít,
vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a készpénz-helyettesítő fizetési eszközzel visszaélést bűnszövetségben vagy üzletszerűen követik el.
(3) A külföldön kibocsátott készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül.

Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése

394. § (1) Aki készpénz-helyettesítő fizetési eszköz hamisításához vagy a készpénz-helyettesítő fizetési eszközön lévő adat technikai eszközzel való rögzítéséhez szükséges anyagot, eszközt, berendezést vagy számítástechnikai programot készít, megszerez, tart, átad, forgalomba hoz, az ország területére behoz, onnan kivisz, vagy azon átszállít, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt bűnszövetségben vagy üzletszerűen követik el.

A magyar szakirodalomban elsőként Kertész Imre határozta meg a számítógépes hamisítások körét 1993-ban. Idetartozik az adatállomány meghamisítása, a hamis kódkártya készítése és használata, valamint a hamis bankjegy-, okiratkészítés. Ezekben a cselekményekben a külvilágban is érzékelhető hamisítást megelőzi az adatok megváltoztatása.[371] Később Nagy Zoltán András már a jogalkotás és jogalkalmazás szempontjait figyelembe véve határozta meg, mi tartozik a számítógépes hamisítás körébe:[372]

371 Kertész 1993: 14.
372 Nagy 2009: 177.

- készpénz-helyettesítő fizetési eszközök hamisítása,
- telefonkártyák hamisítása,
- közokiratok hamisítása,
- pénzhamisítás.

A számítógépes bűncselekmények körében illik néhány szót ejteni a készpénz-helyettesítő fizetési eszközökkel kapcsolatos visszaélésekről. Ennek fő oka a bankkártyák, valamint az internetes bankolás és elektronikus fizetések elterjedésében keresendő. Manapság már gyakorlatilag minden ember rendelkezik valamilyen típusú bankszámlával, és szinte minden üzletben elfogadják a bankkártyával történő fizetést is. Megnőtt ezenkívül az internetes szolgáltatásokat nyújtó oldalak száma, online megrendelhető a napi ebédtől a külföldről beszerzett könyvritkaságokig szinte bármi, és ehhez mindössze egy bankszámlaszám, néhány személyes adat és jelszó begépelése szükséges. Mindenekelőtt fontos azt tisztázni, mi is tekinthető készpénz-helyettesítő fizetési eszköznek, hiszen ez a visszaélések elkövetési tárgya minden esetben. A Btk. 459. § (1) bekezdés 19. pontja egy értelmező rendelkezést tartalmaz, miszerint készpénz-helyettesítő fizetési eszközön a külön jogszabályban meghatározott készpénz-helyettesítő fizetési eszközt, forgatható utalványt, kincstári kártyát, utazási csekket, törvény alapján kibocsátott utalványt és a váltót kell tekinteni, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett. Mint ahogy a fenti definícióból kitűnik, a Btk. ismét egy másik jogszabályhelyre utal, azonban annál tágabban határozza meg a készpénz-helyettesítő fizetési eszköz fogalmát, ugyanis e körbe vonja az utazási csekket és a váltót is. A külön jogszabály, amelyre a Btk. utal, a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (Hpt.). A Hpt. szerint készpénz-helyettesítő fizetési eszköz a csekk, az elektronikus pénz, valamint a pénzforgalmi szolgáltató és az ügyfél közötti keretszerződésben meghatározott olyan személyre szabott dolog vagy eljárás, amely lehetővé teszi az ügyfél számára a fizetési megbízás megtételét. A számítógépes bűnözés körében ebből a meghatározásból kiemelt jelentősége van az elektronikus pénzeszközöknek. Elektronikus pénz az elektronikus pénz kibocsátójával szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – összeg, amelyet pénzeszköz átvétele ellenében bocsátanak ki a pénzforgalmi szolgáltatás nyújtásáról szóló törvényben meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikus pénz kibocsátóján kívül más természetes és jogi személy, jogi személyiség nélküli gazdasági társaság és egyéni vállalkozó is elfogad. Napjaink népszerű fizetőeszközei, a kriptovaluták szintén ebbe a csoportba tartoznak.

A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekményeknek több fajtáját ismeri a törvény, ezek a készpénz-helyettesítő fizetési eszközök hamisítása, valamint a hamisítás elősegítése és a visszaélés készpénz-helyettesítő fizetési eszközzel. Közös vonásuk azonfelül, hogy az elkövetési tárgy azonos, az, hogy a bűncselekmény alanya minden esetben bárki lehet, valamint minden esetben szándékos bűncselekményről beszélünk.

A hamisítás két elkövetési magatartással valósulhat meg. Az egyik a készpénz-helyettesítő fizetési eszköz meghamisítása, a másik a hamis készpénz-helyettesítő fizetési eszköz készítése. Ez a két magatartás látszólag nagyon hasonló, azonban lényeges különbség közöttük, hogy a meghamisítás esetében egy eredetileg szabályos, már meglévő készpénz-helyettesítő fizetési eszköz jogellenes módosításáról beszélünk, míg a hamis készpénz-helyettesítő fizetési eszköz készítése esetében új eszköz létrehozása történik.

Az információs alapjogokkal kapcsolatos bűncselekmények

Az információs alapjogok kategóriájában alapvetően két nagyobb területet, az információszabadság és az adatvédelem kérdését szükséges tárgyalni, kitérve ezek ütközőzónáira is. Az információszabadság a közérdekű adatok nyilvánosságához, megismerhetőségéhez való jog; az adatvédelem, más néven az információs önrendelkezési jog pedig a magánszféra adatainak védelméhez való jog. Informatikai szempontból utóbbinak kiemelkedő a jelentősége, a számítógépes rendszerek és hálózatok kiépülésével ugyanis elvékonyodott a határvonal a magánszféra és a nyilvánosság között. A személyes adatok kezelése és tárolása az informatikai megoldásoknak köszönhetően virágkorát éli. Számítógépes nyilvántartásokban, adatbázisokban megtalálható az állampolgárokra vonatkozó összes információ. Némely adatokat hatóságok kezelnek, ilyen például a lakcímnyilvántartás, más adatokat azonban az internet ökoszisztémájában létező magánpiaci szereplők (például közösségimédia-platformok, internetszolgáltatók). Míg a legtöbb e fejezetben tárgyalt bűncselekmény esetében a közvetítő szolgáltatók azok a szereplők, akik segítői az elkövetők felderítésének, illetve a tartalmak eltávolítása révén az elősegítői a károk mérséklésének, az információs alapjogokkal kapcsolatos visszaélések esetében gyakran a saját adatkezelésük az, ami kifogásolható. A bűncselekményi szintet elérő magatartások esetében elképzelhető tehát, hogy azok a szolgáltatók, akiktől a nyomozó hatóság máskor segítséget várna, éppen a bűncselekmény alanyaivá válnak. Az informatikai

adatkezelésnek és adatvédelemnek igen kiterjedt szakirodalma van, most azonban kizárólag az adatkezelés és a büntetőjog kapcsolata szempontjából vizsgálom a kérdést.

A személyes adatok védelméhez való jog sérelme többféle jogsértést is megvalósíthat. Ilyenek a visszaélés személyes adattal, a magántitok megsértése, a magántitok jogosulatlan megismerése, valamint a levéltitok megsértése.

Személyes adattal visszaélés

A visszaélés a személyes adatokkal a Btk. 219. §-ában szabályozott deliktum. Hasonlóan a szerzői jogsértésekhez, a Btk. itt is csak keretjogszabály, amelyet tartalommal az Infotv. és a GDPR töltenek ki. A bűncselekmény jogi tárgya a személyes adat megismeréséhez és biztonságos kezeléséhez, őrzéséhez való jog. A személyes adat lehet az egyénnel összefüggésbe hozható bármely információ. A GDPR 4. cikk 1. pontja példálózó jelleggel fel is sorolja a legjellemzőbb személyes adatokat, amelyek: „név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó" ismeret.[373] A taxáció természetesen nem zárt, hanem a joggyakorlat által szabadon bővíthető. A NAIH egyik állásfoglalása szerint például személyes adat lehet a peres ügyekben az egy meghatározott személlyel összefüggésbe hozható bírósági ügyszám is.[374]

> 219. § (1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva
>
> a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
>
> b) az adatok biztonságát szolgáló intézkedést elmulasztja,
>
> vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
>
> (2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével az érintett hozzáféréshez való jogának gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.

373 GDPR 4. cikk 1. pont.

374 A NAIH/2020/294/4. számú állásfoglalásban kimondja, hogy közérdekű adatnak minősülnek a bírósági ügyszámok mindaddig, amíg nem válnak személyes adattá, mivel azokat a bíróság közfeladata ellátásával összefüggésben keletkezteti.

(3) A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra vagy bűnügyi személyes adatra követik el.
(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.

A Btk. személyes adattal való visszaélést büntetni rendelő szakaszában általános alanyt használ a törvényhozó, vagyis az elkövető – szemben a magántitok megsértésével – bárki lehet. Az általános alany kérdésével az 1/2012. Büntető Jogegységi Határozat foglalkozott, amely szintén megerősítette, hogy az első fordulatba ütköző bűncselekményt bárki elkövetheti, nem csak az, aki adatkezelőnek minősül. Ezt az álláspontot erősítette meg a BH2012.87 is, amikor kimondta, hogy alanyi oldalon nem feltétel az Infotv. szerinti adatkezelői minőség. A törvény négyféle elkövetési magatartást szabályoz. Az első két alapeset szerint megvalósítható a bűncselekmény jogosulatlan vagy céltól eltérő adatkezeléssel. Adatkezelésnek minősül az adatokon végzett bármilyen művelet vagy a műveletek összessége, például gyűjtése, törlése, megváltoztatása, nyilvánosságra hozatala. Éppen ezért személyes adattal visszaélés könnyen megvalósulhat azáltal, hogy a sértettről annak hozzájárulása nélkül osztanak meg valamilyen személyes adatot, az online környezetben igen gyakran képet vagy videófelvételt. Jogosulatlannak minősül az az adatkezelés, amely a GDPR 6. cikk (1), illetve az Infotv. 5. § (1) bekezdéseiben felsorolt jogalapok hiányában történik. Jogosulatlan az adatkezelés például akkor, ha ahhoz az érintett nem járult hozzá, vagy azt nem jogszabály rendelte el. A céltól eltérő adatkezelés akkor is tényállásszerű, ha az adatkezelésre egyébként megfelelő jogalappal került sor, mivel a célhozkötöttség olyan általános elv, amelynek az adatkezelés teljes folyamatát át kell hatnia.

A jogalkotó az adatbiztonságot is büntetőjogi védelemben részesíti, hiszen aki adatokat kezel, az köteles gondoskodni azok biztonságáról, ennek elmulasztása megvalósítja e szakasz b) pontját, amely a harmadik törvény által szabályozott elkövetési magatartás. Az adatok biztonságáról sokféleképp lehet gondoskodni, lehet ez technikai intézkedés, de személyes jellegű is, például biztonsági őr állítása annak a helyiségnek az ajtaja elé, ahol adatkezelés folyik. Ez a rendelkezés felveti azt a kérdést, hogy mi számít pontosan az adatok biztonságát szolgáló intézkedésnek. Természetesen nem valósul meg bűncselekmény, ha az adatkezelő megtett minden tőle elvárható intézkedést az adatok védelme érdekében, de ennek ellenére valaki jogellenesen hozzáfért azokhoz, például mert a számítógépes rendszer hackertámadás áldozata lett.

A bűncselekmény negyedik elkövetési magatartása az érintett hozzáféréshez való jogának gyakorlása érdekében szükséges tájékoztatására vonatkozó kötelezettség megsértése, amennyiben ez jelentős érdeksérelmet okoz.

Lényeges fordulata ennek a szakasznak, hogy az a) és b) pontban leírt elkövetési magatartások tanúsításával még nem valósul meg bűncselekmény, annak szükséges eleme az is, hogy az elkövetés jogtalan haszonszerzési célból vagy jelentős érdeksérelmet okozva valósuljon meg. A jogtalan haszonszerzési cél nem igényel különösebb magyarázatot.

A személyes adattal való visszaélés haszonszerzési célzattal történő elkövetésére jó példa a *phishing,* vagyis az adathalászat. Ennek lényege, hogy az elkövetők szervereket bérelnek, majd lemásolják bankok, vállalkozások weboldalait, ügyfeleiket pedig e-mailben keresik meg információkérés ürügyén. Az e-mailben megadott linkre kattintva a lemásolt weboldal jön be, ahol a felhasználó megadja belépési adatait és jelszavait, amelyeket a rendszer azonnal továbbít az elkövetőknek, a felhasználónak pedig egy hibaüzenetet közvetít, például azt, hogy a rendszer karbantartás miatt nem elérhető. Hasonló esetek Magyarországon is rendszeresen történnek. A koronavírus-járvánnyal összefüggésben a Google naponta 18 millió adathalászati célú e-mailt szűrt,[375] amelyek igen változatos módokon igyekeztek személyes adatokat vagy pénzt szerezni a felhasználóktól. Az adathalászok gyakran a WHO vagy bankok nevében küldtek üzenetet, de a Nemzeti Kibervédelmi Intézet (NKI) felhívta a figyelmet egy olyan módszerre is, amely során az elkövetők helyi kórházak nevében kérték a felhasználót, hogy egy mellékelt űrlap kitöltése után fáradjon be koronavírus-tesztelésre.[376] A kitöltésre küldött űrlap olyan kártékony makrót tartalmazott, amely kriptopénztárcákat és a bejelentkezési adatokat tároló webes sütiket próbált megszerezni. Szintén az NKI hívta fel a figyelmet arra a módszerre, amelynek során számlaadatok megadására próbálták rávenni az áldozatokat.[377] Az e-mail – amelyet egy pénzintézet nevében írtak, és a koronavírus-járvány miatt online ügyintézésre buzdított – kártékony kódot futtató csatolmányt tartalmazott. Az adathalász e-mailek a bosszúság mellett nem kis anyagi kárt is képesek okozni, a német állam több mint 10 millió eurót veszített adathalászok miatt. Az adathalászat esetében fokozott figyelemmel kell vizsgálni, hogy az elkövető cselekménye nem valósít-e meg egyéb bűncselekményt, hiszen a személyes adatokkal való visszaélés sok esetben egy másik, súlyosabb bűncselekménynek az eszközcselekménye. Nagy Zoltán András a mások személyes adataival történő

375 Juhász 2020.
376 Nemzeti Kibervédelmi Intézet 2020b.
377 Nemzeti Kibervédelmi Intézet 2020a.

csalásoknak három fázisát különíti el.[378] Az első a tulajdonképpeni adathalászat, a Btk. 219. § szerinti visszaélés személyes adattal. Az elkövetési tárgy a személyes adat, tehát az ügyfél belépési kódja, jelszava, hiszen ezek olyan adatok, amelyek közvetlenül kapcsolatba hozhatók vele. Ha az elkövető a személyes adatokat felhasználva már belép egy információs rendszerbe, akkor a cselekmény második fázisa a Btk. 423. § szerinti jogosulatlan belépést valósítja meg. A harmadik fázis a pénz átutalása egy másik számlára, azaz a károkozás, ami a csalás bűntettének minősül.

Érdekes megvizsgálni a jogszabályi rendelkezésnek a jelentős érdeksérelem okozására vonatkozó joggyakorlatát is.

Hazai joggyakorlat

Jelentős érdeksérelem okozása miatt személyes adattal visszaélésnek minősítette a bíróság egy online hírportálon megjelent kép közzétételét, amely a nagy médiaérdeklődéssel övezett Fészekrakó-ügy egyik vádlottját ábrázolta. Az internetes portál egy sajtótájékoztatóról tudósítva tette közzé a vád tárgyát képező felvételt, amelyen a sértett is egyértelműen felismerhető volt. A kommentszekció hozzászólásai egyértelműen alátámasztották, hogy az olvasók ténylegesen fel is ismerték a sértettet, őt becsmérlő jellegű kifejezésekkel illették. A bíróság álláspontja szerint a jelentős érdeksérelem ebben az esetben abban állt, hogy romlott a sértett társadalmi megítélése (3.Bf.1080/2013/12).

Jelentős érdeksérelmet okozott az a terhelt is, aki a volt házastársáról, annak tudta és beleegyezése nélkül, a személye azonosítását lehetővé tevő szexuális felvételeket hozott nyilvánosságra egy internetes közösségi platformon (Fővárosi Törvényszék, 42(II.)Kb.1327/2015).

A jelentős érdeksérelem tehát minden esetben valamilyen negatív eredmény, többnyire a sértett társadalmi megítélésének, megbecsültségének csorbulása. A jelentős érdeksérelem mint eredmény vonatkozásában a bírósági gyakorlat azt mutatja, hogy bekövetkeztének megállapítása nem a sértett szubjektív és elfogult álláspontján alapul, hanem bírói mérlegelésen, amelyben fontos szerepet tölt be a sértett egyéni tulajdonságainak, élethelyzetének és a társadalmi felfogásnak a vizsgálata. Az egyén társadalmi megítélésének csorbulása esetében lényeges annak vizsgálata, hogy a nyilvánosságra került információról hogyan vélekedik általában a közvélemény, és melyek azok a tényezők, amelyek a közfelfogást negatív irányban befolyásolhatják. A korábban említett jogesetben a bíróság megállapította, hogy a hozzájárulás nélkül közzétett szexuális

[378] Nagy 2019: 154.

felvételek a nők megítélését általában jobban csorbítják, hiszen a közfelfogás a férfiakkal tekintetben megengedőbb. Míg a férfiak esetében a szexuális felvételek nyilvánosságra kerülését sokszor a férfiasság és a szexuális teljesítmény bizonyítékaként, mintegy elismeréssel fogadja a társadalom, addig a nők esetében inkább a könnyűvérűséggel összefüggő, negatív vélemények fogalmazódnak meg. A bíróság e megállapításának ellenére, a jelentős érdeksérelem bekövetkeztét esetről esetre kell mérlegelni, hiszen egy intim felvétel hozzájárulás nélküli nyilvánosságra hozatala az érintettek nemétől függetlenül okozhat sérelmet.

Jó példája a jelentős érdeksérelem okozásának az úgynevezett személyazonosság-lopás *(identity theft)*. A személyazonosság-lopás sokféleképpen megvalósulhat. Az egyik leggyakoribb előfordulása, amikor az elkövető álprofilt hoz létre valamilyen online platformon egy másik személy nevében, és onnan terjeszt hazug, lejárató információkat. Gyakran fordul elő az is, hogy az elkövető személyes adatok birtokában más személy nevében vesz igénybe szolgáltatásokat, vásárol hitelre nagy értékű ingóságot.

Ha jelentős érdeksérelem nem következik be, azonban annak reális lehetősége fennáll, a cselekmény kísérleti szakban marad.

Hazai joggyakorlat

Személyes adattal visszaélés kísérlete miatt ítélték el azt a politikust, aki egyes megyei vadásztársaságok által szervezett ingyenes vadászatokról hozott nyilvánosságra információkat (vadászati naplók, trófeabírálati lapok, számlák). A terhelt védekezésében előadta, hogy az ingyenes vadászatok, amelyeken zömében magas rangú politikusok vettek részt, a közvagyont károsították, ezért államtitkári minőségét kihasználva, de hatáskörét túllépve kért be személyes adatokat is tartalmazó információkat a vadásztársaságoktól, földügyi hatóságoktól. A bíróság szerint ugyanakkor az érintetteknek nem származott jelentős hátránya az információk nyilvánosságra hozatalából, amely a köztudatban inkább politikai jellegű lejáratásként jelent meg, így a cselekmény kísérleti szakban maradt (Fővárosi Törvényszék, 28.B.436/2011/56).

Súlyosabban minősül a bűncselekmény, ha különleges személyes adatra követik el, amely a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adat, a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adat, az egészségügyi adat és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó

személyes adat.[379] Jelentős érdeksérelem okozásának szándéka miatt tett feljelentést a NAIH a *www.deres.tv* címen elérhető honlapon közzétett *A nagy köcsög adatbázis 2.* szerkesztőivel szemben. Az adatbázis felállításának célja az LMBTQ-közösséghez tartozó, illetve az azzal sorsközösséget vállaló személyek lejáratása és becsmérlése volt. A különleges személyes adatokon a NAIH álláspontja szerint az elkövetők az alábbi jogosulatlan műveleteket végezték: „személyes adatok jogellenes gyűjtése (a fényképek lementése a Facebookról és ehhez kapcsolódóan nevek gyűjtése), személyes adatok meghatározott célra való rendszerezése, személyes adatok tárolása, adatbázisba rendezett személyes adatok nyilvánosságra hozatala."[380]

A norvég fogyasztóvédelmi bizottság 2020. január elején tette közzé jelentését,[381] amelyben népszerű applikációk adatkezelését vizsgálták. A jelentés megállapítása szerint az olyan közösségi társkereső szolgáltatások, mint a Grindr, az OkCupid vagy a Tinder, reklám- és marketingvállalkozásokkal megoszt olyan adatokat, mint a felhasználó választásai, illetve földrajzi helyzete. Egyes szolgáltatások, például a kimondottan homoszexuálisok számára létrehozott Grindr esetében az adatok megosztása a felhasználók szexuális irányultságának megosztásával járt, amely különleges személyes adat, és nyilvánosságra jutása egyes országokban (például Katarban vagy Palesztinában, ahol tilos az azonos neműek közötti szexuális tevékenység) jelentős hátrányt okozhat.[382] Nemcsak a közösségi társkereső alkalmazásokkal kapcsolatban tárt fel visszásságokat a jelentés, hanem az olyan alkalmazásokra vonatkozóan is, amelyek egészségügyi adatok megadását kérték (például a MyDays ovulációs naptár és cikluskövető), és olyan alkalmazásokkal kapcsolatban is, amelyek vallási meggyőződéssel kapcsolatos adatokat kértek a felhasználóktól (például a muszlimok számára fejlesztett Prayer Time alkalmazás). Bűncselekmény ugyanakkor ezekben az esetekben nem valósul meg, mivel a felhasználónak a regisztrációkor el kell fogadnia az adatkezelési tájékoztatót, amellyel többnyire beleegyezik az adattovábbításba annak érdekében, hogy használhassa a szolgáltatást.

Személyes adataink védelme az online platformokon

Adatkezelési gyakorlatuk miatt a nagy online platformokat sokszor érik kemény kritikák, ezek ugyanakkor főként adatvédelmi és nem büntetőjogi relevanciával bíró ügyek. Jelen kötetben

379 GDPR 9. cikk.
380 Péterfalvi–Eszteri 2017: 405–420.
381 Forbrukerrådet 2020.
382 Singer–Krolik 2020.

a felhasználók büntetőjogi szankció után kiáltó cselekedetein van a hangsúly, így ebben a részben is arra koncentrálok, hogy mit tesz a Facebook a felhasználók által elkövetett jogsértések ellen, nem pedig a cég saját, belső adatvédelmi gyakorlatára.

A Facebook/Meta közösségi alapvelveinek egyik legfontosabb rendelkezése a személyes adatok védelmével összhangban, hogy tiltja a személyes adatok online kereskedelmét, mások személyes adatainak megosztását, illetve a személyes adatok közvetlen vagy külső weboldalra mutató hivatkozáson keresztül történő gyűjtését. A közösségi alapelvek ugyanakkor nem személyes adatokról szólnak, hanem személyhez kötődő információkról, amelyek köre korántsem fog át minden olyan információt, amely valamely személlyel összefüggésbe hozható. Az alapelvek ahelyett, hogy általános feltételekhez – például érdeksérelem okozásához – kötnék a személyes adatok jogosulatlan kezelését, egészen konkrét adatfajtákat és szituációkat írnak le, amelyekben a személyes adatok közzététele eltávolítást von maga után. Tilos a Facebookon és az Instagramon közzétenni az alábbiakat:

- az állam által kiadott azonosító számok, például útlevélszám, személyiigazolvány-szám, társadalombiztosítási azonosító stb.;
- személyhez fűződő, a név ismeretében annak azonosítását lehetővé tévő nyilvántartások adatai, például ingatlan-nyilvántartás, anyakönyvi nyilvántartás, halotti anyakönyvi nyilvántartás adatai, vezetői engedélyek és rendszámok stb.;
- digitális személyazonossághoz kapcsolódó adatok, például e-mail-címek, azonosítók az azokhoz tartozó jelszavakkal, PIN-kódokkal együtt;
- a magánlakás védelme miatt tilos az azt kívülről ábrázoló felvételt megosztani, ha abból egyértelműen beazonosítható, hol található az ingatlan (például jól látható utcanév és házszám, GPS-koordináta);
- az egészségügyi személyes adatok fokozott védelme miatt tilos hivatalos egészségügyi dokumentumok megosztása (például leletek, zárójelentések).

A YouTube közösségi irányelvei külön fejezetet szentelnek a személyes adatokkal való visszaélésnek. A szolgáltató a személyes adatokkal visszaélést viszont kizárólag a személyazonosság-lopással összefüggésben szabályozza. A közösségi iránymutatások e körben egyrészt tiltják más csatornák lemásolását (általános megjelenés és képvilág átvétele), valamint a természetes személyek adatainak felhasználásával végzett tevékenységeket (például csatornák létrehozása más személy nevével és képével). A rajongói csatornák üzemeltetése nem tilos, ebben az esetben a csatorna tulajdonosának kifejezetten fel kell hívnia a figyelmet arra, hogy nem az eredeti alkotót, előadót vagy gazdasági társaságot képviseli. A mások megszégyenítését bemutató tartalmakat a platform nem a személyes adatok védelméről szóló részben, hanem a zaklatásnál szabályozza.

Az X (Twitter) ezzel szemben részletes leírást szentel a magánélet védelmének. A platform felhasználási feltételei rögzítik, hogy tilos más személyek személyes adatait (nevét, lakcímét, tartózkodási helyét, biometrikus adatait stb.) nyilvánosságra hozni azok kifejezett beleegyezése nélkül. Személyes adatnak minősül az érintettre vonatkozó adatok mellett az olyan médiatartalom is, amelyben az érintett képmása megjelenik. Sőt, a szolgáltató a nyilvánosságra hozatallal történő fenyegetést is tiltott magatartásnak tekinti. Kivételszabályt ez a platform is megfogalmaz, amikor elismeri, hogy vannak olyan események, amelyek hírértékkel bírnak, ennélfogva akkor is közzétehetők, ha azokban olyan magánszemélyek jelennek meg, akik nem járultak hozzá kimondottan a tartalom publikálásához.

Levéltitok megsértése

A levéltitok megsértését a Btk. 224. §-a szabályozza.

224. § (1) Aki
- a) másnak közlést tartalmazó zárt küldeményét megsemmisíti, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, illetve
- b) elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított közleményt kifürkész,

ha súlyosabb bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.
(2) A büntetés egy évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt foglalkozás vagy közmegbízatás felhasználásával követik el.
(3) A büntetés
- a) két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény,
- b) bűntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény

jelentős érdeksérelmet okoz.

A bűncselekmény jogi tárgya a magánélet, illetve az emberi méltóság, ugyanakkor a cselekmény nemcsak természetes személy sérelmére, hanem jogi személyek, hatóságok sérelmére is elkövethető. A Btk. 224. §-a két elkövetési tárgyról rendelkezik, a közlést tartalmazó zárt közleményről, valamint az elektronikus hírközlő hálózaton továbbított közleményről. Az első fordulat által szabályozott zárt közlemény nemcsak papíralapú

levél, csomag vagy fizikai adathordozó lehet, a Btk. kommentárja[383] idesorolja az elektronikus küldeményeket és az sms-eket is. A két fordulat közötti különbség információs rendszer segítségével folytatott kommunikáció esetén az elkövetési magatartásban keresendő. Míg az első fordulat elkövetési magatartásai a megsemmisítés, felbontás, megszerzés, valamint az illetéktelen személynek átadás, a második fordulat, a kifürkészés valójában a kommunikációs folyamat lehallgatása. Előbbi történhet például úgy, hogy az elkövető a sértett számítógépe elé ülve elolvassa az e-mail-fiókban lévő leveleket, míg a második esetben a küldemény „elfogása" a kommunikációs folyamatba ékelt eszköz vagy program segítségével történik. A levéltitok megsértése szubszidiárius jellegű bűncselekmény, vagyis megállapításának csak akkor van helye, ha más, súlyosabb bűncselekmény nem valósul meg. A kifürkészéshez szorosan kapcsolódó tényállás például a tiltott adatszerzés, illetve a hivatali bűncselekmények közül a jogosulatlan titkos információgyűjtés vagy leplezett eszköz jogosulatlan használata.

Tiltott adatszerzés

422. § (1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával titokban megfigyeli vagy rögzíti,
c) más postai küldeményét vagy egyéb zárt küldeményét titokban felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti,
e) információs rendszerben kezelt adatokat titokban kifürkész, és az észlelteket technikai eszközzel rögzíti,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(1a) Az (1) bekezdés szerint büntetendő, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

[383] Szomora 2019b.

a) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiséget vagy területet, – a közösségi közlekedési eszköz kivételével – járművet, továbbá más használatában levő tárgyat titokban átkutat,
b) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiségben vagy területen, továbbá – a közösségi közlekedési eszköz kivételével – járművön történteket titokban technikai eszköz alkalmazásával megfigyeli vagy rögzíti.

(2) Az (1) bekezdés szerint büntetendő, aki fedett nyomozó, illetve titkos információgyűjtés folytatására vagy leplezett eszközök alkalmazására feljogosított szervvel titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.

(3) Az (1) bekezdés szerint büntetendő, aki az (1)–(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.

(4) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha az (1)–(3) bekezdésben meghatározott tiltott adatszerzést

a) hivatalos eljárás színlelésével,
b) üzletszerűen,
c) bűnszövetségben vagy
d) jelentős érdeksérelmet okozva

követik el.

422/A. § (1) Aki pilóta nélküli légi jármű jogosulatlan használatával más lakását, egyéb helyiségét, vagy ezekhez tartozó bekerített helyet megfigyeli és az ott történteket rögzíti, ha más bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.

(2) Egy évig terjedő szabadságvesztéssel büntetendő, ha más bűncselekmény nem valósul meg, aki az (1) bekezdésben meghatározott megfigyelés során készített hang- vagy képfelvételt a nagy nyilvánosság számára hozzáférhetővé teszi.

(3) Az (1)–(2) bekezdésben meghatározott bűncselekmény csak magánindítványra büntethető.

A tiltott adatszerzés jogi tárgya szintén a magánélet, ezen belül a magántitok védelméhez való jog. A bűncselekménynek három alapesete van: a tiltott adatszerzés, a fedett nyomozóra, annak felfedésére irányuló tiltott adatszerzés, valamint a tiltott adatfelhasználás. Az első alapeset elkövetési magatartásait a célzatosság határolja el a levéltitok megsértésétől. A felsorolt magatartások célja ebben az esetben személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése.

Hazai joggyakorlat

Ilyen eset, amikor a terhelt a házassági bontóper során felvételt készít a házastársa üzenetváltásairól, hogy azt a bíróságon felhasználja (Bf.III.1.548/2014).

A küldemények felbontásához vagy megszerzéséhez és a kommunikáció kifürkészéséhez kapcsolódó speciális tényállási elem az, hogy az elkövető a jogellenesen tudomására jutott információt rögzítse. A Btk. 2018 óta nemcsak a folyamatban lévő kommunikáció lehallgatását teszi büntetendővé, hanem az információs rendszerben kezelt adatok kifürkészését, az „adatlopást" is. Ebben az esetben az elkövetés tárgya nem az elektronikus hírközlő hálózaton áthaladó küldemény, hanem a már a rendszerben lévő, ott közvetlenül, akár internetkapcsolat nélkül hozzáférhető adat. A tényállásszerűségnek nem feltétele, hogy az információs rendszerbe történő belépés jogtalanul történjen. A Btk. kommentárja szerint[384] akkor is megvalósul, ha az elkövető a számítógép monitorjáról fényképfelvételt készít.

2020-ban a tiltott adatszerzés tényállása kiegészült a jogosulatlan drónhasználattal. Ezek a kis méretű, kereskedelmi forgalomban kapható pilóta nélküli légi járművek bárki számára lehetővé teszik más személyek távoli megfigyelését. A jogosulatlan drónhasználatnak szabálysértési alakzata is létezik, amely jogosulatlan felvételkészítéssel követhető el (például lakóövezetben átrepülés közben). A Btk.-ban szabályozott elkövetési magatartás akkor tényállásszerű, ha a drónnal megfigyelés történik, amely az egyszeri előforduláshoz képest huzamosabb figyelemmel kísérést jelent. A cselekmény csak a drónhasználat jogosulatlansága esetén büntethető, ha a pilóta rendelkezik engedéllyel, a felvételkészítés legfeljebb csak személyes adat megsértését eredményezheti, amennyiben ez jelentős érdeksérelmet okoz, vagy haszonszerzési célt szolgál.

Zaklatás az online térben

A zaklatás jogi tárgya a személy magánszférája, amely az Alaptörvény VI. cikkében foglalt magánélethez való joggal áll szoros kapcsolatban. A magánélethez, magánszférához való jog végső soron az emberi méltósághoz való jogból eredeztethető, annak szubszidiárius alapjoga. Az alapjogi gondolkodás szerint a magánélethez való jog részint magában foglalja az önkifejezéssel, önrendelkezéssel kapcsolatos jogosítványokat,

384 Szomora 2019b: 492–531.

így a saját test, személyes adatok feletti rendelkezés jogát, a véleménynyilvánítás szabadságát, illetve a jóhírnév védelmét,[385] továbbá a Samuel Warren és Louis Brandeis által megfogalmazott háborítatlanságot, vagyis „egyedül hagyatáshoz" való jogot.[386] Egyes, más magánéletébe történő beavatkozások a Btk. 222. §-a által szabályozott zaklatás tényállását is kimeríthetik.

> 222. § (1) Aki abból a célból, hogy mást megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen vagy tartósan háborgatja, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
> (2) Aki félelemkeltés céljából
> a) mást vagy rá tekintettel hozzátartozóját személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével megfenyeget, vagy
> b) azt a látszatot kelti, hogy más életét, testi épségét vagy egészségét sértő vagy közvetlenül veszélyeztető esemény következik be,
> vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
> (3) Aki a zaklatást
> a) házastársa, volt házastársa, élettársa vagy volt élettársa sérelmére,
> b) nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére,
> c) hatalmi vagy befolyási helyzetével visszaélve, illetve
> d) hivatalos személy sérelmére, hivatali tevékenységével össze nem egyeztethető helyen vagy időben
> követi el, az (1) bekezdésben meghatározott esetben két évig, a (2) bekezdésben meghatározott esetben bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.
> (4) Az a tizennyolcadik életévét betöltött személy, aki az (1) bekezdésben meghatározott zaklatást tizennyolcadik életévét be nem töltött személy sérelmére követi el, két évig terjedő szabadságvesztéssel büntetendő.

A zaklatásnak két alapesete van. Az első esetben az elkövetési magatartás más személy rendszeres vagy tartós háborgatásával valósul meg, míg a második esetben a sértett megfélemlítését célzó veszélyes fenyegetés minősül tényállásszerű magatartásnak.

Az első eset kapcsán a leggyakrabban felmerülő kérdés az, hogy mely magatartások merítik ki a rendszeres vagy tartós háborgatás fogalmát, illetve hogy van-e az online

[385] Solove 2008: 1.
[386] Brandeis–Warren 1890: 193–220.

térben megvalósuló zaklató jellegű magatartásoknak olyan *differentia specifica*ja, amely esetlegesen eltérő kezelést indokol.

A háborgatás kifejezés jelentéstartalmát górcső alá véve Ambrus István rámutat arra, hogy a háborgatást a jog olyan gyűjtőkategóriának tekinti, amely a sértett „mindennapi életét negatívan befolyásoló, nyugtalanító, megnehezítő, zavaró magatartásokból tevődik össze".[387] A Legfelsőbb Bíróság értelmezése is ezt támasztja alá, nem elég tehát a más életébe történő kéretlen beavatkozás, hanem a bűncselekmény megvalósulási feltétele az is, hogy a beavatkozáshoz a sértett negatívan viszonyuljon. Háborgatás lehet a sértett folyamatos hívogatása, felbukkanás annak iskolájában, munkahelyén vagy egy jól irányzott fenyegetés, a szóba jöhető magatartások köre olyan széles skálán mozog, hogy a zaklatás tényállása kvázi nyitott törvényi tényállásként jelenik meg a jogirodalomban.

A régi Btk. kiemelte a személyes vagy telekommunikációs eszköz útján történő kapcsolatteremtésre törekvést, a hatályos törvénykönyvünk azonban ezt a példát már nem tartalmazza, mivel a jogalkotónak nem állt szándékában ezzel szűkíteni a háborgató magatartások körét. A Btk. ugyan erre közvetlenül nem utal, de a cselekmény megvalósulásához elegendő, ha ez elkövető csak megpróbálkozik a kapcsolatteremtéssel, a zaklatás megállapításának nem feltétele, hogy a kapcsolat ténylegesen létre is jöjjön.

Hazai joggyakorlat

A háborgató magatartást tényállásszerűnek tekintette a bíróság abban az esetben, amikor a terhelt üzenetei megérkeztek ugyan a sértett fiókjába, azonban azokat a sértett nem olvasta el (BH2011.302).

A sértett magánéletébe való beavatkozásnak önkényesnek kell lennie, amelynek jelentését a Kúria egy vitatott ítéletben értékelte (BH2014.169). A Kúria álláspontja szerint a háborgatás kölcsönössége az önkényességet mindkét oldalon kioltja. Monori Zsuzsanna ezzel az érveléssel szemben kritikaként fogalmazza meg, hogy a zaklató, háborgató magatartások ritkán egyoldalúak[388] (mert például a zaklatás hátterében megromlott élettársi, házastársi viszony áll), a sértett pedig a háborgató magatartására mintegy védekezésképp maga is hasonló magatartással felelhet. Vida Mihály szerint az önkényesség jelentéstartalmához hozzátartozik, hogy az elkövető olyan magatartást

[387] Ambrus–Ujvári 2016: 425.
[388] Monori 2016a: 29–39.

tanúsít, amelyet a sértett nem kíván, vagy visszautasít,[389] ez viszont független attól, hogy úgynevezett „viszonzaklatásról" van-e szó. A Btk. kommentárja szerint nem minősül önkényesnek a magatartás, ha az jogszerű vagy erkölcsileg helyeselhető célból történik, például elvált szülők esetében a láthatási, tartásdíjfizetési kérdések rendezése. Ez az értelmezés azonban számos visszaélésre ad lehetőséget, mivel ahogyan Monori Zsuzsanna leírja, a gyakorlatban gyakran előfordul, hogy az elkövető ténybeli beismerő vallomást tesz, mégis valamilyen jogszerű céllal, méltányolható érdekkel igyekszik alátámasztani, hogy cselekménye indokolt volt.[390] Monori szerint ez a védekezés csupán a kapcsolatfelvételek tartalmi vizsgálatával cáfolható meg.[391]

A zaklatás megállapíthatóságának további eleme, hogy a háborgatás ne egyszeri legyen, hanem az legyen rendszeres vagy tartós. Az egyszeri háborgató magatartás még akkor sem tényállásszerű, ha a sértettben esetleg jelentős félelmet kelt, hiszen a törvényi tényállás egyik eleme, hogy annak többszörösen megvalósulónak (rendszeresnek) vagy időben elhúzódónak (tartósnak) kell lennie. Megosztott ugyanakkor a jogtudomány a tekintetben, hogy ez a fajta rendszeresség egyszerű ismétlődést jelent, vagy kapcsolódik hozzá valamilyen többletfeltétel. Egyes álláspontok szerint a háborgatás rendszeressége egyszerűen többszöri elkövetést jelent,[392] más álláspontok szerint viszont az ismétlődésnek huzamosabb időn át fenn kell állnia, annak mennyiségileg többet kell jelentenie, mint az ismételtség.[393]

Hazai joggyakorlat

Nem valósítja meg a zaklatás bűncselekményét az, aki két napon át küld üzeneteket a sértettnek, mert a háborgatás huzamosabb ideig kifejtett, több napon, több héten át tartó magatartást feltételez (ÍH 2010.97). Szintén nem tényállásszerű az a cselekmény, ahol az elkövető egy napon belül indított telefonhívásokat a sértett felé, mivel a cselekmény nem minősül napi szinten ismétlődőnek, sem folyamatosnak (Szegedi Ítélőtábla, Bf. I.505/2014/5).

A zaklatás tényállásának második alapesete két fordulatból áll. Az első fordulata az erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével való fenyegetés, második alakzata pedig az olyan látszat keltése, hogy más életét, testi épségét vagy

389 Vida–Juhász 2009: 160.
390 Monori 2016a: 29–39.
391 Monori 2016a: 29–39.
392 Szomora 2013: 466.
393 Ambrus–Ujvári 2016: 427.

egészségét közvetlenül sértő vagy közvetlenül veszélyeztető esemény következik be. A zaklatás első alapesetével ellentétben itt nincs szó sem rendszerességről, sem tartósságról, az elkövetés egymozzanatos cselekmény esetében is tényállásszerűnek tekinthető.

A zaklatásnak mindkét esete célzatos magatartást feltételez, azaz csak akkor állapítható meg, ha az elkövető szándéka a sértett megfélemlítése, annak magánéletébe, illetve mindennapi életébe történő önkényes beavatkozás.

Az internet korában a zaklatásszerű magatartások ugrásszerűen megszaporodtak, a zaklatás igen gyakran online szolgáltatásokon keresztül – e-mail vagy közösségimédia-platformok használatával – történik. Az internet világa, a közösségi platformok nagyon megkönnyítik az elkövető dolgát, hiszen már nem szükséges a sértett nyomában járva kiismerni annak napirendjét, hosszan várakoznia a munkahelye, lakása előtt, hanem az otthona kényelméből néhány gombnyomással akár anonimitásba burkolózva is megvalósíthatja a háborgató magatartást.

Az online tér sajátosságaiból adódóan azonban az előbbiekben ismertetett tényállást néhol más szemüveggel kell megvizsgálnunk. A legtöbb online közösségimédia-szolgáltatás ma már lehetőséget biztosít a felhasználók számára, hogy letiltsanak, némítsanak bizonyos ismerősöket, illetve meggátolják, hogy ismeretlenek felvegyék velük a kapcsolatot.

Monori Zsuzsanna felhívja a figyelmet arra, hogy az önkényesség eleme az, hogy a sértett az elkövető közeledését visszautasítsa. Nem minősül a közeledés visszautasításának, ha a sértett nem használja ki a szolgáltatások által biztosított lehetőségeket annak érdekében, hogy az elkövető magatartását, az üzenetek fogadását meggátolja, tehát ha a sértett nem él a szolgáltatások által felkínált lehetőségekkel, az önkényesség megállapítása kizárt, és nem valósul meg zaklatás. A felhasználók védelme körében a nagyobb platformok több lehetőséget is biztosítanak a kommunikáció megakadályozására. A Facebook például azt javasolja a felhasználóknak, hogy töröljék a zaklatót az ismerőseik közül, vagy tiltsák le, hogy az ne kezdeményezhessen kapcsolatot.[394] A felhasználóknak lehetőségük van a zaklató felhasználó fiókját vagy magát az üzenetet is jelenteni, ami gyakorlatilag egy, a platform és a felhasználó viszonyában benyújtott magánindítvány, amely arra irányul, hogy a platformszolgáltató távolítsa el a kérdéses tartalmat. A felhasználó a saját bejegyzései alatt közzétett zaklató, háborgató kommenteket 2018 óta maga is elrejtheti, moderálhatja.[395]

394 Facebook Help Center 2023.
395 Locklear 2019.

Zaklatás az online platformokon

A Facebookot és az Instagramot működtető Meta közösségi alapelvei az ártalmas, bántalmazó kommunikáció számos formáját tilalmazzák. Noha az alapelvekben sűrűn találkozhatunk a zaklatáshoz hasonló jelentésű *harassment,* illetve az azzal rokon *bullying* terminológiával, le kell szögeznünk, hogy ezek nem azonosak azzal a magatartással, amelyet a magyar dogmatikai rendszer szerint zaklatásnak tartunk. A közösségi alapelvek például zaklatásnak minősítik az egyszeri alkalommal történő, ám kéretlen kapcsolatfelvételt. Így tehát, amikor a Facebook vagy az Instagram zaklatásról szóló részeit elemezzük, akkor inkább ártó szándékú, bántó kommunikációról szólunk, amelyek között előfordulnak zaklató, illetve zaklatásszerű magatartások is. A zaklatásszerű kommunikációt a sértettek státuszához igazodó fokozatokba sorolják. Az egyszerű felhasználókon túl a Meta szabályzata külön rendelkezéseket tartalmaz a közszereplőkre, akiknek az átlagembereknél jobban kell tűrniük a kritikát. A platform a közszereplők kategóriáján belül megkülönbözteti a korlátozottan közszereplő egyéneket, akik csak valamilyen események, illetve munkájuk, feladatkörük kapcsán minősülnek közszereplőnek (például újságírók), de a magánéletben már nem.

Az általános szabályok szerint tilos az ártó szándékú kapcsolatfelvétel, így a kéretlen, szexuálisan tolakodó, valamint a tömeges (spamszerű) kapcsolatfelvétel, a közvetlen kommunikáció. Tilos mást a magántelefonszámának, lakcímének vagy e-mail-címének nyilvánosságra hozatalával fenyegetni, illetve tilos a szexuális cselekményekre felhívás és a szexuális tartalmú kommentek hozzáfűzése a bejegyzésekhez. Nemcsak a tényleges ártó kommunikáció tilalmazott, hanem a *bullying*ra, zaklatásra felhívás, valamint az erre utaló szándék kinyilvánítása. Tilos létrehozni olyan csoportokat, amelyeknek az a célja, hogy a résztvevők valamely személlyel összefüggésben ártalmas kommunikációt folytassanak, például halálát, betegségét kívánják. Láthatjuk, hogy a klasszikus zaklatással összehasonlítva markáns eltérések vannak a Meta szabályzatában. A kommunikáció akkor is bántalmazónak minősül, ha csak egy alkalommal történik, nincsen tehát szükség rendszerességre vagy ismétlődésre. Az ártó közlések pedig akkor is tiltottnak minősülnek, ha azok a sértettről szólnak, ám a kommunikációnak nem közvetlenül a sértett a címzettje: tehát amelyeket üzenőfalon, csoportokban, hozzászólásként tesznek közé.

A YouTube közösségi iránymutatásai szintén tiltják a zaklatásszerű tartalmak közzétételét. A platform szabályzata ugyanakkor nem ugyanazt érti zaklatáson, mint a magyar büntetőjog. Zaklatásnak minősül egyrészt más fenyegetése, rendszeres háborgatása, de a platform idesorolja a megszégyenítést és a védett tulajdonságon alapuló gyalázkodást is. A közösségi irányelvek által tilalmazott zaklatás ennélfogva a bántó, sértő közlések tág körét átfogja. Nem tilos azonban közzétenni sértő véleményt abban az esetben, ha az közszereplőkkel vagy a társadalom szempontjából

közérdekűnek minősülő eseményekkel kapcsolatos. Szintén nem tilos az ismeretterjesztés, megelőzés, illetve figyelemfelhívás céljából közzétenni ilyen tartalmakat.
Hasonlóan szélesen értelmezi a zaklatást az X (Twitter) is, ahol ugyanezek a magatartások jelennek meg zaklatás címszó alatt. A platform kifejezetten ebbe a kategóriába sorolja a szexuális tartalmú üzenetek és felvételek kéretlen terjesztését.

Tartalom-bűncselekmények

A tartalommal összefüggő bűncselekmények közös jellemzője, hogy esetükben a számítógép mint az elkövetés eszköze van jelen, és típusosan nagy nyilvánosság vagy mások előtt elkövethető bűncselekményekről van szó. A tartalom-bűncselekmény mint fogalom jogi kategória, hiszen a Cybercrime Egyezményben is megjelenik, noha a nemzeti jogrendszerek többsége – köztük a magyar jogrendszer – nem használja mint csoportosítási szempontot. A Cybercrime Egyezmény nem alkot külön fogalmat a tartalom-bűncselekmények *(content-related offences)* meghatározására, hanem a 3. cím alatt nevesíti azokat a cselekményeket, amelyek idetartoznak. A jogalkalmazó számára azonban fejtörést okozhat, hogy miért csak egy cselekmény, nevezetesen a gyermekpornográfia került az egyezmény e címe alá. Az egyezményhez fűzött kiegészítő jegyzőkönyv két további deliktumot sorol a tartalom-bűncselekmények körébe, ezek a rasszizmussal és az idegengyűlölettel kapcsolatos cselekmények. A Cybercrime Egyezmény a tartalom-bűncselekmények meghatározásával adós marad, és nem határolja le kellően azt a bűncselekményi kört, amelyek ebbe a kategóriába esnek, olybá tűnik tehát, hogy magunknak szükséges e fogalmat megkonstruálnunk. A Cybercrime Egyezmény mentségére legyen mondva, hogy az csak egy minimumlistát tartalmaz, soha nem kívánta tehát teljeskörűen meghatározni azokat a büntetendővé nyilvánítható cselekményeket, amelyek az online térben megjelennek. A tartalom-bűncselekmény mint fogalom nyelvtani értelmezése szerint feltételez egy olyan tartalmat (ami lehet akár szöveg, kép, hang, esetleg audiovizuális tartalom), amely akár elkészítésénél, akár közzétételénél fogva jogellenessé válik. Nem szükséges feltétel, hogy interneten történő nyilvánosságra hozatallal váljon jogellenessé a tartalom, már korábban, az elkészítéskor is az lehet,[396] gondoljunk például a gyermekek szexuális kizsákmányolását ábrázoló felvételekre, amelyeknek még a tartása is bűncselekmény. A Cybercrime Egyezményben nevesített egyetlen deliktumnál jóval tágabb az a bűncselekményi kör,

[396] Szentkuti–Szűts 2003.

amely tartalom-bűncselekménynek minősíthető. Idetartoznak az emberi becsületet és méltóságot sértő bűncselekmények, a köznyugalmat sértő bűncselekmények, valamint a tiltott pornográf felvétellel való visszaélés bűntette. Ezen cselekmények megjelenése főleg az internethez kapcsolható, ahol számtalan kép- és videómegosztó oldal mellett megtalálhatók széles nyilvánosságot biztosító közösségi oldalak, blogok, chatszobák, ahol a felhasználók nagy száma érheti el, töltheti le vagy akár teheti közzé a tiltott tartalmakat. A Btk. a IX. fejezet értelmező rendelkezései között a következőképpen határozza meg a nagy nyilvánosság fogalmát: nagy nyilvánosságon a bűncselekménynek a sajtótermék, médiaszolgáltatás, sokszorosítás vagy elektronikus hírközlő hálózaton való közzététel útján történő elkövetését is érteni kell. Tehát az interneten mint hálózaton elkövetett bűncselekmények esetében a nagy nyilvánosság előtti elkövetés megvalósul, aminek különös jelentősége van az olyan cselekmények esetén, ahol a nagy nyilvánosság előtti elkövetés is tényállási elem (például becsületsértésnél), illetve ahol a nagy nyilvánosság előtti elkövetéssel a bűncselekmény minősített esete állapítható meg (például rágalmazásnál).

Defamatorikus bűncselekmények az online térben

A defamatorikus bűncselekményeknek kiváló terepet nyújt az internet, ahol a viszonylagos névtelenség és a személyes kontaktus hiánya miatt nagyon könnyű sértésekkel vagdalkozni, vagy valakiről valótlanságokat állítani és terjeszteni. Klein Tamás felhívja a figyelmet arra, hogy az online kommunikáció jellemzője a vitastílus trágársága, a stílus alacsony szívonala azonban nem jelenti feltétlenül a tartalom jogellenességét.[397] Ítélkezési gyakorlatában a Fővárosi Törvényszék is azon az álláspontón van, hogy „a kulturált érintkezési formák kialakítása nem a büntetőjog feladata".[398] Ebből eredően nagyon nehéz megállapítani, hogy mi a sértő vagy bántó kommunikációnak az a szintje, amely már átlép egy bizonyos határt, és szankcionálandóvá válik. A Btk. defamatorikus bűncselekmények között szereplő deliktumai mindegyikének a jogi tárgya az emberi becsület, amelynek tartalmát a bírói gyakorlat határozta meg. A becsület egyrészt a társadalmi megbecsülést, másrészt az emberi méltóságot, vagyis az egyén tulajdonságairól, magatartásáról, személyes értékeiről kialakított társadalmi értékítéletet jelenti (BH2000.285). Tóth J. Zoltán szerint „a két sértett jogtárgy nehezen

[397] Klein 2016a: 83.

[398] Fővárosi Törvényszék Bf.10387/2013/7., Bf.6036/2015/15., Bf.7671/2015/5. és Bf.12455/2015/6. számú határozatok.

határolható el egymástól, mivel a jó hírnév sérelme tipikusan az egyén önbecsülését is érinti".[399] Az Alaptörvény Szabadság és felelősség cím alatt a VI. cikkben deklarálja az egyének jó hírnévhez való jogát: „(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák." A defamatorikus cselekmények passzív alanya természetes személy, jogi személy, továbbá jogi személyiséggel nem rendelkező, de konkrétan azonosítható személyösszesség is lehet. A bírósági gyakorlat szerint a büntetőjogi védelem megilleti azokat a személyösszességeket is, amelyeknek nincs jogképességük (BH2004.71). Békés Ádám kiemeli, hogy a defamatorikus bűncselekmények esetében vizsgált kérdések a véleménynyilvánítás szabadsága és az emberi méltóság határterületén fekszenek, így nemcsak azok büntetőjogi, hanem szabálysértési és polgári jogi aspektusait is érdemes számításba venni.[400] Mivel a sértettek számára a polgári jogi igényérvényesítés lehetősége is nyitott, felmerül a kérdés, hogy indokolt-e egyáltalán büntetőjogi szankcióval sújtani azokat, akik másról becsület csorbítására alkalmas tényt állítanak, vagy arra alkalmas kifejezést használnak. Sajó András a becsületsértés és a rágalmazás dekriminalizálását támogatja,[401] míg Halmai Gábor a büntetőjogi szankciórendszer felülvizsgálatát javasolja, amikor amellett érvel, hogy a jelenlegi rendszer lehetőséget ad a kettős jogi értékelésre.[402] A 2023-ban végbement Btk.-módosítás szintén a dekriminalizálás irányába mutat.

Rágalmazás

226. § (1) Aki valakiről más előtt a becsület csorbítására alkalmas tényt állít, híresztel, vagy ilyen tényre közvetlenül utaló kifejezést használ, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés két évig terjedő szabadságvesztés, ha a rágalmazást

a) aljas indokból vagy célból,

b) nagy nyilvánosság előtt, vagy

c) jelentős érdeksérelmet okozva

követik el.

399 Tóth 2017: 180.

400 Békés 2014: 380.

401 Sajó 2005: 3–6.

402 Halmai 2004: 87.

(3) Nem büntetendő rágalmazás miatt annak a cselekménye, aki az (1) bekezdésben meghatározottakat a közügyek szabad megvitatása körében sajtótermék vagy médiaszolgáltatás útján követi el, feltéve, hogy cselekménye nem irányul a sértett emberi méltóságának nyilvánvaló és súlyosan becsmérlő tagadására.

A rágalmazásnak háromféle elkövetési magatartása lehet: a becsület csorbítására alkalmas tény a) állítása b) híresztelése, valamint c) az ilyen tényre közvetlenül utaló kifejezés használata. A bírósági gyakorlat alapján a becsület csorbítására való alkalmasságot nem a sértett egyéni megítélése, hanem a társadalomban kialakult általános értékelés alapján kell megítélni (BH2000.285). A kommentár elkövetési helyként a más előtt történő elkövetést tartja számon, egyes álláspontok szerint azonban ez a fordulat „nem azt jelenti, hogy a cselekmény csak azon a fizikai helyen követhető el, ahol az elkövetővel a harmadik személy, akinek a tényközlés szól, együtt tartózkodik, hanem azt, hogy olyan módon követhető el, amelynek révén a közlésről egy a passzív alanytól különböző személy értesülhet".[403] Ez az állítás napjainkban különösen megállja a helyét, mivel a kommunikációnk jelentős része infokommunikációs technológia használatával, távollevők között zajlik, a rágalmazást pedig elektronikus hírközlő hálózat segítségével is el lehet követni.

Tényállítás minden olyan nyilatkozat és kijelentés, amely tartalma valamely múltban megtörtént vagy jelenben történő esemény, jelenség, illetve állapot (BH2009.135). A joggyakorlat számára az egyik legnagyobb nehézséget a tényközlések és értékítéletek elhatárolása jelenti. Noha a bírósági gyakorlat nem egységes a kérdésben, az alábbi megnyilvánulások az esetjogban tipikusan tényállításnak minősülnek:

- bűncselekménnyel vádolás,
- szabálysértési, fegyelmi eljárás megindításának alapjául szolgáló közlések,
- múltbeli magatartásra vonatkozó közlések, illetve
- személyes, de objektív alapon megítélhető tulajdonságra vonatkozó közlések.

A rágalmazásnak nem tényállási eleme a közlés valósága, tehát annak valósága vagy valótlansága a bíróság számára közömbös, elegendő, ha az elkövető tudata átfogja az állítás becsület csorbítására alkalmas voltát (BH1990.540).

A rágalmazás nemcsak tény állításával, hanem híreszteléssel is megvalósulhat. Tény híresztelése egy más személy korábbi tényállításának továbbítása, illetve terjesztése, például újságcikk interneten történő ismételt megjelentetése (BH2012.143). Ilyennek

403 Halmai 2004: 111.

minősülhet egy online cikk közösségimédia-platformon történő megosztása, de akár egy közösségimédia-platformon közzétett cikk vagy más tartalom továbbosztása is. A Gyulai Törvényszék egyik bírája egy interjúban elmondta, hogy az emberek hajlamosak gyalázkodó tartalmakat megosztani online, holott „a becsület csorbítására alkalmas üzenet első közlője és sokadik megismétlője egyaránt büntethető,"[404] tehát a más által közzétett tartalom megosztása nem mentesíti az elkövetőt. A magyar bíróságok szerint a büntetőjogi felelősség szempontjából nincs jelentősége annak, hogy az elkövető a híresztelt tény valósága tekintetében állást foglalt-e (BH2012.143). A közösségimédia-platformokon megosztott tartalmak esetében azonban a kontextusnak lehet jelentősége, hiszen a bíróság számára nem indifferens a közlő viszonyulása a megosztott információhoz. Ha a közlő az információt eleve tényfeltáró, leleplező, elítélő magyarázattal, véleménnyel tette közzé, a rágalmazás nem megállapítható.

Ahhoz, hogy a rágalmazás megállapítható legyen, a közlésnek elég konkrétnak kell lennie ahhoz, hogy a befogadók számára egyértelmű legyen, hogy ki és milyen cselekményt követett el. Ugyan pontos, tényállás szerinti megnevezések használata nem megkövetelt, múltbeli eseményekre vonatkozó tényközlésnek csak a konkrétan megnevezett, időben, térben beazonosítható eseményekre történő utalások minősülhetnek. Ugyanígy a közlésnek meg kell neveznie azt a személyt, akire vonatkozóan a tényt állítják, legalábbis a közlésből világosan ki kell tűnnie, ki az, akire vonatkozik. „Emiatt például egy *nickname*-re vonatkozó tényállítást rágalmazásnak nem lehet tekinteni. Ezt azzal indokolhatjuk, hogy a harmadik személy előtt egy számára nem egyértelműen azonosítható személyre tett kijelentés »hangzik el«."[405]

A rágalmazás minősített esetei az aljas indokból vagy célból történő, a nagy nyilvánosság előtt történő, illetve a jelentős érdeksérelmet okozó elkövetés. Aljas indok vagy cél lehet a bosszúból történő elkövetés, illetve választási kampányban a másik fél lejáratására törekvés (EBH2014.B.16). Nagy nyilvánosság előtt történik az elkövetés, ha a közönség, a tudomásszerzők száma nem határozható meg pontosan, így az interneten történő közzététel (például közösségimédia-platformon) nagy nyilvánosság előtti közlésnek minősül. A magánlevelezés, zárt csatornán történő csoportos kommunikáció (például zárt fórum, vagy azonnali üzenetküldő applikációk, mint a WhatsApp) ellenben nem minősül nagy nyilvánosságnak. A jelentős érdeksérelem fogalmával korábban a személyes adattal visszaélésnél foglalkoztam, így az ott leírtakat nem ismétlem.

[404] Rágalmazás és becsületsértés a közösségi médiában – Beszélgetés Borombós Anitával, a Gyulai Törvényszék bírájával 2018.

[405] Szentkuti–Szűts 2003.

Hazai joggyakorlat

A becsület csorbítására alkalmas tényállítás nagy nyilvánosság előtti elkövetésének megállapítására lehet alkalmas, ezért a rágalmazás vétségének megállapíthatósága szempontjából tényállásszerű magatartás különböző internetes felületeken annak nyilvános közlése, hogy az egyik egyetem hallgatói önkormányzatának vezetője – e tevékenységének gyakorlása során – részt vett egy jelentős tárgyi súlyú nemi erkölcs elleni bűncselekmény eltussolásában, illetve közpénzt tulajdonított el (EBH2019.B.2).

Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése és nyilvánosságra hozatala

2013-ban két új tényállással is bővült a Btk., ezek a becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése, valamint annak nyilvánosságra hozatala.

226/A. § (1) Aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt készít, ha más bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
226/B. § (1) Aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt hozzáférhetővé tesz, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a bűncselekményt
a) nagy nyilvánosság előtt, vagy
b) jelentős érdeksérelmet okozva követik el.

Ezeknek a cselekményeknek a passzív alanya ugyanaz, mint a rágalmazásé. Elkövetési magatartás a 226/A. § esetében hamis, hamisított vagy valótlan tartalmú hang- és/vagy képfelvétel készítése, a 226/B. § esetében ezek hozzáférhetővé tétele. A valótlan tartalmú felvétel bármilyen formában készülhet, a bűncselekmény akkor valósul meg, ha az a becsület csorbítására objektíve alkalmas. Az online világban a bárki számára hozzáférhető eszközökkel és programokkal nagyon egyszerű képeket, felvételeket meghamisítani, azokat összemontírozni úgy, hogy azok valótlan szituációkat megtörténtként mutassanak be. A hamisított felvételeket a mesterségesintelligencia-alapú applikációk egészen új szintre emelték. Az algoritmus által kreált hamis felvételek (az úgynevezett *deepfake* felvételek) létezése akkor robbant be a köztudatba, amikor

a YouTube-ra felkerült egy felvétel Barack Obama elnök egyik beszédéről, amelyet a valóságban soha nem mondott el.[406] Az ilyen felvételeknek a készítése és a nyilvánosságra hozatala Magyarországon csak abban az esetben bűncselekmény, ha készítésének célja más becsületének csorbítása. Az elkövetési magatartás a második esetben a nyilvánosságra hozatal, de csak abban az esetben minősül a tett büntetendőnek, ha az elkövető tisztában volt a felvétel valótlan voltával. Mivel mind a készítés, mind a nyilvánosságra hozatal célzatos, ezek a cselekmények csak egyenes szándékkal valósíthatók meg.

Hazai joggyakorlat

E tényállás megszövegezését azért találta szükségesnek a jogalkotó, mert a 2013-as bajai időközi választás során egy népszerű online hírportálra felkerült egy felvétel, amelyen egy közvetítőnek tűnő személy pénzt ad át a helyi lakosoknak, valamint pénzt és tűzifát ígér nekik, ha a kormánypárt jelöltjére szavaznak. A felvételről kiderült, hogy hamisítvány, amelyet egy baloldali párt készített és tett közzé. A párt később azzal védekezett, hogy a választási csalást bemutató felvétel valójában oktatóvideónak készült, és nem egy valós szituációt jelenít meg, addigra azonban a felvétel elterjedt, és hátrányosan befolyásolta mind az érintett jelölt megítélését, mind a választóknak a választási eljárásba vetett bizalmát.

Az új deliktum bevezetését nem követték tömegesen elmarasztaló ítéletek, sőt az OBH által működtetett bírósági határozatok tárában 2022-ig egyetlen olyan ítélet sem található, amelyben ezt a tényállást állapította meg a bíróság. Ennek vélhetően az az oka, hogy a hamis hang- vagy képfelvételek ártó szándékú nyilvánosságra hozatala eseteiben a Btk. egyéb tényállásai által biztosított védelem elégséges; a rágalmazás, a becsületsértés, valamint a személyes adattal visszaélés tényállásai mind alkalmazhatók, amennyiben a felvételek nyilvánosságra kerülnek.

Gyakorlati szempontból érdekes lehet a különböző politikai mémek helyzete, amelyek egyes közszereplő politikusokat gyakran ábrázolnak pikírt, gunyoros módon, a humoros jelleg mellett az érintettre nézve kimondottan becsület csorbítására alkalmas módon. Az internetes „népi kultúra" e manifesztációja miatt azonban nem indultak tömegesen nyomozások és büntetőperek, sőt a hazai mémkultúra jelenleg is virágzik, így talán nagy bizonyossággal mondhatjuk, hogy a jogalkalmazónak nem célja, hogy az ilyen felvételek ellen fellépjen.

406 Vincent 2018.

Az elkészült, de nem közzétett felvételek esetében a bizonyítás eleve kétséges, hiszen az ilyen felvételek elkészültéről nem biztos, hogy bárki tudomást szerez, álláspontom szerint a pusztán magáncélból készült ilyen jellegű felvételek esetén nem is célszerű azonnal a büntetőjog eszközrendszeréhez nyúlni.

Becsületsértés

A becsületsértésről a Btk. 227. §-a rendelkezik:

> 227. § (1) Aki a 226. §-ban meghatározottakon kívül mással szemben
> a) a sértett munkakörének ellátásával, közmegbízatásának teljesítésével vagy közérdekű tevékenységével összefüggésben vagy
> b) nagy nyilvánosság előtt
> a becsület csorbítására alkalmas kifejezést használ, vagy egyéb ilyen cselekményt követ el, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
> (2) Az (1) bekezdés szerint büntetendő, aki a becsületsértést tettlegesen követi el.
> (3) Nem büntetendő becsületsértés miatt annak a cselekménye, aki az (1) bekezdésben meghatározottakat a közügyek szabad megvitatása körében sajtótermék vagy médiaszolgáltatás útján követi el, feltéve, hogy cselekménye nem irányul a sértett emberi méltóságának nyilvánvaló és súlyosan becsmérlő tagadására.

A becsületsértés a rágalmazással szubszidiárius viszonyban áll, így a becsületsértés a rágalmazás tényállásába beolvad, ha ez utóbbi is megállapítható. A törvény a becsületsértésnek három elkövetési magatartását ismeri:

1. becsület csorbítására alkalmas kifejezés használata, amely lehet minden olyan kifejezés, ami gyalázkodó, gúnyoló vagy becsmérlő jellegénél fogva sérti az emberi méltóságot;
2. becsület csorbítására alkalmas cselekmény elkövetése; továbbá
3. tettleges becsületsértés (például arc meglegyintése, köpés).

Utóbbi két magatartás az online térben kevéssé releváns, ezért ezeket részletesebben nem tárgyalom. Néhány szót azonban érdemes annak szentelni, hogy mi minősül becsület csorbítására alkalmas kifejezésnek, hiszen a rágalmazás tényállásában szereplő becsület csorbítására alkalmas tényállításhoz képest jelen esetben sokkal szubjektívebb, ezáltal színesebb kategóriáról van szó. Ez esetben is irányadóak a rágalmazásnál

leírtak, miszerint a becsület csobítására alkalmasságnál nem a sértett saját megítélése irányadó, hanem az, hogy az adott kifejezés általában véve, objektíve alkalmas-e arra, hogy valakinek a becsületét csorbítsa.

Hazai joggyakorlat

Egy ügyben a vádlott védekezésében arra hivatkozott, hogy napjainkban a „köcsögözés" már nem minősül sértőnek, hiszen a társadalomban a köcsög szó már-már annyira bevett kifejezés, hogy nélkülözi a sértő jelleget. Az érvelést a bíróság nem fogadta el, és kimondta, hogy az ilyen trágár, gyalázkodó kifejezések használata nem felel meg a társadalomban szokásos érintkezési formák minimumszintjének sem (Pécsi Ítélőtábla, Bhar.75/2014/3).

A bírói gyakorlat a becsületsértő kifejezések megítélésében sem egységes, jellemzően azonban a társadalomban szokásos érintkezési formák minimumszintjének sem megfelelő megnyilvánulások becsületsértők. „Minimumszint" alatti értintkezési forma a gyalázkodást tartalmazó, emberi méltóságot sértő közlésforma, az egyszerű, nem trágár formában megfogalmazott kritika, bírálat tehát többnyire nem becsületsértő. Az emberi méltóságot sértik az érintett személy szellemi képességeire, jellembeli tulajdonságaira, szokásaira vagy testalkatára vonatkozó sértő kifejezések, amelyek rendszerint durva általánosítás formájában kifejezett, megvető, lealacsonyító értékítéletet tartalmaznak (például köcsög, buzi, kurva, pedofil, tetves, púpos).

A kulturált érintkezési formák kialakítása ugyanakkor nem a büntetőjog feladata, így a szitkozódás, szidalmazás, még ha durva formában fogalmazzák is meg, nem feltétlenül eredményeznek büntetőjogi felelősségre vonást, mivel erősen negatív hangvételük ellenére is mellőzik a büntetőjogi értelemben vett becsület csorbítására alkalmasságot. A kulturált emberi magatartástól idegen a durva tapintatlanság, a neveletlenség, a szitkozódás, az ízléstelenség, a gúnyolódás, de az olyan viselkedési formák, amelyek társadalmilag és etikailag elítélendők, nem feltétlenül igénylik a büntetőjogi eszközök igénybevételét.

Hazai joggyakorlat

Az olyan klasszikus cigány átkokat, mint a „rák egye ki a beledet" nem minősítette becsületsértőnek a bíróság. „Az átok azonban sem az érintett személy becsületére, jellemére, sem az egyes tulajdonságaira vonatkozó jellemzést nem foglal magában, ezért büntetőeljárás tárgyát sem képezheti" (Fővárosi Ítélőtábla, Bhar.60/2014/4).

Valakit fasisztának vagy kommunistának nevezni – konkrét, az érintettre vonatkoztatható események, cselekmények említése nélkül – nem tényállítás, hanem olyan értékítélet, amely sem a rágalmazás, sem pedig a becsületsértés szempontjából nem tényállásszerű, ezért bűncselekményt nem valósít meg (EBH2017.B.17).

A becsületsértés két esetben minősül a Btk. szerinti vétségnek, akkor, ha a közlés nagy nyilvánosság előtt történik, vagy akkor, ha a közlés a sértett munkakörével összefüggésben hangzik el. A nagy nyilvánosságra a rágalmazás körében már leírtak irányadók. A munkakörrel összefüggésben elhangzott, lealacsonyító, becsmérlő és az emberi méltóságot durván sértő kifejezések esetében nemcsak a sértett által végzett munka ellátásának módjával, annak minőségével kapcsolatos kijelentések (például alkalmatlan, rossz, kókler) alapozzák meg a becsületsértést, hanem bármilyen, a sértett munkakörének ellátásával, közmegbízatásának teljesítése során elhangzó lealacsonyító kifejezés (például dagadt kurva).

Hazai joggyakorlat

Becsületsértőnek minősítette a bíróság egy társadalmi szervezet képviselőjének azon internetes honlapon közzétett írását, amelyben a helyi csapadékelvezetéssel foglalkozó cég egyik munkatársát bírálta, hiszen tudomása szerint a sértettet a korábbi munkahelyéről azért bocsátották el, mert az képtelen „az ügyfelekkel megfelelően, emberségesen beszélni és viselkedni" (Fővárosi Ítélőtábla, Bhar.186/2018/8). Szintén becsületsértő valakit a munkakörével összefüggésben a „botcsinálta", „hazug királyfi" (Fővárosi Ítélőtábla, Bhar.136/2018/6), a „lakosságellenes", „kegyetlen", „embertelen", „mindig buta", valamint az „alkalmatlan" (Kúria, Bfv.433/2019/8) jelzőkkel illetni. A munkakörrel összefüggésben elkövetett becsületsértés sértettjei a fizikai és az online térben gyakran rendőrök, az intézkedések érintettjei gyakran reagálnak indulatosan az eljárások során. A bírósági gyakorlat egyértelműen abba az irányba mutat, hogy a rendőröket támadó, sértő, trágár kifejezések a munkakörrel összefüggésben elkövetett becsületsértésnek minősülnek. A BH2019.68 ügyben a Kúria kifejezetten kimondta, hogy a rendőrök intézkedésével összefüggésben elhangzott „kurva anyátok" és „Orbán kutyái vagytok" kifejezések sértik az emberi méltóságot, mivel az emberi státuszt nyilvánvalóan és súlyosan becsmérlik, ekként pedig becsület csorbítására alkalmasak.

Említés szintjén fel kell hívni a figyelmet arra, hogy a becsületsértésnek nemcsak vétségi, hanem szabálysértési alakzata is van, amelyről a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi

II. törvény (Szabstv.) szól. Amennyiben a becsületsértő kifejezés használata nem a sértett munkakörével összefüggésben történik, illetve a közlés nem nagy nyilvánosság előtt hangzik el, a becsületsértés szabálysértése megállapításának van helye. Online környezetben a szabálysértési alakzat jelentősége viszonylag csekély, hiszen a közösségi platformokon, videómegosztókon közzétett felvételek elvben korlátlan számú személyt elérhetnek, így a nagy nyilvánosság követelménye minden esetben megvalósul. Szabálysértés valósulhat meg ellenben az olyan számfüggetlen személyközi hírközlési szolgáltatást nyújtó szolgáltatók szolgáltatásain keresztül, amelyek akár végpontok közötti titkosítással, akár anélkül lehetővé teszik a privát kommunikációt (WhatsApp, Viber, Messenger).

Köznyugalom elleni bűncselekmények az online térben

Számítógépes hálózaton, az internet felhasználásával tartalomközléssel megvalósuló bűncselekmények a köznyugalom elleni bűncselekmények, így a háborús uszítás (Btk. 331. §), a közösség elleni uszítás (Btk. 332. §), a nemzeti jelkép megsértése (Btk. 334. § – például magyar zászlók égetését bemutató videófájl), tiltott önkényuralmi jelképek használata (Btk. 335. §) és a közveszéllyel fenyegetés (Btk. 338. §).

Háborús uszítás

> 331. § (1) Aki nagy nyilvánosság előtt háborúra uszít, vagy egyébként háborús hírverést folytat, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.
> (2) Az (1) bekezdés szerint büntetendő, ha súlyosabb bűncselekmény nem valósul meg, aki nagy nyilvánosság előtt a terrorizmus támogatására uszít, vagy egyébként a terrorizmust támogató hírverést folytat.

A háborús uszítás tényállásának megalkotásával a magyar jogalkotó nemzetközi jogból eredő kötelezettségének tett eleget. A *Polgári és politikai jogok nemzetközi egyezségokmánya* (PPJNE)[407] 20. cikkének 1. pontja előírja a részes államok számára, hogy törvényben tiltsák a háborús propaganda minden formáját. A Btk. 331. §-a

[407] 1976. évi 8. törvényerejű rendelet az Egyesült Nemzetek Közgyűlése XXI. ülésszakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről.

a 2017/541. irányelv átültetésével összefüggésben módosult, így ma már tiltja a terrorizmus támogatására uszítást is. Mindkét tényállás esetében a jogi tárgy a háborús és terrorizmussal fenyegetéstől mentes köznyugalom. Mind a háborúval, mind a terrorizmussal összefüggő tényállásnak két alakzata van, az uszítás, illetve a hírverés folytatása. A Btk. kommentárja szerint[408] a háborúra uszítás alatt a háborúra való nyílt felhívást értjük, ami olyan felbujtásszerű cselekmény, amelynek célja mások érzelmeinek befolyásolása. A háborús hírverés az uszításnál tágabb körű, kiterjed a háborús propaganda minden formájára, így a háborúról szóló pozitív megnyilvánulásokra is. A terrorizmus támogatására uszítás jellegét tekintve szubszidiárius cselekmény, amelynek az elkövetése akkor állapítható meg, ha más súlyosabb cselekmény nem valósul meg. Magyarországon a háborús uszítás tényállásával kapcsolatban nem beszélhetünk kiterjedt joggyakorlatról, a 2014–2022 közötti időszakban a *Bírósági Határozatok Gyűjteménye* egyetlen háborús uszítással kapcsolatos esetet sem tartalmazott.

Hazai joggyakorlat

2022 augusztusában a Pest Megyei Főügyészség háborús uszítás miatt emelt vádat egy magyar–algír férfi ellen, aki egy németországi zenemegosztó platformra töltött fel az Iszlám Állam sajtóirodái által előállított buzdító dalokat, úgynevezett *naseed*eket. A dalok az Iszlám Államot dicsőítették, és közvetetten terrorista módszerek alkalmazására buzdítottak. A vádiratban az ügyészség azzal érvelt, hogy a közösségi médiában történő megosztás kimeríti a nagy nyilvánosság fogalmát, az egyik buzdító éneket 733 felhasználó lájkolta. Az ügyben 2023 januárjában született elsőfokú ítélet, amely a kézirat lezárásakor még nem volt jogerős (Az Iszlám Államot dicsőítő propagandát terjesztett – a Pest Megyei Főügyészség sajtóközleménye 2022).

Európában hosszú évekig béke honolt, így hazánkban nem volt jellemző a háborús propaganda a különböző internetes platformokon. Az elmúlt években sokat változott a világ. A 2022-ben kitört orosz–ukrán háború, amelynek a hatásait szomszédos országként Magyarország is igen erőteljesen megérezte, e tekintetben is hozott változást: a hétköznapok felkapott témája lett a háború, amelyben szakértőktől a laikus állampolgárokig mindenki állást foglalt. Jogosan merül fel tehát a kérdés, hogy háborús uszítást követ-e el az, aki Magyarország háborúba lépését szorgalmazza, amellett foglal állást, hogy Magyarország küldjön katonákat a frontvonalra, vagy éppen támogatja, hogy az orosz háborús propagandát közvetítő televíziócsatornák, mint az RTR Planeta

[408] Mezőlaki 2019: 609–651.

szabadon sugározhassanak? E tekintetben a gyűlöletbeszéd kapcsán elemzett uszítás kifejezés adhat támpontot (lásd a következő pontban). A hazai alkotmánybírósági gyakorlat alapján ugyanis az uszítás olyan erőteljes megnyilvánulás, amely nem puszta nyomatékos véleménynyilvánítás, hanem mások érzelmi világát, gondolkodásmódját oly mértékben befolyásolni képes közlés, amely a befogadót akár erőszakos cselekvésre is sarkallhatja. A háborúval, illetve Magyarország abban játszott szerepével kapcsolatban az egyszerű véleménynyilvánítás sem most, sem a jövőben nem minősül majd büntetőjogilag szankcionálandó cselekedetnek, akkor sem, ha a véleménynyilvánítás egy esetleg heves vita közepette történik.

Közösség elleni uszítás

332. § Aki nagy nyilvánosság előtt
- a) a magyar nemzet ellen,
- b) valamely nemzeti, etnikai, faji, vallási csoport, illetve annak tagja ellen, vagy
- c) a lakosság egyes csoportjai, illetve azok tagjai ellen – különösen fogyatékosságra, nemi identitásra, szexuális irányultságra tekintettel – erőszakra vagy gyűlöletre uszít, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

A közösség elleni uszítás büntető törvénykönyvi tényállása bizonyos társadalmi csoportoknak, illetve azok emberi méltóságának védelmét teremti meg, amellyel a jogalkotó részben nemzetközi kötelezettségben foglalt, részben az Alaptörvényben meghatározott védelmi kötelezettségének tesz eleget. A PPJNE 20. cikkének 2. pontja a részes államok kötelezettségévé teszi, hogy tiltsák a nemzeti, faji vagy vallási gyűlölet bármilyen hirdetését, amely megkülönböztetésre, ellenségeskedésre vagy erőszakra izgat. Az Alaptörvény IX. cikke ugyanis kimondja, hogy „a véleménynyilvánítás szabadságának a gyakorlása nem irányulhat a magyar nemzet, a nemzeti, etnikai, faji vagy vallási közösségek méltóságának a megsértésére. Az ilyen közösséghez tartozó személyek – törvényben meghatározottak szerint – jogosultak a közösséget sértő véleménynyilvánítás ellen, emberi méltóságuk megsértése miatt igényeiket bíróság előtt érvényesíteni."

Az elkövetési magatartás a gyűlöletre uszítás, amely mint közlés szorosan kapcsolódik a véleménynyilvánítás szabadságához, így sok elméleti és gyakorlati konfliktus fakad abból, hogy hol húzódik a korlátozhatóság határa. Az Alkotmánybíróság több határozatában is értelmezte a gyűlöletre uszítás és a véleménynyilvánítás szabadságának

viszonyát. A 30/1992. (V. 26.) AB határozat fektette le a véleménynyilvánítás büntetőjogi korlátozásának alapjait. A testület e határozatában megsemmisítette az 1989-es Btk. gyalázkodás tényállását, mivel annak nem volt eleme az elhangzott közlés köznyugalom megzavarására alkalmassága, az alapjog-korlátozáshoz pedig nem találta elegendőnek az elvont, feltételezett veszély okozását. A testület úgy foglalt állást, hogy önmagában a felháborító, gyalázkodó kifejezések nem indokolják a szólásszabadság büntetőjogi eszközökkel történő korlátozását. A 30/1992. (V. 26.) AB határozatban a testület úgy foglalt állást, hogy a vélemény mindaddig szabadon kinyilvánítható, amíg nem csap át gyűlöletre uszításba, vagyis „a véleményt annak érték- és igazságtartalmára tekintet nélkül"[409] védelem illeti meg, és csak igen szűk körben – más alapjog vagy alkotmányos cél érdekében[410] – korlátozható. A testület a gyűlöletre uszítás büntetőjogi eszközökkel való korlátozását már alkotmányosnak találta. Az Alkotmánybíróság megjegyezte, hogy az egyes csoportok elleni gyűlöletkeltés „alkalmas a társadalmi feszültségek kiélezésére, a társadalmi harmónia és béke megzavarására […] a társadalom egyes csoportja közötti erőszakos összeütközésekre".[411] A gyűlöletre uszító vélemények védelme ennélfogva ellentmondana más alapvető jogok és alkotmányos célok érvényesülésének. Az Alkotmánybíróság e határozatában foglalkozott a gyűlöletre uszítás, illetve a korábbi Btk. szóhasználata szerinti „izgatás" meghatározásával is, és megállapította, hogy ez esetben nem csupán kedvezőtlen, sértő vélemények kinyilvánításáról van szó, hanem olyan lázongó kifakadásokról, „amelyek alkalmasak arra, hogy az emberek nagyobb tömegében a szenvedélyeket olyan magas fokra lobbantsák, amelyből gyűlölet keletkezvén, a társadalmi rend és béke megzavarására vezethet". Az izgatás ennélfogva nem terjed ki a bírálatra, a helytelenítésre vagy a kifogásolásra.

A gyűlöletre uszítás kapcsán a testület azt is megjegyezte, hogy a gyalázkodással szemben a köznyugalom megzavarásának intenzitása egy bizonyos mérték fölött indokolja a véleménynyilvánítás korlátozását, valamint azt, hogy a korlátozást ez esetben az is indokolttá teszi, hogy a cselekmény alanyi (egyéni) jogot veszélyeztet. Az ABH ezen megállapításának értelmezéséről azóta sem alakult ki egységes álláspont. Koltay András három csoportra osztja a tárgyban kialakult szakmai álláspontokat.[412] Az értelmezések első csoportját azok az álláspontok képezik, amelyek az Egyesült

409 V/6. pont.
410 II/2.2. pont.
411 IV/1. pont.
412 Koltay 2013: 32.

Államokban alkalmazott nyilvánvaló és közvetlen veszély *(clear and present danger)* doktrínájának meghonosításaként tekintenek az Alkotmánybíróság soraira. Eszerint azokban az esetekben indokolt a büntetőjogi fenyegetettség, amelyekben a közlés alkalmas arra, hogy nyilvánvalóan és közvetlen módon eredményezze a köznyugalom vagy egyének jogainak sérelmét.[413] A második csoportot azok az álláspontok képezik, amelyek szerint az ABH nem vezeti be az amerikai nyilvánvaló és közvetlen veszély elvét, azonban a korlátozáshoz szükségesnek tartják, hogy a vélemény nyomán tényleges és valós veszély keletkezzen.[414] Az értelmezések harmadik csoportját a Koltay András által a büntetőjog „tradicionalista" híveinek nevezett szerzők álláspontjai képezik, akik elutasítják a nyilvánvaló és közvetlen veszély doktrína alkalmazását, és akik szerint immateriális bűncselekmény révén a tényállásszerűséghez elegendő a közlés gyűlölet felkeltésére való alkalmassága.[415]

Hazai joggyakorlat

Folytatólagosan elkövetett közösség elleni uszítás bűntettében találta bűnösnek a Debreceni Ítélőtábla azt a terheltet, aki a beszédében és honlapján veszélyesnek jelölte meg a zsidóságot, Izrael államot, Magyarország szabadkőműves és liberális beállítottságú csoportjait, valamint a homoszexuálisokat, kinyilvánította, hogy ezeknek a szerveződéseknek a célja Magyarország leigázása, megsemmisítése. Narratívájában gyakran jelent meg, hogy a megnevezett csoportok fenyegetést jelentenek: „ránk támadnak, elpusztítanak, megszállnak, leigáznak, veszélyt jelentenek, bennünket gyilkolnak". Az általa vélt veszélyekre történő figyelemfelhívás mellett kommunikációjában gyakran buzdított erőszakos cselekményekre is, beszédeiben és írásaiban gyakran jelentek meg olyan elemek, mint a „harc", „csapat", „sereg", „küzdelem", „akasztófa" „szégyenfa", továbbá hangot adott azon álláspontjának, hogy küzdeni kell. A harmadfokon eljáró bíróság nemcsak az elhangzott kifejezések jelentéstartalmát vizsgálta, hanem figyelembe vette a megformált szövegkörnyezetet és a dramaturgiát is, majd megállapította, hogy a heves, érzelmes közlésmód alkalmas arra, hogy a szenvedélyeket felszítsa (Debreceni Ítélőtábla, Bhar.I.625/2020/32).

413 Ezt az álláspontot képviseli többek között Molnár Péter (Molnár 2001), Kis János és Sólyom László (Kis–Sólyom 2003).

414 Idetartozik Sólyom László (Sólyom 2001), illetve Török Bernát (Török 2013).

415 Ennek az álláspontnak a képviselői között találjuk Szeder Gyulát (Szeder 2002: 1), Bócz Endrét és Györgyi Kálmánt (Bócz–Györgyi 2003), továbbá Vaskuti Andrást (Vaskuti 2005).

A nemzetiszocialista vagy kommunista rendszerek bűneinek nyilvános tagadása, nemzeti jelkép megsértése, önkényuralmi jelkép használata

A nemzetiszocialista vagy kommunista rendszerek bűneinek nyilvános tagadása

Btk. 333. § Aki nagy nyilvánosság előtt a nemzetiszocialista vagy kommunista rendszerek által elkövetett népirtás vagy más, emberiesség elleni cselekmények tényét tagadja, kétségbe vonja, jelentéktelen színben tünteti fel, vagy azokat igazolni törekszik, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

Nemzeti jelkép megsértése

334. § Aki nagy nyilvánosság előtt Magyarország himnuszát, zászlaját, címerét vagy a Szent Koronát sértő vagy lealacsonyító kifejezést használ, illetve azokat más módon meggyalázza, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

Önkényuralmi jelkép használata

335. § Aki horogkeresztet, SS-jelvényt, nyilaskeresztet, sarló-kalapácsot, ötágú vöröscsillagot vagy ezeket ábrázoló jelképet a köznyugalom megzavarására alkalmas – különösen az önkényuralmi rendszerek áldozatainak emberi méltóságát vagy kegyeleti jogát sértő – módon

a) terjeszt,
b) nagy nyilvánosság előtt használ, vagy
c) közszemlére tesz,

ha súlyosabb bűncselekmény nem valósul meg, vétség miatt elzárással büntetendő.

A köznyugalmat sértő bűncselekmények közé tartozik a nemzetiszocialista vagy kommunista rendszerek bűneinek nyilvános tagadása, a nemzeti jelkép megsértése, valamint az önkényuralmi jelkép használata.

A köznyugalom sérelmét a nyilvános tagadás esetében a nácizmus és a kommunizmus áldozatai méltóságának nagy nyilvánosság előtti megsértése okozza. Nemzeti jelkép megsértése esetén az alkotmányos jelképek, az állami szuverenitás külső megjelenési formáinak megsértése támadja a köznyugalmat, önkényuralmi jelkép használata esetén pedig a köznyugalom a demokratikus államrend zavartalan működésében megnyilvánuló közhangulat megzavarása révén sérül. A nemzetiszocialista vagy kommunista rendszerek bűnei nyilvános tagadásának nincs elkövetési tárgya, a másik

két deliktum esetében az elkövetési tárgyak meghatározott jelképek, szimbólumok, abban az esetben is, ha azok nem heraldikai pontossággal követik a jelképek hivatalos formáját. Nemzeti jelkép esetén az elkövetés tárgyai a Magyarország Alaptörvényének I) cikkében meghatározott jelképek (himnusz, címer, zászló), önkényuralmi jelkép használata esetén pedig a horogkereszt, SS-jelvény, nyilaskereszt, sarló-kalapács, ötágú vörös csillag vagy ezeket ábrázoló jelkép.

A nyilvános tagadás négyféle elkövetési magatartással valósítható meg: tagadással, kétségbe vonással, jelentéktelen színben való feltüntetésével, valamint igazolására törekvéssel. Az első elkövetési magatartás a tagadás, ami „a megtörtént valós események meg nem történtként való feltüntetése", a második magatartás a kétségbe vonás, ami „olyan valós vagy valótlan kifejezések használata, amely a valós történeti események megtörténte iránt bizonytalanságot kíván ébreszteni", a harmadik magatartás a jelentéktelen színben való feltüntetés, ami „az alapbűncselekmények súlyának, hatásának elbagatellizálása", míg a negyedik magatartás, az igazolásra törekvés során az elkövető „az alapbűncselekmények elkövetését indokolttá, elfogadhatóvá, szükségessé próbálja […] tenni".[416]

Hazai joggyakorlat

Folytatólagosan elkövetett közösség elleni uszítás bűntettében találta bűnösnek a Kúria azt a terheltet, aki e-mail-üzenetben és közösségi oldalán tett közzé olyan gondolatokat, amelyek révén a Hitler által elkövetett tetteket igazolni törekedett, köztük a következő sorokat: „Jó lenne egy újabb Hitler, aki nemcsak égetéssel próbálkozna, hanem egy atombombát is dobna közéjük, csak először hajtsák őket össze egy olyan helyre, ahol később szobrot lehetne állítani és ünnepeket tartani, hogy itt tűnt el a zsidó elnyomás!" A megfogalmazásból a bíróság arra következtetett, hogy a terhelt egy múltban bekövetkezett esemény társadalompolitikai szükségessége mellett érvel, s mi több, hasonló módszerek alkalmazását a jelenkorban is kívánatosnak tartja. A bejegyzés eljutott a nagy nyilvánossághoz, hiszen a terhelt egy felsőoktatási intézmény munkatársaként jelentős számú személyt elért közösségimédia-fiókján keresztül. A bejegyzést zömében elítélően fogadta a közönség, volt, aki azt javasolta, hogy célszerű lenne, „ha kipróbálná magán a művész úr a hatást, aztán nyilatkozna a tapasztalatokról". (Kúria, Bfv.III.539/2021/31.)

A nemzeti jelkép megsértése kétféle elkövetési magatartással valósítható meg: sértő vagy lealacsonyító kifejezés használatával, valamint meggyalázással. Sértő vagy lealacsonyító

416 Mezőlaki 2019: 609–651.

kifejezésnek minősülnek az olyan szóbeli becsmérlő, megvető, gyalázkodó megnyilvánulások, amelyek az adott nemzeti jelkép méltóságához fűződő társadalmilag kialakult érzületet sértik,[417] míg a meggyalázás olyan magatartás, amely a nemzeti jelképhez fűződő nemzeti önérzetet sérti (például zászló elégetése, címer bemocskolása, a Himnusz trágár előadása stb.).[418]

Az önkényuralmi jelkép használata háromféle magatartással valósítható meg: terjesztéssel, nagy nyilvánosság előtti használattal és közszemlére tétellel. A magatartás tényállásszerűségéhez hozzátartozik, hogy az a köznyugalom megzavarására alkalmas legyen.

A tényállásszerű magatartás megállapításának feltétele mindhárom tárgyalt deliktum esetében, hogy az elkövetés nagy nyilvánosság előtt valósuljon meg. A nagy nyilvánosság kritériuma a bírósági gyakorlat szerint akkor is megvalósul, ha „fennáll annak a reális lehetősége, hogy a bűncselekményről előre meg nem határozható számú személy szerezzen tudomást" (BH1981.223). Az internetes tartalomközléssel történő elkövetés például nagy nyilvánosságnak minősülhet. Online környezetben különösen problémás lehet e köznyugalmat sértő bűncselekmények elkövetőinek felderítése, valamint a jogsértés megszüntetésének kikényszerítése. A virtuális tér nagyobb szolgáltatói többnyire nem magyar joghatóság alatt álló szolgáltatók, ezért működésük során nem kell a magyar jognak megfelelniük. A nemzeti jelképek megsértése, illetve egyes meghatározott önkényuralmi jelképek használata, vagy akár a holokauszttagadás több országban nem számít bűncselekménynek, ezért a platformok felhasználási feltételei egészen a közelmúltig nem foglalkoztak kifejezett tiltásukkal. A nagyobb platformok őshazájában, az Egyesült Államokban a szólásszabadság védelme annyira erős, hogy számos olyan cselekmény folytatását is lehetővé teszi, amelyet az európai jogrendszerek tiltanának. Az amerikai Legfelsőbb Bíróság a Texas v. Johnson ügyben[419] és a United States v. Eichman ügyben[420] is foglalkozott a zászlóégetés kérdésével, és megállapította, hogy a zászlóégetés mint szimbolikus beszéd a védendő közlések kategóriájába tartozik.

Nemzetközi jogforrásokban hiába keressük az ehhez hasonló tartalmak szabályozásával kapcsolatos passzusokat: az egyes bűncselekményekre vonatkozó szabályok területenként változnak, figyelemmel az éppen vizsgált ország történelmére. A posztszovjet térségben – így Magyarországon is – a kommunista diktatúra alatt elkövetett

417 Mezőlaki 2019: 609–651.
418 Mezőlaki 2019: 609–651.
419 Texas v. Johnson, 491 U.S. 397 (1989).
420 United States v. Eichman, 496 U.S. 310 (1990).

bűncselekmények tagadása is bűntettnek számít, más geopolitikai környezetben lévő országok ellenben más hasonló tartalmú jogszabályokat alkalmazhatnak. Svájcban például az örmény népirtás tagadása számít bűncselekménynek, a Perinçek v. Switzerland ügyben a svájci Szövetségi Legfelsőbb Bíróság elmarasztaló ítéletet hozott Doğu Perinçek ügyében.[421]

Az önkényuralmi jelképekkel kapcsolatos problémák nemcsak a közösségimédia-platformokat érinthetik, hanem az online aukciós oldalakat is. Az Ebay már 2001-ben számos olyan termék árusítását tiltotta, amelyeket az erőszak, a gyűlölet, illetve a diszkrimináció dicsőítésével összefüggésben értékesítettek. Az online aukciós oldalon tilos például rabszolgasággal kapcsolatos tárgyakat (bilincseket, adásvételi szerződéseket), néhány kivétellel (például régi fizetőeszközök, katonai modellek) nácizmussal összefüggésbe hozható tárgyakat, náci ideológiával összefüggő médiafájlokat tartalmazó adathordozókat eladásra kínálni.[422] Nehéz ugyanakkor annak meghatározása, hogy mi az eladó szándéka bizonyos tárgyak áruba bocsátásával.

Hazai joggyakorlat

A Fővárosi Ítélőtábla az önkényuralmi jelkép használatának vétsége miatt emelt vád alól felmentette azt a terheltet, aki a Vatera online aukciós oldalon eladásra kínált egy üveg „Führerwein" címkéjű szeszes italt, amelyen Adolf Hitler egyenruhás képe volt látható, karszalagján horogkereszttel. Az ítéletében a bíróság utalt a 14/2000. (V. 12.) számú AB határozatra, amely rögzítette, hogy az önkényuralmi jelképek használata a politikai véleménynyilvánításnak olyan formája, amely korlátozható, amennyiben a tiltott magatartás „nem pusztán egy – helyesnek vagy helytelennek tartott – politikai nézetet fejez ki, hanem annál több: a demokrácia értékei mellett elkötelezett közösségek méltóságát sértve veszélyezteti a köznyugalmat is." A bíróság utalt az Európai Emberi Jogi Bíróságnak a Vajnai kontra Magyarország ügyben hozott ítéletére is, amelyben a testület azt kifogásolta, hogy a magyar (régi) Btk. tényállása túlságosan széles körű, mivel nem kívánja meg annak bizonyítását, hogy a jelkép tényleges használata valóban önkényuralmi propagandának minősül-e. Az ítélőtábla felhívta a figyelmet arra is, hogy a Btk. módosult, miután az AB 46/2013. (II. 21.) határozatában megállapította, hogy a törvény a jelképhasználat tekintetében nem differenciál, hanem a jelképhasználatot általában rendeli büntetni, így aránytalanul korlátozza a véleménynyilvánítás szabadságát. A hatályos Btk. szövegében már

421 Perinçek v. Switzerland Application no. 27510/08. Az ügyben végül az EJEB arra a megállapításra jutott, hogy az elítéléssel Svájc megsértette Perinçek véleménynyilvánítás szabadságához való jogát, és elmarasztalta a svájci államot.

422 Ebay 2023.

a törvényi tényállás része, hogy az önkényuralmi jelkép használata a köznyugalom megzavarására alkalmas legyen, amely jelen ügyben nem történt meg. Az aukciós oldalon közzétett hirdetés megtekintéséhez az érdeklődők csak több lépcsőben juthattak el, a nyitó oldalon figyelmeztetés szerepelt, amely arról tájékoztatta az érdeklődőket, hogy az aukció megtekintése csak 18 éven felüliek számára javasolt. A termékről feltöltött képek ezt követően sem váltak rögtön láthatóvá, azokat csak egy újabb figyelmeztető üzenet elolvasását követően lehetett megtekinteni, amelyben az eladó nyomatékosan felhívta a figyelmet arra, hogy nem kíván a náci ideológiával azonosulni. Az ítélőtábla döntésében kifejtette, hogy a terhelt magatartása nem valósított meg tényállásszerű cselekményt, mivel az értékesített tárgy az „emberiség történelme egy szakaszából fennmaradt olyan tárgyi emlék, mely pusztán a kora, funkciója, saját története folytán – mindenfajta ideológiai azonosulás nélkül – is tárgyát képezheti a történelem iránti érdeklődésnek, a múlt tárgyi kultúrájának megismerését és bemutatását célzó gyűjtői, kutatói szenvedélynek" (Fővárosi Ítélőtábla, Bhar.51/2015/9).

A bíróság ítélete az aukciós platformok számára okozhat némi fejtörést, hiszen ez azt jelenti, hogy az önkényuralmi jelképet ábrázoló dolgok nem tartoznak az automatikusan moderálandó kategóriába. A Vatera általános szerződési feltételei szerint tilos az olyan áruk, termékek, szolgáltatások értékesítése, amelyek gyűlöletkeltésre, fajüldözésre, idegengyűlöletre vagy nemzetek és nemzetiségek közötti konfliktusra adhatnak okot.[423] Panasz esetén azonban a platformnak kell mérlegelnie, hogy egy hirdetést ideológiai célzattal vagy pusztán történelmi érdeklődésből tették közzé.

Az online platformok gyakorlata

Sok online platformnál tehát azt találjuk, hogy még az extrémebb közléseket is védelemben részesítik. A Facebook üzemeltetője egy alkalommal kijelentette, hogy nem törli a neonáci csoportokat, mivel azok nem sértik a platform közösségi útmutatóját. A platformszolgáltató annyit reagált az extrémista csoportok jelenlétére a szolgáltatásában, hogy akit sértenek az ezekben található tartalmak, az lépjen ki az adott csoportból, vagy állítsa le annak követését. A Facebook valamivel korábban azt is kijelentette, hogy alapvetően nem moderálja a holokauszttagadást, amely az Egyesült Államokban nem bűncselekmény, sőt bizonyos esetekben a véleménynyilvánítási szabadság védelme alá tartozik. Németország reakciója a platformszolgáltató álláspontjára az volt, hogy elfogadtak egy jogszabályt, amely megteremti a lehetőségét a gyűlöletbeszéd (ideértve a holokauszttagadást is) eltávolítását elmulasztó platformoknak az 50 millió euróig terjedő bírságolására.

423 Vatera 2023.

Ennek hatására a Facebook több száz tartalmat távolított el a szolgáltatásából, az átláthatósági jelentésében pedig külön menüpontot hozott létre a NetzDG alapján eltávolított tartalmaknak. Egy másik platform, a YouTube esetében egészen 2019-ig kellett várni arra, hogy megfelelő reakció szülessen a holokauszttagadó tartalmak kezelésére. A platformszolgáltató bejelentette, hogy moderálja azokat a tartalmakat, amelyek tagadják, hogy a jól dokumentált erőszakos események megtörténtek. A szolgáltató a holokauszttagadás mellett idesorolja az olyan esetek tagadását is, mint a Sandy Hook iskolában történt lövöldözés. A platform arra is kötelezettséget vállalt, hogy eltávolítja a náci ideológiát dicsőítő tartalmakat, valamint az olyan csoportokat népszerűsítő tartalmakat, amelyek valamely csoport felsőbbrendűségét hirdetik.

Rémhírterjesztés

A rémhírterjesztés szintén egy olyan tartalom-bűncselekmény, amelynek a jelentősége a Covid–19-világjárvány során értékelődött fel. Magyarországon a Btk. 337. §-a az alábbiak szerint szankcionálja a rémhírterjesztést:

337. § (1) Aki közveszély színhelyén nagy nyilvánosság előtt a közveszéllyel összefüggésben olyan valótlan tényt vagy való tényt oly módon elferdítve állít vagy híresztel, amely a közveszély színhelyén alkalmas az emberek nagyobb csoportjában zavar vagy nyugtalanság keltésére, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.
(2) Aki különleges jogrend idején nagy nyilvánosság előtt olyan valótlan tényt vagy való tényt oly módon elferdítve állít vagy híresztel, amely alkalmas arra, hogy a védekezés eredményességét akadályozza vagy meghiúsítsa, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.

A 2020-as koronavírus-járványig a rémhírterjesztés egy viszonylag jelentéktelen passzusa volt a magyar Btk.-nak. A régi, 1978-as Btk. szövege még arról rendelkezett, hogy bármely valótlan tény köznyugalom megzavarására alkalmas, nagy nyilvánosság előtti terjesztése bűncselekmény, a rendelkezés azonban nem állta ki az alkotmányossági próbát, az Alkotmánybíróság a 18/2000. (VI. 6.) AB határozattal megsemmisítette. Az Alkotmánybíróság a szabad véleménynyilvánítási jog korlátjaként vizsgálva a rémhírterjesztés tényállását, arra jutott, hogy a köznyugalom megzavarására alkalmas valótlan tény híresztelése csak abban az esetben eshet korlátozás alá, amennyiben a köznyugalom megbolydulásának veszélye nyilvánvaló és közvetlen. Török Bernát szerint a testület ezzel első alkalommal hozott olyan döntést, amely a büntethetőséghez

nyilvánvaló és közvetlen veszélyt követel meg.[424] Az AB emellett kifejtette, hogy rendkívüli helyzetben, amilyen például közveszély színhelye vagy háború ideje, nincs alkotmányos akadálya a hamis tényállítások szankcionálásának. Az új Btk. a határozat nyomán már csak a közveszély színhelyén történő elkövetést pönalizálja, jelentősen beszűkítve azoknak a szituációknak a körét, amelyekben az elkövetés tényállásszerű lehet. Azt, hogy mi minősül tényállásszerűnek, a Btk. kommentárja akként határozza meg, mint olyan emberi magatartás által kiváltott helyzet, amelyben „meg nem határozható vagy nagyobb számú meghatározott személyt, illetve jelentős értékű anyagi javakat sérelem bekövetkezésének reális lehetősége fenyeget".[425] Kulcseleme a kommentár fogalommeghatározásának, hogy közveszélyt eredményező helyzetet kizárólag emberi magatartás eredményezhet, a természeti csapások, járványok tehát nem eredményeznek közveszélyt. A koronavírus magyarországi megjelenését követően hazánkban is elkezdtek terjedni olyan híresztelések, amelyek alkalmasak voltak a pánikkeltésre, a gyógymódokkal, kezelési módszerekkel kapcsolatos nagyfokú bizalmatlanság felkeltésére, ezzel párhuzamosan sokakban joggal merült fel az igény arra, hogy a jogalkotó tegyen valamit a kór halálosságával szükségtelenül riogató egyénekkel szemben. Mivel a rémhírterjesztés tényállása ezekben az esetekben nem volt alkalmazható, a jogalkotó új bekezdést kapcsolt a Btk. 337. §-ához. A 337. § (2) bekezdése, amely csak a különleges jogrend idején tett valótlan tényállításokra vonatkozik, a járványügyi védekezés eredményességét akadályozó vagy meghiúsító közlésekre vonatkozik. Az új jogszabályhelyet hevesen kritizálták e megfogalmazás miatt, ugyanis nehezen körülhatárolható, hogy melyek azok a közlések, amelyek bármilyen módon hátráltatják a védekezést.[426] Az Alkotmánybíróság nem találta Alaptörvény-sértőnek a jogszabályt, a 15/2020. (VII. 8.) határozatában kijelentette, hogy alapvetően a bírói gyakorlatra tartozik annak kidolgozása, melyek azok a cselekmények, amelyek e körbe tartoznak, s ekként „[a]z általános hatáskörű bíróság juthat arra a következtetésre, hogy a bűncselekménynek nem lehet tárgya sem a kormány különleges jogrend idején hozott egyes intézkedéseinek kritikája, sem jövőbeni eseményekre vonatkozó előrejelzés, és nem lehet tárgya a különleges jogrenddel összefüggésben nyilvánosságra nem hozott adatokkal kapcsolatos találgatás sem".[427] Az eddigi gyakorlat nem igazolta a kritikusok félelmeit. A *Bírósági Határozatok Gyűjteménye* a 2020–2022 közötti időszakra nem tartalmazott jogerős bírósági döntést e tárgyban. A Belügyminisztérium által üzemeltetett

[424] Török 2018: 100–101.
[425] Mezőlaki 2019: 609–653.
[426] Bencze–Ficsor 2020.
[427] 15/2020. (VII. 8.) AB határozat, indokolás, [43] I.1.

bűnügyi statisztikai rendszer szerint a 2020–2022 közötti időszakban mindössze 11 rémhírterjesztéssel összefüggő eset szerepelt a regisztrált bűncselekmények között. Nincs tehát arról szó, hogy a járványhelyzettel, illetve a kormányzati járványkezeléssel kapcsolatban elhangzó kritikus vélemények miatt nagyszámú büntetőeljárás indulna.

Hazai joggyakorlat

Kikristályosodott bírósági gyakorlat híján egyelőre az ügyészség vádemelési gyakorlatán keresztül tudjuk illusztrálni a rémhírterjesztés új elkövetési magatartásának megítélését. A Legfőbb Ügyészségnek az ügyészségi jogalkalmazói gyakorlat egysége érdekében 2020. május 25. napján kiadott iránymutatása szerint a védekezés eredményességét akadályozó vagy meghiúsító magatartás alatt az „az olyan valótlan, vagy elferdített valós tény állítása vagy híresztelése értendő, amely túlmutat az egyes intézkedések kritikáján, és alkalmas olyan emberi cselekvés, mulasztás, illetve ezzel összefüggő következmény előidézésére, amely a védekezést szolgáló járványügyi intézkedések, illetve más, a járvány terjedésének megakadályozása, káros hatásainak megelőzése vagy elhárítása érdekében előírt rendelkezések ellenében hatnak" (15/2020. [VII. 8.] AB határozat, indokolás, [53]). A sajtóban is nagy port kavart esetek sorsa is egyértelműen azt mutatja, hogy az ügyészség szigorú mérce alapján dönt arról, hogy mikor emel vádat, a heves, ám alapvetően kritikus véleménynyilvánítások nem tartoznak ebbe a körbe.

Így például a Gyulai Járási Ügyészség bűncselekmény hiányában megszüntette az eljárást annak a gyulai önkormányzati képviselőnek a Facebookon közzétett bejegyzése esetében, amelyben azt bírálta, hogy a településen harmincezer kórházi ágyat szabadítanak fel. A vehemens hangvételű bejegyzés szerint ez a „haldokló betegek, a magatehetetlen idősek és a rehabilitációra szoruló sérültek hazaküldését jelenti". Az ügyben a város polgármestere tett feljelentést, arra hivatkozva, hogy a lakosság körében nagyfokú nyugtalanságot keltett a haldoklók hazaküldéséről szóló információ. (A fideszes polgármester jelentette fel a gyulai ellenzékit rémhírterjesztés miatt 2020) Szintén megszüntette az ügyészség az eljárást annak a bejegyzésnek az ügyében, amelyben a szerző kijelentette, hogy Orbán Viktor miniszterelnök szándékosan engedi a járványügyi biztonsági intézkedések lazítását az újabb hullám tetőzésekor, ezzel ezreket a halálba küldve.

Vádat emelt viszont az ügyészség akkor, amikor egy pécsi férfi a közösségi oldalán a világjárvány létezését, hátrányos egészségügyi következményeit tagadó, illetve az intézkedések okairól szóló valótlan állításokat tartalmazó bejegyzéseket tett közzé (Vádemelés a rémhírterjesztővel szemben 2020). Szintén vádat emelt az ügyészség annak az orvos végzettségű üzletembernek az ügyében, aki a vírus létezését tagadva ál-ismeretterjesztést folytatott egyebek mellett közösségimédia-platformokon. (Patthy 2021). Vádat emelt az ügyészség annak a Facebook-bejegyzésnek az ügyében is, amelyben a terhelt értelmetlennek nevezte az idősek számára bevezetett vásárlási

időszavot, egészségre ártalmasnak titulálta a védőmaszkot, víruspropagandának és mesterségesen szított hisztériának titulálta a kormányzat intézkedéseit (Szabolcs-Szatmár-Bereg Megyei Főügyészség 2021).

Gyermekpornográfia

45 millió. A *The New York Times* cikke[428] szerint a 2018-as évben ennyi képet és videót jelentettek be a nagy techcégek azért, mert gyermekek szexuális kizsákmányolását ábrázolják. Noha a világ civilizált részein a gyermekek szexuális kizsákmányolása és a gyermekpornográf felvételek készítése, hozzáférhetővé tétele, de már az egyszerű tartása is nemzetközi egyezmények (például a gyermekek jogairól szóló New York-i egyezmény korábban hivatkozott 34. cikke) alapján tilos, úgy tűnik, mégsem sikerül gátat szabni a gyermekeket ábrázoló pornográf felvételek internetes terjedésének. Sőt, a hivatkozott cikk szerint a helyzet egyre súlyosabb, és nemhogy csökken, de exponenciálisan nő az ilyen jellegű tartalmak száma az interneten. Az Europol jelentése szerint 2020-ban a koronavírus-járvány miatt elrendelt karantén és más korlátozó intézkedések növelték a kiskorúak kitettségét az online szexuális bűncselekményeknek, hiszen a járványidőszak alatt a felnőttekhez hasonlóan a gyermekek is többet interneteztek, ám kisebb fokú kontroll mellett.[429] A gyermekpornográfia terjedése az internet egyik legkárosabb jelensége, nem beszélve arról, hogy az internet „nem felejt", az áldozattá vált gyermekekről készült tartalmakat soha, vagy óriási nehézségek árán lehet teljesen eltávolítani. Az internet megkönnyíti a gyermekek szexuális kizsákmányolásával összefüggő tartalmak terjesztését: a hálózaton biztosított a fogyasztó és a terjesztő anonimitása, a különböző kriptovaluták lehetővé teszik a pénzmozgások lekövethetetlenségét, a hozzáférés pedig mindenki számára egyszerű, és nem igényel kockázatos ügyleteket. A gyermekpornográfia azért is különösen veszélyes, mert ahogy Dornfeld László és Mezei Kitti is felhívják rá a figyelmet, a felvételek terjesztését minden esetben megelőzi egy gyermeket ért, fizikai térben is megvalósult abúzus.[430]

428 Keller–Dance 2019.
429 Europol 2022.
430 Dornfeld–Mezei 2017: 33.

A Btk. 204. §-ában szabályozza a bűncselekményt:

204. § (1) Aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt

a) megszerez vagy tart, bűntett miatt egy évtől öt évig,

b) kínál, átad vagy hozzáférhetővé tesz, bűntett miatt két évtől nyolc évig,

c) készít, forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz, bűntett miatt öt évtől tíz évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés az (1) bekezdés a) pontja esetén két évtől nyolc évig terjedő, b) pontja esetén öt évtől tíz évig terjedő, c) pontja esetén öt évtől tizenöt évig terjedő szabadságvesztés, ha az ott meghatározott bűncselekményt

a) tizenkettedik életévét be nem töltött személy sérelmére,

b) az elkövető nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére, illetve a sértettel kapcsolatban fennálló egyéb hatalmi vagy befolyási viszonnyal visszaélve, vagy a sértett kiszolgáltatott helyzetét kihasználva,

c) hivatalos személyként e minőség felhasználásával,

d) sanyargatást vagy erőszak alkalmazását tartalmazó felvételre, vagy e) különös visszaesőként követik el.

(3) A büntetés az (1) bekezdés a) pontja esetén öt évtől tíz évig terjedő, b) pontja esetén öt évtől tizenöt évig terjedő, c) pontja esetén öt évtől húsz évig terjedő szabadságvesztés, ha az ott meghatározott bűncselekményt tizenkettedik életévét be nem töltött személy sanyargatását vagy erőszak alkalmazását tartalmazó felvételre követik el.

(4) Aki az (1) bekezdés c) pontjában meghatározott

a) bűncselekményhez anyagi eszközöket szolgáltat, bűntett miatt egy évtől öt évig,

b) bűncselekményre irányuló előkészületet követ el, bűntett miatt három évig

terjedő szabadságvesztéssel büntetendő.

(5) Aki tizennegyedik életévét betöltött, de tizennyolcadik életévét be nem töltött személyt ábrázoló pornográf felvételt

a) megszerez vagy tart, bűntett miatt három évig,

b) készít, bűntett miatt egy évtől öt évig

terjedő szabadságvesztéssel büntetendő, ha a (2) bekezdés b)–e) pontjában meghatározott valamely körülmény nem áll fenn.

(6) Aki tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf felvételen való szereplésre felhív, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.

(7) Aki tizennegyedik életévét betöltött, de tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf felvételen való szereplésre felhív, bűntett miatt három évig terjedő

szabadságvesztéssel büntetendő, ha a (2) bekezdés b)–e) pontjában meghatározott valamely körülmény nem áll fenn.

(8) E § alkalmazásában pornográf felvétel: a másnak vagy másoknak a nemiséget súlyosan szeméremsértő nyíltsággal, célzatosan a nemi vágy felkeltésére irányuló módon történő ábrázolása, ideértve a nem létező személy vagy személyek valósághű ábrázolását is.

204/A. § (1) Aki

a) olyan pornográf műsoron vesz részt, amelyben tizennyolcadik életévét be nem töltött személy szerepel vagy ilyen személyek szerepelnek, bűntett miatt két évtől nyolc évig,
b) tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban szerepeltet vagy ilyen pornográf műsort szervez, bűntett miatt öt évtől tíz évig

terjedő szabadságvesztéssel büntetendő.

(2) A büntetés az (1) bekezdés a) pontja esetén öt évtől tíz évig, b) pontja esetén öt évtől tizenöt évig terjedő szabadságvesztés, ha az ott meghatározott bűncselekményt

a) tizenkettedik életévét be nem töltött személy sérelmére,
b) az elkövető nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére, illetve a sértettel kapcsolatban fennálló egyéb hatalmi vagy befolyási viszonnyal visszaélve,
c) hivatalos személyként e minőség felhasználásával,
d) sanyargatást vagy erőszak alkalmazását bemutató műsorra, vagy
e) különös visszaesőként

követik el.

(3) A büntetés az (1) bekezdés a) pontja esetén öt évtől tizenöt évig, b) pontja esetén öt évtől húsz évig terjedő szabadságvesztés, ha az ott meghatározott bűncselekményt tizenkettedik életévét be nem töltött személy sanyargatását vagy erőszak alkalmazását bemutató műsorra követik el.

(4) Aki az (1) bekezdés b) pontjában meghatározott

a) bűncselekményhez anyagi eszközöket szolgáltat, bűntett miatt egy évtől öt évig,
b) bűncselekményre irányuló előkészületet követ el, bűntett miatt három évig

terjedő szabadságvesztéssel büntetendő.

(5) Aki tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban szereplésre felhív, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.

(6) Aki tizennegyedik életévét betöltött, de tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban szereplésre felhív, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő, ha a (2) bekezdés b)–e) pontjában meghatározott valamely körülmény nem áll fenn.

(7) E § alkalmazásában pornográf műsor: a más vagy mások nemiségét súlyosan szeméremsértő nyíltsággal megjelenítő, célzatosan a nemi vágy felkeltésére irányuló cselekvés vagy előadás.

A bűncselekmény jogi tárgya a 18 év alattiak egészséges, zavartalan nemi és szexuális fejlődése és a gyermekpornográfiát működtető szervezett bűnözői csoportok elleni küzdelemhez fűződő társadalmi érdek.

Ezen a ponton rögtön meg is kell állnunk egy rövid kitérőre, feltűnő ugyanis, hogy a törvényszöveg a paragrafus címével ellentétben sehol nem tartalmazza a „gyermek" szót. A törvényszöveg a nemzetközi gyakorlattal összhangban következetesen a 18. életévét be nem töltött személyt tekinti gyermeknek, és ezzel a kifejezéssel illeti a passzív alanyt.

A Btk. kommentárja *expressis verbis* rögzíti, hogy a nagykorúság és a kiskorúság közömbös.[431] Ez a distinkció mai szemmel nézve több életszerűtlen helyzetet eredményezhet. A Ptk. szabályai szerint a kiskorú személy házasságkötéssel nagykorúvá válik,[432] a gyámhatóság pedig a már tizenhatodik évüket betöltött személyeknek is engedélyt adhat a házasságkötésre.[433] Tehát az a házasságban élő nagykorú, aki még csak a 16. vagy 17. életévét töltötte be, nem készíthet a házastársával pornográf felvételt, illetve nem küldhet a házastársának magáról pornográf felvételt (szexting), hiszen ez esetben a házastárs elvben felelősségre vonható, hiszen a felvétel tartása tényállásszerűen megvalósul. A hagyományos gyermekpornográfia-tartást el kell határolni az úgynevezett szexting körébe eső tartalmaktól. A szexting (amely az angol *sex* és *texting,* azaz sms-küldés szavak összevonásából keletkezett) a fiatalok által kedvelt tevékenység: tinédzserek és fiatal felnőttek egymásnak küldött erotikus, sokszor kimondottan pornográf (például önkielégítést ábrázoló) tartalmait értjük alatta. Talán érezzük, hogy ezek a felvételek, noha károsak a gyermekek szexuális fejlődése szempontjából, nem ugyanabba a kategóriába tartoznak, mint egy szexuális erőszak eredményeként megszületett felvétel. A gyakorlatban ugyanakkor még korántsem egyértelmű ezeknek a felvételeknek a megítélése. Gyurkó Szilvia szerint ez esetben részleges dekriminalizálásnak van helye,[434] hiszen a jogalkotónak nyilvánvalóan nem az a célja a gyermekpornográfia kriminalizálásával, hogy a nemiséget éppen felfedező kamaszokat ítéljen szabadságvesztés büntetésre. Más álláspontok szerint igenis tiltani kell ezeket a tartalmakat, hiszen ha a felvételek nyilvánosságra kerülnek, és más közönséghez is eljutnak, akkor már komolyabb károkat okozhatnak az azon szereplő gyermekeknek.[435] A Btk. jelenleg alkalmazott megoldása, hogy a büntetési

431 Szomora 2019a.
432 2:10. § [A kiskorúság] (1) bekezdés.
433 4:9. § [A házasságkötési korhatár] (2) bekezdés.
434 Urfi 2020.
435 Ambrus 2021: 105.

tételt három évben rögzíti azokban az esetekben, ahol a sértett 12 és 18 éves kor között volt az elkövetés idején. Ezzel viszont egyrészt nem oldja fel a szexting miatt keletkezett dilemmát, másrészt indokolatlan életkori különbséget tesz, hiszen szexuális bántalmazás, illetve kizsákmányolás esetén lényegtelen, hogy a sértett 11 vagy 13 éves.

Az én véleményem a kérdésben az, hogy Magyarországon a gyermekpornográfia tényállásának átfogó reformjára volna szükség. Egyrészt: a külföldi szakirodalom egy ideje igyekszik kivezetni a gyakorlatból a gyermekpornográfia kifejezés használatát. Helyesen, hiszen a pornográfia alapvetően olyan kereskedelmi műfaj, amelyet nem tilt jogszabály, így ez a kifejezés nem érzékelteti kellően azt, hogy milyen súlyos bűncselekmény valósul meg. A kifejezés a szexuális tartalmak különböző kategóriának megkülönböztetésére sem alkalmas, így a szextingre is vonatkozik, ami figyelembe véve a mai fiatalok szokásait már idejétmúlt. A nemzetközi gyakorlattal összhangban célravezetőbb volna a gyermekek szexuális bántalmazását ábrázoló tartalom vagy a gyermekek szexuális kizsákmányolását ábrázoló tartalom kifejezések egyikének a bevezetése, amely érzékelteti a felvételkészítés mögött meghúzódó cselekmények súlyát, ugyanakkor nem kriminalizál indokolatlanul fiatalokat.

A tiltott pornográf felvétellel visszaélés bűntette esetében jelentősége annak van, ha a képfelvétel rögzítésének időpontjában az azon szereplő személy a 18. életévét még nem töltötte be, az közömbös, hogy a pornográf felvétel nyilvánosságra hozatalának időpontjában a személy már betöltötte-e a 18. életévét (BH2010.267). Ha az elkövető és a sértett nem ismerik egymást, „a hatóság igazságügyi orvos-szakértőt rendel ki annak megállapítására, hogy a képfelvételeken látható személy milyen életkorú. Általában ezzel nincs is probléma, mivel a képfelvételeken látható személyek életkora általában nem az életkori határ közelében található, de egyes esetekben problémát okozhat, ha a passzív alany életkora 16 és 18 év közé esne."[436]

A bűncselekmény elkövetési tárgya a pornográf felvétel és műsor. A törvény meghatározza mind a pornográf felvétel, mind a pornográf műsor fogalmát. A fogalmak jellegzetessége, hogy mind a felvétel, mind a műsor akkor minősül pornográfiának, ha annak célja a nemi vágy felkeltése. A gyakorlat számára azonban nehézséget okozhat annak meghatározása, hogy mely felvétel minősülhet olyannak, amelyet nemi vágy felkeltésére szántak. Peszleg Tibor rávilágít arra a problémára, hogy a nemi vágyat felkeltheti olyan kép is, amelyet alapvetően nem erre szántak.[437] A különböző fétiseket ábrázoló vagy az erőszakot szexualizáló felvételek tipikusan olyanok, amelyek

[436] Peszleg 2004: 58.
[437] Peszleg 2004: 58.

nem keltik fel egy átlagember szexuális érdeklődését. A más számára egyáltalán nem a nemi vágy felkeltését célzó kép, például egy nyaraláson készült meztelen kisgyermeket ábrázoló kép a szexuális magatartászavarral küzdők számára a nemi vágy felkeltésére alkalmas lehet.[438] A pornográfiaként minősítésnek további eleme mindkét fogalom esetében a nemiség súlyosan szeméremsértő nyíltsággal való ábrázolása. Nincs azonban általános zsinórmértéke annak, hogy mi minősül súlyosan szeméremsértő alkotásnak. Önmagában a meztelenség még nem feltétlenül minősül ekként, hiszen a művészi alkotások és az oktatási, tájékoztatási céllal készült felvételek esetében nem beszélhetünk súlyos szeméremsértésről (sem a nemi vágy felkeltésének céljáról). Peszleg Tibor kifejti azt is, hogy a súlyosan szeméremsértő tartalom fogalmát internetes környezetben különösen fontos meghatározni, mégpedig egy gyakorlat által kialakított objektív mérce alkalmazásával. Rámutat arra, hogy a szexuális tartalmú oldalak előtt általában erre történő figyelmeztetés van, így az oldalakat csak az érdeklődők tekintik meg, akik sokkal toleránsabbak a nemiség, illetve a nemi másság iránt, mint a hétköznapi életben, ezért számukra a szeméremsértés fogalma más jelent, mint ami a társadalomban általánosan elfogadott. Peszleg szerint

> „súlyosan szeméremsértő az a kép, amelyeken akár a férfi, akár a női nemi szervek közvetlen izgatását mutatják be, legyen az akár azonos, akár különnemű személy nemi szervével vagy más testrészével, illetve tárggyal vagy eszközzel történő izgatás. Súlyosan szeméremsértő továbbá az is, amikor az izgalmi állapotban lévő nemi szervet – akár férfiét, akár nőét – úgy mutatnak be a képen, hogy az csak a nemi vágy fokozását célozza".[439]

Modern korunk egyik nagy dilemmája, hogy miként szabályozzuk a nem valós kiskorúakat ábrázoló pornográf felvételeket. Mivel megosztó kérdésről van szó, a Cybercrime Egyezmény a részes államokra bízza annak meghatározását, hogy kriminalizálják-e a virtuális felvételeket. Valamivel konkrétabb szabályokat fogalmaz meg a Lanzarote Egyezmény, amely alapján a nem valós gyermeket ábrázoló pornográf felvételeket két csoportra bonthatjuk. Az egyik csoportba tartoznak a nem létező, teljes mértékben színlelt ábrázoláson alapuló felvételek, az úgynevezett virtuális gyermekpornográfia. Ezek lehetnek számítógépes grafikák, rajzok, animációk. A másik csoportba a pszeudo-gyermekpornográfia tartozik, amely során a készítők digitális technológiák alkalmazásával érik el, hogy egy valós, nagykorú személy gyermeknek tűnjön.

[438] Peszleg 2004: 58.
[439] Peszleg 2000: 36.

Az EU-ban a 2011/98/EU irányelv már kimondottan kötelezi a tagállamokat a gyermeknek tűnő személyt ábrázoló (pszeudo-gyermekpornográfia), illetve a valósághű gyermekábrázolást (virtuális pornográfia) bemutató tartalmak kriminalizálására. A nemzetközi egyezmények ellenére a gyakorlati szakembereket megosztja a kérdés. A nem valós kiskorút ábrázoló felvételek esetében két irányvonal mentén oszlanak meg az álláspontok. Az egyik álláspont képviselői szerint a virtuális gyermekpornográfia önmagában nem ártalmas, hiszen nincsen olyan személy, aki akár az előállítás, akár a terjesztés során sérelmet szenvedne.[440] A Mezei Kitti által is hivatkozott másik álláspont szerint[441] ellenben ezek a felvételek egyfajta kapudrogként működnek, hozzájárulva a gyermekek iránti szexuális fantáziák kialakulásához, serkentve a hajlandóságot arra, hogy az ingerküszöb növekedésével később már valós kiskorúakat ábrázoló felvételeket szerezzen be az elkövető. A magyar Btk. szabályai már összhangban vannak mind a Gyermekjogi Fakultatív Jegyzőkönyv, mind a 2011/93/EU irányelv, mind a Lanzarote Egyezmény rendelkezéseivel, azonban erre több mint 10 évet kellett várni. A virtuális gyermekpornográfiára a Btk. így is csak egy helyen, a pornográf felvétel fogalmát kibontó értelmező rendelkezésben utal, akként, hogy a pornográf felvétel fogalmába beleérti a valósághű ábrázolásokat is.

A bűncselekmény elkövetési magatartásai a felvételek megszerzése, tartása, készítése, kínálása, átadása, hozzáférhetővé tétele, forgalomba hozatala, valamint a felvételekkel való kereskedés és azok nagy nyilvánosság számára hozzáférhetővé tétele, valamint pornográf műsorban való szereplésre felhívás és szerepeltetés, pornográf felvételen való szereplésre felhívás, olyan pornográf műsorban szereplés, amelyben tizennyolcadik életévét be nem töltött személy vesz részt, illetve a tizennyolcadik életévüket be nem töltött személyek pornográf műsorban való szerepeltetéséhez anyagi eszközök szolgáltatása.

A gyermekpornográfia törvényben meghatározott első alapesete a megszerzés, illetve a tartás. A megszerzés a Btk. kommentárja szerint „felvétel bármilyen módon történő birtokba vételét jelenti, akár kétoldalú, akár egyoldalú cselekmény által,” [442] míg a tartás folyamatos birtoklást jelent. A kommentár szövege tipikus példának az internetről való letöltést említi. Problémásabb a megítélése a gyermekpornográfiát tartalmazó élő közvetítések *(live-streaming)* megtekintésének, ugyanis ezek esetében nem történik a számítógépen történő tárolás, legfeljebb az internetes böngésző *log* fájljaiból lehet visszakeresni, ha valaki gyermekpornográf jellegű weboldalt látogatott,

[440] Eneman–Gillespie–Stahl 2009.
[441] Mezei 2021.
[442] Szomora 2019a.

ez azonban önmagában nem minősül felvétel tartásának. Bayer Judit az első esetben szereplő cselekmények kriminalizálása ellen szólal fel, amikor arról ír, hogy böngészés közben az ember akaratlanul is olyan oldalra keveredhet, ahol gyermekpornográf felvétel található, és az is „előfordulhat, hogy a számítógép úgy ment el egy másolatot a látogatott oldalról, hogy a tulajdonosnak nincs is arról tudomása. Elektronikus levélben is lehet ilyen képet kapni, akár anélkül, hogy a címzett azt kinyitotta volna."[443] Ezekben az esetekben ugyanakkor nem teljesül a magatartás szándékosságának követelménye, márpedig mindkét nevesített cselekménynek eleme a szándékosság, így a bizonyítási eljárás során szükséges tisztázni, hogy a felvétel milyen körülmények között került a számítógépre. A régi Btk. kommentárja kiemeli:

> „[M]ivel a bűncselekmény valamennyi elkövetési alakzata csak szándékosan követhető el, megszerzés vagy tartás esetén fokozottan vizsgálni kell, hogy a terhelt tudattartalma az általa tudottan tiltott kép megszerzésére vagy tartására kiterjedt-e. Az internettechnika számos esetben lehetővé teszi, hogy a különböző programok anélkül telepítsenek képeket és más felvételeket a felhasználó számítógépére, hogy azokat a felhasználónak külön-külön látnia és engedélyeznie kellene, illetve különböző maliciózus programok útján lehetséges a felhasználó tudtán kívül is bizonyos adatoknak az érintett számítógépére juttatása. Ha bizonyítható – akár szakértő útján –, hogy a letöltött képpel a felhasználó valamilyen műveletet végzett, úgy a megszerzés, de legalábbis általában a tartás szándékossága általában nehezen vitatható."[444]

Ennek következtében tehát nem büntethető, aki akaratán kívül (vírus, spam vagy *pop-up* ablak formájában) találkozott a felvételekkel. Bayer Judit a *Belügyi Szemle* című folyóiratban megjelent tanulmányában kifejti aggályait a képek birtoklása, illetve megszerzése elkövetési magatartásokkal kapcsolatban is. Eszerint pusztán azzal, hogy valaki már létező felvételeket megszerez vagy tart, további jogsérelmet már nem okoz, amennyiben a felvételeket már nem adja tovább. Véleményem szerint ez a megközelítés azért nem helyes, mert azáltal, hogy valaki ilyen felvételekkel rendelkezik, azzal az ilyen felvételek iránti keresleti oldalt erősíti, akkor is, ha azokat nem adja át senkinek. Bizonyos szexuális devianciákkal küzdő egyéneknek megvan az igénye arra, hogy mások elkészítsék, megosszák ezeket a felvételeket, amíg pedig fizetőképes kereslet van, addig kínálat is lesz. Az interneten való böngészéssel ezen oldalak látogatottságát növelik, valamint ha a megszerzés visszterhesen történik,

[443] Bayer 2003: 98–126.
[444] Nagykommentár a Büntető Törvénykönyvről szóló 1978. évi IV. törvény – WK Jogtár.

anyagilag támogatja a készítőket, megosztókat, amivel lényegében a szervezett bűnözést és a gyermekek szexuális kizsákmányolását segítik elő.

A második alapeset a kínálás, átadás, illetve a hozzáférhetővé tétel. Online környezetben a legnagyobb jelentősége a hozzáférhetővé tételnek van, ezért a továbbiakban ezzel foglalkozunk részletesebben. A hozzáférhetővé tétel olyan magatartás, amely révén egy vagy több személy lehetőséget kap a felvétel megismerésére, ugyanakkor annak birtokba vételét (így letöltését) már nem foglalja magában.

A harmadik alapeset a készítést, kereskedést, forgalomba hozatalt, illetve a nagy nyilvánosság számára való hozzáférhetővé tételt foglalja magában. A nagy nyilvánosság számára hozzáférhetővé tételt el kell határolni az előző alapesetben említett hozzáférhetővé tételtől. A nagy nyilvánosság értelmezésére már a rágalmazás tényállásának elemzésénél sor került. Ez a kategória tágabb, mint a kereskedés, illetve a forgalomba hozatal, történhet például úgy, hogy az elkövető feltölti egy weboldalra, videó- vagy fájlmegosztóra a kérdéses tartalmakat. „Az egyezmény indoklása szerint a hozzáférhetővé tétel a gyermekpornográf felvételek mások számára online rendelkezésre bocsátása, illetve a gyermekpornográf weboldalakra mutató hiperlink létrehozatala vagy szerkesztése az oldalak elérésének előmozdítása érdekében."[445]

Mint általában a tartalommal kapcsolatos cselekmények esetében, az internetes közvetítő szolgáltatóknak nagy szerepe van a gyermekek szexuális kizsákmányolását megvalósító cselekmények megelőzésében. A gyermekpornográfia – mivel az generálisan büntetendő – minden legális szolgáltatást nyújtó online platform szabályzata szerint is tilos.

Online platformok a gyermekpornográfia elleni küzdelemben

A generális, tehát a széles közönségnek szolgáltatást nyújtó online platformok általában kevésbé megengedőek a meztelenséget ábrázoló tartalmakkal, mint a jogszabályok. A Facebookon és az Instagramon például tilos a meztelenség bármely formája – nem csak a kiskorúakat ábrázoló felvételek –, abban az esetben is, ha teljes mértékben nélkülözik a szexualitást. Ez alól csak kivételesen lehet eltérni: oktatási célból, illetve a nyilvánosság tájékoztatása céljából a platform eltérést engedhet e főszabály alól. Ilyen például a mellrák szűrése esetében az emlőönvizsgálatot bemutató oktatóanyag. Meztelen kiskorút ábrázoló felvételt csak hírportál mutathat be, éhínséggel, népirtással, háborús vagy emberiségellenes bűncselekményekkel kapcsolatos híranyagok illusztrálására, ekkor is a megfelelő figyelmeztető jelzéssel ellátva. A globális büntetőjogi tilalomból

445 Parti 2008: 114.

és a meztelenség szigorú moderálásából nyilvánvalóan következik, hogy a gyermekpornográfia szintén tilos ezeken a platformokon.

A legújabb nemzetközi trendekkel összhangban a Meta közösségi alapelvei egyáltalán nem használják a gyermekpornográfia kifejezést. A szabályzat e helyett a gyermekek szexuális kizsákmányolásának tilalmáról szól, amely nemcsak az explicit pornográf felvételeket fedi le, hanem a gyermekek sérelmére elkövetett szexuális visszaéléseknek ennél jóval tágabb körét. A gyermekek szereplésével készült vagy gyermekeket ábrázoló szexuális felvételek megosztásán túl a Facebook tiltja a kizsákmányolást dicsőítő, arra buzdító, annak elkövetéséhez tanácsot, segítséget nyújtó tartalmak közzétételét, illetve a platform szabályzata tiltja az olyan vélemények közzétételét, amelyben a közlő gyermekpornográf felvételek készítésének a szándékáról szól, vagy ilyen felvételek készítésével, nyilvánosságra hozatalával fenyeget, vagy elismeri, hogy részt vett ilyen tartalmak előállításában.

A platform a gyermekek szexuális kizsákmányolásáról szóló részben szabályozza a *grooming* tilalmát is, így tilos „illetlen" kapcsolatot folytatni a kiskorú felhasználókkal. Az illetlen kapcsolat a szolgáltató értelmezése szerint a szexuális tevékenységre való felhívás, a kiskorúak szexuális tartalmaknak való közvetlen kitétele, a szexuális tartalmú üzenetváltás, illetve kiskorúak felhívása arra, hogy magukról küldjenek szexuális felvételt.

Enyhébben áll a szexuális tartalmak megjelenítéséhez az X (Twitter), ahol nem vonatkozik teljes tilalom a szexuális tartalmak közzétételére.

Az internet ugyanakkor tele van olyan szolgáltatásokkal is, amelyek kifejezetten pornográf tartalmak megosztására jöttek létre. Többségükben ezek a szolgáltatások nem jogellenesek, ugyanolyan gazdasági szolgáltatásként működnek, mint bármilyen más közösségimédia-platform vagy videómegosztó platform, a tartalommal kapcsolatos ellenőrzés azonban kevésbé szigorúan zajlik rajtuk. A nagyobb szolgáltatók előírják, hogy tilos kiskorúakról készített felvételeket közzétenni, az amerikai szabályokkal összhangban pedig arról is rendelkeznek, hogy a videó feltöltőjének minden esetben nyilatkozatot kell beszereznie a felvétel szereplőitől arról, hogy már elmúltak 18 évesek – az, hogy hogyan ellenőrzik ezeket a követelményeket, viszont már nem transzparens. Szemben az olyan globális szolgáltatásokkal, amelyek átláthatósági jelentéseikben közzéteszik, hogy hány tartalommal kapcsolatos panaszt bíráltak el, hány tartalmat és milyen indokkal távolítottak el, a pornográf tartalmak működéséről nem rendelkezünk ilyen információkkal. Aggasztó azonban, hogy az Egyesült Királyságban nemrég petíció indult az egyik legnagyobb pornográf videómegosztó,

a Pornhub ellen, amiért az olyan tartalmakat sem szűr, amelyben kiskorúak vagy szexuális erőszak szerepelnek.[446]

A 2022-ben elfogadott DSA kötelezi az online platformszolgáltatókat a jogellenes tartalmak elleni fellépésre,[447] konkrét intézkedéseket azonban nem fogalmaz meg. Az online óriásplatformokra vonatkozó többletkötelezettségek ráadásul a legtöbb pornográf platform szolgáltatójára nem vonatkoznak. Az imént említett Pornhub például a havi 32 millió aktív felhasználójával is csak 2024 elején került fel az online óriásplatformok listájára, két hasonló platformmal (Stripchat és XVideos) együtt.

Az audiovizuális médiaszabályozás hatálya az AVMS irányelv módosításának hatálybalépése óta Európában letelepedett pornográf videómegosztókra is kiterjed, ám a szolgáltatók gyakorlatában egyelőre nem tapasztalható jelentős változás. Az AVMS irányelv 28b. cikke előírja, hogy a videómegosztóknak megfelelő intézkedéseket kell hozniuk annak érdekében, hogy megvédjék a közönséget az olyan tartalmakat hordozó műsorszámoktól, felhasználó által létrehozott videóktól és audiovizuális kereskedelmi közleményektől, amelyek gyermekpornográfiával kapcsolatos bűncselekményt valósítanak meg.[448] A megfelelő védelmi intézkedések körét az irányelv nem határozza meg, de nyilvánvaló, hogy itt azokról a legszigorúbb intézkedésekről van szó, amelyek lehetővé teszik a tartalmak hatékony észlelését és eltávolítását. Az irányelvet átültető Ekertv. ezzel párhuzamosan arról rendelkezik, hogy a videómegosztó platformok kötelesek hatékony intézkedéseket és műszaki megoldásokat alkalmazni, ha a szolgáltatásban megjelenő tartalom bűncselekményt vagy bűncselekmény elkövetésére való felhívást valósíthat meg, így különösen, ha gyermekpornográf tartalom megosztását, terjesztését vagy továbbítását valósíthatja meg.[449]

A gyermekpornográf felvételekkel való kereskedelemnek az elsődleges közege a sötét web *(dark web),* amelyet bűnüldözési szempontból a legnehezebb megragadni. A *dark web*en működő illegális szolgáltatókra értelemszerűen nem a DSA és az AVMS médiaszabályozási, hanem a büntetőjog eszközrendszere alkalmazandó, hiszen ezek a szolgáltatások nem minősülnek gazdasági szolgáltatásoknak, nem vonatkozik rájuk a szolgáltatások szabad mozgásának a szabadsága, a társadalom érdeke azt kívánja, hogy az ilyen szolgáltatásokat üldözzék, illetve szüntessék meg.

446 Grant 2020.
447 Lásd például DSA (31) preambulumbekezdés és 9. cikk.
448 AVMS irányelv 28b. cikk c) pont.
449 Ekertv. 15/D. § (1) bekezdés c) pont.

A szerzői jogok megsértésével kapcsolatos bűncselekmények

A széles sávú internetnek köszönhetően ugrásszerűen megnőtt az online elérhető képes, szöveges, zenei, illetve audiovizuális tartalmak száma. A technológiai fejlődés következtében rendelkezésre álló hatalmas tárhelyek mind a magánszemély felhasználók, mind a médiavállalatok számára megkönnyítik a tartalmak elhelyezését az interneten. Az alacsony belépési küszöb miatt az online környezetben nemcsak a lekérhető szolgáltatásokat nyújtó streamingszolgáltatók (Netflix, HBOMax), hanem maguk a felhasználók is képesek magas minőségű tartalmakkal belépni a piacra (lásd például a YouTube vagy a TikTok fiatalok körében igen népszerű tartalom-előállítóit). A bőséggel rendelkezésre álló tartalomkínálatban azonban akadnak olyan elemek is, amelyeket jogszerűtlenül helyeztek el a világhálón. Az online megtalálható alkotások általában szerzői jogi védelem alá esnek, a jogsértéshez pedig a nemzetközi és a magyar büntetőjog is szankciókat kapcsol. E fejezetben elsősorban a szerzői jog büntetőjogi védelméről esik szó, amely az igényérvényesítés egyéb módjai mellett inkább kiegészítő szerepet tölt be. A szerzői művekhez fűződő vagyoni érdekek miatt a fellépés sokszor inkább polgári jogi eszközökkel történik; ezekről számos kiváló munka olvasható a magyar jogirodalomban.[450]

A szerzői jogi védelem alá eső alkotásokat a szerzői jogról szóló 1999. évi LXXVI. törvény 1. § (2) bekezdése ekként határozza meg: „Szerzői jogi védelem alá tartozik – függetlenül attól, hogy e törvény megnevezi-e – az irodalom, a tudomány és a művészet minden alkotása." A törvény példálózó jelleggel meg is határozza azokat az alkotásfajtákat, amelyek igényt tarthatnak a védelemre, idetartozik a szoftver (a számítógépi programalkotás és a hozzá tartozó dokumentáció) akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, ideértve a felhasználói programot és az operációs rendszert is), a zenemű, a filmalkotások és más audiovizuális művek, fotóművészeti alkotások. A szerzői jog logikájából az következik, hogy a védelem a többi alkotásfajtára is kiterjed, akkor is, ha azok nincsenek konkrétan nevesítve az Szjt.-ben. A büntetőjogban ellenben szigorú tilalom vonatkozik a vélelmek alkalmazására és az analógiára. A Kúria 9/2013 elvi határozatában rögzíti, hogy a szerzői jog hatályának és alkalmazhatóságának a kérdése a büntetőügyekben külön vizsgálandó, így az egyes alkotások védettségét automatikusan feltételezni nem lehet.

[450] Lásd például Faludi 2007: 36–48; 2011; Lontai–Faludi–Gyertyánfy 2012; Gyertyánfy 2013; Pogácsás 2014; Grad-Gyenge 2019.

Az Szjt. keretdiszpozíció révén hátteréül szolgál a Btk. XXXVII. fejezetében meghatározott szellemi tulajdonjog elleni bűncselekményeket tartalmazó tényállásoknak. Az új Btk. bevezetése sok változást hozott, amelyek közül gyakorlati szempontból talán az egyik legjelentősebb a szerzői és szerzői joghoz kapcsolódó jogok megsértése kapcsán történt. Az új törvény a korábban a vagyon elleni bűncselekmények közt elhelyezett szellemi tulajdonjogot sértő bűncselekményeket külön fejezetbe szerkesztette. Mivel a Btk. ez esetben keretjellegű szabályokat tartalmaz, a két törvény, a Btk. és az Szjt. szabályait együttesen kell alkalmazni és értelmezni. A fejezetben a Btk. ötféle bűncselekményt szabályoz, amelyek közül a kötet szempontjából a bitorlásnak, a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének, valamint a védelmet biztosító műszaki intézkedés kijátszásának van jelentősége.

Bitorlás

384. § (1) Aki
a) más szellemi alkotását sajátjaként tünteti fel, és ezzel a jogosultnak vagyoni hátrányt okoz,
b) gazdálkodó szervezetnél betöltött munkakörével, tisztségével, tagságával visszaélve más szellemi alkotásának hasznosítását vagy az alkotáshoz fűződő jogok érvényesítését attól teszi függővé, hogy annak díjából, illetve az abból származó haszonból vagy nyereségből részesítsék, illetve jogosultként tüntessék fel,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése

385. § (1) Aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait vagyoni hátrányt okozva megsérti, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés szerint büntetendő, aki a szerzői jogról szóló törvény szerint a magáncélú másolásra tekintettel a szerzőt, illetve a kapcsolódó jogi jogosultat megillető üreshordozó díj, illetve reprográfiai díj megfizetését elmulasztja.

Védelmet biztosító műszaki intézkedés kijátszása

386. § (1) Aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedést haszonszerzés végett megkerüli, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerülése céljából

a) az ehhez szükséges eszközt, terméket, számítástechnikai programot, berendezést vagy felszerelést készít, előállít, átad, hozzáférhetővé tesz, vagy forgalomba hoz,

b) az ehhez szükséges vagy ezt könnyítő gazdasági, műszaki vagy szervezési ismeretet másnak a rendelkezésére bocsátja.

A bitorlás tényállása két elkövetési magatartást foglal magában: az első eset azt rendeli büntetni, ha az elkövető az elkövetés tárgyát sajátjaként tünteti fel, a másik eset pedig azt szabályozza, ha valaki gazdasági szervezetben betöltött munkakörével, tisztségével, tagságával visszaélve követel díjazást vagy részesedést a nyereségből. Online környezetben az első eset fordul elő tömegesen, hiszen még az okostelefonnal elkészített fényképek is élveznek szerzői jogi védelmet. Az interneten található képek, videók saját alkotásként történő megosztása vagyoni hátrány okozása esetén tehát szerzői jogsértést, olykor pedig büntetőjogi szankciót maga után vonó jogsértést eredményezhet. A népszerű kép- és videómegosztó szolgáltatók a felhasználási feltételeikben többnyire egyértelmű szabályokat fogalmaznak meg a más tartalmával való visszaélésre. Az Instagram, amely a fiatalok körében az egyik legnépszerűbb közösségimédia-platform, kifejezetten felhívja a felhasználók figyelmét arra, hogy mindenki olyan tartalmakat osszon meg, amelynek a „tulajdonosa".

A platformok felhasználási feltételei kifejezetten tiltják a más szellemi tulajdonát sértő alkotások közzétételét, ez a magatartás tehát a platform és a felhasználó jogviszonyában szerződésszegő magatartásnak minősül, amelyet a platform szankcionál. E magatartások körébe nemcsak a bitorlás tartozik, hanem a szerzői vagy szerzői joghoz kapcsolódó jogok megsértése is.

A szerzői vagy szerzői jogokhoz kapcsolódó jogok megsértése esetében a vagyoni hátrány okozásával történő elkövetést rendeli büntetni a törvény, a lehetséges elkövetési módokat azonban nem sorolja fel, hiszen az internet miatt ezek annyira változatos formákat ölthetnek, hogy nem célszerű jogi szabályok révén szűkíteni a szankcionálandó magatartások körét. Tipikus elkövetési magatartása a szerzői jog megsértésének a jogosulatlan felhasználás. A Szjt. 17. § szempontjából felhasználásnak minősül a többszörözés, terjesztés, a nyilvános előadás, a nyilvánossághoz közvetítés, az átdolgozás, valamint a kiállítás. Az ilyen jellegű felhasználásokhoz minden esetben a jogosult hozzájárulására van szükség. Vannak azonban bizonyos korlátok, amelyek esetében nem valósul meg jogsértés, ezek a védelmi idő lejárta, valamint a szabad felhasználás

intézménye. A védelmi idő azt jelenti, hogy a szerző halálától számított 75 év elteltével a mű szabadon felhasználhatóvá válik.

A szabad felhasználás egyes eseteit szintén az Szjt. sorolja fel. A kötet témájának szempontjából szükséges ezen intézmény tárgyalása, ugyanis az internetről történő jogellenes letöltések esetében az elkövetők rendszeresen hivatkoznak arra, hogy tevékenységük nem minősül másnak, mint szabad felhasználásnak, épp ezért a szerzői jogok megsértésének büntető törvénykönyvi tényállása nem is alkalmazható esetükben. Ez a védekezés, mint látni fogjuk, több ok miatt sem helytálló. A probléma helyes megközelítése érdekében először azt kell tisztáznunk, lehet-e jogszerű, illetve mikor jogszerű egy műnek az internetes felhasználása. A berni egyezmény[451] egy háromlépcsős tesztet határoz meg, amely szerint a részes országok csak annyiban engedhetik meg az irodalmi és művészeti művek többszörözését, amennyiben az ilyen engedély I. különleges esetre vonatkozik, II. nem sérelmes a mű rendes felhasználására, és III. indokolatlanul nem károsítja a szerző jogos érdekeit. Ez a háromlépcsős teszt vonatkozik az Szjt.-ben szabályozott szabad felhasználásra is. Jogszerű például egy interneten található szerzői mű letöltése akkor, ha az egyéni eredeti jellege alapján szellemi alkotásnak minősül, és a szerző engedélyével közvetítik a nyilvánossághoz. Ez esetben a nyilvánosan hozzáférhető mű saját adathordozóra való letöltése szabad felhasználásnak minősül.

Hogyan ítélendő meg az, amikor valaki az internetről saját maga számára letölt egy olyan művet, amelynek a nyilvánossághoz közvetítése a szerző hozzájárulása és engedélye nélkül történik? Tipikus esete lehet ennek egy warezszerverről történő letöltés, de akár a fájlcsere vagy egy videómegosztó platform tartalmának a letöltése is idesorolható. Ennek a kérdésnek a megválaszolása már jóval több problémát felvet, ugyanis a hatályos Szjt. nem tartalmaz semmilyen konkrét szabályt erre nézve. A gyakorlatban két álláspont alakult ki. Szentkuti Dániel szerint[452] a jogsértő forrásból történő letöltés mindenképpen jogellenes. Ezt az álláspontot támasztja alá az Szjt. is, amely szerint a szabad felhasználás is csak annyiban megengedett, amennyiben nem sérelmes a mű rendes felhasználására, és indokolatlanul nem károsítja a szerző jogos érdekeit. Nagy Zoltán András szerint, ha a feltöltés jogellenes, mert a feltöltő az adott szerzői művet a szerző engedélye nélkül terjeszti, akkor a letöltést is jogellenesnek kell értékelni a *ius ex iniuria non procreatur* (jogellenes cselekmény nem

451 Az irodalmi és a művészeti művek védelméről szóló 1886. szeptember 9-i berni egyezmény.
452 Dósa 2008: 359.

teremt jogszerűt) jogelvnek megfelelően. A jogellenes forrásból történő magáncélú másolatkészítés ellentmondana a berni egyezmény I. lépcsőjében meghatározott különleges eset feltételeinek is.

A másik oldal álláspontja szerint az ilyen letöltés a szabad felhasználás előírásaival nem ellentétes, a magáncélú másolás körébe tartozik. A magáncélú másolat készítése azt jelenti, hogy természetes személy magáncélra a műről másolatot készíthet, e körben a felhasználás díjtalan, és nem szükséges hozzá a szerző engedélye. Ennek egy feltétele van, hogy a másolat készítése jövedelemszerzés vagy jövedelemfokozás célját közvetve sem szolgálja. „A magáncélú másolást mint lehetőséget a jogalkotó elsősorban azért biztosítja a jogalanyok számára, mert a magánszférában végrehajtott többszörözési cselekmények gazdasági súlya viszonylag kicsi, ezért e magatartások jellemzően nem járnak a szerző jogainak indokolatlan csorbításával és nem okoznak neki jelentős vagyoni hátrányt."[453] Ez az elv azonban a digitális többszörözési eljárások tömeges elterjedésének köszönhetően erodálódott, ugyanis bárki tetszőleges mennyiségű másolatot készíthet, illetve a kópiák akár ingyenesen eljuttathatók szinte bárkihez, és ezzel már komoly vagyoni hátrányt lehet okozni a szerzőknek.

A szabad felhasználáshoz való jog nem korlátlan, maga az Szjt. is több ponton limitálja annak lehetőségeit. Nem vonatkozik a szabad felhasználás szoftverre és a számítástechnikai adatbázisra, valamint az Szjt. 35. §-a szerint nem minősül szabad felhasználásnak az sem, ha a műről más személlyel készíttetnek másolatot számítógépen, illetve elektronikus adathordozóra.

Nagy Zoltán András felvázolja a szerzői jogi jogsértések tipikus elkövetési módozatait a hálózatokon,[454] amelyek:

- weboldalakon szerzői mű a szerző engedélye nélkül történő megjelenítése;
- e művek ingyenes vagy díjfizetés ellenében történő letöltésének engedélyezése weboldalakról, FTP- vagy más szerverekről;
- szoftverek védelmi programjának feltöréséhez alkalmas programok feltöltése, onnan letöltés engedélyezése;
- DVD kódjainak feltörése, majd a DVD konvertálása más fájlformátummá;
- szerzői jogi műveket megjelenítő fájlok cseréje;
- hálózatokon keresztül történő (jogszerű vagy jogellenes) belépés és a számítógépről szoftverek lemásolása, használata, terjesztése stb.

[453] Dósa 2008: 285.
[454] Nagy 2009: 232.

A szerzői jogról szóló törvény terjesztésnek tekinti a mű eredeti vagy többszörözött példányainak a nyilvánosság számára történő hozzáférhetővé tételét, forgalomba hozatal vagy forgalomba hozatalra való felkínálás révén. Jó példa erre a warez, ahol „a feltöltés felkínálásnak értelmezhető, akár a szerzői mű a maga teljességében, akár csupán a hozzá vezető link jelenik meg a programban".[455]

A wareznak alapvetően 3 fajtája van:

1. A felhasználó egy szerverről tölti le a terméket (javarészt FTP). Ennek előnye, hogy nagyon gyors, hátránya, hogy elég centralizált, ebből következően könnyen lekapcsolható, ha lefoglalják a szervert, megtalálják rajta a jogosulatlanul megszerzett, hozzáférhetővé tett tartalmakat is. Felelősségre vonás szempontjából ez a legtisztább és legegyszerűbb cselekmény. Ha FTP-szerverre töltik fel a szerzői műveket (például filmeket), azokat a felhasználók többnyire emelt díjas sms-ek fejében letölthetik. De működnek ilyen jellegű ingyenes weboldalak is, például a nemrég bezárt Megaupload, ahova egyszerű regisztráció után bárki feltölthetett fájlokat, és böngészhetett a mások által feltöltött tartalmak között.
2. A felhasználók egymástól töltenek le szerver koordinálásával *(tracker),* vagyis fájlcserélést valósítanak meg. Ennek elnevezése a *peer to peer,* vagyis p2p, mint például a torrent vagy a DC++. Ez bár valamivel lassabb, nagy előnye, hogy kevésbé centralizált, és mivel a konkrét szerzői művek nem helyezkednek el a szerveren, felelősségre vonás szempontjából nagyon problematikus. Ezek esetében nem egy központi szolgáltató gép van, hanem a hálózat tagjai közvetlenül egymással kommunikálnak (Gnutella, µTorrent). Ezek közül a legnépszerűbb a torrent használata. „Az ún. BitTorrent technológia lényege, hogy a fájlokat a felhasználók szeletekben (torrent), darabokban töltik le egymástól oly módon, hogy a szeletek egymást »keresik meg« az interneten, minden csomópont megkeresi a hiányzó részhez a lehető leggyorsabb kapcsolatot, miközben ő is letöltésre kínálja fel a már letöltött fájldarabokat."[456] A torrentszerverek maguk tehát nem tárolnak fájlokat, hanem a tárolt fájlok jegyzékét és azok elérésének útját. A felhasználók a fájl nevére kattintva érik el azt a felhasználót, akinél a fájl egésze van, továbbá azokat a felhasználókat, akiknél az egész fájl egy-egy szeletkéje, részlete található. A torrentfájlok tartalma nem azonos a jogi védelmet élvező szerzői alkotással. A feltöltőnek nem is szükséges a letöltés utolsó mozzanatáig jelen lenni a hálózatban, ha a fájl egészét a felhasználók

[455] Nagy 2010: 34.
[456] Ibolya 2011: 49–59.

között a program szétosztotta, ezt követően a feltöltő kiszállhat, és a letöltők egymástól szerzik be a hiányzó fájlrészleteket.

3. A felhasználók egymástól töltenek le szerver koordinálása nélkül. Ez azért előnyös, mert teljesen decentralizált, így nincs egy központi szerver, amelynek megbénításával lekapcsolható a teljes hálózat. Hátránya, hogy a felhasználóknak maguknak kell megkeresniük egymást. Ennek során pásztázzák az internetet, és keresik, ki rendelkezik ugyanazzal a protokollal. Ha találnak ilyet, annak elmentik az IP-címét, és letöltik tőle az ő listáját az eddig ismert személyekről. Ennek a megoldásnak a hatékonysága nagyon kicsi, épp ezért ez a legkevésbé használt formája a wareznak.

Szerzői és büntetőjogi szempontból érdekes dilemmát vet fel a fájlcserélés helyzete. Fájlcserélés esetében az elfogadott gyakorlat szerint az Szjt.-ben rögzített felhasználási módok közül a nyilvánossághoz közvetítés, valamint többszörözés valósul meg. A letöltéssel a mű többszörözése valósul meg, amely az Szjt. 18. §-a értelmében szerzői engedélyhez kötött tevékenység. Többszörözés a mű anyagi hordozón való rögzítése, bármilyen módon, valamint egy vagy több másolat készítése a rögzítésről. A mű visszaosztása során a nyilvánossághoz közvetítés valósul meg, az Szjt. 26. § (8) bekezdése alapján a szerző kizárólagos joga, hogy művét a nyilvánossághoz közvetítse, és hogy erre másnak engedélyt adjon. E joga kiterjed különösen arra az esetre, amikor a művet vezeték útján vagy bármely más eszközzel vagy módon úgy teszik a nyilvánosság számára hozzáférhetővé, hogy a nyilvánosság tagjai a hozzáférés helyét és idejét egyénileg választhatják meg. Nemzetközi viszonylatban a fájlcserét igyekeznek komoly eszközökkel visszaszorítani, eddig kevés sikerrel. Nagy port kavart a Pirate Bay per, amelynek a végén marasztaló ítélet született az oldal tulajdonosával szemben. A Pirate Bay nevű torrentoldal 2003-ban indult Svédországban, 2006-ban a svéd hatóságok ellenőrzést tartottak a Rix Port80 internetszolgáltatónál, amelynek hálózatán volt elérhető a fájlcsere-szolgáltatás. Az elsőfokú ítéletben egy év szabadságvesztésre és 30 millió svéd koronás (800 millió forintos) kártérítés megfizetésére kötelezték az oldal tulajdonosait. Néhány nappal később azonban a Pirate Bay szerverei más országból újraindultak, és azóta is az egyik legnagyobb torrentszolgáltatást nyújtják. Hiába tehát a szigorú fellépés, a várt eredmény még a marasztaló ítélet ellenére is elmaradt. Sőt külön érdekesség, hogy az ítélet megszületése után több országban, köztük Svédországban is tüntetéseket tartottak a fájlcsere védelmében.

Közfelháborodást váltottak ki az internetes szerzői jogsértések meggátolására készített nemzetközi egyezménytervezetek, a SOPA és az ACTA is. A Stop Online

Piracy Act (a továbbiakban: SOPA) egy amerikai törvényjavaslat, amely drasztikusan bővítette volna az amerikai igazságszolgáltatás lehetőségeit az online szerzői jogsértés és hamisítás elleni harcban. A sértett fél kérésére a bíróság kényszeríthette volna az internetszolgáltatókat, hogy tegyék elérhetetlenné a jogsértő oldalt, az online keresőket, hogy távolítsák el a találataik közül, és a reklámszolgáltatókat és az online fizetési szolgáltatásokat, hogy ne továbbítsanak neki pénzt. A javaslat emellett szigorította volna a jogsértő anyagok közzétételéért járó büntetést: az ilyen anyagok online sugárzása *(streaming)* bűncselekménnyé vált volna, amelyet öt évig terjedő szabadságvesztéssel büntettek volna. Az Anti-Counterfeiting Trade Agreement (a továbbiakban: ACTA) az előbbi törvényjavaslat nemzetközi testvére, azaz a hamisítás elleni kereskedelmi megállapodás, azt a célt szolgálja, hogy az interneten terjedő kalóztartalmakkal szemben hatékony fellépést tudjanak megvalósítani. Az ACTA azt jelentheti, hogy bárkinek az internetes adatforgalmát monitorozhatják, és ha a különböző tartalomfelismerő szoftverek segítségével jogvédett tartalmakat azonosítanak be, akkor megindulhat a szankció az illető internetes tartalomszolgáltatóval, illetve az illető internetezővel szemben. Mindkét tervezet közfelháborodást váltott ki, ellenzői az internet cenzúrázását, valamint az információ szabad áramlásának és az információhoz való hozzáférés jogának csorbítását vélték bennük megtestesülni. Végül sem a SOPA, sem az ACTA nem lépett hatályba, ennek oka az erős társadalmi tiltakozás, amely az egyezmények megalkotását kísérte. A SOPA ellen olyan vállalatok is tiltakoztak, mint a Google, a Wikipedia vagy az Amazon, 2012. január 18-án mintegy 7000 weboldal sötétült el tiltakozás jelleggel. Az ACTA-t 2012-ben aláírták az Európai Unió tagállamai, köztük Magyarország is, azonban 2012 februárjában az Európai Unió Bírósága vizsgálatot indított, hogy az ACTA nem ellentétes-e az uniós joggal, s ratifikálását felfüggesztették.

Magyarországon is zajlottak említésre méltó torrentrazziák. Az egyik nagy visszhangot kiváltó torrentrazzia Magyarországon 2010-ben történt, amelynek során a rendőrök több mint 50 szervert lefoglaltak. Mindennek ellenére az akció kevés sikert hozott, hiszen két héttel később az összes torrentoldal újfent működőképes volt, az ügyben nem történt vádemelés sem.

Speciális helyzetben van az alkotások között a szoftver. Kunos Imre a szerzői és szomszédos jogok megsértése körében még kizárólag a szoftverkalózkodást említi.[457] A szoftverekkel kapcsolatos bűncselekmények jellemző elkövetési magatartásait az alábbiak szerint csoportosította:

[457] Kunos 1999: 28–42.

- munkahelyi, iskolai számítógépről szoftver jogosulatlan lemásolása és használata vagy továbbadása, illetve az így szerzett szoftver nagy tételű másolása;
- interneten behatolás saját vagy más cég szerverére, onnan szoftverek lemásolása, használata, továbbadása;
- legális kereskedelemből származó szoftverek másolása és továbbadása, amely történhet a szoftver önálló illegális kereskedelmével, de legjellemzőbb a hardverrel együtt történő értékesítés;
- nagy felhasználónál az engedélyezett licencszámnál nagyobb számú alkalmazás;
- kereskedelmi szoftverek védelmének feltörése;
- internetes kalózkodás, ahol a kereskedelmi szoftvert felteszik a website-ra, és onnan letölthetők.

A szoftverekkel kapcsolatos jogsértésekkel összefüggő bizonyítási problémákat vet fel Kökényesi-Bartos Attila.[458] Az egyik ezek közül, hogy a szerzői jogi törvény 59. §-a nem zárja ki, hogy a felhasználó biztonsági másolatot készíthessen a szoftverről, erre pedig az elkövetők előszeretettel hivatkoznak. Biztonsági másolat csak akkor készíthető, ha az a felhasználáshoz szükséges, és a szerző szerint egy magánszemély számára általában felesleges a biztonsági másolat készítése, hiszen „ha műpéldánya elveszne, megsérülne, bármikor fordulhat a forgalmazóhoz".[459]

A szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének vétségét több ok miatt problémás felderíteni és bizonyítani. Nagy Zoltán András *A Pirate Bay-per tanulságai* című tanulmányában négy ilyen körülményt fogalmaz meg,[460] ezek: a piaci érdekek, a tárhelyszolgáltatók tevékenysége, a közvetítő szolgáltatók érdekei és végül, de nem utolsósorban a kereső szolgáltatók működése. A piaci érdek az eladások, ezáltal a bevétel növelése. A boltok polcai pedig tele vannak olyan DVD-lejátszókkal, amelyek a DivX-es formátumokat is kezelik, és csak néhány lépést kell tenni a különféle márkájú és kinézetű MP3 lejátszókért. Valószínűleg ezeknek a termékeknek a gyártói tisztában vannak vele, hogy a .avi,.mp3 stb. kiterjesztésű fájlok zömmel illegális forrásból szerezhetők meg az internetről, ugyanakkor a fogyasztóknak olyan termékekre van kereslete, amelyek kezelik ezeket a formátumokat. A tárhely-, illetve a hálózati hozzáférést biztosító szolgáltatóknak lenne lehetőségük a fájlcsere korlátozására, illetve visszaszorítására. Vitathatatlan, hogy egyes tárhelyszolgáltatók különösen kedvező pozícióban vannak ahhoz, hogy a jogsértéseket megakadályozzák, a jogsértő jelleggel

[458] Kökényesi-Bartos 2010: 22.
[459] Kökényesi-Bartos 2010: 22.
[460] Nagy 2010: 33–40.

felkerült tartalmat eltávolítsák. A harmadik személyek tartalmainak tárhelyet biztosító szolgáltatók a felhasználási felételeikben maguk is szabályozhatják a felhasználók magatartását, mintegy kiegészítő védelmet biztosítva, másrészt bejelentések alapján közreműködnek a tartalmak eltávolításában is. A tárhelyszolgáltatók a tárhelybérlő által szervereikre feltöltött adatállományokat, ha nem is rendszeresen, de véletlenszerűen ellenőrizhetik, így az illegális tartalmak méretük és kiterjesztéseik alapján könnyedén azonosíthatók és ellenőrizhetők lennének. Azonban jogszabályi felhatalmazás hiányában ez megmarad lehetőségként, amellyel a tárhelyszolgáltatók ügyfélkörük megtartása érdekében vonakodva élnek. Nagy Zoltán András azt javasolja, hogy a tartalomszolgáltatóknak össze kellene fogniuk abban, hogy azon személyekkel, akikkel szemben polgári vagy büntetőeljárás indult, szerzői jogsértések miatt nem kötnek bérleti szerződést. Más a helyzet azonban azokkal a közösségimédiaplatform-szolgáltatásokkal és videómegosztókkal, amelyeket az Eker. irányelv, illetve a DSA tárhelyszolgáltatónak minősít, nekik ugyanis aktív fellépési kötelezettségük van a szerzői jogsértések ellen. Az Instagram[461] a felhasználó magatartását többféleképpen szankcionálhatja: a legenyhébb szankció a bejegyzés eltávolítása, ismételt jogsértés esetében azonban lehetőség van arra, hogy a szolgáltató a fényképek és videók közzétételének lehetőségét letiltsa, és egyes szolgáltatásfunkciókat blokkoljon. A legszigorúbb szankció a felhasználó kizárása a szolgáltatás igénybevételéből, a felhasználói fiók letiltásával vagy az oldal törlésével. A legnagyobb videómegosztóplatform-szolgáltató, a YouTube kétféle rendszert is bevezetett a szerzői jogot sértő alkotások eltávolítására. Az egyik egy felhasználói bejelentéseken alapuló „három csapás"-rendszer, amelyben ha a tartalom közzétevője 90 napon belül három jogsértést valósít meg, eltiltják a szolgáltatás használatától, felhasználói fiókját megszüntetik.[462] A bejelentések megtételére az Egyesült Államok egyik jogszabálya, a Digital Millenium Copyright Act (DMCA) alapján biztosít lehetőséget a szolgáltató. A másik rendszer a jogtulajdonosokkal való megállapodás révén működtetett mesterséges intelligencián alapuló ContentID rendszer.[463] A ContentID rendszer alkalmas arra, hogy másodpercek alatt azonosítsa azokat a tartalmakat, amelyeket más szerzői jogának megsértésével töltöttek fel, az észlelés jogkövetkezménye viszont a platform és a jogtulajdonos megállapodásától függően többféle lehet. Természetesen lehetőség van arra, hogy ezeket a tartalmakat a szolgáltató azonnal eltávolítsa, lehetőség van azonban arra is,

461 Instagram Help Center 2023.
462 YouTube 2023b.
463 YouTube Súgó 2023a; 2023e.

hogy a tartalmat csak bizonyos földrészeken, régiókban blokkolják, sőt a jogtulajdonos akár úgy is határozhat, hogy a videót a hálózaton hagyja, azonban az annak környezetében megjelenő hirdetések bevételeiből ő kíván részesedni. Mint látjuk, ezekben az esetekben alapvetően nem az az igény dominál, hogy a felhasználót – aki adott esetben nincs is feltétlenül tudatában jogsértő cselekedetének – minél szigorúbban büntessék meg, hanem a vagyoni kár mérséklése.

A harmadik kulcspont az internet-hozzáférést nyújtó közvetítő szolgáltatók tevékenysége. Ezeknek az egyszerű hozzáférés-szolgáltatóknak a hálózatán zajlik a forgalom, így ők gyakorlatilag mindent látnak, amennyiben a felhasználó nem alkalmaz VPN-t, forgalmazása technikailag figyelemmel kísérhető, a szerződési feltételek eszközével korlátozható is lenne. Az ügyfélkör bővítése, a minél nagyobb sávszélesség elfogadtatása magasabb előfizetési díjért azonban komoly ellenérdek, így ők sem tesznek lépéseket a szerzői jogsértések visszaszorítása érdekében. „A keresőszolgáltatók és a cache-szolgáltatók kapcsán egy más jellegű, *in concreto* jogi felelősség vethető fel" [464] – írja Nagy Zoltán András, aki arra is felhívja a figyelmet, hogy e szolgáltatók egy linkadatbázist tárolnak. Az általuk tárolt és a keresésekre válaszként nyújtott linkadatbázis segítségével nemcsak a szerzői alkotásokat tartalmazó linkek érhetők el, hanem a tiltott tartalmat tartalmazó weboldalak is. A legtöbb keresőszolgáltatónál azonban megfigyelhető az a tendencia, hogy ha valaki jogsértő tartalomra hivatkozással felhívást intéz hozzájuk, eltávolítják a kérdéses linket az adatbázisból, csak a jogsértés tényére való utalást feltüntetve a keresési eredmények között.

A Btk. 385. § (5) bekezdése egy mentesítő szabályt iktat be. Eszerint nem valósítja meg az (1) bekezdés szerinti bűncselekményt, aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait többszörözéssel vagy lehívásra történő hozzáférhetővé tétellel sérti meg, feltéve, hogy a cselekmény jövedelemszerzés célját közvetve sem szolgálja. Ennek a rendelkezésnek a hatása főleg a warez- és fájlcserélő oldalak felhasználóit érintheti, mint ahogy azt a törvény indokolása is megemlíti. Dudás Ágnes ugyanakkor rámutat:

> [A törvénynek] „nem célja igazolni e rendszerek működését, ugyanakkor a büntetőjog, mint végső eszköz szempontjából indokolatlannak tűnik a nem jelentős mennyiségű szerzői mű vagy kapcsolódó jogi teljesítmény vonatkozásában megvalósuló, személyes célokat szolgáló felhasználások tömeges kriminalizálása. A szerzői jog területén fennálló nemzetközi kötelezettségeink, így különösen a TRIPS egyezmény csupán a szándékos és kereskedelmi mértékű szerzői jogi kalózkodásra nézve

[464] Nagy 2010: 36.

> teszik kötelezővé a büntetőjogi szankciók előírását, a kereskedelmi mértéket el nem érő cselekmények esetén nincs olyan körülmény, amely ezen a területen a nemzetközi normáknál szigorúbb büntetőjogi szabályozást indokolná."[465]

Ezt a bekezdést mindazonáltal együtt kell értelmezni ugyanezen § (3) bekezdésével, amely értékhatár szerint minősíti az (1) bekezdésben foglalt tényállást. A 385. § (3) bekezdés minősített esetként deklarálja a „nagyobb vagyoni hátrány" okozását. A törvény értelmező rendelkezése szerint nagyobb vagyoni hátrányról beszélhetünk, ha az okozott kár és az elmaradt vagyoni előny 500 001 és 5 000 000 forint közöttre tehető. Vajon ez a szabályozás azt jelenti, hogy 500 ezer forint alatt szabad a pálya a fájlcserélőknek? Távolról sem. Mezei Péter szerzői joggal foglalkozó blogján[466] felhívja a figyelmet arra, hogy a büntetőeljárásról szóló törvény módosulásával a szerzői jog megsértéséből eredő büntetőeljárásoknál a Nemzeti Adó- és Vámhivatal (NAV) állapítja meg a vagyoni hátrány összegét. Ezt az összeget pedig a NAV az internetes terjesztés minimális licencdíja alapján állapítja meg, amely ma filmenként 800 dollár, míg zeneszámoknál a Magyar Hangfelvétel-kiadók Szövetségének (MAHASZ) jogdíjtáblázata az irányadó, ez alapján egy dalért 320, egy albumért 3200 forint kárértéket számolnak fel. Ilyen értékekkel számolva pedig nagyjából három film letöltése az, amivel még nem valósít meg a felhasználó bűncselekményt.

[465] Dudás 2014: 139.
[466] Mezei 2012.

V. Online fenyegetések a büntetőjog határán

Az online környezetben egyre nagyobb kihívást jelentenek azok a magatartások, amelyeket a büntetőjog jelenleg nem fenyeget önálló szankcióval, de a társadalomra nézve károsak és helytelenítendők. Ezeket a magatartásokat Parti Katalin és Kiss Tibor nyomán cyberdevianciának nevezhetjük.[467] A deviancia fogalma minden olyan magatartást magában foglal, amely egy adott közösségben uralkodó és a közösség többsége által egységesen elfogadott normáktól (legyen akár jogi, erkölcsi vagy szokásnorma) való eltérést, elhajlást jelent.[468] A kibertérben előforduló deviáns magatartások közé tartoznak azok a cselekmények, amelyek büntetőjogi normába ütköznek, de azok is, amelyek „csak" erkölcsi normát sértenek. Az interneten előforduló, de a büntetőjog által önálló tényállással nem kriminalizált, társadalomra veszélyes cselekmények esetében a jogalkotó előtt két út áll: az egyik, hogy megpróbálja ezeket a cselekményeket valamilyen már létező büntetőjogi tényállás ernyője alá vonni, a másik pedig, hogy új tényállást alkot. Mindkét megoldásnak megvannak a maga előnyei és hátrányai. A meglévő tényállások sok újfajta magatartásra is ráilleszthetők, ezért a meglévő rendelkezések alkalmazásával elkerülhető a büntető törvénykönyv hosszan tartó és nehézkes módosítása, a megjelenő jelenségekre sokkal rugalmasabban adható válasz. A módszer hátránya azonban, hogy megkívánja a normaszöveg részéről az általános, nagy vonalakban történő szövegezést, amely, noha magatartásoknak széles körét képes lefedni,

[467] Kiss–Parti–Prazsák 2019.
[468] Kiss–Parti–Prazsák 2019: 56.

nem feltétlenül alkalmas arra, hogy az egyes devianciák jellegzetességeit tekintetbe vegye. A másik módszer, a normaalkotás ellenben lehetővé teszi, hogy az új tényállások megfogalmazásakor a jogalkotó figyelembe vegye mindazokat a tulajdonságokat, amelyek az adott magatartást jellemzik. Ez a jogbiztonságot és a normavilágosságot is előmozdítja, hiszen egzakt, jól lehatárolható tényállásokat eredményez, amelyek szűk körben teszik lehetővé a jogalkalmazó általi kötetlen értelmezést.

A kötet jelen része olyan magatartásokkal foglalkozik, amelyek nyilvánvaló problémát jelentenek az online térben, ám nem kapcsolódik hozzájuk önálló tényállás a Btk.-ban. Az egyes cselekmények leírása és a jelenlegi szabályozási környezet bemutatása mellett *de lege ferenda* javaslatokkal is kívánok élni. Mivel a bemutatott tényállások között több olyan is van, amelyek esetében szükség lenne önálló tényállások megfogalmazására, vagy legalább a meglévőknek a változó körülményekhez igazítására, az egyes részekhez kapcsolódva az esetleges jövőbeli szabályozás alkotmányos alapjairól is szó esik majd. Ahogyan az emberi magatartások általában, a kibertér devianciái is nagyon sokfélék, így lehetetlen vállalkozás az összes online megjelenő ártalmas magatartásról kimerítő jelleggel szólni. A kötetben így csak a legnagyobb társadalmi problémákat okozó magatartásokat tárgyalom. Idesorolhatók:

- a szexuális tartalmakkal kapcsolatos visszaélések (köztük a hozzájárulás nélkül közzétett szexuális felvételek [bosszúpornó] és a hamisított felvételek [*deepfake* pornográfia]);
- veszélyes magatartásokra buzdítás;
- öncélú, brutális erőszak-ábrázolás;
- a behálózás *(grooming);*
- a *cyberbullying;*
- az álhírek, a félretájékoztatás egyes fajtái *(fake news);*
- terrorista tartalmak.

A szexuális tartalmakkal kapcsolatos visszaélések

Az egyre olcsóbb mobileszközök, jobb minőségű videókamerák és a közösségi oldalak megteremtették annak a lehetőségét is, hogy ne csak a pornográfiaipar professzionális tartalom-előállítói, hanem bárki készíthessen és oszthasson meg szexuális jellegű tartalmakat. Az eroticizált, hovatovább kimondottan pornográf tartalmak ugrásszerű növekedése nemcsak az erkölcs és a morál társadalmi jelentőségének erodálódásához

vezet, hanem komoly individuális veszélyeket is rejt magában. A tartalmak számával arányosan nőnek a szexuális jellegű visszaélések, ami pedig kimondottan aggasztó, hogy a jogsértések nem kizárólag kisebb weboldalakon történnek, hanem milliók által használt népszerű szolgáltatásokban is. Az egyik legnagyobb pornóvideó-megosztó esetében egymást érik a botrányok, a szolgáltatásban található jogsértő anyagok, zömében gyermekpornográfia, valós szexuális erőszakot ábrázoló felvételek, hozzájárulás nélkül közzétett szexuális felvételek miatt. A *New York Times* 2020-ban terjedelmes cikket hozott le arról, hogy a Pornhub platformon, amelyre felhasználók is tölthetnek fel tartalmat, számtalan kiskorúakat ábrázoló felvétel[469] található. A cikket követően két nagy hitelkártya-szolgáltató, a Visa és a Mastercard is felfüggesztette[470] a platformon keresztül bonyolított fizetési szolgáltatását. A Visa ellen két évvel később bírósági eljárás indult,[471] mivel feltehetően tudott arról, hogy a Pornhubot üzemeltető Mindgeek gyermekpornográf tartalmakat monetizál. A platformszolgáltató ugyan ígéretet tett arra, hogy jobban odafigyel a tartalomszűrésre, de nem sok idő telt el az újabb botrányig. 2022 nyarán a *New Yorker* hozott le egy cikket arról, hogy az áldozatoknak egyáltalán nincs könnyű dolguk,[472] ha azt szeretnék elérni, hogy az őket ábrázoló felvételeket töröljék. A cikkben leírt történetekből az körvonalazódik, hogy a platformszolgáltatók majdhogynem az áldozatokat hurcolják meg, akiknek gyakran ügyvédi segítséget kell igénybe venniük ahhoz, hogy a szolgáltató számára is elfogadhatóan meg tudják indokolni, miért kérik az őket ábrázoló tartalmak eltávolítását. A szóban forgó felvételek pedig az eltávolítást követően hamar újra megjelennek.

Jelen fejezet egyik célja, hogy bemutassa azokat a visszásságokat, amelyek napjainkban a szexuális tartalmakkal kapcsolatban merülnek fel, és feltárja, hogy ezek kezelésére a jelenlegi jogszabályi kereteken belül rendelkezésre állnak-e adekvát megoldások. A fejezetben már a címválasztáskor is tudatosan tartózkodtam a bűncselekmény kifejezés használatától, főként amiatt, hogy a vizsgált magatartások között több olyan is van, amely esetében élénk szabályozási-jogpolitikai diskurzus folyik a büntethetőségről, illetve a büntetendőségről. A szabályozási megoldások között különös figyelmet szentelünk a büntetőjognak, azt vizsgálva, hogy vajon indokolt-e az *ultima ratio* jellegű eszközökhöz fordulni, ha szexuális tartalmakkal kapcsolatos visszaélésekről van szó, és ha igen, indokolt-e új tényállások megalkotása, vagy elegendő-e ezeket

469 Kristof 2020.
470 Robertson 2020.
471 Robertson 2022.
472 Kolhatkar 2022.

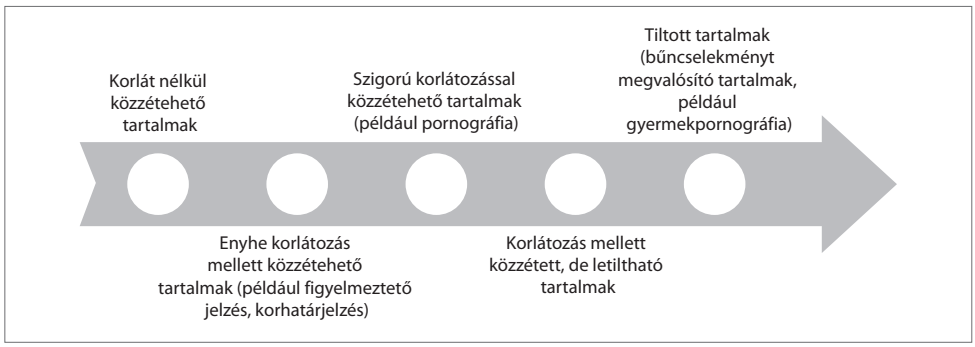
a cselekményeket a már meglévő rendelkezések keretei között kriminalizálni. A szexuális tartalmakkal kapcsolatos jogellenes cselekmények az online térben számtalan formában megvalósulhatnak, éppen e sokszínűség miatt a problémahalmaz kezelésére nem adható uniformizált megoldás. Ahogyan a jogellenes magatartások is különböző formákat ölthetnek, az ezekre adott válaszoknak is differenciáltaknak kell lenniük.

A pornográfia szabályozásáról általában

A szexuális tartalmakkal kapcsolatos visszaélések több, jogtudományi szempontból is érdekes kérdést felvetnek, annak ellenére, hogy a szabályozásuk jelenleg nem áll a tudományos érdeklődés középpontjában. Mielőtt azonban rátérnénk arra, hogy mit értünk pontosan „visszaélések" alatt, a kontextus megteremtése érdekében érdemes néhány szót ejteni a pornográfia szabályozásáról általánosságban. A téma összetettségét illusztrálja, hogy a pornográfiaszabályozás jogtudományi szempontból három síkon is vizsgálható: alkotmányjogi, tartalomszabályozási és büntetőjogi síkon. Az alkotmányjogi síkon a pornográfia és a szólásszabadság egymáshoz való viszonyát érdemes górcső alá venni, míg a tartalomszabályozás síkján elsősorban azokról a médiajogi szabályokról kell szólni, amelyek közérdekvédelmi indokkal teszik lehetővé a tartalomterjesztés korlátozását. A három sík közül a legtöbb kurrens kérdés a büntetőjogi síkon merül fel.

Noha időről időre megjelennek a társadalmi diskurzusban a betiltásra irányuló kezdeményezések, a pornográfia önmagában nem jogellenes. Ez természetesen nem jelenti azt, hogy minden korlátozás nélkül közzétehetők az ilyen jellegű tartalmak, a sérülékenyebb felhasználói csoportok – különösen a kiskorúak – védelme indokolhatja bizonyos tartalmi korlátok felállítását, a pornográf tartalmakra így az általános szabályoknál szigorúbb előírások vonatkoznak. Ha egy skálán jelenítjük meg a tartalmakra vonatkozó korlátozások rendszerét, a pornográfia valahol a skála közepén helyezkedik el (lásd 6. ábra).

A skála egyik végpontján a mindenféle korlát nélkül közzétehető tartalmak helyezkednek el, idetartozik a médiaszolgáltatók műsorszámainak és a felhasználók által közzétett videóknak a nagyobbik része; szexualitás ezekben a tartalmakban nem kaphat helyet. A skála közepén helyezkednek el azok a tartalmak, amelyeknek a közzététele nem tilos, ellenben szigorú előírásokhoz kötött.



6. ábra: *A tartalomkorlátozások rendszere*

Forrás: A szerző saját szerkesztése

A pornográfián kívül idetartoznak az öncélú vagy túlzott erőszakot ábrázoló tartalmak, illetve bizonyos termékek (tipikusan alkohol-, illetve dohánytermékek) reklámjai. A hozzáférést korlátozó szabályok ebben az esetben médiaigazgatási, közigazgatási jellegűek, és a normaszegő magatartás szankciója is ehhez igazodik.

Teljesen más a helyzet a skála másik végén, ahol azok a tiltott tartalmak helyezkednek el, amelyeknek a közzététele bűncselekményt valósít meg (ezek legtipikusabb példája a gyermekpornográfia). Ezeknél nem csupán az a cél, hogy a teljes potenciális közönséget elzárjuk a hozzáféréstől, de az is, hogy a fogyasztók és az előállítók felelősségre vonása büntetőjogi szankciókkal megtörténjen. A skála túlsó vége elé azonban egy olyan kategória is beékelhető, ahol a szigorú tartalomkorlátozások mellett a sérelmet elszenvedő fél akaratától függ, hogy büntetőjogi útra tereli-e az ügyet, és kéri-e a tartalom tiltását. A személyiségi jog megsértésével járó cselekmények esetében a büntetőjogi szankcióval való fenyegetettség több esetben fennáll, de nem szükségszerűen bekövetkező eredménye a jogsértő cselekménynek. A személyiségi joggal kapcsolatos bűncselekmények többsége (így például a rágalmazás és a becsületsértés) is magánindítványra büntethető, vagyis magánvádas eljárás, ahol nem az állam, hanem maga a sértett léphet fel büntető igényével. Többnyire azonban a személyiségi jogsértések esetén a magánjogi igényérvényesítés a domináns, mivel polgári peres eljárás keretében is lehetőség van jóvátételt kérni, ami a sértett oldalán gyakran egyszerűbb és gyorsabb módja az ügy rendezésének. Jórészt ebbe a csoportba tartoznak az olyan tartalmak, amelyek előállításának és terjesztésének kimondottan kedvez a közösségi média és a mesterségesintelligencia-alapú tartalomszerkesztő

alkalmazások könnyű hozzáférhetősége. Ilyen újfajta jelenség a szexuális felvételek hozzájárulás hiányában történő közzététele, a bosszúpornó *(revenge porn)*[473] és az algoritmusok által manipulált felvételek *(deepfake)*[474] közzététele.

A hozzájárulás nélkül közzétett szexuális felvételek szabályozása

A hozzájárulás nélkül közzétett szexuális felvétel *(non-consensual sexual imagery)* kifejezés valójában nem jogi terminológiai fogalom, inkább olyan általános megjelölés, amellyel azokat a visszaéléseket illetik, ahol szexuális jellegű felvétel közzétételére az abban szereplő személy(ek) kifejezett hozzájárulása nélkül került sor. A köznyelvben a jelenséget sokszor emlegetik bosszúpornóként *(revenge porn),* ez azonban a jelenségnek csak egy mozzanatára mutat rá, arra, amikor egy-egy szexuális felvételt bosszúvágyból, például egy párkapcsolat megromlását követően tesznek közzé. Jogtudományi szempontból a bosszúpornó fogalom használatát kerülendőnek tartom, hiszen a jelenség hátterében sokkal összetettebb problémakör húzódik, amelyet indokolatlanul szűkítene, ha kizárólag a bosszúvágy által fűtött cselekményekkel foglalkoznánk. A szexuális felvételek hozzájárulás hiányában történő közzététele David Ryan szerint történhet anyagi haszonszerzés vagy becsületsértés céljából, de akár egy zaklatásba vagy párkapcsolati erőszakba is illeszkedhet.[475] Már önmagában a hozzájárulás hiánya is többféle szituációhoz kapcsolódhat: az első, amikor a felvétel elkészítése a sértett tudtával és beleegyezésével történt, a nyilvánosságra hozatala azonban nem, a második, amikor a sértett a szexuális aktusba ugyan beleegyezett, a felvételkészítésbe és annak a nyilvánosságra hozatalába viszont már nem, esetleg nem is tudott arról, hogy felvétel készül (ez az úgynevezett kukkolás, avagy *peeping*). A harmadik és legsúlyosabb eset, amikor a sértett magába az aktusba sem egyezett bele (például amikor magatehetetlen sértett ellen elkövetett szexuális erőszakról készül felvétel). Kerülendőnek tartom a pornográfia kifejezés használatát is, hiszen ez a kifejezés összeforrt a kereskedelmi céllal előállított szexuális tartalmak körével, amelyeket a szereplők hozzájárulásával készítenek és tesznek közzé. A hagyományos

[473] A bosszúpornónak jelenleg nincsen elfogadott általános definíciója. Jelen kötet a bosszúpornó kifejezést azokra a szexuális tartalmakra használja, amelyeket az abban szereplő személy(ek) hozzájárulása, tudta nélkül készítettek és/vagy tettek közzé a világhálón.

[474] Deepfake pornográfiának nevezzük azokat a szexuális tartalmakat, amelyeket algoritmusok segítségével, valós felvételek montázsolásával készítenek el.

[475] Ryan 2018: 1053–1076.

pornográfia célja alapvetően a szexuális vágykeltés – előállítására egy egész iparág jött létre –, és haszonszerzési céllal történik, ez azonban nem mondható el a hozzájárulás nélkül közzétett szexuális felvételekről, ahol a közzétevő fő célja a felvétel egy vagy több szereplőjének megalázása, vagyis sérelem okozása.

Mivel viszonylag újfajta magatartásról van szó, az Európai Unióban nem mindenhol foglalkoztak jogalkotási szinten a jelenséggel, egyes országokban – köztük Magyarországon – pedig meglévő jogszabályi rendelkezések keretei közé igyekeznek beszorítani azt.

Hozzájárulás nélkül közzétett szexuális felvételek az Európai Unió egyes tagállamaiban és az Egyesült Királyságban

Az EU-ban viszonylag kevés tagállam rendelkezik kifejezetten olyan jogszabályokkal, amelyek a hozzájárulás nélkül közzétett szexuális felvételek kérdését igyekeznek rendezni. A hozzájárulás nélkül hozzáférhetővé tett szexuális felvételek szabályozásának egyik úttörője Olaszország, ahol a 69/2019. számú, az olasz büntető törvénykönyvet módosító jogszabály vezette be a szexuális tartalmú képek vagy videók tiltott terjesztésének tényállását a büntetőjogba. Az olasz szabályok meglehetősen szigorúak, a hozzájárulás nélkül elküldött, továbbított, nyilvánosságra hozott vagy közzétett szexuális tartalmú képek és videók esetében az elkövetőt hat évig terjedő szabadságvesztéssel, valamint 5-15 ezer euró közötti bírsággal rendeli sújtani.

A német büntető törvénykönyv szerint jogszerűtlennek minősített tartalmak körébe tartozik a becsületsértés (§ 186), a szándékos becsületsértés (§ 187) és az intim magánszféra megsértése fényképfelvételek készítése által (§ 201a).

Franciaországban a digitális köztársaság törvény (Loi pour une République numérique) 2016 óta büntetni rendeli azokat, akik más intim szféráját szándékosan megsértik, a jogszabály kifejezetten megjelöli a szexuális felvételekkel kapcsolatos visszaéléseket,[476] és a közzétételükért két év szabadságvesztés és 60 ezer eurós bírság kiszabását rendeli el.

Az Egyesült Királyságban 2015 óta bűncselekmény magánjellegű szexuális felvételt vagy videót hozzájárulás nélkül megosztani.[477] A jogszabályt számos kritika

[476] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique Article 67.
[477] Erről a 2015-ös Criminal Justice Court Act rendelkezik.

érte, főképp amiatt, hogy csak azokat az eseteket rendeli büntetni, ahol a közzététel gyötrelem okozásának céljából történik, tehát ha az elkövető arra hivatkozik, hogy ilyesmi nem állt szándékában, elkerülheti a felelősségre vonást.

Hozzájárulás nélkül közzétett szexuális felvételek Magyarországon

A szexuális felvételek hozzájárulás nélküli közzététele mint a Parti Katalin és szerzőtársai által cyberdevianciaként[478] jellemzett magatartás nem jelenik meg önálló tényállásként a büntető törvénykönyvben. Mivel a hozzájárulás nélküli közzététel a cselekmény szituációs elemeinek függvényében több bűncselekmény tényállását is kimerítheti, a Btk. több deliktuma is szóba jöhet az elbírálás során. A sértettnek személyes adattal visszaélés, zaklatás, rágalmazás, becsületsértés, szexuális kényszerítés, zsarolás, valamint becsület sértésére alkalmas hamis hang- vagy képfelvétel készítése miatt is lehetősége van a rendőrséghez fordulni, a felsoroltak közül azonban nem mindegyik magánindítványra üldözendő cselekmény, így nem indifferens, hogy melyik képezi az eljárás tárgyát. Mivel egyik felsorolt tényállás sem kifejezetten szexuális felvételek hozzájárulás nélküli közzétételének a kriminalizálását szolgálja, ezért a tényállásszerűség vizsgálatakor számos problémába ütközhet a jogalkalmazó. A Clare McGlynn és Erika Rackley által a brit jogrendszer vonatkozásában megfogalmazott kritika[479] jelen esetben a magyar szabályozásra is jól ráillik, a szabályrendszer ugyanis nem kimondottan a szexuális felvételek hozzájárulás nélküli közzétételét kezeli, éppen ezért töredezett, és legfeljebb csak egyedi esetek kezelésére alkalmas.

A szexuális kényszerítés (Btk. 196. §) esetében például tényállási elem, hogy maga az aktus is a sértett akarata ellenére történjen. A hozzájárulás nélkül közzétett felvételek esetében azonban a sértett az aktusba többnyire beleegyezik, sőt gyakran abba is, hogy arról felvétel készüljön, a hozzájárulás kizárólag a közzétételre nem terjed ki. A zaklatás tényállása (Btk. 222. §) szintén nem minden esetben alkalmazható, mivel a cselekmény elkövetésének feltétele a rendszeres és tartós háborgatás, amely egyetlen kép vagy videó közzététele esetén nem valósul meg. Szóba jöhet esetleg a veszélyes fenyegetéssel elkövetett zaklatás, ám itt a fenyegetés általában nem a felvételek közzétételével egyidejűleg történik meg, hanem éppen a felvétel nyilvánosságra hozatalával

[478] Kiss–Parti–Prazsák 2019.
[479] McGlynn–Rackley 2017.

fenyeget a terhelt. A rágalmazás tényállása (Btk. 226. §) elméletben alkalmazható a bosszúból közzétett szexuális felvételek esetén, már amennyiben egy videófelvételt tényállításnak tekintünk. A Btk. indokolása szerint „tényállítás az olyan nyilatkozat, amely a múltban megtörtént vagy a jelenben megtörténő eseményre, jelenségre vagy állapotra vonatkozik". A filmfelvétel, amely egy szexuális aktus megtörténtét mutatja be, önmagában még nem minősíthető a közlő nyilatkozatának. A feltöltő által hozzáfűzött magyarázat, leírás azonban már felfogható ekként, így mindenképpen vizsgálni kell, hogy a közzétételre milyen kontextusban került sor. Becsületsértés (Btk. 227. §) abban az esetben valósulhat meg, ha a szexuális felvétel közzétételét becsületsértésre alkalmas egyéb cselekménynek fogjuk fel. A zsarolás tényállásának az elkövető haszonszerzési célzata szükségszerű eleme (Btk. 367. §), tehát a bosszúból közzétett szexuális felvételek esetén csak akkor alkalmazható, ha az elkövető anyagi haszonra törekedve oszt meg intim felvételeket, vagy helyezi azok feltöltését kilátásba. A hozzájárulás nélkül közzétett szexuális felvételekre leginkább a személyes adattal való visszaélés tényállása illik. A magyar bírósági gyakorlat a képmáshoz való jog mint személyiségi jog védelméből kiindulva adatvédelmi alapokra helyezi az intim felvételek hozzájárulás nélküli megosztásának kérdését. A magyar bírósági gyakorlatban a személyes adat (e körbe tartozik a képmás is) jogosulatlan kezelése jelentős érdeksérelmet okoz abban az esetben, ha szexuális felvételek közzétételéről van szó.

Hazai joggyakorlat

Az első nagyobb sajtóvisszhangot kapó eset 2010-ben történt. Az adatvédelmi biztos 2010-es beszámolója számot ad arról, hogy két weboldal, az excsajok.hu, illetve az expasik.hu működésével kapcsolatban több panasz is érkezett. A nevezett portálokon lehetőség volt megjelentetni fényképeket és videókat, amelyek mellett gyakran a felvétel szereplője beazonosíthatóságát elősegítő adat is szerepelt. Az adatvédelmi biztos személyes adattal visszaélés vétsége miatt feljelentést tett, amelyet követően eltávolították a kérdéses oldalt. Az eltávolítás azonban csak átmeneti volt, a portálok tartalmát nem sokkal később feltöltötték egy külföldi szerverre, és egy palaui doménen még 2020 májusában is elérhetők voltak.

Jelentős érdeksérelmet okozott az a terhelt is, aki a volt házastársáról, annak tudta és beleegyezése nélkül, a személye azonosítását lehetővé tevő szexuális felvételeket hozott nyilvánosságra egy internetes közösségi platformon (Fővárosi Törvényszék, 42(II.)Kb.1327/2015).

Hozzájárulás nélkül közzétett szexuális felvételek az Egyesült Államokban

A kontinentális európai szabályokhoz viszonyítva egészen új aspektusból tárulkozik fel a probléma, ha a *common law* jogrendszerek felől közelítünk hozzá. A hozzájárulás nélkül közzétett szexuális felvételek kérdését az amerikai kiberbűnözéssel kapcsolatos fejezetben szándékosan nem tárgyaltam, hiszen szövetségi szinten ezek a tartalmak egyáltalán nem szabályozottak. Néhány állam, köztük New York, Maine és New Jersey már büntetni rendelik a hozzájárulás nélkül közzétett szexuális felvételeket, ezt a szabályozási vívmányt azonban beárnyékolja az az alkotmányossági vita, amely a pornográf felvételek és a szólásszabadság korlátozása mentén bontakozott ki. Az amerikai alkotmányjogban a szólásszabadság olyan kitüntetett alapjog, amelynek igen kevés esetben kell engednie. A szólásszabadság csak kevés esetben korlátozható, a korlátozások listája pedig rövid és zárt. A hozzájárulás nélkül közzétett szexuális felvételeket kriminalizáló törvényeknek az alkotmányossága azért kérdéses, mert – ahogyan több más szerző mellett Andrew Koppelman[480] is rávilágít – ezek a jogszabályok a közléseket, a „beszédet" a tartalom alapján korlátozzák, ami az Egyesült Államokban tilos, kivéve, ha kényszerítő állami érdekről *(compelling state interest)* van szó. A Reed v. Gilbert ügyben a Legfelsőbb Bíróság kimondta, hogy egy közlés korlátozása akkor minősül tartalomalapúnak, ha a tárgyalt téma, a kifejtett gondolat vagy üzenet miatt korlátozzák.[481] A tartalomalapú korlátozás tilalma alól ugyan vannak kivételek, például a gyűlöletkeltés, a gyermekpornográfia, az obszcenitás és a magánszemély sérelmére elkövetett becsületsértés, a bosszúpornónak nevezett jelenség azonban egyik kategóriába sem illik. A United States v. Stevens ügyben azt is kimondta a Legfelsőbb Bíróság, hogy a védelmet nem élvező beszéd kategóriáit nem lehet tovább bővíteni. A bíróság álláspontja szerint az Alkotmány maga nem olyan dokumentum, amely korlátokat állít, ezért a szólásszabadság korlátait a bíróság állapította meg, és az összes, a bíróság által konstituált korlát a védelmet nem élvező közlések régen lefektetett és korábban elismert kategóriáin alapul.[482] A Legfelsőbb Bíróság felfogása szerint a szólásszabadság csak akkor korlátozható erőteljesebben, ha a szóban forgó korlát a gyakorlatban alkalmazott, rég elfogadott, közmegegyezésen nyugvó tradíción alapul. A hírértékkel nem bíró, magánjellegű, hozzájárulás nélkül

480 Koppelman 2016: 661–693.

481 Regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed – Reed v. Gilbert, 135. S. Ct. 2218, 2227 (2015).

482 United States v. Stevens, 559 U.S. 460, 470, 471 (2010).

közzétett szexuális tartalmak korlátozásához azonban nem kapcsolódik a társadalom által elfogadott hagyomány, mivel az elmúlt évek egyik újhullámos jelenségéről van szó.

További probléma a szexuális felvételek hozzájárulás nélküli közzétételének a korlátozásával az is, hogy a károkozás, amelyen a korlátozás alapulna, nézőpontalapú. Egyes vélemények nézőpont alapján történő diszkriminálása *(viewpoint discrimination)* pedig az Egyesült Államok jogrendszerében szintén tilos. A Snyder v. Phelps ügyben a Legfelsőbb Bíróság kimondta, hogy egyes közlések nem tilthatók meg pusztán azon az alapon, hogy a társadalom egy csoportja azokat sértőnek találja, és úgy találta, hogy a szólásszabadság védelmét élvezi az, amikor tüntetők egy Irakban elhunyt katona temetésén „Isten utálja az USA-t", „Köszönöm Istenem a 9/11-et", „Köszönet Istennek a halott katonákért" feliratú transzparensekkel demonstrálnak.[483] Ezt a logikát követve Koppelman kifejti,[484] hogy a bosszúpornó esetében a sérelmet az okozza, hogy a közönség vagy annak egy része elfogadja a közzétevő nézőpontját, azt, hogy a képen, videóban szereplő nő egy mindenre kapható, értéktelen szajha. A közlés korlátozásával a jogalkotó azt az attitűdöt ítélné meg hátrányosan, amely elítéli azokat a nőket, akikről ilyen felvétel került nyilvánosságra. Koppelman amellett érvel, hogy az amerikai Legfelsőbb Bíróság által meghatározott kivételek a szólásszabadság Első Alkotmánykiegészítésben biztosított jogának merev értelmezésén alapulnak, ez a merev értelmezés pedig a szólásszabadság alapvetően liberális felfogásából fakad. A szólásszabadság liberális felfogása szerint a szabad véleménynyilvánítás egyrészt a kormányzat korlátozásának, másrészt a nyilvános vitákban, közbeszédben aktívan részt vevő állampolgárok ideájának alapja.

Hasonló vitáknak a kontinentális alapjogi gondolkodás nem ad táptalajt, az ezekhez a jogrendszerekhez tartozó országok a szólásszabadság jóval szélesebb körű korlátozására biztosítanak lehetőséget. Az Emberi Jogok Európai Egyezménye lehetővé teszi a pornográf közlések korlátozását arra hivatkozással, hogy azok sértik a közerkölcsöt,[485] ez azonban nem jelenti az ilyen típusú közlések teljes tilalmát. Mások jó hírnevének és jogainak védelme az EJEB szerint a véleménynyilvánítás korlátozásának

[483] Snyder v. Phelps, 131 S. Ct. 1207, 1214 (2011).

[484] Koppelman 2016: 661–693.

[485] EJEE 10. cikk 2. E kötelezettségekkel és felelősséggel együtt járó szabadságok gyakorlása a törvényben meghatározott, olyan alakszerűségeknek, feltételeknek, korlátozásoknak vagy szankcióknak vethető alá, amelyek szükséges intézkedéseknek minősülnek egy demokratikus társadalomban a nemzetbiztonság, a területi sértetlenség, a közbiztonság, a zavargás vagy bűnözés megelőzése, a közegészség vagy az erkölcsök védelme, mások jó hírneve vagy jogai védelme, a bizalmas értesülés közlésének megakadályozása vagy a bíróságok tekintélyének és pártatlanságának fenntartása céljából.

egy másik legitim célja lehet, amennyiben a szólásszabadság joga konfliktusba kerül a magánszféra tiszteletben tartásának az EJEE 8. cikke által biztosított jogával.

Állami szinten már vannak törekvések a hozzájárulás nélkül közzétett szexuális felvételek kriminalizálására, így az Egyesült Államok több tagállama is büntetni rendeli azt, ha valaki ily módon tesz hozzáférhetővé más személyről készült pornográf felvételeket. Az állami szinten bevezetett jogszabályokat több kritika is érte, köztük a New York állam által bevezetett törvényt,[486] amellyel kapcsolatban a legfőbb ellenérv az volt, hogy továbbra is a zaklatással kezeli analóg módon a hozzájárulás nélkül közzétett pornográf felvételeket, amelyek esetében így a tényállásszerű elkövetéshez szükséges a károkozási szándék. Nem csak New York államban létezik hasonló, összesen 24 állam fogalmaz meg vétkességi követelményt, amely azt jelenti, hogy az elkövető szándékának arra kell irányulnia, hogy ártson másnak. Danielle Citron és Mary Anne Franks arra is felhívják a figyelmet, hogy a zaklatás tényállásának eleme a rendszeresség, így aki csak egy videót tesz közzé, nem valósítja meg azt.[487] A szerzőpáros arra is rámutat, hogy a hozzájárulás nélkül közzétett felvételeket gyakran azonosítjuk azzal az esettel, amikor a sértett a felvétel készítésébe beleegyezik, vagy maga küld szexuális tartalmú felvételt partnerének, később pedig ezek a felvételek kerülnek nyilvánosságra, amelyhez a sértett nem adta hozzájárulását. A bosszúvágyból nyilvánosságra hozott szexuális tartalmú felvételek azonban jóval több és mélyebben gyökerező problémát érintenek néhány felelőtlenül elkészített felvételnél, a szerzők szerint bosszúpornóként kell kezelni a titokban, vagy a nyíltan, de a sértett beleegyezése nélkül elkészített felvételeket is, hiszen az ezek nyilvánosságra hozatalával történő zsarolás a párkapcsolati erőszak egyik formája lehet.[488]

A szexuális deepfake-ek szabályozása

A *deepfake* kifejezés két szó összevonásából keletkezett, a *deep* arra a mélytanulási technikára utal, amellyel a mesterséges intelligenciát használó algoritmusok az emberi agyhoz hasonlóan képesek elsajátítani új ismeretanyagokat, a *fake* pedig hamisat, megtévesztőt jelent. A *deepfake* pornográfia jelensége 2017-ben került be a köztudatba,

[486] Ellis 2019.
[487] Citron–Franks 2014: 345.
[488] Citron–Franks 2014: 346.

amikor híresség, többek között Gal Gadot[489] vagy Scarlett Johansson[490] arcait montírozták pornográf felvételekre. A technológia fejlődésének köszönhetően az ilyen felvételek elkészítéséhez nem kell hollywoodi stúdiókat megszégyenítő felszerelés, sem technikai tudás, egy egyszerű applikációval bárki készíthet hasonló videókat. Éppen ezért a jelenség már nem kizárólag a sztárokat érinti, hanem a hétköznapi embert is, haragosai bárkiről készíthetnek hasonló digitális kreálmányt.

A pornográf *deepfake*-ek szabályozásáról szóló diskurzusban markánsan különböző álláspontokat találunk. Vannak olyan szerzők, ilyen Tyrone Kirchengast, akik szerint a technológiát nem kell kriminalizálni, de még szabályozni sem feltétlen.[491] Mások ellenben a büntetőjogi eszközökkel való fellépést sürgetik.

A szexuális deepfake-ek szabályozása Magyarországon

A pornográf *deepfake*-ek esetében gondosan el kell választanunk egymástól a technológia szabályozását, illetve a technológia felhasználásával elkövetett magatartások szabályozását. A *deepfake* mint technológia teljesen legitim célokra is használható, sőt a szórakoztatóipar előszeretettel használja is: a 2020-as *Star Wars* filmben, a *Zsivány Egyes*ben ezzel a technológiával alkotta újra a Disney Leia hercegnőt az őt játszó Carrie Fisher régi jelenetei alapulvételével.[492] A technológiát azonban kártékony célokra is lehet használni, szabályozói szempontból ezek a magatartások igényelnek hangsúlyosabb figyelmet. A jogrendszerünk szerencsére technológiafüggetlenül szabályozza az üldözendő cselekményeket, tehát az egyes magatartások megítélése esetében nem azok a technikai eszközök bírnak jelentőséggel, amelyeket az elkövető felhasznált, hanem a cselekmény és annak eredménye. A magyar Btk. pedig szabályozza azt az esetet, amikor valaki hamis kép- vagy hangfelvétel készítésével vagy felhasználásával okoz sérelmet másnak. A *deepfake* felvételek esetében megoldást jelent a Btk. 226/B. szakasza, amely a becsület csorbítására alkalmas hamis kép- vagy hangfelvételek készítését és nyilvánosságra hozatalát is büntetni rendeli.

489 Turton–Justus 2018.
490 Hollister 2018.
491 Kirchengast 2020.
492 Chichizola 2020.

A hamisított szexuális felvételek az Egyesült Államokban

Hasonlóan a hozzájárulás nélkül hozzáférhetővé tett szexuális felvételek esetéhez az amerikai jog a pornográf *deepfake*-ekhez is a szólásszabadság oldaláról közelít.

Alkotmányjogi szempontból a *deepfake* pornográfia két témakört érinthet: a hamis beszédet és az obszcenitást. A hamis közlések alapjában véve nem minősülnek értékesnek, hiszen nem mozdítják előre a közügyekről folyó diskurzust. Az amerikai bíróságok többnyire azonban vonakodnak a közlések előzetes korlátozásától, a New York Times v. Sullivan ügyben pedig a Legfelsőbb Bíróság azt is kimondta, hogy csak akkor ítélhető meg kártérítés választott köztisztséget viselők becsületének megsértése esetén, ha a hamis tényközlést ártó szándékkal tették.[493] A Gertz v. Robert Welch ügyben[494] a bíróság azt is kimondta, hogy az egyes államok felállíthatják saját felelősségi rendszerüket a magánszemélynek sérelmet okozó rágalmazó hazugságokért.

Douglas Harris azt vizsgálta, hogy obszcenitásra hivatkozással korlátozhatók-e általánosságban a *deepfake* felvételek,[495] és arra jutott, hogy a *deepfake* pornográf felvételek általánosságban nem minősülnek a Miller-teszt szerint obszcénnek: az olyan hamis felvételek, amelyek nem erőszakosak, vagy művészi értéket képviselhetnek, nem korlátozhatók. Azt, hogy milyen tartalmak minősülnek obszcénnek, az úgynevezett Miller-teszt segítségével lehet eldönteni, amelyet a Miller v. California ügyben[496] dolgozott ki a Legfelsőbb Bíróság. Ez alapján az obszcenitás megítélésekor az alábbi faktorokat kell figyelembe venni:

a) hogy az átlagember, aki kortárs közösségi standardokat vesz figyelembe, úgy találja-e, hogy az alkotás mint egész kizárólag a szexuális vágy kielégítésére irányul *(appeals to the prurient interest);*
b) hogy az alkotás sértő módon ábrázol vagy ír-e le szexuális cselekvést;
c) hogy az alkotás mint egész nélkülözi-e a komoly irodalmi, művészi, politikai vagy tudományos értéket.

A pornográfia azonban általában nem minősíthető obszcénnek, csak azok a különösen extrém fajtái, mint a különös kegyetlenséget fetisizáló, állatokkal való fajtalankodást bemutató pornográfia, illetve a gyermekpornográfia. A szexuális tartalmakat tehát általánosságban megilleti az Első Alkotmánykiegészítés védelme, és csak különösen

493 New York Times Co. v. Sullivan, 376 U.S. 254 (1964).
494 Gertz v. Robert Welch Inc., 418 U.S. 323 (1974).
495 Harris 2019: 99–128.
496 Miller v. California, 413 U.S. 15, 23 (1973).

indokolt esetben korlátozhatók. Harris felveti a kérdést, hogy lehet-e összefüggés az obszcenitás megállapíthatósága és a felvételek valóságtartalma között. Az Ashcroft v. Free Speech Coalition ügyben[497] a Legfelsőbb Bíróság egy olyan szövetségi törvény alkotmányosságát vizsgálta, amely tiltotta a kiskorúakat, illetve kiskorúnak látszó személyeket szexuális tartalmú cselekmény közben ábrázoló kép- és filmfelvételek – ideértve a digitálisan, számítógéppel előállított felvételeket is – készítését. A bíróság ezt a jogszabályt alkotmánysértőnek ítélte amiatt, hogy túl tágan korlátozta a szólásszabadság jogát, és rámutatott arra, hogy nem minden szexuális tevékenység sérti a közízlést *(prurient interest),* amely tinédzsereket ábrázol. A Bíróság a szólásszabadság korlátozását itt a közlés által ténylegesen okozott kár esetében engedné meg, a digitálisan előállított, nem a valóságot ábrázoló felvételeket pedig általánosságban erre alkalmatlannak ítélte. Harris álláspontja szerint ez az érvelés a *deepfake* pornográf felvételek esetében nem állja meg a helyét, hiszen az igenis kárt okoz a benne szereplő jó hírében, biztonságérzetében.[498] Geoffrey Stone azonban rámutat,[499] hogy a jelenlegi bírósági gyakorlat szerint ezek a felvételek nem minősülnek egyébnek, mint „érzéki szórakoztatásnak" *(salacious entertainment),* amelyet, hasonlóan a vulgáris szatírához és paródiákhoz, megillet az Első Alkotmánykiegészítés által biztosított védelem.

Több jogszabály hivatkozik arra, hogy a sértettnek akkor van joga fellépni a róla közzétett szexuális felvételekkel szemben, ha észszerű elvárása lehetett volna a magánszféra védelme. Douglas Harris kiemeli,[500] hogy a *deepfake* pornográfia esetében ez nem feltétlenül jelent kapaszkodót, hiszen a bemutatott aktus meg sem történt, a felvételeken pedig egy másik ember intim testrészei látszanak.

Szövetségi szinten még nem született ezeket a jelenségeket kezelő norma, noha már voltak erre irányuló kezdeményezések. 2016-ban az intim magánszféra védelméről szóló törvényjavaslatot terjesztették a kongresszus elé (Ending Nonconsensual Online User Graphic Harassment Act – ENOUGH), 2018-ban pedig kifejezetten a *deepfake* pornográfia tilalmáról szóló törvényjavaslatot (The Malicious Deep Fake Prohibition Act – MDFPA), de végül egyikből sem lett elfogadott jogszabály.

2019-ben ismét nekifutott az amerikai törvényhozás a *deepfake*-ek szabályozásának, a DEEPFAKES Accountability Act[501] az ilyen technológiával készített felvételek

[497] Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).
[498] Harris 2019: 106.
[499] Stone 2017.
[500] Harris 2019: 106.
[501] Teljes nevén Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019.

könnyű azonosítása érdekében számos azonosítást megkönnyítő műszaki intézkedés megtételére kötelezte volna a tartalom-előállítókat. A *deepfake* felvételeket így el kellett volna látni vízjellel, valamint külön a felhasználók tájékoztatását szolgáló figyelmeztető jelzésekkel. A javaslat szerint, aki zaklatási célból vagy másik személy megalázása érdekében e műszaki kötelezettségeknek nem tesz eleget, büntetőjogi felelősségre is vonható, abban az esetben, ha a felvétel szexuális jellegű, alkalmas arra, hogy erőszakot vagy fizikai kárt okozzon, fegyveres vagy diplomáciai konfliktust idézzen elő, vagy beavatkozzon a demokratikus folyamatokba, különösen a választásokba. A törvényjavaslatot végül nem fogadták el abban a törvényalkotási ciklusban, amelyben azt benyújtották.

A platformok magánszabályozásának szerepe a hozzájárulás nélkül közzétett szexuális felvételek és a deepfake pornográfia eltávolításában

A nagyobb platformok felhasználási feltételeit (bizonyos platformok esetében közösségi iránymutatásait) olvasva felfedezhetünk közös elveket és irányokat, a szabályrendszer azonban korántsem mondható egységesnek, az egyes platformokat vizsgálva igen színes kép rajzolódik ki. Természetesen ez jelentheti azt, hogy az online platformok a saját tevékenységükhöz legjobban illeszkedő, a hatékony védelmet leginkább megteremtő módon szabják fazonra a tartalommal és a felhasználói magatartásokkal kapcsolatos előírásaikat. A pesszimista álláspont szerint viszont a platformok effajta magánszabályozása eredményezhet egy olyan mértékben töredezett szabályozási környezetet, amelyben a jogkövetésre törekvő felhasználónak kihívást jelent eligazodni. E fejezetben több kiemelt platform szabályrendszerét elemezve mutatjuk be a szexuális tartalmak szabályozásával kapcsolatos legfontosabb közös elemeket és különbségeket.

A tiltott tartalmak köre

A pornográf tartalmakra vonatkozó szabályok vizsgálatának alapkérdése, hogy az egyes szolgáltatók miként viszonyulnak azokhoz: tiltják vagy engedik azok feltöltését? Esetleg köztes megoldásként bizonyos korlátozásokkal engedik meg a szexuális tartalmak feltöltését? A legnagyobb platformok többsége elzárkózik a szexualitást és a meztelenséget ábrázoló tartalmaktól, a YouTube, a Facebook, a Tumblr, az Instagram és a Twitch mind tiltják az ilyen jellegű alkotásokat. A teljes tiltást, illetve a korlátozást alkalmazó

online platformok esetében indokolt körbejárni azt is, hogy a tartalmaknak pontosan mely körét érinti a tilalom. A pornográfia egzakt definíciójához Potter Stewart bíró 1964-es szállóigévé vált mondata óta („*I know it when I see it.*"[502]) sem kerültünk sokkal közelebb, globális vagy uniós szinten elfogadott jogszabályi definíciója e tartalmak körének továbbra sincs. A platformszolgáltatók többsége ezért részletesen leírja, milyen típusú tartalmakat tilt vagy korlátoz, e korlátozás pedig a legtöbb vizsgált platform esetében igencsak széles körű, ami komoly kérdéseket vet fel a szólásszabadság néhol indokolatlanul szigorúnak tűnő korlátozásával összefüggésben. A tiltást alkalmazó platformok ugyanis nem kizárólag a pornográfiát, hanem a szexualitást és a meztelenséget általában tiltják. A Tumblr felnőtt tartalomként *(adult content)* definiál és töröl minden olyan fényképet, videót és GIF-et, amely valós emberi nemi szervet, női mellbimbókat ábrázol, vagy szexuális aktust mutat be.[503] Hasonló szigorral állapította meg a tiltott tartalmak körét a Facebook, ahol tilos valódi meztelen felnőttet, szexuális tevékenységet, illetve az ahhoz kapcsolódó magatartásokat és eszközöket (például szexuális játékszereket) explicit módon bemutató képek közzététele. A felhasználási feltételeiben a Facebook arról ír,[504] hogy alapvetően mindenfajta szexuális tartalmat eltávolít, hogy megakadályozza a hozzájárulás nélkül közzétett tartalmak megosztását, illetve a kiskorúakat ábrázoló tartalmak terjedését. A tartalmak visszaállítását az azt feltöltő felhasználó kérheti. 2019 júliusa és szeptembere között 30,3 millió tartalmat távolított el platform a szexualitással kapcsolatos előírások megsértése miatt, panasszal azonban mindössze a feltöltők 10%-a élt. A panaszok alapján viszonylag kevés, 814 ezer bejegyzést állítottak vissza.

Valamivel engedékenyebb a YouTube, amely azokat a szexualitást és meztelenséget ábrázoló videókat moderálja, amelyek célja szexuális örömszerzés. A célzat meghatározása ez esetben okozhat jogalkalmazási nehézségeket. A nyilvánvalóan pornográf tartalmak esetében vitathatatlan az elkészített felvétel célja, az erotikus művészfilmekből kivágott jelenetek vagy a hétköznapi élethelyzeteket fetisizáló (a platform példája szerint ilyen lehet az orvosi injekció vagy az evés) videók esetében azonban már nehezebb következtetéseket levonni mind a videót feltöltő felhasználó szándékát, mind a befogadó(k) percepcióját illetően. Azokat a videókat, amelyek esetében az örömszerzési célt nem tekinti megvalósultnak a szolgáltató, törlés helyett korhatárossá teszi. Korhatárossá tételt eredményezhet a szexuális tevékenységre ösztönző

[502] Jacobellis vs. Ohio, 378 U.S. 184, 197 (1964).
[503] Tumblr Help Center 2023.
[504] Meta Transparency Center 2023c.

provokatív tánc, a szexuálisan explicit trágár nyelvezet, de a szereplők miliőhöz nem illő, indokolatlanul lenge ruházata is.

Az erőszakos, kegyetlen, megalázó fétisek az összes platform szerint moderálandók, akkor is, ha meztelenséget egyáltalán nem is tartalmaznak. Hasonló a helyzet a vérfertőzést, kannibalizmust, nekrofíliát, állatpornográfiát támogató, népszerűsítő tartalmakkal. A meztelenséget, szexualitást ábrázoló tartalmakat akkor is törlik a platformok, ha azokat digitálisan állították elő (például animációk), és valós szereplőket egyáltalán nem tartalmaznak.

Nem ennyire elutasító a Snapchat és a Twitter, ahol korlátozásokkal ugyan, de megoszthatók szexualitást és meztelenséget bemutató tartalmak. A Snapchat például csak a kifejezetten pornográf tartalmak közzétételére és népszerűsítésére létrehozott felhasználói fiókokat tiltja, a szexualitás, a meztelenség előfordulását azonban nem zárja ki[505] a felhasználói interakciók közül.[506] A Twitter felhasználási feltételei kifejezetten szólnak arról, hogy a vállalat tisztában van azzal, hogy bizonyos tartalmak érzékeny témákat érintenek, így erőszakos vagy felnőtteknek szóló tartalmak lehetnek, de ezeket a véleménynyilvánítás szempontjából fontos tartalmaknak tekinti, így minimálisan korlátozza őket. Az ilyen tartalmakat nem szabad olyan helyen közzétenni, amely a platform szerkezetében kiemelt helyen jelenik meg (például élő közvetítésben), továbbá a felhasználó köteles megjelölni a fiókját mint érzékeny tartalmat közlő fiókot. Ez esetben a platform minden felhasználó számára figyelmeztetést helyez el a megtekintés előtt.[507] A tartalmak korhatárossá tétele is viszonylag széles körben elfogadott gyakorlat. A legtöbb szolgáltatásban van lehetőség arra, hogy a tartalom feltöltője megjelölje azokat a tartalmakat, amelyek nagykorúaknak szólnak. Ezek előtt a tartalmak előtt figyelmeztetés jelenik meg, és többnyire csak regisztrált felhasználók számára elérhetők.

A platformok harmadik csoportját azok a szolgáltatások képezik, amelyek kimondottan szexuális tartalmak megosztására jöttek létre, esetükben nyilvánvalóan értelmetlen volna tiltásról beszélni. Azonban még az ilyen platformok rendeltetéséből sem következik az, hogy az összes tartalmi előírás és szabály felett állnak, sőt egyes szabályok érvényesülésére fokozottabb figyelmet kell(ene) fordítaniuk, a felülvizsgált AVMS irányelv rendszerében éppen ezek azok a szolgáltatók, amelyeknek a tartalom ártalmasságával arányban a legszigorúbb intézkedéseket kell alkalmazniuk. Ezeknél a platformoknál is alapvető követelmény, hogy biztosítsák, kiskorúak ne férhessenek

505 Természetesen ez alól a gyermekekről készített felvételek kivételt képeznek.
506 Snapchat Privacy and Safety Hub 2023.
507 X Help Center 2023c.

hozzá a szolgáltatáshoz. Európában igen nagy számban fordulnak elő ilyen weboldalak. A Similarweb globális népszerűségi listáján megvizsgált első ötven pornográf jellegű weboldal[508] negyede európai (főként cseh és ciprusi) joghatóság alatt áll. Az AVMS irányelv átültetésének tapasztalatai jelenleg azt mutatják, hogy a tagállamok nem foglalkoznak érdemben a felnőtt platformok szigorúbb szabályozásával,[509] inkább intézményesített prüdériával ezekről a szolgáltatásokról tudomást sem véve próbálják megvalósítani az irányelv kiskorúak védelmére vonatkozó törekvéseit. Általános tartalmi szabályok természetesen ezekre a platformokra is irányadók, tehát a szolgáltatásukban nem szerepelhetnek olyan felvételek, amelyeknek a közzététele önmagában is bűncselekményt valósít meg (például gyermekpornográfia), álláspontom szerint azonban a kimondottan szexuális tartalmak felhasználók általi megosztására szakosodott platformokat indokolt lenne többletkötelezettségekkel sújtani.

A hozzájárulás nélkül közzétett szexuális felvételek és a deepfake

Az összes vizsgált platform zéró toleranciát hirdetett a hozzájárulás nélkül közzétett felvételekkel kapcsolatban, felismerve, hogy ez mások magánéletének súlyos megsértését jelenti. A „bosszúpornót" a platformok viszonylag egységesen definiálják: többnyire azokat a hozzájárulás nélkül közzétett képfelvételeket tekintik idetartozónak, amelyek nem kereskedelmi céllal, privát helyzetben készültek, és amelyek szereplője (közel) meztelen, szexuális tevékenységet folytat, vagy szexuális pózban látható.[510] A hozzájárulás hiányának elsődleges indikátora a kontextus: a címek, képaláírások és hozzászólások tartalmából többnyire megítélhető, hogy ilyen jellegű felvételről van-e szó, de szintén valószínűsíti, hogy a felvételt hozzájárulás nélkül tették közzé, ha azt bejelentették a rendőrségen, panaszt tettek a platformnál, vagy a bulvármédiában megjelent a felvételek kiszivárgásának ténye. Ezek az indikátorok azonban már csak az utólagos moderálást segítik, ekkor azonban a károkozó magatartás már megvalósult, így a prevenciót nem szolgálják. A szolgáltatók a hozzájárulás nélkül közzétett tartalmak közé sorolják a titokban készített felvételeket is, továbbá a kukkolást, valamint az *upskirting*et,[511] ahol a tartalom készítésének a módszere eleve kizárja a beleegyezést. A Facebook az áldozatsegítés érdekében egy új

[508] Similarweb 2023.
[509] ERGA 2022.
[510] Meta Transparency Center 2023a.
[511] Az *upskirting* jelentése a szoknya alá befényképezéssel elkövetett kukkolás.

tartalomszűrő technológiát is bevezetett, amelynek lényege, hogy az áldozatok – vagy potenciális áldozatok – feltölthetik azokat a képeiket egy szerverre, amelyeket nem kívánnak nyilvánosságra hozni. Ha a platformra valaki olyan képet próbál feltölteni, amely egyezik az adatbázisban szereplő felvétellel, azt a szolgáltató automatikusan blokkolja.[512] Noha a megelőzés és az áldozatsegítés méltányolható és támogatható elképzelés, a gyakorlat adatvédelmi szempontból erősen kifogásolható, ezzel ugyanis a Facebook a világ legnagyobb érzékeny adatokból álló adatbázisának birtokosa lesz. A rendszer biztonsági hibái és az egyes felvételek kiszivárgása beláthatatlan károkat okozhat. A hozzájárulás nélkül közzétett felvételeket még a kimondottan pornográf felvételek megosztására létrehozott platformok is tiltják. A Twitter ugyan elfogadó a szexuális tartalmakkal kapcsolatban, a hozzájárulás nélkül közzétett tartalmakat azonban ez a platform is tiltja. A Twitter a bejelentés szempontjából két kategóriára bontja a tartalmakat: azokra, amelyeket bárki bejelenthet, és azokra, amelyeket csak az érintett bejelentésére távolítanak el. Mivel a platformszolgáltató alapvetően engedékeny, csak akkor távolítanak el tartalmat az olyan személyek kérésére, akik nem szereplői a felvételeknek, ha az fenyegetést tartalmaz, vagy nyilvánosságra hozza a szereplő kapcsolattartási adatait.

A kimondottan pornográf tartalmakat kínáló platformoknál a felhasználási feltételek részeként szerepel az a kitétel, hogy a videó feltöltőjének, készítőjének írásos beleegyezést/hozzájárulást kell kérnie az összes szereplőtől a tartalom megosztása előtt. Az amerikai jog a tartalom közzétevőinek kifejezett kötelezettségévé teszi, hogy olyan nyilvántartást vezessenek, amelyen feltüntetik a szereplők életkorát (U.S. Code § 2257). E rendelkezés irányadó azokra a felvételekre, amelyek szexuálisan explicit tevékenységet ábrázolnak, akkor is, ha azokat digitálisan manipulálták. Arról azonban már nincs adat, hogy az ilyen platformok ellenőrzik-e ezeknek az írásos hozzájárulásoknak a meglétét, ahogyan arról sem, hogy hány esetben távolítanak el bejelentés alapján hozzájárulás nélkül közzétett tartalmakat. A jogszabályi rendelkezések érvényesüléséről ugyan nincs kézzelfogható adat, a sajtóban azonban markáns vélemények jelennek meg egyes pornográf tartalmakat kínáló platformokkal kapcsolatban. Így például a *Guardian* provokatív véleménycikke arról szól, hogy a Pornhub, ahelyett, hogy azzal foglalkozna, hogy a koronavírus-járvány idején ingyenes prémiumtagságot biztosít Olaszországban, foglalkozhatna a saját pandémiájával, a bosszúpornóval.[513] A hozzájárulás nélkül közzétett felvételeket azonosítás után ugyanis nehézkesen

[512] Davis 2019.
[513] Mahdawi 2020.

távolítja el a platform, és az algoritmusuk, amely azt hivatott biztosítani, hogy ezek a tartalmak ne jelenhessenek meg újra az oldalon, könnyen kijátszható. Egy másik cikk arra hívja fel a figyelmet, hogy a portál kegyetlenséget, bántalmazást és szexuális erőszakot tartalmazó felvételek közzétételét is megengedi, amelyek eltávolíttatása a rendelkezésre álló mechanizmusok ellenére is nehézkes.[514]

Jogszabályi rendelkezések hiányában a platformok a *deepfake* felvételeket is törekednek magánszabályozás révén kezelni. Több platformszolgáltató fellépett a hamisított felvételekkel szemben, így a *deepfake* pornográfiát betiltotta a Reddit, a Pornhub és a Twitter is.

A cyberbullying ezer arca

Megan Meier, Amanda Todd és Tyler Clementi mindannyian tinédzserek, akik internetes megfélemlítés, azaz *cyberbullying* miatt követtek el öngyilkosságot. Tetteik nemcsak médiafigyelmet irányítottak az online tér egyik új jelenségére, hanem több esetben jogalkotást is indukáltak.

Megan Meier 13 évesen akasztotta fel magát, mert egyik barátnőjének édesanyja, Lori Drew a Myspace nevű platformon álnév alatt virtuálisan megalázta és bántalmazta.[515] Drew-t információs rendszerhez való jogosulatlan hozzáféréssel vádolták meg, mert hamis felhasználói fiókot hozott létre a Myspace-en. A másodfokon eljáró bíróság ebben az ügyben felmentő ítéletet hozott, ugyanis nem tekintette információs rendszer megsértésének azt, ha valaki egy platform felhasználási feltételeit megsértve álnéven regisztrál.[516] Az esetet követően az amerikai Kongresszus vizsgálta a szövetségi szintű *bullying*ellenes törvény megalkotásának lehetőségét, végül alkotmányossági aggályok miatt elvetette azt.[517]

Amanda Todd, kanadai tinédzser 19 évesen vetett véget életének, miután egy holland férfi rávette, hogy küldjön ruhátlan felvételeket magáról, majd ezekkel zsarolta. Az elkövető kilétére a Facebook segítségével derült fény. A Facebook akkori biztonsági főnöke, Joe Sullivan egy interjúban azt nyilatkozta,[518] hogy a Facebook szűri a hamis profilokat, az algoritmus pedig megjelöli azokat a felhasználói fiókokat,

514 Grant 2020.
515 Pilkington 2008.
516 United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
517 Lipton 2012: 104.
518 White 2014.

amelyek 80%-ban nőket jelölnek ismerősnek, illetve, amelyeken a születési dátum folyamatosan változik. A holland elkövetőt elítélték, a bíróság pedig döntött a kiadatásáról Kanadának,[519] ahol időközben elfogadtak egy törvényt, amely bünteti a *cyberbullying*ot.[520]

Tyler Clementi 18 évesen ugrott le a New Jersey-i George Washington hídról, miután az egyetemi csoporttársa a Twitteren közzétett róla egy felvételt, amelyen homoszexuális viszonyt folytat.[521] A videót közzétevő csoporttárs végül vádalkut kötött, és magánélet megsértése *(attempted invasion of privacy)* miatt ítélték el.[522]

A bemutatott eseteket kivétel nélkül az online megfélemlítéssel *(cyberbullying)* hozták összefüggésbe, ellenben egyik elkövetőt sem emiatt szankcionálták – részben a megfelelő büntetőjogi tényállások híján. A *cyberbullying,* az infokommuniációs eszközök alkalmazásával elkövetett bántalmazás egyre több gyermeket, serdülőt érint,[523] az online megjegyzések, kommentek gyakran lesújtóan bántóak.[524] Maguk a bántalmazók az online tér személytelensége miatt nem látják azonnal, hogy milyen az áldozataik fizikai reakciója, ezért nem tudják felmérni, hogy online tevékenységük mekkora kárt okoz.[525] A jelenségre adott állami reakciók több nehezen megválaszolható kérdést is felvetnek, nemcsak Magyarországon, hanem az Egyesült Államokban is,[526] ahol először kapott nagyobb médiafigyelmet. Jelen fejezet arra koncentrál, hogy indokolt-e a *cyberbullying* önálló tényállásként való beemelése a büntető törvénykönyvbe. Ennek érdekében a *cyberbullying* fogalom jelentését vizsgálom, majd azt igyekszem feltárni, hogy a jelenlegi anyagi büntetőjogban találhatóak-e olyan tényállások, amelyek lefedik ezt a jelenséget, illetve azt, hogy egy újabb *bullying*specifikus tényállás megalkotása nem jár-e túlzott alapjog-korlátozással. Mivel a *cyberbullying* az online térben gyakran iskolákban és közösségimédia-platformokon vagy videómegosztó platformokon valósul meg, a fejezet azt is vizsgálja, hogy a büntetőjogi szabályozáson túl milyen egyéb lehetőségek állnak rendelkezésre a *cyberbullying* visszaszorítása érdekében.

519 AFP in the Hague 2016.
520 Government of Canada 2023.
521 Parker 2012.
522 Schweber–Foderaro 2016.
523 David-Ferdon–Hertz 2007: 1.
524 Calvert 2010: 20.
525 Calvert 2010: 20.
526 Lipton 2012: 101.

A cyberbullying fogalma

A *cyberbullying* szabályozásával kapcsolatos problémák azzal kezdődnek, hogy a jelenségnek még pontos magyar elnevezése sincsen, de tartalmáról az angolszász jogirodalomban is vita folyik. Ami az összes meghatározásnak közös eleme, az az, hogy a magatartás tanúsítása online infokommunikációs eszköz segítségével történik. Darcy K. Lane is megjegyzi, hogy az online és a fizikai térben történő bántalmazás között számos különbség van, az online környezetben megvalósuló bántalmazó magatartások sokszor nem is igényelnek közvetlen kontaktust a sértettel, ennek megfelelően speciálisan kell őket kezelni.[527] A *cyberbullying* kifejezés a magyar szakirodalomban is többféle fordításban jelenik meg. Monori Zsuzsanna online- vagy cyber-megfélemlítésként használja,[528] de Kiss Tibor, Parti Katalin és Prazsák Gergő is ezt a megoldást követik.[529] Az NMHH által működtetett online szótár, a *gyerekaneten.hu* ellenben zaklatásként aposztrofálja a *cyberbullying*ot,[530] ahogyan Péli-Tooth Viktóriánál is ekként jelenik meg.[531]

Tartalmát tekintve a *cyberbullying* sok összetevőből áll. A *gyerekaneten.hu* a bántó, megalázó üzenetek, hozzászólások interneten keresztül történő küldésével azonosítja a *cyberbullying*ot, de idesorolja a kínos képek engedély nélküli közzétételét, és a kiskorú felhasználóknak címzett szexuális tartalmú üzeneteket is. Kiss Tibor szerint a „cybermegfélemlítés szándékos tartalomküldés, tartalommegjelenítés vagy kommunikáció útján valamely szükségletkielégítés, feszültséglevezetés céljából alkalmazott fenyegető, megfélemlítő, pszichés erőszak előidézésére alkalmas magatartások összessége".[532] A *cyberbullying* valójában egy ernyőfogalom, amely számos, egymástól gyakran markánsan különböző magatartásformát takar, amelyek közös elemei, hogy az elkövetés helyszíne a virtuális tér, jellegét tekintve pedig erőszakos, bántó közlések útján valósul meg. Domonkos Katalin a *cyberbullying* alábbi fajtáit azonosítja:[533]

- *flaming*, azaz oltogatás (egyes fordítások szerint lángháború): online veszekedés dühös és trágár nyelvezet használatával, illetve támadó jellegű hozzászólások küldése valakiről nyilvános fórumra;

527 Lane 2011: 1791–1793.
528 Monori 2016b: 78.
529 Kiss–Parti–Prazsák 2019: 78.
530 *Cyberbullying* 2023.
531 Péli-Tooth 2015: 39.
532 Kiss–Parti–Prazsák 2019: 78.
533 Domonkos 2014: 60.

- *harassment* vagy *stalking* (zaklatás);
- *denigration* (befeketítés), azaz valótlan tartalmú közlések révén a másik lejáratása;
- *exclusion* (kiközösítés);
- *impersonation,* azaz személyiséglopás, amelyet szokás *identity theft* kifejezéssel is említeni;
- *outing* (kibeszélés);
- *trickery* („trükközés", becsapás);
- *sexting:* szexuális tartalmú fényképeket, videókat tartalmazó üzenetek küldése.

Más szerzőknél egyéb magatartások is ebbe a körbe tartoznak, ilyen például a *doxing,* azaz mások interneten található adatainak szisztematikus megkeresése és közzététele,[534] valamint a *puppeting,*[535] amely a személyiséglopás egy olyan rosszindulatú formája, ahol az elkövető a sértett személyazonosságát felvéve járatja le őt. A *cyberbullying* körébe szokás sorolni az internetes trollkodást, ami mások szándékos provokálását jelenti, sértő, bántó üzenetekkel.[536] Parti Katalin az online megfélemlítés körébe sorolja a hozzájárulás nélkül készített szexuális felvételek közzétételével való fenyegetést, a „ringyógyalázást" *(slut shaming),* illetve a bosszúpornót *(revenge porn)* is.[537]

Noha az online megfélemlítés többnyire olyan jelenség, amelyet gyermekekkel, tinédzserekkel hoznak összefüggésbe, a probléma nem csak a fiatalabb generációkat érintheti. A munkahelyi zaklatás is megvalósulhat online formában, egy Európai Parlament számára készített tanulmány pedig ennek is több formáját ismeri, így megkülönbözteti a munkavégzéssel kapcsolatos zaklatást (más munkájának folyamatos becsmérlése, teljesíthetetlen feladatok, betarthatatlan határidők kiszabása), a munkahelyi személyes zaklatást (munkavégzéssel kapcsolatos folyamatos élcelődés, pletykák terjesztése) és a munkahelyi kiközösítést. [538]

A cyberbullying szabályozása Magyarországon

Egy ennyire összetett cselekményt nagyon nehéz szabályozói oldalról megragadni úgy, hogy egy esetleges normaszöveg ne legyen se túl-, se pedig alulszabályozó. Egyetértek

534 Newman 2017.
535 Monori 2016b: 78.
536 Diaz 2016: 137.
537 Parti 2016: 125.
538 Hoel–Vartia 2018: 12.

Miskolczi Barna álláspontjával, a *cyberbullying* jelenség elleni fellépés érdekében egy önálló büntetőjogi tényállás megalkotása plakatív jogalkotás lenne.[539] Az előző pontban felsorolt magatartások között előfordul számos olyan, amelyet a magyar jogrendszer már most is kriminalizál. Ennek ellenére hazánkban is felmerült már a Btk. kibővítése az internetes zaklatás tényállásával,[540] mivel egyes álláspontok szerint[541] a jelenség hazánkban is jelen van, és nem csak az angolszász országok sajátja.

A *cyberbullying* kezelésére – noha valóban nincsen önálló büntető törvénykönyvi tényállás – jelenleg is több lehetőség van, a következőkben ezeket tekintem át.

A cyberbullying mint zaklatás

A *cyberbullying*ot leggyakrabban a zaklatás törvényi tényállásával szokták azonosítani. Noha a *cyberbullying* körébe tartozó magatartások egy része valóban megfeleltethető a hagyományos zaklatásnak, ez nem szükségszerűen van így. Álláspontom szerint a *cyberbullying*ra az esetek többségében éppen a zaklatás tényállása nem alkalmazható. Monori Zsuzsanna négy feltételt fogalmaz meg,[542] amelyek együttes fennállása esetén a *cyberbullying* zaklatásnak minősíthető:

1. tényállásszerűség,
2. büntethetőség,
3. magánindítvány előterjesztése,
4. bizonyíthatóság.

A *cyberbullying* akkor lehet tényállásszerű, ha a Btk.-ban foglalt rendszeres vagy tartós háborgatás megvalósul, az elkövető pedig azt azzal a kifejezett céllal műveli, hogy áldozatát megfélemlítse, vagy magánéletébe, mindennapi életvitelébe önkényesen beavatkozzon. Zaklatás lehet a veszélyes fenyegetés is, amennyiben az elkövető személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével fenyeget, vagy azt a látszatot kelti, hogy más életét, testi épségét vagy egészségét sértő vagy közvetlenül veszélyeztető esemény következik be.

Nem minősíthető zaklatásnak az a fenyegetés szintjét el nem érő, online bántalmazó magatartás, amely egyszeri (például egy támadó, lejárató bejegyzés valakinek

539 Miskolczi 2018: 166.
540 Nem csak a dohányzást, az internetes zaklatást is vasszigorral büntetné Lázár János 2018.
541 Pongó 2015.
542 Monori 2016b: 78.

az üzenőfalán), sem pedig az, amikor a bántó kommunikáció címzettje nem közvetlenül a sértett. A Btk. kommentárja rámutat arra, hogy a sértettnek és a passzív alanynak egybe kell esnie, ami a régi Btk. alapján még nem volt így: korábban a munkavállalót lejáratót, munkáltatónak küldött üzenetek is megalapozták a zaklatás megállapítását.[543] Ez többé nincs így, tehát a *cyberbullying* azon eseteire, ahol a tettes nem is kerül kapcsolatba a sértettel, mert a lejáratást az iskolai levelezőlistán, csak csevegőcsoportban vagy egyéb online közösségben valósítja meg, a zaklatás nem lesz megállapítható.

A büntethetőség alsó korhatára a *cyberbullying* esetén különösen releváns: a magyar Btk. a 14. életévnél húzza meg a büntethetőség határát, az online megfélemlítést azonban jellemzően fiatalok követik el fiatalok ellen. A zaklatás kizárólag magánindítványra üldözendő cselekmény, ami azt jelenti, hogy a sértett azon igénye nélkül, amely az elkövető felelősségre vonására irányul, nincs helye eljárásindításnak.

Az előbbiekben leírtak alapján viszonylag szűk körben van lehetőség fellépésre, az online *bullying*gal összefüggő esetek jelentős része nem tényállásszerű. Az online térben zajló megfélemlítés ennél jóval összetettebb, ráadásul a Btk.-ban megjelenő zaklatás csak kisegítő, alárendelt tényállás, ami azt jelenti, hogy csak akkor állapítható meg, ha más, súlyosabb bűncselekmény nem valósul meg. A *cyberbullying* egyes fajtáinak azonban többször van olyan mozzanata, amelyet más büntető törvénykönyvi rendelkezés büntetni rendel.

A cyberbullying és más bűncselekmények

A tartalomközléssel megvalósuló deliktumok közül szóba jöhet a rágalmazás és a becsületsértés, amennyiben az elkövető a becsület csorbítására alkalmas tényt állít vagy híresztel, ezekre közvetlenül utaló kifejezést használ, vagy becsület csorbítására alkalmas kifejezést használ (például közösségi oldalon, fórumon vagy chatszobában). A *cyberbullying* gyakran együtt jár azzal, hogy az áldozatot bizonyos információk közzétételével fenyegetik, ha nem tesz meg valamit, vagy nem fizet a bántalmazójának. Amennyiben az elkövető magatartása haszonszerzési célú, a zsarolás bűntette állapítható meg. Amennyiben az elkövető azért bántalmaz vagy kényszerít mást arra, hogy valamit tegyen, ne tegyen vagy eltűrjön, mert az bizonyos társadalmi csoporthoz tartozik (például homoszexuális), akkor a közösség tagja elleni erőszak tényállásának alkalmazása vizsgálandó. Az online megfélemlítés nagyon gyakran hozható összefüggésbe szexuális

[543] Szomora 2019b.

felvételekkel, ahol az elkövető azzal fenyegeti a sértettet, hogy nyilvánosságra hozza a szexuális együttléteikről készült felvételeket, vagy azokat a képeket, ahol a sértett ruhátlanul szerepel. Minden esetben vizsgálni kell a sértett életkorát is. Aki 18 éven aluli személyről szexuális felvételeket tart, az már a gyermekpornográfia tényállását valósítja meg.

Amennyiben az elkövető kommunikációjával azt kívánja elérni, hogy a sértett önkezével vessen véget életének (például azt üzeni a sértettnek, hogy a világ jobb hely lenne nélküle, nem is kellene léteznie), azt kell vizsgálni, hogy az öngyilkosságban közreműködés tényállása megvalósul-e. E tényállás kapcsán fel kell hívni a figyelmet arra is, hogy az elkövető nemcsak akkor büntethető, ha a sértett öngyilkossága sikeres volt, hanem akkor is, ha azt csupán megkísérli. Az öngyilkosságban közreműködés minősített esete, ha a nagykorú elkövető kiskorút bír rá az öngyilkosságra, mivel a kiskorúak személyisége még kiforratlan, ezáltal különös védelemben indokolt őket részesíteni. *Bullying*ként szokás azonosítani az olyan internetes kihívásokat is, amelyek veszélyes feladatok elvégzésére buzdítanak, s elvégzésükkel a sértett magának okozhat kárt. 2017-ben ilyen volt a kék bálna kihívás *(Blue Whale Challenge),* amelyet az írt be a köztudatba, hogy több tinédzser is öngyilkos lett a feladatok teljesítése során.[544] Ezekben az esetekben azonban nem feltétlenül történik büntetőjogi tényállást kimerítő cselekmény.

A Btk. az ember cselekvési szabadságát egyéb módon korlátozó magatartásokat a kényszerítés cím alatt rendeli büntetni. A büntető törvénykönyvi tényállás szerint a kényszerítést az követi el, aki mást erőszakkal vagy fenyegetéssel arra kényszerít, hogy valamit tegyen, ne tegyen vagy eltűrjön, és ezzel jelentős érdeksérelmet okoz.[545] A már említett internetes kihívások többnyire ártalmatlan feladatokkal kezdődnek, majd folyamatosan terelik a résztvevőt az egyre deviánsabb, veszélyesebb cselekvések felé. 2019-ben terjedt a WhatsApp nevű üzenetküldő szolgáltatásban a Momo kihívás,[546] amelyben egy torz lény küldött különböző feladatokat a résztvevőknek, azzal fenyegetve őket, hogy ha nem teljesítik azokat, családjukat, barátaikat bántódás éri, vagy közzétesznek róluk olyan információkat a közösségi médiában, amelyek nyilvánosságra hozatala a sértettek számára megalázó lenne. A kihívások eleinte viszonylag szelídek voltak, a résztvevőnek hajnalig fent kellett maradnia, vagy horrorfilmet kellett néznie, később viszont már felkerült a palettára a bolti lopás, a garázdaság, végül az öngyilkosság.

544 Hempel 2017.
545 Btk. 195. §.
546 Dickson 2019.

A *cyberbullying* jelenséggel összefüggő magatartások nagy részét tehát valamilyen formában már most is büntetni rendeli a Btk., ezért nehezen lehetne olyan tényállást alkotni, amely nincsen túlzott átfedésben a már létezőkkel. Parti Katalin szerint, ha a napjainkra jellemző kriminalizálási tendenciát követjük, akkor olyan absztrakt tényállásokat kell megállapítani, amelyek minden utólag megjelenő magatartás szabályozására alkalmasak.[547] Ily mértékben absztrakt tényállásokat megalkotni a már meglévő tényállásokkal való párhuzamosságok kiküszöbölésével egyidejűleg legfeljebb úgy lehetne, ha a *cyberbullying* címszó alatt a jogalkotó kizárólag azokat a megnyilvánulásokat rendelné bünteti, amelyek jelenleg – noha bántó természetűek – még nem jogellenesek. Ez azonban az online közlések oly mértékű korlátozását jelentené, amely véleményem szerint a szólásszabadsággal összeegyeztethetetlen volna, hiszen olyan magatartásokra szorítkozna, amelyek a sértett objektív megítélése szerint bántók, ám nem mutatnak túl a társadalomban jelenleg elfogadott objektív mércén. A következő részben a *cyberbullying* és a szólásszabadság kapcsolatát tekintem át, bevonva a vizsgálódásba az amerikai szólásszabadság doktrínájával összefüggő elemzéseket is.

A cyberbullying és a szólásszabadság

Az alapjogok korlátozásával kapcsolatban az Alkotmánybíróság kimondta, hogy azok csak akkor korlátozhatók, „ha másik alapvető jog és szabadság védelme vagy érvényesülése, illetve egyéb alkotmányos érték védelme más módon nem érhető el".[548] Az Alkotmánybíróság álláspontja ebben a kérdésben tehát összhangban van az Alaptörvény I. cikk (3) bekezdésével, amely kimondja, hogy „alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható". A korlátozásnak ebben az esetben is meg kell felelnie az arányosság követelményének, vagyis az alapjogsérelemnek arányban kell állnia a cél fontosságával. A *cyberbullying*ot megvalósító magatartások sérthetik az egyén magánélethez való jogát, illetve méltóságát, amennyiben azok a sértett társadalmi megbecsülését, illetve egyéni önbecsülését csorbítják. A büntető törvénykönyvben megtalálható olyan magatartások, amelyek az online térben *bullying*nak minősülhetnek, már kiállták az alkotmányosság próbáját, ezért ebben a részben

[547] Parti 2016: 145.
[548] 30/1992. (V. 26.) AB határozat III. rész 2.2. pont 2. bekezdés.

a zaklatás, a rágalmazás, a becsületsértés, a verbálisan megvalósuló kényszerítés alapjogi vonatkozásait nem tárgyaljuk. Garzuly Éva kiemeli, hogy a szólásszabadság „a közügyek vitatásának körén kívül eső, öncélú, megalázó, bántó vagy sértő és csak a magán- vagy családi élettel kapcsolatos kifejezéseket értelemszerűen nem védi,"[549] azonban a *cyberbullying* körébe eső, még nem kriminalizált magatartások büntetőjogi szankcióval való fenyegetése nem feltétlenül szükséges, és nem biztos, hogy arányos. Az ilyen közlések kriminalizálása tekintetében figyelemmel kell lennünk arra, hogy az Alkotmánybíróság a büntetőjogra *ultima ratio* megoldásként tekint, amely a jogrendszer egészének a szankciós záróköve, vagyis csak akkor alkalmazható, ha más jogágak szankciói nem segítenek.[550] A 13/2014. (IV. 18.) AB határozatban az emberi méltóságot sértő közlések tekintetében azt állapította meg a testület, hogy a büntetőjog csak „a legsúlyosabb esetekkel szemben nyújthat oltalmat, amikor a közölt vélemény alkotmányos jogot sért vagy a jogsérelem veszélye közvetlenül jelen van".

A *cyberbullying* és a szólásszabadság összefüggéseinek vizsgálatakor azért tartom különösen fontosnak az amerikai jogirodalmi álláspontok ismertetését, mert az Egyesült Államok a szólásszabadságnak a kontinentális jogrendszerek által biztosított védelemnél erősebb védelmet biztosít, ugyanakkor ez az ország az elsők között volt, amelyik a jelenség szabályozására törekedett. A szólásszabadság határainak kijelölésében így hasznos lehet az amerikai szólásszabadsággal kapcsolatos jogi gondolkodás és jogalkalmazási gyakorlat ismerete. Török Bernát azt írja, hogy szavaink hatását sokszor nehéz megbecsülni, és nagyon könnyű túlbecsülni.[551] Ez az állítás különösen igaz az online térben, ahol a beszélő általában nem látja, hogy milyen reakciót vált ki a tényleges címzettből, így csak egy ideából tud kiindulni, a hatásból, amelyet szerinte a közlésének ki kellene váltania. Parti Katalin hívja fel a figyelmet arra, hogy a *cyberbullying* esetében az elkövetők gyakran védekeznek azzal, hogy nem állt szándékukban sérelmet okozni, kijelentéseiket viccnek vagy ugratásnak szánták.[552] Edwin Baker álláspontja szerint a véleménynyilvánítás esetében a sérelmet valójában nem feltétlenül a közlés tartalma okozza, hanem az, ahogyan a sértett ahhoz mentálisan viszonyul.[553] Van, akit nem zavar egy élesebb kritika, vagy nem bánt a külsejét illető sértő megnyilvánulás, az identitáskereső fiatalok, akik sokszor nem rendelkeznek kiforrott személyiséggel, viszont gyakran vágynak megerősítésre társaik

[549] Garzuly 2015: 46.
[550] 30/1992. (V. 26.) AB határozat IV. rész 4. pont 1–2. bekezdések.
[551] Török 2019: 254.
[552] Parti 2016 144.
[553] Baker 1996–1997: 987–988.

részéről, a csoporton belüli megbecsülés kivívásának igénye pedig fogékonyabbá teszi őket a befolyásolásra és érzékenyebbé a kritikával szemben. Baker ugyanakkor azzal érvel, hogy az effajta relatív ártalomokozásért nem lehet a közlőt felelősségre vonni, ami azonban vitatható álláspont. Török Bernát például Baker álláspontjának kritikájaként azt fogalmazza meg, hogy ha elfogadjuk Baker következtetését, akkor a kommunikációt „helyes lenne laboratóriumi körülményekhez szabni, ahol a beszélő minden esetben jogosan tekinthetné a hallgatóságát sztoikus bölcsek gyülekezetének, nem számolva a közösségi élet ennél lényegesen színesebb valóságával".[554]

Az Egyesült Államokban már 44 tagállam bünteti valamilyen formában a *cyberbullying*ot,[555] noha ezek többsége a *cyberbullying*ot nem önálló cselekményként rendeli büntetni, inkább több olyan magatartást büntet, amely *cyberbullying*ként klasszifikálható. Ilyen az online zaklatás *(cyberharassment)* és az online üldözés *(cyberstalking)*.[556] Néhány esetben felmerült a *cyberbullying* önálló törvényi szabályozása, ezek a kezdeményezések azonban a legtöbb esetben nem jártak sikerrel. A *cyberbullying* önálló kriminalizálására törekvő People v. Marquan ügyben[557] a New York-i fellebbviteli bíróság azért nyilvánította érvénytelennek Albany megye *cyberbullying*ról szóló jogszabályát, mert az túlságosan tág teret engedett a közlések korlátozásának, és büntetni rendelte, ha a közlő szándéka más zaklatása, bosszantása, fenyegetése, bántalmazása, piszkálása, megfélemlítése, kínzása vagy megalázása. Ebből az következik, hogy az olyan magatartások, amelyek a sértettet „bosszantják" vagy „piszkálják", ha okoznak is mentális diszkomfortérzetet, még nem elégségesek a közlő szankcionálásához. Parti Katalin rámutat arra is, hogy „pszichológiai kutatások szerint vitatott, hogy a gyerekkori *bullying* természetes része-e a felnőtté válásnak, a közösségi státuszkeresésnek, a dominanciaharcnak, az önállósodásnak,"[558] ezért nincsen közmegegyezésre számot tartó álláspont arról sem, hogy mi minősül még megengedhetőnek. Az online térben tett megnyilvánulások lelki sebeket okozhatnak, és közvetetten fizikai sérelmeket is előidézhetnek, ezért bizonyos szélsőséges esetekben indokolt azok szabályozása. A *cyberbullying* további szabályozása esetében azonban tekintettel kell lenni arra, hogy a szélsőségesen bántó vagy durva közlések korlátozása már más büntetőjogi tényállásokon keresztül megvalósul, másrészt arra, hogy a sérelemérzet sokszor az életkori sajátosságból fakadó érzékenység eredménye. Dworkin – a pornográfiaszabályozással

554 Török 2019: 257.
555 Cyberbullying Research Center: Bullying Laws Across America.
556 Mosser 2016: 81.
557 People v. Marquan M., 2014 WL 2931482.
558 Parti 2016: 144.

összefüggésben – hívja fel a figyelmet arra, hogy nem tekinthetünk sérelemnek bármely másnak okozott lelki megrázkódtatást *(mental distress)*.[559]

Az egyik ok, amely miatt az USA-ban felmerülhetett a *cyberbullying* önálló törvényi szabályozása, az, hogy a rágalmazás és a becsületsértés az Egyesült Államokban nem számít bűncselekménynek, az ellen csak polgári eljárásban *(tort of defamation)* van lehetőség fellépni, így az Egyesült Államok jogrendszere nem nyújt büntetőjogi védelmet az olyan folyamatos, becsületet csorbító, illetve az emberi méltóságot sértő kifejezések ellen, mint például a magyar jog. A rendelkezésre álló, zaklatást büntetni rendelő tényállások sem minden esetben alkalmasak arra, hogy megfelelő védelmet nyújtsanak az ilyesfajta online támadások áldozatainak. Eugene Volokh felhívja a figyelmet arra, hogy az online zaklatás tényállásai klasszikusan a sértettnek szóló, sértettet célzó kommunikációt rendelték büntetni, ez azonban átalakulóban van. A zaklatással összefüggő szabályokat több esetben interpretálják úgy, hogy az akkor is megvalósul, ha a közlés nem a sértett*nek*, hanem a sértett*ről* szól, amely révén a szabályozás gyakorlatilag visszatér a rágalmazó közlések kriminalizálásához.[560] Volokh szerint az olyan zaklató jellegű megnyilvánulások kriminalizálása, amelyek nem közvetlenül a sértettnek szólnak *(one-to-one-speech),* hanem szélesebb körben osztanak meg a sértettről információt *(one-to-many-speech),* alkotmányellenesnek minősülnek, mivel az első alkotmánykiegészítés többnyire védi a nyilvánosság előtt elhangzott közléseket, akkor is, ha azt a közléssel érintett személy esetleg sértőnek találja.[561] Észak-Karolina legfelsőbb bírósága érvénytelenné nyilvánította az állam *cyberbullying*ról szóló jogszabályát a State v. Bishop ügyben,[562] jogszerűtlenné nyilvánította a kiskorúról szóló magánjellegű, személyes vagy szexuális információk internetes közzétételét, amennyiben azok célja félelemkeltés vagy gyötrelem okozása.[563] Az észak-karolinai legfelsőbb bíróság álláspontja szerint a jogszabály nem szabta feltételül, hogy a közlés nyomán sérelem keletkezzen, és a félelemkeltés, valamint a gyötrelem okozásának fogalmait is túl általánosan határozta meg, így azok akár az egyszerű bosszantást is jelenthetik.

Alison King találóan kifejti, hogy a *cyberbullying*ot megvalósító közlések korlátozását szolgáló jogszabályok alkotmányosságát nem azért kell vizsgálni, mert más online bántalmazása értékes beszédnek minősülne – sőt az ilyen típusú közlések igen

[559] Dworkin 1981: 177.
[560] Volokh 2013: 738.
[561] Volokh 2013: 743.
[562] State v. Bishop, 2016 WL 3221098.
[563] Balasubramani 2016.

csekély közösségi értéket hordoznak –, hanem azért, mert az ilyen szabályok magukban foglalják annak a veszélyét, hogy értékes közlések is korlátozás alá esnek.[564] Noha az első alkotmánykiegészítés széles körben védi a szólásszabadságot, vannak bizonyos közlésfajták, amelyekre a védelem hatóköre nem terjed ki. Ilyen az obszcenitás, a gyermekpornográfia, a valós fenyegetés, a támadó szavak, illetve a bűncselekmény elkövetésére való felbujtás. Az erőszakkal való fenyegetés tiltása a Virginia v. Black ügy szerint nem alkotmányellenes, ha tényleges fenyegetést fejez ki, vagy erőszakcselekmény nyilvánvaló és közvetlen veszélyét idézi elő.[565] Ebben az ügyben a bíróság úgy ítélte, hogy a kereszt mint szimbólum elégetése különösen veszélyes formája a fenyegetésnek. A támadó szavak tiltásának megengedhetőségével több esetben foglalkozott az Egyesült Államok Legfelsőbb Bírósága. A Chaplinsky v. New Hampshire ügyben a vizsgált magatartás jogellenességét mondta ki a bíróság, amikor a tettes egy Jehova tanúiról szóló könyvet osztogatott egy forgalmas utcán, miközben más vallások követőit gyalázta. A legártalmasabb közlések tehát az Egyesült Államokban sem élveznek feltétlen védelmet, hiszen azt a Chaplinsky-ügyben is elismerte a Legfelsőbb Bíróság, hogy a beszéd egyes szűkre szabott kategóriái korlátozhatók az első alkotmánykiegészítés sérelme nélkül.[566]

Az eddig leírtakon túl fel kell hívni a figyelmet az amerikai *cyberbullying*szabályozás egyik sajátosságára is. A *cyberbullying*nak minősülő közlések korlátozása ugyanis több esetben nem a büntetőjog rendszerén belül történik, hanem arra az iskolák, felsőoktatási intézmények kapnak lehetőséget, amely lépés a tanulók szólásszabadságát korlátozó eszköz, de szükséges az iskolai környezet biztonságának fenntartása érdekében. Az Egyesült Államokban több precedensértékű ítélet foglalkozik a véleménynyilvánítás szabadságának egyetemi campusokon, illetve iskolai épületekben való korlátozásával, a *cyberbullying* szabályozása pedig többnyire ezekre csatlakozik, és nem szabályozza az iskolai környezeten kívüli online kommunikációt. A Bethel School District v. Frazer ügyben a Legfelsőbb Bíróság az iskola házirendjét a szólásszabadság érvényesülése elé helyezte arra hivatkozással, hogy az iskola egy olyan speciális közeg, ahol a kiskorú tanulók befolyásolhatóak. Az olyan szórólapok közzététele, amelyek ugyan nem uszítanak követlenül gyűlöletre, azonban a homoszexuálisokra nézve degradálóak lehetnek, korlátozható az oktatási intézmény által, amely felelős a diákok szellemi és erkölcsi fejlődésének biztosításért.[567]

564 King 2010: 865–866.
565 Virginia v. Black, 538 U.S. 343 (2003).
566 Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).
567 Bethel School District v. Frazer, 478 US 675 (1986).

Az online platformok szerepe a cyberbullying elleni fellépésben

Az amerikai *cyberbullying*szabályozás egyik üzenete számunkra, hogy az Egyesült Államokban annyira fontosnak tekintik az iskolák szerepét, hogy jogszabályok külön felhatalmazást adnak nekik a hallgatói, tanulói szólásszabadság korlátozására. Az iskolák szerepe nemcsak a tanulók közléseinek korlátozásában jelentős, hanem a diákok és a szülők edukálásában is. Az iskolák és pedagógusok szerepének vizsgálatát, noha alapvető fontosságúnak tartjuk, meghagyjuk a pedagógiai jellegű tanulmányok számára.

Az iskolák szerepe mellett fontosnak tartjuk az online szolgáltatási tér szereplőinek a reakcióját is a vizsgált jelenségre. A *cyberbullying*ot szinte kizárólag valamilyen online szolgáltatás használatával követik el, legyen az egy álnéven regisztrált Facebook-profil, egy kisebb iskolai vagy munkahelyi WhatsApp-csoport vagy a YouTube, ahova az elkövető a sértett méltóságát súlyosan sértő videót posztol. A közösségimédia-szolgáltatók szerepe két fronton lehet jelentős. Az egyik a moderálás, a másik pedig a felhasználók oktatása, a tájékoztatás.

A platformok felhasználói feltételeikben gyakran a rájuk vonatkozó jogszabályoknál szigorúbb szabályokat szabnak a felhasználók által közzétehető megnyilvánulások esetében. Jelen fejezetben három szolgáltató, egy klasszikus közösségimédiaplatform-szolgáltató, a Facebook, egy videómegosztóplatform-szolgáltató, a YouTube, valamint a világ számos pontján népszerű mikroblog-szolgáltatás, a Twitter felhasználási feltételeit vizsgáljuk.

A Facebook szabályozásának jellegét illusztrálja, hogy a szabályzat nem jogi fogalmakkal dolgozik, az egyes kategóriák teljesen összemosódnak, így igen nehéz megállapítani, hogy mi az, amit a platform jogsértő jellege miatt, és mi az, amit üzleti vagy egyéb érdeke miatt tilt. A Facebook közösségi alapelvei a megfélemlítés és a zaklatás cím alatt rendelkeznek olyan magatartásokról, amelyek akár a *cyberbullying* jelenség körébe eső magatartásokat is megvalósíthatják. A platform bejelentés alapján eltávolítja az olyan tartalmakat, amelyek megalázóak, megszégyenítőek, illetve amelyek zaklató jellegűek. A platform felhívja a felhasználói figyelmét arra, hogy tilos más felhasználókat önbántalmazásra vagy öngyilkosságra felhívni, tilos mást kapcsolattartási adatainak kiadásával fenyegetni. Tilos olyan Facebook-csoportokat létrehozni, amelyek célja más megalázása vagy megszégyenítése.

Összemosódnak az egyes fogalmak a YouTube esetében is. A platform zaklatás és internetes zaklatás *(cyberbullying),*[568] valamint megfélemlítés címszavak alatt

[568] YouTube Súgó 2023f.

szabályozza a *bullying*gal is összefüggésbe hozható magatartásokat. Tiltja a huzamosabb ideig tartó gúnyolódást és rosszindulatú sértéseket, valamint a kiskorúak megszégyenítését, megsértését. A platform a zaklatás kategóriájába sorolja mások személyes adatainak közzétételét, illetve a káros magatartások tanúsítására való ösztönzést is. Érdekessége a YouTube szabályzatának, hogy azokat a tartalmakat is tiltja, amelyekben csak megjátsszák a mással szembeni súlyosabb erőszakot.

Az előző két platformnál valamivel részletesebbek a Twitter felhasználási feltételei. A Twitter tiltja az egyének vagy csoportok ellen irányuló erőszakos fenyegetéseket, valamint az erőszakot dicsőítő tartalmak megosztását.[569] A platform szerint idetartozik az emberöléssel, szexuális erőszakkal való fenyegetés, a komoly fizikai sérülés okozásával való fenyegetés. A Twitteren közzétett tartalmak nem lehetnek fenyegetőek,[570] így a felhasználók nem kívánhatják más halálát, sérülését vagy halálos betegségét, tilosak a támadó jellegű inzultusok, illetve a kéretlen szexuális közeledés (például kéretlen felnőtt tartalmak küldése más felhasználók számára, szexuális tartalmú üzenetek).[571] A felhasználói fiókokkal kapcsolatos szabály, hogy tilos olyan fiókot regisztrálni, amelynek a célja más fenyegetése.[572]

A platformok közül több részt vesz a felhasználói tudatosság fejlesztésében. A Facebook például létrehozott egy központi oldalt, amelynek a célja a gyermekek, a szülők és a pedagógusok informálása a *cyberbullying* jelenségről. A már említett kék bálna kihívásra reagálva több platform (a Tumblr, a Facebook és a YouTube) is frissítette a szolgáltatását, így ha valaki a kihívással kapcsolatos kifejezésekre keres, az oldal tetején megjelenik egy tájékoztató arról, hogy hol lehet mentálhigiénés tanácsadást igénybe venni, vagy milyen krízisvonalat lehet felkeresni.

A platformok közreműködhetnek az elkövetők kézre kerítésében is. Shira Auerbach a jogérvényesítés egyik korlátját abban látja, hogy az online környezetben nem tudják megállapítani az elkövető kilétét.[573] Jacqueline Lipton az online szolgáltatók szerepének nagy jelentőséget tulajdonít, mivel ők hozzáférnek a felhasználóik azonosításához szükséges adatokhoz; más kérdés, hogy sokszor üzleti érdekeik azt diktálják, hogy ezeket az adatokat ne adják ki.[574]

[569] X Help Center 2023d.
[570] X Help Center 2023d.
[571] X Help Center 2023a.
[572] X Help Center 2023b.
[573] Auerbach 2009: 1643–1644.
[574] Lipton 2012: iii.

A platformok szerepe tehát a *cyberbullying* visszaszorításában jól azonosítható, ám bizonyos területeken fejleszthető. A szabályzatokban tett általánosító kijelentések nem biztos, hogy megfelelően tájékoztatják a felhasználókat arról, hogy milyen tartalmak közzététele megengedett. A platformok arra sem hívják fel a felhasználók figyelmét, hogy melyek azok a tartalmak, amelyeket jogellenességük miatt tiltanak, és melyek azok, amelyek pusztán a platform magánérdekei, erkölcsi-etikai megfontolásai végett kerültek be a szabályzatba.

A valótlan közlés, a hamis hír (fake news) és a félretájékoztatás (disinformation) mint büntetőjogi probléma

Valótlanságot állítani morális értelemben lehet bűn, de ha hazugságért bíróság elé állítanánk az embereket, összeroppanna az igazságszolgáltatási rendszer. A hazugság-igazság kettősét a szólásszabadság szempontjából vizsgáló alkotmányjogi doktrínák a valótlanságok megítélésekor különbséget tesznek a tényállítások és a véleménynyilvánítások között. A véleménynyilvánítás oldaláról közelítve a hazugság is bírhat értékkel. John Milton *Areopagitica*jában éppen a hazugságok megismerhetősége az, ami elősegíti az igazság diadalát, hiszen a hazugságok cáfolata „némít el a legjobban és legbiztosabban".[575] Az Alkotmánybíróság 36/1994. (VI. 24.) határozatának sűrűn idézett fordulata, amely szerint a jog a „véleményt annak érték- és igazságtartalmára tekintet nélkül védi", azt az álláspontot erősíti, hogy valótlant állítani megengedett. A testület a 18/2000. (VI. 6.) határozatban is megerősítette a hazugság „értékét", amikor kimondta, hogy a „véleménynyilvánítás szabadságának csupán igen korlátozott lenne az értéke, ha nem jelentene többet, mint az igaz tények állításához való jogot". A valótlan tényközlésekkel szemben már kevésbé megengedő a jog, a gyakorlat számára ugyanakkor a tények és vélemények elhatárolása sokszor ütközik nehézségekbe.

Napjainkban népszerű téma a közbeszédben a hamis hírek vagy álhírek *(fake news)* terjedése, amelyek az interneten villámgyorsan képesek rengeteg emberhez eljutni. Mivel a *fake news* és más valótlanságok kifejezetten káros folyamatokat indíthatnak el a társadalomban vagy az egyénekben, felmerült a jogi eszközökkel, sőt akár a büntetőjogi eszközökkel történő korlátozásuknak a lehetősége. Az álhírek szabályozása ennek ellenére Európára nem jellemző, inkább a kevésbé demokratikus rendszerek élnek a szabályozás adta lehetőségekkel. Malajziában például az álhírek terjesztése

[575] Milton 2018: 30.

bűncselekmény, hat év szabadságvesztéssel, illetve 500 ezer ringgit mértékű bírsággal büntethető.[576] Oroszországban szintén büntethető az, aki álhíreket terjeszt, a pénzbüntetés mértéke akár a 1,5 milliárd rubelt is elérheti.[577] Szingapúrban az álhírnek minősített cikkek eltávolítására is lehetőség van.[578] Ugyan nincsen kifejezetten ebből a célból létrehozott jogszabály, Olaszországban lehetőség van a hamis híreket bejelenteni a rendőrségen,[579] Franciaországban pedig választásikampány-időszakban a bíróság elrendelheti a hamis hírek eltávolítását.[580]

Jelen fejezet célja kettős: az egyik, hogy feltérképezze a valótlan állítások, azon belül pedig a dezinformáció és a *fake news* jelenlegi szabályozási környezetét, a másik pedig, hogy kísérletet tegyen a lehetséges jövőbeli szabályozási irányok kijelölésére. Egy-egy új – vagy újszerű – jelenség észlelésekor természetes reakció a szabályozás igényének megjelenése. Az álhír, azaz *fake news* – noha a kifejezés neologizmus – egyáltalán nem új jelenség. Előzményeit az ókori Rómában is megtalálhatjuk, ahol Octavianus (a későbbi Augustus császár) az egyiptomi despota uralkodónő, Kleopátra által behálózott bábként festette le riválisát, Marcus Antoniust. Octavianus Marcus Antonius állítólagos végrendeletét is ismertette a római néppel és a szenátussal,[581] amelyben az állt, hogy Marcus Antonius a római uralom alatt álló kelet-mediterrán térség jelentős részét Kleopátrától született gyermekeire hagyná, Alexandriában kívánta magát eltemettetni, utódjául pedig Caesar és Kleopátra fiát jelöli meg (aláásva ezzel Octavianus hatalmát). Arról, hogy a végrendelet mennyiben volt valós, máig sincs egyetértés a történészek között,[582] mindenesetre elég volt ahhoz, hogy a római népben ellenérzés alakuljon ki, és a szenátus árulónak bélyegezze Marcus Antoniust, aki végül saját kardjával szúrta szíven magát. Marcus Antonius állítólag azért vetett véget önkezével életének, mert értesült Kleopátra halálhíréről, ami szintén valótlan hír volt, hiszen Kleopátra csak jóval később ölelte a halálát hozó kígyót a keblére: miután értesült Marcus Antonius öngyilkosságáról. Természetesen ezek az ókori történelemből kiragadott példák még nem a mai értelemben vett álhírek, inkább csak arra mutatnak rá, hogy a valótlan információk terjesztése stratégiai célok elérésére nem a modern kor vívmánya. A mai formában is ismert álhírterjesztés a modern hírmédiával együtt jelent

576 Beech 2018.
577 Putin Signs 'Fake News', 'Internet Insults' Bills Into Law 2019.
578 Fullerton 2019.
579 Giuffrida 2018.
580 Fiorentino 2018.
581 MacDonald 2017.
582 Sirianni 1984: 236–241.

meg, terjedésének és mennyiségének pedig a közösségi platformok a megszokottnál jóval nagyobb teret biztosítottak.

Az álhír fogalmának jelentéstartalma valójában nem tisztázott, az álhírnek minősülő információk terjesztése tulajdonképpen többféle magatartást takar. Az álhír ráadásul több más fogalommal, például a dezinformációval párhuzamosan használatos, noha nem feltétlenül ugyanarra a jelenségre vonatkoznak. A fejezet első része éppen ezért a fogalmak tisztázására és rendszerezésére törekszik.

A fogalmak tisztázása után látni fogjuk, hogy az álhírek esetében korántsem a jog által szabályozatlan terrénumról van szó, a hamisság több jogágban is felbukkan, egyes esetekben pedig a valótlanság állításához a törvényhozó büntetőjogi szankciót is kapcsolt. A fejezet áttekinti az interneten megvalósuló közléseknek azokat a formáit, amelyek büntetőjogi tényállást sértenek, különös figyelmet fordítva arra, ahol a közlés valótlansága a tényállás elemét képezi. Ezenfelül áttekintjük azokat a közléseket is, amelyek ugyan valótlanok, terjesztésük mégsem szankcionálandó, mivel ezek esetében a szabad véleménynyilvánításhoz fűződő érdek erősebb, mint a társadalom érdeke a felelősségre vonásra.

Mi az álhír (fake news) és a félretájékoztatás (disinformation)?

Papp János Tamás felhívja a figyelmet arra, hogy a hamis hírnek nincs tudományos konszenzus alapján elfogadott definíciója, és az álhír sem számít tudományos szakszónak.[583]

A kifejezés pontos tartalmának meghatározásakor már ott problémával szembesülünk, hogy magának a „hír"-nek sincsen definíciója. A Cambridge English Dictionary szerint a hír a közelmúlt eseményeiről szóló információ vagy tájékoztatás.[584] A szótári megfogalmazás azonban túlegyszerűsítő, és valójában a hírnek csak a köznyelvi definícióját adja meg. E definíció szempontjából közömbös, hogy a hír a sajtóban jelenik meg, vagy a szomszédasszony újságolja. A köznyelvi definíció azt sem veszi számításba, hogy a közlés nagy nyilvánosság előtt zajlik, vagy magánszemélyek osztják meg egymással. A tömegkommunikáció-elmélet gondolkodói a „hírt" a sajtóhoz kapcsolják. Pamela Shoemaker szerint a hír „az, ami nap mint nap megjelenik az újságokban, médiumokban".[585] A tömegkommunikációs hírfogalmat alapul véve tehát a hamis

583 Papp 2020: 141–164.
584 Cambridge Dictionary [é. n.].
585 Shoemaker–Cohen 2012: 106.

hírek is olyan információk, amelyek a hagyományos hírmédiában (akár nyomtatott, akár televíziós) vagy online (internetes sajtótermékekben vagy közösségi oldalakon) jelennek meg.

Az Európai Bizottság kutatócsoportja által készített tanulmány szűkebb és tágabb álhír *(fake news)* definíciókat különböztet meg.[586] A szűkebb definíciók csak a bizonyítottan hamis információkat tekintik álhíreknek. Hunt Allcott és Matthew Gentzkow úgy határozzák meg az álhíreket, mint szándékosan és bizonyíthatóan rossz vagy valótlan híreket, amelyeket azzal a céllal alkottak, hogy pénzt keressenek és/vagy ideológiát népszerűsítsenek velük.[587] Álláspontjuk szerint nem tartoznak a hamis hírek közé a ferdítések, összeesküvés-elméletek, a pletykák és a politikusok valótlan állításai. Azt viszont, hogy melyik információ minősül hírnek, ők sem vizsgálják, ráadásul a közzétételhez nemcsak a hamisság, hanem az ártó szándék követelményét is hozzákapcsolják.

A hamis hírek tágabb definíciói már magukban foglalják a szándékos félretájékoztatást *(disinformation)* és a hírek eltorzítását is. Claire Wardle és Hossein Derekshan a károkozás és a hamisság három dimenzióját különböztetik meg: a) a téves tájékoztatást *(misinformation),* amikor a valótlan információt ártó szándék nélkül osztják meg másokkal, b) a félretájékoztatást *(disinformation),* amikor valótlan információt tudatosan, károkozási szándékkal osztanak meg, illetve c) az ártó szándékú tájékoztatást *(malinformation),* amikor valós információt osztanak meg ártó szándékkal.[588]

A hamis hír *(fake news)* sokak szerint már elhasznált kifejezés, a brit kormányzat egyenesen megtiltotta annak használatát szakpolitikai dokumentumokban, mivel az egy gyengén megfogalmazott félrevezető terminus, amely összemossa a hamis információk egyes fajtáit, az egyszerű hibától a demokratikus folyamatokba való idegen beavatkozásig.[589] A brit Alsóház Digitális, Kultúra, Média és Sport Bizottságának jelentése[590] inkább a dezinformáció és a téves tájékoztatás kifejezések alkalmazását javasolja. A dezinformáció fogalmát a jelentés úgy határozza meg, mint hamis és/vagy manipulált információ szándékos terjesztése, amelynek a célja a közönség megtévesztése vagy félrevezetése károkozás vagy politikai, személyes vagy anyagi haszonszerzés céljából. A téves tájékoztatás a hamis információ tévedésből történő megosztása.

586 Martens et al. 2018: 10.
587 Allcott–Gentzkow 2017: 211–236.
588 Wardle–Derekshan 2017.
589 Murphy 2018.
590 House of Commons Digital, Culture, Media and Sport Committee 2019.

Az EU magas szintű szakértői csoportja szintén elveti az álhír kifejezés használatát, és a dezinformáció kifejezést alkalmazza. Ennek két oka van, az egyik, hogy az álhír kifejezés nem képes lefedni a félretájékoztatás összes esetkörét, mivel nem foglalja magában azokat a tartalmakat, amelyeket valós tények bedolgozásával állítottak elő, és azokat a gyakorlatokat sem fedi le, amelyek az információ terjedését segítik, például a hamis követők, botok, manipulált videók, targetált reklámok, szervezett trollkodás, mémek.[591] A második ok, amiért a csoport elveti az álhír kifejezés alkalmazását, az, hogy politikusok gyakran használják a kifejezést azokra a tudósításokra, amelyekkel egyszerűen nem értenek egyet, ami megtévesztő lehet.

A magas szintű szakértői csoport a dezinformációt úgy határozza meg, mint „olyan igazolhatóan hamis, pontatlan vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy közérdeknek való károkozás céljából hoznak létre, hoznak nyilvánosságra és terjesztenek". Nem tartoznak a félretájékoztatás körébe a jelentéstételi hibák, a szatírák és paródiák, illetve az egyértelműen azonosítható módon pártokhoz köthető hírek és kommentárok.[592] A megtévesztő jellegű kereskedelmi közlemények szintén nem minősülnek dezinformációnak, ahogyan az egyén személyét sértő valótlan – rágalmazásnak, illetve becsületsértésnek minősülő – közlések sem.

A valótlan közlések és a büntetőjog kapcsolódásai

Az álhír, illeve a dezinformáció fogalmai a büntetőjogi terminológia számára is értelmezhetetlenek. E jelenségek a társadalmi diskurzusban nyilvánvalóan károsak, ám nem lehet őket egyetlen Btk.-beli tényállás alá rendezni. Ez részben abból fakad, hogy a valótlan vélemények nem érik el azt a társadalomra veszélyességi szintet, amely szankcionálást indokolna. Az esetek másik részében pedig a közlés valóságtartalmának jelenleg is van büntetőjogi relevanciája, annak hír voltától teljesen függetlenül. A büntető törvénykönyvben több olyan, közlésekkel megvalósítható deliktum is található, amelyeknél a közlés valóságtartalmának van jelentősége, a következőkben ezeket tekintjük át.

[591] European Commission, Directorate-General for Communications Networks, Content and Technology 2018: 10.

[592] European Commission, Directorate-General for Communications Networks, Content and Technology 2018: 10.

Hamis vád és hamis tanúzás

Az igazságszolgálatás elleni bűncselekmények között több olyan deliktumot is találunk, ahol a kinyilvánított közlés társadalomra veszélyessége annak hamisságában rejlik. Ilyen a Btk 268. §-ában szabályozott hamis vád, amelynek alapján bűntettet követ el az, aki mást bűncselekmény elkövetésével hamisan vádol. A Btk. Nagykommentárja[593] szerint a vádolás arra vonatkozó valótlan tényállítás, hogy konkrétan beazonosítható személy bűncselekményt követett el, amennyiben az alkalmas arra, hogy büntetőeljárás induljon a megvádolt személy ellen. A BJD 7330. számú döntés foglalkozott azzal, hogy hamis vád csak kifejezett tényállítással – olyan tartalmú kijelentéssel, „amely szerint valamely bűncselekmény törvényi tényállását alkotó esemény múltbeli megvalósulása a megvádolt személy magatartásaként realizálódott" – valósítható meg. A Btk. hivatkozott tényállása meghatározza az elkövetés helyét is: annak hatóság előtt kell történnie. A hamis vád fogalmának ugyan megfelelő, de sajtó útján tett állítások – például egy politikus sikkasztásáról szóló valótlan újságcikk – nem merítik ki e tényállást.

A hamis vádhoz e tekintetben nagyon hasonlít a hamis tanúzás, amelyet a Btk. 272. §-a szabályoz. Eszerint a tanú, aki a hatóság előtt az ügy lényeges körülményére valótlan vallomást tesz, hamis tanúzást követ el. A bűncselekmény alanya ez esetben speciális, hiszen az csak tanú, szakértő vagy tolmács lehet. Az elkövetés helye ebben az esetben is tényállási elem, azt csak hatóság előtt lehet elkövetni. Internetes közléssel, esetleg egy televíziónak adott interjúval nem valósítható meg a tényállás, akkor sem, ha az elkövető a megfelelő büntetőeljárásbeli pozícióval rendelkezik.

A rémhírterjesztés

A rémhírterjesztésről a kötet korábbi részében már részletesen esett szó. A Btk. 337. §-ában megfogalmazott tényállása már megvalósulhat hamis hírek terjesztésével, félretájékoztatással. A Btk. 337. §-ában szabályozott deliktumnak a 2020-as koronavírus-járvány eseményeire reagáló Btk.-módosítás óta két alapesete van. Mindkét alapeset elkövetési magatartása valótlan tény vagy való tény elferdített állítása, híresztelése. A Btk. tehát nemcsak a teljességében valótlan, koholt tények közlésével tekinti megvalósíthatónak a tényállást, hanem azzal is, ha valaki valós, objektíve létező tényeket közöl, azonban azokat „összefüggéseiből torzítva ragadja ki, a kedvező vagy

[593] Mezőlaki 2019: 609–651.

a kedvezőtlen mozzanatokat a maga szempontja szerint emeli ki".[594] Az információ manipulálásával, kiszínezésével megvalósított tényközlés, illetve híresztelés tehát tényállásszerű magatartás lehet. A két alapeset közötti különbség az elkövetés helyében, illetve annak körülményeiben rejlik. Az első alapeset elkövetési magatartása csak akkor lesz tényállásszerű, ha azt közveszély színhelyén, nagy nyilvánosság előtt tanúsítják. A közveszély fogalmát a büntetőjogban úgy kell értelmezni, mint olyan emberi magatartás következtében kialakult helyzetet, amelyben fennáll a közeli, valós veszélye annak, hogy nagyobb számú személy vagy jelentős értékű dolog sérül, semmisül meg. Különös jelentősége van annak, hogy a közveszély emberi magatartás által bekövetkező esemény, vagyis nem lehet közveszélynek minősíteni a természeti katasztrófákat (például hurrikán) vagy járványokat. A Btk. kommentárja a helyszín fogalmát tágan értelmezi, amikor rögzíti, hogy az elkövetőnek nem kell fizikailag a cselekmény színhelyén tartózkodnia. A cselekmény akkor is megvalósulhat, ha az elkövető kommunikációját a közveszély helyszínén tartózkodó, előre meg nem határozható számú befogadó (a nagy nyilvánosság) észlelheti. A rádió- vagy televízióadáson keresztül továbbított közlések, de akár még a közösségimédia- vagy videómegosztó platformokon streamelt közlések is megvalósíthatják a cselekményt. Ebből tehát arra következtethetünk, hogy az elkövető fizikai helye a tényállás szempontjából másodlagos, a rémhírterjesztés társadalomra veszélyességét az jelenti, hogy egy pontosan meghatározott földrajzi helyen (a közveszély helyszínén) fejt ki negatív hatást. Az elkövetés azonban így is csak abban az esetben lesz tényállásszerű, ha a közlés alkalmas arra, hogy a színhelyen lévő emberekben zavart vagy nyugtalanságot keltsen. Az eredmény bekövetkezése (vagyis a zavar, illetve a nyugtalanság tényleges kialakulása) nem feltétele a magatartás tényállásszerűségének, elegendő, ha a közlés a nevezett eredmény kiváltására objektíve alkalmas. A Btk. kommentárja szerint a cselekmény csak szándékosan követhető el, az elkövető tudatának pedig a tényállás összes elemére ki kell terjednie. Ez egyrészt jelenti azt, hogy az elkövetőnek tisztában kell lennie azzal, hogy az általa tett közlés valótlan vagy torzított, másrészt azzal, hogy kommunikációja miatt zavar vagy nyugtalanság keletkezhet, harmadrészt pedig azzal, hogy a közlés közveszély színhelyén, nagy nyilvánosság előtt történik. A tévedésből terjesztett hamis információval *(misinformation)* akkor sem valósítja meg a tényállást, ha gondatlanul járt el, vagyis például azért nem ismerte fel a híresztelt tény valótlanságát, mert a tőle elvárható figyelmet és körültekintést elmulasztotta. A jelenleg hatályos Btk. tehát nem követeli meg azt, hogy a továbbadott információk tekintetében az egyén

[594] Mezőlaki 2019: 609–651.

mint tényellenőrző szervezet *(fact-checker)* járjon el. A nem hiteles forrásból származó valótlan információk továbbközlése (például közösségi oldalon történő megosztása) tehát – az összes törvényi feltétel teljesülése mellett – csak abban az esetben minősülhet rémhírterjesztésnek, ha az elkövető tudata átfogja az általa terjesztett információ valóságtartalmat nélkülöző vagy valóságot elferdítő mivoltát.

A második alapeset a különleges jogrend idején a védekezés eredményességét akadályozó vagy meghiúsító módon való elkövetést rendeli büntetni. Az elkövetési magatartások ebben az esetben is ugyanazok, mint az első alapesetben, az elkövetés viszont nincsen meghatározott helyhez kötve. Az elkövetés feltétele ebben az esetben a különleges jogrend fennállása. A különleges jogrend alkotmányos szempontból speciális időszak, az Alaptörvény által minősített, illetve a békétől eltérő időszakok gyűjtőfogalma.[595] Különleges jogrendnek minősül:

- a rendkívüli állapot,
- a szükségállapot,
- a veszélyhelyzet,
- a váratlan támadás,
- a megelőző védelmi helyzet és
- a terrorveszélyhelyzet.

A közlés ezekben az esetekben akkor tényállásszerű, ha az akadályozza vagy meghiúsítja a védekezést. A Btk. 2020. évi XII. törvénnyel történt kiegészítését széles körben kritizálták. A Magyar Helsinki Bizottság az új tényállásban főképp azt kifogásolja, hogy a védekezés, illetve a védekezés eredményessége olyan jogilag bizonytalan fogalmak, amelyek alkalmatlanok arra, hogy az állampolgárok a magatartásukat hozzájuk igazítsák.[596] Bencze Mátyás és Ficsor Krisztina arra hívják fel a figyelmet, hogy „a jogi normák általános fogalmakat tartalmaznak, így elkerülhetetlen, hogy értelmezés útján tárjuk fel a jelentésüket".[597] A szerzők arra is rámutatnak, hogy ennek a kérdésnek az eldöntésére „társadalomtudományi (szociálpszichológiai, statisztikai) módszerekre és elemzésekre lenne szükség", ezek pedig nem állnak sem a jogalkalmazó, sem az állampolgár rendelkezésére.

Ezek az elméletek azonban a tekintetben pontatlanok, hogy az átlagpolgár és a bíróság ismeretei között mindig van különbség. A legtöbben vélhetően nehezen tudnák elhatárolni egymástól a rágalmazás és a becsületsértés tényállásait, hiszen a törvény

595 Till 2019.
596 Magyar Helsinki Bizottság 2020.
597 Bencze–Ficsor 2020.

ezekben a deliktumokban becsület csorbítására alkalmas tény vagy vélemény közléséhez rendel büntetőjogi szankciót, anélkül természetesen, hogy taxatíve felsorolna minden e körbe tartozó kifejezést. Álláspontom szerint a rémhírterjesztés új tényállása esetében sincsen szükség a védekezés akadályozására vagy meghiúsítására alkalmas magatartások tételes felsorolására – vélhetően nem is lehetséges ilyen listát alkotni, ahogyan a becsület csorbítására alkalmas kifejezésekről sem készíthető a teljesség igényével lista –, elegendő a cselekmény objektív alkalmassága. Koltay András kifejti, hogy ezeknek az információknak a köre meglehetősen szűk, és nem tartozik ide minden járványhelyzettel összefüggő valótlan tényállítás (például a Velencébe visszatérő hattyúkról és a Szardínia partjainál látott delfinekről szóló valótlan hír aligha minősülhet rémhírterjesztésnek).[598] Nem minősül rémhírterjesztésnek a valós, bár nyugtalanító információk közzététele,[599] sem pedig a vélemények közlése.[600]

Akárcsak az első alapeset, a különleges jogrend idején történő rémhírterjesztés is csak szándékos bűncselekmény lehet, tehát az elkövető tudattartalmának át kell fognia azt, hogy valótlan állítása alkalmas lehet arra, hogy a védekezést akadályozza vagy meghiúsítsa.

A fogyasztók megtévesztése

A Btk. védelemben részesíti a megalapozott fogyasztói döntéshozatalt, amikor a 417. §-ban büntetni rendeli a megtévesztő kereskedelmi kommunikációk bizonyos körét. A kereskedelmi kommunikáció, amely megjelenhet a sajtóban, a rádióban, a televízióban, sőt online felületeken is, médiatartalomnak minősül ugyan, de nem számít hírnek. Az online térben folytatott kereskedelmi tevékenységek körében a fogyasztók megfelelő tájékoztatásának különösen nagy jelentősége van, hiszen az interneten látott hirdetések esetében a fogyasztó nem tudja megtekinteni, megvizsgálni az árut, a döntéshozatal során pusztán az arról közzétett információkra hagyatkozik. Az *Index.hu* hírportál még 2017-ben hívta fel a figyelmet arra a problémára, hogy az interneten széles körben alkalmazott automatikus hirdetéskiszolgáló rendszereken egészen nyilvánvalóan valótlan hirdetések is tömegesen vannak jelen.[601] Az olyan szlogenek,

598 Koltay 2020.

599 Jen 2020.

600 Varga Judit szerint a rendőrség tévedett, amikor rémhírterjesztés gyanújával két férfit a véleménye miatt állított elő 2020.

601 Hanula 2017.

mint a „Fogyás, ami megrémíti az orvosokat! Ez a furcsa módszer 26 kiló zsírtól szabadít meg egy hét alatt!", vagy az „Egy furcsa nyelvtanulási módszer hihetetlen eredményei!", annak ellenére, hogy valótlanok, rendszeresen megjelennek különböző portálokon. A fogyasztók megtévesztésére különösen jó terepet teremtenek a különböző online piacterek. Olaszországban kilenc hónap szabadságvesztésre ítéltek egy TripAdvisor-felhasználót, amiért az valótlan értékeléseket tett közzé, ezzel növelve egyes szálláshelyek értékelését és látogatottságát.[602]

A fogyasztók megtévesztésének általános alakzatát a tényállás (2) bekezdése szabályozza, míg az (1) bekezdés egy speciális alakzatról, a szervezett termékbemutatón történő megtévesztésről szól. A fogyasztók megtévesztésének általános alakzata háromféle elkövetési magatartással is megvalósítható: valótlan tény állításával, valós tény megtévesztésre alkalmas módon állításával, illetve megtévesztésre alkalmas tájékoztatással. Mindegyik közlésnek az áru lényeges tulajdonságára kell vonatkoznia, amely tulajdonságok a (4) bekezdés értelmezése szerint az áru összetétele, műszaki jellemzői és az árunak az adott célra való alkalmassága, az áru eredete, származási helye és előállításának módja, az áru tesztelése, ellenőrzöttsége vagy annak eredménye. A megtévesztésre alkalmas tájékoztatás magában foglalja a tudatosan hiányos információk közlését is, ami „a kelendőség ellen ható információk elhallgatását jelenti, tevéssel és (részben) mulasztással is megvalósítható".[603]

A valótlan hirdetéseket kínáló oldalakkal kapcsolatban az igazi nehézség nem a tényállásszerűség megállapítása, hanem a felelősségre vonás. Az oldalak ugyanis többnyire külföldi doménen vannak bejegyezve, és olyan külföldön bejegyzett cégekhez tartoznak, amelyek probléma esetén gyorsan megszüntetik a honlapjukat.[604] Azok a szereplők, akik az online környezetben hatékonyan felléphetnek a megtévesztő kereskedelmi kommunikáció ellen, a közvetítő szolgáltatók. Idetartoznak azok a közvetítő szolgáltatók, amelyeknek a felületein a hirdetők közvetlenül elhelyezhetik a hirdetéseiket (például a Facebook online piactere, de azok a tárhelyszolgáltatók is, amelyek harmadik személyek adásvételei számára biztosítanak felületet, mint az Ebay), de idetartoznak a hirdetéskiszolgáló rendszerek (mint a Google AdSense), de akár a doménregisztrátorok is.

602 Horton 2018.
603 Karsai 2019a: 972–988.
604 Hanula 2016.

Az online platformok szerepe a félretájékoztatás elleni fellépésben

Az Európai Bizottság kezdeményezésére 2018-ban született meg a dezinformáció visszaszorítását célzó gyakorlati kódex (Code of Practice on Disinformation). A kódex aláírói azok az online platformok (köztük olyan közösségimédia-platformok, mint a Facebook és a Google), amelyek fő tevékenysége, hogy felhasználói tartalmaknak biztosítanak megjelenési felületet, de maguk is nagy hatással vannak az online információáramlásra azáltal, hogy ezeket a tartalmakat rendszerezik, rangsorolják, csoportosítják, vagy ha szükséges, törlik.

A kódex céljai között szerepel, hogy védelmet nyújtson a félretájékoztatás ellen, lehetővé tegye a hirdetések elhelyezésének ellenőrzését, hogy a félretájékoztatás terjesztői minél kevesebb bevételre tegyenek szert, biztosítsa a politikai hirdetések elhelyezésének átláthatóságát, továbbá, hogy elősegítse a megbízható tartalmak könnyű megtalálhatóságát.

A Bizottság a kódex végrehajtásáról szóló önértékelések közzétételekor[605] több kritikát is megfogalmazott platformokkal szemben, többek között azt, hogy a 2019 májusában lezajlott európai parlamenti választások alkalmával sem sikerült megfékezniük az automatizált eszközökkel, tömegesen terjesztett álhírek áradatát. Az Európai Bizottság szerint sürgős szükség volna arra, hogy a platformok együttműködjenek tényellenőrzőkkel és más független szervezetekkel is, valamint arra, hogy a platformok közelítsék egymáshoz a gyakorlataikat, mert eltérően hajtják végre a kódex rendelkezéseit. Az álhírek *(fake news)* és a félretájékoztatás *(disinformation)* kérdését az Unió jelenleg nem jogalkotás útján kívánja kezelni – habár az EP-választások előtt a Bizottság megvillantotta ennek a lehetőségét[606] –, hanem elsősorban ön- és társszabályozás megerősítése révén. A gyakorlati kódex felülvizsgálatát követően 2022-ben a platformok újabb vállalásokat tettek:

- demonetizálják a félretájékoztató tartalmakat, hogy készítőik ne jussanak anyagi haszonhoz a hirdetési bevételekből;
- biztosítják a politikai reklámok átláthatóságát azáltal, hogy nyilvánossá teszik, ki a megrendelő, illetve hogy kinek az érdekében készült;
- támogatják a kutatási tevékenységeket, amelyek a dezinformációt vizsgálják;
- kiterjesztik a tényellenőrzést az Európai Unión belül, több nyelv támogatását teszik lehetővé a tényellenőrző szoftvereknek;

[605] European Commission 2019.
[606] Stupp 2018.

- átláthatósági központokat hoznak létre, ahonnan a felhasználók tájékozódhatnak a kódex alapján tett intézkedésekről;
- megerősítik a kódex érvényesülésének ellenőrzését szolgáló rendszert.[607]

A világ rendjét felborító koronavírus-járvány új kihívás elé állította a platformszolgáltatókat. Az otthon biztonságában töltött idő növekedésével párhuzamosan az internet forgalma is megnövekedett,[608] így a négy fal közé szorult felhasználók az átlagosnál jóval több időt kezdtek közösségi felületeken tölteni. Az emberek tájékoztatását szolgáló valós információk mellett azonban megugrott a hamis információk mennyisége is, olyannyira, hogy a WHO „infodémiának"[609] nevezte a valótlan információk özönét. 2022 februárjában az orosz–ukrán háború kitörése mozgatta meg az európai közérdeklődést, magával hozva a hiteles, gyors, megbízható információkhoz jutás szerepének felértékelődését.

Gyilkosság és erőszak a kibertérben

2016 elején egy kanadai bíróság egy 1949-ben megállapított és nem sűrűn alkalmazott tényállás, a közerkölcs megsértése *(corrupting morals)* miatt ítélte el egy weboldal üzemeltetőjét.[610] Mark Mareket, az internetes szennyoldalak között viszonylag népszerűnek számító Bestgore.com üzemeltetőjét azért ítélte hat hónap szabadságvesztésre a bíróság, mert obszcén tartalmakat helyezett el a felületen, közöttük azt a felvételt, amelyen egy férfi, Luka Magnotta brutálisan megöli, feldarabolja és megeszi áldozatát. A videó valódiságához kétség sem férhetett, az áldozat testrészeit az elkövető postán elküldte kanadai kormányzati tisztségviselőknek.[611] Marek az általa üzemeltetett, felkavaró tartalmaknak tárhelyet biztosító oldalt (*gore site*-ot) közérdekű tevékenységet ellátó oldalnak minősítette, részben amiatt, hogy álláspontja szerint a felhasználók közössége segíthet azonosítani a hasonló bűncselekmények elkövetőit. Az üzemeltető másik érve azt volt, hogy az ehhez hasonló weboldalak valójában *reality*-hírportálok, hiszen valósághűen, cenzúra nélkül mutatják be a közönségnek az eseményeket,[612]

607 The Strengthened Code of Practice on Disinformation 2022.
608 Reardon 2020.
609 Richtel 2020.
610 Blais 2016.
611 Anderson 2012.
612 Jeffries 2012.

nem titkolva azt, hogy a valóság a filmen és a televízióban látottaktól eltérően sokszor kegyetlen és brutális.

Az ítélet ellenére az említett weboldal továbbra is gond nélkül üzemel, sőt számtalan hasonló portál található az online térben. Ennek ellenére az ártalmas internetes tartalmak elleni fellépés kapcsán leggyakrabban az olyan globális szolgáltatók tevékenységéről, felelősségéről és szabályozásáról hallunk, mint a Facebook, a YouTube vagy a Twitter. Noha néhány esetben a közismert és széles körben használt szolgáltatók gyakorlata is kifogásolható egyes tartalmak vonatkozásában, az igazán durva tartalmak nem ezeken a felületeken találhatók. A legnagyobb szolgáltatók, amelyek tevékenysége jellemzően jelentős médiafigyelmet kap, a jogszabályi előírásoknak és a saját felhasználási feltételeiknek megfelelően moderálják a tartalmakat. A kisebb, rétegszolgáltatások nyújtására létrehozott platformokkal összefüggő problémákról kevesebbszer esik szó, holott ezek a felületek is igen nagy mennyiségű felhasználót érnek el, kumulálva pedig egyáltalán nem elhanyagolható problémát okoznak az internet egészséges működése szempontjából. Az egyértelműen jogsértő és a jogszerűség mezsgyéjén egyensúlyozó tartalmakat az olyan platformokon „éri meg" megosztani, ahol kicsi a moderálás valószínűsége, biztosítható az anonimitás és a titkosítás. Ezek a rétegszolgáltatások gyakran nem a nyílt interneten, hanem a sötét weben találhatók.

Jelen fejezet fókuszában a szélsőségesen erőszakos tartalmak és azok a szolgáltatások állnak, ahol ezek megtalálhatók. A szélsőségesnek minősített tartalmak tipizálásán túl ismertetjük az európai, a magyar, illetve az amerikai tartalomszabályozás körébe eső rendelkezéseket.

Az online található szélsőségesen erőszakos tartalmak jogi megítélése

A szélsőségesen erőszakos, illetve extrém tartalmak kategóriája nem homogén. Valójában még arról sincsen konszenzus, hogy milyen tartalmakat minősíthetünk szélsőségesnek, hiszen sok tartalom megítélése a felhasználók szubjektív értékítéletétől és világnézetétől függ. Az erőszak bemutatása egyes kultúrákban kevésbé kifogásolható, más kultúrákban ellenben elfogadhatatlan (Kínában például tilos az olyan videójátékok forgalmazása, amelyek vért ábrázolnak[613]). A szélsőségesen erőszakos tartalmakról mind az európai, mind a magyar jog szűkszavúan rendelkezik. E szabályok is többnyire tartalomszabályozási és nem büntetőjogi jellegűek. Ebben az alfejezetben azt

[613] Liszewski 2019.

tekintem át, hogy hol találkozhat a tartalomszabályozás és a büntetőjog eszközrendszere, figyelmet szentelve annak, hogy a szélsőséges, erőszakos tartalmak terjesztése mikor igényel büntetőjogi szankciót.

Az audiovizuális médiaszolgáltatásokat és a videómegosztó platformokat szabályozó audiovizuális médiaszolgáltatásokról szóló irányelv (AVMS irányelv) a 2019-es módosítását megelőzően a valószínűsíthetően káros, illetve súlyosan káros tartalmakat különböztette meg egymástól a kiskorúak védelmének szabályai körében.[614] A súlyosan káros tartalmak közé sorolta a pornográfiát és az indokolatlan erőszakot – azt azonban, hogy mikor minősül indokolatlannak az erőszak, már nem határozta meg. A hatályos irányelv ezt a megkülönböztetést megszüntette, és már csak káros tartalmakról rendelkezik. A módosított irányelv új rendszerében a káros tartalmak nem választhatók élesen ketté, inkább egy skálán helyezhetők el, amelynek az egyik végpontjához közel a kevésbé káros, míg a másik végpontjához közel a súlyosan káros tartalmak helyezkednek el. Az irányelv azt is kimondja, hogy a legkárosabb tartalmak – például az öncélú[615] erőszak és a pornográfia – esetében a legszigorúbb tartalomkorlátozó intézkedéseket kell alkalmazni.[616]

A kiskorúak védelmére fókuszáló tartalomszabályozás mellett az AVMS szól azokról a tartalmakról is, amelyek terjesztése uniós bűncselekményt valósít meg (azaz terrorista bűncselekmény elkövetésére való nyilvános uszítás, gyermekpornográfiával kapcsolatos bűncselekmény, valamint rasszizmussal és idegengyűlölettel kapcsolatos bűncselekmény).[617]

Arra nézve, hogy a gyűlöletkeltő, illetve a bűncselekményt megvalósító tartalmaktól milyen módszerekkel kell megvédeni a közönséget, az irányelv nem rendelkezik. Ezekben az esetekben ugyanakkor csak egyfajta intézkedés képzelhető el a megfelelő védelem biztosítása érdekében: az ilyen jellegű tartalmak eltávolítása, hiszen a társadalom érdeke ezekben az esetekben nem a hozzáférés korlátozása egy sérülékeny csoport védelme érdekében, hanem az, hogy senkinek ne legyen hozzáférése azokhoz. A szolgáltató kötelessége a DSA rendelet és az Eker. irányelv szolgáltatói felelősséget szabályozó passzusaival[618] összhangban a tartalom törlése, mivel a szolgáltató akkor

614 2010-es AVMS irányelv 27. cikk.

615 Az irányelv eredeti, angol nyelvű szövege továbbra is a *gratuitous* jelzőt használja, a magyar öncélú jelző használata tehát inkább a fordítás során végzett nyelvi változtatás, és nem tartalmi jellegű.

616 2018-as AVMS irányelv 6a. cikk (1).

617 2018-as AVMS irányelv 28b. cikk (1).

618 Eker. irányelv 12–14. cikkek.

mentesül a harmadik személyek által megosztott tartalmakért viselt felelősség alól, ha a tartalom természetéről való tudomásszerzést követően intézkedik azok eltávolításáról.

E szabályok alapján kiviláglik, hogy a szélsőséges erőszakot ábrázoló tartalmak a skála súlyosan káros tartományában helyezkednek el, és amennyiben ezzel együtt közzétételük bűncselekményt is megvalósít, az eltávolítás elrendelése az egyetlen lehetséges megoldás, a közzétevőjük egyidejű büntetőjogi felelősségre vonása mellett. Ebben a tartományban helyezkednek el azonban olyan tartalmak is, amelyek nem sértenek uniós büntetőjogi normát, azonban jellegüknél fogva megbotránkoztathatnak és félelmet kelthetnek. Ezek közzétételét vagy a tagállami jogrendszerek, vagy a platformok felhasználási feltételei tiltják meg.

Ilyenek lehetnek az olyan tartalmak, amelyek sértik az emberi méltóságot. Az emberi méltósággal összefüggő rendelkezést az irányelv normatív erővel bíró rendelkezései esetében csak a kereskedelmi közleményeknél találunk,[619] az irányelv preambuluma azonban kimondja, hogy a tagállamok kötelessége az emberi méltóság védelme és tiszteletben tartása,[620] amely ekként a médiaszolgáltatókra és videómegosztókra vonatkozó kötelezettségek meghatározásában ölthet testet. Az emberi méltóságot sértő tartalmak esetében az sem ritka, ha azok közzététele valamely tagállamban bűncselekményt (például rágalmazást) vagy más jogsértést (például személyiségi jogsértést) valósít meg. Az emberi méltóság médiaszabályozásbeli védelmével kapcsolatban Koltay András kiemeli, hogy azt az európai országok jellemzően a hírnév és becsület megsértésének alternatívájaként vagy azzal azonos rendelkezésként fogalmazzák meg, tehát az emberi méltóság megsértése esetén akár médiahatósági eljárás is indulhat.[621]

Az AVMS irányelv szabályait hazánkban az Ekertv., az Mttv.[622] és az Smtv.[623] ültetik át, azonban a súlyosan káros tartalmak további lehetséges fajtái tekintetében ezek sem igazítanak el. Az audiovizuális médiaszolgáltatások tekintetében az Mttv. szerint[624] az a műsorszám, amely pornográfiát vagy szélsőséges, illetve indokolatlan erőszakot tartalmaz, a VI. korhatári kategóriába sorolandó, így médiaszolgáltatásban például csak akkor tehető közzé, ha a médiaszolgáltató biztosítja, hogy a médiaszolgáltatás titkosított formában tartalmazza a műsorszámot.[625] Az Mttv. nem kívánja

619 A 2018-as AVMS irányelv 9. cikke előírja, hogy a kereskedelmi közlemény nem sértheti az emberi méltóság tiszteletben tartását [9. cikk (1) c) i. pont].

620 2018-as AVMS irányelv (60) preambulumbekezdés.

621 Koltay 2012: 39.

622 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról.

623 2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól.

624 Mttv. 9. § (5) bekezdés.

625 Mttv. 10. § (1) bekezdés e) pont és 11. § (2) bekezdés.

ezeket a tartalmakat teljesen elzárni a közönség elől, csupán azt kívánja biztosítani, hogy a nézők kifejezett akaratukon kívül ne találkozhassanak ilyen tartalmakkal a médiaszolgáltatásokban. A Nemzeti Média- és Hírközlési Hatóság (NMHH) Médiatanácsának korhatár-besorolást segítő klasszifikációs ajánlása[626] szerint szélsőséges, illetve indokolatlan az erőszak, ha „az egyes erőszakos cselekmények oly mértékben elhúzódóan és kegyetlen részletességgel kerülnek ábrázolásra, hogy az messze túllépi a dramaturgiailag szükségszerűt", illetve ha „az erőszak nem játszik integráns szerepet a cselekmény, a jellem vagy a téma kibontásában, vagy ha felismerhető ok nélkül, túlzón, csak magáért az erőszakért van jelen, abból a feltételezésből kiindulva, hogy az erőszak a nézők számára attraktív, figyelemfelkeltő hatású, ezért magasabb nézettséget garantál". Az Mttv. ugyan nem tesz kimondott megkülönböztetést a fikciós erőszak és a hús-vér emberek bántalmazását, kiszolgáltatott, megalázott helyzetét bemutató műsorok között, az Smtv. rendelkezéseit vizsgálva azonban elmondható, hogy van ilyen különbség. Az Smtv. a médiaszolgáltatásokkal szemben előírja, hogy azok tartsák tiszteletben az emberi méltóságot, tehát médiaszolgáltatásban nem mutathatók be a megalázó, kiszolgáltatott helyzetben lévő emberek.[627]

A videómegosztó platformok vonatkozásában az AVMS-ben foglaltakhoz hasonló követelményeket fogalmaz meg az Ekertv., amely a 2020-ban elfogadott módosítását követően szabályozza a videómegosztóplatform-szolgáltatók tevékenységét. A videómegosztóplatform-szolgáltatások hatékony műszaki megoldásokkal kötelesek biztosítani, hogy a kiskorúak fizikai, szellemi, lelki vagy erkölcsi fejlődésére káros, az emberi méltóságot sértő, a gyűlöletkeltésre vagy erőszakra uszításra alkalmas, illetve a bűncselekményt megvalósító műsorszámok és felhasználók által előállított videók korlátozottan jussanak el a közönséghez.[628] Az AVMS irányelv rendelkezéseit egy ponton tehát kiegészíti az Ekertv., hiszen az emberi méltóságot sértő tartalmak korlátozásáról az irányelv nem rendelkezik, az Ekertv. pedig a gyűlöletkeltéssel, illetve az erőszakra uszítással párhuzamosan nevesíti. Az emberi méltóság védelmének *expressis verbis* kimondása üdvözlendő, elhelyezése a törvényben azonban elméleti szempontból vitatható. Az emberi méltóság olyan alapjog, amelynek az elismeréséből fakad „a gyűlöletbeszéd tilalma, a nevesített személyiségi jogok (képmás, hangfelvétel, személyes adatok védelme, jóhírnév, becsület stb.), a gyermekek védelme, de még akár a kereskedelmi közlemények korlátozása is".[629]

626 Nemzeti Média- és Hírközlési Hatóság 2011.
627 Smtv. 14. §.
628 Ekertv. 15/D. §.
629 Koltay 2012: 40.

Az Ekertv. nem határozza meg, hogy mi minősül hatékony intézkedésnek, csupán annyit rögzít, hogy az intézkedés akkor hatékony, ha arányban áll a tartalom által okozható hátránnyal, ártalommal,[630] a kiskorúakra legkárosabb tartalmak esetében pedig a legszigorúbb hozzáférés-korlátozás alkalmazását írja elő.[631] Egy ponton a magyar jogalkotónak is lehetősége lett volna meghatározni, hogy mi minősül hatékony intézkedésnek. A bűncselekményt megvalósító tartalmak esetében nem elegendő a hozzáférés egyszerű korlátozása. Azzal, hogy a jogalkotó az emberi méltóságot sértő tartalmakat is ebben a kategóriában helyezte el, amellett foglalt állást, hogy az ilyen tartalmaknak a videómegosztó platformokon sincs helyük. Noha az álláspont teljes mértékben helyeselhető, okozhat a jövőben jogalkalmazási problémákat, hogy más, nem Magyarországon honos platformok vonatkozásában nem érvényesül ilyen követelmény – legfeljebb csak abban az esetben, ha a platform felhasználási feltételei tiltják az emberi méltóságot sértő tartalmak közzétételét.

Magyarország azon tagállamok közé tartozik, ahol a jogalkotó a bűncselekménynek minősülő tartalmak listáját bővítette olyan tartalmakkal, amelyek az uniós jog szerint nem, de a magyar jog szerint bűncselekménynek minősülnek. Az Ekertv. nem szűkíti a bűncselekmények listáját a nemzetközi jog által szankcionálandó tartalomközlésekre, hanem azokat az „így különösen" fordulat használata révén csak exemplifikatív módon helyezi el a törvényben.

A magyar Btk. tényállásai közül több is szóba jöhet, ha valaki szélsőségesen erőszakos tartalmakat tesz közzé online, ezek többnyire a felhasználók személyiségi jogainak, illetve emberi méltóságának megsértéséhez kapcsolódnak. Személyes adattal való visszaélést valósít meg a tartalom közlője, amennyiben egy kép vagy videó feltöltésével a szereplőknek jelentős érdeksérelmet okoz, illetve amennyiben a tartalmat haszonszerzési céllal hozza nyilvánosságra.[632] A kiszolgáltatott személy megalázásának tényállása jöhet szóba, amennyiben a tartalom készítője maga veszi rá a felvétel szereplőjét arra, hogy magát megalázó magatartást tanúsítson.[633] Az egyéb emberi méltóságot sértő bűncselekmények, így a rágalmazás,[634] a becsületsértés,[635] illetve a kegyeletsértés[636] akkor állapíthatók meg, ha a felvételeket olyan tényállításoknak

630 Ekertv. 15/F. § (4).
631 Ekertv. 15/F. § (4).
632 Btk. 219. §.
633 Btk. 225. §.
634 Btk. 226. §.
635 Btk. 227. §.
636 Btk. 228. §.

vagy véleményközléseknek minősítjük, amelyek alkalmasak a szereplők jó hírnevének, illetve becsületének csorbítására. A szélsőséges erőszakot ábrázoló tartalmak az emberi méltóságot minden esetben semmibe veszik, a becsület csorbítására alkalmas jellegük azonban igényel némi magyarázatot. Koltay András mutat rá arra, hogy a magyar büntetőjogi jogalkalmazási gyakorlat a méltóságot a becsület részének tekinti, összemosva az egyes fogalmakat és tágabb értelmezést adva a büntetőjogi becsületsértés fogalmának.[637] A „normális" emberi reakció egy-egy ilyen felvétel alapján a sajnálat, elkeseredés, illetve az együttérzés az áldozattal, illetve annak családjával, akiknek a társadalmi megítélése nem csorbul, méltóságuk ellenben sérül. A 1194/2005. számú büntető elvi határozatban a Legfelsőbb Bíróság rámutatott arra, hogy a becsületen büntetőjogi értelemben az emberi méltóságot is érteni kell, és kegyeletsértésnek minősítette az olyan fényképek napilapban történő közzétételét, amelyek egyedileg azonosítható halottat boncolás után, szánalmat keltő testi állapotban ábrázolnak. Tehát

> „aki olyan megalázó képfelvételt tesz közzé, amelyen az elhunyt holtteste elhanyagolt környezetben, felmosóvödör, vérgyanús felmosórongy mellett álló csupasz fémasztalon fekszik, és a felvétel őt boncolás utáni állapotában, mellkasán végighúzódó, összevarrt boncolási sebbel és más boncolás ejtette sebekkel ábrázolja, olyan durván sérti az emberi méltóságot, és a hozzátartozók kegyeleti érzését, ami büntetőjogi felelősségre vonásra ad alapot".

Mutatis mutandis egy felvétel durván erőszakos jellege, szereplőinek kiszolgáltatott állapotban való ábrázolása élő emberek esetében is alkalmas a becsület csorbítására.

Az Egyesült Államokban szintén van példa a szélsőségesen erőszakos tartalmak bizonyos fajtáinak a kriminalizálására. Az Egyesült Államok jogrendszere széles körben védi a véleménynyilvánítás szabadságát, ez a védelem a legtöbb esetben kiterjed a szélsőségesen erőszakos tartalmakra is. Az obszcenitás és az állatkínzás kapcsolatával is több esetben foglalkoztak az amerikai bíróságok. A United States v. Stevens ügyben[638] a Legfelsőbb Bíróság alkotmányellenesnek ítélte azt a jogszabályt, amely általános jelleggel tiltotta az állatkínzást bemutató felvételek kereskedelmi célú készítését, birtoklását, továbbá adásvételét. Az ilyen felvételek egy alcsoportját, az állatok eltaposását, összenyomását fetisizáló felvételeket (úgynevezett *animal crush video*) tiltó jogszabály[639] azonban a United States v. Richards ügyben kiállta az alkotmá-

637 Koltay 2012: 41.
638 United States v. Stevens, 559 U.S. 460 (2010).
639 H.R.5566 – Animal Crush Video Prohibition Act of 2010.

nyossági próbát,[640] mivel az ilyen felvételek obszcén jellegűnek minősülnek, ekként korlátozhatók. Az ítélet középpontjában az a megállapítás állt, hogy az állatkínzást ábrázoló videóknak ez a fajtája fetisizálja az állatok elleni erőszakot, ezért kizárólag a szexuális érdeklődés kielégítésére irányul *(appeals to the prurient interest)*. Catherine A. MacKinnon kiemeli, hogy az emberek megölését ábrázoló felvételek esetében viszont nem érvényesülnek hasonló szabályok.[641] Musa K. Farmand a Richards-ügy analógiájára az első alkotmánykiegészítéssel összeegyeztethetőnek tartja a gyilkosságot fetisizáló videók (úgynevezett *snuff film*) szövetségi szintű kriminalizálását,[642] hiszen azok az emberölést ábrázoló felvételek, amelyek nem politikai véleménynyilvánítással vagy közérdekű problémával függenek össze, igen gyakran szexuális devianciák kielégítése miatt kerültek fel a világhálóra.

A szélsőségesen erőszakos tartalmak az egyes platformok felhasználási feltételeiben

A platformszolgáltatók felhasználási feltételei jellemző módon jóval részletesebben szabályozzák a felhasználói magatartásokat, mint a jogszabályok, ezért néhány platform szabályainak vizsgálata segítheti annak megállapítását, hogy – az uniós és a magyar szabályokon túl – mely tartalmak minősülnek különösen ártalmasnak.

A Facebook és a YouTube tiltják az öngyilkosságot és önsanyargatást[643] népszerűsítő, ösztönző vagy azok elkövetéséhez útmutatást adó tartalmak közzétételét. Az öngyilkosság sem a nemzetközi, sem a magyar jog szerint nem bűncselekmény, ám az élet elleni cselekmények többnyire jellegüknél fogva erőszakosak. Amennyiben valaki úgy dönt, hogy saját maga teszi közzé öngyilkosságát (például élőben közvetíti azt egy közösségi oldalon), személyiségi jogsértést értelemszerűen nem valósít meg, hiszen magának okoz sérelmet. A platformok tiltják a mások szenvedését, megalázását dicsőítő tartalmak közzétételét és az erőszak olyan szélsőséges megnyilvánulási formáit ábrázoló tartalmakat, mint a csonkítás, kínzás, gyilkosság, kivégzés, sebesült vagy halott embereket ábrázoló felvételek közzététele, valamint az állatok megsebesítését, kínzását, életének kioltását ábrázoló felvételek, amennyiben

640 United States v. Richards, 755 F.3d 269 5th Circuit (2014).

641 MacKinnon 2004.

642 Farmand 2016: 1919.

643 Önsanyargatás, amikor a felhasználó saját magának okoz testi sérülést, vagy öncsonkítást, táplálkozási zavarokat mutat be.

azokat nem a megfelelő kontextusban mutatják be. A nyílt erőszakot tartalmazó felvételek és a felnőtt tartalmak megengedettek, amennyiben a felhasználó azokat érzékeny tartalomként kategorizálja, és úgy helyezi el, hogy azt csak annak legyen lehetősége megtekinteni, aki kíváncsi rá (profilképben, fejlécképben elhelyezni ilyen tartalmakat tehát tilos). Tilos továbbá az olyan szélsőséges tartalmak közzététele, amelyek szexuális erőszakot, illetve indokolatlan brutalitást *(gratuitous gore)* ábrázolnak, mivel az ilyen felvételek egyrészt elfogadottá teszik a szélsőségesen erőszakos magatartásokat és a szexuális devianciákat, másrészt hátrányosan befolyásolják az egyének általános közérzetét.

Sok platform, például a Facebook és a YouTube eleve szigorúan korlátozza a meztelenséget és a szexualitást ábrázoló tartalmak közzétételét. A szexuális tartalmak erőszakosabb formáit azonban még megengedőbb szolgáltatók is korlátozzák, így például a X-en (Twitter) nem lehet közzétenni szexuális erőszakot, szexuális bántalmazást bemutató tartalmakat, sem pedig olyan tartalmakat, amelyek az erőszakot (például fizikai sérülések okozását) szexualizálják.

Az erőszakos tartalmak közzététele és a közérdek

A Facebook már 2013-ban is csak ideiglenesen volt hajlandó eltávolítani azt a felvételt, amely egy mexikói nő lefejezését ábrázolta,[644] a szolgáltató közösségi alapelvei szerint a szélsőségesen erőszakos tartalmak feltöltésére korhatárossá tétel és figyelmeztetés elhelyezése mellett továbbra is van lehetőség.[645] A Facebook hasonlóan más szolgáltatókhoz, a moderálás során figyelembe veszi a kontextust, amely faktor az eltávolításról való döntés meghozatala során gyakran nagyobb súllyal esik latba, mint az, hogy az adott tartalom ténylegesen mit ábrázol. A platform szabályzata szerint például a csonkítást, belső szerveket, emberek felgyújtását, kannibalizmusról szóló felvételeket közzé lehet tenni, amennyiben azok egészségügyi jellegűek, vagy politikai véleménynyilvánításnak (például az önmagát tiltakozásképp felgyújtó buddhista szerzetes fényképe[646]) minősíthetők. Az állatok elpusztítását, pusztulását bemutató felvételek szintén megengedettek, amennyiben azok vadon élő állatok egymás közötti harcát

644 Clark 2013.
645 Meta Transparency Center 2023b.
646 Worth 2011.

mutatják be (például természetfilmek), illetve vadászati, élelmiszer-előkészítési vagy -feldolgozási kontextusban tartalmaznak ilyen képsorokat. Az X (Twitter) felhasználási feltételei[647] azt rögzítik, hogy a szolgáltató igyekszik tiszteletben tartani, hogy egyes emberek azt akarják megmutatni, hogy mi történik a világban, ami gyakran érzékeny témákat ábrázoló erőszakos, felnőtt felhasználóknak szóló tartalmak közzétételével jár, ugyanakkor elismeri, hogy vannak emberek, akik el akarják kerülni, hogy ilyen tartalmakkal találkozzanak. A véleménynyilvánítás szabadsága, főként a közügyekben, a platformok felfogása szerint megelőzi a felhasználók nyugalmához fűződő érdeket és a szereplők emberi méltósága megőrzésének érdekét.

Egyes felvételek annak ellenére, hogy szélsőséges erőszakot tartalmaznak, lehetnek társadalmilag értékes közlések, amennyiben közérdeklődésre számot tartó, az egész társadalmat vagy annak egy rétegét érintő problémákra hívják fel a figyelmet. Az Egyesült Államokban 2020 májusában látott napvilágot egy felvétel a közösségi médiában, amely egy afroamerikai férfi, George Floyd ellen foganatosított rendőri intézkedést mutatott be.[648] Az intézkedés alá vont hiába jelezte a torkán térdeplő rendőrnek több alkalommal, hogy nem kap levegőt, a rendőrök ezzel nem törődtek, az áldozat pedig később, a kórházba szállítás során elhunyt. A feltöltött videó hamar virálissá vált, és országszerte zavargásokat váltott ki az Egyesült Államokban, a közösségi-média-platformok pedig felkavaró jellege ellenére sem moderálták azt, mivel olyan tartalomról van szó, amely rávilágít a rasszizmussal párosuló rendőri brutalitásra, és erősíti a rendőrség elszámoltathatóságát.[649]

Vannak olyan videómegosztó platformok, amelyek szolgáltatói úgy tekintenek magukra, mint az állampolgárok általi tudósítások platformjai, amelyek kendőzetlenül feltárják az igazságot azzal, hogy vágatlanul, kitakarás nélkül mutatnak be gyomorforgató kivégzéseket, baleseteket, gyilkosságokat. Ilyen például a LiveLeak, amelynek a jelmondata „a média újradefiniálása", és amely elsőként tette közzé a Saddam Hussein kivégzését[650] tartalmazó felvételt. A szolgáltató álláspontja szerint az információhoz jutás szabadságához az is hozzátartozik, hogy a felhasználók elől ne legyen elrejtve a „véres valóság".

[647] X Help Center 2023c.
[648] Burch–Eligon 2020.
[649] Burch–Eligon 2020.
[650] Cook 2014.

Az internet keselyűi

Az internet számtalan olyan tartalomnak is helyet ad, amelyeknek nincsen a társadalom szempontjából jelentőségük, céljuk csupán a meghökkentés, indulatkeltés, szexuális perverziók kielégítése. A szélsőségesen erőszakos, de a közbeszéd szempontjából értékkel nem bíró tartalmak terjedése az interneten nem a 21. század egyik új devianciája, az első sokkoldalak, a *Rotten.com* és az *Ogrish* az 1990-es években indultak. Az ilyen portálokon fellelhető tartalmak terjesztéséhez pusztán új felületet szolgáltatott a közösségi média, amelyen mindenki megoszthatja azokat a borzalmakat, amelyekkel szembesül. Az ilyen tartalmak manapság viszonylag sok embert elérnek, egy 2018-ban megjelent cikk felhívta arra a figyelmet, hogy a fiatalok körében népszerű közösségi fórumnak, a Redditnek a *Watch People Die* elnevezésű szekciója több mint 425 ezer feliratkozóval rendelkezett, mielőtt a szolgáltató végül eltávolította azt.[651] A LiveLeak nevű videómegosztó havonta 15-20 millió egyedi látogatót számlál, ami azt mutatja, hogy sok embernek van igénye ilyen jellegű tartalmakra.[652] Gyakran fordul elő, hogy nem könnyű elhatárolni egymástól a valódi hírértékkel rendelkező információkat azoktól, amelyek pusztán hatásvadászatból, meghökkentésből kerülnek fel a világhálóra. A közösségi média alapjaiban alakította át a háborúkról szóló tudósításokat is, hiszen az okoseszközök elterjedése óta már nemcsak a professzionális hírmédia képes tudósítani a frontvonalról, hanem maguk az események résztvevői, a katonák is.[653] Ezek a felvételek azonban sokszor nem a háború eseményeiről történő tényszerű tájékoztatást kívánnak nyújtani, hanem azokba a történésekbe nyújtanak betekintést, amelyek nem – vagy jelentős finomítást követően – kerülnek be a hírekbe: bemutathatják a háború áldozatait, a katonai táborokban fogva tartottak körülményeit, de akár a fogvatartottakkal szemben alkalmazott embertelen, megalázó bánásmódot is szemléltethetik. Noel Whitty az ilyen felvételek létjogosultsága mellett érvelve arról ír, hogy azok alkalmasak lehetnek arra, hogy felhívják a figyelmet a frontvonalon történő emberi jogsértésekre, ezáltal heves társadalmi reakciót váltsanak ki.[654] Példaként egy iraki civil, Baha Mousa esetét említi, aki egy brit fogolytáborban halt meg 2003-ban. A fogva tartás során készült felvételek felkerültek az internetre, a negatív társadalmi és politikai reakció pedig médiafigyelemmel kísért vizsgálatot eredményezett

651 Dahl 2018.
652 Herrman 2019.
653 Andén-Papadopoulos 2009: 921.
654 Whitty 2010: 689.

a fogolytáborokban lévő körülményekkel összefüggésben.[655] Ugyan Whitty szerint ezek a felvételek elősegítik az emberi jogok megsértésével kapcsolatos esetek napvilágra kerülését és az elkövetők felelősségre vonását, más álláspontok, köztük Stanley Cohen álláspontja szerint éppen ellenkező hatást is elérhetnek: érzéketlenné teszik a társadalmat, és elősegítik az olyan stratégiák kidolgozását, amelyek az emberi jogok megsértésének tagadását könnyítik meg.[656] Sok háborúban készült felvétel pedig még csak távolról sem azzal a céllal kerül fel az internetre, hogy felhívja a társadalom figyelmét az emberi jogok megsértésére. 2005-ben a *nowthatsfuckedup.com* nevű weboldal esete váltott ki nagy felháborodást: a weboldal megjelentette az amerikai katonák iraki háborúban készített felvételei közül azokat is, amelyek holttesteket, csonkolt végtagokat ábrázoltak, gyakran háborús trófeaként vagy szexualizált kontextusban bemutatva azokat.[657] A weboldalt az Egyesült Államokban a tartalom obszcén jellege miatt sikerült eltávolítani, azóta azonban más néven, de újra működik.

Online terror – az internet terrorista célú használatának szankcionálása

Terror, főnév: „Kegyetlen, kíméletlen, erőszakos módszer(ek), eljárás, bánásmód, megfélemlítés, főként hatalmi, politikai céllal, egyénekkel, tömegekkel v. társadalmi osztályokkal szemben."[658] A terrorizmus mint kifejezés és jelenség nem a 21. század terméke, sőt az internet terrorista célú használatára használt „kiberterrorizmus" kifejezés első megjelenése is 1979-re tehető.[659] A modern kori terrorizmus a 2001. szeptember 11-i Word Trade Center elleni terrortámadást követően vált mindennapjaink részévé, a terrorcselekmények, illetve a terrorizmusról, terrorszervezetekről szóló tudósítások azóta sem szűnnek. A szélsőséges csoportok ugyanúgy, ahogyan más szervezett csoportok, hamar megtanulták kiaknázni az internet előnyeit és céljaikra hasznosítani a világhálót. Ez jogalkalmazási szempontból hatalmas kihívást jelent, hiszen a nemzetközi jogban még a terrorizmusnak sincsen egzakt módon meghatározott fogalma, nincs tehát közös fogalmi alap, amely mentén

655 Whitty 2010: 689.
656 Cohen 2004.
657 Kushner 2005.
658 Pusztai 2008.
659 Oleksiewicz 2016: 136.

az online terrorizmus megítélhető és üldözhető lenne. Sami Zeidan arra hívja fel a figyelmet, hogy a terrorizmus szó politikai értéke jelenleg megelőzi a jogit, így az egyes érdekcsoportok kommunikációja során könnyen értelmezhető fals módon.[660] Jason Burke osztja azt a nézetet, hogy a terrorizmus meghatározása többnyire szubjektív, kiemeli viszont, hogy annak minden esetben eleme a komoly erőszak elkövetése vagy annak szándéka, illetve az, hogy az erőszak alkalmazása mindig valamilyen cél megvalósítása, ügy előrevitele (politikai, ideológiai, vallási) érdekében történik.[661] A terrorizmus fogalmában rejlő bizonytalanság azt eredményezi, hogy a kibertérben megvalósuló cselekmények minősítése is ingatag lábakon áll. Amikor az internet terrorista célú használatáról esik szó, sok magatartásforma szóba jöhet. Az internet terrorista célú használatának minősül a kiberterrorizmus, de a terrorista uszítás is. Az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala (a továbbiakban: UNODC) az internet terrorista célú használatának hat esetét különbözteti meg:[662]

1. propaganda, amely magában foglalja a toborzást, radikalizálást és a terrorizmusra uszítást;
2. finanszírozás, például adománygyűjtés terrorszervezetek támogatására;
3. kiképzés;
4. tervezés, különösen titkosított kommunikációs csatornákon nyílt forrású információk használatával;
5. végrehajtás;
6. kibertámadások, kiberterrorizmus.

Az internet és a terrorizmus kapcsolatát több metaforával próbálták leírni. Egyesek szerint virtuális kiképzőtábor, mások szerint olyan forrás, amely nyitva áll az önmagukat radikalizáló szimpatizánsok számára,[663] lehet ugyanakkor elkövetési eszköz (például kritikus infrastruktúrák elleni botnettámadások esetén), de lehet olyan közvetítő közeg, amely elősegíti a polgárok nyugalmának és biztonságérzetének megzavarását. A fejezetben az internet terrorista célú használatának büntetőjog szempontjából is releváns magatartásait veszem számba.

660 Zeidan 2004: 491.
661 Burke 2003: 22.
662 UNODC 2012: 3.
663 Stenersen 2018: 215–216.

Kiberterrorizmus

Általában véve kiberterrorizmuson az interneten keresztül elkövetett, terrorcselekménynek minősíthető cselekményeket értjük. Gillespie szerint[664] az információs rendszerek elleni erőszak, azok működésének megzavarása vagy az abba történő beavatkozás minősíthető kiberterrorizmusnak. Ugyanakkor Dornfeld László gondolataira reflektálva indokolt kiemelni, hogy nincsen egységes szakirodalmi álláspont a tekintetben, hogy hol húzódik a határ az internetes polgári engedetlenség és a terrorizmus között.[665]

Mint a kiberbűncselekmények esetén általában, a fogalmi lehatárolást az is nehezíti, hogy a szakirodalomban több egymással azonos értelemben megjelenő fogalommal találkozhatunk. A kiberterrorizmus fogalmának vizsgálata során így olyan kifejezésekbe is belefuthatunk, mint a hacktivizmus vagy a kiberhadviselés. Noha ezeknek a cselekményeknek egyes elemei megjelennek a kiberterrorizmusban is, nem összekeverendő jelenségekről beszélhetünk, markánsan különbözik ugyanis a célzat és az elkövetői kör is.

A hacktivizmus kifejezés a hackelés és az aktivizmus szavak összevonásából keletkezett, arra utal, amikor személyek vagy csoportok politikai indíttatásból törnek fel rendszereket, alakítanak át weboldalakat *(defacing)*. Ezek a cselekmények, még akkor is, ha nemes cél motiválja őket, nem jogszerűek, eszköztáruk többnyire az információs rendszer vagy adat megsértéséből tevődik össze. Az egyik leghíresebb magyar példája az a 2012-es eset, amikor az Anonymous nevű csoport az Alkotmánybíróság honlapján átírta az Alaptörvény szövegét, és – egyebek mellett – kiegészítette azzal, hogy „az informatikában dolgozók 2^5, azaz 32 évesen a fizetésük 150%-val nyugdíjba mehetnek, továbbá nyugellátás mellett adómentességet élvezzenek".[666]

A kiberaktivizmus vagy más néven online aktivizmus kizárólag jogszerű, a véleménynyilvánítás normális rendjébe illeszkedő cselekményeket takar, amelyek az új technológiákat kommunikációs csatornaként alkalmazva törekszenek a közvélemény befolyásolására.

A kiberhadviselés alatt elsősorban az államok, államokhoz kapcsolható militáns szervezetek katonai jellegű támadásait értjük, amelyek célja politikai, illetve katonai erőfölény elérése. Egyes szerzők, például Berki Gábor szerint kiberhadviselésről csak abban az esetben beszélhetünk, ha ismert a támadó állam kiléte.[667]

[664] Gillespie 2016: 107.
[665] Dornfeld 2019: 47.
[666] Az Anonymous átírta az alaptörvényt 2012.
[667] Berki 2016: 260–264.

Az ENSZ korábban már hivatkozott jelentése a kiberterrorizmus kifejezés helyett a kibertámadás fogalmat határozza meg. Kibertámadás alatt a számítógépes hálózatoknak a más hálózatok elleni támadások végrehajtására való szándékos felhasználását értjük.[668] Ennél szűkebb fogalom a terrorista céllal végrehajtott kibertámadások kategóriája, mivel az ilyen jellegű támadások esetében az elkövető szervezetnek vagy személynek konkrét célja van.

Terrorista propaganda és terrorizmusra uszítás az interneten

Ezekiel Rediker szerint a terrorizmusra uszítás megítélésének az egyik alapkérdése az, hogy meddig terjed a véleménynyilvánítás szabadsága, és hol kezdődik a terrorizmusra uszítás.[669] A kérdés vizsgálata amerikai–európai összehasonlításban is érdekes, főképp, mivel az Egyesült Államok erőteljesebb védelmet biztosít a véleménynyilvánítás szabadsága számára, mint az európai országok. Annak érdekében, hogy vizsgálat tárgyává tehessük, hogy mikor korlátozható – akár a büntetőjog eszközeivel – a terrorizmusra uszítás, elsősorban azt kell tisztázni, hogy mit értünk pontosan a terrorizmushoz kapcsolódó egyes fogalmak – mint az uszítás, a radikalizálás és a propaganda – alatt.

Az ENSZ jelentése[670] a terrorizmusra uszítást a terrorista propaganda egyik fajtájának tekinti, és elhatárolja azt másfajta magatartásoktól. A jelentés felhívja arra a figyelmet, hogy a propaganda maga nem általánosságban kriminalizálandó, hiszen a támogató vélemények kifejtése, a hírek megosztása, az eszmékkel való szimpátia kinyilvánítása olyan megnyilvánulások, amelyek a demokratikus társadalomban az esetek túlnyomó részében védelmet élveznek.

A jelentés a propaganda körében több magatartást különböztet meg egymástól, ilyen a tájékoztatás, a radikalizálás, a toborzás, valamint a későbbi uszítás. Ilyen a toborzás, amelyhez az internet remek lehetőséget kínál: könnyen és gyorsan lehet elérni a szimpatizánsokat, jelszóval védett felületeken vagy privát chatszobákban. A terrorcselekmények, sikertelen tervek és az elmúlt években zajlott bírósági tárgyalások tapasztalatait összegezve Anja Dalgaard-Nielsen arra figyelmeztet, hogy azok az európai fiatalok, akik nem töltöttek hosszabb időt Európán kívül, különösen jól radikalizálhatók.[671] Az Európai Bizottság radikalizációval foglalkozó szakértői

668 UNODC 2012: ii.
669 Rediker 2015: 322.
670 UNODC 2012: ii.
671 Dalgaard-Nielsen 2010: 798–799.

csoportjának a jelentése arra is rámutatott,[672] hogy a célcsoportot gyakran azok a személyek képezik, akik igazságtalanságot, kirekesztettséget vagy megaláztatást tapasztaltak, így könnyebben befolyásolhatók. Az ilyen személyek gyakran használják a világhálót identitáskeresésre és kapcsolatépítésre, ami a terrorista csoportok számára igen előnyös. A beszervezés előzménye az ENSZ-jelentés szerint a radikalizálás,[673] azaz az eszmék elfogadtatása, az azokkal való azonosulás, a célszemélyek meggyőzése.

Nehéz ugyanakkor meghúzni a határvonalat a terrorcselekmény elkövetésére uszítás és a propaganda más formái között. Az internetes kommunikáció jelentőségére hívja fel a figyelmet Dorothy E. Denning, aki szerint ezek a felületek nemcsak a toborzásra és az érdeklődők tájékoztatására alkalmasak, hanem a későbbi fizikai világban megvalósuló cselekedetek megtervezésére is.[674] Ben Saul szerint a propaganda az erőszakos cselekmények szolgálólánya, amely igazolja és naturalizálja az elkövetett cselekményeket, felpuhítja az emberek pszichéjét, és érzéketlenné teszi őket a terrorizmus brutális hatásaival szemben.[675] Ben Saul értelmezésében a propaganda valójában fokozatosan készíti elő tényleges terrorcselekmények elkövetését, azaz valójában elnyújtott módon uszít. A propaganda e formája azonban még nem foglalja magában a sérülés bekövetkezésének közvetlen veszélyét, lassan ágyaz meg a sértési szándék kialakulásának, hatása pedig nagyban függ a célcsoport befogadókészségétől, éppen ezért nem tartozik a korlátozandó közlések közé.

A 2000-es évek közepére megszaporodtak az EU-ban az olyan kezdeményezések és jogi aktusok, amelyek bűncselekményekkel, köztük a terrorcselekmények elleni küzdelemmel foglalkoztak,[676] kritikusaik szerint ezek azonban nem teremtettek átfogó és egységes megközelítést.[677] A 2002/475/IB kerethatározat a kriminalizálandó cselekmények felsorolásával határozta meg a terrorizmus fogalmát, és úgy rendelkezett, hogy terrorista cselekményeknek minősülnek azok a kerethatározatban megnevezett cselekmények, amelyek az elkövetés módja vagy összefüggéseik folytán egy államot vagy nemzetközi szervezetet komolyan károsíthatnak, amennyiben a következő célok valamelyikével követik el:

672 Alonso 2008.
673 UNODC 2012: 11.
674 Denning 2010: 194–213.
675 Saul 2005: 868.
676 Rediker 2015: 335.
677 Rediker 2015: 336.

- a lakosság megfélemlítése, vagy
- állami szerv vagy nemzetközi szervezet kényszerítése, hogy valamely intézkedést megtegyen vagy ne tegyen meg, vagy
- egy állam vagy nemzetközi szervezet alapvető politikai, alkotmányos, gazdasági vagy társadalmi rendjének súlyos megzavarása vagy lerombolása.[678]

A kerethatározatot 2008-ban módosította a 2008/919/IB tanácsi kerethatározat, amely kiegészítette a terrorista tevékenységgel összefüggő bűncselekmények listáját – egyebek mellett – a terrorista bűncselekmény elkövetésére való nyilvános izgatással, terroristák toborzásával, valamint a terroristák kiképzésével.[679] A kerethatározat terrorista bűncselekmény elkövetésére való nyilvános izgatás alatt az olyan magatartásokat értette, amelyek valamely üzenet terjesztésében vagy egyéb módon a nyilvánosság számára hozzáférhetővé tételében nyilvánultak meg, amennyiben annak közlése azzal a szándékkal történik, hogy a kerethatározatban felsorolt bűncselekmények egyikének elkövetésére uszítson, ha ez a magatartás – akár a terrorista bűncselekmény közvetlen támogatásával, akár anélkül – annak veszélyével jár, hogy elkövethetnek egy vagy több ilyen bűncselekményt. Az uszítás fogalmát a kerethatározat nem fogalmazta meg, így arra sem derült fény, hogy a terrorista cselekmény elkövetésének veszélye esetében a veszélynek távolinak vagy közvetlennek kell lennie. A kerethatározatot 2017-ben váltotta fel a terrorizmus elleni küzdelemről szóló irányelv,[680] amely jelentősen módosított a terrorista bűncselekmény elkövetésére való nyilvános izgatás meghatározásán. Az irányelv 5. cikke már izgatás helyett uszításról rendelkezik. Terrorista bűncselekmény elkövetésére való nyilvános uszítás tehát valamely üzenetnek azzal a szándékkal való terjesztése vagy egyéb módon a nyilvánosság számára – bármilyen eszköz révén akár online, akár offline módon történő – hozzáférhetővé tétele, hogy az irányelvben meghatározott „cselekmények valamelyikének elkövetésére felbujtson, amennyiben ez a magatartás közvetlenül vagy közvetve – például a terrorista cselekmények dicsőítése révén – szorgalmazza terrorista bűncselekmények elkövetését, és ezáltal annak veszélyével jár, hogy sor kerülhet egy vagy több ilyen bűncselekmény elkövetésére”.[681] Az irányelv immár kimondottan nevesíti az online elkövetést mint

678 1. cikk.

679 3. cikk (2).

680 Az Európai Parlament és a Tanács (EU) 2017/541 irányelve a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról.

681 Az Európai Parlament és a Tanács (EU) 2017/541 irányelve a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról,

lehetséges elkövetési módot, több kifejezés meghatározásával azonban adós marad. Nem fogalmazza meg, hogy mi minősül a terrorista cselekmények dicsőítésének, sem pedig azt, hogy milyen távolinak kell lennie az elkövetés veszélyének, ezzel viszont lehetővé teszi, hogy ezekben a kérdésekben meglehetősen eltérő tagállami szabályok és értelmezések szülessenek.

Az ENSZ már hivatkozott jelentése az egyszerű propagandát az uszítástól két tulajdonság mentén határolja el. Az egyik a szándék: akkor minősülhet egy közlés uszításnak, ha az elkövető szándéka arra irányul, hogy valakik terrorista cselekmény elkövetésének előkészületét, annak kísérletét vagy magát a cselekményt valósítsák meg. További elhatárolási szempont, hogy az uszító közlés alapján a terrorcselekmény elkövetésének legalább a bizonyítható tervezési fázisig el kell jutnia.[682] A jelentés a francia jogot hozza példaként, amely szerint önmagában az, hogy valaki robbanóanyagok elkészítéséhez bocsát rendelkezésre instrukciókat, még nem minősül terrorizmusra uszításnak.

Mivel az uszítás elhatárolása a védendő közlésektől alapjogi kérdés, az EJEB ítélkezési gyakorlata iránytűként szolgálhat. Az EJEB több ügyben vizsgálta az uszítás és az erőszak lehetősége között fennálló kapcsolatot. A Leroy v. France ügyben[683] nem állapította meg az EJEE 10., véleménynyilvánítás szabadságát deklaráló cikkének sérelmét abban az esetben, amelyben egy újságírót egy francia bíróság ellentmondásos rajzoknak egy baszk újságban való közzétételéért ítélt el. A rajz a World Trade Center lerombolását ábrázolta, amelyhez a szerző azt a terrorcselekmény támogatásaként és dicsőítéseként értelmezhető megjegyzést fűzte, miszerint: „Mind álmodoztunk róla… a Hamasz megtette" (*We have all dreamt of it… Hamas did it*[684]). Az EJEB a közlést azért tartotta korlátozhatónak, mert abból egyértelműen kitűnt, hogy a közlő morálisan támogatja a terrorcselekmény elkövetőit, ráadásul a publikálás választott időpontja a terrortámadáshoz közel esett. A Sürek v. Turkey ügy[685] alapját az képezte, hogy egy török újság tulajdonosát felelősségre vonták két olyan olvasói levél közzététele miatt, amelyek erőteljesen kritizálták az ország délkeleti részében zajló katonai műveleteket. Az EJEB nem állapította meg a szólásszabadság megsértését, mert az ügy tárgyát képező olvasói levelek véres revansra buzdítottak azáltal, hogy felkavarták

5. cikk.

682 Az Európai Parlament és a Tanács (EU) 2017/541 irányelve a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról.

683 Leroy v. France, App. no. 36109/03 (2008).

684 A mondat a Sony híres reklámszlogenjének (We have all dreamt of it… Sony did it) eltorzítása.

685 Sürek v. Turkey (No. 1.), 1999-IV. 353, 355.

az olvasók érzelmeit, és megszilárdították a régebben beágyazódott előítéleteket, amelyek korábban is halálos kimenetelű erőszakhoz vezettek. A Ceylan v. Turkey ügyben[686] az EJEB egy szakszervezeti vezető által közzétett cikket vizsgált, amely a délkelet-törökországi régióban zajló katonai cselekményeket „állami terrorizmusnak", „tömeggyilkosságnak" és „véres mészárlásnak" nevezte, és a demokratikus erők reakcióját próbálta kiváltani. A Bíróság, elismervén a politikai jellegű beszéd fontosságát, úgy találta, hogy a cikk nem ösztönöz erőszakra, fegyveres ellenállásra vagy engedetlenségre, így a korlátozás sértette az Egyezmény 10. cikkét. A Karatas v. Turkey ügyben[687] a Bíróság a művészi kifejezések hatását vizsgálta, és megállapította, hogy a kis közönséget megcélzó költészetnek csak korlátozott hatása lehet a nemzetbiztonságra, abban az esetben is, ha egyes sorok erőszakos magatartásra hívnak fel, és agresszív természetűek. Ehhez hasonlóan az Incal v. Turkey ügyben az EJEB azt állapította meg, hogy egy pamflet terjesztésének tiltása ellentétes az Egyezmény 10. cikkével. Az előbbi esetekből az rajzolódik ki, hogy a Bíróság számos faktort számításba vesz, amikor egy-egy közlés uszító jellegét vizsgálja, így fontos tényező lehet a közlés formája (újságcikk – vers), az országban uralkodó politikai helyzet, a közlő szándéka, illetve az, hogy hány emberhez képes az üzenetét eljuttatni.

Az Egyesült Államok a szólásszabadság szélesebb körű védelme érdekében a gyűlöletbeszédnél használt nyilvánvaló és közvetlen veszély elvének alkalmazásával ítéli meg a terrorizmusra uszítást. A terrorszervezetekkel kapcsolatban Alexander Tsesis kifejti,[688] hogy önmagában olyan szervezethez tartozni, amely valamilyen változásért küzd, nem jogellenes akkor sem, ha ez demokráciaellenes intézmények támogatásával történik. A szervezet célja és tevékenysége azonban egyes szélsőséges esetekben megalapozhat jogellenességet. A Dennis v. United States ügyben[689] az amerikai Kommunista Párt vezetőit azért ítélték el, mert szándékosan és tudatosan támogatták az erőszakos hatalomátvétel megszervezését. Az ügyben a bíróság kimondta, hogy az államnak nem kötelessége megvárni, hogy puccsot kíséreljenek meg, előbb is felléphet az ilyen jellegű támadások ellen. A későbbiek folyamán a bíróság megkülönböztette egymástól a támogató fellépés *(advocacy)*, valamint az uszítás *(incitement)* magatartásait. A Brandenburg v. Ohio ügy[690] megállapítása szerint az erőszakos közlések is az első alkotmánykiegészítés által védettek, amennyiben nem uszító jellegűek, és nem

686 Ceylan v. Turkey, App. no. 23556/94.
687 Karatas v. Turkey, App. no. 23168/94.
688 Tsesis 2019: 663.
689 Dennis v. United States, 341 U.S. 494, 509, 515, 516 (1951).
690 Brandenburg v. Ohio, 395 U.S. 444, 447-49 (1969).

hordozzák magukban a fenyegetés beváltásának közvetlen veszélyét. Az uszítás tartalmának amerikai értelmezésével a gyűlöletbeszédről szóló fejezet szólt részletesen, az ott leírtak a terrorcselekmény elkövetésére való uszítás esetében is irányadók.

Az internetes közvetítő szolgáltatók és a terrorizmus

A magánszereplők a kulcstényezői a terrorizmus elleni küzdelemnek, hiszen mind az internetes infrastruktúra, mind a felhasználók által használt üzenetküldő, illetve közösségimédia-szolgáltatások piaci szereplők tulajdonában vannak.[691] A közösségimédia-felületeken közzétett tartalmak gyorsan elérhetnek nagy közönséget, a feltöltött tartalmak ráadásul könnyen és gyorsan tovább oszthatók. A brit R. v. Roshanara Choudhry ügy vádlottja például YouTube-videókon keresztül tanulta meg az erőszakos cselekmények elkövetésének módszereit. A terrorszervezetek a sajtóorgánumokat megszégyenítő formában és tartalommal vannak jelen az online térben, az ISIS több Twitter-fiókkal is rendelkezik,[692] de az al-Kaida vagy a Hezbollah is rendelkeznek online jelenléttel.[693]

A 2010-es években megszaporodtak a terrorista támadások az Európai Unióban. Ezt követően jött létre 2015-ben az EU Internet Forum az online terrorista tartalmakról, amely az EU belügyminisztereiből, az internet nagyobb piaci szereplőiből és más érdekeltekből álló csoport.[694] Az Európai Parlament 2018-ben közzétett ajánlásában az online platformokat sürgette, hogy legyenek proaktívabbak a felhasználóik terrorista tartalmaktól való védelme érdekében.[695]

Az Európai Bizottság 2018-ban ajánlást tett közzé az illegális online tartalmak kezeléséről,[696] amelyben néhány bekezdést a terrorista tartalmakkal kapcsolatos ajánlásoknak szentel. A Bizottság ajánlása felhívta arra a figyelmet, hogy a terrorizmus sajátosságai miatt a terrorcselekményeket bemutató, azokkal kapcsolatos online

691 UNODC 2012: 123.
692 Berger 2015.
693 Weimann 2015: 139.
694 European Commission 2019.
695 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről.
696 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről.

tartalmak sajátos kezelést igényelnek.[697] A Bizottság a tárhelyszolgáltatók szerepét tekinti a leghangsúlyosabbnak[698] a tartalmak terjesztésében, ezért ajánlásában rögzíti, hogy azoknak minden észszerű intézkedést meg kell tenniük annak érdekében, hogy ne tölthessenek fel terrorista tartalmakat. Az egyik ilyen észszerű intézkedés a Bizottság szerint a megfelelő hatóságokkal, különösen az Europollal való együttműködés,[699] amelynek keretében a szolgáltatóknak biztosítaniuk kellene, hogy az együttműködéssel érintett hatóságok kérésére eltávolítsák azokat a tartalmakat, amelyeket terrorista jellegűnek ítélnek meg. A Bizottság az ajánlásban arra is kitér, hogy az ilyen tartalmak jellemzően a közzétételüket követő egy órában képesek a legnagyobb károkat okozni,[700] éppen ezért az együttműködésben érintett hatóságoktól és az Europoltól érkező jelzéseket a szolgáltatóknak egy órán belül el kellene tudniuk intézni. Az ajánlás ezen a területen támogatja az automatizált tartalomszűrő eszközök alkalmazását is.[701]

Az ajánlás mentén hasonló követelményeket fogalmazott meg a terrorista cselekmények elleni fellépésről szóló 2021/784 rendelet, amely szintén egy órán belüli eltávolítási kötelezettségről rendelkezik. A platformszolgáltatókat a gyors eltávolításon kívül adatmegőrzési kötelezettség is terheli, így a nyomozás során eljáró szerveknek tájékoztatást kell adniuk a tartalmat feltöltő felhasználó forgalmazás közben keletkezett és szolgáltató által tárolt személyes adatairól.

Mind az ajánlás, mind a rendelet ambiciózus, több esetben azonban megvalósíthatatlan beavatkozást vár el a szolgáltatóktól. A terrorcselekménnyel összefüggésbe hozható tartalmak moderálása – főként *live streaming* esetén – nehezen szorítható egy óra alá, legfeljebb amennyiben a feltöltött tartalomra azonnal érkezik felhasználói panasz, és annak jogsértő jellege annyira egyértelmű, hogy a moderátor haladéktalanul el is távolítja. Az automatizált tartalomszűrő eszközök, ahogy azt a VII. részben is látni fogjuk, léteznek, de nem elég fejlettek ahhoz, hogy hézagmentes védelmet biztosítsanak. Nem szól az ajánlás egy lényeges kérdésről, az újbóli feltöltések megakadályozásáról, amelyre viszont már adottak a technikai lehetőségek. 2016-ban

697 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről (32).

698 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről (33).

699 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről (34).

700 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről (35).

701 A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről (36).

az EU Internet Forumon jelentették be egy olyan *hash*-adatbázis létrehozását,[702] amely a terrorista tartalmak eltávolítását véglegessé és visszafordíthatatlanná teheti azáltal, hogy a hash-kód azonossága (tartalmi egyezés) esetén nem engedi feltölteni újból ugyanazokat a felvételeket. A közösségi médiaszolgáltatók tehát összefogtak annak érdekében, hogy azok a terrorista felvételek, illetve toborzóvideók, amelyeket már valamelyikük egyértelműen azonosított és törölt, egyedi *hash*-azonosítót (egy digitális ujjlenyomatot) kapjanak, így újbóli feltöltésük esetén azonnal és mérlegelés nélkül eltávolíthatók legyenek.[703]

A YouTube az elmúlt években erőteljesen lépett fel a terrorista tartalmakkal szemben, és sikerült is visszaszorítania az ilyen jellegű tartalmakat.[704] A szolgáltató Közösségi Irányelveiben azonban nem található meg a terrorizmusra uszítás szófordulat. A terrorista cselekményekre való uszítást, a terror dicsőítését a platformszolgáltató külön nem szabályozza, ám ezekre a tartalmakra is irányadóak a gyűlöletkeltő[705] és a szélsőségesen erőszakos, megbotránkoztató tartalmakra vonatkozó szabályok.[706] A Facebook és az X (Twitter) közösségi alapelvei hasonló szabályozási megoldást választottak. Noha sok platform felhasználási feltételei rendelkeznek a tartalmak moderálásáról, előfordul, hogy egyes panaszokkal nem foglalkoznak a moderátorok, kiváltképp, amikor az amerikai jog szerint egyes közlések a véleménynyilvánítási jellegük miatt védettek. 2015-ben a Lakin v. Facebook ügyben[707] 20 ezer izraeli indított eljárást a Facebook ellen, mert hagyta, hogy palesztin terroristák erőszakos támadások elkövetésére uszítsanak a szolgáltatáson keresztül. A felperesek azzal érveltek, hogy a Facebooknak jogszabályi kötelezettsége lenne eltávolítani ezeket a tartalmakat, és kérték a bíróságot, hogy kötelezze a céget ennek megtételére. Eugene Volokh véleménycikkében[708] rámutatott az ügy kilátástalanságának két okára. Az egyik az Első Alkotmánykiegészítés, amely a véleménynyilvánítás szabadságát védi. A felperesek a kérelmüket az izraeli jogszabályokra hivatkozva terjesztették elő, amely szerint büntetendő a terrorizmus dicsőítése, a terrorszervezetek támogatására való felhívás, ez a szabály ellenben ellentétes az amerikai joggal, amely csak az uszítás kapcsán már kifejtett esetekben teszi lehetővé a véleménynyilvánítás szabadságának korlátozását.

[702] European Commission 2019.
[703] Facebook Newsroom 2016.
[704] Katz 2018.
[705] YouTube Súgó 2023d.
[706] YouTube Súgó 2023c.
[707] Lakin v. Facebook Inc., No. 12831/15 (N.Y. Sup. Ct. Oct. 26, 2015).
[708] Volokh 2015.

A másik ok, amely miatt az eljárás nem vezetett eredményre, az amerikai közvetítő szolgáltatók felelősségét kizáró jogszabály, a CDA volt, amely kimondja, hogy a tárhelyszolgáltató nem vonható felelősségre harmadik személy által közzétett tartalomért.

Az előbbiekben felsorolt platformok kifejezetten tiltják, hogy veszélyesnek minősített magánszemélyek és csoportok használják a szolgáltatásaikat. A Facebook közösségi alapelvei például veszélyesnek minősítik azokat a csoportokat, amelyeket erőszakszervezetek, terrorista csoportok, szervezett bűnözői csoportok hoznak létre.[709] A YouTube szintén tiltja az ilyen szervezetek működését, az általuk előállított tartalmak közzétételét, illetve az ilyen szervezetek dicsőítését, népszerűsítését, támogatását célzó tartalmakat.[710] A YouTube ugyanakkor vonakodott eltávolítani egyes terrorcselekményekkel összefüggésbe hozható tartalmakat. Egyes platformok moderációját jelenleg még könnyű kijátszani. A YouTube esetében, ha a feltöltő a nem listázott tartalmak között helyezi el a videóját, az nem jelenik meg mások találati listáiban, csak a link birtokában lehet ahhoz hozzáférni, vagyis más szolgáltatásokon keresztül kimondottan a célközönséghez juttatható el. Hasonló módszer, amikor a feltöltött videó valójában ártalmatlan: képeket és/vagy zenét tartalmaz a videó leírásában, azonban olyan linkek találhatók benne, amelyek továbbirányítják a felhasználót más platformokra, a már tényleges, terroristák által előállított tartalmakra.[711] Az ajánlások és a jó gyakorlatok ellenére az is előfordul, hogy egyes tartalmak átjutnak a szolgáltatók szűrőjén. A christchurchi terrortámadást élőben követhették a felhasználók a Facebookon, a videót pedig hamar tömegek osztották meg, megnehezítve ezzel az eltávolítást. A támadás után indult el a Christchurch Call nevű kezdeményezés, amelynek célja a terrorista és az erőszakos extrémista tartalmak visszaszorítása. A felhívást a világ számos országa és a legnagyobb szolgáltatók is támogatják. A felhívásban a korábban már részletesen tárgyalt ajánlásokhoz hasonló vállalások szerepelnek: a terrorista tartalmak feltöltésének megakadályozása, a panaszkezelési, értesítési-eltávolítási eljárások működtetése. Újdonság viszont, hogy megjelenik az élő közvetítésekkel kapcsolatos kockázatok kezelésének igénye, valamint annak lehetővé tétele, hogy az élő közvetítések is tartalmi felülvizsgálat alá vonhatók legyenek. Ez jelenleg nem működő konstrukció, mivel az élő közvetítések folyamatos figyelemmel kísérésének emberierőforrás-igénye kielégíthetetlen. Ha történik is moderálás az élő közvetítések esetében, a moderátornak is kell idő ahhoz, hogy feldolgozza, mit lát, ami tényleges

[709] Meta Transparency Center 2023d.
[710] YouTube Súgó 2023b.
[711] Katz 2017.

terrortámadás esetén elfogadhatatlan késlekedést jelent. Az átgondolatlan, gyors moderálás ellenben magában hordozza azt a veszélyt, hogy olyan – akár erőszakos – tudósítások nem jutnak el a nyilvánossághoz, amelyeknek hírértéke, társadalmi relevanciája van. Mivel a platformoknak jelenleg nem állnak rendelkezésére olyan eszközök, amelyekkel az élő közvetítéseket hatékonyan moderálhatnák, inkább azt a megoldást választották, hogy átfogalmazták az élő közvetítésekkel kapcsolatos szabályzataikat, és szigorítottak az élő bejelentkezések lehetőségén. Néhány felhasználót tehát a platformok elzárnak attól a lehetőségtől, hogy valós időben osszanak meg bizonyos tartalmakat, tudósítsanak bizonyos eseményekről.

Vákát oldal

VI. Az informatikai bűncselekmények nyomozásának egyes kérdései

Egy olyan világban, amelyben a technológia annyira mélyen áthatja életünket, hogy napjaink egy részét virtuális környezetben töltjük el, mindenki óhatatlanul digitális nyomok tömkelegét hagyja maga után. Az előző fejezetekben szó esett arról, hogy milyen jogsértéseket lehet elkövetni az online térben, valamint arról, hogy az anyagi büntetőjog milyen válaszokat ad hazánkban, illetve a nemzetközi színtéren ezekre a jelenségekre. Szó esett arról is, hogy az online működő közvetítő szolgáltatók hogyan igyekeznek megakadályozni a jogsértéseket, illetve csökkenteni az azok által okozott kárt, saját rendelkezéseikkel kiegészítve a büntetőjogi rendelkezéseket. Mindez azonban nem sokat ér, ha az interneten rejtőzködő elkövetők kilétét nem sikerül felderíteni, és nem vonják őket felelősségre.

Az eredményes nyomozás, a büntetőeljárások lefolytatása, valamint a jogsértő tartalmak eltávolítása, a jogsértések megszüntetése legalább olyan fontos, mint a társadalomra és az egyénekre veszélyes online magatartások átlátható rendszerben történő kriminalizálása. Az internet, azon belül az egyes szolgáltatások elképzelhetetlen mennyiségű felhasználói adatot rögzítenek és tárolnak, a hozzáértők elvben tehát ki tudják nyerni a számukra szükséges adatokat. A kötet jelen szerkezeti egysége azzal foglalkozik, hogy mi minősül az online térben elkövetett bűncselekmények bizonyítására alkalmas eszköznek, valamint azzal, hogy miként van lehetőségük a nyomozó hatóságoknak hozzáférni ezekhez az eszközökhöz. A korábban leírtak fényében vélhetően nem árulunk el nagy titkot azzal, hogy ezen a területen is kiemelt szerepe van azoknak a magánkézben lévő vállalkozásoknak, amelyeknél az adatok keletkeznek.

A szolgáltatók és a nyomozó hatóságok közötti viszony azonban – ahogyan azt látni fogjuk – egyelőre bonyolult, és rendezésre vár. A kötet jelen része az informatikai bűncselekmények nyomozásának azon kihívásait igyekszik feltárni, amelyek a nyomozó hatóság tagjainál felmerülhetnek, a következő fejezet pedig ezeket a problémás kérdéseket a nyomozásokban szerepet játszó, közreműködő közvetítő szolgáltatók tevékenységén keresztül mutatja be.

A digitális bizonyíték fogalma és forrásai

A 21. században nem számít kirívónak az amerikai Robert Durall ügye,[712] aki – a böngészője keresési előzményei alapján – olyan kifejezésekre keresett rá, mint „fojtogatás", „emberölés", „házastárs + gyilkosság", „altató + tabletták + halál" *(suffocation, homicide, spouse + kill, sleep + pills + death),* mielőtt megölte a feleségét. Ezeket a keresési kulcsszavakat a bíróságon arra használták, hogy bizonyítsák velük az előre kiterveltséget.

Az angolszász jog régóta bizonyítási eszköznek tekinti az elektronikusan tárolt információt (*electronically stored information* – ESI), és ismerik az úgynevezett digitális vagy elektronikus bizonyíték fogalmát is. A magyar jogban az elektronikusan tárolt adatok helyzete annak ellenére bizonytalan, hogy a jogirodalomban egyre gyakrabban találkozhatunk ezzel a fogalommal. Mivel az információtechnológia fejlődésének eredményei a magyar bűnelkövetőket sem kerülték el, hazánkban is egyre sűrűbben fordulnak elő olyan esetek, amelyekben az elkövetett bűncselekménynek technológiai vetülete van. A büntetőeljárásról szóló törvény rendelkezéseit vizsgálva megállapítható, hogy az adat és annak hordozója nem feltétlenül képeznek szoros és elválaszthatatlan egységet, nem tisztázott viszont annak a kérdése, hogy mely esetekben lehet vagy kell külön kezelni az adatot és az azt tároló információtechnológiai eszközt. A digitális bizonyítékok jogi aspektusaival foglalkozó tudományos munkák száma meglehetősen csekély, noha nagy szükség lenne arra, hogy az elektronikusan tárolt adatok eljárásjogi szerepe és rendszertani elhelyezése tisztázott és egyértelmű legyen.

A kötet ezen része arra keresi a választ, hogy szükséges-e, hogy az elektronikusan tárolt információ önálló bizonyítási eszközként jelenjen meg a magyar büntetőeljárásban. Gyakorlati problémákon keresztül demonstrálom, hogy a büntetőeljárás során milyen problémákat vethetnek fel a digitálisan tárolt adatok, illetve milyen következményekkel járhat azok nem megfelelő kezelése, összegyűjtése. Ahhoz, hogy

[712] Bartley 2000.

bemutatható legyen az elektronikusan tárolt információk jelentősége, mindenképpen célszerűnek tartom az olyan alapfogalmak tisztázását, mint a digitális bizonyíték, illetve a digitális bizonyítási eszköz. A fogalommeghatározásokon túl bemutatjuk a bizonyítás hatályos magyar szabályait, különös tekintettel a büntetőeljárásról szóló törvény bizonyításról, valamint kényszerintézkedésekről szóló rendelkezéseire. Mivel az elektronikusan tárolt információ mint bizonyítási eszköz angolszász jogterületről származik, indokoltnak tartom bemutatni a témában keletkezett, főleg az Egyesült Államokban publikált külföldi szakirodalmat.

A digitális bizonyíték fogalma

A bizonyítás sajátos megismerési folyamat, amelynek célja a múltban történt események lehető legpontosabb feltárása. E megismerés folyamán az eljáró hatóság bizonyítékokat gyűjt, amelyek olyan adatok, amelyek büntetőjogilag releváns tényekre vonatkoznak, és amelyeket a törvény által megengedett forrásokból (bizonyítási eszközökből) szereztek be. A bizonyítási eszköz tehát a bizonyíték hordozója, a bizonyíték pedig az az információ, amelyet a bizonyítási eszközből nyerünk. A leggyakrabban elhangzó példa ennek szemléltetésére a tanú vallomása: ez esetben a tanúvallomás a bizonyítási eszköz, az információ, amelyet a hatóság a vallomásból nyer, pedig a bizonyíték. Nem ennyire egyértelmű a helyzet azonban információtechnológiai környezetben. Mivel manapság a legtöbb bűncselekménynek van valamilyen technológiai vetülete, a hatóságok a nyomozás során gyakran találkoznak olyan bizonyítékokkal, amelyeket információtechnológiai eszköz hordoz, ez az úgynevezett digitális bizonyíték. Először a digitális bizonyítékokkal foglalkozó tudományos társaság (Scientific Working Group on Digital Evidence) tett kísérletet a digitális bizonyíték fogalmának meghatározására 1998-ban. A társaság a következő definíciót alkotta: „Bizonyító erejű információk, amelyeket bináris formában tároltak vagy továbbítottak."[713] A fenti meghatározás egyik fő problémája, hogy csak a bináris formában tárolt információkat tekinti digitális bizonyítéknak, amely ugyan kétségkívül az egyik legnépszerűbb, de korántsem az egyetlen számrendszer. A hexadecimális, azaz a tizenhatos számrendszer használata szintén népszerű az informatikában, az egyes programozási nyelvekben sűrűn fordulnak elő hexadecimális számok. Máté István Zsolt kiemelte, hogy ebben a definícióban a hangsúly „a puszta adatra kerül, s az adathordozót, bárminemű is

[713] Scientific Working Groups on Digital Evidence and Imaging Technology 2015: 7.

legyen az, elhagyja a meghatározásból".[714] Eoghan Casey szerint digitális bizonyíték „minden olyan adat, amely alátámaszthatja, hogy bűncselekmény történt, vagy amely összekapcsolja a bűncselekményt annak elkövetőjével".[715] Hasonló a digitális bizonyíték fogalma a brit jogban is, a Rendőrfőnökök Egyesülete *Útmutató a számítógép-alapú elektronikus bizonyítékokhoz* című kiadványában[716] a következőképpen definiálta a fogalmat: „a számítógép-alapú elektronikus bizonyíték olyan nyomozási értékkel bíró információ és adat, amelyet számítógépen tárolnak, vagy számítógép segítségével továbbítottak." Az európai szabályozásban szintén nem ismeretlen a digitális bizonyíték. Az Európa Tanács Számítástechnikai Bűnözésről szóló egyezményének preambuluma rögzíti azt, hogy „jelen Egyezmény célja, hogy […] lehetővé tegye a bűncselekmények elektronikus formában megjelenő bizonyítékainak összegyűjtését".[717] Az egyezmény eljárásjogi szabályai emellett több esetben szólnak elektronikus bizonyítékról (14. cikk, 23. cikk, 25. cikk, 35. cikk, 46. cikk), ellenben nem definiálja, hogy mit ért elektronikus bizonyítékon. A magyar jogirodalomban szintén találhatunk kísérletet a digitális bizonyíték definiálására. Peszleg Tibor szerint a digitális bizonyíték „olyan számítástechnikai eszközről beszerzett adat, amelyet bűncselekménynél valamilyen formában számítástechnikai eszközön tároltak, vagy amelyek feldolgoztak információkat a bűncselekményekkel kapcsolatban."[718]

A fenti definícióknak két közös elemük van:

1. Az információk, adatok a büntetőjogilag releváns tényekre vonatkoznak.
2. Olyan információkról, adatokról van szó, amelyeket számítógép (információs rendszer) tárol vagy továbbít. E pont tekintetében van némi különbség az egyes meghatározások között, hiszen a digitális bizonyítékokkal foglalkozó tudományos társaság definíciója az adathordozóknak a számítógépnél tágabb körét öleli fel.

A digitális bizonyítékok számos olyan kérdést felvetnek, amelyekre még nem született egységes és kielégítő válasz. Ahogy arról már korábban esett szó, a bizonyíték fogalmának egyik kulcseleme, hogy az információ megszerzése törvény által megengedett forrásból, azaz bizonyítási eszközből történjen.

714 Máté 2014: 88.
715 Casey 2012: 7.
716 Association of Chief Police Officers 2011: 6.
717 Cybercrime Egyezmény preambulum.
718 Peszleg 2005: 25–40.

A digitális bizonyíték forrásai

A digitális bizonyítékok esetében azonban nem teljesen egyértelmű, hogy mit tekintsünk a bizonyíték forrásának. A szakirodalmat és a vonatkozó jogszabályi rendelkezéseket vizsgálva megállapítható, hogy e vonatkozásban két elmélet létezik: az egyik szerint a digitális bizonyítékok forrása minden esetben az a tárgy (adathordozó), amely a bizonyítékot tartalmazó adatot (amely lehet szöveges, kép-, videófájl vagy akármilyen program, illetve alkalmazás) tárolja. Ezen elmélet szerint a digitális bizonyítékokat minden esetben olyan tárgyi bizonyítási eszközök hordozzák, amelyek képesek elektronikus formában létező adatok rögzítésére, tárolására, továbbítására. Ilyen eszközök lehetnek a *desktop*ok (asztali számítógépek), laptopok, táblagépek, játékkonzolok, okostelefonok, CD-k, DVD-k, pendrive-ok, nyomtatók. A másik elmélet, amely főleg angolszász területen honosodott meg, ennél jóval komplexebb képet fest. Ezen elmélet szerint a bizonyítékforrás az elektronikusan tárolt adat (szövegfájl, táblázat, képfájl, videófájl, hangfájl, naplófájlok, metaadatok stb.), hiszen a hatóságok közvetlenül ezekből nyerik a releváns információt, a hardver csupán olyan szerepet tölt be, mint egy iratokat tároló szekrény. Nem mindegy azonban, hogy ez az információ milyen viszonyban van az őt hordozó fizikai komponenssel, bizonyos esetekben ugyanis az információ kizárólag a hardverrel együttesen vizsgálható és értékelhető. Az Egyesült Államokban igen részletes és precedenseken alapuló szabályok határozzák meg azt, hogy mikor szükséges a hardvert az adattal együtt vizsgálni, és mikor van szükség csupán a tárolt adatok információtartalmára. A két elmélet közötti legmarkánsabb különbség az, hogy míg az első az adatra és annak tárolójára elválaszthatatlan egységként tekint, addig a második lehetőséget biztosít arra, hogy a hatóság az adatot és az azt tároló hardvert egymástól függetlenül kezelje, aminek az adat megismerésére irányuló kényszerintézkedések során van nagy jelentősége. Magyarországon a problémát jelenleg az jelenti, hogy sem a büntetőeljárásról szóló törvény rendelkezéseiből, sem a szakirodalom vizsgálatából nem szűrhető le egyértelmű állásfoglalás a fenti kérdésben. A büntetőeljárásról szóló törvény ugyan a bizonyítási eszközök taxatív felsorolásában az új Be. hatálybalépése óta külön is nevesíti az elektronikus adatot, de azokra a tárgyi bizonyítási eszközök szabályait rendeli alkalmazni (Be. 205. §). Jogosan merülhet fel tehát a kérdés, hogy valójában mi a digitális bizonyíték forrása: az adathordozó mint tárgyi bizonyítási eszköz, avagy maga az információs rendszerben tárolt adat, amely valamilyen információt hordoz? E körben indokoltnak tartjuk visszautalni a kötet II. részére, amelyben szó esett az adat fogalmáról is. A fogalommeghatározásokról szóló fejezetben nemcsak az adat

fogalmáról, de az adat és az információ viszonyáról is szó esett, amely elméletben lehetővé teszi, hogy magára az adatra tekintsünk a bizonyíték forrásaként. Ezt a zavart a Be. későbbi rendelkezései sem oldják fel maradéktalanul, hiszen a lefoglalás szabályai körében a törvény az elektronikus adat lefoglalásának számtalan módját lehetővé teszi. A Be. 315. §-a alapján az elektronikus adat lefoglalható másolatkészítéssel, áthelyezéssel, a teljes adathordozó lemásolásával, de akár magának a fizikai adathordozónak a lefoglalásával is. A lefoglalás módozatai sokszínűségének hátterében az a jelenség áll, amelyet Tremmel Flórián is megfogalmaz, aki szerint „egyre több bizonyítási mód önálló jelentőségre tesz szert, s egyszersmind sui generis eljárási szabályozás lévén legalizálódik".[719] A következetesség hiánya különösen a Be. azon rendelkezései kapcsán okoz problémát, amelyek a digitális bizonyítékok, illetve az azokat hordozó bizonyítási eszközök megszerzését és megőrzését szolgáló kényszerintézkedésekre vonatkoznak. A digitális bizonyítékok forrásának tisztázása azért kiemelkedően fontos feladat, mert a jelenlegi szabályozási és értelmezési bizonytalanságok a jogbiztonságot, illetve az eljárásban részt vevő személyek jogait veszélyeztetik. A következő részben azokat a dilemmákat mutatom be részletesen, amelyek amiatt merülhetnek fel, hogy nem tisztázott, hogy milyen bizonyítási eszközhöz rendeljük a digitálisan tárolt adatot.

Az elektronikusan tárolt információ az amerikai büntetőeljárásban

Az amerikai büntetőeljárásban sokkal átláthatóbb szabályok vonatkoznak erre a területre, a digitális bizonyíték forrása kapcsán több precedensértékű döntés is született. Az Egyesült Államokban kialakult rendszer szerint a digitális bizonyíték forrása az elektronikusan tárolt információ *(electronically stored information),* a hardver és az adat nem interdependensek, hanem egymástól függetlenül is kezelhetők.

Ha az amerikai büntetőeljárás bizonyításról szóló törvényi rendelkezéseit vizsgáljuk, azt találjuk, hogy a bizonyítási eszközöket sem a szövetségi büntetőeljárásról szóló törvény (Federal Rules of Criminal Procedure), sem a bizonyítékok szövetségi szabályairól szóló törvény (Federal Rules of Evidence) nem sorolja fel tételesen. Ennek oka a kontinentális és az angolszász büntető-eljárásjogi rendszerek közötti eltérésben keresendő. A kontinentális jogrendszerekben ugyanis a bizonyítékok összegyűjtése és értékelése már az ügy bíróság elé kerülését megelőzően, az eljárás nyomozati szakaszában megtörténik, és ez az eljárás törvényi szinten szabályozott,

[719] Tremmel 2006: 67.

szigorú formaságokhoz kötött. Ezzel szemben, ahogy azt Tremmel Flórián is kifejtette,[720] az amerikai bizonyítási rendszer negatíve kötött, hiszen főszabályként bármi lehet bizonyíték, kivéve, amelyet jogszabály vagy a bíróság kizár. A bizonyítékok felhasználhatóságáról való döntés *(admissibility)* a bíróság egyedi mérlegelésére van bízva, a részletes eljárási szabályokkal szemben a hangsúly sokkal inkább az eljárási garanciákon van. Törvényi szinten csak annyi rögzítettek a bizonyítási eszközökről, hogy „minden releváns bizonyíték felhasználható, kivéve ha az alkotmány, szövetségi törvény, a bizonyítékokról szóló szövetségi törvény vagy a Legfelsőbb Bíróság által előírt egyéb szabályok másképp rendelkeznek".[721] Ennek megfelelően bizonyítási eszköz lehet minden, amit az Alkotmány vagy jogszabály nem tilt, amennyiben az ügyben eljáró bíró azt adott ügy viszonylatában relevánsnak ítéli. A bizonyíték akkor releváns, „ha alkalmas arra, hogy egy tényt valószínűbbé vagy kevésbé valószínűvé tegyen, mint az a bizonyítási eszköz hiányában lenne, és a tény következményekkel bír a cselekmény meghatározásánál".[722] A relevancia kritériumának teljesülése azonban önmagában nem elégséges ahhoz, hogy egy bizonyíték az eljárás során felhasználható legyen. Gordon Mahler szerint a bizonyítékok mérlegelése egy számos technikai szabállyal megtűzdelt rendszer, amely az amerikai jogi egyetemeken külön tantárgy.[723] Ennek megfelelően az elektronikusan tárolt információknak is számos követelménynek kell megfelelniük ahhoz, hogy bizonyítékként felhasználhatók legyenek. Az elektronikusan tárolt információk bizonyítékként való felhasználhatóságáról először 2007-ben egy polgári ügyben, a Lorraine v. Markel ügyben született döntés. A döntéshez fűzött indokolás[724] egy ötlépcsős tesztet ír elő, állapít meg, amelyen az elektronikusan tárolt információknak át kell menniük ahhoz, hogy az eljárás során bizonyítékként értékelhetők legyenek. Ha az elektronikusan tárolt információ az említett teszten sikeresen átmegy, akkor a büntetőeljárásban bizonyítékként felhasználható. Az, hogy a Lorraine v. Markel döntés polgári eljárásban született, nem jelenti azt, hogy büntetőügyben nem alkalmazható. A United States v. O'Keefe ügyben a bíróság kimondta, hogy „botorság lenne figyelmen kívül hagyni a polgári eljárásban alkalmazott szabályokat csak azért, mert büntetőügyről van szó, különösen akkor, ha jobbnak tűnik ezen szabályokat

720 Tremmel 2006: 63.
721 Federal Rules of Evidence Rule 402. General Admissibility of Relevant Evidence.
722 Fantoly 2012.
723 Mahler 2003: 77.
724 Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007).

alkalmazni, amikor a dokumentumok előállítása mind polgári, mind büntetőügyekben ugyanazokat a problémákat veti fel, mint újra feltalálni a kereket."[725]

Az egyes kényszerintézkedések, főleg a lefoglalás esetében igen részletes szabályok vonatkoznak arra, hogy mikor van szükség az elektronikusan tárolt információ mellett az azt hordozó hardverre is. Az Egyesült Államok Igazságügyi Minisztériuma (United States Department of Justice) 1994-ben ajánlást adott ki a számítógépek átvizsgálásáról és lefoglalásáról, valamint az elektronikus bizonyítékok összegyűjtéséről. Az ajánló az első kiadás óta folyamatosan frissül, hogy lépést tudjon tartani a legújabb technológiai fejleményekkel, a legfrissebb eljárási szabályokkal és az esetjoggal. Az ajánlás elválasztja egymástól azokat az eseteket, amelyekben a hardver lefoglalása, és amelyekben a tárolt információ lefoglalása szükséges. A dokumentum szerint: „a legfontosabb döntés, amelyet a nyomozóknak meg kell hozniuk, amikor összeállítják a lefoglalandó dolgok listáját, az, hogy a lefoglalandó dolog a számítógép fizikai komponense (hardver) vagy csupán az információ, amelyet a hardver tartalmaz."[726] Bizonyos esetekben ugyanis a hardver csupán az elektronikusan tárolt információk tárhelyéül *(container)* szolgál, így önmagában csekély a relevanciája. Minden ügyben egyedi mérlegelést kíván annak eldöntése, hogy a sikeres bizonyításhoz szükség van-e a hardverre, vagy elegendő a tárolt adat. A döntés meghozatalához elsősorban azzal kell tisztában lennünk, hogy a számítógépek milyen lehetséges szerepeket tölthetnek be egy bűncselekményben. Az amerikai Donn Parker[727] a bűncselekményekben megjelenő számítógépek (információs rendszerek) lehetséges szerepeit tanulmányozta, és listát készített azokról a szerepekről, amelyekben a számítógép egyes alkotóelemei előfordulhatnak:

- A számítógép lehet fizikai valójában (hardver) az elkövetés tárgya (például amikor a számítógépet vagy infokommunikációs eszközt ellopják vagy megrongálják).
- A számítógépes környezet lehet az elkövetés tárgya. Ez az eset akkor következhet be, ha a sérelem nem a hardverben következik be, hanem valamely számítógépes adatban, amely lehet valamely futtatott program vagy a számítógépen tárolt információ. Tipikus példa, amikor a számítógépet vírussal vagy más *malware*-rel fertőzik meg, amely akadályozza annak helyes működését.
- A számítógép fizikai valójában (hardver) lehet az elkövetés eszköze: ritkán ugyan, de előfordul, hogy a számítógép valamilyen fizikai komponensével követnek el

[725] U.S. v. O'Keefe, 537 F. Supp. 2d 14 (D.D.C. 2008).
[726] Jarrett et al. 2009: 70.
[727] Casey 2012: 40.

bűncselekményt. Ilyen például az a 2010-es emberölési eset, amelyben három fiatal számítógép-vezetékkel fojtott meg egy férfit.[728]

- A számítógépes környezet mint az elkövetés eszköze (a számítógép az elkövetés eszköze azokban az esetekben, amikor az elkövető a számítógépet arra használja, hogy azzal valamilyen bűncselekményt kövessen el). Tipikus példák a zaklatás, gyermekpornográf tartalmak letöltése, online aukciós csalás.

Az amerikai igazságügyi minisztérium útmutatója szerint a hardverre akkor van szükség, ha az tiltott eszköz, a bűncselekmény gyümölcse vagy eszköze. Eoghan Casey szerint tiltott eszköz a hardver, amennyiben az „olyan eszköz, amelyet tilos az állampolgároknak birtokolni. Például bizonyos esetekben tilos az egyéneknek az Egyesült Államokban olyan hardvert birtokolni, amely az elektronikus kommunikáció lehallgatására szolgál."[729] A bűncselekmény gyümölcse az információs rendszer, ha azt az elkövetés során szerezték, vagy az elkövetés során jött létre, ilyenek tipikusan a lopott alkatrészek, amelyek vonatkozásában kétségen felül áll, hogy az elkövető birtokából el kell vonni. A hardver akkor lehet a bűncselekmény eszköze, ha azt fizikai sérülés okozására használják, ám Eoghan Casey szerint van ennél jóval szemléletesebb példa is: az olyan speciálisan elkészített, felszerelt, konfigurált hardver is lehet a bűncselekmény elkövetésének eszköze, amelyet bizonyos bűncselekmények elkövetésére hoztak létre. Példának hozza az úgynevezett *sniffer*eket, amelyek a hálózati forgalom lehallgatására alkalmas eszközök. Minden más esetben elegendő pusztán az elektronikusan tárolt információt beszerezni, amely a hardver analógiájára lehet tiltott információ, a bűncselekmény gyümölcse, illetőleg eszköze, valamint maga a bizonyíték is. Tiltott információ például a gyermekpornográfia. Az információ a bűncselekmény eszköze akkor lehet, amennyiben a bűncselekmény megvalósítására használták, például a vírusok és egyéb kártékony kódok. Egyéb esetekben, ha az információ birtoklása nem tiltott, és nem is használták a bűncselekmény eszközéül, az információ a bűncselekmény bizonyítéka. Az Egyesült Államok Igazságügyi Minisztériumának ajánlása utóbbira egy vállalkozás elektronikusan tárolt meghamisított üzleti könyveit, valamint a drogkereskedők tranzakcióinak listáját hozza példaként. Az amerikai büntetőeljárási rendszert vizsgálva megállapítható, hogy az elektronikus információ beemelése a bizonyítási eszközök közé korántsem elvetendő gondolat, hiszen a hardver és az információ elválasztása

[728] Számítógép-vezetékkel fojthatták meg a jászberényi pedofilt 2015.
[729] Casey 2012: 44.

változatosabb jogszabályi lehetőségek kialakítását teszi lehetővé, amely által a büntetőeljárási rendszer jobban alkalmazkodhat az egyes ügyek sajátosságaihoz.

Ahogy Tremmel Flórián is megjegyzi:

> „[A] kriminalisztika folytonosan kutatja, bővíti és gazdagítja azoknak az információhordozóknak a körét, fajtáit, amelyek felhasználásával a bűncselekmények nem csak felderíthetők, hanem bizonyíthatók is lesznek. E két tendencia együttes megléte a bűnügyek gyakorlatában bizonyos feszültséggel is járhat: egyfelől elavulttá válhatnak eljárásjogi rendelkezések (például eskü), másfelől pedig még törvényes szabályozást, elismerést nem nyert potenciális bizonyítási eszközök és bizonyítási módok kerülhetnek előtérbe."[730]

A hardver és az információ elválasztása során kiemelendő, hogy a megfelelő kényszerintézkedés megválasztása, illetve a végrehajtásának módszere az adott ügy körülményeit, illetve az információs rendszer tulajdonságait figyelembe véve esetenként mérlegelendő, a jogrendszer feladata biztosítani azt az egyértelmű és világos keretrendszert, amely meghatározza, hogy milyen lehetőségek állnak a nyomozó hatóságok rendelkezésére. Az adathordozó tartalmának lefoglalásával kapcsolatos szabályok kialakításához jó példa lehet az 1996. évi LVII. számú, a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló törvény (a továbbiakban: versenytörvény, Tpvt.), amely részletesen, garanciális szabályok beépítésével rendelkezik mind az egyes adatok, mind az adathordozó teljes tartalmának az átmásolásáról. Az előbbieken túl szükségesnek látom egy olyan ajánlás elkészítését, amely útmutatásul szolgál az informatikai elemet tartalmazó bűncselekmények nyomozásában részt vevő személyeknek. Mivel az információs rendszerek vizsgálata és szakszerű lefoglalása nagyon sok esetben hozzáértő személyt igényel, indokoltnak tartom a nyomozó hatóság tagjainak, állományának továbbképzését. A szakmai tudás átadását Peszleg Tibor is kiemelten fontos feladatként tartja számon, tanulmányában azt írja, hogy „igazságügyi szakértőt csak akkor célszerű kirendelni, ha ténylegesen szakkérdés megállapítása szükséges, nem pedig a digitális írástudás pótlására".[731]

730 Tremmel–Fenyvesi–Herke 2009: 40.
731 Peszleg 2005: 32.

A digitális bizonyítékok megszerzése és megőrzése

A magyar büntetőeljárás számos olyan lehetőséget biztosít a nyomozó hatóságok számára, amelyek által a digitális bizonyítékok megismerhetők, megszerezhetők, illetve megőrizhetők. Ezeket a lehetőségeket a büntetőeljárásról szóló törvény, valamint a rendőrségről szóló törvény tartalmazzák. A digitális bizonyíték megismerhető:

- adatszerző tevékenység után, adatkéréssel, feltételes adatkéréssel (Be. 261–266. §);
- az adathordozónak, illetőleg az adatnak a lefoglalásával (Be. 315. §);
- információs rendszerben tárolt adatok megőrzésére kötelezéssel (Be. 316. §);
- titkos információgyűjtéssel az ügyészségről szóló törvény, a rendőrségről szóló törvény, a Nemzeti Adó- és Vámhivatalról szóló törvény vagy a nemzetbiztonsági szolgálatokról szóló törvény alapján; illetőleg
- bírói engedélyhez között leplezett eszközök alkalmazásra révén (Be. 231. §).

Speciális jellegük folytán jelen kötet nem tárgyalja a titkos információgyűjtéssel és a titkos adatszerzéssel kapcsolatos dilemmákat, hiszen ezek olyan jellegű tevékenységek, amelyek gyakorlati alkalmazásáról meglehetősen kevés nyilvánosságra hozható információ áll rendelkezésre.

Az adatkérés

A megkeresés jogintézménye az egyik legjobb példa a hardver és az adat elválaszthatóságára. A Be. szabályai szerint a büntetőeljárásban a bíróság, az ügyészség és a nyomozó hatóság, illetve az előkészítő eljárást folytató szerv bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől adatszolgáltatást kérhet. Amennyiben az adatkérés elektronikus hírközlési szolgáltatót érint, szükség van az ügyészség engedélyére is.

A régi Be. egyes rendelkezéseit sok kritika érte korábban a hírközlési adatvédelmi irányelv érvénytelenné nyilvánításával összefüggésben. A korábbi törvény ugyanis a 178/A. szakaszában úgy rendelkezett, hogy a nyomozó hatóság – többek között – a hírközlési szolgáltatást nyújtó szervezettől az ügyész jóváhagyása nélkül is igényelhette adatok szolgáltatását, ami nem volt megtagadható. Ezzel a jogalkotó egy fontos alkotmányossági garanciát iktatott ki, hiszen pont az ügyészi jóváhagyás hivatott biztosítani, hogy a nyomozó hatóság csak indokolt esetben és meghatározott

céllal élhessen az adatszerzés lehetőségével. A jelenleg hatályos Be. adatkérést szabályozó 261. §-a ellenben már ügyészi engedélyhez köti az elektronikus hírközlési szolgáltatótól való adatkérést, a jogalkotó tehát ezt a problémát korrigálta.

Fennmaradó probléma viszont, hogy a Be. lehetőséget biztosít az ügyészi jóváhagyás „kiiktatására", hiszen ha az adatkérés engedélyezése olyan késedelemmel járna, amely az adatkéréssel elérni kívánt célt jelentősen veszélyeztetné, engedély nélkül is kérhető az adatszolgáltatás. Azonban ha az ügyészség utólag nem engedélyezi az adatkérést, a beszerzett adatok bizonyítékként nem használhatók fel. Megjegyzendő, hogy a Be. ugyan rendelkezik arról, hogy az adatszolgáltatás iránti megkeresés csak akkor lehetséges, ha az az ügy jellege miatt szükséges, azonban az ügyészi jóváhagyás „kiiktatása" miatt gyakorlatilag nincs, aki ellenőrizné, hogy egy egyedi esetben valóban szükség van-e az adatokra, ennek eldöntése teljes mértékben az adott ügyben eljáró nyomozó hatóságtól függ.

Az adatkérés legtipikusabb formája a híváslisták ellenőrzése, illetve annak az ellenőrzése, hogy egy felhasználó számára milyen IP-címek voltak egy adott időszakban kiosztva. Ha a nyomozó hatóság hírközlési szolgáltatótól igényel egy felhasználó azonosításához szükséges adatokat, fel sem merül kérdésként, hogy a hatóság részére azt az információs rendszert, illetve adathordozót, amelyen az eredeti adat található, fizikai valójában kellene megküldeni, hiszen ezek a szolgáltatók igen nagyszámú felhasználó adatait tárolják egy helyen. A nyomozó hatóság általában megelégszik azzal, ha a szolgáltató nyilvántartásából kinyeri az adatkéréssel érintett információkat, és azokat valamilyen adathordozón átadja, 2021 óta pedig lehetőség van arra is, hogy a nyomozó hatóság közvetlen hozzáféréssel nyerje ki a szükséges adatokat a szolgáltató nyilvántartásából vagy adatállományából.[732] Ennek oka, hogy az eljárás szempontjából az adat és annak a tartalma, az általa hordozott információ a lényeges, nem pedig az, hogy milyen adathordozón tárolták.

Az adatkérés egy speciális formája a feltételes adatkérés, amelynek elrendelése esetén a szolgáltató akkor köteles adatszolgáltatást teljesíteni, ha valamilyen feltétel, például hívás indítása, fogadása, fizetés indítása bekövetkezik.[733]

[732] Be. 263. § (1) bekezdés.
[733] Be. 266. §.

A lefoglalás

A digitális bizonyítékok megismerési lehetősége a lefoglalás, amelyet már a Be. kényszerintézkedésekről szóló részében szabályoz a jogalkotó. A digitális bizonyítékok megszerzésének esetei közül általában a lefoglalás okozza a legtöbb problémát, és ez a kényszerintézkedés jelenik meg a leggyakrabban a médiában is, amikor informatikai bűncselekmények nyomozásáról esik szó. A lefoglalás jogintézménye tükrözi a leginkább a digitális bizonyítékok forrásával kapcsolatos polémiát. A büntetőeljárásról szóló törvény 308. §-ának (2) bekezdése kötelezővé teszi a lefoglalást, ha annak tárgya bizonyítási eszköz. Az elektronikus adatok lefoglalására a törvény külön rendelkezéseket tartalmaz, és öt végrehajtási módot határoz meg, amelyek:

- az elektronikus adatról másolat készítése,
- az elektronikus adat áthelyezése,
- az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítése,
- az azt tartalmazó információs rendszer vagy adathordozó lefoglalása, vagy
- jogszabályban meghatározott más mód.[734]

Ugyan a törvény lehetőséget ad a teljes információs rendszer tárgyi bizonyítási eszközként történő lefoglalására, ez sok esetben nem szerencsés. Egyrészt a teljes rendszer számtalan olyan egységből áll, amelyek a büntetőeljárás szempontjából nem releváns hardverkomponensek (például videokártya, hangkártya, tápegység). Ezek a komponensek igen gyakran azonban nagyobb értékkel bírnak, és a technológia rohamos fejlődésének következtében gyorsan amortizálódnak, így a lefoglalás elszenvedőjének komoly anyagi kárt okozhat, ha a hatóság az adathordozóval együtt ezeket az eszközöket is lefoglalja. A teljes konfiguráció lefoglalása személyiségi jogi aggályokat is felvet. Az adatvédelmi biztos 2009-es beszámolója[735] alapján számtalan esetben előfordul, hogy a lefoglalt számítógép olyan személyes adatokat is tartalmaz, amelyek a büntetőeljárással semmilyen összefüggésben nincsenek. Ezek a személyes adatok sok esetben hosszú hónapokig maradnak a nyomozó hatóságnál, ami a személyes adatok védelméhez fűződő jog sérelmét jelentheti. Az információs rendszer nemcsak egy különálló számítógép lehet, hanem az adatok automatikus kezelését, tárolását, továbbítását biztosító, egymással kapcsolatban lévő berendezések összessége is, vagyis

[734] Be. 315. § (1) bekezdés.
[735] *Az adatvédelmi biztos beszámolója* 2009.

akár egy céges hálózat összes számítógépére/szerverére kiterjeszthető a lefoglalt dolgok köre. (Sőt, ezen az úton elindulva, ha egy számítógép az internethez csatlakozik, az összes internethez csatlakoztatott eszközt tekinthetnénk egy információs rendszernek.) A cég működéséhez szükséges eszközök lefoglalása azonban veszélyezteti a kényszerintézkedéssel érintett cégek üzletszerű működését. Egy *webhosting* szolgáltatást nyújtó vállalkozás például működésképtelen a szerverei nélkül, hiszen az általa nyújtott szolgáltatás lényege pont az, hogy tárhelyet biztosít a felhasználói számára. A felhasználók számára is előnytelen következményekkel járhat egy szerver lefoglalása: egy-egy szerver ugyanis általában több felhasználó számára biztosít tárhelyet, így a lefoglalással vétlen harmadik személyek weboldalai válhatnak elérhetetlenné, illetve ezen személyek személyes adatai kerülnek szükségtelenül a nyomozó hatósághoz. A teljes konfiguráció lefoglalásának tagadhatatlanul vannak azonban bizonyos előnyei is. A legnagyobb előnye az, hogy kevés szakértelmet igényel, ezért a lefoglaláshoz nem szükséges szaktanácsadó igénybevétele, a rendszer áramtalanítását követően azt a nyomozó hatóság tagjai is el tudják végezni. További előnye a teljes rendszer lefoglalásának, hogy ezáltal a szükséges vizsgálatok laboratóriumban kontrollált körülmények között végezhetők el, valamint biztosítható, hogy a lefoglalás után az eredeti adatokban semmilyen változás ne következzen be.

A második lehetőség, hogy a hatóság csak az érintett adatot tartalmazó adathordozót foglalja le, ez köznyelvi értelemben jelentheti ugyanúgy egy pendrive lefoglalását, mint a winchester kiszerelését az információs rendszerből. Az adathordozó lefoglalásának kétségtelenül előnye, hogy a lefoglalás elszenvedőjének nem okoz a szükségesnél nagyobb sérelmet, valamint ez a módszer is lehetővé teszi az adathordozó későbbi kontrollált környezetben történő vizsgálatát. Hátránya ellenben, hogy bizonyos adathordozók szakszerű kiszereléséhez minden esetben hozzáértő személy szükséges. Hátrány lehet továbbá, hogy a lefoglalást követően kiderülhet, hogy a lefoglalt adathordozó inkompatibilis a vizsgálatot végző szervezet rendszerével (például az adathordozó beszerelése egy másik rendszerbe *„incompatible BIOS translation detected”* hibaüzenetet eredményezhet), vagy ahogy Peszleg Tibor is rávilágít, vannak olyan eszközök, amelyek „olyan egységet képezhetnek, hogy ha megbontják őket, már nem lehetséges az eredeti adattartalom visszaállítása (például RAID tömbök esetében)”.[736]

[736] Lásd Peszleg 2010: 23–31. Peszleg Tibor gondolataihoz ugyanakkor szükséges hozzáfűzni, hogy vannak szoftverek, amelyekkel a RAID helyreállítható, ha mindegyik lemezt bitről bitre lemásoljuk. Ennek a lehetőségnek a komplexitása ugyanakkor függ attól, hogy az információ hol tárolódik, a RAID vezérlőn tárolt adatot jellemzően nehezebb kinyerni, mint a lemezen tárolt adatot.

Harmadik opcióként lehetőség van arra, hogy a hatóság csak az adathordozó tartalmát, vagyis az adatokat foglalja le akár másolás, akár áthelyezés révén. A lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló 11/2003. (V. 8.) IM-BM-PM együttes rendelet megerősíti azt a nézetet, hogy az adat önmagában is lefoglalható. A rendelet 67. § (1) bekezdése arról rendelkezik, hogy mikor kell másolatkészítéssel lefoglalni az adatot. Eszerint „az elektronikus adat lefoglalását másolat készítésével kell végrehajtani, ha a) a lefoglalt dolog érintett őrizetében hagyásának feltételei fennállnak, és b) a másolat készítését követően az adat eredeti helyen való további tárolása a büntetőeljárás érdekeit nem veszélyezteti". Áthelyezéssel kell végrehajtani a lefoglalást abban az esetben, ha „az adat eredeti helyen történő további tárolása a büntetőeljárás érdekeit veszélyezteti". A másolatkészítés és az áthelyezés közötti fő különbség tehát az, hogy a másolatkészítés során az adat egy példánya megmaradt az eredeti helyén, míg a nyomozó hatóság egy másodpéldányt foglal le; az áthelyezés esetén azonban az állomány úgy kerül a hatósághoz, hogy az eredeti tárolási helyéről eltávolítják. A magyar nyomozó hatóságok gyakorlatában sokáig egyáltalán nem volt jellemző az adat helyszíni lefoglalása, a hatóság számítógépek lefoglalásánál rendszerint a teljes gépet lefoglalta, majd később szakértő bevonásával végezte el a szükséges műveleteket. Az új Be. azonban e tekintetben szemléletváltást hozott, hiszen a szolgáltatók, információs rendszerek tulajdonosai érdekeit is szem előtt tartva a törvény úgy rendelkezik, hogy a lefoglalást „úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse".[737]

Az adat lefoglalásának módszertani kérdéseiről sem a törvény, sem a kormányrendelet nem szól részletesen, pedig a másolás módszerének komoly jelentősége van.

Az adat átmásolására ugyanis kétféle lehetőség is rendelkezésre áll: az egyik, amikor a hatóság a rendszert a helyszínen átvizsgálja, és a relevánsnak ítélt adatokat hagyományos módon másolja ki az információs rendszerből közvetlenül egy adathordozóra (esetleg egy másik információs rendszerre). Ennek a módszernek az előnye, hogy nem kell hozzá különös szakértelem, illetve, ha a lefoglalás elszenvedője együttműködő, a rendszer adminisztrátora, tulajdonosa maga is feltárhatja a hatóság előtt az egyes bizonyítékokat. Emellett viszont számos szempontból aggályos, az alkalmazása kihívás elé állítja ugyanis mind a hitelesség, mind a teljesség kriminalisztikai elvének érvényesülését. A digitális bizonyíték akkor hiteles, ha a későbbiekben is pontosan

[737] Be. 315. § (4) bekezdés.

meghatározható, hogy az adat egy bizonyos számítógépről/helyszínről származik, illetve, hogy a digitális bizonyítékot tartalmazó adat pontos és teljes mását foglalták le, továbbá, hogy az adat a lefoglalása óta változatlan maradt. Ezen alapelvek érvényesülését hivatott biztosítani a 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67/A. §-ának (2) bekezdése, amely arról rendelkezik, hogy a lefoglalásnak lehetőség szerint utólag meg nem változtatható adathordozóra kell történnie, amely a lefoglalás időpontjában adatokat nem tartalmazhat. Ezenfelül rendelkezik arról, hogy az átmásolás során biztosítani kell, hogy az eredeti adatok ne változzanak meg, ami általában csak speciális írásvédő eszköz vagy szoftver segítségével valósítható meg. A teljesség elve azt jelenti, hogy minden bizonyítékot le kell foglalni, azonban ha a lefoglalást végző nem rendelkezik kellő szakértelemmel, fontos bizonyítékok veszhetnek el. A számítógép ugyanis sokszor az átlagfelhasználó számára láthatatlan helyeken is tárol információkat, valamint olyan adatokat kezel, amelyeket a gép működés közben nem ment a merevlemezre. Előbbire példák lehetnek a metaadatok, a *cache* tartalma, illetve a RAM által ideiglenesen tárolt információk, utóbbira pedig a *sandbox*ban futó alkalmazások adatai (például a chatablakban folytatott beszélgetés).

Az adatok lefoglalására nyitva áll egy másik lehetőség is, mégpedig amikor a hatóság bitazonos, *hash* kulccsal ellátott tükörmásolatot készít a teljes adathordozóról. A hitelesség biztosítására ebben az esetben egy *hash*kulcsnak nevezett ellenőrző kód szolgál, amely egy egyedi adatállományhoz rendelt karaktersorozat. Abban az esetben, ha az eredeti és a tükörmásolat bitről bitre ugyanazokat az adatokat tartalmazza, a *hash*kulcs azonos, azonban ha bármelyik adathordozón utólag változtatnak, az ellenőrzés során eltérő értékeket kapunk. A tükörmásolat-készítés hátránya, hogy nem praktikus, ha nagy mennyiségű információ lefoglalása szükséges, ugyanis rendkívül idő- és erőforrás-igényes. A tükörmásolat készítésére vonatkozó előírások azonban korántsem ismeretlenek a magyar jogban. A versenytörvény a tényállás tisztázása című részben rendelkezik arról, hogy „a vizsgáló jogosult az adathordozóról fizikai tükörmásolatot készíteni, és a tükörmásolat felhasználásával az adathordozón lévő adatokat átvizsgálni, ha valószínűsíthető, hogy az adathordozón a vizsgált magatartáshoz kapcsolódó, a felhasználó által a számítógép rendeltetésszerű használata során már nem megjeleníthető adatok találhatók". [738]

[738] Tpvt. 65. § (2) bekezdés.

Az információs rendszerben tárolt adatok megőrzésére kötelezés

Az elektronikusan tárolt adat külön jelenik meg az információs rendszerben tárolt adatok megőrzésére kötelezésének szabályai között is. A Be. 316. §-ának (1) bekezdése arról rendelkezik, hogy „a bűncselekmény felderítése, illetve a bizonyítás érdekében elektronikus adat megőrzésére kötelezést lehet elrendelni", amely lényegében a birtokos, feldolgozó, illetve az adatkezelő rendelkezési jogát korlátozza. A törvény indokolása szerint ennek a kényszerintézkedésnek a bevezetésére azért volt szükség, mert a számítógépes hálózatokon tárolt adatok mennyisége az utóbbi években ugrásszerűen növekedett, és a jogalkotó felismerte, hogy adott esetben egy teljes szerver lefoglalása a vétlen hálózatüzemeltetőnek méltánytalanul nagy hátrányt okozhat. A kényszerintézkedés elrendelését követően azonnal meg kell kezdeni az érintett adatok átvizsgálását, amely két eredményre vezethet: a megőrzésre kötelezést meg kell szüntetni, vagy az adat lefoglalását kell elrendelni. A nyomozó hatóságok nagyon ritkán alkalmazzák ezt a kényszerintézkedést, általában az adatok lementésére, a bizonyítékok biztosítására törekednek, hiszen ha a bűncselekmény elkövetésével gyanúsítható személy a kényszerérintézkedés érintettje, a nyomozás érdekeivel ellentétes az adatokat ilyen személyek őrizetében hagyni. Az elkövetéshez nem köthető esetekben (például sértett vagy harmadik személy) a kényszerintézkedés elszenvedője pedig szinte mindig együttműködő, ezért végrehajtható a lefoglalás, kimentés.

A büntetőjogilag releváns információk megőrzésének egy másik módja az Eht.-ban szabályozott, elektronikus hírközlési szolgáltatókat terhelő általános adatmegőrzési kötelezettség. Bizonyos adatfajták megőrzése ugyanis a szolgáltatók *ex lege* kötelezettsége. A megőrzés e fajtájáról bővebben az internetes közvetítő szolgáltatók kötelezettségeivel foglalkozó VII. részben szólok.

Speciális eszközök a malware-ek felderítésében

Annak ellenére, hogy a magyar sajtó többször számolt be arról, hogy nyomozás van folyamatban információs rendszer és adatok megsértésének bűntette miatt, a médiában nagy port kavart események utóéletéről, a vádelemelésről és az esetleges ítélethirdetésekről már szinte soha nem lehet hallani.

Az online környezet viszonylag nagymértékű anonimitást biztosít a benne mozgó szereplőknek, de alapesetben az elkövető az IP-cím alapján azonosítható. Az IP-cím a hálózati környezetben az egyes eszközök, például a számítógépek azonosítására

használt egyedi megjelölés. Az IP-cím forgalmazási és személyes adat, ezért a tárolására és kezelésére szigorú szabályok vonatkoznak. A hírközlési adatvédelmi irányelv[739] arra kötelezi a tagállamokat, hogy biztosítsák a nyilvánosan elérhető elektronikus hírközlési szolgáltatások segítségével történő közlések és az azokra vonatkozó forgalmi adatok – így az IP-címek – titkosságát. E szabály alól az irányelv akkor enged kivételt, ha a kérdéses adatok megismerése a nemzetbiztonság, a nemzetvédelem és a közbiztonság védelme érdekében, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használata megelőzésének, kivizsgálásának, felderítésének és üldözésének biztosítása érdekében szükséges. Ennek nyomán az Eht. rendelkezései közt is találhatunk olyan szabályt, amely bizonyos adatfajták esetében megőrzési kötelezettséget ír elő az elektronikus hírközlési szolgáltatást nyújtók számára.

A törvény rendelkezései értelmében a megőrzéssel érintett adatok köre kizárólag az előfizető személyével (előfizető neve, számlázási címe), valamint a forgalmazás tulajdonságaival (IP-cím, portszám, MAC-cím) kapcsolatos adatokra terjed ki, a közlésnek a tartalmára nem. A nyomozó hatóság megkereséssel kérhet adatszolgáltatást a hírközlési szolgáltatóktól ezen adatok megismerése érdekében.

Az Eht. szabályai azonban csak a Magyarország területén végzett vagy területére irányuló elektronikus hírközlési tevékenységre vonatkoznak; a szolgáltatók által tárolt adatfajták és az adatok megőrzésének időtartama országonként igen eltérő lehet. Ugyanakkor az informatikai bűncselekmények nincsenek tekintettel az országhatárokra: az információs rendszereket megfertőző kártékony programok terjedése nem áll meg a határoknál – a fertőzöttség a kártevő népszerűségétől függ, nemritkán globális. E nemzetközi jellegből fakadóan egy ország nyomozó hatósága ritkán elegendő a teljes hálózat felderítéséhez és az irányító-vezérlő központ lekapcsolásához. A fertőzések országhatárokon belüli felszámolása csak a távközlési és a biztonságtechnikai piac segítségével valósítható meg, ráadásul csak ideig-óráig hatásos, hiszen ha az irányító központ fennmarad, a kártevő újra képes lesz fertőzni.

Az ENSZ korábban már hivatkozott tanulmánya arról számolt be, hogy a jelentéskészítésben közreműködő országok több mint fele nyilatkozott úgy, hogy a kiberbűncselekmények, amelyekkel a rendőrség találkozik, 50-100%-ban tartalmaznak nemzetközi elemet.[740] A magyar tapasztalatok egybevágnak az ENSZ tanulmányában foglaltakkal: az ORFK úgy nyilatkozott, hogy – mivel a számítógépes bűnözés a legtöbb

[739] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv).

[740] UNODC 2013.

esetben országhatárokon átnyúló bűnelkövetési módszerekkel történik – szinte minden alkalommal szükség van nemzetközi bűnügyi együttműködésre. A tapasztalatok azt mutatják, hogy nehézkes a közvetlen kapcsolatfelvétel a külföldi internetszolgáltatókkal, azonban néhány esetben angol nyelvű megkeresésre már érdemi válasz érkezett. Az esetek túlnyomó többségében azonban csak bűnügyi jogsegélykérelem keretében lehetséges tőlük adatokat beszerezni.

A gyakorlatban könnyen előfordulhat, hogy mire a jogsegélykérelem átfut, a megkereséssel érintett adatok már rég nincsenek a szolgáltató birtokában. A Cybercrime Egyezmény ugyan lehetővé teszi a tárolt és a forgalmi adatok megőrzésére kötelezést (16–17. cikk), a gyakorlat azonban azt mutatja, hogy ez a jogintézmény nem funkcionál megfelelően. Problémát jelenthet, hogy az IP-cím elfedésére többféle, hozzáértést különösebben nem igénylő lehetőség van. A Tor böngésző például proxyszervereken keresztül bonyolítja a hálózati forgalmazást a végpontok között, és ismertek olyan proxyszerverek, amelyek úgy biztosítanak anonimitást a felhasználónak, hogy a külvilág felé hamis IP-címet mutatnak. Az anonimizáló proxyszerverek láncolatán keresztül technikailag visszafejthető a kapcsolat a hálózati kommunikáció kiindulópontjáig, ez azonban a proxyszerverek tipikusan külföldi elhelyezkedése miatt idő- és erőforrásigényes, ráadásul ha a szerver olyan országban található, mint például Thaiföld vagy Venezuela, a jogsegélykérelem eredménytelen is lehet. Az elkövetői körökben népszerű Tor használata esetén a kapcsolat csak jelentős nehézségek árán, nagy szakértelemmel fejthető vissza.

Kiterjedt *malware*-fertőzés, például botnethálózat esetében az elkövető által használt eszköz, vagyis a rendszer irányítójának azonosítása is többlépcsős folyamat eredménye. Egy botnet hálózati infrastruktúrájának feltérképezése a megfertőzött végpontok (zombik) kommunikációjának megfigyelésén keresztül az irányító szerverek (Command & Control server) meghatározásával lehetséges, ez műszaki tudást és jellemzően több ország nyomozó hatóságainak együttműködését igénylő feladat, a bűnügyi területen zajló nemzetközi együttműködések részletes tárgyalása azonban túlmutat e kötet keretein. Lényegében, ha el akarunk jutni a botnethálózat irányítójához, vissza kell fejtenünk a hálózati kommunikációt több lépcsőben addig, amíg el nem érünk a kiindulópontjáig, ami műszaki értelemben lehetséges, az egyes technikák alkalmazásának viszont nemritkán jogi korlátja van.

Egy, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) által készített tanulmány kifejezetten a botnetek vonatkozásában tárgyalja a felderítéssel, a fertőzöttség mérésével, illetve az ilyen hálózatok felszámolásával kapcsolatos lehetőségeket, azonban az általa javasolt megoldások a legtöbb olyan *malware*-fajtánál

alkalmazhatók, amelynél aktív hálózati kommunikáció zajlik.[741] Az infrastruktúra feltérképezésére a tanulmány aktív és passzív technikákat javasol. Passzív technikák azok az eszközök, amelyek esetében olyan jeleket keresnek, amelyek a botnettevékenységre utalnak, az adatgyűjtés pedig kizárólag megfigyelésen alapul, és nem történik beavatkozás a hálózati kommunikációba. Ezek: adatcsomag-elemzés *(packet inspection),* adatfolyam-analízis (*flow*-rekordok elemzése), DNS-alapú megközelítések, spamlisták elemzése, az applikációk naplófájljainak elemzése, csapdaállítás (*honeypot*ok létrehozása), a vírusirtó szoftverek jelentéseinek elemzése. Az aktív technikák már a megfigyelt eszközökkel történő kapcsolatfelvételt is magukban foglalják, ezek a kifejezetten invazív technikák már nemcsak a hálózat azonosítására adnak lehetőséget, hanem a beavatkozásra és a lekapcsolásra is (például az úgynevezett *sinkholing* technika). A passzív és aktív technikák elhatárolása azért releváns, mert míg a passzív technikák – az alkalmazásukkal okozott jogkorlátozás súlyának figyelembevételével – hagyományos adatszerző tevékenység, illetve titkos felderítés körében alkalmazhatók, az aktív technikák a jog szürkezónájában mozognak, alkalmazásuk pedig egyes országokban kifejezetten tilos. A passzív technikák között is differenciálhatunk a tekintetben, hogy vannak olyanok, amelyek a forgalmazási adatok elemzésén alapulnak, és olyanok is, amelyek a kommunikáció (adatcsomag) tartalmának elemzéséből engednek következtetni a *malware*-fertőzés jellemzőire.

A korábban tárgyalt, forgalmazásra vonatkozó adatok esetében a szolgáltatónak törvényből eredő megőrzési kötelezettsége van bizonyos adatfajták tekintetében, a kommunikáció tartalmának megismerését lehetővé tévő technikák viszont már leplezett eszközöknek (korábban a titkos információgyűjtés, illetve a titkos adatszerzés körébe tartozó eszközöknek) minősülnek. Gyányi Sándor – szintén a botnetek vonatkozásában – kiemeli, hogy a forgalmazási információk elemzése kevésbé erőforrás-igényes, a botnet tagjairól pedig az „adatfolyam jellemzői (forrás- és célcím, portcímek, alkalmazott magasabb rétegbeli protokollok, az adatfolyam időtartama, mérete) árulkodhatnak".[742] A forgalmazási adatok ismerete azonban még nem biztos, hogy elégséges egy hálózat felderítéséhez – Gyányi is rávilágít, hogy azokban az esetekben, ahol a „normális" hálózati kommunikáció közé vegyül a gyanús akció nyoma is, csak igen összetett szűrési módszerekkel lehetne pusztán fejléc-információkból azonosítani a gyanús kommunikációt.[743]

741 Hogben 2011.
742 Gyányi 2011.
743 Gyányi 2011: 109.

A 2018. június 30-áig hatályban lévő szabályok értelmében az elektronikus kommunikáció a nyomozás megkezdését megelőzően titkos információgyűjtés, azt követően pedig titkos adatszerzés keretében volt megismerhető az erre hatáskörrel rendelkező szerveknek. Mind az 1998. évi XIX. törvény, azaz a régi büntetőeljárásról szóló törvény (régi Be.), mind a titkosszolgálati eszközök és módszerek folytatására feljogosított szervek jogállásáról szóló törvények lehetőséget teremtettek a számítástechnikai eszköz vagy rendszer útján továbbított (például LAN) vagy tárolt (például merevlemez) adatok megismerésére, valamint az elektronikus hírközlési szolgáltatás útján továbbított (például a nyílt interneten zajló) kommunikáció megfigyelésére. Az új Be. jelentős mértékben változtatott a szabályokon, és „leplezett eszközök" megnevezéssel összevonta a titkos információgyűjtésre és a titkos adatszerzésre vonatkozó rendelkezéseket, valamint bevezette az úgynevezett előkészítő eljárás intézményét, amelynek célja annak megállapítása, hogy fennáll-e a bűncselekmény gyanúja.

Az új kódexet már a hatálybalépése előtt számos kritika érte, amelyek közül a legnagyobb hangsúlyt kétségtelenül az kapta, hogy az a tény, hogy a nyomozó hatóság az előkészítő eljárás keretében alkalmazhat leplezett eszközöket a bűnügyi felderítéshez, látszólag nem érintette a büntetőeljáráson kívüli titkos információgyűjtésre vonatkozó szabályokat. Ennek kapcsán ismét előtérbe került a bűnügyi és a rendészeti felderítés elválasztásával kapcsolatos, már az előző eljárási kódex rendelkezései kapcsán is folytatott vita. Finszter Géza különbséget tesz a bűncselekmény elkövetőinek és a bizonyítás eszközeinek felkutatását célzó bűnügyi felderítés és a közbiztonságot és a közrendet veszélyeztető tevékenységek elhárítására irányuló rendészeti felderítés között.[744] A felderítés egyes típusai indokolttá teszik az eltérő szabályozást, amihez hozzátartozik a még elfogadható jogkorlátozással járó eszközök körének eltérő meghatározása is.

Ebből az aspektusból vizsgálva, a kiterjedt *malware*-fertőzések, illetve a botnethálózatok igen érdekes kérdéseket vetnek fel. A botnethálózatok esetében a bűnügyi és rendészeti célok kumuláltan vannak jelen. A botnethálózat kiépítésével már eleve a felhasználókat tömegesen érintő jogsértés történik, ezért ezzel szemben indokolt lehet a bűnügyi felderítés eszközeinek alkalmazása. Az ilyen hálózatok végső célja azonban ritkán merül ki fertőzött gépekből álló hálózatok puszta kialakításában, így egy zombigépekből álló hálózat létrehozása tipikusan eszközcselekménye valamilyen egyéb deliktumnak. Ahogy arról korábban esett szó, egy botnet számos további

744 Finszter 2003: 37.

cselekmény elkövetésére, például DDOS-támadások lefolytatására, spamküldésre, tömeges adatvisszaélésre felhasználható, amelyek megelőzése már rendészeti cél.

Aggodalomra ad okot a rendőrségről szóló törvénynek[745] (a továbbiakban: Rtv.) az a 2018 nyarán hatályba lépett rendelkezése, amely lehetőséget teremt arra, hogy a rendőrség a titkos információgyűjtés keretében azonosítsa a kommunikációhoz használt információs rendszert, illetve megszerezze a hollétének megállapításához szükséges adatokat.[746] *Malware*-fertőzések esetén nem tudjuk, hogy a végpontokból kiindulva hány felhasználó kommunikációjának vizsgálata szükséges, amíg eljutunk a megfertőzött rendszerekkel kommunikáló irányítószerverig. Egy botneten belül például nem ritka, hogy 600 ezer végpont *(host)* található – ha csak a töredékük kommunikációját vizsgálják, még az is tömeges jogkorlátozással jár, amelynek elszenvedői ráadásul olyan harmadik személyek, akik semmilyen kapcsolatban nem állnak az elkövetéssel, sőt mivel rendszerük fertőzés áldozata, ők a sértettek. Ilyenkor ráadásul még a bírói engedélyhez kötött eszközök esetében alkalmazandó arányossági tesztet sem kell elvégezni, tehát nem kötelező vizsgálni, hogy az érintett eszköz alkalmazása aránytalanul korlátozza-e az érintett vagy más személy alapvető jogát.

Árnyalja ugyan a képet, hogy az egyes közlések tartalma az internetes kommunikáció csomagkapcsolt jellegéből fakadóan nem fejthető vissza, vagy csak nehezen, hiszen minden közlés részekre bontva érkezik és távozik. Ezenkívül a hálózati kommunikáció vizsgálata során az adatcsomag-elemzést automatizált eszközök végzik, amelyek mintákat keresnek, így képesek a kártékony kommunikációra utaló nyomokat tartalmazó adatcsomagok szűrésére. Ugyanakkor a jogbiztonság szempontjából célszerű lenne tisztázni, hogy az Rtv. e pontja milyen módszerek alkalmazását teszi lehetővé a kommunikációhoz használt információs rendszer azonosítása érdekében bírói engedélyhez nem kötött eszközként, illetve, hogy ez a rendelkezés felhatalmazást ad-e a rendőrségnek arra, hogy egy botnet vagy egyéb *malware* irányító szerverének lokalizálása érdekében olyan leplezett eszközöket alkalmazzon, amelyek egyébként bírói engedélyhez kötött eszközök lennének. További garanciális szabály lehet annak megfogalmazása, hogy az olyan hálózati kommunikáció megfigyelése, amely nagyszámú végpont forgalmát érinti, kizárólag csak olyan automatizált eszközzel történhet, amely megfelelően képes szűrni a *malware*-tevékenységre utaló kommunikációt a hálózaton zajló egyéb forgalomból.

[745] 1994. évi XXXIV. törvény a rendőrségről.
[746] Rtv. 66. § (1) bekezdés e) pont.

Az új Be. és a hatálybalépésekor módosuló ágazati jogszabályok különbséget tesznek az információs rendszer titkos megfigyelése és a lehallgatás között. A két intézmény közötti lényeges különbség, hogy az információs rendszer megfigyelése esetében magának az eszköznek és a benne zajló folyamatoknak a vizsgálata (például alkalmazások naplófájljainak vizsgálata) történik, a lehallgatás ellenben a rendszer elektronikus hírközlő hálózaton folytatott kommunikációjának a megfigyelését teszi lehetővé. A törvény felhatalmazást ad arra, hogy a megfigyelés érdekében a nyomozó hatóság *malware*-t telepítsen a célrendszerre, azonban ezt virágnyelven akként fogalmazza meg, hogy az „ehhez szükséges elektronikus adat az információs rendszerben […] elhelyezhető".[747] A lehallgatás szintén történhet az információs rendszer megfigyelésével, az elektronikus kommunikáció megfigyelése pedig közvetlenül a szolgáltatást biztosító internetszolgáltató segítségével. Mivel a hálózati kommunikáció megfigyelésére a hozzáférést lehetővé tévő hírközlési hálózat üzemeltetőjének rendszerén keresztül van lehetőség, az új Be. az eljárás sikerének érdekében rögzíti, hogy a hírközlési szolgáltatást, információs rendszerben tárolt adatok továbbítását, feldolgozását, kezelését végző szervezetek kötelesek együttműködni a titkos információgyűjtés folytatására, illetve leplezett eszközök alkalmazására törvényben feljogosított szervezetekkel. E szervezetek kötelezettségeiről az Eht. szól részletesen,[748] amely külön cím alatt szabályozza a titkos információgyűjtés és a leplezett eszközök alkalmazása érdekében való együttműködést. A törvény alapján a szolgáltató köteles biztosítani a továbbított küldemények, közlések, kezelt adatok megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit, köteles megfelelő műszaki rendszert, így különösen alapkiépítésű monitoring-alrendszert létesíteni (amelynek költségét a szolgáltató viseli).

A büntetőeljárás keretében alkalmazott leplezett eszközök továbbra is csak meghatározott személyi körrel szemben alkalmazhatók. Leplezett eszközt főszabály szerint azzal szemben lehet alkalmazni, aki gyanúsított, illetve aki bűncselekmény elkövetésével gyanúsítható, ilyen személy azonban a botnet-infrastruktúrák felderítésének megkezdésekor még nincs, és lehetséges, hogy a későbbiek folyamán is csak az irányítószerverig, pontosabban a szerver üzemeltetőjéig jut el a nyomozó hatóság, az elkövetőig már nem. A kiberbűncselekményekről szóló tankönyv is említi azt a problémát, hogy vannak olyan szerverhosting-szolgáltatások, amelyek a szerverszolgáltatás mellett többletszolgáltatásként anonimitást is kínálnak az ügyfeleiknek.[749] Az előkészítő eljárás részeként mással szemben kizárólag akkor lehet leplezett eszközt

[747] Be. 232. § (1) bekezdés.
[748] Eht. 92. §.
[749] Simon 2012: 210.

alkalmazni, ha megalapozottan feltehető, hogy a bűncselekmény elkövetőjeként szóba jöhető személlyel közvetlenül vagy közvetve kapcsolatot tart, vagy ha kívülálló személyt elkerülhetetlenül érint. A *malware*-ek esetében mindkét kitétel meglehetősen rugalmas értelmezést tesz lehetővé, mivel a kártékony szoftverekre építő hálózati infrastruktúráknál technikai értelemben van kapcsolat a sértett fertőzött rendszere és a fertőzést kihasználó elkövető információs rendszere között, ez a kommunikáció azonban sokszor a sértett tudta nélkül folyik. Nyitott kérdés, hogy a sértettek *malware*-rel fertőzött rendszereinek megfigyelése indokolható-e a bűnüldözési érdekre hivatkozással. Az Alkotmánybíróság is rávilágított,[750] hogy a bűnös kapcsolattartás megítélése meglehetősen szubjektív.

A szűk értelemben vett informatikai bűncselekményeket tekintve egyelőre még igen sok a nyitott kérdés, kezdve azzal a problémával, hogy az információs rendszerekkel kapcsolatos bűnözés mint jelenség általánosan elfogadott fogalomrendszerének kidolgozása még várat magára, egészen annak pontos meghatározásáig, hogy a kibertérben folyó nyomozás során meddig terjednek a hatáskörrel rendelkező szervek lehetőségei. Ezeket a kérdéseket vélhetően és remélhetőleg a kiberbűncselekmények nyomozásában jártas szakemberek az eljárások során gyűjtött tapasztalatok alapján megválaszolják majd. Már manapság is többször olvashatunk sikeres, átfogó nemzetközi együttműködésen alapuló megoldásokról: az Europol már több pozitív tapasztalatról is beszámolt, például 2017-ben az Andromeda nevű botnethálózatot sikerült nemzetközi együttműködés keretében lekapcsolni,[751] 2015-ben a Ramnit botnetet,[752] 2014-ben pedig a Gameover Zeust.[753]

Speciális eszközök a határokon átnyúló kiberbűncselekmények nyomozásában

Az online térben megvalósított bűncselekmények csak a legritkább esetekben kapcsolódnak csupán egyetlen országhoz. A tartalomközléssel megvalósított bűncselekmények esetében egyáltalán nem elképzelhetetlen, hogy az elkövető és a sértett eltérő országokban tartózkodnak, kiterjedt *malware*-fertőzéseknél pedig kifejezetten ritka, hogy

750 2/2007. (I. 24.) AB határozat.
751 Andromeda Botnet Dismantled in International Cyber Operation 2017.
752 Botnet Taken Down Through International Law Enforcement Cooperation 2015.
753 International Action Against 'Gameover Zeus' Botnet and 'CryptoLocker' Ransomware 2014.

a fertőzés csak egy országban érint információs rendszereket.[754] A kiberbűncselekmények esetén az elkövetésnek szinte bármelyik mozzanatához kapcsolódhat nemzetközi elem, ez pedig a nemzetközi együttműködés fontosságát kiemelt szintre emeli.

Noha ezt a felismerést mind a nyomozó hatóságoknál dolgozó gyakorlati szakemberek, mind a jogalkotók osztják, a nemzetközi együttműködés mégis számos ponton ütközik nehézségekbe. A nemzetközi együttműködés sajnos lassú és nehézkes. Mezei Kitti hívja fel a figyelmet arra, hogy az olyan esetek kétharmadában, ahol az elektronikus bizonyíték külföldön található, nem lehet rendesen lefolytatni a büntetőeljárást.[755]

A nemzetközi elemet tartalmazó kiberbűncselekmények nyomozásának két neuralgikus pontja van: az egyik a joghatóság megállapítása, a másik pedig az eljárási cselekmények külföldi lefolytatása, a nemzetközi jogsegély. A következőkben ezt a két területet vizsgálom meg részletesen.

Joghatóság a kiberbűncselekmények esetén

A joghatóság lényegében az a rendezőelv, amely az államok közötti ügyeloszlást határozza meg, vagyis amely alapján megállapítható, hogy konkrétan mely ország hatóságainak és bíróságainak joga és kötelessége eljárni. Hazai jogunkban a Btk. rendelkezései alapvetően a területi elvet tükrözik, amely szerint a magyar állam büntetőhatalma az ország területén elkövetett cselekményekre terjed ki.[756] Ismeri emellett a személyi (más néven állampolgársági) elvet is, amely alapján magyar joghatóság alá tartozik a saját állampolgár által külföldön elkövetett bűncselekmény is, amennyiben az a magyar jog szerint bűncselekmény.[757] Kiegészítő elvekként tartalmazza a Btk. a védelmi elvet (állam elleni bűncselekmény esetén a cselekmény magyar joghatóság alá tartozik),[758] illetve az univerzális joghatóság elvét (nemzetközi jog által üldözött cselekmény esetén magyar bíróság is eljárhat). Témánk szempontjából fontos további kiegészítő elv az úgynevezett passzív személyi elv is, amely szerint magyar állampolgár sértett ellen, nem magyar állampolgár által külföldön elkövetett cselekményre

[754] Napjaink népszerű kártékony szoftverei világszerte képesek fertőzni. A Kaspersky biztonsági cég adatai alapján a WannaCry zsarolóvírus mintegy 230 ezer számítógépet fertőzött meg 150 országban.
[755] Mezei 2020b: 230.
[756] Btk. 3. § (1) bekezdés a)–b) pont.
[757] Btk. 3. § (1) bekezdés c) pont.
[758] Btk. 3. §.

is a magyar jog alkalmazandó, ha a cselekmény a magyar jog szerint büntetendő.[759] Ezek a joghatósági szabályok klasszikusan a fizikai térben elkövetett cselekményekre szabottak, például ha a rendőrség talál egy holttestet késsel a mellkasában, egyértelmű vagy legalábbis könnyen megállapítható az elkövetés helye, és feltételezhető, hogy az elkövető is a helyszínen tartózkodott. Az online térben korántsem ilyen egyszerű a helyzet, hiszen a virtuális világban már az elkövetés helyének megállapítása is komoly fejtörést okozhat. Gyűlöletbeszéd esetében például hová tehető az elkövetés helye, a közlő tartózkodási helyére, vagy oda, ahol az érintett személyek lakóhelye van, és az erőszakos cselekmény közvetlen bekövetkezésének veszélye fenyeget? Esetleg abba az országba, ahol az a szerver van, amely a közlést tárolja, vagy annak a közösségimédia-platformnak a székhelye szerinti országba, amely a szervert tulajdonolja?

Nem könnyű kérdések, a magyar törvények rendelkezéseiből pedig nem következik rájuk egyértelmű válasz. A kiberbűncselekményekre speciális jellegüknél fogva több nemzetközi egyezmény, illetve az EU joganyaga is tartalmaz joghatósági szabályokat, az alábbiakban ezeket tekintem át.

Joghatóság a nemzetközi jogban

A 2021-ben 20 éves Cybercrime Egyezmény 22. cikke szól a joghatóságról. A részes országok nemzeti jogához hasonlóan a Cybercrime Egyezmény is a területi elvet tekinti elsődlegesnek, vagyis az állam joghatósága a területén elkövetett bűncselekményekre terjed ki. Másodlagos kapcsolóelvként az elkövető állampolgárságát alkalmazza az Egyezmény, vagyis ha a területi elv alapján nem sikerül megállapítani, melyik országnak van joghatósága, az elkövető állampolgársága szerinti állam is jogosult eljárni. Néhány sorral korábban a gyűlöletbeszéd példáján keresztül részleteztem, hogy miért lehet problémás az elkövetési hely meghatározása az online közegben, amely megnehezíti a területi elv alkalmazását. Tóth Dávid és Gáspár Zsolt hipotetikus példán keresztül illusztrálják a pozitív (több ország kíván eljárni) és negatív (egy ország sem akar eljárni) joghatósági konfliktusokat.[760] A területi elv kritikájaként kifejtik, hogy több esetben előfordul, hogy az elkövetés helye (itt: ahonnan az elkövető végrehajtja a cselekményt) szerinti országban nem is indul büntetőeljárás, mivel az adott ország területén nem volt a cselekménynek sértettje.[761] Ráadásul az elkövető

[759] Btk. 3. § (2) bekezdés b) pont.
[760] Tóth–Gáspár 2020.
[761] Tóth–Gáspár 2020: 144.

VPN használatával könnyen be tudja csapni a helymeghatározó rendszereket, amelyek a használt IP-cím alapján teljesen más országhoz kapcsolhatják az elkövetést, mint ahol az ténylegesen történt.

A kettős inkrimináció elve szintén akadályát jelentheti a büntetőeljárás lefolytatásának, amennyiben más országban követik el a cselekményt, mint ahol az eredmény bekövetkezik. Hazánkban a kettős inkrimináció elve alapján csak abban az esetben szankcionálható külföldi állampolgár nem Magyarországon elkövetett cselekménye, amennyiben a cselekmény a magyar és az érintett ország joga szerint is bűncselekmény. Hasonló elvet a nemzetközi jog alapján számos más ország is alkalmaz, így a büntetőeljárásoknál problémát jelenthet, ha az elkövető cselekménye komoly károkat okoz ugyan, de olyan országból követi azokat el, ahol az adott cselekmény nem bűncselekmény.

A passzív alany állampolgárságára építő másodlagos elv pedig a soksértettes, több országot érintő ügyekben okozhat összeütközéseket,[762] például egy olyan kiterjedt *malware*-fertőzés esete, amely több ország számos számítógépét megfertőzte.

A joghatóság nemcsak a bűncselekmény elkövetőjének felelősségre vonása során okozhat problémát, hanem akkor is, amikor egy bűncselekménynek minősülő tartalom egy olyan szolgáltató szerverén található, amely nem az EU-ban van. Ez esetben a tartalom, az elektronikus adat ideigleges vagy végleges eltávolítására kötelező bírósági vagy más szerv által hozott határozat végrehajtása csakis a szolgáltató jóindulatán múlik.

Joggyakorlat: a LoveBug-ügy tanulságai

A kettős inkrimináció elve képezte akadályát a LoveBug elnevezésű *malware* készítője ellen lefolytatandó büntetőeljárásnak (Rawat 2021; Brenner 2006). A 2000-es években villámgyorsan terjedt el az interneten keresztül egy vírus, amely tömegesen küldött „ILOVEYOU" (szeretlek) tartalmú fertőző e-maileket. A vírus hamar leterhelte a teljes internethálózatot, és több nagyvállalat egész céges levéltárhelyét megtöltötte, nagyjából nyolcmilliárd dollárnyi kárt okozva. A LoveBug kártevő készítőjét hamar sikerült felderíteniük a nyomozó hatóságoknak: egy Fülöp-szigeteki egyetemista, állítása szerint véletlenül, eresztette szabadjára a vírust a világhálón. Hiába az óriási összegű kár, a Fülöp-szigeteknek a 2000-es években nem volt olyan törvénye, amely a *malware*-terjesztést büntetni rendelte volna. A helyi ügyészség megvizsgálta annak a lehetőségét, hogy emelhetnek-e vádat készpénz-helyettesítő fizetési eszközzel visszaélés ügyében, ám arra a következtetésre jutottak, hogy annak semmi köze nincs a számítógépes

762 Tóth–Gáspár 2020: 144.

rendszerek akadályozásához. Mivel nem valósult meg a kettős inkrimináció, az elkövető ellen végül nem emeltek vádat, cselekménye büntetlen maradt (Frank 2000).

Joggyakorlat: Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme, 433 F.3d 1199 (9th Cir. 2006)

A Yahoo-ügyben a joghatóság egy bírósági határozat végrehajthatósága kapcsán merült fel. Az ügy fő kérdése az volt, hogy az amerikai bíróságoknak elő kell-e segíteniük azoknak az ítéleteknek a végrehajtását, amelyeket az USA-n kívüli bíróságok hoztak az Egyesült Államokban honos cégek külföldi leányvállalatainak ügyében. Franciaországban például tilos az önkényuralmi jelképek használata, így egy francia bíróság jogsértőnek találta a náci ereklyék online aukciókon történő értékesítését. A francia diszkriminációellenes nonprofit szervezet, a *La Ligue Contre Le Racisme et l'antisemitisme* pert indított az aukciós oldalt üzemeltető Yahoo ellen, amiért az lehetővé teszi, hogy francia felhasználók is lássák az aukciókat, és licitáljanak az ott meghirdetett termékekre. A Yahoo védekezésképpen arra hivatkozott, hogy amerikai vállalatként a francia jog rendelkezései nem vonatkoznak rá, a francia bíróság azonban nem így látta, és ezer frankos pénzbüntetést szabott ki a vállalatra. A francia bíróság azzal érvelt, hogy ha Franciaország a szolgáltatás célországa, akkor eleget kell tenni a francia jog rendelkezéseinek, és a szóban forgó aukciókat el kell távolítani, vagy a francia IP-címmel internetező felhasználók számára elérhetetlenné kell tenni. A francia hatóságok felvették a kapcsolatot az Egyesült Államokkal a bíróság határozatában foglaltak kikényszerítése végett, amelyre válaszul a Yahoo pert indított. A cég a szólásszabadságot biztosító első alkotmánykiegészítés sérelmére hivatkozva azt állította, hogy a francia bíróság ítéletének végrehajtása az Egyesült Államok területén az amerikai felhasználók szólásszabadságának csorbulásához vezet, mivel az amerikai jog nem tiltja az önkényuralmi jelképek használatát, így a náci emléktárgyak internetes árusítását sem.
Az 9th Circuit Court fellebbviteli fórumként eljárva végül arra jutott, hogy amerikai bíróságoknak nincs joghatóságuk egy francia szervezet elleni perben döntést hozni, a kérdés érdemi tárgyalásáig tehát el sem jutottak. Az ehhez hasonló joghatósági problémák természetesen azzal a következménnyel járnak, hogy a bírósági határozat külföldön végeredményben kikényszeríthetetlen.

Brenner és Koops szerint a problémát alapvetően nem az okozza, hogy vannak joghatósági viták az országok között, hanem az, hogy nincsenek egységes mechanizmusok, amelyek segítséget nyújtanak annak megállapításához, hogy mely országhoz kötődik a legszorosabban a cselekmény, s így feloldanák a konfliktust.[763] A Cybercrime Egyezmény mindössze javaslatot tesz arra, hogy az országok a vitás kérdéseket egyeztetés

[763] Brenner–Koops 2004: 1–46.

révén oldják fel,[764] azonban ennek elmaradásához nem rendel jogkövetkezményt. Célszerű lehet tehát olyan nemzetközi testület felállításában gondolkodni, amely döntést tud hozni hasonló kérdésekben, vagy legalábbis amelyhez az Egyezmény részes országai útmutatásért fordulhatnak.

Joghatóság az Európai Unióban

Az EU területén ennél összetettebb joghatósági szabályok érvényesülnek, az egyes uniós aktusok ráadásul az egyes cselekményekre külön-külön szabályokat állapítanak meg.

A tisztán informatikai bűncselekmények (jogosulatlan hozzáférés, beavatkozás a rendszer működésébe és az adattal kapcsolatos visszaélések) esetében a 2013/40/EU irányelv rendezi a joghatósági kérdéseket. Az irányelv 12. cikke értelmében a területi elv és az állampolgársági elv közösen érvényesül, vagyis egy tagállamnak akkor is van joghatósága eljárni, ha a cselekményt részben vagy egészben a területén követték el, és akkor is, ha azt egy állampolgára követte el. Az elkövetés helyét az irányelv igen tágan értelmezi, helyesen, hiszen ezzel elébe megy annak a problémának, amely szerint a virtuális térben elkövetett cselekmények esetén az elkövetés valójában több helyhez is kapcsolódhat egyszerre. Az irányelv szerint akkor is tagállam területén elkövetettnek minősül a cselekmény, ha az elkövető fizikailag annak területén tartózkodik az elkövetéskor, és akkor is, ha az elkövető ugyan másutt van, de az információs rendszer, amely ellen a cselekményt elkövetik, a tagállam területén található. Az elkövetési hely kiterjesztéséből az a probléma fakadhat, hogy egyszerre több tagállam tekinti a cselekményt a saját területén elkövetettnek. Ez tipikusan akkor fordul elő, ha az elkövető és a cselekménnyel érintett információs rendszer különböző tagállamokban vannak, de akkor is lehetséges, ha az elkövető célpontjai nemcsak a saját tartózkodási helye szerinti tagállamban, hanem számos más országban voltak (például egy számítógépes vírus terjesztése esetén). Ezekben az esetekben a tagállamok közötti egyeztetésen múlik, hogy melyikük fogja lefolytatni a büntetőeljárást, célszerű azonban olyan ország joghatóságában megállapodni, amelyhez az ügy a legszorosabban kapcsolódik.

A 2011/93/EU irányelv a gyermekpornográfiát, valamint a gyermekkel való szexuális tartalmú kapcsolatfelvételt *(grooming)* rendeli büntetni a tagállamokban. Az irányelv által szabályozott cselekmények eredményes üldözése érdekében az irányelv a joghatóság megállapításának közös szabályait is rendezi. E cselekmények tekintetében

[764] Cybercrime Egyezmény 22. cikk 5. pont.

szintén elsődleges a területi és az állampolgársági elvek kombinált alkalmazása. Egy tagállam eljárhat, ha a cselekményt részben vagy egészben a területén követték el,[765] illetve ha az elkövető az állampolgára.[766] Kiegészítő elvként a tagállamok diszkrecionális jogkörükben dönthetnek úgy, hogy megállapítják joghatóságukat akkor is, ha a fenti feltételek nem teljesülnek. Erre az alábbi esetekben van lehetőség:

- ha a sértett lakóhelye vagy tartózkodási helye az adott tagállam területén található;
- ha a cselekményt olyan jogi személy javára követték el, amely az adott államban telepedett le; valamint
- ha az elkövető szokásos tartózkodási helye a tagállamban van.[767]

Mivel a cselekmény sértettjei kiskorúak, érthető és logikus lépés az állampolgárságuk szerinti tagállamnak biztosítani az eljárás lehetőségét, hiszen egy idegen nyelven, adott esetben távoli országban zajló eljárás, az idegen és akár többször megismételt eljárási cselekmények (például tanúkihallgatás) további traumát okozhat a sértettnek, akinek a legfőbb érdeke, hogy az eljárás a hozzá legközelebbi helyen, megszokott, biztonságos keretek között folyjék. Az irányelv a kettős inkrimináció elvét is lerontja azáltal, hogy úgy rendelkezik, hogy a tagállam joghatósága nincs alárendelve annak a feltételnek, hogy a cselekmény az elkövetés helyén is bűncselekménynek minősüljön.

A 2019/713/EU irányelv szabályozza a materiális és immateriális készpénz-helyettesítő fizetési eszközök csalárd felhasználását, valamint az információs rendszerekkel kapcsolatos csalást. A joghatóságot megállapító rendelkezések nem térnek el az EU egyéb, kiberbűncselekményekkel foglalkozó jogi aktusaiban fellelhető rendelkezésektől, tehát az elsődleges ugyanúgy a területi és az állampolgársági elvek alkalmazása.[768]

A joghatósággal kapcsolatos egyik fő kérdés napjainkban, hogy az egyik tagállam kötelezhet-e egy másik tagállamban letelepedett szolgáltatót bizonyos intézkedések megtételére, illetve az ilyen jellegű kötelezéseknek milyen joghatásuk van a nemzeti jogban. A nemzetközi vonatkozású ügyekről szóló előző pontban láthattuk, hogy egy európai ország határozatainak kikényszerítésére az USA-ban nem sok esély van. Az Európai Unióban valamelyest eltérő a helyzet, ugyanis lehetőség van a határozatok

765 17. cikk (1) a).
766 17. cikk (1) b).
767 17. cikk (2).
768 12. cikk (1).

külföldi végrehajtására az Európai Unió általános hatályú, közvetlenül alkalmazandó kötelező jogi aktusa, törvény, kormányrendelet vagy viszonosság alapján.[769]

Hagyományosan ezeket a határozatokat a társhatóság (a külföldön hatáskörrel rendelkező hatóság) bevonásával kell végrehajtani, az utóbbi években jól megfigyelhető tendencia, hogy az Unió azzal igyekszik elsősegíteni a jogellenes tartalmak elleni hatékonyabb fellépést, hogy a tagállamok számára megengedi a más tagállam területén letelepedett jogi személyek közvetlen kötelezését. Jó példa erre az Európai Parlament és a Tanács 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről, amely lehetőséget ad arra, hogy a tagállamok illetékes hatóságai eltávolítási végzéseket bocsássanak ki más tagállamokban letelepedett közvetítő szolgáltatók szerverein található tartalmak eltávolítása esetében. Ezek az eltávolítási végzések jellemzően nem illeszkednek bele a büntetőeljárás hagyományos rendszerébe, hiszen nem büntető-eljárásjogi kényszerintézkedésekről van szó (mint például a belföldi elektronikus adat ideigleges eltávolítása esetében), amelyek büntetőeljárási jogsegély igénybevételével hajthatók végre külföldön, hanem közigazgatási határozatokról. A szolgáltatóknak az eltávolítási végzést kötelező végrehajtaniuk. A gyermekek szexuális bántalmazása elleni fellépésről szóló rendelet tervezetében található eltávolítást és a hozzáférés letiltását elrendelő végzések esetében előreláthatólag hasonló szabályozási logika érvényesül majd. Ez természetesen nem jelenti azt, hogy a szolgáltató felett joghatósággal rendelkező tagállam teljesen eszköztelen, hiszen akár saját kezdeményezésére, akár a szolgáltató jelzése alapján megvizsgálhatja az eltávolítási végzést, és amennyiben azt a rendelet szabályaiba vagy az EU Alapjogi Chartájába ütközőnek találja, rendelkezhet annak érvénytelenségéről. Az egyelőre nyitott kérdés, hogy a szuverenitásról szóló tanokkal hogyan egyeztethető össze egy ilyen lépés.

Hasonló eszközöket tartalmaz a DSA is, amely alapján lehetőség van a jogellenes tartalom elleni fellépésre vonatkozó, valamint az információközlésre kötelező határozatot megküldeni bármely tagállam közvetítő szolgáltatóinak, azzal, hogy ezeknek a határozatoknak a végrehajtása eleve nem kötelező. A szolgáltatók azt megvizsgálják, és ezt követően tájékoztatják a kibocsátó nemzeti igazságügyi vagy közigazgatási hatóságot a határozatban foglaltak végrehajtásáról, illetve a végrehajtás terjedelméről.

[769] Boros 2016.

Nemzetközi jogsegély a kiberbűncselekmények esetén

Ha egy cselekmény külföldi elemet tartalmaz, általában más állam bíróságát vagy hatóságát kell megkeresni a szükséges eljárási cselekmények foganatosítása érdekében, ezt hívjuk jogsegélynek. A nemzetközi jogsegélynek nincsenek egységesen, minden ország vonatkozásában használatos eljárási szabályai, az egyes országokkal való ilyesfajta kapcsolatot, illetve az egyes jogterületekre vonatkozó szabályokat bi- vagy multilaterális egyezmények külön-külön tartalmazzák. Ezek a jogsegélyegyezmények általában nem egy bűncselekménycsoportra fókuszálnak, hanem általánosságban véve a határokon átnyúló nyomozás eljárási szabályaira.[770] Ezekben a jogsegélyegyezményekben tehát olyan szabályokat nem találunk, amelyek külön a kiberbűncselekmények sajátosságaira – különösen az online tér bizonyítékainak illékony természetére – figyelemmel szabályoznák a büntetőeljárási cselekményeket. Ezzel együtt az elektronikus kommunikáció elterjedtsége miatt manapság nehezen képzelhető el olyan bűncselekmény, amelynek nem marad valamilyen nyoma a virtuális térben, vagy valamilyen hírközlési szolgáltató rendszerében. A jogsegélyegyezmények bizonyítékok megszerzésére vonatkozó rendelkezései ezért többnyire foglalkoznak valamilyen formában a hírközlési vagy más információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatóknál tárolt adatok megszerzésével, megőrzésével, illetve eltávolításával.

Jogsegély az Európai Unió tagállamai között

Az EU tagállamai közötti bűnügyi együttműködésre vonatkozó szabályoknak az EU tagállamai közötti bűnügyi jogsegélyről szóló egyezmény[771] (a továbbiakban: Jogsegélyegyezmény) ad keretet. Mivel nemzetközi egyezmény, és nem klasszikus uniós jogforrás, elfogadásához tagállami ratifikálásra volt szükség.[772] A Jogsegélyegyezmény egyik legjelentősebb eredménye, hogy megteremti annak a lehetőségét, hogy bűnügyi jogsegély esetében a tagállamok igazságügyi hatóságai közvetlenül lépjenek kapcsolatba

[770] Például a 2006. évi XL. törvény a Magyar Köztársaság Kormánya és az Amerikai Egyesült Államok Kormánya között a kiadatásról és a kölcsönös bűnügyi jogsegélyről szóló, Budapesten, 1994. december 1-jén aláírt szerződések módosításáról szóló szerződések kihirdetéséről.

[771] Egyezmény a Tanács által az Európai Unióról szóló szerződés 34. cikkének megfelelően létrehozott, az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről.

[772] Villányi 2003: 215.

egymással. Erre korábban az igazságügyi minisztériumok közreműködésével volt lehetőség, ami rendkívüli módon lassította az eljárásokat. A nemzetközi együttműködés az egyezmény ellenére is sokszor lassú és nehézkes.

A Jogsegélyegyezménynek nem célja, hogy teljesen, átfogó jelleggel rendezze az EU tagállamai közötti jogsegély szabályait, ezt már az 1. cikk is világosan tükrözi, amely azt rögzíti, hogy az egyezmény csak egyéb nemzetközi egyezmények szabályait kívánja kiegészíteni, hogy ezáltal hatékonyabbá tegye a nemzetközi együttműködést. A Jogsegélyegyezmény az 1959. április 20-i kölcsönös bűnügyi jogsegélyről szóló egyezmény, annak 1978. március 17-i kiegészítő jegyzőkönyve, valamint az 1985. évi Schengeni Végrehajtási Egyezmény és a Benelux-szerződés szabályaihoz fűz kiegészítéseket. A Jogsegélyegyezmény szabályait tehát nem önmagukban, hanem a megjelölt további egyezmények szabályaival szerves egységben lehet és kell vizsgálni és értelmezni. A Jogsegélyegyezmény azt is rögzíti, hogy ha vannak olyan tagállamok közötti egy- vagy többoldalú megállapodások, amelyek kedvezőbbek a Jogsegélyegyezmény szabályainál, akkor ezek rendelkeznek primátussal, így felülírhatják az abban rögzítetteket.

A Jogsegélyegyezmény további részei a jogsegélykérelmekkel kapcsolatos eljárási rendelkezéseket, valamint néhány különös eljárási cselekményt szabályozó rendelkezést tartalmaznak: a 4. cikk a megkeresés alaki követelményeivel, 5. cikke az eljárási iratok kézbesítésével, a 6. cikk a jogsegély iránti megkeresések megküldésével kapcsolatos szabályokat tartalmazza, a 7. cikk pedig a megkeresés nélküli iratcseréről szól. A kiberbűnözés szempontjából különös jelentősége a különleges eljárási cselekményeket szabályozó rendelkezéseknek van. A közös nyomozócsoportok felállításáról szóló 13. cikk lehetővé teszi, hogy a tagállamok közösen nyomozzanak határon túli elemet tartalmazó bűncselekmények, valamint az olyan bűncselekmények esetében, amelyek esetében összehangolt és egyeztetett fellépésre van szükség. A közös nyomozócsoport tagjai megkereshetik saját illetékes hatóságaikat, illetve a csoporton belül közvetlenül információt szolgáltathatnak. Kiegészítő rendelkezéseket tartalmaz az egyezmény a távközlés lehallgatásával kapcsolatban is, amelyek alapján lehetőség van lehallgatást kezdeményezni akkor is, amikor az intézkedéssel érintett személy nem abban az országban tartózkodik, ahol a nyomozás folyik, illetve amikor abban a tagállamban tartózkodik ugyan, de a lehallgatáshoz más ország technikai segítségnyújtása szükséges.

A Jogsegélyegyezményhez 2001-ben kiegésző jegyzőkönyvet[773] fűztek, amelynek elsődleges célja a szervezett bűnözés, a pénzmosás és a pénzügyi bűncselekmények

[773] 2005. évi CXVI. törvény az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló, 2000. május 29-én kelt egyezmény és az egyezmény 2001. október 16-án kelt kiegészítő jegyzőkönyve kihirdetéséről.

elleni fellépés. A kiegészítő jegyzőkönyv így főként a pénzmozgások felderítésével kapcsolatos eljárásokat szabályozza, köztük a bankszámlákra és a banki műveletekre vonatkozó információkérést, valamint a banki műveletek ellenőrzése iránti megkeresést.

Más tagállamban letelepedett internetes közvetítő szolgáltatók megkeresése

Az informatikai bűncselekmények esetében gyakran előfordul, hogy az adatkéréssel, megőrzéssel, az elektronikus adatok hozzáférhetetlenné tételével kapcsolatban megkeresni kívánt szolgáltató nem abban a tagállamban található, mint a megkereső szerv (a Facebook és a Google európai központjai például Írországban vannak, így e cégek ír joghatóság alá tartoznak). Az ilyen megkeresések esetében az elintézés eredményességét rontó tényező, ha a megkereséseket központi hatóságok bonyolult rendszerén keresztül előterjesztve kell eljuttatni a szolgáltatókhoz. Több uniós jogi aktusban is találunk olyan szabályokat, amelyek lehetővé teszik azt, hogy az egyes tagállamok megkereséseikkel közvetlenül a szolgáltatókhoz forduljanak, a letelepedés helye szerinti tagállam hatóságainak kihagyásával. Vizsgálódásunk előtt mindenképpen indokolt rögzíteni, hogy a terület jelen sorok írásakor jelentős reform alatt állt. 2022-ben fogadták el a DSA-t, amely a közvetítő szolgáltatók esetében vezette be a jogellenes tartalmak elleni fellépésre vonatkozó végzések, valamint az információszolgáltatásra vonatkozó végzések intézményeit. Ezenfelül az EU két másik jogalkotási aktus elfogadására is készült: az egyik a gyermekek szexuális bántalmazása elleni fellépést fejleszteni kívánó rendelettervezet, a másik pedig az elektronikus bizonyítékok összegyűjtésének hatékonyabb eszközeit, a közlésre kötelező európai határozatot és a megőrzésre kötelező európai határozatot szabályozó rendelettervezet.

Az összes felsorolt dokumentumban nagy a hangsúly a közvetlenségen, mind a DSA, mind az rendelettervezetek kiemelt kérdésként kezelik a határokon átnyúló bizonyítás eredményességét elősegítő információáramlást. A szabályozott, illetve szabályozni kívánt határozatokat és végzéseket a tagállamok arra kijelölt szerveinek közvetlenül a szolgáltatókhoz kell eljuttatniuk, ami a jogalkotó elképzelése szerint jelentősen gyorsítja majd a bizonyítékok összegyűjtését. Jómagam némiképp nagyobb szkepticizmussal tekintek az uniós jogalkotás eme vívmányaira, hiszen azt, hogy melyik határozatot melyik szerv jogosultsága lesz kibocsátani, már attól függ, hogy a tagállamok belső jogukban az intézményrendszer melyik elemére telepítik ezt a hatáskört. A gyakorlatban mindenesetre a hírközlést, a médiaszolgáltatásokat, a nyomozással és bizonyítási eljárással összefüggő ügyeket sohasem ugyanazok a szervek intézik, így

az előbbiekben felsorolt határozatok és végzések kibocsátása igen nagy valószínűséggel különböző szervek hatáskörébe fog tartozni. Megfelelő koordináció és kommunikáció híján könnyen előállhat olyan helyzet, hogy ugyanazon jogellenes tartalom vonatkozásában több szerv többféle intézkedés megtételére felhívó határozatot hoz, ami egyrészt csökkenti az átláthatóságot, másrészt növeli mind a tagállami hatóságok, mind a szolgáltatók munkaterhét.

Jogsegély az Európai Unió tagállamai és harmadik országok között

Az EU tagállamai és a harmadik országok közötti jogsegélyre továbbra is a központi hatóságokon (Magyarországon az Igazságügyi Minisztériumon) keresztül van lehetőség. Ennek menetét a 7. ábra szemlélteti.

Mint látható, a jogsegélykérelem elintézése több eljárási lépcsőben történik, ami nemcsak idő-, de erőforrás-igényes is.

A büntetőeljárás nyomozati szakaszában gyakran merülnek fel a bizonyítással kapcsolatos jogsegély iránti megkeresések. Számítógépes környezetben főként az adat megszerzésére kötelezés, valamint a hozzáférés biztosítása releváns eszközei a távoli helyeken fellelhető bizonyítékok összegyűjtésének. A Cybercrime Egyezmény eljárásjogi rendelkezései körében szól az elektronikus bizonyítékokkal kapcsolatos minimumszabályokról, amelyeket minden részes államnak be kell vezetnie a saját jogrendszerébe.

7. ábra: *A jogsegély menete az EU-tagállamok és harmadik országok között*

Forrás: European Commission 2018

A Cybercrime Egyezmény alapján a részes államoknak lehetővé kell tenniük a rendszerben tárolt számítástechnikai adatok (ideértve a forgalmi adatokat) gyors megőrzésének elrendelését,[774] valamint a közlésre kötelezést, azaz a területükön tartozkodó személyek kötelezését a rendszerben vagy az adathordozón tárolt adatok átadására és az információs szolgáltatókat az előfizetőkre vonatkozó és a forgalmi adatok átadására. A Cybercrime Egyezmény kimondottan rendelkezik az informatikai bűncselekmények esetében nyújtott jogsegélyről is, azzal, hogy a legszélesebb körű együttműködésre buzdítja a részes államokat ezen a területen. A Cybercrime Egyezmény nem kíván a bilaterális jogsegélyegyezmények helyébe lépni, így kimondja, hogy ha két állam között van hatályban jogsegélyegyezmény, akkor elsősorban ennek a szabályait kell alapul venni az informatikai bűncselekmények esetében folytatott nyomozás és bizonyítás során. Ha azonban két olyan országról van szó, amelyek részesei a Cybercrime Egyezménynek, ám közöttük nincsen jogsegély-megállapodás, akkor az Egyezmény szabályai kötelezőek rájuk nézve. A részes államok kötelesek kijelölni olyan központi hatóságokat, amelyek feladata az informatikai bűncselekményekkel kapcsolatos jogsegélykérelmek intézése, ideértve azok küldését, fogadását és a válaszadást. A Cybercrime Egyezmény jogsegélyről szóló szabályai értelmében jogsegély keretében az alábbi intézkedések megtétele kérhető a részes államoktól:

- tárolt számítástechnikai adat gyors megőrzése;
- megőrzött forgalmi adat gyors átadása;
- tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély;
- forgalmi adat valós idejű összegyűjtésével kapcsolatos jogsegély;
- tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély.

Arról azonban már nem szólnak a Cybercrime Egyezmény szabályai, hogy milyen forgalmi adatokat és mennyi ideig kell tárolniuk az államoknak, e tekintetben tehát meglehetősen sokféle szabályozási megoldással találkozhatunk, ha olyan országokra tekintünk, amelyek nem tagjai az Európai Uniónak. Nemegyszer fordul elő a gyakorlatban, hogy mire a jogsegélykérelem a megkeresett országba érkezik, az már csak arról tudja tájékoztatni a megkeresőt, hogy a megőrzési kötelezettség időtartama a saját belső jogszabályai szerint eltelt, így a kért adatokat törölték. Ez többnyire az elkövetők malmára hajtja a vizet, akik tudatosan letelepedhetnek olyan országokban, ahol a megőrzés időtartama alapvetően rövid.

774 Cybercrime Egyezmény 16. cikk.

A felhőszolgáltatások népszerűsége szintén okoz fejtörést a nyomozó hatóságoknak, hiszen a felhőalapú adattárolás lényege, hogy az adatok akár több országban, több szerveren vannak jelen. Ez történhet akár úgy is, hogy a teljes büntetőeljárással érintett adatnak több másolata található több szerveren, vagy akár úgy is, hogy annak egyes részei szétszórtan találhatók meg.

United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018)

Az Egyesült Államokban a United States v. Microsoft Corp. ügyben merült fel a kérdés, hogy egy ország területén letelepedett szolgáltató köteles-e adatszolgáltatást teljesíteni abban az esetben, ha a nyomozó hatóság által kért adatokat más országban tárolja. Az Egyesült Államokban a nyomozó hatóság egy alkalommal egy kábítószer-csempészet ügyében folyó eljárás kapcsán kérte a céget bizonyos adatok átadására. A Microsoft a forgalmi adatokat ugyan átadta, de a tartalmi adatokat (e-mail-üzeneteket) nem, arra hivatkozva, hogy azokat írországi adatközpontjában tárolja. Az ügyben másodfokon eljárt 2nd Circuit Court úgy határozott, hogy az ilyen lefoglalást elrendelő határozatok területi hatálya kizárólag az Egyesült Államok területére terjed ki. A Legfelsőbb Bíróság végül megsemmisítette az ítéletet, és új lefoglalási határozat kiadását javasolt a nyomozó hatóságnak, mivel időközben a kongresszus elfogadott egy felhőszolgáltatásokról szóló törvényt (Clarifying Lawful Overseas Use of Data Act – CLOUD Act), amely az adatok átadását kötelezővé teszi abban az esetben is, ha azokat külföldön tárolják. Érdekessége az ügynek, hogy Írország, ahol a szóban forgó adatokat tárolták, *amicus curiae*-t terjesztett elő, amelyben jelezte, hogy a harmadik országba történő adattovábbítás ellentétben áll az EU általános adatvédelmi rendeletével (GDPR), valamint az ír joggal is, hiszen az adatokat az USA hatóságainak az USA és Írország között fennálló jogsegélyegyezmény szabályai szerint kellett volna kérniük, nem pedig közvetlenül a cégtől. Az Európai Adatvédelmi Testület egyébként a CLOUD Act szabályait uniós jogba ütközőnek tekinti, mindezt annak ellenére, hogy az EU, ahogy alább is látni fogjuk, maga is a közvetlenség elvét hangsúlyozza a határokon átnyúló bizonyításban.

Vákát oldal

VII. Az internetes közvetítő szolgáltatók szerepe és felelőssége a kiberbűncselekmények felderítésében és nyomozásában

Egyre gyakrabban hangzik el a sajtóban és a közéleti vitákban, hogy a kisebb-nagyobb techcégeknek hozzá kell járulniuk az internet *jogszerű,* illetve *helyes* működéséhez. A kijelentés és a hozzá kapcsolódó, a vállalkozások, tevékenységek állami szabályozására, esetleg a vállalatok önszabályozásának erősítésére tett ígéretek ugyan hangzatosak, de gyakran nem váltják be a hozzájuk fűzött reményeket. Nem csoda, hiszen már akkor komoly nehézségekkel találjuk szembe magunkat, ha meg kívánjuk határozni, hogy mikor működik jogszerűen egy nemzetek felett álló – pontosabban azokat összekapcsoló –, ezerféle eszközből álló globális hálózat. Melyik ország vagy nemzetközi szervezet szabályai képezhetnék azt a mércét, amelyhez a *helyes* működést viszonyítjuk? Képesek lennénk-e egyáltalán megalkotni egyetlen, az internetre vonatkozó szabályrendszert, amely szükségképpen együtt járna azzal, hogy az államok szuverenitásukat részben feladva alávetik magukat egy közösen kidolgozott normarendszernek? Az elmúlt években – ahogy Klein Tamás is felhívja erre a figyelmet[775] – eljutottunk odáig, hogy az internetre már nem jogmentes területként tekintünk, az viszont, hogy az online térre is afféle *res communis omnium usus*ként tekintsünk, mint mondjuk

[775] Klein 2018a.

a világűrre, még várat magára. Az internet mint infrastruktúra fizikai és matematikai törvényszerűségeken alapuló, nemzetközi szinten is szabványosított műszaki megoldások halmaza, tehát alapvetően nem magának az internetnek a helyes működését kell biztosítani, hanem a világháló használata során tanúsított magatartásokra szükséges hatást gyakorolni. A világháló használata során tanúsított magatartások azok, amelyek jogellenesek lehetnek, s ezzel sérthetik a többi felhasználót, illetve befolyásolhatják a hálózatot alkotó műszaki berendezések rendeltetésszerű működését. Ennélfogva a szabályozási kérdések fókuszpontjában többnyire nem az infrastruktúra működése, hanem az infrastruktúra használata áll. Az internet működésében számos szereplő játszik fontos szerepet: vannak szolgáltatók, amelyek a hálózati infrastruktúrát üzemeltetik, és hozzáférési pontokat építenek ki, vannak olyanok, amelyek tárhelyet biztosítanak az információk tárolásához, vannak olyanok, amelyek az online térben való eligazodást könnyítik meg, továbbá olyan szolgáltatókat is találunk, amelyek maguk is igénybe veszik az előbbi szolgáltatások valamelyikét, hogy aztán saját tartalmaiknak és a felhasználóik interakciójának biztosítsanak felületet. Egy felhasználó a böngészés során a felsorolt szolgáltatások közül akár az összeset igénybe veheti, úgy, hogy ennek nem szükségszerűen van tudatában. Ha valahol emberölés történik, a rendőrséget hívjuk, nem az épület tulajdonosát. Miért tennénk hát másként az online környezetben, amelyben az állam büntető igényének érvényesítésére szintén az igazságszolgáltatás szervei jogosultak? Ugyanakkor egyes szolgáltatóknak olyan befolyása van az infrastruktúrára, illetve annak egyes elemeire, hogy közreműködésükre szükség van a nyomozás során. Amellett, hogy a szolgáltatók – jellemzően törvényi kötelezettségből fakadóan – kötelesek segíteni a nyomozó hatóság munkáját, és egyes kényszerintézkedéseket is maguk hajtanak végre, elképzelhető, hogy maguk is felelőssé tehetők a harmadik személyek által továbbított információkért. A szolgáltató érdeke nyilvánvalóan azt kívánja, hogy ő maga mentesüljön a felelősség alól, a büntetőeljárás érdeke pedig azt, hogy a bűncselekmény elkövetője felelősségre vonható legyen. Ideális esetben ez a két érdek egymással párhuzamos, a szolgáltató azáltal, hogy teljesíti jogszabályban foglalt kötelezettségeit, és segíti a nyomozó hatóság munkáját, megalapozza saját mentesülését is. Elképzelhetők viszont olyan esetek, amikor a szolgáltató és a nyomozó hatóság érdekei konkurálnak: egyes szolgáltatóknak nem áll érdekében hozzájárulni a nyomozás eredményességéhez, hiszen amennyiben felvállalják, hogy bizonyos információkról tudomásuk volt, elveszítik az ágazati jogszabályok által biztosított felelősség alóli mentesülés lehetőségét. Jelen rész azokat a kérdéseket igyekszik körbejárni, amelyeket a közvetítő szolgáltatók kettős és néhol ellentmondásos szerepe felvet.

A büntetőeljárás egyéb szereplőinek helyzete az új Be. rendelkezéseinek tükrében, a közvetítő szolgáltatók büntetőeljárásbeli pozíciója

A közvetítő szolgáltató elnevezés nem egyfajta szereplőt illet, hanem az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatók egy jogszabály által meghatározott csoportjára vonatkozik. A közvetítő szolgáltatók egymástól való következetes elhatárolása a tárgyalt téma szempontjából azért különösen fontos, mert az egyes szereplők viszonyulása a jogsértő információkhoz, ennek okán pedig a nyomozásban való közreműködésük és a felelősségük léte és mértéke eltérő lehet. A közvetítő szolgáltatók fajtáit az Ekertv. az Eker. irányelvhez hasonlóan, annál valamivel bővebben állapítja meg. Közvetítő szolgáltatónak minősül:

- az egyszerű adatátvitelt és hozzáférést biztosító szolgáltató,
- a gyorsítótároló szolgáltató,
- a tárhelyszolgáltató,
- a keresőszolgáltató, valamint
- az alkalmazásszolgáltató.[776]

A DSA rendelet a listát az online platform fogalmával egészítette ki.[777] Röviden indokolt szólni az elektronikus hírközlési szolgáltató fogalmáról is, mivel a későbbiekben tárgyalt Be. rendelkezései a kötelezettségek alanyaként sok esetben ezeket a szolgáltatókat említik. Az Eht. értelmező rendelkezései alapján az elektronikus hírközlési szolgáltatás fő ismérve, hogy az teljesen vagy nagyrészt jeleknek elektronikus hírközlési hálózaton történő átviteléből, és ahol értelmezhető, irányításával jár.[778] Eszerint van átfedés a közvetítő szolgáltatók és az elektronikus hírközlési szolgáltatók között: az egyszerű adatátvitelt és hozzáférést biztosító közvetítő szolgáltatók, tehát az internetszolgáltatók elektronikus hírközlési szolgáltatónak is minősülnek.

Az új Be. az eljárás résztvevőinek körét kiegészítette a vagyoni érdekeltek, illetve az egyéb érdekeltek kategóriáival is, a közvetítő szolgáltatók pedig tevékenységüktől függően bármelyik szerepkörben megjelenhetnek. Vagyoni érdekelt lehet a szolgáltató, ha elkobozható vagy lefoglalt dolog, például szerver vagy más adathordozó tulajdonosa (gyakorlatilag bármelyik közvetítő szolgáltató), vagy olyan elektronikus adattal rendelkezésre jogosult, amelynek végleges hozzáférhetetlenné tétele

776 Ekertv. 2. § l. pont.
777 DSA 3. cikk i) pont.
778 Eht. 188. § 14. pont.

rendelhető el (tárhelyszolgáltató).[779] Egyéb érdekeltként vehet részt az eljárásban a közvetítő szolgáltató, amelynek jogára vagy jogos érdekére a büntetőeljárásban hozott határozat közvetlen hatással van, vagy amely az őt érintő eljárási cselekménynyel összefüggésben a Be. által meghatározott jogosultsággal vagy kötelezettséggel rendelkezik.[780] Ahogy azt a fejezet következő részeiben látni fogjuk, a közvetítő szolgáltatók e feltételeknek maradéktalanul megfelelnek. A Be. több kötelezettséget is megfogalmaz a szolgáltatók számára, amelyekkel összefüggésben a szolgáltatói felelősség kérdésével is indokolt foglalkozni.

Az internetes közvetítő szolgáltatók részvétele az egyes kényszerintézkedések végrehajtásában

A közvetítő szolgáltatókkal szemben az az általánosan megfogalmazható elvárás, hogy ne korlátozzák, hanem inkább segítsék a nyomozó hatóság munkáját. Jogrendszerünk nem bízza a szolgáltatókra annak eldöntését, hogy milyen mértékben kívánnak közreműködni a nyomozó hatóság munkájában, mind a büntetőeljárási törvény, mind az elektronikus hírközlésről szóló törvény kifejezetten a nyomozással kapcsolatos kötelezettségeket telepít a szolgáltatókra. Ezek a rendelkezések több ponton kiegészülnek az EU szabályaival, amelyek meghatározzák, hogy bizonyos súlyos bűncselekmények (például a gyermekek szexuális bántalmazását ábrázoló tartalmak) esetében mit kell tenniük az egyes szolgáltatóknak. Az alább részletesen is tárgyalt kötelezettségek nem egyaránt vonatkoznak az összes közvetítő szolgáltatóra, azonban nem minden esetben egyértelmű, hogy egyes előírások miért csak bizonyos szolgáltatókra vonatkoznak, s más szolgáltatókat miért nem terhelnek azonos vagy legalábbis hasonló kötelezettségek. A bemutatott kötelezettségek teljesítésének elmulasztásához az azokat előíró jogszabályok sok esetben jogkövetkezményeket is kapcsolnak, ezért joggal merül fel a kérdés, hogy ezek megtételének elmulasztása szükségszerűen eredményez-e a más által rendelkezésre bocsátott információért való felelősséget az olyan esetekben, amelyekben egyébként a szolgáltató az Eker. irányelv és törvény szerinti kimentési okokra hivatkozhatna.

[779] Be. 57. § (1) bekezdés.
[780] Be. 58. § (1) bekezdés.

Adatszolgáltatás, adatmegőrzés

Kiindulópontként a Be. annyit rögzít, hogy a büntetőeljárás, illetve adott esetben az előkészítő eljárás során bármely szervtől, jogi személytől és jogi személyiséggel nem rendelkező szervezettől kérhető adatszolgáltatás,[781] erre irányuló megkeresés esetén tehát a közvetítő szolgáltatók és a közvetítő szolgáltatónak nem minősülő elektronikus hírközlési szolgáltatók egyaránt kötelesek átadni a birtokukban lévő adatokat az igénylő szerv számára, illetve megadni számukra a szükséges tájékoztatást. Elektronikus hírközlési szolgáltatótól csak ügyészi engedéllyel kérhető adatszolgáltatás,[782] kivéve akkor, amikor az engedélyezés olyan késedelemmel járna, amely az elérni kívánt célt jelentősen veszélyeztetné. Amennyiben a megkeresett szervezet az adatszolgáltatást határidőn belül nem teljesíti, vagy alaptalanul megtagadja, illetve amennyiben titoktartási kötelezettségének nem tesz eleget, rendbírsággal sújtható, illetve ellene kényszerintézkedések rendelhetők el.

Az adatszolgáltatás teljesítése természetszerűleg magában foglalja azt, hogy a szolgáltatónak rendelkezésére áll a szóban forgó információ, mert például tárolja azt. A magyar büntetőeljárás rendszerében két típusú adatmegőrzési kötelezettséggel találkozunk, az általános adatmegőrzési kötelezettséggel, valamint az egyedi ügyben történő megőrzésre kötelezéssel.

Az adatmegőrzés első típusa az Eht. 159/A. §-ban szabályozott bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettség, amely általános jellegű megőrzési kötelezettséget takar, és csak az elektronikus hírközlési szolgáltatókat terheli. Ez azt jelenti, hogy éppen folyó büntetőeljárásoktól függetlenül a törvényben szabályozott szolgáltatói körnek ezeket az adatokat meg kell őrizniük előfizetőikről, illetve igénybe vevőikről, hogy a bíróság, az ügyészség vagy a nyomozó hatóság esetleges megkeresése esetén át tudják azokat adni. A tárolt adatokkal kapcsolatban általában két kulcskérdés merül fel: az első, hogy a szolgáltatók pontosan milyen típusú adatokat kötelesek tárolni, a másik pedig, hogy meddig kötelesek tárolni a felhasználók adatait.

A szolgáltatások nyújtásával kapcsolatosan keletkezett információkat némi egyszerűsítést alkalmazva három csoportra oszthatjuk. Az egyik csoportot az úgynevezett „forgalmazási" adatok képezik, amelyek az információátvitellel szükségképpen együtt járó technikai jellegű adatok (IP-címek, portszámok, MAC-címek), amelyek, mint

[781] Be. 261. § (1) bekezdés.

[782] Be. 262. § (1) A nyomozó hatóság és a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve kizárólag az ügyészség engedélyével kérhet adatszolgáltatást c) az elektronikus hírközlési szolgáltatótól.

a postai küldeményeken a címzés, a feladó és a címzett azonosításához szükségesek. A másik csoportot az információküldés alanyaira vonatkozó adatok képezik, idetartoznak a szolgáltatás igénybe vevőjével kapcsolatos adatok (előfizetéses konstrukciókban az előfizető neve, számlázási címe). A harmadik kategóriába a közlés tartalma, az átvitt, illetve tárolt információ tartozik. A szolgáltatók tradicionálisan törekednek arra, hogy minél kevesebb adatot tároljanak. A szolgáltatók lehetőség szerint csak a jogszabály által előírt adatokat, illetve a szolgáltatás igénybe vevője által tárolni kért adatokat őrzik meg. Ennek okai részben gazdaságiak (az adatok tárolása költség- és erőforrásigényes feladat), részben pedig adatvédelmi és felelősségtelepítési szabályokon alapulók.

Minél tovább őrzi a szolgáltató a közléshez kapcsolódó információkat, annál nagyobb a személyes adatok védelméhez való jog sérülésének veszélye. Jelen kötetnek nem célja az internetes adatvédelem egyes aspektusainak tárgyalása, annyit azonban mindenképpen rögzíteni kell, hogy a készletező adatgyűjtés alapvetően tilos. Ugyan nem az internetes közvetítő szolgáltatók tevékenységével összhangban, de az EJEB foglalkozott az adatmegőrzés alapjogi aspektusaival.

Catt v. the United Kingdom, Application no. 43514/15

A Catt kontra Egyesült Királyság ügyben a Bíróság azt állapította meg: egy politikai aktivista személyes adatainak kezelése és felhasználása rendőrségi hírszerzési célokra sérti a magánélethez való jogot. A kérelmező politikai aktivista részt vett számos demonstrációban, amelyek között erőszakos megmozdulás is volt, ezért többször letartóztatták, de egy alkalommal sem szabtak ki rá büntetést. 2010-ben a kérelmező a brit adatvédelmi törvény (Data Protection Act) alapján igényelte azokat az információkat, amelyeket a rendőrség tárolt róla, és kiderült, hogy az „Extrémista adatbázisban" 66 rekord szerepel róla. A kérelmező kérte a róla tárolt adatok törlését, amelyet végül a brit Legfelsőbb Bíróság utasított el, mert az ilyen adatok megőrzését szükségesnek tartotta ahhoz, hogy a rendőrség tájékozottabban tudja értékelni a közrenddel kapcsolatos kockázatokat és veszélyeket, valamint ahhoz, hogy tanulmányozhassa az erőszakos cselekedetekkel összefüggésbe hozott demonstráló csoportok szerkezetét. Az EJEB elismerte, hogy a rendőrségnek először össze kell gyűjtenie az adatokat ahhoz, hogy azokat értékelni tudja, azonban kimondta, hogy a megőrzésük már nem volt szükségszerű, hiszen békés megmozdulásokon való részvétellel a kérelmező nem cselekedett a demokratikus folyamatokon kívül. Az ilyen típusú adatmegőrzés így azzal a hatással járhat, hogy az állampolgárok nem mernek részt venni a véleménynyilvánító demonstrációkon.

Az adatmegőrzési kötelezettség az információs társadalom egyes szolgáltatóit nem azonos időtartamban és nem azonos adatfajták tekintetében terheli. Az elektronikus hírközlési szolgáltatóknak az Eht. által tételesen felsorolt adatfajták tekintetében általános adatmegőrzési kötelezettségük van, amely időkorláthoz kötött. Az Eht. adatmegőrzésre vonatkozó szabályainak európai uniós háttere meglehetősen viharos pályát járt be, ugyanis a magyar szabályok alapját is képező hírközlési adatvédelmi irányelv[783] érvénytelenségét mondta ki az EUB a Digital Rights Ireland, valamint Seitlinger egyesített ügyekben.[784] Az érvénytelenség okául a Bíróság azt jelölte meg, hogy az ilyen terjedelmű adatmegőrzési kötelezettség a magánélethez való, valamint a személyes adatok védelmére vonatkozó alapvető jogokba olyan súlyos módon avatkozott be, ami nem állja ki az alapjog-korlátozás szükségességi-arányossági tesztjét. Az EuB álláspontját arra alapozta, hogy a hatóságok közelebbről meg nem határozott, súlyosnak minősített bűncselekmények esetében bármikor adatszolgáltatást kérhettek, ezért a szolgáltató az összes felhasználóra és hírközlési eszközre vonatkozó adatot köteles volt tárolni, hiszen bármikor, bármelyik felhasználója tekintetében érkezhetett hozzá hasonló megkeresés.

Az Eht. szabályai azonban az irányelv érvénytelenségének kimondását követően sem változtak érdemben, a magyar jog továbbra is az adatok rendkívül széles körének megőrzésére kötelezi az elektronikus hírközlési szolgáltatókat, teszi mindezt úgy, hogy az irányelv egyik legfontosabb garanciális szabályát is figyelmen kívül hagyva az adatmegőrzés célját nem korlátozza a súlyos bűncselekmények üldözésére. Az Eht. 159/A. § az alábbi adatok megőrzésére kötelezi az elektronikus hírközlési szolgáltatókat:

- az előfizetők személyes adatai;
- hívószámok és más műszaki-technikai azonosítók;
- felhasználói végberendezés vagy előfizetői hozzáférési pont létesítési címe és típusa;
- előfizetők, felhasználók hívószámai, egyedi műszaki-technikai azonosítói, felhasználói azonosítói, az igénybe vett elektronikus hírközlési szolgáltatás típusa, a kommunikáció dátuma, kezdő és záró időpontja;
- hívásátirányítás és hívástovábbítás esetén a hívásfelépítésben részt vevő köztes előfizetői vagy felhasználói hívószámok;

[783] 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.

[784] C-293/12 és C-594/12, a Digital Rights Ireland Ltd. kontra Írország és Kärntner Landesregierung kontra Michael Seitlinger és társai egyesített ügyekben hozott 2014. április 8-i ítélet.

- a felek készülékazonosítója (IMEI), valamint mobil-előfizetői azonosítója (IMSI);
- hálózat- és cellaazonosítók, valamint a cella tényleges földrajzi helyének meghatározásához szükséges adatok;
- internet-hozzáférés, internetes elektronikus levelezési, internetes telefonszolgáltatás esetében IP-cím, felhasználói azonosító, portszámok.

Az Eht.-ban lefektetett szabályokat vizsgálva az Alkotmánybíróság 15/2022. (VII. 14.) határozatában mulasztásban megnyilvánuló alkotmányellenességet állapított meg. Az Alkotmánybíróság a vonatkozó nemzetközi gyakorlat áttekintése során arra hívta fel a figyelmet, hogy az előfizetők tárolt adataiból kirajzolhatók teljes kommunikációs profilok, amely a személyiség meghatározó szelete, így a kommunikációra vonatkozó adatmegőrzésnek magas alkotmányos mércén kell átesnie. Ugyan az Alkotmánybíróság azt nem vitatta, hogy egy ilyen átfogó jellegű, lényegében készletre történő adatgyűjtés hátrányosan hat az érintettek magánéletére, mégsem semmisítette meg a kifogásolt jogszabályhelyet. A testület felfogása szerint ugyanis a probléma nem az adatok széles körének a megőrzésében rejlik – hiszen azokat a gazdasági szereplőnek minősülő szolgáltatók mind fizikailag, mind adminisztratív szempontból külön kezelik, és csak akkor használják fel őket, ha arra nyomós bűnüldözési, nemzetbiztonsági, honvédelmi érdekből van szükség –, hanem abban, hogy a jogalkotó nem konkretizálta, hogy az őrzött adatokból mely jogosult „milyen eljárásban, milyen célra és mennyire kiterjedt adatszolgáltatást kérhet”.[785] Az Alkotmánybíróság szerint ez a hiányosság mindenképpen orvoslandó, a jogszabály egyéb pontokon történő korrekciója azonban szükségtelen.

Mivel a közvetítő szolgáltatók közül csak az internetszolgáltató minősül elektronikus hírközlési szolgáltatónak is, a közvetítő szolgáltatók többségét, így a tárhelyszolgáltatókat, a keresőmotor-szolgáltatókat, illetve a gyorsítótároló szolgáltatókat nem terheli általános adatmegőrzési kötelezettség, noha a büntetőeljárás sikeréhez sokszor hozzá tudnának járulni. Warezoldalak esetében például a szerverhosting-szolgáltatók a szervereken keresztül bonyolított kommunikáció összes forgalmazási adatának birtokában lehetnek, de olyan eset is előfordult már, hogy egy kábítószer-kereskedőhöz

[785] Az Alkotmánybíróság 15/2022. (VII. 14.) AB határozata az elektronikus hírközlésről szóló 2003. évi C. törvény 157. § (2), (3) és (10) bekezdése, valamint 159/A. §-a szerinti szabályozással kapcsolatos mulasztásban megnyilvánuló alaptörvény-ellenesség megállapításáról [40].

a World of Warcraft című online játékba történő bejelentkezései alapján jutottak el a hatóságok.[786] Annak a törvényjavaslatnak az indokolása, amellyel végül 2016-ban módosult az Ekertv.,[787] úgy szól, hogy a jogszabály-módosítás célja az volt, hogy megteremtse az Ekertv. hatálya alá tartozó szolgáltatók adatmegőrzési, adatszolgáltatási és együttműködési kötelezettségét, ezzel ellentétben a törvény kizárólag az alkalmazásszolgáltatók számára ír elő kifejezett adatmegőrzési kötelezettséget, ezt is csak igen speciális esetekben. Azok az alkalmazásszolgáltatók, amelyek oly módon biztosítanak az igénybe vevők között titkosított kommunikációt, hogy a kommunikáció tartalma vagy a kommunikációs csatorna felépítésével kapcsolatos funkciók nem kizárólag a felhasználó végberendezésén valósulnak meg (végpont-végpont közötti titkosítás), kötelesek a továbbított küldemények, közlések tartalmát a külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén átadni, valamint az alkalmazás igénybevételével kapcsolatosan keletkező vagy kezelt metaadatokat megőrizni és átadni.[788] Ezzel a rendelkezéssel a törvény gyakorlatilag az olyan kommunikáció megfigyelésének lehetőségét biztosítja, amely elektronikus hírközlési szolgáltatókhoz hasonló tevékenységet végző szolgáltatóknak a többnyire üzenetküldésre használt alkalmazásain (Viber, WhatsApp) keresztül zajlik, vagyis a hagyományos lehallgatással egyenértékű megismerési lehetőséget teremt az erre jogosult szervek számára.

Noha általános adatmegőrzési kötelezettség nem terheli az összes közvetítő szolgáltatót, csak az elektronikus hírközlési szolgáltatókat, a büntetőeljárás során a bíróság, ügyészség vagy a nyomozó hatóság egyedi jelleggel elrendelheti elektronikus adatok megőrzését,[789] amely a lefoglalással azonos hatású kényszerintézkedés.

A megőrzésre kötelezett bárki lehet, akár természetes, akár jogi személy, ha az adat birtokosa, feldolgozója vagy kezelője. Ez a csoport értelemszerűen lefedi az összes további olyan közvetítő szolgáltatót, amelyet nem terhel általános adatmegőrzési kötelezettség. A megőrzésre kötelezett köteles az adatot változatlanul megőrizni és biztosítani annak biztonságos tárolását, valamint megakadályozni annak megváltoztatását, törlését, megsemmisítését, továbbítását, jogosulatlan másolat készítését

786 AFP 2010.

787 T/10307. számú törvényjavaslat a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról.

788 Ekertv. 3/B. §.

789 Be. 316. §.

és az ahhoz való jogosulatlan hozzáférést.[790] Az adatmegőrzés e fajtájánál fontos kritérium, hogy az azt előírő szerv pontosan és jól körülhatárolhatóan meg tudja határozni, hogy mely adatokra van szüksége, illetve valószínűsítenie kell azt is, hogy az intézkedés végrehajtására kötelezett a birtokában van ezeknek az adatoknak.

Az adatvédelmi aggályokon túl bizonyos szolgáltatóknak amiatt is érdeke lehet minél kevesebb adatot tárolni, hogy sikerrel tudjanak hivatkozni az Ekertv. felelősségkorlátozó rendelkezéseire.

A szóba jöhető szolgáltatók a gyorsítótároló és a tárhelyszolgáltatók, amelyeknek a tevékenysége alapvetően harmadik személyek által rendelkezésre bocsátott információnak a tárolásából áll. Ezek a szolgáltatók a harmadik személyek által rendelkezésre bocsátott jogellenes információ miatt viselt felelősség alól akkor mentesülhetnek, ha haladéktalanul intézkednek a törlésről, amint tudomást szereznek az információ jogellenességéről. Esetükben tehát fő kérdés, hogy az erre jogosult szerv adatkérése keletkeztet-e olyan tudomásszerzést, amely esetében a törlésről is rendelkezniük kell, hogy megfeleljenek az Ekertv. a felelősség alóli mentesülést biztosító rendelkezéseinek. Véleményem szerint nem, hiszen az adatkérés tárgya a büntetőeljárással összefüggő bármely[791] adat lehet, a szolgáltatóknak pedig nem kötelességük vizsgálni azt, hogy mi volt a nyomozó hatóság célja az adatkéréssel, sem azt, hogy vannak-e olyan adatok a szolgáltatásában, amelyek jogellenesek lehetnek. Noha a törvény nem sorolja fel, hogy az adatkéréssel milyen típusú adatok lehetnek érintettek, az adatkérés intézménye döntően nem a jogsértő tartalmú információk megszerzését célozza, hanem az adott szolgáltató nyilvántartásaiban kezelt, az igénybe vevő személyével és a forgalmazással kapcsolatos adatok megismerését. A jogellenes tartalmak megszerzésére lehetőség van külön kényszerintézkedés, az elektronikus adat vagy az adathordozó lefoglalásának keretében, illetve az elektronikus adat megőrzésére kötelezés keretében.

A megőrzés időtartama esetében nem találunk egységes, minden szolgáltatótípusra egyaránt alkalmazandó szabályokat. Az elektronikus hírközlési szolgáltatók adattípus függvényében fél- egy éves időtartamban kötelesek tárolni, az egyedi ügyben elrendelt adatmegőrzési kötelezettség esetében a megőrzés időtartama pedig a határozatot hozó szerv döntésének a függvénye, jellemzően a büntetőeljárás befejezéséig tart.

790 Be. 316. § (1)–(4) bekezdés.
791 Be. 261. §.

Együttműködés titkos információgyűjtés és leplezett eszköz alkalmazása érdekében

A Be. rendelkezései szerint a büntetőeljárásban bírói engedéllyel lehetőség van az információs rendszer titkos megfigyelésére, illetve az elektronikus hírközlő hálózat vagy eszköz útján folytatott kommunikáció lehallgatására.[792] A két megoldás közötti különbség, hogy a kommunikáció mindig dinamikus folyamat, így a hatóság a lehallgatni kívánt végpontra érkező és az onnan kimenő adatcsomagokat vizsgálja, míg megfigyelés esetében egy információs rendszert (például számítógépet) vizsgálnak át, amelybe az eszköz kommunikációjának figyelemmel kísérésén túl az eszközben tárolt adatok és az azon végzett műveletek vizsgálata is beleértendő. Az ügyészségről,[793] a rendőrségről,[794] a Nemzeti Adó- és Vámhivatalról,[795] valamint a nemzetbiztonsági szolgálatokról[796] szóló törvények arra is lehetőséget biztosítanak, hogy a felsorolt szervek titkos információgyűjtés keretében az információs rendszert titokban megfigyeljék, illetve lehallgassák. Annak érdekében, hogy a felsorolt szervek törvény által biztosított lehetőségeikkel élhessenek, az Eht. együttműködésre kötelezi az elektronikus hírközlési szolgáltatókat.[797] Az együttműködés keretében az elektronikus hírközlési szolgáltató köteles biztosítani a hálózatban továbbított közlemények, közlések, illetve az általa kezelt adatok megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit. A hatóságok igényeinek megfelelő műszaki rendszert – így különösen alapkiépítésű monitoring alrendszert[798] – kötelesek létesíteni, amelynek a költségeit a törvény szintén az együttműködésre kötelezett szolgáltatóra telepíti.

792 Be. 232. § (1) bekezdés.

793 2011. évi CLXIII. törvény az ügyészségről.

794 1994. évi XXXIV. törvény a Rendőrségről.

795 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról.

796 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.

797 Eht. 92. §.

798 Az alapkiépítésű monitoring alrendszer meghatározását az Eht. értelmező rendelkezései között találjuk. Eszerint alapkiépítésű monitoring alrendszer az olyan, a Nemzetbiztonsági Szakszolgálat által meghatározott műszaki alapkövetelmények szerint Magyarország területén létesített és működtetett rendszer, amely lehetővé teszi az elektronikus hírközlési feladatokat ellátó szervezet előfizetői, illetve felhasználói köréből tetszőlegesen kiválasztható, az előfizetők (felhasználók) összlétszámának legalább 0,1-0,6%-át kitevő, 150 000 előfizetői létszám alatt 0,6%, de legalább 60, 150 000 – 1 000 000 előfizetői létszám között 0,3%, de legalább 900, 1 000 000 előfizetői létszám felett 0,1%, de legalább 3000 (a teljes előfizetői körből egy előfizetőre számított átlagforgalom legfeljebb kétszeresével forgalmazó) előfizető vagy felhasználó kommunikációjának egyidejű ellenőrizhetőségét és azok kísérőadatainak késedelem nélküli, teljes körű, folyamatos, egyidejű kiválasztását és kiadását a kilépési pontra.

A szolgáltatók és a titkos információgyűjtés, illetve leplezett eszközök alkalmazására feljogosított szervezetek együttműködésének rendjét részletesen a 180/2004. számú kormányrendelet[799] szabályozza. A rendelet 2015 óta nem módosult, annak ellenére, hogy az új Be. 2018. július 1-jén hatályba lépett, és jelentősen átalakította a korábban titkos információgyűjtésként, valamint titkos adatszerzésként ismert jogintézményeket. Feltehetően a rendelet szabályait jelenleg a leplezett eszközök alkalmazására, illetve a titkos információgyűjtésre kell vonatkoztatni. A titkos információgyűjtés feltételeit a szolgáltató az alábbi módokon biztosítja:

- az eszközök elhelyezésére zárt helyet biztosít;
- biztosítja, hogy megfelelő alkalmazottak álljanak rendelkezésre;
- 24 órás váltásos ügyeletet vagy készenlétet biztosít;
- lehetővé teszi a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) tagjainak belépését;
- a hálózatán a bérelt vonali összeköttetéseket térítésmentesen átengedi.

A külső engedélyhez nem kötött titkos információgyűjtés során a felhatalmazott szervek vagy közvetlenül maguk kérelmezik a szolgáltatótól az együttműködést, vagy az NBSZ-en keresztül igénylik az adatszolgáltatást. Az engedélyhez kötött titkos információgyűjtés esetében mindig az NBSZ jár el kérelmezőként. A rendelet részletesen szól a költségviselés szabályairól: a szolgáltatónak kell viselnie az adatkapcsolat és egyeztetett felület kiépítésének költségét, az alapkiépítésű monitoring alrendszer és a kilépési pont közötti összeköttetés kialakításának költségét, valamint a rendszer- és szolgáltatásfejlesztés költségeit. A rendelet előírja, hogy a további részletszabályok meghatározása érdekében, valamint az Eht. által szabályozott adatszolgáltatás teljesítése érdekében a titkos információgyűjtésre felhatalmazott szervezetek az elektronikus hírközlési szolgáltatókkal együttműködési megállapodások megkötését kezdeményezhetik. Mivel az együttműködési megállapodás gyakorlatilag egy atipikus szerződés, a törvényen alapuló szerződési kötelezettségnél fogva – a szolgáltatók kötelesek a megállapodást a kezdeményezéstől számított 60 napon belül megkötni – az amúgy is gyengébb pozícióban lévő szolgáltató mint alany akarata a szerződéskötés tekintetében meg van kötve, ezáltal tehát csorbát szenved a szerződéskötési szabadság alapelve. Szerződéskötési kötelezettséget természetesen jogszabály keletkeztethet,[800] amennyiben

[799] 180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

[800] Ptk. 6:71. § [Szerződéskötési kötelezettség jogszabály alapján].

azt valamilyen közérdekű cél indokolja, így a kiberbűncselekmények felderítéséhez fűződő társadalmi érdek az alapját képezheti egy ilyen kötelezettség megfogalmazásának. A rendelet meglehetősen következetlen a tekintetben, hogy csak a titkos információgyűjtésre felhatalmazott szervek számára teszi lehetővé az együttműködési megállapodások kezdeményezését. Az említett megállapodások ugyanakkor az Eht. 92. §-ában foglalt adatszolgáltatás teljesítésének rendjét is tartalmazzák, ez utóbbit viszont a bűncselekmények felderítésében és nyomozásában részt vevő szervek jóval tágabb köre kérelmezheti. Az Országos Rendőr-főkapitányság és a Magyar Telekom között 2016-ban kötött megállapodás[801] például a titkos információgyűjtő és adatszerző tevékenység végzéséhez szükséges adatigénylésen túlmenően a bűnügyi és szabálysértési tevékenység végzése során kérelmezhető adatigénylés rendjét is tartalmazza. A kormányrendelet bevezet egy speciális egyeztetési eljárást, amelyet akkor kell lefolytatni, ha a felek valamely kérdésben nem tudnak megállapodni. A rendelet ezen része a média- és hírközlés-szabályozás szervezetének és ágazati jogszabályainak módosulását követően nem változott, így annak ellenére, hogy 2010 óta nem létezik, az egyeztetési eljárás lefolytatására kijelölt szervként a Nemzeti Hírközlési Hatóság (a továbbiakban: NHH) elnöke szerepel. Az NHH jogutódja 2010 óta az NMHH,[802] ezért vélelmezhetjük, hogy az egyeztetési eljárás lefolytatására e szervezetnek az elnöke jogosult. A rendelet arról is rendelkezik, hogy amennyiben a szolgáltató az egyeztetési eljárás eredményeként született döntésben foglaltakat nem teljesíti, az Eht.-ban[803] rögzített jogkövetkezmények[804] alkalmazásának van helye.

Elektronikus adat ideiglenes vagy végleges eltávolítása

A tartalom-bűncselekmények esetében az elkövető felelősségre vonásán felül az is a társadalom érdekét szolgálja, hogy a jogsértő információk minél hamarabb, lehetőség

801 Az Országos Rendőr-főkapitányság és a Magyar Telekom Távközlési Nyilvánosan Működő Részvénytársaság között kötött együttműködési megállapodás (2016. január 14.).

802 Eht. 167. § (1) bekezdés.

803 A rendelet az Eht. 33. §-ára utal, a törvény egyes szakaszai viszont a rendelet hatálybalépése óta már módosultak, így a szolgáltatókkal szemben alkalmazható szankciók a 48. §-ban találhatók.

804 Az Eht. 48. §-a alapján: jogsértő magatartás megszüntetésére kötelezés, jogsértő magatartás tanúsításának megtiltása, kötelezettségszabás, bírság, bírság a vezető tisztségviselő részére, közlemény közzétételére kötelezés, az elektronikus hírközlési szolgáltatás nyújtására vonatkozó jogosultság felfüggesztése, az elektronikus hírközlési tevékenység végzésének megtiltása, a rádiófrekvenciák és azonosítók használatára vonatkozó engedélyek visszavonása.

szerint még a büntetőeljárás jogerős befejezése előtt elérhetetlenné váljanak. A tartalom közzétevője nem minden esetben hajlik az eltávolításra, kiváltképp, ha annak jogellenességét vitatja. Máskor a tartalom feltöltője külföldön tartózkodik, vagy azonosíthatatlan, ezért a magyar hatóságok számára utolérhetetlen. A közvetítő szolgáltatók ellenben könnyen elérhetők, és a tartalomterjesztési értéklánc több pontján is képesek megakadályozni az információkhoz való hozzáférést. Logikus tehát második lépcsőben ezeket a szolgáltatókat kötelezni a tartalmakhoz való hozzáférés megakadályozására vagy a tartalom eltávolítására. Ezt elismerve az Eker. irányelv az összes közvetítő szolgáltató esetében rögzíti, hogy a bíróságoknak vagy a közigazgatási hatóságoknak lehetőségük van a szolgáltatót a jogsértés megszüntetésére vagy megelőzésére kötelezni, továbbá tárhelyszolgáltatók esetében az információ eltávolítására, illetve hozzáférhetetlenné tételére kötelezni.[805] A jogsértő tartalmak eltávolíttatásának a büntetőeljárás rendszerén belül, illetve azon kívül is több módszerét ismeri a magyar jog, ezek azonban csak részben állnak össze koherens rendszerré, inkább egymás mellett létező, lazán kapcsolódó eszközök, amelyek akár párhuzamosan is alkalmazhatók. A büntetőeljárásról szóló törvény két egymásra épülő megoldást kínál az elektronikus adatok ideiglenes hozzáférhetetlenné tételére:

- A közvádra üldözendő bűncselekmények esetében ideiglenes eltávolításra kötelezhetők a tárhelyszolgáltatók, illetve a tárhelyszolgáltatást is végző közvetítő szolgáltatók.
- Az olyan súlyos bűncselekmények esetében, mint a kábítószer-kereskedelem, a gyermekpornográfia, az állam elleni bűncselekmény vagy a terrorcselekmény, lehetőség van kényszerintézkedésként elrendelni az elektronikus adathoz való hozzáférés ideiglenes megakadályozását is, amennyiben az első pontban megnevezett kötelezettséget az eltávolításra kötelezett nem teljesítette, illetve amennyiben a tárhelyszolgáltató külföldön található, és a jogsegélykérelem nem hozott eredményt. Ebben az esetben a kötelezett már az elektronikus hírközlési szolgáltató, amely a hozzáférés megakadályozását az NMHH által meghatározott eljárás és műszaki előírások szerint valósítja meg.[806] Köznyelvi értelemben ez alatt a weboldalak blokkolását értjük.

Mindkét intézkedés kizárólag ideiglenes jelleggel, a büntetőeljárás jogerős befejezéséig rendelhető el, amennyiben a bíróság döntésében megállapítja, hogy az elektronikus

[805] Eker. irányelv 12. cikk (3), 13. cikk (2), 14. cikk (3).
[806] A kényszerintézkedés részletes ismertetését lásd bővebben Christián 2015.

adat jogsértő, a Btk. szabályainak[807] megfelelően intézkedésként elrendeli annak végleges hozzáférhetetlenné tételét, viszont ha nem találja az adatot jogsértőnek, akkor az elektronikus adat visszaállításáról, illetve a hozzáférés megakadályozásának feloldásáról rendelkezik. A kereső- és gyorsítótár-szolgáltatók esetében nem fogalmaz meg olyan szabályt a Be., amelynek értelmében kötelezhetők lennének a tartalomhoz való hozzáférés megakadályozására, így arra következtethetünk, hogy a magyar jogrendszer esetükben megelégszik az Ekertv. által szabályozott közvetett eltávolítási kötelezettség előírásával, amennyiben a tartalmak jogsértő jellegéről vagy eltávolíttatásáról tudomást szereznek.[808]

Az elektronikus adat eltávolítása esetében is van jelentősége a szólásszabadság védelmének, abban az esetben, ha az eltávolított adat közlésként értékelhető tartalom. A weboldalak blokkolásának kérdésével az EJEB több ítéletében is foglalkozott. A Kablis v. Oroszország ügyben[809] az EJEB megállapította, hogy a véleménynyilvánítás szabadságát korlátozták az orosz hatóságok, amikor egy aktivista közösségimédia-fiókját felfüggesztették, és blogbejegyzéseit törölték. Grigoriy Kablis online jelenlétét azért szüntették meg az orosz hatóságok, mert az aktivista olyan „népi gyűlést" szervezett, amelynek a megszervezésére irányuló igényt a hatóságok korábban elutasították. Az EJEB a gyülekezéshez való jog megsértése mellett a véleménynyilvánítás szabadságának megsértését is megállapította, mivel az orosz hatóságok azelőtt intézkedtek a blokkolásról, hogy a bíróság határozott volna a tartalom jogellenességéről. Ez rámutat a tartalomblokkolás egyik legfontosabb garanciájára: a tartalom jogellenességét bíróságnak kell megállapítania vagy valószínűsítenie (utóbbi esetben azonban a blokkolás csak ideiglenes lehet, és az eljárás befejezéséig tarthat). A Bíróság azt is megállapította, hogy a blokkolás előtt vizsgálni kell a jogellenesség fajtáját, így a szólásszabadság korlátozása nem indokolt abban az esetben, amikor a közlés célja vélemény kifejtése aktuális témáról, és az internetes bejegyzések nem hívnak fel erőszakos, garázda vagy jogsértő cselekedetek elkövetésére. Az EJEB rámutatott arra is, hogy az orosz információs törvény rendelkezései semmitmondóak és túlságosan tágan értelmezhetők, így például nem írják elő az ügyészség számára, hogy megvizsgálja, hogy indokolt-e a teljes weboldal blokkolása, vagy az elérni kívánt cél megvalósítható bizonyos tartalmak blokkolásával, információk törlésével.

A tömeges közléskorlátozással, például egész blogok vagy weboldalak hozzáférhetetlenné tételével az Ahmet Yıldırım v. Törökország és a Cengiz és mások v.

[807] Btk. 77. §.
[808] Ekertv. 9. § e) és 11. § b) pont.
[809] Kablis v. Russia, App. nos. 48310/16 és 59663/17.

Törökország ügyekben foglalkozott az EJEB. Ezekben az ügyekben a Bíróság megállapította, hogy Törökország jelentősen korlátozza az internetes felhasználók jogait azzal, hogy az olyan tartalmakat is eltávolíthatják, amelyek nem jogellenesek, de a befoglaló weboldal eltávolítása révén osztják a valóban jogellenes tartalmak sorsát.

A Cengiz v. Törökország ügyekben[810] hozott ítélet egy török blokkoló határozatra vonatkozóan született, amellyel Törökország a teljes YouTube-ot blokkolta. A Bíróság megállapította, hogy a YouTube egy olyan internetes platform, amely politikai és társadalmi kérdésekről nyújt információkat, elősegítve a civil újságírás fejlődését, a teljes hozzáférhetetlenné tétel pedig sérti az állampolgárok információhoz való hozzájutásának jogát. A blokkolásra azért került sor, mert a szolgáltatásban megjelentek olyan videók, amelyek Mustafa Kemal Atatürk[811] emlékét gyalázták, a Bíróság szerint néhány tartalom jogellenessége azonban nem alapozza meg egy akkora szolgáltatás teljes blokkolását, mint a YouTube.

Hasonló megállapítást tett az EJEB az Ahmet Yıldırım v. Törökország ügyben,[812] amelyben egy török PhD-hallgató élt panasszal, hogy „kollaterális" cenzúra áldozata lett amiatt, hogy a török hatóságok büntető bírósági határozat alapján blokkoltak több olyan weboldalt, amelynek a Google biztosított tárhelyet. A weboldalakat azért blokkolták, mert kapcsolatban álltak egy olyan weboldallal, amely Atatürk emlékét sértő tartalmat tárolt. A Bíróság arra jutott, hogy ilyen széles körű korlátozás lehetőségét nem teremti meg a török jog, akkor sem, ha legitim célt szolgál.

Az előbbiekben ismertetett szabályokon felül a Be.-ben találhatunk egy, a hagyományos büntetőeljárási dogmatikától meglehetősen idegen rendelkezést, amellyel azt kívánja előmozdítani, hogy a szolgáltatók, amelyek a kényszerintézkedés végrehajtásában érintettek lehetnek, minél hamarabb tudomást szerezzenek a tárhelyükön található kifogásolható tartalomról. Az ügyészségnek és a nyomozó hatóságnak van lehetősége arra, hogy a tartalom hozzáférhetetlenné tételére vonatkozó kényszerintézkedések foganatosítását megelőzően felhívják a médiatartalom-szolgáltató, a tárhelyszolgáltató, illetve a tárhelyszolgáltatást végző közvetítő szolgáltató figyelmét a jogsértő tartalmakra.[813] Ez az értesítés tulajdonképpen egy figyelmeztetés, amely felhívja ugyan a szolgáltató figyelmét a jogsértő tartalomra, annak megítélését és a foganatosítandó intézkedést azonban már a szolgáltató saját hatáskörébe delegálja. A felhívás kézhezvételét követően a szolgáltató saját belátása alapján intézkedhet a szóban

[810] Cengiz and Others v. Turkey, 48226/10 and 14027/11.
[811] A Török Köztársaság megalapítója és első miniszterelnöke, köztársasági elnöke.
[812] Ahmet Yıldırım v. Turkey, App. no. 3111/10.
[813] Be. 338. §.

forgó elektronikus adat önkéntes eltávolításáról. A rendelkezés főképp azt kívánja elősegíteni, hogy a jogellenes tartalmak minél gyorsabban váljanak elérhetetlenné, hiszen a szolgáltató önkéntes lépése esetén a kényszerintézkedés elrendelésének bírói engedélyezésére sem kell várni. Másodsorban e rendelkezés a szolgáltató felelősségre vonását is megalapozza. A törvény ugyan hangsúlyozza, hogy a felhívás teljesítése nem kötelező, mindazonáltal érdemes megvizsgálni, hogy a hatályos jogunk szerint hogyan alakul a szolgáltató tartalomért viselt felelőssége, ha tudomást szerez a potenciálisan jogsértő tartalomról, de nem tesz semmit annak eltávolítása érdekében. Ahogy azt a fejezet előző részében kifejtettem, az Eht. szubjektív kimentési okként, a harmadik személy tartalmáért viselt felelősség alóli mentesülés egyik feltételeként azt jelöli meg, hogy a szolgáltatónak ne legyen tudomása a tartalom jogsértő jellegéről. A nyomozó hatóság felhívásának kézhezvételét követően azonban a kimentés lehetősége gyakorlatilag megszűnik, hiszen ekkor már igen nehezen lehetne arra hivatkozni, hogy a szolgáltató előtt nem volt ismert, hogy a szolgáltatást használva harmadik személy jogellenesen tárol, illetve továbbít elektronikus adatot, a hatóság kérésének mérlegelésével ugyanis a tudomásszerzés megtörténik. Amennyiben a szolgáltatói felelősség oldaláról közelítjük meg a Be.-nek ezt a szabályát, azt a következtetést vonhatjuk le, hogy a felhívás teljesítése csak fenntartásokkal nevezhető önkéntesnek, hiszen a szolgáltatónak azt a körülményt is mérlegelnie kell, hogy a teljesítés elmulasztásával a saját felelősségre vonását – és esetleges szankcionálását – alapozza meg, amely kevésbé vonzó lehetőség, mint a szóban forgó tartalom egyszerű hozzáférhetetlenné tétele.

A 2021/784 rendelet alapján kibocsátott eltávolítási végzések végrehajtása

A terrorista tartalmak elleni fellépésről szóló új uniós rendelet megteremti annak a lehetőségét, hogy a tagállamok arra kijelölt igazságügyi vagy közigazgatási hatóságai felszólítsák a tárhelyszolgáltatókat a terrorista tartalmak eltávolítására vagy hozzáférhetetlenné tételére.[814] A tárhelyszolgáltatóknak azonnali eljárási kötelezettségük van, hiszen nagyon rövid időn belül intézkedniük kell a jelzett tartalommal szemben, mindössze egy órájuk van. Magyarország kijelölt hatósága az NMHH, amely a közigazgatási rendtartásról szóló törvény rendelkezései szerint folytatja le a tárhelyszolgáltatókkal kapcsolatos eljárásokat. E szolgáltatók az NMHH döntését közigazgatási perben támadhatják meg. A rendelet szerint az eltávolítani kért adatok

[814] 3. cikk.

vonatkozásában a szolgáltatókat megőrzési kötelezettség terheli, azaz az eltávolított tartalmak tárolásáról a bizonyítási eljárásban való későbbi felhasználás érdekében gondoskodniuk kell, így biztosítva, hogy azok esetleges hiánya ne kompromittálja a büntetőeljárás sikerét.

A rendelet szól arról is, hogy mi a teendő abban az esetben, ha az a szolgáltató, amelynél az eltávolítani kért tartalom található, nem a végzést kibocsátó tagállamban telepedett le. Ebben az esetben a kibocsátó tagállam hatósága ugyanúgy küldheti a végzést közvetlenül az érintett tárhelyszolgáltatónak, azzal, hogy a végzés megküldésével egyidejűleg tájékoztatnia kell a tárhelyszolgáltató székhelye szerinti illetékes hatóságot is. Az illetékes hatóság saját hatáskörében 72 órán belül megvizsgálhatja a végzést, és ha az súlyosan vagy nyilvánvalóan sérti a rendeletet vagy az EU Alapjogi Chartáját, a jogsértést megállapító határozatot fogad el, amellyel az eltávolítási végzés hatályát veszti.

A jogsértő tartalmak eltávolításának büntetőeljáráson kívüli eszközei

A jogsértő tartalmak eltávolítására a büntetőeljárás eszközein túl is van mód. Az Ekertv. például csak akkor teszi lehetővé a tárhelyszolgáltató és a keresőmotor-szolgáltató felelősség alóli mentesülését, ha az a jogsértő tartalmat haladéktalanul eltávolítja, miután annak létezéséről tudomást szerez. Ez a kötelezettség attól függetlenül áll fenn, hogy a szolgáltató milyen forrásból értesült arról, hogy a szolgáltatását jogellenes célra használják, a felelősséget egyaránt megalapozza a nyomozó hatóság Be. 338. § szerinti felhívása és a felhasználó panasza. Az Ekertv. értesítési-eltávolítási eljárást is bevezet, amelynek alkalmazására azonban csak két esetben, szerzői jogsértés és kiskorú személyiségi jogának megsértése esetén van lehetőség. Az értesítési-eltávolítási eljárás első lépése a közvetítő szolgáltató értesítése, amelyet teljes bizonyító erejű magánokiratba vagy közokiratba foglaltan, illetve a kiskorú személyiségi jogát sértő tartalom esetében ajánlott postai küldeményként lehet megtenni. Az értesítés alapján a szolgáltatónak 12 órán belül kötelessége intézkedni az információhoz való hozzáférés felfüggesztése vagy a tartalom eltávolítása iránt.[815] Az egyszerű adatátviteli szolgáltatást nyújtó szolgáltatók esetében nem fogalmaz meg a törvény hasonló elvárásokat, így ha ezek a szolgáltatók tudomást szereznek arról, hogy a hálózatukon jogellenes tevékenység zajlik, nem kötelesek intézkedni annak megszüntetéséről.

[815] Ekertv. 13. § (4) bekezdés.

A DSA rendelet egyik újítása a jogellenes tartalmak elleni fellépésre vonatkozó végzések kibocsátásának lehetővé tétele.[816] A végzéseket nemcsak a joghatóság szerinti, hanem bármely tagállam igazságügyi vagy közigazgatási hatósága közvetlenül megküldheti a közvetítő szolgáltatónak. A végzésben meg kell jelölni azt az uniós vagy nemzeti jogi rendelkezést, amely alapján a végzést kibocsátó hatóság a szóban forgó tartalmat jogellenesnek találja. A szolgáltatónak indokolatlan késedelem nélkül tájékoztatnia kell a kibocsátót arról, hogy a végzést végrehajtotta-e, és ha igen, milyen mértékben és módon.

Médiatartalomnak minősülő információk esetén a Médiatanácsnak is van lehetősége a médiaszolgáltatás és az internetes sajtótermék közvetítésének felfüggesztésére, vagyis arra, hogy eltávolításra kötelezze a közvetítő szolgáltatót.[817] A törvény indokolása ezt a lehetőséget mint a „jogérvényesítés folyamatának ultima ratio jellegű jogintézményét" határozza meg, amelynek alapja, hogy „a jogsértő tartalom közlését, a célközönséghez eljutását végső soron kizárólag a műsorterjesztő és a közvetítő szolgáltató tudja megakadályozni". A közvetítő szolgáltató abban az esetben kötelezhető, ha a jogsértő médiaszolgáltató nem tesz eleget az alaphatározatban foglaltaknak. A 2018. december 18-án hatályba lépett új audiovizuális médiaszolgáltatásokról szóló irányelv (a továbbiakban: AVMS irányelv) a tárhelyszolgáltatók egy meghatározott csoportjára, a videómegosztóplatform-szolgáltatókra is telepít kötelezettségeket a jogellenes tartalmak eltávolításával kapcsolatban. Az irányelv 28a. cikke arról rendelkezik, hogy a videómegosztóplatform-szolgáltatóknak meg kell tenniük a megfelelő intézkedéseket annak érdekében, hogy megvédjék a felhasználóikat az olyan tartalmaktól, amelyek gyűlöletkeltők, vagy amelyek az Európai Unió joga szerint bűncselekményt valósítanak meg. Az irányelv nem fogalmaz meg konkrét eltávolítási kötelezettséget a szolgáltató számára, hanem csupán arról rendelkezik, hogy a platformszolgáltatónak létre kell hoznia olyan eszközöket, amelyek segítségével a felhasználók panaszt tehetnek az ilyen tartalmak ellen, illetve ki kell dolgoznia olyan eljárásokat, amelyekkel ezek a panaszok kezelhetők. Az irányelvben található intézkedések listája exemplifikatív jellegű, a szolgáltató a saját igényeinek megfelelő további intézkedéseket is bevezethet, amennyiben azok hozzájárulnak az irányelvben megfogalmazott célok eléréséhez. Noha az AVMS irányelv maga nem fogalmaz meg eltávolítási kötelezettséget, a tárhelyszolgáltatók felelősségét ebben az esetben is megalapozza, ha a tudomásukra jutott jogsértő tartalmat nem távolítják el, a különböző bejelentési és panasztételi

[816] DSA 9. cikk.
[817] Mttv. 188. § (2) bekezdés.

mechanizmusok pedig épp azt célozzák, hogy a szolgáltató értesüljön a felhasználók által kifogásolt tartalmakról.

A jogsértő tartalmak elleni fellépés eszközei Európa-szerte az úgynevezett forródrótok, *hotline*-ok; ezek olyan jogsegélyszolgálatok, amelyek megkönnyítik a jogsértést észlelő felhasználóknak a panasztételt. Magyarországon 2005 óta működik az Internet Hotline, amely az INHOPE hálózat része. Az Internet Hotline-nál kilenc tartalmi kategóriában lehet bejelentéseket tenni, amelyek az alábbiak:

- hozzájárulás nélkül hozzáférhetővé tett tartalom;
- pedofil tartalom;
- zaklatás;
- rasszista, idegengyűlöletre uszító tartalom;
- erőszakot megjelenítő tartalom;
- drogfogyasztásra csábító tartalom;
- terrorcselekményre buzdító, terrorizmust népszerűsítő, elősegítő tartalom;
- adathalászhonlapok, vírusokkal, kém- és féregprogramokkal fertőzött tartalmak;
- egyéb, kiskorúakra káros tartalmak.

Amennyiben a Hotline munkatársai úgy találják, hogy a bejelentett tartalom jogellenes, arra kérik a tartalom létrehozóját (a tartalomszolgáltatót), hogy a tartalmat tegye hozzáférhetetlenné. Ha a tartalomszolgáltató nem reagál, a Hotline a tartalmat tároló szerver üzemeltetőjéhez – a tárhelyszolgáltatóhoz – fordul. Az Internet Hotline, noha kétségtelenül hasznos eszköz, pusztán jogsegélyszolgálat, így döntése nem minősül hatósági döntésnek.

Az internetes közvetítő szolgáltatók felelőssége harmadik személyek jogellenes tartalmaiért

A jogirodalomban sok vitát generálnak a szolgáltatók felelősségének létével és terjedelmével foglalkozó kérdések, de ezek a diskurzusok többnyire a szolgáltatók polgári jogi, ezen belül is a jogsértő tartalmakért viselt felelősségére koncentrálnak.[818] Érdemes azonban a közvetítő szolgáltatói felelősséget ennél tágabb kontextusban vizsgálni. Az információs környezetben elkövethető jogsértő cselekmények nem kizárólag tartalomhoz kapcsolódhatnak. A büntetőjog az úgynevezett informatikai

[818] Lásd erről Koltay 2019a, illetve Klein 2016b.

bűncselekményeknek többfajta osztályozását ismeri, amelyek közül – széles körű elfogadottsága miatt – a Cybercrime Egyezmény rendszerét ismertetjük. Az egyezmény az információs környezetben elkövethető deliktumokat három csoportra bontja. Az első csoportba tartoznak a szűk értelemben vett informatikai bűncselekmények, ahol az információs rendszer az elkövetés eszköze és tárgya is egyben. A második csoportot az információs rendszer felhasználásával elkövetett csalás képezi. A harmadik csoportba tartoznak az úgynevezett tartalom-bűncselekmények, ahol a számítógép csupán az elkövetés eszköze. A legváltozatosabb tényállások tartoznak ebbe a csoportba, klasszikusan a gyermekpornográfia és a szerzői jogsértések, de tulajdonképpen minden olyan bűncselekményt idesorolhatunk, amely tartalommal kapcsolatos. Így a Magyarországon pönalizált becsületsértés, rágalmazás, illetve a gyűlöletbeszéd is ebbe a körbe sorolhatók. Az DSA rendelet közvetítő szolgáltatók kimentési lehetőségeiről szóló cikkei sem tartalomról, hanem információról szólnak, ezért a felelősség kérdéseit nem célszerű szűken, csak a tartalomnak minősülő információk kapcsán vizsgálni. A rosszindulatú számítógépes programok *(malware)* terjesztése esetében például nem beszélhetünk tartalommal összefüggő jogsértésről, a kártékony kódok terjesztése mindazonáltal adatok továbbításával történik, így információval kapcsolatos jogsértésről már igen. Nem indokolt továbbá a közvetítő szolgáltatók felelősségét csupán polgári jogi oldalról, kártérítési felelősségként vizsgálni. A büntetőjogi felelősség, bár kétségtelenül csak kivételes esetben merülhet fel, néhány gondolatra mindenképp érdemes, mivel a lisszaboni szerződés[819] a jogi személyek büntetőjogi felelősségre vonásának lehetőségét is megteremtette. A kötet ezen része elsőként a közvetítő szolgáltatók felelősségének általános európai és magyar szabályait ismerteti, ezt követően pedig azokat a kötelezettségeket mutatja be, amelyek a DSA rendeletben foglaltakon túlmenően is felelősséget keletkeztethetnek.

A közvetítő szolgáltatók felelőssége általában

Az Ekertv. kiindulási pontként rögzíti, hogy a szolgáltatók felelnek az általuk rendelkezésre bocsátott jogellenes tartalmú információért.[820] Érdekesebb kérdés a más személyek által rendelkezésre bocsátott információért való felelősség kérdése. Kőhidi Ákos a szűk értelemben vett felelősség fogalmát úgy definiálja, mint „valamely

[819] Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (2007/C 306/01).

[820] Ekertv. 7. § (1).

normaszegő magatartás miatti következmény viselésének kötelezettsége".[821] A közvetítő szolgáltatók esetében joggal merül fel a kérdés, hogy a másért való felelősség speciális esetéről beszélünk, vagy a szolgáltató közvetlen felelősségéről, amelyet az keletkeztet, hogy valamely rá vonatkozó magatartási szabályt nem tartott be? A magyar jogirodalomban jelenleg az utóbbi elgondolás az elfogadott,[822] Bayer Judit szavaival élve „a szolgáltató nem azért […] felelős, amit valaki más tett, hanem azért, amit ő maga mulasztott el megtenni".[823] A kommentekért viselt felelősség egyes kérdéseit elemezve Klein Tamás is arra a következtetésre jut, hogy a szolgáltatói felelősségnek a tartalom jogsértő voltától független feltételhez kell kapcsolódnia.[824] Ennek mentén a DSA rendelet (és az Ekertv.), amikor a mentesülés feltételeit meghatározzák, pozitív magatartási előírásokat is megfogalmaznak, és ha a szolgáltatók nem ezen elvárások mentén cselekszenek, felelősségre vonhatók a más által rendelkezésre bocsátott jogellenes információért. Az DSA rendelet elődje, az Eker. irányelv a 2000-es években igen széles körű mentesülési lehetőséget biztosított a szolgáltatók számára, ami a szolgáltatások közvetítői jellegéből adódott: ezek olyan szolgáltatások, amelyek csupán technikai, automatikus és passzív jellegűek,[825] a szolgáltató nem gyakorol felügyeletet afelett, hogy az igénybe vevő hogyan és milyen céllal használja a szolgáltatást, tudomása sincs az esetleges jogsértésekről. Az Eker. irányelv által lefektetett kimentési lehetőségek olyan horizontális jellegű rendelkezések, amelyek az összes jogterület tekintetében, tehát mind a közjog, mind a magánjog rendszerében érvényesülnek. A kimentési rendszer ugyanakkor nem homogén természetű, az irányelv azon az alapon differenciál a szolgáltatók között, hogy azok milyen tevékenységet végeznek, pontosabban, hogy tevékenységük végzése közben milyen viszonyba kerülnek az információval, és milyen mértékű kontrollal rendelkeznek felette. Kőhidi Ákos[826] felhívja a figyelmet arra, hogy az egyszerű továbbítás és a gyorsítótárolás esetében a felelősségkorlátozó tények objektív természetűek, míg a tárhelyszolgáltatás és a keresőmotor-szolgáltatás esetében szubjektív elem is megjelenik: a tudomásszerzés.

A magyar jog az Eker. irányelvből átvett szabályokon túlmenően, szűk körben a kiskorúak személyiségi jogának megsértése és szerzői jogsértések esetében az úgynevezett értesítési-eltávolítási eljárást is bevezeti.

821 Kőhidi 2016: 46–47.
822 Lásd erről Bayer 2007: 37–47, illetve Klein 2020.
823 Bayer 2007: 37–47.
824 Klein 2016b.
825 Eker. irányelv (42) preambulumbekezdés.
826 Kőhidi 2016: 86.

A 2022-ben elfogadott DSA rendelet nem változtatott a közvetítő szolgáltatói felelősség alapjain, sőt inkább megerősíti a szolgáltatók korlátozott felelősségének rendszerét. A DSA továbbra is fenntartja azt az alapelvet, amely alapján a szolgáltatók nem kötelezhetőek arra, hogy előzetes, *ex ante* tartalomszűrést végezzenek. A DSA a szolgáltatókat védő szabályként beiktat egy új, az amerikai CDA nyomán már ismert szabályt, a „jó szamaritánus"-klauzulát,[827] amely biztosítja, hogy a szolgáltatók ne legyenek felelősségre vonhatók abban az esetben sem, ha önkéntes, saját kezdeményezésű vizsgálatokat végeznek, vagy a jogellenes tartalmak észlelésére és azonosítására vonatkozó intézkedéseket tesznek, s e tevékenységük révén szereznek tudomást a szolgáltatásukban lévő jogellenes információkról.

A közvetítő szolgáltatók büntetőjogi felelősségéről

A közvetítő szolgáltatók büntetőjogi felelősségének rendszere illeszkedik az Ekertv. előbbiekben ismertetett szabályaihoz. Mint ahogyan arról korábban esett szó, az Ekertv. felelősségkorlátozó szabályai az összes jogágban érvényesülnek, így a büntetőjogi felelősségre vonásra is csak nagyon szűk körben van lehetőség. Ebből kiindulva a közvetítő szolgáltatók büntetőjogi felelőssége fel sem merülhet, hiszen a bűncselekményt az követi el, aki a tényállásszerű magatartást megvalósítja, illetve aki ehhez segítséget nyújt. Amennyiben a szolgáltatónak csupán valamely alkalmazottja nyújt segítséget az adott cselekmény elkövetéséhez, részesként felel, a szolgáltatót mint gazdasági társaságot azonban ekkor sem terheli büntetőjogi felelősség. A közvetítő szolgáltatók által nyújtott szolgáltatások többnyire jogszerűen nyújtott gazdasági szolgáltatások, amelyeknek nem célja a bűnelkövetők segítése. A szolgáltató tettesként akkor lenne felelősségre vonható, ha valamilyen tényállási elemet megvalósítana, ami ritka ugyan, de nem példa nélküli. Éppen hazánkban 2017–18-ban született ítélet első fokon a Coldfusion-ügyben, amelyben a warezszervert üzemeltető elkövetők gazdasági társaságot hoztak létre jogellenes tevékenységük hatékony végzéséhez.[828] Elméletileg természetesen nem kizárt, hogy gazdasági társaságok bűnsegédként közreműködve az elkövetők rendelkezésére bocsátják szolgáltatásaikat, ennek azonban szükségszerű feltétele az, hogy az érintett szolgáltató a bűncselekmény elkövetésének szándékáról tudjon, sőt a megvalósításhoz

[827] DSA 7. cikk.
[828] Lándori 2017.

szándékos segítséget nyújtson, ami viszont – ha a szolgáltató gazdasági társaság – már bűnszervezetben való elkövetést feltételez. A segítségnyújtás lehet pszichikai (ha a szolgáltató biztatja, utasítja az igénybe vevőt) vagy fizikai (az infrastruktúra rendelkezésre bocsátása) tevékenység. Az Ekertv. a tárhelyszolgáltatók és keresőszolgáltatók esetében kifejezetten rendelkezik arról, hogy ha a szolgáltatás igénybe vevője a szolgáltató megbízásából vagy utasítására cselekszik, a szolgáltató szándékos magatartásának következményeként nem mentesül a felelősség alól.[829] A szolgáltató lehet bűnsegéd mulasztással is, vagyis azáltal, hogy nem tesz eleget valamely törvényi kötelezettségének. A mulasztás jellegéből fakadóan az említett jogszabályban meghatározott kötelezettségeknek mindenképpen olyanoknak kell lenniük, amelyek aktív, tevőleges magatartásra kötelezik a szolgáltatót, ezekből pedig többet is találunk a Be.-ben és más jogszabályokban. Korábban már ismertettük a jogsértő tartalmak hozzáférhetetlenné tételének a büntetőjogi, illetve közigazgatási jogi eszközrendszerét, így az elektronikus adatok ideiglenes hozzáférhetetlenné tételének, végleges hozzáférhetetlenné tételének és az Ekertv. szerinti felelősségkorlátozásnak a szabályait. Ha a felsoroltak nyomán a szolgáltatónak jogszabályból eredő kötelezettsége van a jogsértő információ (ideértve a jogellenes tartalmakat is) eltávolítására, vagy arra az elrendelésére jogosult bármely szerv kötelezi a szolgáltatót, és ennek a szolgáltató nem tesz eleget, fennáll a lehetősége annak, hogy mulasztásos bűnsegédi magatartást valósít meg. Az eltávolítási, illetve a hozzáférhetetlenné tételi kötelezettségnek természetesen csak az olyan szolgáltatók tudnak eleget tenni, amelyek rendelkeznek az ezt lehetővé tévő kontrollal a szolgáltatáson áthaladó, az abban tárolt vagy az azon keresztül elérhető információk felett. A gyorsítótároló, illetve a keresőmotor-szolgáltatók nem az információt, pusztán az elérési utat rögzítik, így ennek a feltételnek jobbára csak a tárhelyszolgáltatók és az internetszolgáltatók (egyszerű hozzáférést biztosító szolgáltatók) felelnek meg. A Be. szabályai ezzel összhangban ideiglenes eltávolításra csak a tárhelyszolgáltatókat, ideiglenes hozzáférhetetlenné tételre pedig csak az internetszolgáltatókat kötelezhetik, míg a Btk. szerinti végleges hozzáférhetetlenné tétel csak tárhelyszolgáltató esetében rendelhető el.[830] Az a szolgáltató, amely az Eht. szerinti általános vagy a Be. szerinti egyedi adatmegőrzési kötelezettségét ignorálja, szintén tekinthető bűnsegédnek. A tárgyalt bűnsegédi magatartás megállapíthatósága szorosan kötődik a tartalom jogellenes voltához, vagyis a szolgáltató csak abban az esetben minősíthető egyértelműen

[829] Ekertv. 12. §. A 10–11. §-ok rendelkezései alapján a szolgáltató nem mentesül a felelősség alól, ha az igénybe vevő a szolgáltató megbízásából vagy utasításai alapján cselekszik.

[830] Be. 336–337. §.

bűnsegédnek, ha bíróság úgy határoz, hogy a szóban forgó adat (tartalom) bűncselekményt valósít meg. Ha az eljárás lezárultával a bíróság megállapítja, hogy nem történt bűncselekmény, az, hogy a szolgáltató renitens magatartása bűnsegélynek minősüljön, dogmatikailag kizárt.

Polgári igény érvényesítése büntetőeljárásban

A büntetőeljárással összefüggésben érdemes kitérni egy nagyon érdekes problémára is. A sértettnek lehetősége van arra, hogy magánfélként polgári jogi igényét a büntetőeljárás során érvényesítse, akkor, ha igénye kártérítésre, dolog kiadására vagy pénz fizetésére irányul. A büntetőeljárási törvény magyarázata[831] felhívja arra a figyelmet, hogy ugyan „a törvényszakasz ezt expressis verbis nem foglalja magában, […] kiolvasható belőle, hogy az igényt a sértett érvényesítheti a […] terhelttel szemben". A közvetítő szolgáltatók a büntetőeljárásnak nem terheltjei, ellenben ahogy az EUB ítéletei is bizonyítják, a jogsértő, így akár a bűncselekményt megvalósító tartalmakért viselt felelősségük megállapítható. A Delfi-ügyben[832] az Emberi Jogok Európai Bírósága kimondta, hogy a szolgáltatót felelőssé lehet tenni a gyűlöletkeltő kommentekért. Az Index MTE ügyben[833] – bár a bíróság a konkrét ügyben nem mondta ki a szolgáltató felelősségét – megerősítette, hogy a közvetítő szolgáltató felelhet harmadik személyek jogsértő tartalmaiért. A leírtakból az következik, hogy ha egy tartalommal kapcsolatban büntetőeljárás is folyik, adhéziós eljárás keretei között nincs lehetősége a sértettnek a közvetítő szolgáltatóval szemben fennálló igényét a közvetítő szolgáltatóval szemben érvényesíteni, az ilyen ügyek *ipso jure* polgári bírósághoz tartoznak. A közvetítő szolgáltató ugyanakkor, ha vagyoni érdekeltként van jelen az eljárásban, az elkobzással, vagyonelkobzással, illetve az elektronikus adat hozzáférhetetlenné tételével kapcsolatos igényét az ügydöntő határozat jogerőre emelkedését követően egyéb törvényes úton érvényesítheti.[834] A törvény magyarázata meglehetősen éles kritikával illeti ezt a szakaszt, mivel „nem állapítható meg még az sem, hogy a büntetőbíróság jogerős ügydöntő határozata után a vagyoni érdekeltnek kivel szemben

831 Belovics–Erdei 2018: 128.

832 DELFI AS v. Estonia, App. no. 64569/09.

833 Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, no. 22947/13. 2016. február 2-i ítélet.

834 Be. 57. § (4) bekezdés.

és milyen igényt van módja egyéb törvényes úton érvényesíteni".[835] A kötet szerzője azon az álláspontonvan, hogy a vagyoni érdekelt a bíróság döntésére okot adó magatartást tanúsító személy ellen fordulhat. A jelenleg tárgyalt témával összefüggésben óhatatlanul felmerül a kérdés, hogy például egy tárhelyszolgáltató, amelyet elektronikus adat végleges hozzáférhetetlenné tételére kötelezett a büntetőeljárásban hozott határozat, és amelynek a terhelt által rendelkezésre bocsátott tartalom vonatkozásában a felelősségét a későbbiekben bíróság megállapította, megkísérelhet-e úgy kibújni a jogkövetkezmény viselése alól, hogy e rendelkezést kihasználva megpróbálja azt a terheltre testálni, akinek a magatartása nélkül a szolgáltató elmarasztalása sem következett volna be. Mindez már egy olyan felelősségi spirálhoz vezetne, amely gyakorlatilag ellehetetlenítené azt, hogy a sértett belátható időn belül kártérítéshez jusson.

Új felelősségelméletek

A kötet ez idáig a közvetítő szolgáltatói felelősségnek csak az egyik lehetséges megközelítésével – a fennálló kötelezettség elmulasztása miatt fennálló felelősséggel – foglalkozott. Az ilyen típusú felelősségkonstruálás azonban nem minden szolgáltató esetében lehetséges, hiszen az imént ismertetett kötelezettségek megtételének elmulasztása – noha ágazati jogszabályban foglalt szankciót vonhat maga után – nem eredményez polgári jogi felelősséget, ha az Ekertv. szerinti kimentési okok egyébként fennállnak. A mulasztásalapú felelősségtelepítésnek igazán csak az olyan szolgáltatók esetében van jelentősége, amelyek esetében a jogellenes információról való tudomásszerzés keletkeztet kötelezettségeket, amelyek feltételei a felelősség alóli mentesülésnek (tárhelyszolgáltatók, gyorsítótár-szolgáltatók, keresőszolgáltatók). Az internet és az alkalmazásszolgáltatók esetében viszont nincsenek tudomásszerzés esetére előírt kötelezettségek, a kimentés törvényileg meghatározott objektív feltételekhez kapcsolódik. Ebből kifolyólag az ilyen szolgáltatóknak nem kötelességük megszüntetni, illetve megakadályozni a jogsértéseket, még észlelés esetén sem. A számítógépes vírusok, például botnethálózatokat kialakító *malware*-ek esetében azonban a szolgáltatói észlelésnek és reagálásnak kiemelt szerepe lehet.

Az amerikai jogirodalomban megjelentek olyan elméletek is, amelyek szerint a közvetett felelősség alkalmazása az internetszolgáltatók esetében is kívánatos lehet, mint ahogy a munkáltató felelhet a munkavállaló által okozott kárért, az internetszolgáltatót

[835] Belovics–Erdei 2018: 130.

is terhelheti felelősség a vele szerződéses viszonyban álló felhasználó jogsértő magatartásáért. Doug Lichtman és Eric Posner[836] modelljükben négy feltételt állapítanak meg, amelyek teljesülése esetén a közvetett felelősség doktrínája vonzó megoldás lehet. Ezek:

- A jogsértő a jog által utolérhetetlen, például mert nehezen azonosítható, vagy nincsenek megfelelő erőforrásai ahhoz, hogy helytálljon az okozott kárért.
- A magas tranzakciós költségek miatt a felelősség megosztásának szerződéses rendezése valószínűtlen.
- A közvetett felelősséggel bíró fél észlelheti vagy megelőzheti a jogsértést, illetve egyéb módon hatást gyakorolhat a jogsértőre.
- A közvetett felelősség kilátásba helyezése arra ösztönözheti a felelőst, hogy internalizálja a jelentősebb negatív externáliákat (például beépíti az árba).

Giancarlo Frosio Reinier Kraakman „kapuőr"-elméletét[837] alkalmazza az internetes közvetítő szolgáltatókra, és négy feltételt rendel a kapuőrök felelősségének megállapításához.

- A jogsértés előfordulása elfogadhatatlanul magas, mert az elkövetők, tekintettel az online környezet sajátosságaira, nem kontrollálhatók.
- A közvetítő szolgáltatók maguktól nem akadályozzák meg a jogsértéseket, nem kifejezett kötelezettség hiányában nem alkalmaznak előzetes szűrést.
- A közvetítő szolgáltatók hatékonyan vissza tudnák szorítani a jogsértést, de ezt nem teszik meg, vagy olyan megoldásokat alkalmaznak, amelyeket a jogsértők minimális ráfordítással meg tudnak kerülni.
- A közvetítő szolgáltató szankcionálásának szociális és gazdasági költsége nem túlzottan magas.[838]

A közvetítői felelősség kérdésével foglalkozó magyar munkák is említést tesznek arról, hogy a szolgáltatók felelősségre vonása mellett pragmatikus érvek szólnak, hiszen „szemben az ismeretlen, beazonosíthatatlan felhasználókkal a szolgáltató könnyedén azonosítható és eljárás alá vonható".[839] A szolgáltatók az általános szerződési feltételeik megfogalmazásakor többnyire igyekeznek megszabadulni a felelősségtől, ezért nem egy tárhelyszolgáltató ÁSZF-jében találhatunk olyan formulát, amely kizárja

836 Lichtman–Posner 2004.
837 Kraakman 1986: 53.
838 Frosio 2018: 1–33.
839 Dornfeld 2018: 114–115.

a szolgáltató felelősségét az előfizető tartalmaiért, illetve kimondja, hogy amennyiben harmadik személy a szolgáltató ellen eljárást kezdeményez, az előfizető köteles a szolgáltató helyébe lépni az eljárás során, ha pedig ez nem lehetséges, úgy köteles viselni az eljárás költségeit.

Frosio azt is megjegyzi, hogy a közvetítő szolgáltató felelősségre vonása *(liability)* helyett napjainkban egyre jobban előtérbe kerül az ilyen szolgáltatók felelősségvállalása *(responsibility)*. A felelősségvállalás a jogsértések elleni proaktív fellépést feltételez, amely a jó szamaritánus közérdekű szerepvállalásának „jutalmaként" egyben a felelősségre vonás elkerülését eredményezi. A magyar szabályozásban és vállalati kultúrában is találunk olyan elemeket, amelyek a szolgáltatók egyre erőteljesebb felelősségvállalásának irányába mutatnak. A VII. részben ismertetett leplezett eszközök hatékony alkalmazása érdekében a nyomozó hatóság és a szolgáltatók közötti együttműködési megállapodások a két fél közötti partnerségi viszonyt demonstrálják. A nagyobb távközlési szolgáltatók gyakorlatában a társadalmi felelősségvállalás keretei között mind a médiatudatosság fejlesztése, mind a Nemzeti Kibervédelmi Intézettel történő együttműködés megjelenik,[840] a felhasználók magatartásának befolyásolására pedig az egyes szolgáltatások felhasználási feltételeiben, illetve az ÁSZF-ekben rögzített szabályok szolgálnak. Bizonyos szempontból üdvözlendő a cégek felelősségvállalása, ugyanakkor veszélyeket is hordoz magában. Frosio felhívja a figyelmet annak a veszélyére, hogy a felelősségvállalás egyben arra ösztönzi a szolgáltatókat, hogy maguk szabályozzanak és akadályozzák meg a vélhetően jogsértő tevékenységeket, ami a tisztességes eljáráshoz való jog és az alkotmányos garanciák érvényesülését a háttérbe szorítja, mivel a közlések elnémítása többnyire a *mainstream* etikai álláspontnak megfelelően történik.[841] Hasonló álláspontot fogalmaz meg Koltay András, amikor felhívja a figyelmet arra, hogy a szolgáltatók olyan „pszeudojogrendszert" hoznak létre, amelyben a döntések „semmiféle jogállami garanciát nem hordozó eljárásban születnek".[842]

Nem vitás, hogy a magánszektor szereplői nagyon sokat tehetnek a kiberbűncselekmények felderítése, valamint a jogsértő tartalmak eltávolítása érdekében. Nem egyértelmű azonban, hogy a magyar szabályozás pontosan milyen szerepet szán az internetes közvetítő szolgáltatóknak a büntetőeljárásban: néhol úgy tűnik, hogy a szabályozás a szolgáltatókra úgy tekint, mint amelyek partnerei a nyomozó hatóságnak (például együttműködési megállapodások, igényérvényesítés vagyoni érdekeltként), máskor azonban a terhelthez hasonlóan inkább elszenvedői az eljárásnak. Mindez

840 DIGI 2023; Magyar Telekom 2023a; 2023b.
841 Frosio 2018: 3.
842 Koltay 2014: 99–124.

azonban nem jelenti azt, hogy a szolgáltatók működésüket az állami szabályozástól teljesen függetleníthetik, állami szabályozásra továbbra is szükség van, amely kijelöli a kereteket, amelyek a szolgáltató tevékenységének irányát meghatározzák, és biztosítják, hogy az alapvető jogállami garanciák a szolgáltató és a felhasználó viszonyában érvényesüljenek.

A társadalmi felelősségvállalás és a platformok magánszabályozásának szerepe a tartalom-bűncselekmények elleni fellépésben

A populáris kultúra szuperhősképregényeinek visszatérő eleme, hogy miként lehet olyan korlátlan hatalmú lények felett ellenőrzést gyakorolni, mint a szuperhősök. A Marvel-képregények világában az ENSZ égisze alatt született sokoviai egyezmény hivatott biztosítani, hogy az olyan természetfeletti erővel bíró karakterek, mint Vasember, Hulk, a Skarlát Boszorkány vagy Amerika Kapitány egy nemzetközi szervezet kontrollja alatt végezhessék tevékenységüket.[843] A hatalom korlátozásának kérdése természetesen nem a képregényekből fakad, gyakorlatilag már az államok létezése óta foglalkoztatja a gondolkodókat. Napjainkban a korlátozhatósággal és elszámoltathatósággal kapcsolatos kérdések nemcsak az állami szereplők vonatkozásában jelennek meg, hanem akkor is, amikor az internetes ökoszisztéma szereplőinek egymásra és a társadalomra gyakorolt hatásairól folyik a diskurzus. A globálisan jelen lévő techóriások tagadhatatlanul hatást gyakorolnak életünkre. A Facebooknak 2019-ben 2,9 milliárd felhasználója volt,[844] ami azt jelenti, hogy a Föld lakosságának 1/3-a használja a közösségi oldalt. A Google által üzemeltetett YouTube-ra percenként 500 órányi tartalom kerül fel,[845] amelyek között találunk kedves emlékként feltöltött családi videókat, zenei videóklipeket, közérdeklődésre számot tartó eseményekről készített tudósításokat, de – amíg a moderátorok nem szűrik őket – terrorista propagandát és öngyilkosságra buzdító felvételeket is. Az online platformok életünkre gyakorolt hatásának vannak kevésbé feltűnő megnyilvánulásai annál, hogy a munkaidőnk egy részét macskás videók nézegetésével töltjük el. A platformok funkcióinak használata a felhasználóknak csak pár kattintásba telik, a felhasználóbarát felület mögött azonban komplex programkódok futnak. A legtöbb szolgáltatás összetett háttérfolyamatai az egyszerű

[843] Muchichka 2017: 215.
[844] Statista 2023.
[845] Statista 2022.

felhasználó számára láthatatlanok, mégis nagymértékben befolyásolják a felhasználói élményt, nem beszélve azokról a kihívásokról, amelyeket a társadalom elé állítanak. A platformok működése átláthatatlan, ez pedig olyan dilemmákat hív életre, mint a választások manipulálása, a szűrőbuborék-jelenség hatása a társadalmi diskurzusra, vagy a feledtetéshez való jog. Az online platformokat gyakran nevezik kapuőröknek is, hiszen meghatározó befolyást gyakorolnak az online információáramlásra, más szóval: hatalmuk van az információáramlás felett. Eldöntik, hogy milyen információkat kell törölni, moderálni, és hogy mely tartalmak jutnak el a világon szinte mindenkihez, vagy merülnek feledésbe a szolgáltató szervereinek valamelyikén. Egyes hangokat felerősítenek, másokat elhalkítanak számukra bizonyára logikus, ám a külső szemlélő számára átláthatatlan algoritmusok segítségével. A platformszolgáltatók felső vezetésén kívül vélhetően senki nem ismeri azokat az érdekeket, amelyek a szolgáltató tartalommal kapcsolatos politikáit formálják, hiszen a magánkézben lévő vállalatoknak a cég érdekeit szolgáló üzleti döntései többnyire nem jutnak el a nyilvánossághoz. Amikor olyan események rázzák meg az online világot, mint a christchurchi mészárlás élő közvetítése[846] vagy a Cambridge Analytica-botrány,[847] rendre előkerül a platformok ellenőrzésének és elszámoltathatóságának gondolata, és sokakban megfogalmazódnak olyan kérdések, mint a „Miért nem tudnak fellépni a platformok a terrorista tartalmak ellen?", vagy „Miért nem lépnek fel a platformok a gyermekek szexuális kizsákmányolását ábrázoló tartalmak ellen?" E kérdéseket inkább úgy kellene feltenni, hogy „Miért kellene egy magánkézben lévő vállalkozásnak törődnie a közérdekkel, ha jogszabály nem kötelezi őt erre?" Túl azon, hogy a platformok kötelezettségeit jogszabályok határozzák meg (többnyire a minimumra szorítkozva), többször felmerül az elképzelés, hogy a platformoknak mint az információáramlás kapuőreinek közfeladatot is el kell(ene) látniuk. Ezzel az elgondolással az alapvető probléma a megvalósíthatóság: hogyan tudna egy alapvetően saját gazdasági érdekeit szem előtt tartó cég őrködni a használat, a tartalmak jogszerűsége és a demokratikus információáramlás fölött úgy, hogy elfogulatlan és pártatlan legyen? Látszólag ez hatékony külső kontroll nélkül lehetetlen vállalkozás: azt kérni egy cégtől, hogy függetlenítse magát a befektetői érdektől és az aktuálpolitikai befolyástól, hogy ne a profitmaximalizálás jegyében végezze tevékenységét és afelé húzzon, aki többet fizet, hanem a közjó motiválja cselekedeteinek legalább egy részét. Springer is felhívja a figyelmet arra, hogy az önszabályozás hasznos lehet, mert az értéklánc több pontján működő szereplők erősségeit

[846] Porter 2019.
[847] Confessore 2018.

és tapasztalatát ötvözi, ugyanakkor veszélyeket is hordoz magában, mivel a szereplők motivációit nem feltétlenül értjük.[848] Éppen ezért az ön- és társszabályozás esetében nagy figyelmet kell fordítani az átláthatóságra és az elszámoltathatóságra, különösen akkor, ha a szolgáltató szűrési, moderálási tevékenysége alapjogokat (például a véleménynyilvánítás szabadságát) érinti.

Végig a sárga köves úton – magánszabályozás, önszabályozás, társszabályozás

Az online szolgáltatókra jellemző, hogy működésüket maguk is szabályozzák. Az internetet szabályozó uniós és nemzeti szabályok jellemzően nem túl részletesek, ezért olyan jogon túli szabályozási megoldások is létrejöttek, amelyek alkalmasak lehetnek arra, hogy kitöltsék a szabályozási hézagokat. A jogon túli szabályozás mögött megbúvó motivációk sokfélék lehetnek. A magánszabályzás révén a szolgáltatók azt remélik, hogy az állam szabályozási monopóliumát nem terjeszti ki további, működésükkel összefüggésbe hozható területekre. Jack Balkin szerint az állami beavatkozás ily módon történő megelőzése kifejezetten ösztönzőleg hat a magánszabályozásra.[849] A jogon túli szabályozási megoldásokat motiválhatja a szolgáltató gazdasági érdeke is. A felhasználói elégedettség szorosan összefügg a platform használatával, a csalódott fogyasztó hajlamosabb ritkábban használni vagy elhagyni az adott szolgáltatást, ezért a platformok számtalan olyan normát bevezetnek, amelyek célja a felhasználói elégedettség növelése. A jogon túli szabályozási megoldásoknak több formáját is megkülönböztethetjük, ezek a magánszabályozás, az önszabályozás, valamint a társszabályozás. Noha egymáshoz hasonlító jelenségekről van szó, több szempontból mégsem szabad őket azonosan kezelnünk, ezért az alábbiakban bemutatjuk az egyes megoldások lényeges vonásait.

Az önszabályozás

Az önszabályozás az olyan magatartás-szabályozó eszközök gyűjtőneve, amelyek által „szervezetek, érdekcsoportok saját magukat szabályozzák, az általuk megalkotott

[848] Callanan 2015: 89.
[849] Balkin 2018: 1193.

előírásokat saját magukra nézve kötelezőnek ismerik el, azok érvényesülését maguk ellenőrzik".[850] Az önszabályozás maga is többféle lehet, attól függően, hogy az állam miként viszonyul hozzá. A Bartle–Vass-féle multidimenzionális szabályozási modellben[851] az önszabályozás három formában jelenik meg:

- Tiszta önszabályozásról beszélünk, amikor a szabályozás nem törvényi alapon nyugszik, az állam szerepe korlátozott, felügyeleti joga pedig legfeljebb informális.
- Államilag elismert *(ex post)* önszabályozásról beszélünk, ha az állam utólag jóváhagy egy magatartási kódexet, majd ellenőrzi is annak érvényesülését.
- Kötelező *(ex ante)* önszabályozásról pedig akkor beszélünk, ha törvény írja elő ilyen rendszerek alkalmazását, a létrehozott szabályok pedig kötelező erejűek a szabályozott csoport tagjaira nézve.

Az önszabályozási rendszereket mindig az adott iparágban tevékenykedő szereplők alakítják ki, az adott rendszerhez csatlakozás pedig önkéntes. Az internet és média világában nem ismeretlenek az önszabályozási rendszerek. Az összes ilyen rendszert felsorolni nyilvánvalóan lehetetlen és szükségtelen, ezért jelen fejezetben csak példálózó jelleggel néhány fontosabb rendszert emelünk ki.

Az USA-ban az internetszolgáltatóknak önszabályozás keretében is lehetőségük van tartalomszűrést, valamint tartalomblokkolást végezni. A szolgáltató harmadik személyek tartalmaiért viselt felelősség alóli immunitását szabályozó törvények, a CDA és a DMCA egyaránt támogatják a szolgáltatói kezdeményezésre történő szűrést.[852] Nemcsak az USA-ban, hanem az Egyesült Királyságban is létezik önszabályozás keretében végzett internetszűrés. A brit médiahatóság, az Ofcom jelentése szerint[853] az internetszolgáltatók hálózati szintű szűrést *(network level filtering)* végeznek anélkül, hogy erre vonatkozó kötelezettséget jogszabály írna elő számukra. Az internetes önszabályozásban fontos szerep jut az ICANN-nak.[854] Az ICANN egy amerikai székhelyű nonprofit szervezet, amely saját maga, illetve tagszervezetek útján a doménnevek kiosztásáért, valamint a nyilvántartók és regisztrátorok tevékenységének felügyeletéért felelős, és ezek eljárásrendjét is szabályozza. Magyarországon az Ekertv. 15/A. § alapján a Magyarországi Internetszolgáltatók Tanácsa Tudományos Egyesület önszabályozással doménregisztrációs szabályzatot állapít meg, mivel

850 Csink–Mayer 2012: 35.
851 Sarkady 2017: 118.
852 Lásd 47 USC § 230. és DMCA 512. cikk g) 1. alpont.
853 Ofcom 2015.
854 Internet Corporation for Assigned Names and Numbers.

a doménnévkiosztásban érvényesül néhány alapvető szabály. Túl a doménnevekre vonatkozó formai követelményeken, amelyek többnyire a szolgáltatás műszaki jellemzői miatt szükségesek, vannak egyéb tartalmi kritériumok, amelyeknek a regisztrált doménneveknek meg kell felelniük. A doménnév nem lehet jogellenes, megbotránkozást vagy félelmet keltő, ilyen doménnevet tehát nem lehet regisztrálni. Amennyiben a jogellenes domén bejegyzése mégis megtörténik, a bíróság megállapíthatja a használat jogellenességét, és elrendelheti a delegálás megszüntetését, vagy a doménhasználót eltilthatja a domént azonosító név vagy megjelölés használatától. Ebben az esetben a nyilvántartónak vissza kell vonnia a delegálást. Az önszabályozás nagy múltra tekint vissza a tartalomszabályozásban, különösen a reklámszabályozás és a kiskorúak védelme területén, de egyre gyakrabban jelennek meg önszabályozási kezdeményezések a jogellenes tartalmak visszaszorításának érdekében is.

Európában jelentősnek mondható a reklám-önszabályozás, európai és tagállami szinten egyaránt. Az európai szintű reklám-önszabályozást az Európai Önszabályozó Reklámszervezet (EASA) fogja össze, amely a tagállami reklám-önszabályozó szervek közös szervezete. Az EASA rendeltetése, hogy működési és etikai standardokat alakítson ki, amelyek lehetővé teszik a hatékony reklám-önszabályozást. Ezeket a standardokat a szervezet a Reklám Önszabályozási Chartában rögzíti, amelynek a magyar Önszabályozó Reklámtestület is részese.

Szintén több önszabályozási kezdeményezés irányul a kiskorúak online térben való védelmére. Ilyen önszabályozási rendszerek az alábbiak:

- Alliance to Better Protect Children Online,
- CEO Coalition: Better Internet for Kids,
- Safer Social Networking Principles for the EU.

A tartalomszabályozás esetében az EU kifejezett eszközökkel támogatja az önszabályozást. Az audiovizuális médiaszolgáltatók és videómegosztók esetében az AVMS irányelv szól a jogon túli szabályozási lehetőségek ösztönzéséről. Az irányelv egyik jelentős újítása, hogy az uniós szintű magatartási kódexek létrehozását is biztosítja.[855] Ilyen magatartási kódexet egy-egy iparág uniós szintű szabályozására hozhatnak létre az érdekelt piaci szereplők, a tagállami kontroll helyett pedig az Európai Bizottság gyakorol ellenőrzési jogosítványokat. Uniós szinten már van néhány példa önszabályozó rendszerre.

[855] AVMS 4a. cikk.

2016-ban jött létre a jogellenes online gyűlöletbeszéddel szembeni fellépést szolgáló kódex,[856] amelyet a Facebook, a Microsoft, a Twitter[857] és a YouTube írtak alá. A kódexben a szolgáltatók vállalták, hogy olyan bejelentő rendszereket üzemeltetnek, amelyek lehetővé teszik a tartalmak eltávolítását, hozzáférhetetlenné tételét, a bejelentéseket pedig törekszenek 24 órán belül elbírálni. A kódexhez csatlakozó vállalkozások azt is vállalták, hogy létrehoznak egy hálózatot az olyan megbízható bejelentőknek *(trusted flaggers),* akik tevékenységüknél fogva jó minőségű, valós bejelentéseket tesznek.

2018-ban hozták létre a Félretájékoztatásról szóló gyakorlati kódexet,[858] azért, hogy a 2019-es EP-választások előtt a platformok összehangoltan lépjenek fel az álhírekkel és a dezinformációval szemben. A kódexhez csatlakoztak a legnagyobb szolgáltatók, így a Facebook, a Google, a Twitter, a Mozilla, később, 2019 folyamán pedig a Microsoft.

A társszabályozás

A társszabályozás az állami és az önszabályozás között helyezkedik el.[859] A társszabályozási rendszer alapvetően az állami jogalkotó és a társszabályozó szervezet együttműködésére épül, amelynek során a szabályozás alanyaira irányadó normarendszer kialakítása együttesen történik. Az állam többnyire a jogi kereteket alakítja ki, és jogszabály formájában megfogalmazza az elérendő célokat, amelyeket a társszabályozási szerv tartalommal tölt ki. Társszabályozás esetében a magatartási kódexek elfogadása, módosítása állami hozzájáruláshoz kötött.[860] A társszabályozásnak speciális formája működik Magyarországon, ahol a társszabályozó szervezeteknek a jogalkotó átengedte a hagyományosan közigazgatási szervek által közhatalom birtokában végzett jogalkalmazást. A médiaigazgatás területén működő társszabályozó szervek a NMHH Médiatanácsával közigazgatási szerződést köthetnek,[861] amely lefekteti az eljárás kereteit, és garanciákat állapít meg arra az esetre, ha a rendszer működése nem elégséges.

856 The EU Code of Conduct on Countering Illegal Hate Speech Online.
857 A Twitter később, 2023 folyamán kilépett a kódexből.
858 Code of Practice on Disinformation.
859 Marsden 2011: 76–100.
860 Csink–Mayer 2012: 61.
861 Mttv. 193. § (1) bekezdés.

A magánszabályozás

A platformok nem határozhatnak meg ugyan új bűncselekményeket, és nem folytathatnak rendészeti tevékenységet, saját szabályrendszerük révén mégis megtilthatnak bizonyos magatartásokat, és a normaszegésért szankciót is kilátásba helyezhetnek. Kate Klonick egyenesen önálló szabályozóknak nevezi a platformokat, amelyek saját szabályozott környezetet működtetnek, kontrollálják a felhasználók magatartását, és döntéshozatali eljárásokat folytatnak le.[862] Néhány platform felhasználási feltételeit végigböngészve levonható az a következtetés, hogy a szolgáltatók jelenleg is többet tesznek a tartalomszabályozás frontján, mint ami tőlük a jogszabályok által elvárható lenne. E körben számos olyan tartalom feltöltését tiltják, ami egyébként nem, vagy nem minden országban minősül jogellenesnek. A szolgáltatók ezzel olyan kortárs problémákat is képesek kezelni, amelyeket még nem szabályoznak jogi normák, illetve amelyek az egyes nemzeti, kulturális különbségekből fakadnak. Amellett, hogy a platformok szabályozása alkalmas arra, hogy kiegészítő védelmet nyújtson azokon a területeken, amelyeket az állam nem, vagy nem megfelelően szabályoz, a szabályok kialakításában megfigyelhető túlzott rugalmasságnak káros hatásai is lehetnek. Koltay András felhívja a figyelmet arra, hogy az, hogy a platformok szabályozása az állami szabályozáshoz viszonyítva hol szigorúbb, hol megengedőbb, kiszámíthatatlan szabályozási környezetet teremt.[863] Az egyik legnagyobb videómegosztó, a YouTube tiltja[864] az alábbi tartalmak feltöltését:

- meztelenséget vagy szexualitást ábrázoló tartalom;
- káros vagy veszélyes jeleneteket bemutató tartalom;
- gyűlölködő tartalom;
- erőszakos vagy megbotránkoztató tartalom;
- zaklatás, internetes zaklatás, bullying;
- spam, félrevezető adatok, átverések;
- fenyegetések;
- szerzői jogot sértő tartalmak;
- személyes adattal való visszaélést megvalósító tartalmak.

862 Klonick 2018: 1662–1664.
863 Koltay 2019b: 233.
864 YouTube 2023a.

Egy másik nagy platform, a Facebook kifogásolható tartalomnak minősíti az alábbiakat:

- gyűlöletbeszéd;
- erőszakos és durva tartalom;
- meztelenség és szexualitás;
- szexuális jellegű felhívás;
- kíméletlen és érzéketlen tartalom;
- csalás és félrevezetés, kéretlen tartalmak (spam);
- szellemi tulajdont sértő tartalmak;
- álhírek.

Az előbbi listákon több olyan tartalomkategória is szerepel, amelyek közzététele nem, vagy nem minden esetben sért büntetőjogi normát. A platformokon különbséget kell tenni azok között a tartalmak között, amelyek erkölcsi normát és azok között, amelyek jogi normát sértenek. A jogi normát sértő tartalmak körét jogszabályok határozzák meg, és ebbe a csoportba tartoznak a bűncselekményt megvalósító tartalmak is. A jogi normát sértő tartalmak ellen a platformoknak kötelességük a joghatóságuk szerinti állam jogának megfelelően fellépni, az egyéb tartalmak ellen azonban ez pusztán lehetőségük. A nem jogi normát sértő tartalmak közé tartoznak például a veszélyes magatartásokat bemutató tartalmak. A különböző internetes kihívások (például a Tide Pod Challenge, amelynek a lényege mosókapszulák elfogyasztása volt[865]) gyakran olyan magatartásra buzdíthatnak, amely káros, önveszélyes, de jogi normát nem sért. Ezek a tartalmak legfeljebb morális alapú rosszallást válthatnak ki, mivel a büntetőjog fő funkciója a társadalomra veszélyes cselekmények megakadályozása, az egyéneket nem védheti meg önmaguktól. A veszélyes jelenetek csoportjába sorolható a káros magatartások, szenvedélyek népszerűsítése, például étkezési zavarok, orvosilag nem elismert gyógymódok ajánlása, illetve az olyan ismeretek átadása, amelyek elősegíthetik jogsértő magatartások megvalósítását (például oktatóvideók számítógépes vírusok programozásához, útmutató fegyverek, robbanóanyagok, tudatmódosító szerek készítéséhez).

Egyes tartalmi tilalmakat annyira általánosan fogalmaznak meg a platformok, hogy egyedileg szükséges mérlegelni, hogy az adott tartalom megvalósít-e bűncselekményt. Az erőszakos tartalmakat és a meztelenséget, szexualitást a platformok jellemzően teljesen tiltják. Kétségtelen, hogy vannak olyan erőszakos vagy szexuális felvételek (például gyermekpornográfia), amelyek bűncselekményt valósítanak meg, a legtöbb

[865] Bever 2018.

esetben azonban csak egyes felhasználói típusokra nézve (például kiskorúak) lehetnek ártalmasak. Ezek esetében a platform tiltó, korlátozó intézkedése inkább a médiajogi tartalomszabályozással rokon intézmény, nem pedig a bűncselekmények megelőzésének eszköze. Ebbe a körbe tartoznak azonban olyan tartalmak is, amelyek viszonylag új magatartásokkal hozhatók összefüggésbe (mint a bosszúpornó vagy a bullying), így kezelésükre még nem született adekvát jogi válasz. Az ilyen tartalmak esetében a platformok magánszabályozás révén történő tiltása nagymértékben hozzájárulhat a társadalomra veszélyes magatartások visszaszorításához és a fennálló jogsértések megszüntetéséhez. Noha a társadalomra veszélyes tartalmak eltávolítása méltányolható cél, a jogi fogódzó nélkül végzett tartalommoderálás magában hordozza annak veszélyét, hogy a platform olyan tartalmakat is eltávolít, amelyek nem illegálisak, s így lényegében magáncenzúrát valósít meg.

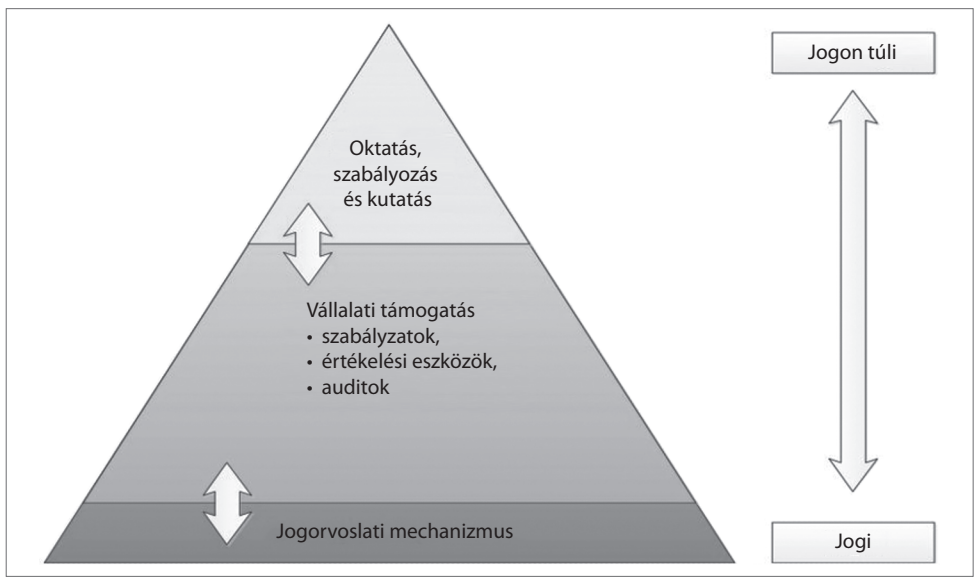
A magánszabályozás a szólásszabadság kapcsán érdekes alapjogi kérdést is felvet. Alapjogot korlátozni ugyanis csak kivételes esetben, a jogrendszerek nagy részében törvényi formában lehetséges, ezért kérdés, hogy hogyan biztosítható, hogy a platformok saját szabályzataik megalkotásával ne korlátozzák túlságosan az egyének jogait, így a szólásszabadsághoz való jogot. Egyes nézetek szerint a felhasználók azzal, hogy a regisztráció során elfogadják a platform felhasználási feltételeit, beleegyeznek abba, hogy jogaikat bizonyos korlátozások mellett gyakorolják. Ha a felhasználó ezzel nem ért egyet, nem köteles igénybe venni a szolgáltatást. Más elgondolások szerint a platformok már rég kinőtték az egyszerű szolgáltatásnyújtó szerepét, és sokkal jelentősebbek: a szólásszabadság gyakorlásának feltételeit biztosítják az online térben, amely szükségképpen határt szab cselekedeteiknek, és előírja, hogy milyen tartalommal fogadhatnak el szabályokat. Mark Zuckerberg, a Facebook vezérigazgatója maga nyilatkozta, hogy a platform kiáll a szólásszabadság védelme mellett, és nem alkalmaz tényellenőrzést politikai hirdetések és politikusok megszólalásai esetében.[866] A platform közösségi iránymutatása azonban számos tartalomtípus megosztását tiltja, vagyis a politikai beszédét kivéve más közlések cenzúrázását megengedhetőnek tartja.[867]

A veszélyes tartalmak moderálása és a szólásszabadság túlzó korlátozása között vékony határvonal húzódik, a szolgáltatók pedig nehéz helyzetben vannak, ha a tartalmakról kell dönteniük. Az egyensúly megtalálásában két intézmény együttes

[866] Kang–Isaac 2019.
[867] Edelman 2019.

alkalmazása a szolgáltatók segítségére lehet. Az egyik a társadalmi felelősségvállalás eszköztára,[868] a másik pedig a döntéshozatal külső kontrolljának eszköztára.

Emily B. Laidlaw doktori értekezésében[869] egy újfajta hibrid vállalatirányítási modellt vázol fel, amely magában foglalja a társadalmi felelősségvállalás keretében az alapjogok biztosításának érdekében tett intézkedéseket és az állami kontroll jogi eszközrendszerét (lásd 8. ábra). A szabályozási modell csúcsán a tájékoztatást, képzést és kutatást magában foglaló jogon kívüli eszközök találhatók, amelyeket mind az állam, mind a szolgáltatók és szervezeteik alkalmazhatnak. A piramis alján azok a jogorvoslati lehetőségek vannak, amelyek jogsérelem esetén a felhasználó által vehetők igénybe. A két szint között helyezkednek el azok a jogi és jogon kívüli eszközökből álló intézkedések, amelyek a rendszer működésének hatékonyságát erősítik és javítását biztosítják (például értékelési rendszerek, auditmódszertanok, szakpolitikai jellegű ajánlások).[870]



8. ábra: *Laidlaw vállalatirányítási modellje*

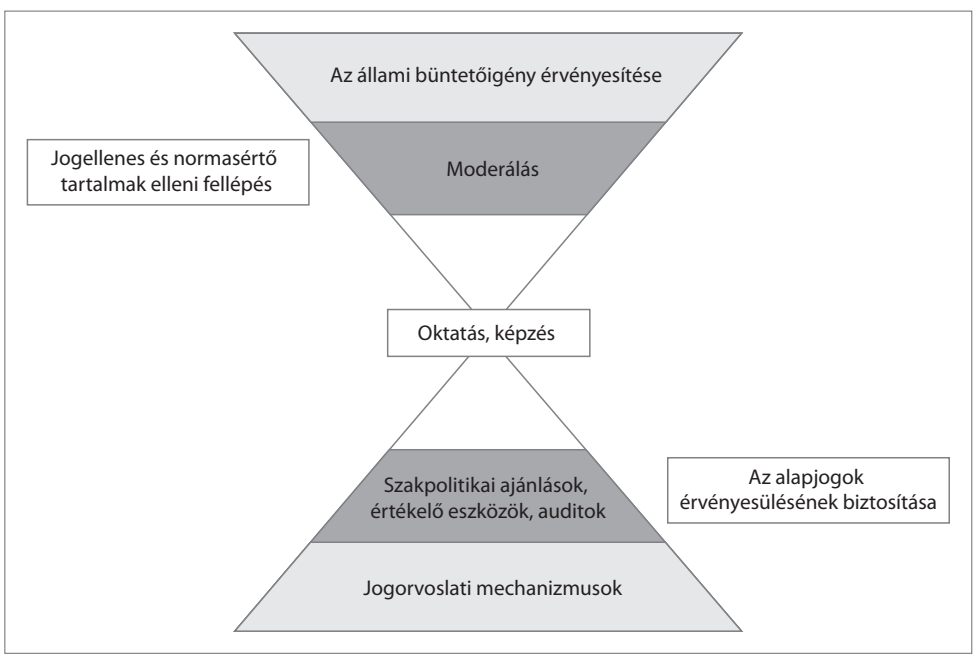
Forrás: Laidlaw 2012: 227

868 A társadalmi felelősségvállalás jelen tanulmány keretei között azt jelenti, hogy a vállalatok működésük során figyelembe veszik a társadalom érdekeit, a közérdekre figyelemmel szabályozzák működésüket és határoznak meg magukra és felhasználóikra bizonyos előírásokat.

869 Laidlaw 2012.

870 Laidlaw 2012: 227.

A Laidlaw-féle modell jól kiegészíthető a kiberbűncselekmények és más társadalomra veszélyes tartalmak elleni fellépés modelljével. Mivel az ez utóbbi modellbe tartozó tevékenységek eredménye többnyire alapjog-korlátozáshoz – a tartalmat közzétevők szólásszabadságának korlátozásához – vezet, a két rendszer közötti kapcsolatot egy homokórához hasonlító ábrán lehet a legjobban szemléltetni (lásd 9. ábra). A két modell találkozási pontja az oktatási, kutatási tevékenység, amely a bűncselekményt megvalósító tartalmak esetében is nagy hangsúlyt kap. Az oktatási-kutatási tevékenység kiterjed egyrészt a felhasználók és a szolgáltatók munkatársainak (például a moderátoroknak) az edukálására, másrészt az online térben való jogellenes cselekedetekkel kapcsolatos tudatosság mérését és erősítését célzó intézkedésekre. A jogellenes tartalmakkal szembeni fellépés legszigorúbb formája, amikor az állam avatkozik be, és vagy büntető igényét érvényesíti a feltöltővel szemben, vagy a szolgáltatót kötelezi a tartalom eltávolítására (például elektronikus adat ideiglenes vagy végleges hozzáférhetetlenné tételére kötelezéssel). A jogellenes vagy más normába ütköző tartalmakkal szembeni fellépés középső szintje a szolgáltatók, illetve szervezeteik által önkéntes alapon előírt moderálás, a moderálás hátterét képező közösségi alapelvek, irányelvek megalkotása.



9. ábra: *A kiberbűncselekmények elleni fellépés modellje*
Forrás: A szerző saját szerkesztése

Ahhoz, hogy biztosított legyen az alapjogok védelme és a jogellenes tartalmak eltávolítása közötti egyensúly, a szabályozási rendszer működésének átláthatónak kell lennie.

A magánszabályozás, valamint az ön- és társszabályozási rendszerek működésének átláthatósága

A platformok magánszabályozása, valamint az ön- és társszabályozási rendszerek sok szempontból különböznek, valamiben azonban hasonlítanak egymáshoz: az átlátható működés mindegyik rendszer szempontjából alapvető tényező. Az átláthatóság a jogon kívüli szabályozás esetében azt jelenti, hogy a szolgáltatók döntéseiket maguk alkotta vagy általuk kötelezőnek elismert szabályoknak megfelelően, a nyilvánosság számára ellenőrizhető módon hozzák meg. Az átlátható működés garantálja, hogy az állampolgárok információt szerezhessenek arról, hogy a szolgáltatók betartják-e a saját maguk által vagy a piaci szereplők egy csoportja által megfogalmazott szabályokat, továbbá azokról az esetekről, amikor a szolgáltatók döntéseiket állami vagy piaci beavatkozás következtében hozzák meg.

Az ön- és társszabályozási rendszerek működésének átláthatósága

Az Európai Parlament, az Európai Unió Tanácsa és az Európai Bizottság 2003-ban intézményközi megállapodást hoztak létre a jogalkotás javításáról,[871] amelyben a Bizottság feladatává teszik, hogy biztosítsa, hogy az ön- és társszabályozási rendszerek megfeleljenek az átláthatóság elvének.[872] Az AVMS irányelv a videómegosztóplatform-szolgáltatók által ön- és társszabályozás révén kialakított kódexek esetében előírja, hogy a kódexekben foglalt célkitűzéseket rendszeresen, átláthatóan és független módon nyomon kell követni.[873] Az OECD szerint az iparági önszabályozás egyik nagy kihívása az áltáthatóság biztosítása, egyes önszabályozási rendszerek ugyanis

871 Interinstitutional agreement on better law-making (2003/C 321/01). The European Parliament, the Council of the European Union and the Commission of the European Communities.

872 Interinstitutional agreement on better law-making (2003/C 321/01). The European Parliament, the Council of the European Union and the Commission of the European Communities 17. pont.

873 AVMS irányelv (12) preambulumbekezdés és 4a cikk.

nélkülözik a magatartási szabályok értékelésére és a beszámolásra vonatkozó eljárásokat.[874] Az OECD fontosnak tekinti az önszabályozás átláthatóságának fejlesztését, és az átláthatóságot az iparági önszabályozás sikerét előmozdító tényezők között tartja számon. Az átláthatóság biztosítása az önszabályozási rendszerekben azért is nehézkes, mert a rendszerekhez való csatlakozás önkéntes alapon történik, ha az egyes iparági szereplők nem értenek egyet annak működésével, kiléphetnek belőle. Az átláthatóság teljes körű biztosítása azért is akadályokba ütközhet, mert az iparág nem biztos, hogy saját maga szankcionálására fordítja erőforrásait.[875] A hatékony önszabályozás egyik feltétele, hogy legyen egy független szerv, amely érvényesíti a szabályokat, és felülvizsgálja a döntéseket. Ismertek olyan szabályozási modellek, mint a Sarkady Ildikó által is említett ausztrál modell, ahol az állam által szabályozott önszabályozásról beszélünk. Ebben a modellben a szabályokat az állami jogalkotó alkotja meg, azok kikényszerítése, érvényesítése viszont az önszabályozó szerv feladata.[876] Az ilyen kváziszabályozásnak is nevezett[877] modellben a működés átláthatóságának biztosítéka az, hogy ha a szabályozásban részt vevő szereplők működése nem elégséges, az állam szabályozás révén beavatkozhat.

A társszabályozási rendszerek átláthatóságának elsődleges biztosítéka a rendszernek alapot adó jogi szabályozás, valamint az állam által megvalósított felügyeleti tevékenység. Magyarországon a médiaszabályozás területén kialakított társszabályozási rendszer a Médiatanács és a társszabályozó szervezet közötti közigazgatási szerződésekre épül, amelyek törvényességi felügyeletét a Médiatanács látja el. A Médiatanács által végzett felügyelet a társszabályozási szervezet közigazgatási szerződésben meghatározott tevékenységére terjed ki,[878] vagyis jelentősen korlátozott tartalmú felügyeletet jelent.[879] A felügyelet során a Médiatanács adatszolgáltatásra kötelezheti a társszabályozó szervezetet, szankcióként felmondhatja a közigazgatási szerződést, illetve a társszabályozási rendszer elégtelen működése esetén gyakorolhatja hatósági hatáskörét. A Médiatanács ezenfelül jogorvoslati jellegű tevékenységet is végez, mivel a társszabályozásban részt vevő szervezet kötelezettséget kiszabó döntéseit

874 OECD 2015.
875 Csink–Mayer 2012: 41.
876 Sarkady 2017: 123.
877 Csink–Mayer 2012: 38.
878 Mttv. 201. § (1) bekezdés.
879 Lapsánszky 2019: 998.

automatikusan, egyéb döntéseit pedig a beadvány előterjesztőjének vagy a döntés kötelezettjének kérelmére felülvizsgálja.[880]

A magánszabályozás működésének átláthatósága

A platformok a szabályokat ideális esetben nemcsak megalkotják, hanem azoknak érvényt is szereznek. Például, ha felhasználói bejelentés érkezik egy közösségi iránymutatásokkal ellentétes tartalomról, eltávolítják azt, azonban ha úgy ítélik meg, hogy a szóban forgó tartalom csak egy adott régió vagy ország számára sértő, van lehetőségük arra is, hogy IP-cím alapján csak meghatározott helyen tegyék elérhetetlenné azt. A szabályok betartásának kikényszerítése alapvetően üdvözlendő tevékenység, amennyiben az kiszámítható módon, átláthatóan történik. Nem véletlen, hogy a jogbiztonság és az átlátható jogi szabályozás kiemelten védett érdekek. Az állampolgároknak az államszervezet működésébe vetett bizalma akkor szilárd, ha az eljárások előre meghatározott normák alapján, pontosan megfogalmazott eljárásrend szerint történnek, egy olyan rendszerben, ahol mindenkinek van lehetősége arra, hogy előre lássa magatartása lehetséges következményeit, és gyakorolja jogait. A platformok döntéshozatalát szabályozó normák azonban nem ezekre az elvekre épülnek, Koltay András a magánszabályozás egyik fő problémáját az eljárási garanciákat nélkülöző döntéshozatalban látja.[881] A közösségimédia-platformok esetében az eljárási garanciáknak azt kellene érvényre juttatniuk, hogy a szolgáltatók tájékoztatást adjanak a panasz elbírálásáról, a moderálási elvekről, illetve az eljárás eredményéről indokolt döntés szülessen. Indokolási kötelezettségük a platform üzemeltetőinek többnyire nincsen, ahogyan néhány homályosan megfogalmazott követelmény kivételével arról sem történik tájékoztatás, hogy pontosan hogyan zajlik a moderátori döntéshozatal, vagy hogy milyen szempontokat mérlegel, aki az ügyben eljár. Arra sincsen garancia, hogy globálisan, jobb esetben régiónként működtetett irodában olyan moderátor foglalkozik a kifogásolt tartalmakkal, aki ért a panaszos nyelvén, a moderátoroknak gyakran elég egy kéthetes képzés ahhoz, hogy munkába állhassanak.[882]

Az online platformok tartalommenedzsmentjének átláthatóságával kapcsolatban az uniós jog a DSA rendelet elfogadásáig csak olyan szabályokat fogalmazott meg, amelyek az üzleti felhasználók és platformszolgáltatók viszonyrendszerét érintik,

[880] Mttv. 199. § (1) bekezdés.
[881] Koltay 2019b: 233.
[882] Solon 2017.

továbbá amelyek csak a videómegosztó platformokra vonatkoznak. Az Európai Parlament és a Tanács 2019/1150 rendelete a közösségimédia-platformok számára is fogalmaz meg átláthatósági követelményeket.[883] A rendelet a szerződési feltételekkel kapcsolatban azt a követelményt támasztja, hogy azok legyenek világosan és érthetően megfogalmazottak, könnyen hozzáférhetők, és tartalmazzák a szolgáltatásnyújtás platformszolgáltató általi egyoldalú megszüntetésének, illetve felfüggesztésének lehetséges eseteit.[884] A platformszolgáltatónak az üzleti felhasználók hozzáférésének korlátozásával, illetve felfüggesztésével kapcsolatban minden esetben indokolással ellátott döntést kell hoznia.[885]

A DSA a tartalommoderálási tevékenység vonatkozásában már az összes közvetítő szolgáltatót kötelezi úgynevezett átláthatósági jelentések közzétételére. A nagyobb közösségimédia-platformok már korábban is rendszeresen tettek közzé úgynevezett átláthatósági jelentéseket *(transparency report),* amelyekben számot adtak a moderált tartalmak mennyiségéről és a törlés indokáról is.[886] Az átláthatósági jelentések jellemzően különbséget tettek a moderált tartalmak két csoportja között, és külön kezelték azokat a tartalmakat, amelyeket a platformok saját kezdeményezésre vagy felhasználói panaszra távolítottak el a közösségi iránymutatások vagy alapelvek megsértése miatt, és azokat a tartalmakat, amelyeket kormányzati vagy harmadik személyek megkeresései alapján távolítottak el.

A DSA a közvetítő szolgáltatók vonatkozásában már meghatározza az átláthatósági jelentések kötelező adattartalmát is,[887] így azokban mindenképpen közzé kell tenni:

- a tagállami hatóságoktól kapott végzések számát a jogellenes tartalom típusa szerint kategorizálva, ehhez kapcsolódva pedig a kézhezvételről való tájékoztatáshoz és a végrehajtáshoz szükséges medián időt;
- a magánszemélyek által tett bejelentések számát a kifogásolt tartalmak típusa szerinti bontásban, valamint a bejelentés nyomán elvégzett intézkedéseket;
- a megbízható bejelentők által benyújtott bejelentéseket, valamint az azok nyomán elvégzett intézkedéseket;
- tájékoztatást a saját kezdeményezésre végzett tartalommoderálásról;

883 Az Európai Parlament és a Tanács 2019/1150 rendelete az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról (11) preambulumbekezdés.

884 3. cikk (1).

885 4. cikk (1).

886 Lásd a Meta, illetve a Google átláthatósági jelentéseit.

887 DSA 15. cikk.

- a belső panaszkezelési rendszeren keresztül a szerződési felvételekkel összhangban kapott panaszok számát;
- automatizált eszközök használatát tartalommoderálás céljából.

Az online platformot üzemeltető szolgáltatóknak az átláthatósági jelentéseiket bővebb adattartalommal kell közzétenniük.[888] Az általános tartalmi elemeken túl az átláthatósági jelentéseknek tartalmazniuk kell:

- a peren kívüli vitarendezési testületek elé terjesztett viták számát, azok kimenetelét, az eljárás lefolytatásához szükséges medián időt, valamint a viták azon hányadát, amelyben a szolgáltató a testület határozatait végrehajtotta;
- a jogellenes tartalmakat rendszeresen nyilvánosságra hozó felhasználókkal szemben kiszabott felfüggesztések számát, megkülönböztetve a nyilvánvalóan jogellenes, valamint a megalapozatlan panaszok miatti felfüggesztéseket.

Még több kötelezettsége van az online óriásplatformot – azaz a havi 45 milló aktív felhasználót elérő platformot – üzemeltető szolgáltatóknak.[889] Az összes korábban említett adaton túl az óriásplatformok vonatkozásában az alábbi információk is közzé teendők:

- az Európai Unióban kínált szolgáltatás tekintetében nyújtott tartalommoderálásra fordított emberi erőforrások, a tagállamok hivatalos nyelvei szerinti lebontásban;
- a moderálást végző személyek képesítése és nyelvi szakértelme, a számukra nyújtott képzés és támogatás;
- pontossági mutatók.

Az átláthatóság követelménye a videómegosztóplatform-szolgáltatások szabályozásában is megjelenik, noha a 2022-ben elfogadott DSA fényében ezek a szabályok kiüresedettnek tűnnek. Az AVMS irányelv szól arról, hogy a platformoknak olyan átlátható mechanizmusokat kell kialakítaniuk, amelyekkel a felhasználók jelezhetik a panaszaikat, valamint biztosítaniuk kell, hogy a panaszkezelési eljárásuk átlátható legyen.[890]

Az átláthatóság további biztosítéka nemcsak a döntéshozal számszerű áttekinthetősége, hanem az is, hogy az alanyok (felhasználók) magatartását szabályozó normák

888 DSA 24. cikk.
889 DSA 42. cikk.
890 AVMS 28b. cikk.

legyenek könnyen elérhetők és közérthetők. Ehhez szorosan kapcsolódik, hogy a lefolytatott eljárások ne csak egy számként jelenjenek meg a rendszerben, hanem az érintettek azok eredményéről indokolással ellátott döntésben értesüljenek, és legyen lehetőségük jogorvoslat igénybevételére. Fontos szempont, hogy az egyes döntések meghozatalát az állami, kormányzati szereplők vagy a nagyobb piaci erővel bíró vállalkozások ne befolyásolják. A döntéshozatal transzparenciáját biztosítja az is, ha működik a külső kontroll intézménye, vagyis ha van egy olyan szerv, amely felügyeli a szabályozás működését, vagy amely a döntések elleni jogorvoslat lehetőségét biztosítja.

Az online platformok által alkalmazott mesterségesintelligencia-alapú tartalommoderálás szabályozási kérdései

Az egyik legnagyobb videómegosztó platform, a YouTube a 2020-as koronavírus-járvány világjárvánnyá válását követően bejelentette, hogy nagyjából 120 ezer alkalmazottját küldi haza, hogy otthonról dolgozzanak, ezzel párhuzamosan pedig megerősíti az automatikus tartalommoderálást.[891] A cég kijelentette azt is, hogy az emberi felülvizsgálat hiányában több olyan tartalmat is törölhetnek véletlenül, amelyek nem sértik a cég közösségi iránymutatásait, mivel ezek a rendszerek még nem tökéletesek. A járvány hatására nemcsak a YouTube kezdett egyes automatizálható folyamatokat gépekkel végeztetni, hanem több olyan online platform is, amelyek lehetővé teszik a felhasználóik által előállított tartalmak megosztását. A Facebook felhasználói ebben az időszakban furcsa jelenségnek lehettek tanúi: a platform ugyanis kéretlen üzenetnek (*spam*nek) minősített több olyan bejegyzést, amelyet nagyobb hírportálok (a *The Atlantic* vagy a *USA Today*) tettek közzé. A vállalat ezt a spamszűrő algoritmus meghibásodásával magyarázta.[892]

Az információtechnológia folyamatos fejlődésével egyre több feladat válik automatizálhatóvá, egyes döntések meghozatalára pedig a „robotok" is képesek lesznek, ilyen az online tartalomszolgáltatók által alkalmazott tartalomszűrés is. A közösségi médiában megjelenő tartalmak mennyisége már jó ideje nem teszi lehetővé, hogy a szolgáltatók kizárólag emberi munkaerővel szűrjenek, ezért az online platformok egy része a tartalomszűréshez már ma is használ „mesterséges intelligenciát", amely

[891] Leskin 2020.
[892] Matsakis–Martineau 2020.

ez esetben speciális, mélytanulás révén kialakított algoritmusokat[893] jelent. A jogellenes és ártalmas tartalmak kezelésében a szolgáltatók többnyire a mesterséges intelligenciában látják a megoldást,[894] sőt a legnagyobb platformszolgáltatók szinte kivétel nélkül mesterségesintelligencia-alapú algoritmusokat használnak a tartalomszűrésre, amelyek ma már jóval több tartalmat moderálnak, mint az emberi moderátorok. Ez utóbbira tekintettel a kérdés napjainkban már nem az, hogy alkalmazható-e a mesterséges intelligencia a tartalommoderálásban, hanem az, hogyan alkalmazható úgy, hogy a társadalom érdekeit és a polgárok tájékoztatását szolgálva működhessen.

Az algoritmikus tartalomszűrés azonban jelenleg egy olyan alulszabályozott területe a technológiajognak, amelynek számos alapjogi vonatkozása is van. Két alapjog különösen érintett, ha automatizált tartalomszűrésről beszélünk: az egyik a szólásszabadság joga, amely áll egyrészt a beszéd szabadságából, másrészt az információhoz hozzájutás szabadságából. A platformok azáltal, hogy moderálnak egyes felhasználói közléseket, hatást gyakorolnak a véleménynyilvánítás szabadságára, azáltal pedig, hogy találati listákat állítanak össze, vagy éppen személyre szabott ajánlatokat tesznek, az információhoz jutás szabadságára. A másik alapjog, amely fokozottan érintett, ha algoritmikus tartalomszűrésről esik szó, a személyes adatok védelméhez, illetve a magánélethez való jog. A jelenleg használt algoritmusok többsége ugyanis gépi tanulás révén szerzi meg a döntéshozatalhoz szükséges információkat, vagyis minél több adattal rendelkezik, annál hatékonyabban képes funkcionálni, ami komoly adatvédelmi kihívásokat jelent az őket alkalmazó vállalatok számára.

Jelen fejezet fő célja, hogy körbejárja az algoritmikus tartalomszűrés főbb szabályozási kérdéseit, különös tekintettel azok alapjogi vonatkozásaira. Ennek kapcsán négy témakört tartok szükségesnek részletesen vizsgálni:

- azt, hogy mit értünk pontosan tartalomszűrés és tartalommoderálás alatt;
- az automatizált tartalommoderálás és a mesterséges intelligencia működésének alapjait;
- a platformok által végzett automatizált tartalommoderálás előnyös, illetve káros hatásait;
- valamint a szabályozással összefüggő fontosabb dilemmákat, kérdéseket.

[893] Az algoritmusok tág értelemben véve egy-egy probléma megoldására, feladat elvégzésére létrehozott, lépésekből álló utasításssorozatok.

[894] Mark Zuckerberg a céget ért kritikákra gyakran válaszol azzal, hogy mesterséges intelligenciával tervezik megoldani a problémát (We are working on AI to solve it).

Ződi Zsolt gondolataival egyetértve, számításba véve, hogy a mesterséges intelligenciák nagy része manapság csak egyes szűken meghatározott feladatok ellátására alkalmas, a szabályozás akkor lehet hatékony, ha kialakul egy általános és több különös, egyes ágazati mesterséges intelligenciákra alkalmazandó szabályrendszer.[895] Jelen fejezet a mesterséges intelligencia szabályozásának általános kérdéseit nem tárgyalja részletesen, hanem egy speciális terület, a tartalomszűrés szabályozási kérdéseire koncentrál.

Mit értünk tartalomszűrés és moderálás alatt?

A kötet a tartalomszűrés fogalmát viszonylag tágan értelmezi, és idesorolja azokat az eseteket, amikor a platformszolgáltató *meg*szűri, és azokat is, amikor *ki*szűri a szolgáltatásában található információkat. A véleménynyilvánítás szabadságának oldaláról közelítve Tim Wu a tartalomszűrésnek ezt a két fajtáját megerősítő beszédszabályozásnak *(affirmative speech control),* illetve negatív beszédszabályozásnak *(negative speech control)* nevezi.[896]

A megerősítő közlésszabályozás Wu szerint magában foglalja annak kiválasztását, hogy mit ajánl a platform a felhasználó figyelmébe, például a keresési eredményekben, hírfolyamokban és hirdetésekben. A negatív beszédszabályozás ezzel szemben a nemkívánatos, jogellenes vagy tiltott tartalmak törlését, valamint a felhasználó megbüntetését, illetve szolgáltatás használatától való eltiltását jelenti.[897]

Megszűri a felhasználókhoz eljutó információkat a platform, amikor egy adott felhasználó számára egyénre szabva bizonyos szempontok alapján rendszerezi és kategóriákba sorolja a tartalmakat.

Szűr a szolgáltató, amikor:

1. *Ajánlásokat tesz.* A tartalmat több szempont szerint képes rendezni a szolgáltató. Gyakori például, hogy a nézettség alapján legnépszerűbb felvételeket gyűjtik csokorba mondjuk egy *„trending content"* szekcióban. A legnépszerűbb tartalmak összeállításán túl a legtöbb videómegosztó teljesen személyre szabott ajánlásokat is tud tenni, mondjuk egy „neked ajánljuk" szekcióban. Az automatizált ajánló rendszerek (*automated recommendation system* – ARS) feladata, hogy adatot gyűjtsenek a felhasználókról és a felhasználói szokásokról, majd ezek révén próbálják megjósolni, hogy mi az, amit a felhasználó nézni, vásárolni vagy olvasni

[895] Ződi 2018: 205.
[896] Wu 2019: 2014.
[897] Wu 2019: 2014.

szeretne.[898] A platform algoritmusa meglepő precizitással vesz számításba jó néhány faktort, például a felhasználó életkorát, lakhelyét, keresési előzményeit, de még azt is, hogy korábban melyik videókat nézte végig, melyekbe tekert bele, melyekről kattintott el. A tartalomajánló rendszereknek több fajtája is létezik, a szakirodalom ilyennek minősíti a szerkesztői ajánlást, a népszerűség alapján (azaz más felhasználók pozitív visszajelzése alapján) történő ajánlást, a tartalomalapú szűrést, illetve a kollaboratív szűrést *(collaborative filtering)*.[899] Témánk szempontjából utóbbiról érdemes bővebben szót ejteni. A kollaboratív szűrés során az algoritmus adatokat gyűjt a felhasználóról, majd a hasonló ízléssel rendelkező felhasználók által fogyasztott tartalmak listájából választja ki az olyan tartalmakat, amelyek más felhasználók számára is érdekesek lehettek.

2. *Egyedi lekérésre találati listát állít össze.* A videómegosztók egyedi lekérdezésre találati listákat is összeállítanak. Noha a felhasználó egy szempillantás alatt megkapja a keresési eredményt, a háttérben itt is bonyolult programkódok futnak, amelyek működése nagyon hasonló az ajánlások rendszeréhez.
3. *Moderál.* Kiszűr a platformszolgáltató bizonyos tartalmakat, amelyek valamilyen oknál fogva nemkívánatosak az adott szolgáltatásban, vagyis moderál. Moderálás alatt nemcsak a kifogásolható tartalom teljes eltávolítását kell érteni, hanem azt is, amikor a szolgáltató korlátozza az ahhoz való hozzáférést. A korlátozás lehet területi alapú, amikor az adott tartalom csak egy adott régió felhasználói számára hozzáférhetetlen, és lehet életkoralapú, amikor korhatárossá tesznek egy tartalmat, így a megfelelő életkor alatti felhasználók nem érhetik el azokat.

Hogyan alkalmazható a mesterséges intelligencia tartalommoderálásra?

Ha a jogalkotó egy új jelenséget szabályozni kíván – és ezt jól kívánja tenni –, nem árt tisztában lenni a szabályozott terület és technológia alapvető működési elveivel. A mesterségesintelligencia-alapú tartalomszűrő algoritmusok működésének megismerése nem egyszerű, gyakran még programozásban jártas szakemberek számára sem. Miskolczi Barna és Szathmáry Zoltán azonban kiemelik, hogy a jogi szabályozás sikerességéhez elengedhetetlen, hogy közös nyelvi, fogalmi és tartalmi alapok kialakítása során a szabályozás tárgyát érintő összefonódó tudományterületek megfelelő

[898] Ricci–Rokach–Shapira 2011.
[899] Zibriczky 2015.

súlyt kapjanak.[900] A szabályozási kérdések megfelelő kontextusba helyezéséhez ezért elengedhetetlen a működéssel kapcsolatos alapok ismertetése, amely hozzásegít annak azonosításához, hogy melyek a működésnek azon aspektusai, ahol jogi eszközökkel be lehet avatkozni, és melyek azok a területek, amelyeket hiába szabályozunk, mert a technológia még nem feltétlenül teszi lehetővé az alkalmazást.

Maga a mesterséges intelligencia mint fogalom nem újdonság; elképzelés és *science fiction* szintjén már az 1960-as években megjelent. Napjainkban a technológia fejlődése, a számítási kapacitás robbanásszerű emelkedése és az elérhető ár hozzájárultak ahhoz, hogy a mesterséges intelligencián alapuló megoldások elterjedhessenek. Ahogyan a technológiai újítások esetében ez olyan gyakori, a mesterséges intelligenciának sincsen általánosan elfogadott definíciója. Z. Karvalics László tanulmánya jól mutatja, hogy a mesterségesintelligencia-fogalmak jelenleg differenciáltak.[901] A mesterséges intelligencia köznyelvi felfogásához talán a Z. Karvalics László által erős mesterséges intelligencia (*strong artificial intelligence* – SAI) fogalma áll a legközelebb, amely olyan gépekre vonatkozik, amelyek bármely olyan intellektuális feladatot képesek teljesíteni, amelyet az ember.[902] Az emberi intelligenciát Ray Kurzweil elmélete szerint akkor éri utol a gépi intelligencia, amikor annak exponenciális növekedése szingularitáshoz vezet.[903] Noha a technológiai fejlődés hatalmas léptékben halad előre, itt egyelőre még nem tartunk. Az Európai Bizottság közleménye a közös európai adattér kialakításáról úgy határozza meg a mesterséges intelligenciát, mint intelligens viselkedésre utaló rendszer, amely konkrét célok elérése érdekében elemzi a környezetét, és – bizonyos mértékű autonómiával – intézkedéseket hajt végre.[904] A megfogalmazás, különösen annak azon fordulata, amely „intelligens viselkedésre utaló" rendszert említ, arra enged következtetni, hogy a gépek cselekedetei valójában nem intelligens cselekvések, pusztán az intelligencia látszatát keltik azáltal, hogy az emberi gondolkodás utánzására törekszenek. A tényleges intelligencia hiányára utal a részleges autonómiára történő hivatkozás is: a mesterségesintelligencia-alapú megoldások csak a megalkotóik által beléjük programozott keretek között rendelkeznek döntési szabadsággal, vagyis ha a programjuk által meghatározott kritériumok teljesülnek, kötelesek annak megfelelően eljárni, nincsen saját akaratuk. Vegyünk egy példát: ha egy tartalomszűrő rendszer

[900] Miskolczi–Szathmáry 2018: 43.
[901] Z. Karvalics 2015: 7–41.
[902] Z. Karvalics 2015: 10.
[903] Kurzweil 2014.
[904] *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. A közös európai adattér kialakítása felé.* COM(2018) 232 végleges.

a rendelkezésére álló adatok és a programozói által meghatározott szempontok szerint elemez egy feltöltött videót, majd a vizsgálat alapján arra az eredményre jut, hogy egy tartalom gyűlöletkeltő, és a programozásában az szerepel, hogy „HA a tartalom gyűlöletkelő, AKKOR el kell távolítani", nincs lehetősége másképp cselekedni, törölnie kell a tartalmat. Az autonómia hiánya nemcsak a döntés eredményét (a tartalom gyűlöletkeltő) követő cselekvési lehetőség korlátosságában (el kell távolítani) mutatkozik meg, hanem abban is, hogy ezek az eszközök jellemzően csak egyes, viszonylag szűken meghatározott feladatokat képesek elvégezni. Egy hitelkérelmek elbírálására létrehozott MI lehet, hogy nagy pontossággal meghatározza, hogy kinek biztonságos és kinek nem biztonságos hitelt adni, autonóm járművet azonban nem tud vezetni. A jelenleg használt mesterséges intelligencia tehát a Brooks által szűk mesterséges intelligenciának (*narrow artificial intelligence* – NAI) nevezett program, amely egyes részfeladatokat képes magas szinten ellátni.[905] Az ENSZ szólás- és véleményszabadsághoz való jog előmozdításával és védelmével foglalkozó különleges raportőrének jelentése szerint a mesterséges intelligencia nem egyetlen dologra utaló kifejezés, hanem olyan folyamatok és technológiák összefoglaló elnevezése, amelyek lehetővé teszik a számítógép számára, hogy kiegészítsenek vagy kiváltsanak egyes, emberek által végzett feladatokat.[906]

A mesterséges intelligenciát valójában algoritmusok, modellek alkotják, *deep learning* esetében például túlnyomórészt súlyozó mátrixok összessége. Szemben azonban azokkal az egyszerűbb algoritmusokkal, amelyek gyakorlatilag egy „receptet", lineáris lépéssorozatot használnak egy-egy probléma megoldására, a mesterséges intelligencia a kapott feladat, célmeghatározás függvényében maga alakítja ki a megoldáshoz szükséges lépéseket, előre meghatározott utasításkészlet nélkül, módosítva az alkalmazott modelleket. A mesterséges intelligencia fejlesztésének egyik újabb trendje a *deep learning* mellett a gépi tanulás *(machine learning)* azon fajtája, ami lényegében algoritmusok és statisztikai modellek együttese, amely képessé tesz egy számítógépes rendszert arra, hogy a rendelkezésére álló adatok alapján hozott döntések eredményeit, valamint a döntés következtében keletkezett új adatokat beépítse a döntési folyamatába[907] (például Naive Bayes vagy KNN-algoritmusok).

905 Brooks 2003.

906 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 3.

907 Nichols – Herbert Chan – Baker 2019.

A mesterségesintelligencia-alapú tartalomszűrés előnyei és hátrányai

Mint minden technológiának, a mesterségesintelligencia-alapú tartalomszűrésnek is megvannak a maga előnyei és hátrányai, ezek közül egyes előnyöket és hátrányokat a technológiát alkalmazó vállalkozás realizál, mások azonban a felhasználó vagy a társadalom oldalán jelentkeznek.

A mesterségesintelligencia-alapú tartalommoderálás előnyei

A mesterségesintelligencia-alapú tartalomszűrő használatához a platformszolgáltatóknak elsősorban gazdasági érdeke fűződik. Minden vállalkozás azt szeretné, ha a felhasználói minél több időt töltenének a szolgáltatásával. A személyre szabott ajánlatok, a felhasználó érdeklődését célzó találati listák éppen ennek a felhasználói kötődésnek (*engagement*nek) a létrehozását könnyítik meg. A személyre szabott ajánlások rendszerének iskolapéldája a Netflix, amely az ajánlásoknál a felhasználó stílusát figyelembe vevő indexképeket használ. Tehát a romantikus filmek kedvelői egy világos, pasztellárnyalatú képet kapnak, míg a krimik kedvelői sötétebb tónusú indexképpel találkoznak.

Szintén könnyű belátni, hogy a platform miért szeretné, ha minél kevesebb kifogásolható tartalom jelenne meg a szolgáltatásában. A botrányt egyetlen cég sem szereti. Az új-zélandi terrortámadás élő közvetítése elképesztően rossz sajtót hozott a Facebooknak.[908] Olyan is előfordult már, hogy hirdetők a reklámjaikat vonták ki a YouTube-ról azért, mert a platform válogatás nélkül rendelte őket, gyakran olyan ártalmas tartalmakhoz, amelyekhez a hirdető nem szerette volna a nevét adni.[909] Annak ellenére, hogy az automatikus szűrés nem működik 100%-os pontossággal, a kezelendő tartalmak mennyisége miatt mégis hatékonyabb, mint az emberi munkavégzés. A feltöltött tartalmak mennyisége nem is tenné lehetővé kizárólag emberi moderátorok alkalmazását. A YouTube-ra például percenként 500 órányi videót töltenek fel, és több mint 5 milliárd videó található a szervereiken. A platformok által alkalmazott tartalommoderálás célja kettős: az egyik cél, hogy azokat a tartalmakat, amelyek jogszabályi rendelkezést sértenek, eltávolítsák, a másik cél pedig az, hogy

[908] Wong 2019.
[909] Statt 2017.

azok a tartalmak, amelyek erkölcsi, etikai szempontból kifogásolhatók, vagy egyes felhasználói csoportokat sérthetnek (de jogi normába többnyire nem ütköznek), ne jelenhessenek meg a szolgáltatásban.

Az automatizálás elősegíti az emberi moderátorok egészséges és biztonságos munkavégzéshez való jogának érvényesülését. Szintén egy világsajtót megjárt hír, hogy egy nagy platformszolgáltató munkatársai depresszióval és pánikbetegséggel küzdenek, erről még egy dokumentumfilm is készült. A Facebook peren kívüli egyezség keretében vállalta, hogy összesen 52 millió dollárt fizet ki a jelenlegi és volt moderátorainak, akiknek napi nyolc órában az a feladata, hogy erőszakos tartalmakat, szexuális erőszakot, gyermekbántalmazást vagy éppen állatkínzást nézzenek.[910] A legártalmasabb tartalmakat jó eséllyel már az algoritmus is tudja szűrni, és nem lesz szüksége egy hét után mentálhigiénés szakemberre.

Az, hogy a platform algoritmusokkal automatikusan szűr, végső soron elősegíti egyes jogszabályi előírások betartását is. Az EU joga egyre több tartalommal kapcsolatos előírást fogalmaz meg az olyan internetes közvetítő szolgáltatók számára, amelyek hagyományosan nem tartoznak az európai médiaszabályozás hatálya alá. Ilyenek a videómegosztó platformok, valamint a videómegosztó platformnak minősített közösségimédia-platformok, amelyek számára a 2018-ban felülvizsgált audiovizuális médiaszolgáltatásokról szóló irányelv egy sor új kötelezettséget fogalmazott meg. Az irányelv alapvetően három célt jelöl meg a szolgáltatók számára:

- meg kell védeniük a kiskorúakat az ártalmas tartalmaktól;
- meg kell védeniük a felhasználókat a gyűlöletkeltő tartalmaktól;
- meg kell védeniük a felhasználókat azoktól a tartalmaktól, amelyeknek a közzététele az EU joga szerint bűncselekménynek minősül (például a gyermekpornográfia).

A platformoknak a felettük joghatósággal bíró tagállam szabályainak is meg kell felelniük, így tartalmi jellegű előírásokat az országok az irányelvnél bővebb körben is meghatározhatnak. Tipikusan ilyenek lehetnek a reklámokra és a termékmegjelenítésekre vonatkozó korlátozó jellegű előírások. A platformok ezenfelül kötelezhetők arra is, hogy egyéb nemzeti jogszabályoknak megfelelően távolítsanak el bizonyos tartalmakat.

[910] Newton 2020.

A mesterségesintelligencia-alapú tartalommoderálás hátrányai

Amellett, hogy a felsorolt okokból jó, hogy vannak mesterségesintelligencia-alapú tartalomszűrési lehetőségek, említést érdemel az automatizálás árnyoldala is. A mesterséges intelligencia használatának társadalomra és egyénre gyakorolt kockázatai között főképp az alapjogi kockázatokról kell említést tenni.

Az Európa Tanács internetes közvetítő szolgáltatókkal foglalkozó szakértői csoportja 2017-ben tanulmányt adott ki (Wagner-tanulmány)[911] arról, hogy az automatikus adatfeldolgozó technikák (különösen az algoritmusok) hogyan érintik az emberi jogokat.

A Wagner-tanulmány azonosítja azokat az alapjogokat, amelyeket az algoritmust használó döntéshozatali rendszerek megsérthetnek. Ezek:

- tisztességes eljáráshoz való jog,
- magánélethez való jog, adatvédelem,
- véleménynyilvánítás szabadsága,
- egyesülési szabadság,
- jogorvoslathoz való jog,
- a diszkrimináció tilalma,
- szabad választás.

A Wagner-tanulmány az automatizált döntéshozatalt általában vizsgálja, így nemcsak a tartalomszűrést, hanem a bírósági, hatósági döntéshozatalt, az önvezető járművek döntéseinek alapjogokra gyakorolt hatásait is elemzi. Jelen kötet témája szempontjából azonban nem mindegyik alapjognak van egyforma relevanciája, így e fejezetben a tartalommoderálásnak az adatvédelemre és a szólásszabadságra gyakorolt hatásait vizsgálom tüzetesebben.

Az Eli Pariser által szűrőbuborékként *(filter bubble),* Sunstein által „Napi Én"-ként és visszhangkamraként *(echo chamber)* leírt jelenségek azt mutatják, hogy a tartalomszűrés negatív irányba befolyásolja a vélemények terjedését. A platform azt szeretné, ha a felhasználó minél több időt töltene tartalomfogyasztással, ezt pedig úgy éri el, hogy olyan tartalmakat ajánl, amelyekről azt feltételezi, hogy a felhasználókat érdekelni fogják. Sunstein abból indul ki, hogy a fogyasztó maga is személyre szabhatja a fogyasztását, vagyis beállíthatja, hogy mi érdekli, és mi az, ami hidegen hagyja, azaz

911 Wagner 2017.

létrehozhat magának egy „Napi Én”-t.[912] A szűrőbuborék azt jelenti, hogy a tartalomajánló rendszerek és az egyénre szabott találati listák a felhasználó érdeklődéséhez, meggyőződéséhez közel álló tartalmakat előre rangsorolják, így a felhasználó egyre kisebb eséllyel találkozik a sajátjától ellentétes nézőpontokkal, ami végső soron intellektuális izolációhoz vezet.[913] A visszhangkamra-effektus pedig azt eredményezi, hogy az emberek csak a saját véleményüket megerősítő helyeslő álláspontokkal találkoznak az online kommunikáció során, ami gátat szab az eltérő gondolkodásmódú emberek közötti érdemi vitáknak. A tartalomszelekció egyik káros hatása lehet a nyúlüregeffektus *(rabbit hole effect).* A nyúlüregeffektus lényege, hogy a platformok tartalomajánló rendszerei igyekeznek a felhasználó által megtekintett tartalmakhoz hasonló tartalmakat kínálni, ami azt eredményezi, hogy a felhasználó egyre jobban elmerül egyfajta tartalomtípusban. Ahogyan a felhasználó egyre mélyebbre jut a virtuális nyúlüregben, egyes véleményeknek egyre radikálisabb, extrémebb formáival találkozhat, ami végső soron a felhasználó radikalizálódásához vezethet.[914]

Az indokolatlan tartalommoderálással is megakadályozhatják a szolgáltatók azt, hogy egyes értékes vélemények sok emberhez eljussanak. Jó példa erre, hogy a Facebook letiltott egy olyan élő közvetítést, amely azt mutatta be, hogy az amerikai rendőrök gyakran alkalmaznak túlkapásokat a feketékkel szemben.[915] Ez utóbbi, noha erőszakos tartalom, a társadalmi párbeszéd szempontjából fontos mondanivalót hordoz, és közbeszédre érdemes. Ezzel párhuzamosan az is előfordulhat, hogy kevésbé értékes, sőt kimondottan káros magatartások terjednek futótűzként, vagyis válnak virálissá. Ezek lehetnek ártatlan kihívások, mint a hazánkban is népszerű „jeges vödör”-kihívás *(ice bucket challenge),* amely odáig fajult, hogy több országban még politikusok is jeges vízzel teli vödröket borítottak magukra,[916] lehetnek viszont kifejezetten veszélyes magatartásra buzdító tartalmak is.

A vélemények szabad kifejezése mellett az információhoz jutás szabadságát és a médiapluralizmust is képesek kedvezőtlen irányba befolyásolni az algoritmusok. A platformoknak ugyanis megvan az a képessége, hogy az ajánlásokon és találati listákban rangsoroljanak, ezáltal egyes hangokat felerősítsenek, másokat pedig elhalkítsanak.

Ahhoz, hogy az algoritmusok minél pontosabb ajánlásokat tudjanak tenni, minél több adatra van szükségük, a *big data* (vagyis az olyan hatalmas adatkészletek, amelyek

912 Sunstein 2013.
913 How Filter Bubbles Distort Reality. Everything You Need to Know 2017.
914 Roose 2019.
915 Speri–Biddle 2016.
916 Sírás lett a vége – Falus Ferenc vödrös akciója 2014.

számítógépes eszközökkel jól elemezhetők különböző trendek, mintázatok és összefüggések feltárása érdekében) a mesterséges intelligencia működésének alapja. Minél több adata van a programnak, annál precízebb, ez viszont komoly adatvédelmi kérdéseket vet fel. Az általános adatvédelmi rendelet (GDPR)[917] több garanciát is biztosít az érintettek számára, amikor az adatkezelés automatizáltan történik. Az érintetteknek jogukban áll megismerni, hogy az adatok automatizált kezelése milyen logika alapján történt, valamint azt, hogy a profilalkotásra épített adatkezelés milyen következményekkel járhat.[918] Az érintettek jogosultsága annak kérelmezése, hogy ne terjedjen ki rájuk a kizárólag automatikus adatkezelésen alapuló döntések hatálya, amennyiben a döntés az érintette vonatkozó egyes személyes jellemzők kiértékelésén alapul, és amely rá nézve joghatással jár.[919] A GDPR példaként az online hitelkérelmeket és a munkaerő-toborzást citálja,[920] de a tartalomszűrések esetében is hozhat a szolgáltató olyan döntéseket, amelyek joghatással járnak. A tartalommoderálás körében a felhasználó tartalmának eltávolítása végső soron a felhasználó véleménynyilvánítási szabadságát korlátozza, ugyanakkor megnyitja annak lehetőségét, hogy a felhasználó a platformnál panasszal éljen, vagy bírósághoz forduljon, ha az eltávolítással nem ért egyet.

A tartalomszűrés felerősítheti a társadalom egyes csoportjai közötti diszkriminációt is. Szeretnénk azt hinni, hogy a gép a rangsorolás vagy szűrés során pártatlanul dönt, de ez nem feltétlenül van így, hiszen működése olyan adatkészleteken alapul, amelyeket emberi programozók táplálnak be. Az, hogy a döntéshozatal során milyen faktorokat vesz számításba, és ezeket hogyan súlyozza, szintén a beállításán múlik, amelyet emberek végeznek, akiknek a kulturális háttere, világnézete visszatükröződhet a beállításokban. A gép által ismert adatok Solon Barocas és Andrew Selbst szerint oly módon tökéletlenek, amely lehetővé teszi, hogy az algoritmus örököljje a korábbi döntéshozó előítéleteit, vagyis az adatkészlet tükrözi a társadalomban széles körben elterjedt torzulásokat.[921] Az Instagram DeepText algoritmusa[922] egy időben

[917] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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.

[918] GDPR (63) preambulumbekezdés.

[919] GDPR 22. cikk.

[920] GDPR (71) preambulumbekezdés.

[921] Barocas–Selbst 2016: 671.

[922] A DeepText olyan mélytanulásra képes algoritmus, amely, ha új kifejezéssel találkozik, akkor annak értelmét más környező szavak és ugyanannak a szónak más szövegkörnyezetben való megjelenése alapján következteti ki.

gyalázkodásnak minősítette a „mexikói" szót, amelyet az amerikai szlengben gyakran használnak az „illegális" kifejezés szinonimájaként.[923]

A tartalommoderálásra használt mesterséges intelligencia hátrányai gyakran a technikai korlátokból adódnak. Noha a technológia rohamléptékben fejlődik, nem tökéletes, a gépi hibákat pedig nehéz felismerni, még nehezebb korrigálni.

A tartalommoderáló rendszerek megfelelő működéséhez például nagyon pontosan meg kell határozni, hogy mi minősül káros tartalomnak. A brit médiahatóság (Ofcom) részére készített jelentés a mesterséges intelligencia felhasználásáról a tartalommoderálásban a káros tartalmakat hét fő- és számos alkategóriába sorolja.[924] Káros tartalomnak minősül a gyermekek elleni erőszak, az erőszak és az extrémizmus, a gyűlöletbeszéd és a zaklatás, a megbotránkoztató tartalmak (például az öngyilkosság, állatkínzás), a szexuális tartalmak, a kegyetlen vagy érzéketlen tartalmak, illetve a spam.

Nem elegendő azonban csupán a káros tartalmak kategóriáit megállapítani, hanem a tartalmak azonosításának feltételeit is meg kell határozni, vagyis rögzíteni kell, hogy melyek azok az elemek, amelyek egyenként vagy összességükben károssá tesznek egy tartalmat. Mindezt úgy kell megtenni, hogy az egy automatizált adatfeldolgozó eszköz számára is egyértelmű legyen, a jog és az informatika nyelve azonban nem ugyanaz. A jogszabályokban több olyan fordulat van, amely mérlegelést kíván a jogalkalmazó részéről. Vegyük például a becsületsértés vagy a rágalmazás tényállását, ahol a törvény egyik fordulata a kifejezés becsület csorbítására alkalmasságát jelöli meg a tényállásszerűség feltételeként. A becsület csorbítására alkalmasság nem objektív kategória, a bíróságnak azt kell mérlegelnie, hogy az adott élethelyzetben elhangzott kifejezés alkalmas volt-e a becsületcsorbításra, ezt pedig nem tudja megállapítani pusztán abból a tényből, hogy az állítás valamikor, valahol elhangzott. A mesterséges intelligenciának tehát egyértelmű, világos szabályokat kell megfogalmazni, amely sokszor a jogszabályi előírásoknál sokkal részletesebb szabályrendszert feltételez. A szűrőrendszerekbe például be lehet táplálni azokat a kifejezéseket, amelyeket becsületsértőnek minősítenek, a rendszer ezeket minden alkalommal ki fogja szűrni.

A közösségimédia-szolgáltatók a szűréshez több módszert együttesen alkalmaznak, amelyek attól függenek, hogy milyen típusú a vizsgált tartalom: más technikák szolgálnak a szöveges, a képes, az audiovizuális, illetve az ezeket vegyítő multimédiás tartalmak elemzésére. Egyes megoldások, mint a metaadat-elemzés, a *hashing* vagy a digitális ujjlenyomat elemzése *(fingerprinting)* bármilyen tartalom esetében

[923] Thompson 2017.
[924] Winchcomb 2019: 31.

használhatók.[925] A szöveges tartalmak elemzésének a kulcstechnikái pedig a szószedetek, feketelisták létrehozása, valamint a természetes nyelvfeldolgozás (*natural language processing* – NLP), amely gyakran mélytanulással *(deep learning)* támogatott. A legegyszerűbb módja a szöveges tartalmak automatizált szűrésének a szavak vagy nagyobb szövegrészek összevetése egy adatbázis elemeivel. A szöveges tartalmak moderálása történhet egyes feketelistán szereplő szavak alapján is. Ezeknek eklatáns példái a közösségi médiában alkalmazott káromkodásszűrők (*swear filter* vagy *profanity filter*).[926] Ezek a kezdetleges megoldások nem tudják értelmezni az emberi kommunikációra jellemző elemeket, az iróniát vagy akár a szarkazmust, és nem értelmezik a kontextust sem.[927] Az online világban márpedig nemcsak az számít, hogy mit, hanem az is, hogy hogyan kommunikálunk, nem mindegy például, hogy valaki egy tartalmat támogató vagy elítélő kommentárral tesz közzé; az online kommunikációban a közlések egyik legfontosabb attribútuma a kontextus.[928] Sokan használnak például kétértelmű szlenget, a magyar nyelvben a cigánysághoz tartozó személyekre gyakran használják a „svéd", valamint a „c típusú állampolgár" kifejezéseket, amelyek tipikusan olyan szavak, amelyek megfelelő moderálásához tisztában kell lenni a kontextussal, amelyben megjelennek. Sajtóhírekből gyakran hallunk arról, hogy a képi elemek felismerésére szolgáló algoritmusok sem reagálnak tökéletesen, szintén a kontextus ismeretének hiányára visszavezethető okból. A Facebook például a meztelenség tilalmára vonatkozó irányelv megsértése miatt törölte olyan szobrok képeit, mint a bolognai Neptun-szobor,[929] de olyan ikonikus fotók is a moderálás áldozatává váltak, mint a vietnami napalmtámadás elől menekülő kislányról készült Pulitzer-díjas kép.[930]

A kontextus fontosságát jól példázzák a mémek, amelyek megfelelő értékeléséhez az algoritmusnak kulturális hátteret, sztereotípiákat és attitűdöket is fel kellene ismernie, de említhetnénk az olyan kommunikációs eszközöket is, mint az irónia vagy a szarkazmus, ahol a kimondott szavak jelentésén túl nagy jelentősége van a beszélő mimikájának, hanglejtésének is. A mesterségesintelligencia-alapú tartalommoderálás egyelőre az egyszerű esetek szűrésére alkalmas, azokban az esetekben azonban, ahol kívülről jövő információra is szükség van a megértéshez, nem alkalmas, mivel

925 *The Impact of Algorithms for Online Content Filtering or Moderation* 2020.
926 Spectrumlabs 2023.
927 Grimmelmann 2015.
928 Weisbeck 2014.
929 Helmore 2017.
930 Temperton 2016.

ezek azok a tartalmak, amelyek gyakran még egy emberi moderátornak is fejtörést okozhatnak.[931] Ebbe a kategóriába sorolható a rágalmazás, a becsületsértés, a gyűlöletbeszéd, de még az álhírek is.

Natasha Duarte és szerzőtársai arra is rámutatnak, hogy a nagyobb cégek általában az angol nyelv alapulvételével fejlesztik algoritmusaikat, így a kisebb nyelveken közzétett tartalmak moderálása pontatlanabb, mivel kevesebb tanítóadat áll rendelkezésre, hátrányosabb helyzetbe hozva azokat, akik kisebb nyelvi közösségekhez tartoznak.[932]

Az algoritmus döntése alapvetően két irányban lehet téves:

- fals pozitív az a moderálási eredmény, amikor az algoritmus olyan tartalmat minősít törlendőnek, amelyet nem kellene;
- fals negatív az a döntés, amely ténylegesen ártalmas tartalmat minősít ártalmatlannak, s ennélfogva azt nem távolítják el.[933]

A mesterséges intelligencia esetében hangsúlyosabban van jelen a döntéshozatal átláthatatlanságának problémája is. Az algoritmusokat Frank Pasquale nyomán nem véletlenül nevezik fekete dobozoknak *(black box),*[934] hiszen egyedül a bemenő információk *(input),* valamint a generált eredmény *(output)* látható, a döntéshozatal menete átláthatatlan. Egy bírósági vagy hatósági döntéssel ellentétben a mesterséges intelligencia egy matematikai folyamat terméke, amelyhez nem tartozik indokolás. Míg az emberi moderátorokat fel lehet szólítani a döntésük indoklására, a mesterséges intelligencia esetében Maayan Perel és Niva Elkin-Koren egyenesen arra figyelmeztetnek, hogy ha bepillantunk a „motorháztető alá", és fel akarjuk tárni az algoritmusok döntésének a hátterében álló okokat, valójában komoly adatelemzést kellene végrehajtanunk ahhoz, hogy értékelhető információkat nyerjünk.[935]

A platformok egyelőre nem tudják megfelelően moderálni az élő közvetítéseket sem, mivel ez olyan valós idejű követést igényelne, ahol minden képkockán azonosítani kellene minden releváns elemet, továbbá az egyes képkockák közötti összefüggéseket valós időben.

A platformok sok esetben nem tudják azonosítani a manipulált felvételeket sem, amelyeket gyakran szintén mesterséges intelligencia segítségével hoznak léte. Az úgynevezett *deepfake* tartalmak esetében az alkalmazás képes arra, hogy egy-egy

931 Vincent 2019.
932 Duarte–Llansó–Loup 2017.
933 Cambridge Consultants 2019: 37.
934 Pasquale 2015.
935 Perel–Elkin-Koren 2017.

személynek az interneten nyilvánosan elérhető fényképeiből, videóiból olyan felvételt állítson össze, amely olyan, mintha valós lenne. Ha egy algoritmus megtanulta, mit kell moderálni, a hamis tartalmat gyártó algoritmus egy idő után megtanulja azt, hogy mi az, amit moderálnak, és változtat. Így ezek az algoritmusok gyakorlatilag egymást tanítják és fejlesztik.

Amennyiben a szűrésre használt algoritmusok nem működnek tökéletesen, károkat okozhatnak a demokratikus diskurzusokban: túlmoderálás esetén bizonyos közéleti vitákban értékes tartalmak elveszhetnek, az indokolatlan moderálásnak áldozatul esett felhasználók így nem tudnak élni véleménynyilvánítási szabadságukkal, az alulmoderálás viszont azzal járhat, hogy a tömegesen megjelenő, ám kevéssé értékes (például kattintásvadász) vagy ártalmas (félretájékoztató) tartalmak elnyomják a közérdeklődésre jogosan számot tartó tartalmakat.

A szabályozás lehetséges irányai

Ha azonosítottuk a mesterségesintelligencia-alapú tartalomszűrés előnyeit és hátrányait, meg tudjuk határozni, hogy melyek azok a területek, tulajdonságok, amelyeket a szabályozásnak meg kell erősítenie, és melyek azok, amelyeket meg kell szüntetnie.

Az Európai Bizottság *Fehér könyv*e szabályozás- és beruházásorientált stratégiát támogat,[936] ami azt jelenti, hogy a mesterséges intelligencia szabályozása elkerülhetetlen a nem túl távoli jövőben. A *Fehér könyv* egyik nevesített célja, hogy feltérképezze azokat a szakpolitikai lehetőségeket, amelyek elősegítik a mesterséges intelligencia terjedését és az azokhoz kapcsolódó kockázatok kezelését.[937]

A *Fehér könyv* azt is kiemeli, hogy a mesterséges intelligencia fejlesztőire és alkalmazóira már ma is alkalmazandók az alapvető jogokra, fogyasztóvédelemre, valamint a termékbiztonságra és termékfelelősségre vonatkozó uniós jogszabályok.[938] Ezeket a szabályokat azonban felül kell vizsgálni abból a szempontból, hogy a mesterséges

[936] *Fehér könyv a mesterséges intelligenciáról. A kiválóság és a bizalom európai megközelítése.* COM(2020) 65 végleges 1.

[937] *Fehér könyv a mesterséges intelligenciáról. A kiválóság és a bizalom európai megközelítése.* COM(2020) 65 végleges.

[938] *Fehér könyv a mesterséges intelligenciáról. A kiválóság és a bizalom európai megközelítése.* COM(2020) 65 végleges 12.

intelligencia sajátosságait figyelembe véve alkalmasak-e a megfelelő szintű védelem biztosítására, és amennyiben szükséges, felül kell vizsgálni a meglévő szabályokat.[939]

Arra azonban figyelemmel kell lenni, hogy a mesterségesintelligencia-alapú tartalomszűrő eszközök egyes tulajdonságai abból erednek, hogy a technológia nem kellően fejlett. Vannak olyan jelenségek, amelyeket a mesterségesintelligencia-alapú tartalomszűrés a technológiai korlátokból fakadóan jelenleg nem tud hatékonyan kezelni, itt tehát egy elhamarkodottan elfogadott szabályozás nem feltétlenül ér el sikereket.

A mesterségesintelligencia-alapú tartalomszűrés szabályozásának egyik kulcsfontosságú eleme lehet a minőségi adatkészlet használatának megfogalmazása, amely a mesterséges intelligencia esetében arra vonatkozik, hogy a megfelelő és pártatlan döntések elérése érdekében ezeket a rendszereket olyan adatkészlettel kell tanítani, amelyek a felhasználók, élethelyzetek sokszínűségét tükrözik. A Bizottság *Fehér könyv*ének egyik megállapítása, hogy az alapjogok sérelmének kockázata eredhet az egyoldalú, elfogultságokat tükröző adatok felhasználásából, például abból, ha a rendszer tanítása csak, vagy főként fehér férfiaktól származó adatok felhasználásával történt.[940]

A szabályozásnak megfelelően kell kezelnie a platformszolgáltató felelősségének kérdését. A jelenlegi felelősségi rendszer a platformszolgáltató harmadik személyek tartalmaiért viselt felelősségét limitálja, ez a konstrukció azonban a mesterségesintelligencia-alapú tartalommoderálás elterjedésével egyre kevésbé fenntartható. A *Forbes* cikke kiemeli, hogy a szolgáltatók több alkalommal demonstrálták a tartalomszűrő rendszerük fejlettségét (egyes rendszerek már milliszekundumok alatt meg tudják különböztetni a brokkolit a vadkendertől[941]), problémás helyzetek esetén azonban szívesen hivatkoznak arra, hogy a technológia még gyerekcipőben jár, és kezdetleges.[942] A mesterséges intelligenciát használó tartalomszűrés képességeinek tükrében szükséges újragondolni az egyes szolgáltatók kötelezettségeit és a felelősségük mértékét.

A szabályozásnak célul kell tűznie a működés átláthatóságának növelését. Frank Pasquale az internetes szolgáltatók és a pénzügyi szektor működését vizsgálva „feketedoboz-társadalomként" *(black box society)* jellemzi a jelenlegi társadalmi berendezkedést, amelyben mindenki megismerheti a döntéseket megalapozó adatokat és az eljárások

939 *Fehér könyv a mesterséges intelligenciáról. A kiválóság és a bizalom európai megközelítése.* COM(2020) 65 végleges.

940 *Fehér könyv a mesterséges intelligenciáról. A kiválóság és a bizalom európai megközelítése.* COM(2020) 65 végleges 13.

941 Hamilton 2019.

942 Leetaru 2019.

kimenetelét, a döntéseket is, arra azonban keveseknek van rálátásuk, hogyan következik az egyik a másikból.[943] Pasquale felhívja a figyelmet arra, hogy az átláthatóság önmagában nem elégséges feltétele az elszámoltathatóságnak, mert az átláthatósági követelményekre a szolgáltatók gyakran a folyamatok olyan mértékű megbonyolításával reagálnak, amely ellenőrizhetetlen és megérthetetlen.[944] Az Európa Tanács tanulmánya arra is rámutat, hogy a gépi tanulás esetében a mesterséges intelligencia fejlettsége elérhet egy olyan pontot, ahol az átláthatóság biztosításához nem elégséges csupán a döntéshozatali mechanizmust megalapozó forráskód átadása, hiszen a gép maga formálja a programját. A tanulmány az átláthatóságot nem az algoritmus működését szabályozó matematikai műveletek teljes körű nyilvánosságra hozatalában látja, hanem abban, hogy az algoritmus működtetője felhívja a figyelmet arra, hogy ilyen eszközt használ, elmagyarázza a döntések meghozatalának módját és szempontjait.[945]

A szabályozásnál figyelembe kell venni, hogy a jelenlegi mesterségesintelligencia-alapú tartalomszűrés csak az egyik lába egy sokrétű folyamatnak. A Tim Wu által hibrid rendszereknek nevezett konstrukcióban[946] a tartalomszűrés a humán és a mesterséges intelligencia egymást kiegészítő szerepére épít. A mesterséges intelligencia egyfajta előszűrést végez, azaz megjelöli azokat a tartalmakat, amelyek kifogásolhatók lehetnek, a moderátor pedig meghozza a végső döntést. A tanulásra képes mesterséges intelligenciák az emberi moderátorok visszajelzéseiből képesek tanulni, amennyiben a rendszer által megjelölt tartalom valóban káros, ez megerősíti a korábbi tapasztalatokat, amennyiben azonban a moderátor felülbírálja a mesterséges intelligencia döntését, az adatkészletben keletkezik egy új referenciapont, amely a következő döntés meghozatalakor már figyelembe vehető.

Az emberi felügyelet gondolata az Európai Bizottság jogellenes online tartalmak hatékony kezeléséről szóló ajánlásában is megjelenik. Az ajánlás szerint biztosítani kell, hogy a döntések pontosak és megalapozottak legyenek, ezért az emberi felügyeletet, illetve a döntések ember általi megerősítését lehetővé kellene tenni az automatizált tartalommoderálás esetében a hibás döntések elkerülése végett.[947] Az emberi tényező nemcsak a döntéshozatal validálása esetében lehet jelentős, hanem a döntésfelülvizsgálatban is szerepet játszhat. Meg kell teremteni annak lehetőségét, hogy

[943] Pasquale 2015: 3.
[944] Pasquale 2015: 16.
[945] Committee of Experts on Internet Intermediaries (MSI-NET) 2018: 38.
[946] Wu 2019: 2016.
[947] Az Európai Bizottság ajánlása a jogellenes online tartalmak hatékony kezeléséről (27) preambulumbekezdés és 20. pont.

a platformok döntéseivel szemben a felhasználó jogorvoslattal élhessen, amely lehet akár egy független szervezet – mint a Facebook által felállított Oversight Board – vagy állami szereplő, hatóság vagy bíróság. Ezekben az esetekben a végső döntéseket egy ember mondaná ki.

Az új technológiák esetében egyre gyakoribb a *soft-law* jellegű szabályozási eszközök alkalmazása, amelyek jelenleg azt a dilemmát próbálják áthidalni, hogy a technológia még túl képlékeny és ritkán alkalmazott ahhoz, hogy arra jogszabályt lehessen építeni. Az ilyen megoldások, noha csekély mértékben alkalmasak arra, hogy befolyásolják egyes piaci szereplők magatartását, nem biztos, hogy hatékonyak. Ződi Zsolt blogbejegyzésében több mint 150 mesterséges intelligenciát szabályozó etikai kódex létezéséről ír,[948] amelyek gyakran egymásnak ellentmondanak, de a mesterséges intelligenciával szoros kapcsolatban lévő robotika szabályozása is hasonló etikai kódexen keresztül kezdődött meg. Klein Tamás az uniós kezdeményezésre megalkotott Robotikai Chartáról ír, amely a robotika területén alkotott első etikai kódex.[949]

[948] Ződi 2020.
[949] Lásd Klein–Tóth 2018: 114; továbbá Klein 2018b.

VIII. Pro futuro – adalékok egy jövőbeli szabályozási koncepcióhoz

A kötet egyes részeiben igyekeztem betekintést nyújtani abba, hogy az online bűnözés milyen kihívásokat jelent napjaink jogalkotói és jogalkalmazói számára. A II., fogalmi alapokat lefektető rész illusztrálja azt, hogy az információtechnológiával kapcsolatos kriminális cselekedetek definiálása és csoportosítása, azoknak a szereplőknek a meghatározása, akik jelen vannak az online szolgáltatási térben, már önmagában is kihívást jelentő feladat. Az online tér elképesztő tempóban változik és fejlődik. Ez a gyors ütemű fejlődés egyrészt azt eredményezi, hogy folyamatosan alakulnak ki olyan új magatartásfajták, amelyek nem, vagy jelentős nehézségek árán helyezhetők el a meglévő fogalmi keretek között. Ugyanez igaz az online tér szolgáltatóira, hiszen rendszeresen alakulnak ki olyan új üzleti modellek, amelyek az egyes jogszabályba foglalt szolgáltatói kategóriák egyes tulajdonságait vegyítik. Ezek a multifunkciós vagy hibrid szolgáltatások már ma is léteznek, ilyenek a közösségimédia-platformok, amelyek egyszerre közvetítő szolgáltatók, azon belül tárhelyszolgáltatók, bizonyos funkcióik pedig videómegosztóplatform-szolgáltatásnak, esetleg online aukciós platformnak minősíthetők. Ezek a jelenségek a szabályozás számára azért jelentenek nehézséget, mert bármely területről legyen szó, szinte lehetetlen egymástól tisztán elkülöníthető, jól lehatárolható fogalmakat, kategóriákat alkotni, és azt sem lehet előre látni, hogy a jövőben létrejövő új jelenségek, szolgáltatófajták milyen hatékonysággal lesznek beilleszthetők a létező keretrendszerekbe. Mivel a jogrendszer jellemzően rugalmatlanul reagál a technológiai fejlődés következtében változó életviszonyokra, célszerű a jogforrási hierarchiában magasabban elhelyezkedő

jogszabályokat a technológiasemlegesség elvének szemmel tartásával megfogalmazni, a változásokra rugalmasabban reagálni képes keretkitöltő normákra bízva a részletszabályok finomhangolását. A magyar jogalkotás még érezhetően a törvényi szabályozást preferálja, az EU-ban azonban már erősen támogatott az úgynevezett ön- és társszabályozási rendszerek alkalmazása, ahol a részletszabályok kidolgozása megvalósulhat az iparággal együttműködésben.

Az EU által támogatott ön- és társszabályozás ugyanakkor számos kihívást tartogat, és legfeljebb csak a technológiaszabályozás esetében lehet sikeres. Az egyik ilyen kihívás az, hogy a létrejövő szabályozási struktúra ne az ipari lobbi eredménye legyen, hanem valóban a felhasználók javát szolgálja. Ebben a konstrukcióban az állam mint szabályozó, illetve a szolgáltató mint szabályozott jogalany viszonya átalakul, és a korábbi hierarchikus kapcsolat helyett inkább az érdekcsoportok közötti párbeszéd dominál.

Büntetőjogi területen azonban az ilyen ön- és társszabályozási rendszerek létrehozásának alkotmányos korlátai vannak, hiszen a magatartások büntetendővé nyilvánítása csak törvény által lehetséges. A pönalizációt nem igénylő, ám ártalmasnak tekintett magatartások esetében a szolgáltatók beavatkozhatnak magánszabályozás révén, ez azonban nem eredményezheti azt, hogy a büntetőjog folytonos felülvizsgálat nélkül marad. Sőt, a jövőben inkább fokozottan kell figyelni arra, hogy melyek azok az ártalmas online magatartások, amelyek már indokolttá teszik a büntetőjogi szankció kilátásba helyezését. A technológiaszabályozás és a büntetőjog metszéspontjainál tehát egy olyan dichotóm szabályozási rendszerre van szükség, amelyben a technikai környezetet szabályozó normák elkülönülnek a klasszikus büntető anyagi és eljárásjogi szabályokról.

A továbbiakban először a büntető anyagi és eljárásjogi szabályozási szükségszerűségekről és elképzelésekről szeretnék részletesen szólni, amelyek hosszabb távon biztosíthatják az informatikai bűncselekmények elleni eredményes fellépést. Ezt követően tárgyalom azoknak az eljárásjogi intézkedéseknek a naprakészségét, amelyek az informatikai bűncselekmények elleni eredményes fellépés esetén kulcsfontosságúak. Végül, de nem utolsósorban pedig arra teszek kísérletet, hogy a platformok hézagkitöltő magánszabályozásának nemzeti jogra gyakorolt hatásairól szóljak, illetve feltárjam, hogy hogyan reagálhat a nemzeti jog a külföldön letelepedett, magánkézben lévő piaci szereplők szabályozási törekvéseire.

A büntető anyagi jog reformja

Az egyes bűncselekményeket részleteiben tárgyaló fejezetekben több esetben felmerültek a jelenlegi szabályozási környezet gyenge pontjai és hiányosságai. Noha a magyar büntető törvénykönyv alapvetően a modern anyagi kódexek közé tartozik, mégis van néhány olyan terület, ahol nem minden esetben tudott lépést tartani a folyamatosan változó technológiai környezet miatt megjelenő új ártalmas magatartásokkal. Vannak olyan területek is, ahol az életviszonyok egyszerűen olyan irányban fejlődtek, hogy már nem indokolt fenntartani egyes magatartásoknak a büntetőjogi szankcióval való fenyegetését. A büntető anyagi jog az alábbi területeken szorulna reformra.

Az elmúlt évek gyakorlata azt mutatja, hogy az etikus hackerek tevékenységének a megítélése sokszor problémát jelent a jogalkalmazás során. Noha az etikus hackerek tevékenysége kimeríti a Btk. 423. §-ban foglalt tényállást, cselekedeteik általában nem károkozásra, hanem valamilyen sérülékenység kéretlen kivizsgálására irányulnak. Az etikus hackerek megítélése a bírói gyakorlatban egyértelmű, bizonyos esetekben ugyanis a bíróság közérdekű bejelentőnek minősíti az információs rendszerek sérülékenységeinek a hackerek eszköztárával történő feltárását, más esetekben azonban elmarasztaló ítéletet hoznak. Mivel a joggyakorlat ezen a területen nem egységes, indokoltnak tartanám, hogy az ilyen jó szándékú „elkövetők" esetében a törvény adjon lehetőséget a büntethetőség megszüntetésére. Ebben az esetben szükséges lehet azoknak a feltételeknek a rögzítése is, amelyeket a foglalkoztatási viszonyon kívül eljáró etikus hackereknek teljesíteniük kell ahhoz, hogy a cselekményüket ne kövesse büntetőjogi szankció. Ilyen követelmény például a jóhiszeműség (abban a tudatban járt el, hogy javítja a feltört rendszer biztonságát), az arányosság (a sérülékenység kivizsgálásához szükséges hozzáférésen túlmenően nem használja a rendszert), illetve a bejelentési és dokumentálási kötelezettség (tevékenységét lépésről lépésre köteles dokumentálni, és az eredményeit átadja a rendszert működtető személynek vagy szervezetnek).

A kötet V. része több olyan magatartásra hívja fel a figyelmet, amely a büntetőjog határterületén helyezkedik el, mivel nem mindig egyértelmű, hogy ezek megvalósítják-e valamely törvényben szereplő bűncselekmény törvényi tényállását. Idetartozik a pornográf felvételeknek hozzájárulás nélkül történő közzététele, a *cyberbullying*, a félretájékoztatás, illetve a szélsőségesen erőszakos tartalmak terjesztése. Ezeket a problémákat a hatályos jogunk nem kezeli kielégítően, ezért mindenképp ajánlott a büntető anyagi jog felülvizsgálata az információs társadalom új jelenségeinek figyelembevételével.

A hozzájárulás nélkül közzétett pornográf felvételek és a hamisított felvételek által okozott probléma kétséget kizáróan valós. Az előfordulás számosságára és az áldozatoknak okozott kárra tekintettel e cselekmények büntetőjogi fenyegetettsége egyáltalán nem tűnik túlzó lépésnek. Az, hogy az USA, Németország, Franciaország, Olaszország és az Egyesült Királyság is megtette a kezdő lépéseket ebbe az irányba, azt mutatja, hogy olyan problémáról van szó, amely országtól és régiótól független, és amelyre figyelni kell. Napjainkban „nem létezik éles határ a pornográfia és az internetes kultúra egyéb szegmensei között, a mindennapok részévé váltak ezek a tartalmak, nem keltenek többé megütközést",[950] ezért a szabályozásnak sem szabad szemérmesnek maradnia, ha a pornográf tartalmak által okozott sérelmekről van szó. A szabályozási megoldások egyelőre még vetnek fel kérdéseket. Alapjogi szempontból talán az egyik legjelentősebb az, hogy az egyének számára okozott sérelem indokolja-e a közléstípus előzetes, teljes tilalmát és a szólásszabadság büntetőjogi eszközökkel történő korlátozását. Az amerikai szakirodalmi álláspontok szerint erre a kérdésre a válasz igen, hiszen a sérelmek utólagos orvoslása, a reparáció nehezen lehetséges, így inkább a prevencióra szükséges összpontosítani. Ezek a sérelmek mélyebb sebet ejtenek a társadalmon, nem csupán egymástól független egyéni jogsérelmek, alkalmasak ugyanis a nemek közötti egyenlőtlenségek konzerválására, sőt erősítésére.

A *cyberbullying* valójában egy olyan halmaz, amely többféle magatartást foglal magában. A *cyberbullying*nak minősülő magatartások ugyan tartalmaznak közös elemet – lelki sérülést okoznak a sértettnek –, de több ponton különböznek is egymástól. Az *cyberbullying* körébe tartozó egyes magatartások közötti különbségek gyakorlatilag kivitelezhetetlenné teszik azt, hogy létrehozzunk egyetlen olyan önálló tényállást, amely hatékony büntetőjogi védelmet nyújt. Ezt támasztja alá, hogy a kifejezésnek már a magyarra fordítása is okoz nehézségeket, hiszen egyes szerzők a zaklatással, mások a megfélemlítéssel azonosítják, amelyek a büntetőjogi értékelés szempontjából korántsem ugyanolyan magatartások. A *cyberbullying* mint fogalom lehet, hogy figyelemfelkeltően hangzik, de nem képes leírni ezt az igencsak összetett jelenséget. A fogalom mögött álló magatartásokat vizsgálva arra jutunk, hogy azok egy részét a büntetőjog már ma is szankcionálja, így a magyar jogban büntetendő a rágalmazás, a becsületsértés, a zaklatás, az öngyilkosságra rábírás, a kényszerítés is. Az előbbiekben felsorolt bűncselekmények nincsenek az online térhez kötve, éppen ezért ugyanúgy elkövethetők offline, mint a virtuális világban. Természetesen nem zárható ki, hogy

[950] Pap 2020.

vannak olyan közlések, amelyek megvalósítják a *cyberbullying*ot, mégsem rendelik büntetni őket, ezeknek a közléseknek a kriminalizálása viszont már alkalmas lehet arra, hogy a szólásszabadságot elfogadhatatlan mértékben korlátozza. A sértő közlések, bántó vélemények visszaszorítása érdekében álláspontom szerint célszerűbb a büntetőjognál kevésbé radikális eszközöket keresni. Ilyen eszközöket alkalmazhatnak az iskolák, de akár azok az online platformok is, ahol a fiatalok kommunikációjának nagy része zajlik. Az eszközök lehetnek tartalommoderálásban megnyilvánuló eszközök (mint a sértő közlések törlése, a felhasználók tiltása egyes csoportokból vagy akár a teljes szolgáltatásból), de lehetnek a felhasználók tudatosságának fejlesztésére hivatott eszközök is.

Hasonlóan alulszabályozott a szélsőségesen erőszakos, illetve a más embereket megalázó helyzetben ábrázoló felvételek kérdése is. Noha a büntetőjogunk ismer olyan tényállásokat, mint a kegyeletsértés vagy a kiszolgáltatott helyzetben lévő személy megalázása, ezek sokszor nem fedik azokat a tartalomközléseket, amelyek az interneten terjednek.

Az említett hiányosságok mellett indokolt rávilágítani egy büntetőpolitikai jellegű dilemmára is, mégpedig arra, hogy mikortól indokolt büntetőjogi szankció kilátásba helyezése. Attól ugyanis, hogy egy cselekményt morálisan elítélendőnek tartunk, az nem biztos, hogy olyan mértékben veszélyes a társadalomra, hogy kriminalizálása indokolt. A korábban már említett magánszabályozás és a büntetőjogi szabályozás közötti kényes egyensúly fenntartása a jövő egyik nagy jogpolitikai kihívása lesz. Ami egészen biztos, hogy egy-egy kodifikációs reformmal korántsem ér véget a munka: az online tér magatartásait folyamatosan figyelemmel kell kísérni, szükség szerint pedig a megalkotott normák korrekciója is elvégzendő.

A büntetőeljárás-jog reformja

A kötet részletesen szól az elektronikus adat ideiglenes eltávolításáról, ahol a kényszerintézkedés alapjait a Be., míg a szolgáltatók kötelezettségeivel kapcsolatos technikai jellegű szabályokat az Eht. szabályozza. Hasonló rendszert figyelhetünk meg az elektronikus adat lefoglalásánál, ahol az alapokat szintúgy a Be. fekteti le, a részletszabályokat viszont rendeleti szinten szabályozta a jogalkotó.

Az állami szabályozás hézagait jelenleg a platformok magánszabályozás révén töltik ki. Ez egyrészről üdvözlendő, hiszen a felhasználók számára a védelem minimális szintje biztosított, és nem maradnak védtelenül abban az átmeneti időszakban,

amíg a jogrendszer nem reagál az új jelenségekre. Ha megfigyeljük az online tér folyamatait, azt találjuk, hogy vannak olyan szolgáltatók, amelyek megalkotják és be is tartatják saját szabályaikat már-már az állami szabályozás konkurenciáivá válva. Előnye továbbá az, hogy a szolgáltatók rugalmasabban reagáló saját szabályai az állami büntető jogrendszer számára olyan korai jelzőrendszert jelenthetnek, amely időben felhívja az állam figyelmét az esetleges szabályozási szükséghelyzetre. Több szempontból viszont ez a konstrukció egyáltalán nem szerencsés. Hátránya ennek a megoldásnak, hogy az egyes platformok eltérő szigorral, szemléletmóddal szabályozzák ugyanazokat a jelenségeket. A felhasználók számára ez sokszor bizonytalan helyzetet teremt, ami a hatékony jogérvényesítés korlátja lehet, ráadásul még a nagy szolgáltatókat is sokszor éri kritika amiatt, hogy nem kezelik elég átláthatóan a felhasználói panaszokat. Az állami szuverenitás szemszögéből nézve pedig kifejezetten rémisztő, hogy magánkézben lévő szolgáltatók töltenek be magatartás-formáló, szankcionáló, ezzel együtt pedig alapjog-korlátozó szerepet. Az államok esetében az évszázados jogfejlődés eredményeként kialakult államhatalmi ágak elválasztásának koncepciója a magáncégként működő platformok esetében nem létezik. Noha a Facebook kísérletezik egy külső felügyelő testület (Oversight Board) működtetésével, kérdés, hogy a gazdasági társaságok alapvetően profitorientált szemlélete miként állítható a közjó szolgálatába, e platformok kontrollját ezért mindenképpen célszerű az államhoz telepíteni.

Már a sajtó vonatkozásában is felmerült, hogy az a negyedik hatalmi ág,[951] amelynek egyik feladata a hatalom ellenőrzése. Cservák Csaba ugyan elveti a sajtó hatalmi ágként történő definiálását, de azt elismeri, hogy a sajtó úgynevezett uralmi ág, amely „az egy bizonyos rendezési elv alapján szerveződő tényezőknek a rendszere, amelyek közhatalmi funkciókat nem töltenek be, mindazonáltal a szervezési elvből vagy tevékenységből kifolyólag a társadalom nagy részére hatást gyakorolnak".[952] Ha a sajtót kiterjesztjük a médiára és a közösségi médiára, kétségkívül olyan uralmi tényezőt láthatunk, amely globálisan is komoly hatással van a társadalmi folyamatokra. Amennyiben a média valóban a negyedik hatalmi ág, akkor a közvetítő szolgáltatók szabályozásának túl kellene lépnie a szabályozó állam, szabályozott jogalany felépítésű hierarchikus kapcsolaton, és egy olyan partnerség kialakítására kellene törekedni, ami a fékek és ellensúlyok rendszerét valósítja meg államon kívüli szereplőkkel.

951 Lásd Nagy 2007: 49–56.
952 Cservák 2015: 32.

Ennek lehetséges gyökere azokban az ön- és társszabályozási rendszerekben sarjadzik, amelyeket az Európai Unió is támogat, és amely lehetővé teszi, hogy az államok és a globális hatás gyakorlására képes online szereplők kölcsönösen ellenőrizzék egymást. A megszokott alá-fölé rendeltségen túllépő, inkább szimbiotikusként jellemezhető kapcsolat azonban szükségképpen maga után vonja a jelenlegi felelősségi rendszerek újragondolását. A jelenlegi korlátozott felelősségi rendszer a harmadik személyek által elhelyezett tartalmakért telepít felelősséget a szolgáltatóra, ami egy fenntarthatatlan rendszert eredményezett. Mind az USA, mind az Európai Unió célul tűzte ki a platformok immunitásának, illetve korlátozott felelősségének felszámolását.[953] A szabályozás viszont lassan halad, az EU-ban 2022-ben elfogadott DSA rendelet például az irányváltás ellenére is megtartja az online platformok korlátozott felelősségének rendszerét. Új alapokra helyezni a szolgáltatói felelősséget nem egyszerű, hiszen ha mereven ragaszkodunk ahhoz, hogy a szolgáltatókat a harmadik személyek tartalmaiért tegyük felelőssé, az lesújtó lenne a szektorra nézve. A szolgáltatókat a harmadik személyek tartalmáért korlátlanul felelőssé tevő rendszer az online szólásszabadság radikális korlátozásához vezetne, hiszen a szolgáltatók a felelősség elkerülése végett még szigorúbb szabályokat vezetnének be. A járható út az lenne, ha a szolgáltatókra tartalmakkal, átláthatósággal, panaszkezeléssel kapcsolatban telepítene kötelezettségeket a jogrendszer, ami értelemszerűen erősebb állami szabályozást feltételez, és a szolgáltatók részéről nagyobb aktivitást vár el, mint a jelenlegi platformpasszivitásra építő felelősségi rendszer. A szolgáltatók felelősségre vonása ebből következően viszont szűkebb körű lehetne, nem akkor, ha egy jogsértő tartalom mégis felkerül a szolgáltatásba, hanem akkor, ha a szolgáltató vétkesen elmulaszt eleget tenni kötelezettségének.

Mind a DSA, mind az e-bizonyításról szóló rendelettervezet és a gyermekek szexuális kizsákmányolásáról szóló rendelettervezet is a jelenleginél nagyobb hangsúlyt helyez a közvetítő szolgáltatók közreműködésére a büntetőeljárásokban. Az új típusú eszközök magyar jogba integrálása azonban több kérdést felvet, ahogyan az is, hogy ezek az új eszközök egymással hogyan fognak együttműködni. A mondás, miszerint sok bába közt elvész a gyerek, a jogellenes tartalmak elleni fellépés esetében is irányadó, hiszen ha az igénybe vehető eszközök rendszere túl szövevényes, azok az eljárások egyszerűsítése helyett inkább bonyolítják majd azokat. Csábító gondolat

[953] A Biden-adminisztráció egyik célkitűzése kifejezetten az online platformoknak immunitást biztosító CDA 230. §-ának eltörlése. Lásd Kelly 2020.

lenne a tartalommoderálását a platformszolgáltatókra bízni, ez ugyanakkor az igazságszolgáltatás olyan jellegű privatizációjával járna, ami a büntetőjogi normát is sértő tartalom-bűncselekmények esetében álláspontom szerint nem megengedhető.

A jelenlegi szabályozási javaslatok egyik nagy hiányossága ráadásul, hogy kizárólag a nagy piaci szereplőkre fókuszálnak. A Facebook, a Twitter, a TikTok és a Google gyakran felbukkanó szereplői az új szabályozási törekvéseknek, amelyek nem veszik számításba, hogy az online szolgáltatási tér ennél sokkal összetettebb. Sokszor a legártalmasabb tartalmakat hordozó platformok azok, amelyek a legalacsonyabb szintű védelmet nyújtják. A kötet szólt a Pornhub-esetről, amelynek folyományaként nagy hitelkártya-szolgáltatók függesztették fel a fizetési szolgáltatások nyújtását a platformnak, mert gyermekekről és szexuális erőszakról készült felvételek szerepeltek rajta.[954] A nevezett szolgáltató kifejezetten nagy szereplőnek minősül a saját kategóriájában, számos olyan kisebb pornográf tartalmakra szakosodott szolgáltató létezik, amelyre nem irányul ekkora figyelem. A szélsőséges erőszakot ábrázoló tartalmakat megjelenítő oldalakról szintén esett szó a kötetben. Megbecsülni is nehéz, hány ilyen portál lehet, amiatt is, hogy a *dark web* az illegális tartalomkínáló portálok jelentős részének ad otthont. Ezek a szolgáltatások kézzelfogható problémát jelentenek, hiszen az internetes tartalomáramlás egyik jellemzője, hogy a *niche* az új mainstream.[955] A tartalomáramlás új modelljében a korábban lineárisan szerveződő nagy tömegű közönség fragmentálódik, ahogyan az igény szerint lekérhető tartalmak aszinkronossá teszik a fogyasztást. A korábbi nagy tömegű felhasználói bázisok kisebb csoportokra tagozódnak, és az érdeklődésük szerinti rétegszolgáltatások felé fordulnak. Ezek a rétegszolgáltatások gyorsan jönnek létre, és gyorsan el is tűnhetnek, kis méretüknél és számosságuknál fogva pedig problémát jelenthetnek a techóriásokra koncentráló jogalkotónak. A nagy cégek túlszabályozása, a büntetőjogi határterületen lévő tartalmak generális tilalmazása könnyen eredményezheti, hogy az érdeklődő közönség ezek felé a nehezen ellenőrizhető rétegszolgáltatások felé sodródik, vagyis a nem kellően átgondolt jogalkotás nem megszünteti, hanem szétteríti a problémákat az interneten. A szabályozási koncepciók kidolgozásakor tehát olyan lépcsőzetes rendszer kialakítására kell törekedni, amely a nagy szereplők kontrollja mellett kellő hatásfokkal szabályozza a kisebb szereplők tevékenységét is.

[954] Kristof 2020.
[955] Allocca 2018.

A kisebb szereplők tartalomterjesztésre gyakorolt hatását megvillantva érezhető, hogy a kutatási feladat a kötet lezárásával még nem ért véget. Az alapok lefektetése, az online tér jogsértéseivel, illetve a közvetítő szolgáltatók szerepével kapcsolatos szabályozási dilemmáknak az ismertetése azonban reményeink szerint alkalmas azoknak az irányoknak a kijelölésére, amelyek segítenek az élhető és biztonságos online tér megteremtésében.

Vákát oldal

Felhasznált források és irodalom

Könyvek és folyóiratcikkek

Allcott, Hunt – Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* 31(2), 211–236. Online: https://doi.org/10.1257/jep.31.2.211

Allocca, Kevin (2018): *Videocracy.* New York: Bloomsbury.

Ambrus István (2021): *Digitalizáció és büntetőjog.* Budapest: Wolters Kluwer.

Ambrus István – Ujvári Ákos (2016): A zaklatás bűncselekményének gyermekévei. *Magyar Jog,* 63(7–8), 424–435.

Andén-Papadopoulos, Kari (2009): Body Horror on the Internet. US Soldiers Recording the War in Iraq and Afghanistan. *Media, Culture and Society,* 31(6), 921–938. Online: https://doi.org/10.1177/0163443709344040

Aranyi Attila – Koós Szabolcs – Dörnyei József (1979): *Bevezetés a jogi informatikába.* Budapest: Tankönyvkiadó.

Auerbach, Shira (2009): Screening Out Cyberbullies. Remedies for Victims on the Internet Playground. *Cardozo Law Review,* 30(4), 1641–1675.

Augusztinyi Krisztina (2008): A számítástechnika felhasználásával megvalósuló bűncselekmények. *Rendészeti Szemle,* 56(3), 66–79.

Baker, C. Edwin (1996–1997): Harm, Liberty, and Free Speech. *Southern California Law Review,* 70(4), 979–1020.

Balkin, Jack M. (2018): Free Speech in the Algorithmic Society. Big Data, Private Governance, and New School Speech Regulation. *University of California Davis Law Review,* 51, 1149–1210. Online: https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-3_Balkin.pdf

Balogh Zsolt György (1998): *Jogi informatika.* Budapest: Dialóg Campus.

Barocas, Solon – Selbst, Andrew D. (2016): Big Data's Disparate Impact. *California Law Review,* 104(3), 671–732.

Bartóki-Gönczy Balázs – Pogácsás Anett (2019): A médiatartalom-szolgáltatásnak nem minősülő internetes tartalomszolgáltatások szabályozása. In Koltay András (szerk.): *Magyar és európai médiajog.* Budapest: Wolters Kluwer, 719–756.

Bayer Judit (2003): A számítástechnikai bűnözés elleni küzdelem nemzetközi dimenziói. *Belügyi Szemle,* 51(7–8), 98–126.

Bayer Judit (2007): A szolgáltatások felelősségének szabályozása a legújabb alkalmazások és az amerikai tapasztalatok fényében. *Médiakutató,* 8(4), 37–47.

Békés Ádám (2014): Büntetőjogi rágalmazás és becsületsértés. In Csehi Zoltán – Koltay András – Navratyil Zoltán (szerk.): *A személyiség és a média a polgári és a büntetőjogban. Az új Polgári Törvénykönyvre és az új Büntető Törvénykönyvre tekintettel.* Budapest: CompLex Wolters Kluwer, 379–422.

Belovics Ervin – Erdei Árpád szerk. (2018): *A büntetőeljárási törvény magyarázata.* Budapest, HVG-ORAC.

Berki Gábor (2016): Kiberháborúk, kiberkonfliktusok. In Pintér István (szerk.): *A virtuális tér geopolitikája.* Budapest: Geopolitikai Tanács, 260–264.

Blutman László – Karsai Krisztina – Katona Tibor (2008): Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? *Ügyészek Lapja,* 15(3), 5–16.

Boros Anita (2016): *Közérthető közigazgatási hatósági eljárás* [ePub]. Budapest: Wolters Kluwer. Online: https://doi.org/10.55413/9789632956220

Borsi Zoltán – Baturin, J. M. szerk. (1989): *Számítástechnika és a jog. A tudományos-műszaki haladás hatása a jogi életre.* Ford. Vajda Alajos – Erdész Ivánné Zaljajeva Szurija. Budapest: KJK.

Brandeis, Louis D. – Warren, Samuel D. (1890): The Right to Privacy. *Harvard Law Review,* 4(5), 193–220. Online: https://doi.org/10.2307/1321160

Brenner, Susan W. (2001): State Cybercrime Legislation in the United States of America. A Survey. *Richmond Journal of Law and Technology,* 7(3), 28–32.

Brenner, Susan W. (2006): Cybercrime Jurisdiction. *Crime Law and Social Change,* 46(4–5), 189–206. Online: https://doi.org/10.1007/s10611-007-9063-7

Brenner, Susan W. (2010): *Cybercrime. Criminal Threats from Cyberspace.* Santa Barbara: Praeger.

Brenner, Susan W. – Koops, Bert-Jaap (2004): Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law,* 4(1), 1–46.

Britz, Marjie T. (2013): *Computer Forensics and Cyber Crime. An Introduction.* 3. kiadás. London: Pearson.

Brooks, Rodney A. (2003): *Flesh and Machines. How Robots Will Change Us.* New York: Vintage.

Burke, Jason (2003): *Al Qaeda. The True Story of the Radical Islam.* London: I.B. Tauris.

Callanan, Cormac (2015): Evolution, Implementation and Practice of Internet Self-regulation, Co-regulation and Public–Private Collaboration. In Tropina, Tatiana – Callanan, Cormac (szerk.): *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security.* Berlin–Heidelberg: Springer.

Calvert, Clay (2010): Fighting Words in the Era of Texts, IMs and E-mails. Can a Disparaged Doctrine Be Resuscitated to Punish Cyber-Bullies? *DePaul Journal of Art, Technology and Intellectual Property Law,* 21(1). Online: https://via.library.depaul.edu/cgi/viewcontent.cgi?&article=1080&context=jatip

Casey, Eoghan (2012): *Digital Evidence and Computer Crime.* 3. kiadás. Amsterdam: Elsevier.

Christián László (2015): Kiberrendészet. A jogellenes internetes tartalmak blokkolásának lehetőségei az új hazai szabályozás tükrében. In Koltay András – Török Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején 2.* Budapest: Wolters Kluwer, 491–515.

Citron, Danielle – Franks, Mary Anne (2014): Criminalizing Revenge Porn. *Wake Forest Law Review,* 49, 345–391.

Cohen, Stanley (2004): *States of Denial. Knowing about Atrocities and Suffering.* Cambridge: Polity Press.

Collingridge, David (1980): *Social Control of Technology.* New York: St. Martin's Press.

Cservák Csaba (2015): A hatalmi ágak megosztásának XXI. századi kérdései az Alaptörvényt követően. *Pro Futuro,* 5(2), 24–37. Online: https://doi.org/10.26521/Profuturo/2015/2/5359

Csink Lóránt – Mayer Annamária (2012): *Variációk a szabályozásra. Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban.* Budapest: Médiatudományi Intézet.

Dalgaard-Nielsen, Anja (2010): Violent Radicalization in Europe. What We Know and What We Do Not Know. *Studies in Conflict & Terrorism,* 33(9), 797–814. Online: https://doi.org/10.1080/1057610X.2010.501423

David-Ferdon, Corinne – Hertz, Marci Feldman (2007): Electronic Media, Violence and Adolescents. An Emerging Public Health Problem. *Journal of Adolescent Health,* 41(6). Online: https://doi.org/10.1016/j.jadohealth.2007.08.020

Denning, Dorothy E. (2010): Terror's Web. How the Internet is Transforming Terrorism. In Jewkes, Yvonne – Yar, Majid (szerk.): *Handbook of Internet Crime.* Cullompton: Willan, 194–213.

Diaz, Fernando L. (2016): Trolling & the First Amendment. Protecting Internet Speech in the Era of Cyberbullies & Internet Defamation. *University of Illinois Journal of Law, Technology & Policy,* 16(1), 135–159.

Dinwoodie, Graeme B. (2017): A Comparative Analysis of the Secondary Liability of Online Service Providers. In Dinwoodie, Graeme B. (szerk.): *Secondary Liability of Internet Service Providers.* Berlin–Heidelberg: Springer, 1–72.

Dobrocsi Szilvia – Domokos Andrea (2018): Kiberbűnözés. In Homicskó Árpád Olivér (szerk.): *Egyes modern technológiák etikai, jogi és szabályozási kihívásai.* Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 49–73.

Domonkos Katalin (2014): Cyberbullying: zaklatás elektronikus eszközök használatával. *Alkalmazott Pszichológia,* 14(1), 59–70.

Dornfeld László (2018): A közvetítő szolgáltatók felelőssége az internetes tartalmakért. *Kriminológiai Közlemények,* 78, 101–117.

Dornfeld László (2019): Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs–Budapest: Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 46–63.

Dornfeld László – Mezei Kitti (2017): Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog,* 14(6), 32–37.

Dósa Imre szerk. (2008): *Az informatikai jog nagy kézikönyve.* Budapest: CompLex.

Downes, Larry (2009): *The Laws of Disruption. Harnessing the New Forces that Govern Life and Business in the Digital Age.* New York: Basic Books.

Doyle, Charles (2014): *Cybercrime. An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws.* Washington, D.C.: Congressional Research Service. Online: https://crsreports.congress.gov/product/pdf/RL/97-1025

Dudás Ágnes (2014): *Szerzői jog a digitális korban.* Budapest: Typotex.

Dworkin, Ronald (1981): Is There a Right to Pornography? *Oxford Journal of Legal Studies,* 1(2), 177–212. Online: https://doi.org/10.1093/ojls/1.2.177

Eneman, Marie – Gillespie, Alisdair A. – Stahl, Bernd Carsten (2009): Criminalising Fantasies. The Regulation of Virtual Child Pornography. *Proceedings of the 17th European Conference on Information Systems,* 8–10. Online: www.academia.edu/54342712/Criminalising_Fantasies_The_Regulation_of_Virtual_Child_Pornography

Faludi Gábor (2007): A jogsértéssel elért gazdagodás megtérítésére irányuló igény a szerzői jogi törvény bírói gyakorlatában. *Védjegyvilág,* 17(1–2), 36–48.

Faludi Gábor (2011): A szerzői mű egysége védelmének egyes kérdései. *Infokommunikáció és Jog,* 8(5), 163–169.

Fantoly Zsanett (2012): *A büntető tárgyalási rendszerek sajátosságai és a büntetőeljárás hatékonysága.* Budapest: HVG-ORAC.

Farmand, Musa K. Jr. (2016): Who Watches This Stuff? Videos Depicting Actual Murder and the Need for a Federal Criminal Murder-Video Statute. *Florida Law Review,* 68(6). Online: https://scholarship.law.ufl.edu/flr/vol68/iss6/19

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

Fehér Katalin (2016): *Digitalizáció és új média. Trendek, stratégiák, illusztrációk.* Budapest: Akadémiai.

Finszter Géza (2003): *A rendészet elmélete.* Budapest: KJK-Kerszöv.

Frosio, Giancarlo (2018): Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility. *Oxford International Journal of Law and Information Technology,* 26(1). 1–33. Online: http://dx.doi.org/10.2139/ssrn.2976023

Garzuly Éva (2015): A büntetőjog mint ultima ratio az egyes alkotmánybírósági határozatok tükrében. *Büntetőjogi Szemle,* 4(1–2), 42–49.

Gebicka, Aleksandra – Heinemann, Andreas (2014): Social Media & Competition Law. *World Competition,* 37(2), 149–172. Online: https://doi.org/10.54648/woco2014017

Gelányi Anikó – Csepely-Knorr Tamás (2009): A jogosulatlan wifi használat minősítése, avagy ha nyitva van az ajtó, akkor bemehetek? *Infokommunikáció és Jog,* 6(5), 201–205.

Gercke, Marco (2011): *Understanding Cybercrime. A Guide for Developing Countries.* Geneva: ICT Applications and Cybersecurity Division, Policies and Strategies Department – ITU Telecommunication Development Sector.

Gillespie, Alisdair A. (2016): *Cybercrime. Key Issues and Debates.* New York: Routledge.

Gillespie, Tarleton (2010): The Politics of 'Platforms'. *New Media & Society,* 12(3), 347–364.

Görgényi Ilona et al. (2020): *Magyar büntetőjog. Különös rész.* Budapest: Wolters Kluwer.

Grad-Gyenge Anikó (2019): *Kézikönyv a szerzői jog érvényesítéséhez.* Budapest: ProArt Szövetség a Szerzői Jogokért.

Grimmelmann, James (2015): The Virtues of Moderation. *Yale Journal of Law and Technology,* (17)1, 42–109. Online: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1110&context=yjolt

Gyányi Sándor (2011): *Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudomány Kar Katonai Műszaki Doktori Iskola. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12255

Gyertyánfy Péter (2013): A szerzői jog bírói gyakorlata 2006-tól: a jogok keletkezése, forgalmuk; a személyhez fűződő jogok. *Iparjogvédelmi és Szerzői Jogi Szemle,* 8(3), 70–92.

Halmai Gábor (2004): Becsületvédelem és sajtószabadság. *Fundamentum,* 8(4), 81–94. Online: https://epa.oszk.hu/02300/02334/00017/pdf/EPA02334_Fundamentum_2004_04_081-094.pdf

Harris, Douglas (2019): Deepfakes. False Pornography Is Here and the Law Cannot Protect You. *Duke Law & Technology Review,* 17(1), 99–128. Online: https://scholarship.law.duke.edu/dltr/vol17/iss1/4

Hill, Joshua B. – Marion, Nancy E. (2016): *Introduction to Cybercrime. Computer Crimes, Laws and Policing in the 21st Century.* Santa Barbara: Praeger.

Hoel, Helge – Vartia, Maarit (2018): *Bullying and Sexual Harassment at the Workplace, in Public Spaces, and in Political Life in the EU.* Online: www.europarl.europa.eu/RegData/etudes/STUD/2018/604949/IPOL_STU(2018)604949_EN.pdf

Ibolya Tibor (2011): A „torrentrazziák" büntetőjogi megítélése. *Belügyi Szemle,* 59(2), 49–59.

Irk Ferenc szerk. (1999): Magyar kriminálpolitikai és rendvédelmi koncepció. *Kriminológiai Közlemények,* 57, 15–126.

Kabay, Michel E. (2008): *A Brief History of Computer Crime. An Introduction for Students.* Online: www.mekabay.com/overviews/history.pdf

Karsai Krisztina (2019a): A fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények. In Karsai Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest: Wolters Kluwer, 972–988.

Karsai Krisztina (2019b): Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In Karsai Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest: Wolters Kluwer, 989–996.

Kertész Imre (1993): A számítógépes hamisítás. *Rendészeti Szemle,* 31(4), 13–20.

King, Alison Virginia (2010): Constitutionality of Cyberbullying Laws. Keeping the Online Playground Safe for Both Teens and Free Speech. *Vanderbilt Law Review,* 63(3), 845–884. Online: https://scholarship.law.vanderbilt.edu/vlr/vol63/iss3/6

Kirchengast, Tyrone (2020): Deepfakes and Image Manipulation. Criminalisation and Control. *Information & Communications Technology Law,* 29(3), 308–323. Online: https://doi.org/10.1080/13600834.2020.1794615

Kiss Tibor – Parti Katalin – Prazsák Gergő (2019): *Cyberdeviancia.* Budapest: Dialóg Campus.

Klein Tamás (2016a): A szólásszabadság az interneten. In Tóth András – Klein Tamás (szerk.): *Bevezetés az Infokommunikációs Jogba.* Budapest: Patrocinium, 75–106.

Klein Tamás (2016b): A tárhelyszolgáltató „omnipotens" felelőssége mint alkotmányjogi problematika. A harmadik személy tartalmáért való szolgáltatói felelősség az interneten. In Koltay András – Török Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején.* III. kötet. Budapest: Wolters Kluwer, 349–374.

Klein Tamás (2018a): Az online diskurzusok egyes szabályozási kérdései. In Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest: Médiatudományi Intézet, 11–40.

Klein Tamás (2018b): Robotjog. In Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog.* Budapest: Wolters Kluwer, 179–215.

Klein Tamás (2020): *Sajtószabadság és demokrácia.* Budapest: Gondolat – Dialóg Campus.

Klein Tamás – Tóth András (2018): A robotika egyes szabályozási kérdései. In Homicskó Árpád Olivér (szerk.): *Egyes modern technológiák etikai, jogi és szabályozási kihívásai.* Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 93–117.

Klonick, Kate (2018): The New Governors. The People, Rules and Processes Governing Online Speech. *Harvard Law Review,* 131(6), 1598–1670.

Koltay András (2012): Az emberi jogok, az emberi méltóság és az alkotmányos rend védelme a magyar médiaszabályozásban. *In Medias Res,* 1(1), 37–66.

Koltay András (2013): A gyűlöletbeszéd korlátozása a magyar jogrendszerben. In Koltay András (szerk.): *A gyűlöletbeszéd korlátozása Magyarországon. Alkotmányos és jogalkalmazói megközelítések európai kitekintéssel.* Budapest: Wolters Kluwer, 1–123.

Koltay András (2014): Az újmédia kapuőreinek hatása a médiaszabályozásra. In Gellén Klára (szerk.): *Jog, innováció, versenyképesség.* Budapest: Wolters Kluwer, 99–124.

Koltay András (2019a): A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Medias Res,* 8(1), 1–56.

Koltay András (2019b): *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása.* Budapest: Wolters Kluwer.

Kondorosi András (2014): Az információs rendszer felhasználásával elkövetett csalás. *Infokommunikáció és Jog,* 11(2), 73–75.

Koppelman, Andrew (2016): Revenge Pornography and First Amendment Exceptions. *Emory Law Journal,* 65(3), 661–693.

Kőhidi Ákos (2016): *Fájlcsere és felelősség.* Budapest: Nemzeti Média- és Hírközlési Hatóság.

Kökényesi-Bartos Attila (2010): A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése bűncselekmény megállapíthatóságával kapcsolatos problémák. [Az Ügyészek szakmai tudományos konferenciáján, a szekcióülésen elhangzott előadás szerkesztett változata. Balatonlelle, 2010. november 4–5.] *Ügyészek Lapja,* 17(2. különszám), 21–25.

Kraakman, Reinier H. (1986): Gatekeepers. The Anatomy of a Third-Party Enforcement Strategy. *Journal of Law, Economics and Organization,* 2(1), 53–104.

Kunos Imre (1999): A számítógépes bűnözés. A modern információtechnológia felhasználása a bűnözésben. *Belügyi Szemle,* 47(11), 28–42.

Kurzweil, Ray (2014): *A szingularitás küszöbén. Amikor az emberiség meghaladja a biológiát.* Budapest: Ad Astra.

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

Laidlaw, Emily B. (2012): *Internet Gatekeepers, Human Rights and Corporate Social Responsibilities.* PhD-disszertáció. The London School of Economics and Political Science.

Lane, Darcy K. (2011): Taking the Lead on Cyberbullying. Why Schools Can and Should Protect Students Online. *Iowa Law Review,* 96(5), 1791–1811.

Lapsánszky András (2019): Társszabályozás és önigazgatás a médiaigazgatásban. In Koltay András (szerk.): *Magyar és európai médiajog.* Budapest: Wolters Kluwer, 985–1001.

Levi, Michael (2008): Organized Fraud and Organizing Frauds. Unpacking Research on Networks and Organization. *Criminology & Criminal Justice,* 8(4), 389–419. Online: https://doi.org/10.1177/1748895808096470

LICHTMAN, Douglas Gary – POSNER, Eric (2004): Holding Internet Service Providers Accountable. *John M. Olin Program in Law and Economics Working Paper,* 217. Online: https://chicagounbound.uchicago.edu/law_and_economics/236/

LIPTON, Jacqueline D. (2012): Cyberbullying and the First Amendment. *Florida Coastal Law Review,* 14(1), 99–130.

LONTAI Endre et al. (2012): *Magyar polgári jog. Szerzői jog és iparjogvédelem.* Budapest: Eötvös.

MACKINNON, Catherine A. (2004): Of Mice and Men. A Feminist Fragment on Animal Rights. In SUNSTEIN, Cass R. – NUSSBAUM, Martha Craven (szerk.): *Animal Rights. Current Debates and New Directions.* Oxford: Oxford University Press, 263–276.

MAHLER, Gordon (2003): Az amerikai büntetőeljárás vázlata. In TÓTH Mihály (szerk.): *Büntető eljárásjogi olvasókönyv.* Budapest: Osiris, 71–83.

MARSDEN, Christopher T. (2011): Co- and Self-regulation in European Media and Internet Sectors. The Results of Oxford University's Study. In OSCE: *Self-regulation, Co-regulation, State Regulation,* 76–100.

MARTENS, Bertin et al. (2018): *The Digital Transformation of News Media and the Rise of Disinformation and Fake News.* Sevilla: European Commission. Online: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf

MÁTÉ István Zsolt (2013): Digitális bizonyíték. In TÖRŐ Csaba et al. (szerk.): *IX. Jogász Doktoranduszok Országos Szakmai Találkozója 2013.* Budapest: Károli Gáspár Református Egyetem, 86–94.

MCGLYNN, Clare – RACKLEY, Erika (2017): Image-Based Sexual Abuse. *Oxford Journal of Legal Studies,* 37(3), 534–561. Online: https://doi.org/10.1093/ojls/gqw033

MEZEI Kitti (2018): A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro,* 8(1), 66–83. Online: https://doi.org/10.26521/Profuturo/2018/1/4674

MEZEI Kitti (2020a): A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban. *Rendőrségi Tanulmányok,* 3(2), 23–43.

MEZEI Kitti (2020b): *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest: L'Harmattan.

MEZEI Kitti (2021): Az online gyermekpornográfia és a büntetőjog. *Ügyészek Lapja,* 28(4), 19–30.

MEZŐLAKI Erik (2019): Az igazságszolgáltatás elleni bűncselekmények. In KARSAI Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest: Wolters Kluwer, 609–651.

MILTON, John (2018): Areopagitica. Beszéd Anglia Parlamentjéhez az engedélyhez nem kötött nyomtatás jogáért. *In Medias Res,* 7(1), 1–34.

MISKOLCZI Barna (2018): A cyberbullying. In MISKOLCZI Barna – SZATHMÁRY Zoltán (szerk.): *Büntetőjogi kérdések az információk korában. Mesterséges intelligencia, Big Data, profilozás.* Budapest: HVG-ORAC, 166–174.

MISKOLCZI Barna – SZATHMÁRY Zoltán (2018): *Büntetőjogi kérdések az információk korában. Mesterséges intelligencia, Big Data, profilozás.* Budapest: HVG-ORAC.

Molnár Péter (2001): Uszítás vagy gyalázkodás? *Fundamentum,* 5(4), 110–126.

Monori Zsuzsanna Éva (2016a): A Kúria határozata a zaklatás bűncselekményéről. A háborgatással elkövetett zaklatás fogalomrendszerének értelmezése és annak lehetséges veszélyei. *Jogesetek Magyarázata,* 7(4), 29–39.

Monori Zsuzsanna Éva (2016b): Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. *In Medias Res,* 5(2), 246–261.

Mosser, Jamie (2016): Cyberbullying and the Law. *Northern Illinois University Law Review,* 36(3), 79–96.

Muchichka László (2017): A béke politikája az Amerika Kapitány: Polgárháborúban. In Tóth Csaba (szerk.): *Fantasztikus világok.* Budapest: Athenaeum.

Nagy Zoltán (2007): Negyedik hatalmi ág? *Mediárium,* 1(1), 49–56.

Nagy Zoltán András (1991): Az informatika és a büntetőjog. *Magyar Jog,* 38(1), 21–26.

Nagy Zoltán András (2009): *Bűncselekmények számítógépes környezetben.* Budapest: Ad Librum.

Nagy Zoltán András (2010): A Pirate Bay-per tanulságai. De lege ferenda a fájlcseréről. *Ügyészek Lapja,* 17(2), 33–40.

Nagy Zoltán András (2018): A számítógépes bűnözés története. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére.* Budapest: Dialóg Campus, 471–480.

Nagy Zoltán András (2019): A csalás-jellegű cselekmények az e-kereskedelem körében. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs–Budapest: Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 148–168.

Nagy Zoltán András – Mezei Kitti (2017): A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modernkori magyar rendészettudományig.* Pécs: Magyar Hadtudományi Társaság, Határőr Szakosztály, Pécsi Szakcsoport, 163–168.

Nagykommentár a Büntető Törvénykönyvről szóló 1978. évi IV. törvényhez, Btk. 300/E. §-ához – WK jogtár

Nichols, James A. – Herbert Chan, Hsien W. – Baker, Matthew A. B. (2019): Machine Learning. Applications of Artificial Intelligence to Imaging and Diagnosis. *Biophysical reviews,* 11(1), 111–118. Online: https://doi.org/10.1007/s12551-018-0449-9

Noszkay Erzsébet (1999): *Informatikai és rendszerszervezési alapismeretek.* Budapest: Múzsák.

Oleksiewicz, Izabela (2016): Dilemmas and Challenges for EU Anti-Cyberterrorism Policy. The Example of the United Kingdom. *Teka Komisji Politologii i Stosunków Międzynarodowych,* 11(3), 135–146.

Papp János Tamás (2020): A hamis hírek alkotmányos helyzete és szerepe a demokratikus nyilvánosság befolyásolásában. *In Medias Res,* 9(1), 141–164.

Parker, Donn B. – Nycum, Susan – Aura, Stephen (1973): *Computer Abuse.* Menlo Park: Stanford Research Institute.

Parti Katalin (2007): A számítástechnikai bűnözés elleni nemzetközi fellépés szükségessége. *Rendészeti Szemle,* 55(2), 123–137.

Parti Katalin (2008): *Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze.* PhD-disszertáció. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola Infokommunikációs és Jogi Doktori Program.

Parti Katalin (2016): A megfélemlítés (bullying) szabályozása Magyarországon és külföldön. *In Medias Res,* 5(1), 114–146.

Parti Katalin – Kiss Anna (2014): A számítástechnikai bűnözésről akkor és most. In Bárd Petra – Hack Péter – Holé Katalin (szerk.): *Pusztai László emlékére.* Budapest: Országos Kriminológiai Intézet – Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar, 297–310.

Pasquale, Frank (2015): *The Black Box Society. The Secret Algorithms That Control Money and Information.* Cambridge: Harvard University Press.

Péli-Toóth Viktória (2015): Kortárs online zaklatás, a cyberbullying jelenség. In Elek Balázs – Fázsi László (szerk.): *Az ítélőmesterség dilemmái. Tanulmányok Dr. Remes Zoltán bíró emlékére.* Debrecen: Printart-Press, 36–57.

Perel, Maayan – Elkin-Koren, Niva (2017): Black Box Tinkering. Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review,* 69(1), 181–221. Online: http://dx.doi.org/10.2139/ssrn.2741513

Peszleg Tibor (2000): Internet és bűnözés. *Belügyi Szemle,* 48(12), 30–35.

Peszleg Tibor (2004): Internet és pedofília. *Belügyi Szemle,* 52(11–12), 54–66.

Peszleg Tibor (2005): Interneten, számítógépen történő nyomrögzítés. *Ügyészek Lapja,* 12(1), 25–40.

Peszleg Tibor (2010): A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. *Ügyészek Lapja,* 17(2), 23–31.

Péterfalvi Attila – Eszteri Dániel (2017): A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata. In Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* Budapest: ELTE ÁJK, 405–420.

Peterson, Jason H. (2014): Global Cyber Intermediary Liability. A Legal & Cultural Strategy. *Pace Law Review,* 34(2), 586–630. Online: https://doi.org/10.58948/2331-3528.1858

Pogácsás Anett (2014): Mit veszíthet egy szerző? Gondolatok a sérelemdíj szerzői jogban betöltött szerepéről. In Csehi Zoltán et al. (szerk.): *(L)ex Cathedra et Praxis. Ünnepi kötet Lábady Tamás 70. születésnapja alkalmából.* Budapest: Pázmány Press, 617–633.

Polt Péter (1983): A számítógépes bűnözés. *Belügyi Szemle,* 21(6), 60–64.

Pusztai Ferenc szerk. (2008): *Magyar értelmező kéziszótár.* Budapest: Akadémiai.

Pusztai László (1989): Számítógép és bűnözés. *Kriminológiai és Kriminalisztikai Tanulmányok,* 26, 85–146.

Rawat, Meetali (2021): Transnational Cybercrime. Issue of Jurisdiction. *International Journal of Law Management & Humanities,* 4(2), 253–266. Online: http://doi.one/10.1732/IJLMH.26049

Rediker, Ezekiel (2015): The Incitement of Terrorism on the Internet. Legal Standards, Enforcement, and the Role of the European Union. *Michigan Journal of International Law,* 36(2), 321–351. Online: https://repository.law.umich.edu/mjil/vol36/iss2/3

Reményi Édua – Koltay András szerk. (2017): *A szólásszabadság káprázata. A szólásszabadság brit, amerikai és francia klasszikusainak szöveggyűjteménye.* Budapest: CompLex Wolters Kluwer.

Ricci, Francesco – Rokach, Lior – Shapira, Bracha (2011): Recommender Systems: Introduction and Challenges. In Ricci, Francesco – Rokach, Lior – Shapira Bracha – Kantor, Paul B. (szerk.): *Recommender Systems Handbook.* Boston: Springer, 1–35. Online: https://doi.org/10.1007/978-0-387-85820-3_1

Ryan, David (2018): European Remedial Coherence in the Regulation of Non-consensual Disclosures of Sexual Images. *Computer Law & Security Review,* 34(5), 1053–1076. Online: https://doi.org/10.1016/j.clsr.2018.05.016

Sajó András (2005): Becsületvédelem és büntetőjog – megjegyzések a becsületsértés dekriminalizálásáról. *Büntetőjogi Kodifikáció,* 5(1), 3–6.

Sarkady Ildikó (2017): Az önszabályozás szerepe a modern szabályozási struktúrákban. *Iustum Aequum Salutare,* 13(3), 115–150.

Saul, Ben (2005): Speaking of Terror. Criminalising Incitement to Violence. *University of New South Wales Law Journal,* 28(3), 868–886.

Setterfield, Rosalind C. (2019): *The Regulation of 'Revenge Porn' in England and Wales. Are Existing Legal Solutions Effective?* PhD-disszertáció. University of Surrey. Online: https://doi.org/10.15126/thesis.00851986

Shoemaker, Pamela J. – Cohen, Akiba A. (2012): *News Around the World. Content, Practitioners, and the Public.* New York: Routledge.

Siegler Eszter (1997): A számítógéppel kapcsolatos és a számítógépes bűncselekmények. *Magyar Jog,* 44(12), 736–742.

Simon Béla (2012): *Csúcstechnológiai bűnözés és nyomozása.* Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar.

Solove, Daniel J. (2008): *Understanding Privacy.* Cambridge–London: Harvard University Press.

Sorbán Kinga (2018): Vírusok és zombik a büntetőjogban – Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res,* 7(2), 369–386. Online: https://inmediasresfolyoirat.hu/imr/article/view/174/175

Sólyom László (1983): *A személyiségi jogok elmélete.* Budapest: KJK.

Sólyom László (2001): *Az alkotmánybíráskodás kezdetei Magyarországon.* Budapest: Osiris.

Stenersen, Anne (2018): The Internet. A Virtual Training Camp? *Terrorism and Political Violence,* 20(2), 215–233. Online: https://doi.org/10.1080/09546550801920790

Stone, Geoffrey R. (2017): *Sex and the Constitution. Sex, Religion, and Law from America's Origins to the Twenty-First Century.* New York – London: Liveright.

Sunstein, Cass R. (2013): *Republic.com 2.0.* Budapest: Wolters Kluwer.

Szabó Imre (2003): Internetes bűncselekmények – különös tekintettel az internetes csalásra. In Kiss Daisy (szerk.): *E-akták. Tanulmányok az internetjog világából.* Budapest: Bibó István Szakkollégium Internetjogi Kutatócsoport, 301–324.

Szabó Imre (2008): Informatikai bűncselekmények. In Dósa Imre (szerk.): *Az informatikai jog nagy kézikönyve.* Budapest: CompLex.

Szabó Imre (2014): *Az internet közvetítő szolgáltatóinak büntetőjogi felelősségéről.* PhD-disszertáció. ELTE Állam- és Jogtudományi Doktori Iskola.

Szathmáry Zoltán (2011): A számítástechnikai bűncselekmények. *Magyar Jog,* 58(3), 160–170.

Szathmáry Zoltán (2012): A számítástechnikai bűncselekmények és rendszertani elhelyezkedésük. *Jogtudományi Közlöny,* 67(4), 169–178.

Szathmáry Zoltán (2020): Etikus és nem etikus hacking – a kéretlen sérülékenységvizsgálat büntetőjogi kérdései. *Magyar Jog,* 67(6), 340–346.

Szeder Gyula (2002): A társadalom békéjének büntetőjogi védelméről. *Magyar Jog,* 49(1), 1–11.

Szentkuti Dániel – Szűts Márton (2003): Az Internet és a büntetőjogi felelősség egyes kérdései. *Jogelméleti Szemle,* 4(3). Online: https://jesz.ajk.elte.hu/szentkuti15.html

Szomora Zsolt (2013): Zaklatás. In Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvhöz.* Budapest: CompLex.

Szomora Zsolt (2019a): A nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények. In Karsai Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest: Wolters Kluwer, 443–472.

Szomora Zsolt (2019b): Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények. In Karsai Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest: Wolters Kluwer, 492–531.

Szomora Zsolt (2019c): Záró rész. In Karsai Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest: Wolters Kluwer, 1049–1083.

Till Szabolcs (2019): Különleges jogrend. In Jakab András – Fekete Balázs (szerk.): *Internetes Jogtudományi Enciklopédia.* Online: http://ijoten.hu/szocikk/kulonleges-jogrend

Torma András (1993): *Jogi informatika.* Miskolc: Bíbor.

Tóth Dávid – Gáspár Zsolt (2020): Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén. *Büntetőjogi Szemle,* 9(2), 140–150.

Tóth J. Zoltán (2017): *A büntetőjogi rágalmazás és becsületsértés. A defamatorikus bűncselekmények elméleti és gyakorlati megítélése a véleménynyilvánítási szabadság és az emberi méltósághoz való jog kontextusában.* Budapest: Médiatudományi Intézet.

Tóth Mihály (2002): *Gazdasági bűnözés és bűncselekmények.* Budapest: KJK-Kerszöv.

Tóth Mihály (2006): Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In Gál István László – Nagy Zoltán András (szerk.): *Informatika és büntetőjog.* Pécs: Pécsi Tudományegyetem, 180–188.

Török Bernát (2013): A gyűlöletbeszéd tilalmának médiajogi mércéi. *Jogtudományi Közlöny,* 68(2), 59–72.

Török Bernát (2018): *Szabadon szólni, demokráciában.* Budapest: HVG-ORAC.

Török Bernát (2019): A bántó szavakról. *In Medias Res,* 8(2), 253–273.

Tremmel Flórián (2006): *Bizonyítékok a büntetőeljárásban.* Budapest–Pécs: Dialóg Campus.

Tremmel Flórián – Fenyvesi Csaba – Herke Csongor (2009): *Kriminalisztika.* Budapest–Pécs: Dialóg Campus.

Trengove, Markus et al. (2022): A Critical Review of the Online Safety Bill. *Patterns,* 3(8). Online: https://doi.org/10.1016/j.patter.2022.100544

Tsesis, Alexander (2019): Terrorist Speech on Social Media. *Vanderbilt Law Review,* 70(2), 651–708.

Vámos Tibor (2002): Információs bűnözés – rémlátások és valós veszélyek. *Belügyi Szemle,* 50(11–12), 5–9.

Varga Balázs (2003): Informatikai bűncselekmények. *Jogi Fórum,* 2003. december 9. Online: www.jogiforum.hu/publikacio/2003/12/19/informatikai-buncselekmenyek/

Varga Zoltán szerk. (2004): *Nagykommentár a Büntető törvénykönyvről szóló 1978. évi IV. törvényhez.* Budapest: KJK-Kerszöv.

Vaskuti András (2005): A közösség elleni izgatás bírói gyakorlata. In Ligeti Katalin (szerk.): *Wiener A. Imre ünnepi kötet.* Budapest: KJK, 185–205.

Vavró István (1989): A komputer jog egyes problémáinak megoldása Magyarországon. In Borsi Zoltán – Baturin, J. M. (szerk.): *Számítástechnika és a jog. A tudományos-műszaki haladás hatása a jogi életre.* Budapest: KJK, 367–379.

Vida Mihály – Juhász Zsuzsanna (2009): Zaklatás. In Nagy Ferenc (szerk.): *A magyar büntetőjog különös része.* Budapest: HVG-ORAC, 159–161.

Villányi József (2003): Az EU kölcsönös bűnügyi jogsegélyéről szóló egyezményhez kapcsolódó jogalkotási feladatok. *Publicationes Doctorandorum Juridicorum,* 3, 209–252. Online: https://acta.bibl.u-szeged.hu/7535/1/juridpol_doct_003_209-252.pdf

Volokh, Eugene (2013): One-to-One Speech vs. One-to-Many Speech, Criminal Harassment Laws, and „Cyberstalking". *Northwestern University Law Review,* 107(2), 731–794.

Wagner, Benjamin (2017): *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications.* Council of Europe, Committee of Experts on Internet Intermediaries (MSI-NET). Online: https://rm.coe.int/study-hrdimension-of-automated-data-processing-incl-algorithms/168075b94a

Weimann, Gabriel (2015): *Terrorism in Cyberspace. The Next Generation.* Washington, D.C.: Woodrow Wilson Centre Press – Columbia University Press.

Whitty, Noel (2010): Soldier Photography of Detainee Abuse in Iraq. Digital Technology, Human Rights and the Death of Baha Mousa. *Human Rights Law Review,* 10(4), 689–714. Online: https://doi.org/10.1093/hrlr/ngq041

Wu, Tim (2019): Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems. *Columbia Law Review,* 119(7), 2001–2028.

Z. Karvalics László (2015): Mesterséges intelligencia. A diskurzusok újratervezésének kora. *Információs Társadalom,* 15(4), 7–41. Online: https://doi.org/10.22503/inftars.XV.2015.4.1

Zeidan, Sami (2004): Desperately Seeking Definition. The International Community's Quest for Identifying the Specter of Terrorism. *Cornell International Law Journal,* 36(3), 491–496.

Zibriczky Dávid (2015): Perszonalizált tartalomajánló szolgáltatás IPTV és OTT rendszerek számára. *HTE Medianet,* 70, 49–55. Online: www.hte.hu/documents/847429/1921516/HT_2015_2_10_Zibriczky.pdf

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

Ződi Zsolt (2023): *Platformjog. Elméletek és hatályos szabályok.* Budapest: Ludovika.

Sajtó- és blogcikkek

2 millió forintot csalt ki a társkereső oldalon megismert nőtől – a Bács-Kiskun Megyei Főügyészség sajtóközleménye (2021). *Magyarország Ügyészsége,* 2021. május 20. Online: https://ugyeszseg.hu/2-millio-forintot-csalt-ki-a-tarskereso-oldalon-megismert-notol-a-bacs-kiskun-megyei-fougyeszseg-sajtokozlemenye/

2003: az internet, informatika egy éve (2003). *Origo,* 2003. december 19. Online: www.origo.hu/techbazis/20031219200031.html?pIdx=4

A fideszes polgármester jelentette fel a gyulai ellenzékit rémhírterjesztés miatt (2020). *444,* 2020. május 18. Online: https://444.hu/2020/05/18/a-fideszes-polgarmester-jelentette-fel-a-gyulai-ellenzekit-remhirterjesztes-miatt

AFP in the Hague (2016): Dutch Court to Extradite Man Accused of Cyberbullying Teen who Killed Herself. *The Guardian,* 2016. június 28. Online: www.theguardian.com/world/2016/jun/28/cyberbulling-suicide-netherlands-canada-amanda-todd

Anderson, Lessley (2012): Snuff: Murder and Torture on the Internet, and the People Who Watch It. *The Verge,* 2012. június 13. Online: www.theverge.com/2012/6/13/3076557/snuff-murder-torture-internet-people-who-watch-it

Andromeda Botnet Dismantled in International Cyber Operation (2017). *Europol,* 2017. Online: www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

Az Anonymous átírta az alaptörvényt (2012). *Index,* 2012. március 4. Online: https://index.hu/tech/2012/03/04/az_anonymous_atirta_az_alaptorvenyt/

Az Elender-hekkelés ítélete és tanulságai (2003). *Prohardver,* 2003. december 15. Online: https://prohardver.hu/hir/az_elender-hekkeles_itelete_es_tanulsagai.html

Az Iszlám Államot dicsőítő propagandát terjesztett – a Pest Megyei Főügyészség sajtóközleménye (2022). *Magyarország Ügyészsége,* 2022. augusztus 9. Online: https://ugyeszseg.hu/az-iszlam-allamot-dicsoito-propagandat-terjesztett-a-pest-megyei-fougyeszseg-sajtokozlemenye/

Az oroszok visszabombázzák Észtországot az online kőkorszakba (2007). *Index,* 2007. május 31. Online: https://index.hu/tech/net/eszt290507/

Az ügyészség szerint nem terjesztett rémhírt a gyulai férfi sem (2020). *Index,* 2020. május 15. Online: https://index.hu/belfold/2020/05/15/az_ugyeszseg_szerint_nem_terjesztett_remhirt_a_gyulai_ferfi_sem/

Balasubramani, Venkat (2016): North Carolina State Supreme Court Strikes Down Cyberbullying Statute. *Technology & Marketing Law Blog,* 2016. június 13. Online: https://blog.ericgoldman.org/archives/2016/06/north-carolina-state-supreme-court-strikes-down-cyberbullying-statute.htm

Bartley, Nancy (2000): A Trial of Tangled Webs. *The Seattle Times,* 2000. május 8. Online: http://community.seattletimes.nwsource.com/archive/?date=20000508&slug=4019710

Beech, Hannah (2018): As Malaysia Moves to Ban 'Fake News,' Worries About Who Decides the Truth. *The New York Times,* 2018. április 2. Online: www.nytimes.com/2018/04/02/world/asia/malaysia-fake-news-law.html

Bencze Mátyás – Ficsor Krisztina (2020): A koronavírus kihívásai és a jogtudomány: a rémhírterjesztés tényállásának jogalkalmazási kérdései. *TKJTI,* 2020. április 2. Online: https://jog.tk.mta.hu/blog/2020/04/a-remhirterjesztes-tenyallasanak-jogalkalmazasi-kerdesei

Bever, Lindsey (2018): Teens Are Daring Each Other to Eat Tide Pods. We Don't Need to Tell You that's a Bad Idea. *The Washington Post,* 2018. január 13. Online: www.washingtonpost.com/news/to-your-health/wp/2018/01/13/teens-are-daring-each-other-to-eat-tide-pods-we-dont-need-to-tell-you-thats-a-bad-idea/

Bhageshpur, Kiran (2019): Data Is The New Oil – And That's A Good Thing. *Forbes,* 2019. november 15. Online: www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=3486ddfb7304

Blais, Tony (2016): Edmonton Gore-site Owner Pleads Guilty to Corrupting Morals in Magnotta Video Case. *Edmonton Journal,* 2016. január 25. Online: https://edmontonjournal.com/news/crime/edmonton-gore-site-owner-pleads-guilty-in-magnotta-video-case

Bócz Endre – Györgyi Kálmán (2003): Hol az alkotmányosság határa? *Népszabadság,* 2003. október 30.

Bodoky Tamás (2007): Elfuserálták a nagy warezrazziát. *Index,* 2007. december 27. Online: https://index.hu/tech/jog/warez9956/

Botnet Taken Down Through International Law Enforcement Cooperation (2015). *Europol,* 2015. február 25. Online: www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation

Burch, Audra D. S. – Eligon, John (2020): Bystander Videos of George Floyd and Others Are Policing the Police. *The New York Times,* 2020. május 26. Online: www.nytimes.com/2020/05/26/us/george-floyd-minneapolis-police.html

Chichizola, Corey (2020): Rogue One Deepfake Makes Star Wars' Leia And Grand Moff Tarkin Look Even More Lifelike. *Cinemablend,* 2020. december 9. Online: www.cinemablend.com/news/2559935/rogue-one-deepfake-makes-star-wars-leia-and-grand-moff-tarkin-look-even-more-lifelike

Clark, Liat (2013): The Weird World of Facebook's Moral Code. Beheadings Good, Breastfeedings Bad. *Wired,* 2013. október 22. Online: www.wired.co.uk/article/facebook-beheading

Confessore, Nicholas (2018): Cambridge Analytica and Facebook. The Scandal and the Fallout So Far. *The New York Times,* 2018. április 4. Online: www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Conger, Kate (2016): Facebook Employees Say Deleting 'Napalm Girl' Photo Was a Mistake. *TechCrunch,* 2016. szeptember 12. Online: https://techcrunch.com/2016/09/12/facebook-employees-say-deleting-napalm-girl-photo-was-a-mistake/

Cook, James (2014): Q&A: The Man Behind LiveLeak, The Islamic State's Favourite Site For Beheading Videos. *Business Insider.* Online: www.businessinsider.com/profile-of-hayden-hewitt-founder-of-liveleak-2014-10?r=UK

Dahl, Kieran (2018): Exploitation on the Internet? The Morality of Watching Death Online. *The Guardian,* 2018. október 12. Online: www.theguardian.com/technology/2018/oct/12/reddit-r-watch-people-die

Dickson, Ej (2019): What Is the Momo Challenge? *Rolling Stone,* 2019. február 26. Online: www.rollingstone.com/culture/culture-news/what-is-momo-challenge-800470/

Edelman, Gilad (2019): How Facebook Gets the First Amendment Backward. *Wired,* 2019. november 7. Online: www.wired.com/story/facebook-first-amendment-backwards/

Egyre több az internetes csalás (2004). *Origo,* 2004. szeptember 14. Online: www.origo.hu/techbazis/20040914egyre.html

Ellis, Emma Grey (2019): New York's Revenge Porn Law Is a Flawed Step Forward. *Wired,* 2019. július 24. Online: www.wired.com/story/new-york-revenge-porn-law/

European Commission (2019): *STATEMENT/19/6166 Code of Practice on Disinformation One Year On: Online Platforms Submit Self-Assessment Reports.* Online: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_6166

Evron, Gadi (2009): Dutch ISPs Sign Anti-Botnet Treaty. *Darkreading,* 2009. szeptember 29. Online: www.darkreading.com/risk/dutch-isps-sign-anti-botnet-treaty

Felmentették az Elender-hackereket (2004). *Index,* 2004. május 5. Online: https://index.hu/tech/jog/lendrhck0505/

Fiorentino, Michael-Ross (2018): France Passes Controversial 'Fake News' Law. *Euronews,* 2018. november 22. Online: www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

Frank, Robert (2000): Philippine Prosecutors Drop Charges in 'Love Bug' Case. *The Wall Street Journal,* 2000. augusztus 22. Online: www.wsj.com/articles/SB966862157148570125

Fullerton, Jamie (2019): Singapore to Introduce Anti-Fake News Law, Allowing Removal of Articles. *The Guardian,* 2019. április 1. Online: www.theguardian.com/world/2019/apr/01/singapore-to-introduce-anti-fake-news-law-allowing-removal-of-articles

Giuffrida, Angela (2018): Italians Asked to Report Fake News to Police in Run-up to Election. *The Guardian,* 2018. január 19. Online: www.theguardian.com/world/2018/jan/19/italians-asked-report-fake-news-police-run-up-election

Grant, Harriet (2020): World's Biggest Porn Site Under Fire Over Rape and Abuse Videos. *The Guardian,* 2020. március 9. Online: www.theguardian.com/global-development/2020/mar/09/worlds-biggest-porn-site-under-fire-over-videos-pornhub

Hamilton, Isobel Asher (2019): Facebook Used Pictures of Weed and Broccoli to Showcase the Breakneck Speed of its AI in Spotting Harmful Content. *Business Insider,* 2019. március 14. Online: www.businessinsider.com/facebook-used-pictures-of-cannabis-and-broccoli-to-show-off-ai-system-2019-3

Hanula Zsolt (2016): Majdnem megtanultam három nyelvet egy hónap alatt. *Index,* 2016. augusztus 29. Online: https://index.hu/tech/2016/08/29/majdnem_megtanultam_harom_nyelvet_egy_honap_alatt/

Hanula Zsolt (2017): Az internetet a reklám tette naggyá, és az is rontja el. *Index,* 2017. április 28. Online: https://index.hu/tech/2017/04/28/az_internetet_a_reklam_tette_naggya_es_az_is_rontja_el/

Helmore, Edward (2017): Facebook Blocks Photo of Neptune Statue for Being 'Explicitly Sexual'. *The Guardian,* 2017. január 2. Online: www.theguardian.com/world/2017/jan/02/facebook-blocks-nude-neptune-statue-bologna-italy

Hempel, Jessi (2017): Killing the Blue Whale Challenge. *Wired,* 2017. július 26. Online: www.wired.com/story/killing-the-blue-whale-challenge/

Herrman, John (2019): The Internet's Endless Appetite for Death Video. *The New York Times,* 2019. március 24. Online: www.nytimes.com/2019/03/24/style/really-bad-stuff.html

Hollister, Sean (2018): Scarlett Johansson Slams Deepfakes, Says She Can't Stop the Internet from Pasting Her Face on Porn. *The Verge,* 2018. december 31. Online: www.theverge.com/2018/12/31/18163351/scarlett-johansson-slams-deepfakes-internet-lost-cause

Horton, Alex (2018): A Man Was Sentenced to 9 Months in Prison. His Crime? Posting Fake Reviews on TripAdvisor. *The Washington Post*, 2018. szeptember 12. Online: www.washingtonpost.com/world/2018/09/12/man-tried-sell-fake-tripadvisor-reviews-hes-going-prison-after-landmark-ruling-italy/

How Filter Bubbles Distort Reality. Everything You Need to Know (2017). *Fs.blog*, 2017. Online: https://fs.blog/filter-bubbles/

Huszonnyolc vádlott az évszázad magyar warezperében (2012). *Index*, 2012. szeptember 20. Online: https://index.hu/tech/2012/09/20/mar_targyaljak_a_legnagyobb_warez_ugyet/

Ingyenes program a tárcsázós csalás ellen (2004). *Origo*, 2004. augusztus 2. Online: www.origo.hu/techbazis/20040802ingyenes.html

International Action Against 'Gameover Zeus' Botnet and 'CryptoLocker' Ransomware (2014). *Europol*, 2014. június 2. Online: www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

Itt az első magyar kórházi zsarolóvírus (2016). *Index*, 2016. április 8. Online: https://index.hu/tech/2016/04/08/itt_az_elso_magyar_korhazi_zsarolovirus/

IWiW-es csalás terjed a neten (2010). *Origo*, 2010. október 28. Online: www.origo.hu/techbazis/20101028-iwiwes-csalas-terjed-a-neten.html

Jeffries, Adrianne (2013): Should You Go to Jail for Posting Video of a Real Murder? *The Verge*, 2013. október 16. Online: www.theverge.com/2013/10/16/4841522/bestgore-corrupting-public-morals-mark-marek-luka-magnotta

Juhász Edina (2020): 18 millió koronavírus témájú adathalász levelet szűr ki naponta a Google. *Index*, 2020. április 17. Online: https://index.hu/techtud/2020/04/17/18_millio_csalo_level_naponta/

Kang, Cecilia – Isaac, Mike (2019): Defiant Zuckerberg Says Facebook Won't Police Political Speech. *The New York Times*, 2019. október 17. Online: www.nytimes.com/2019/10/17/business/zuckerberg-facebook-free-speech.html

Katz, Rita (2017): How Terrorists Slip Beheading Videos Past YouTube's Censors. *Vice*, 2017. május 26. Online: www.vice.com/en_us/article/xyepmw/how-terrorists-slip-beheading-videos-past-youtubes-censors

Katz, Rita (2018): To Curb Terrorist Propaganda Online, Look to YouTube. No, Really. *Wired*, 2018. október 20. Online: www.wired.com/story/to-curb-terrorist-propaganda-online-look-to-youtube-no-really/

Keller, Michael H. – Dance, Gabriel J. X. (2019): The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? *The New York Times*, 2019. szeptember 29. Online: www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

Kelly, Makena (2020): Joe Biden Wants to Revoke Section 230. *The Verge*, 2020. január 17. Online: www.theverge.com/2020/1/17/21070403/joe-biden-president-election-section-230-communications-decency-act-revoke

Kis János – Sólyom László (2003): Az alkotmány és a szólásszabadság. *Népszabadság,* 2003. október 11.

Kolhatkar, Sheelah (2022): The Fight to Hold Pornhub Accountable. *New Yorker,* 2022. június 13. Online: www.newyorker.com/magazine/2022/06/20/the-fight-to-hold-pornhub-accountable

Koltay András (2020): Koronavírus és szólásszabadság vészhelyzet idején. *Index,* 2020. március 24. Online: https://index.hu/velemeny/2020/03/24/szolasszabadsag_btk_remhirterjesztes_szigoritas/

Kovács Bálint (2018): Viagogo-botrány: 53 nyomozást rendelt el a magyar rendőrség. *Index,* 2018. szeptember 20. Online: https://index.hu/kultur/2018/09/20/viagogo-botrany_53_nyomozast_rendelt_el_a_magyar_rendorseg/

Krebs, Brian (2008): Internet Providers Cut Off Host of Spam E-mail. *Los Angeles Times,* 2008. november 13. Online: www.latimes.com/archives/la-xpm-2008-nov-13-fi-spam13-story.html

Kristof, Nicholas (2020): The Children of Pornhub. *The New York Times,* 2020. december 4. Online: www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html

Kushner, David (2005): Casualty of Porn. *Rolling Stone,* 2005. december 5. Online: https://web.archive.org/web/20100410051402/www.rollingstone.com/news/story/8878187/casualty_of_porn

Lándori Tamás (2017): Már nyolc éve tart, de még mindig nincs vége a nagy magyar warezpernek. *Magyar Nemzet,* 2017. április 19. Online: https://magyarnemzet.hu/ex-lex/2017/04/mar-nyolc-eve-tart-de-meg-mindig-nincs-vege-a-nagy-magyar-warezpernek

Leetaru, Kalev (2019): The Problem With AI-Powered Content Moderation Is Incentives Not Technology. *Forbes,* 2019. március 19. Online: www.forbes.com/sites/kalevleetaru/2019/03/19/the-problem-with-ai-powered-content-moderation-is-incentives-not-technology/#f03fd755b7bf

Lerman, Rachel (2019): Facebook Is Using AI to Crack Down on 'Revenge Porn'. *Business Insider,* 2019. március 15. Online: www.businessinsider.com/facebook-artificial-intelligence-revenge-porn-2019-3

Leskin, Paige (2020): YouTube Warns More Videos than Usual Could Be Removed as Content Moderation is Automated Amid Coronavirus Outbreak. *Business Insider,* 2020. március 16. Online: www.businessinsider.com/youtube-coronavirus-content-moderation-video-review-machine-learning-community-guidelines-2020-3

Liszewski, Andrew (2019): China's New Video Game Rules Officially Ban Blood, Corpses, Mahjong, and Poker. *Gizmodo,* 2019. április 22. Online: https://gizmodo.com/chinas-new-video-game-rules-officially-ban-blood-corps-1834221957

MacDonald, Eve (2017): The Fake News that Sealed the Fate of Antony and Cleopatra. *The Conversation,* 2017. január 13. Online: https://theconversation.com/the-fake-news-that-sealed-the-fate-of-antony-and-cleopatra-71287

Mahdawi, Arwa (2020): Pornhub Should Forget the Coronavirus and Focus on Its Own Pandemic: Revenge Porn. *The Guardian,* 2020. március 14. Online: www.theguardian.com/commentisfree/2020/mar/14/pornhub-forget-coronavirus-focus-on-pandemic-revenge-porn

MARTINEAU, Louise Matsakis Paris (2020): Coronavirus Disrupts Social Media's First Line of Defense. *Wired,* 2020. március 18. Online: www.wired.com/story/coronavirus-social-media-automated-content-moderation/

MEZEI Péter (2012): Elfogadták az új Btk.-t. *Szerzői jog a XXI. században,* 2012. június 26. Online: http://copyrightinthexxicentury.blogspot.com/2012/06/elfogadtak-az-uj-btk-t.html?m=1

MURPHY, Margi (2018): Government Bans Phrase 'Fake News'. *The Telegraph,* 2018. október 22. Online: www.telegraph.co.uk/technology/2018/10/22/government-bans-phrase-fake-news/

NELSON, Leonard (2017): The Deep Web, the Dark Web, and Simple Things. *Medium,* 2017. április 1. Online: https://medium.com/@smartrac/the-deep-web-the-dark-web-and-simple-things-2e601ec980ac

Nem csak a dohányzást, az internetes zaklatást is vasszigorral büntetné Lázár János (2018). *HVG,* 2018. október 19. Online: https://hvg.hu/itthon/20181019_Nem_csak_a_dohanyzast_az_internetes_zaklatast_is_vasszigorral_buntetne_Lazar_Janos

NEWMAN, Lily Hay (2017): What to Do if You're Being Doxed. *Wired,* 2017. szeptember 12. Online: www.wired.com/story/what-do-to-if-you-are-being-doxed/

NEWTON, Casey (2020): Facebook Will Pay $52 Million in Settlement with Moderators who Developed PTSD on the Job. *The Verge,* 2020. május 12. Online: www.theverge.com/2020/5/12/21255870/facebook-content-moderator-settlement-scola-ptsd-mental-health

NICAS, Jack (2018): How Fake Mark Zuckerbergs Scam Facebook Users Out of Their Cash. *The New York Times,* 2018. április 25. Online: www.nytimes.com/2018/04/25/technology/fake-mark-zuckerberg-facebook.html

ORFK: Ketten tettek feljelentést a WannaCry miatt (2017). *HVG,* 2017. június 16. Online: https://hvg.hu/tudomany/20170616_wannacry_zsarolovirus_orfk_magyar_feljelentesek

PAP Lázár (2020): Pornó: zugbizniszből a fősodorba és a mindennapokba. *Mandiner,* 2020. február 3. Online: https://mandiner.hu/cikk/20200213_porno

PARKER, Ian (2012): The Story of a Suicide. *New Yorker,* 2012. január 30. Online: www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide

PATTHY Loránd Imre (2021): Vádat emeltek Gődény György ellen rémhírterjesztésért. *Index,* 2021. június 21. Online: https://index.hu/belfold/2021/06/21/ugyeszseg-godeny-gyorgy-vademeles-remhirterjesztes

PILKINGTON, Ed (2008): Death of 13-year-old Prompts Cyberbullying Test Case. *The Guardian,* 2008. június 17. Online: www.theguardian.com/world/2008/jun/17/usa.news

PONGÓ Tamás (2015): Cyberbullying, az ellenség, amely köztünk él. *Jogászvilág,* 2015. április 20. Online: https://jogaszvilag.hu/cyberbullying-az-ellenseg-amely-koztunk-el/

PORTER, Jon (2019): Facebook Says the Christchurch Attack Live Stream Was Viewed by Fewer than 200 People. *The Verge,* 2019. március 19. Online: www.theverge.com/2019/3/19/18272342/facebook-christchurch-terrorist-attack-views-report-takedown

Putin Signs 'Fake News', 'Internet Insults' Bills Into Law (2019). *The Moscow Times,* 2019. március 18. Online: www.themoscowtimes.com/2019/03/18/putin-signs-fake-news-internet-insults-bills-into-law-a64850

Rankin, Jennifer – Henley, Jon (2016): Islamic State Claims Attacks at Brussels Airport and Metro Station. *The Guardian,* 2016. március 22. Online: www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard

Reardon, Marguerite (2020): Coronavirus Transforms Peak Internet Usage Into the New Normal. *CNET,* 2020. március 23. Online: www.cnet.com/news/coronavirus-has-made-peak-internet-usage-into-the-new-normal/

Richtel, Matt (2020): W.H.O. Fights a Pandemic Besides Coronavirus: An 'Infodemic'. *The New York Times,* 2020. február 6. Online: www.nytimes.com/2020/02/06/health/coronavirus-misinformation-social-media.html

Robertson, Adi (2020): Visa and Mastercard Cut off Pornhub After Report of Unlawful Videos. *The Verge,* 2020. december 10. Online: www.theverge.com/2020/12/10/22168240/mastercard-ending-pornhub-payment-processing-unlawful-videos

Robertson, Adi (2022): Visa Could Be Liable for Helping Monetize Pornhub Videos of Children, Says Court. *The Verge,* 2022. augusztus 1. Online: www.theverge.com/2022/8/1/23287036/visa-mindgeek-pornhub-child-sexual-abuse-videos-court-liability

Roose, Kevin (2019): YouTube's Product Chief on Online Radicalization and Algorithmic Rabbit Holes. *The New York Times,* 2019. március 29. Online: www.nytimes.com/2019/03/29/technology/youtube-online-extremism.html

Sandler, Rachel (2018): Facebook Has Apologized for Flagging Parts of the Declaration of Independence as Hate Speech. *Business Insider,* 2018. július 5. Online: www.businessinsider.com/facebook-declaration-of-independence-hate-speech-2018-7?r=US&IR=T

Schweber, Nate – Foderaro, Lisa W. (2016): Roommate in Tyler Clementi Case Pleads Guilty to Attempted Invasion of Privacy. *The New York Times,* 2016. október 27. Online: www.nytimes.com/2016/10/28/nyregion/dharun-ravi-tyler-clementi-case-guilty-plea.html

Singer, Natasha – Krolik, Aaron (2020): Grindr and OkCupid Spread Personal Details, Study Says. *The New York Times,* 2020. január 13. Online: www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html

Sírás lett a vége – Falus Ferenc vödrös akciója (2014). *Mandiner,* 2014. augusztus 25. Online: https://mandiner.hu/cikk/20140825_siras_lett_a_vege_falus_ferenc_vodros_akcioja

Solon, Olivia (2017): Underpaid and Overburdened. The Life of a Facebook Moderator. *The Guardian,* 2017. május 25. Online: www.theguardian.com/news/2017/may/25/facebook-moderator-underpaid-overburdened-extreme-content

Speri, Alice – Biddle, Sam (2016): Facebook Removes Potential Evidence of Police Brutality Too Readily, Activists Say. *The Intercept*, 2016. augusztus 8. Online: https://theintercept.com/2016/08/08/facebook-removes-potential-evidence-of-police-brutality-too-readily-activists-say/

Statt, Nick (2017): YouTube is Facing a Full-Scale Advertising Boycott Over Hate Speech. *The Verge*, 2017. március 24. Online: www.theverge.com/2017/3/24/15053990/google-youtube-advertising-boycott-hate-speech

Stupp, Catherine (2018): Commission Threatens to Legislate on 'Fake News' Ahead of 2019 EU Election. *Euractiv*, 2018. április 26. Online: www.euractiv.com/section/digital/news/commission-threatens-legislation-on-fake-news-ahead-of-2019-eu-election/

Számítógép-vezetékkel fojthatták meg a jászberényi pedofilt (2010). *Origo*, 2010. február 12. Online: www.origo.hu/itthon/20100212-szamitogepvezetekkel-fojthattak-meg-a-jaszberenyi-pedofilt.html

Társkereső oldalakon megismert nőket csapott be egy férfi – a Komárom-Esztergom Vármegyei Főügyészség sajtóközleménye (2023). *Magyarország Ügyészsége*, 2023. március 29. Online: https://ugyeszseg.hu/tarskereso-oldalakon-megismert-noket-csapott-be-egy-ferfi-a-komarom-esztergom-varmegyei-fougyeszseg-sajtokozlemenye/

Temperton, James (2016): Facebook Makes U-Turn on Decision to Censor an Iconic Vietnam War Photo. *Wired*, 2016. szeptember 9. Online: www.wired.co.uk/article/facebook-terror-of-war-vietnam-napalm-girl-image-censored

Thompson, Nicholas (2017): Instagram's Kevin Systrom Wants to Clean Up the &#%$@! Internet. *Wired*, 2017. augusztus 14. Online: www.wired.com/2017/08/instagram-kevin-systrom-wants-to-clean-up-the-internet/

Tinderen csábította el magyar áldozatát a bitcoincsaló (2021). *Index*, 2021. január 13. Online: https://index.hu/belfold/2021/01/13/tinder_crypto_banyaszat_bitcoincsalas_kamu_profil_randi/

Tolna Vármegyei Rendőr-főkapitányság (2015): Trükkös csalók „unokázós" módszere. *Police.hu*, 2015. szeptember 8. Online: www.police.hu/hirek-es-informaciok/bunmegelozes/aktualis/trukkos-csalok-unokazos-modszere

Turton, William – Justus, Matthew (2018): "Deepfake" Videos Like that Gal Gadot Porn Are Only Getting More Convincing – and More Dangerous. *Vice*, 2018. augusztus 27. Online: www.vice.com/en_us/article/qvm97q/deepfake-videos-like-that-gal-gadot-porn-are-only-getting-more-convincing-and-more-dangerous

Urfi Péter (2020): Szexképeket küldözgető kamaszok: mihez kezdjen velük a törvény? *444*, 2020. augusztus 22. Online: https://444.hu/2020/08/22/szexkepeket-kuldozgeto-kamaszok-mihez-kezdjen-veluk-a-torveny

Vádemelés a rémhírterjesztővel szemben (2020). *Magyarország Ügyészsége*, 2020. május 6. Online: https://ugyeszseg.hu/vademeles-a-remhirterjesztovel-szemben/

Vincent, James (2018): Watch Jordan Peele Use AI to Make Barack Obama Deliver a PSA About Fake News. *The Verge*, 2018. április 18. Online: www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

Vincent, James (2019): AI Won't Relieve the Misery of Facebook's Human Moderators. *The Verge*, 2019. február 27. Online: www.theverge.com/2019/2/27/18242724/facebook-moderation-ai-artificial-intelligence-platforms

Volokh, Eugene (2015): Lawsuit Tries to Apply Foreign Speech Restrictions in U.S. Court, Hold Facebook Liable for Not Censoring Allegedly Terrorism-Inciting Pages. *The Washington Post*, 2015. november 13. Online: www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/12/lawsuit-tries-to-apply-foreign-speech-restrictions-in-u-s-court-hold-facebook-liable-for-not-censoring-allegedly-terrorism-inciting-pages/

Weisbeck, Daniel (2014): Context is King – Long Live the King. *Wired*, 2014. január. Online: www.wired.com/insights/2014/01/context-king-long-live-king/

White, Patrick (2014): On the Trail of Amanda Todd's Alleged Tormentor. *The Globe and Mail*, 2014. május 31. Online: www.theglobeandmail.com/news/world/on-the-trail-of-amanda-todds-alleged-tormentor/article18935075/?page=all

Wong, Julia Carrie (2019): Facebook Finally Responds to New Zealand on Christchurch Attack. *The Guardian*, 2019. március 29. Online: www.theguardian.com/us-news/2019/mar/29/facebook-new-zealand-christchurch-attack-response

World of Warcraft Helps Nab Alleged Drug Dealer (2010). *Australian Broadcasting Corporation*, 2010. január 5. Online: www.abc.net.au/news/2010-01-06/world-of-warcraft-helps-nab-alleged-drug-dealer/1199372

Worth, Robert F. (2011): How a Single Match Can Ignite a Revolution. *The New York Times*, 2011. január 23. Online: www.nytimes.com/2011/01/23/weekinreview/23worth.html

Ződi Zsolt (2020): Az etikai kódexek hiábavalóságáról a mesterséges intelligencia szabályozásában. *ITKI blog*, 2020. július 3. Online: www.ludovika.hu/blogok/itkiblog/2020/07/03/az-etikai-kodexek-hiabavalosagarol-a-mesterseges-intelligencia-szabalyozasaban

Tájékoztató és forrásweboldalak, szakértői anyagok

A 189. szerződés aláírásának és ratifikálásának jegyzéke. Online: www.coe.int/en/web/conventions/full-list?-module=signatures-by-treaty&treatynum=189

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. A közös európai adattér kialakítása felé. COM(2018) 232 végleges. Online: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52018DC0232

Alonso, Rogelio et al. (2008): *Radicalisation Processes Leading to Acts of Terrorism. A Concise Report Prepared by the European Commission's Expert Group on Violent Radicalisation.* Online: www.clingendael.org/sites/default/files/pdfs/20080500_cscp_report_vries.pdf

Association of Chief Police Officers (2011): *Good Practice Guide for Computer-based Electronic Evidence.* Online: https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf

Az adatvédelmi biztos beszámolója (2009). Online: www.naih.hu/files/Adatvedelmi-biztos-beszamoloja-2009.PDF

Az Európai Unió bel- és igazságügyi minisztereinek, valamint az uniós intézmények képviselőinek közös nyilatkozata a 2016. március 22-i brüsszeli terrorista merényletek kapcsán (2016). Online: www.consilium.europa.eu/hu/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/

Berger, J. M. (2015): The Evolution of Terrorist Propaganda. The Paris Attack and Social Media. *Brookings,* 2015. január 25. Online: www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/

Broadcasting Authority of Ireland (2019): *Submission to the Department of Communications, Climate Action & Environment Public Consultation on the Regulation of Harmful Content on Online Platforms and the Implementation of the Revised Audiovisual Media Service Directive.* Online: www.bai.ie/en/download/134036

Budapesti Rendőr-főkapitányság (2023): *Szervezeti felépítés.* Online: www.police.hu/sites/default/files/szervezeti_felepites_pdf/BRFK_szervezeti%20%C3%A1bra_2023_08.pdf

Bundeskriminalamt [é. n.]: *Was ist Cybercrime?* Online: www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html

Cambridge Dictionary (é. n.): News. In *Cambridge Advanced Learner's Dictionary & Thesaurus.* Online: https://dictionary.cambridge.org/dictionary/english/news

Committee of Experts on Internet Intermediaries (MSI-NET) (2018): *Algorithms and Human Rights. Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) and Possible Regulatory Implications.* Online: https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

Consultation Outcome. Online Harms White Paper (2020). Online: www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

Cyberbullying (2023). Online: https://gyerekaneten.hu/szocikk/Cyberbullying?referer=kereses

Davis, Antigone (2019): *Detecting Non-Consensual Intimate Images and Supporting Victims.* Online: https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/

DIGI (2023): *Kiskorúak védelme.* Online: https://digi.hu/hasznos/kiskoruak-vedelme

Duarte, Natasha – Llansó, Emma – Loup, Anna (2017): *Mixed Messages? The Limits of Automated Social Media Content Analysis.* Online: https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf

Ebay (2023): *Sértő tartalmakra vonatkozó irányelv.* Online: www.ebay.com/help/policies/prohibited-restricted-items/offensive-materials-policy?id=4324

ERGA (2022): *The Implementation(s) of Article 28b AVMSD. National Transposition Approaches and Measures by Video-Sharing Platforms.* Online: https://erga-online.eu/wp-content/uploads/2022/12/2022-12-ERGA-SG1-Report-Article-28b.pdf

European Commission (2018). *Security Union: Facilitating Access to Electronic Evidence.* Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343

European Commission (2019): *Fighting Terrorism Online. EU Internet Forum Committed to an EU-wide Crisis Protocol.* Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009

European Commission, Directorate-General for Communications Networks, Content and Technology (2018): *A Multi-Dimensional Approach to Disinformation. Report of the Independent High level Group on Fake News and Online Disinformation.* Online: https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en

Europol (2022): *Exploiting Isolation. Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic.* Online: www.europol.europa.eu/publications-events/publications/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

Europol (2023): *Cybercrime.* Online: www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Facebook Help Center (2023): *What Should I Do if I'm Being Bullied, Harassed or Attacked by Someone on Facebook?* Online: www.facebook.com/help/116326365118751

Facebook Newsroom (2015): *Partnering to Help Curb Spread of Online Terrorist Content.* Online: https://about.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/

Fehér könyv a mesterséges intelligenciáról. A kiválóság és a bizalom európai megközelítése. COM(2020) 65 végleges. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52020DC0065

Forbrukerrådet (2020): *Out of Control. How Consumers Are Exploited by the Online Advertising Industry.* Online: https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf

Földes Ádám (2007): *A Társaság a Szabadságjogokért (TASZ) jogvédő szervezet véleménye az elektronikus hírközlésről szóló 2003. évi C. törvény módosításáról szóló tervezetről.* Online: http://tasz.hu/files/tasz/imce/TASZ_Eht_velemeny.pdf

Gawer, Annabelle (2014): *Online Platforms: Contrasting Perceptions of European Stakeholders. A Qualitative Analysis of the European Commission's Public Consultation on the Regulatory Environment for Platforms.* Online: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15932

Government of Canada (2023): *Together We Can Stop Cyberbullying.* Online: www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbrbllng/prnts/lgl-cnsqncs-en.aspx#a01

Hogben, Giles szerk. (2011): *Botnets. Detection, Measurement, Disinfection & Defence.* Online: www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport

Home Affairs Committee (2013): *E-crime.* Online: https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/7004.htm

Home Office (2010): *Cybercrime Strategy.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

House of Commons Digital, Culture, Media and Sport Committee (2019): *Disinformation and 'Fake News'. Final Report.* Online: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm

Instagram (2023): *Közösségi Irányelvek.* Online: https://help.instagram.com/477434105621119/?helpref=hc_fnav&bc[0]=Instagram%20S%C3%BAg%C3%B3&bc[1]=Adatv%C3%A9delmi%20%C3%A9s%20biztons%C3%A1gi%20k%C3%B6zpont

Instagram Help Center (2023): *Copyright.* Online: www.facebook.com/help/instagram/126382350847838?ref=related

Jarrett, H. Marshall et al. (2009): *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Online: www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Locklear, Mallory (2019): Facebook Adds New Tools to Address Harassment and Bullying. *Engadget,* 2019. augusztus 8. Online: www.engadget.com/2018-10-02-facebook-tools-address- harassment-bullying.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAM8xNlDMWJzZ7hcL2cFx1lj1cu4OCBNyxfv HVFrXuKiNJEIKibU2Bm5c72VqUnwETJxCMrDumuCHR8moPOj2JOocVZ44MPPz-

Magyar Helsinki Bizottság (2020): *Rémhírterjesztés újratöltve.* Online: www.helsinki.hu/remhirterjesztes-ujratoltve/

Magyar Telekom (2023a): *Gyermekeink védelme a digitális korban.* Online: www.telekom.hu/rolunk/fenntarthatosag/edukacio/gyermekvedelem

Magyar Telekom (2023b): *Kibervédelem.* Online: www.telekom.hu/rolunk/telekom_vilaga/biztonsagi_tartalmak/kibervedelem

McGuire, Mike – Dowling, Samantha (2013a): Cyber-Dependent Crimes. In McGuire, Mike – Dowling, Samantha: *Cyber Crime. A Review of the Evidence Research Report 75.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

McGuire, Mike – Dowling, Samantha: Cyber-Enabled Crimes. In McGuire, Mike – Dowling, Samantha (2013b): *Cyber crime. A Review of the Evidence Research Report 75.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Meta Transparency Center (2023a): *A Facebook közösségi alapelvei. Felnőttek szexuális kizsákmányolása.* Online: https://transparency.fb.com/hu-hu/policies/community-standards/adult-sexual-exploitation/

Meta Transparency Center (2023b): *Erőszakot megjelenítő és durva tartalom.* Online: www.facebook.com/communitystandards/graphic_violence

Meta Transparency Center (2023c): *Felnőtt meztelenség és szexuális tevékenység.* Online: https://transparency.fb.com/hu-hu/policies/community-standards/adult-nudity-sexual-activity/

Meta Transparency Center (2023d): *Veszélyes szervezetek és magánszemélyek.* Online: www.facebook.com/communitystandards/dangerous_individuals_organizations

Nemzeti Kibervédelmi Intézet (2020a): *Magyar nyelvű Covid-19 témájú levéllel próbálnak pénzügyi adatokat szerezni a csalók.* Online: https://nki.gov.hu/it-biztonsag/hirek/figyelem-magyar-nyelvu-covid-19-temaju-levellel-probalnak-penzugyi-adatokat-szerezni-a-csalok/

Nemzeti Kibervédelmi Intézet (2020b): *Nem szűnik a Covid-19 fertőzéstől való félelmet kihasználó csaló üzenetek sora.* Online: https://nki.gov.hu/it-biztonsag/hirek/nem-szunik-a-covid-19-fertozestol-valo-felelmet-kihasznalo-csalo-uzenetek-sora/

Nemzeti Kibervédelmi Intézet (2023): *IT Biztonsági Tudástár.* Online: https://nki.gov.hu/it-biztonsag/tudastar/

Nemzeti Média- és Hírközlési Hatóság (2011): *A médiatartalmak korhatár-besorolásánál irányadó szempontokra, az egyes műsorszámok közzététele előtt és közben alkalmazható jelzésekre, illetve a minősítés közlésének módjára vonatkozó jogalkalmazási gyakorlat elvi szempontjai.* Online: http://nmhh.hu/dokumentum/1456/klasszifikacios_ajanlas_20110719.pdf

OECD (2005): *Spam Issues in Developing Countries.* Online: www.oecd.org/internet/ieconomy/34935342.pdf

OECD (2010): *The Economic and Social Role of Internet Intermediaries.* Online: www.oecd.org/internet/ieconomy/44949023.pdf

OECD (2011a): *The Protection of Children Online. Risks Faced by Children Online and Policies to Protect Them.* Online: http://dx.doi.org/10.1787/5kgcjf71pl28-en

OECD (2011b): *The Role of Internet Intermediaries in Advancing Public Policy Objectives.* Online: www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm

OECD (2012): *The Protection of Children Online. Risks Faced by Children Online and Policies to Protect Them.* Online: www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf

OECD (2015): *Industry Self-Regulation. Role And Use In Supporting Consumer Interests.* Online: www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En

OECD (2019): *What Is an "Online Platform"? An Introduction to Online Platforms and Their Role in the Digital Transformation.* Online: https://doi.org/10.1787/19e6a0f0-en

Ofcom (2015): *Report on Internet Safety Measures. Strategies of Parental Protection for Children Online.* Online: www.ofcom.org.uk/__data/assets/pdf_file/0019/27190/Internet-safety-measures-first-report.pdf

Rágalmazás és becsületsértés a közösségi médiában – Beszélgetés Borombós Anitával, a Gyulai Törvényszék bírájával (2018). *Jogi Fórum,* 2018. szeptember 17. Online: www.jogiforum.hu/hirek/39637

Scientific Working Groups on Digital Evidence and Imaging Technology (2015): *Digital & Multimedia Evidence Glossary.* Online: www.leva.org/wp-content/uploads/2019/10/SWGDE-Glossary.pdf

Shachtman, Noah (2011): Pirates Of The Isps. Tactics For Turning Online Crooks Into International Pariahs. *Brookings,* 2011. július 25. Online: www.brookings.edu/articles/pirates-of-the-isps-tactics-for-turning-online-crooks-into-international-pariahs/

Snapchat Privacy and Safety Hub (2023): *Community Guidelines.* Online: www.snap.com/en-US/community-guidelines

Spectrumlabs (2023): *Profanity Filter.* Online: www.spectrumlabsai.com/profanity-filters

Statista (2022): *Hours of Video Uploaded to YouTube Every Minute as of February 2022.* Online: www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/

Statista (2023): *Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2023.* Online: www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Szolnoki Törvényszék (2019): Pénzbüntetésre ítélték első fokon a fiatal hackert. *Magyarország Bíróságai,* 2019. július 10. Online: https://birosag.hu/aktualis-kozlemenyek/szolnoki-torvenyszek-penzbuntetesre-iteltek-elso-fokon-fiatal-hackert

Társaság a Szabadságjogokért (2017): *Nyertünk, megszüntette a nyomozást az ügyészség a BKK-botrány etikus hackere ellen.* Online: https://tasz.hu/cikkek/nyertunk-megszuntette-a-nyomozast-az-ugyeszseg-a-bkk-botrany-etikus-hackere-ellen

Telekom (2023): *Lakossági általános szerződési feltételek, 2/C melléklet.* Online: www.telekom.hu/rolunk/szolgaltatasok/aszf/lakossagi

The Communications Security, Reliability and Interoperability Council (2012): *Final Report U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs).* Online: www.m3aawg.org/system/files/20120322_WG7_Final_Report_for_CSRIC_III_5_0.pdf

The Crown Prosecution Service (2019): *Cybercrime – Prosecution Guidance.* Online: www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

The Impact of Algorithms for Online Content Filtering or Moderation (2020). Online: www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf

The Strengthened Code of Practice on Disinformation (2022). Online: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

Tumblr Help Center (2023): *Appealing Content Flagged as Explicit.* Online: https://tumblr.zendesk.com/hc/en-us/articles/231885248

United Nations (2010): *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World.* Online: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

UNODC (2012): *The Use of the Internet for Terrorist Purposes.* Online: www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

UNODC (2013): *Comprehensive Study on Cybercrime. Draft.* Online: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC [é. n.]: *Global Programme on Cybercrime.* Online: www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

Vatera (2023): *Általános szerződési feltételek.* Online: https://img-ssl.vatera.hu/license/vatera_main_content_hu.html?v1272965733131

Vihul, Liis et al. (2012): *Legal Implications of Countering Botnets. Joint Report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA).* Online: https://ccdcoe.org/uploads/2012/03/VihulCzosseckZiolikowskiAasmannIvanovBruggemann2012_LegalImplicationsOfCounteringBotnets.pdf

Wardle, Claire – Derakhshan, Hossein (2017): *Information Disorder. Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe Report, DGI(2017)09.* Online: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

Winchcomb, Tim (2019): *Ofcom: Use of AI in Online Content Moderation.* Online: www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf

X Help Center (2023a): *Abuse and Harassment.* Online: https://help.twitter.com/en/rules-and-policies/abusive-behavior

X Help Center (2023b): *Abusive Profile Information.* Online: https://help.twitter.com/en/rules-and-policies/abusive-profile

X Help Center (2023c): *Sensitive Media Policy.* Online: https://help.twitter.com/en/rules-and-policies/media-policy

X Help Center (2023d): *Violent Speech Policy.* Online: https://help.twitter.com/en/rules-and-policies/violent-speech

YouTube Súgó (2023a): *A Content ID működése.* Online: https://support.google.com/youtube/answer/2797370?hl=hu

YouTube Súgó (2023b): *Erőszakos szélsőséges vagy bűnszervezetekre vonatkozó irányelvek.* Online: https://support.google.com/youtube/answer/9229472?hl=hu&ref_topic=9282436

YouTube Súgó (2023c): *Erőszakos vagy megrázó tartalmakra vonatkozó irányelvek.* Online: https://support.google.com/youtube/answer/2802008?hl=hu

YouTube Súgó (2023d): *Gyűlöletkeltésre vonatkozó irányelv.* Online: https://support.google.com/youtube/answer/2801939?hl=hu

YouTube Súgó (2023e): *További információ a Content ID-követelésekről.* Online: https://support.google.com/youtube/answer/6013276

YouTube Súgó (2023f): *Zaklatásra és internetes zaklatásra vonatkozó irányelvek.* Online: https://support.google.com/youtube/answer/2802268?hl=hu&visit_id=637241964270348024-3785549682&rd=1

YouTube (2023a): *Szabályok és Irányelvek. Közösségi Irányelvek.* Online: www.youtube.com/about/policies/#community-guidelines

YouTube (2023b): *Szabályok és irányelvek. Szerzői jog.* Online www.youtube.com/howyoutubeworks/policies/copyright/

Az Országos Rendőr-főkapitányság és a Magyar Telekom Távközlési Nyilvánosan Működő Részvénytársaság között kötött együttműködési megállapodás (2016). Online: www.police.hu/sites/default/files/ot_2_0.doc

Jogszabályok, jogszabálytervezetek és egyéb jogi dokumentumok

1978. évi IV. törvény a Büntető Törvénykönyvről

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

1994. évi XXXIV. törvény a rendőrségről

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról

1998. évi XIX. törvény a büntetőeljárásról (régi)

1999. évi LXXVI. törvény a szerzői jogról

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

2003. évi C. törvény az elektronikus hírközlésről

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

2005. évi CXVI. törvény az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről szóló, 2000. május 29-én kelt egyezmény és az egyezmény 2001. október 16-án kelt kiegészítő jegyzőkönyve kihirdetéséről

2006. évi XL. törvény a Magyar Köztársaság Kormánya és az Amerikai Egyesült Államok Kormánya között a kiadatásról és a kölcsönös bűnügyi jogsegélyről szóló, Budapesten, 1994. december 1-jén aláírt szerződések módosításáról szóló szerződések kihirdetéséről

2009. évi CLXI. törvény a gyermekek eladásáról, a gyermekprostitúcióról és a gyermekpornográfiáról szóló, a Gyermek jogairól szóló egyezményhez fűzött Fakultatív Jegyzőkönyv megerősítéséről és kihirdetéséről

2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól

2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról

2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról

2011. évi II. törvény az Európa Tanács terrorizmus megelőzéséről szóló, Varsóban, 2005. május 16-án kelt Egyezménye kihirdetéséről

2011. évi CLXIII. törvény az ügyészségről

2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről

2013. évi V. törvény a Polgári Törvénykönyvről

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

2015. évi XCII. törvény az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és szexuális zaklatás elleni védelméről szóló Egyezménye kihirdetéséről, valamint ezzel összefüggésben egyes törvények módosításáról

2017. évi XC. törvény a büntetőeljárásról

2018. évi XXI. törvény az Európa Tanács terrorizmus megelőzéséről szóló Egyezménye Kiegészítő Jegyzőkönyvének kihirdetéséről

2020. évi XII. törvény a koronavírus elleni védekezésről

1976. évi 8. törvényerejű rendelet az Egyesült Nemzetek Közgyűlése XXI. ülésszakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről

180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről

A Bizottság (EU) 2018/334 ajánlása (2018. március 1.) az illegális online tartalom hatékony kezelésére irányuló intézkedésekről

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Online platformok és a digitális egységes piac. Lehetőség és kihívás Európa számára

A Bizottság közleménye: Iránymutatások az audiovizuális médiaszolgáltatásokról szóló irányelv értelmében a „videomegosztóplatform-szolgáltatás" fogalommeghatározásában szereplő alapvető funkció kritériumának gyakorlati alkalmazására vonatkozóan

A Gyermek jogairól szóló, New Yorkban, 1989. november 20-án kelt Egyezmény

A Miniszteri Bizottság R (89) 9 számú ajánlása a számítógéppel kapcsolatos bűnözésről

A Miniszteri Bizottság R (95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról

A számítástechnikai bűnözésről szóló egyezményhez csatolt, a megerősített együttműködésről és az elektronikus bizonyítékok átadásáról szóló második kiegészítő jegyzőkönyv

A számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv

Anti-Counterfeiting Trade Agreement

Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről (1994)

Az ENSZ Közgyűlésének 45/121. számú határozata

Az ENSZ Közgyűlésének 55/63. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

Az ENSZ Közgyűlésének 56/121. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

Az ENSZ Közgyűlésének 60/177. számú és 64/211. számú határozatai

Az ENSZ Közgyűlésének 65/230. számú határozata a bűnmegelőzésről és büntető igazságszolgáltatásról szóló tizenkettedik ENSZ Kongresszusról

Az Európa Tanács terrorizmus megelőzéséről szóló, Varsóban, 2005. május 16-án kelt Egyezménye

Az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és szexuális zaklatás elleni védelméről szóló Egyezménye (a Lanzarote Egyezmény)

Az Európai Bizottság ajánlása a jogellenes online tartalmak hatékony kezeléséről

Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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

Az Európai Parlament és a Tanács (EU) 2017/541 irányelve a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról

Az Európai Parlament és a Tanács (EU) 2018/1808 irányelve a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (Audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról

Az Európai Parlament és a Tanács (EU) 2019/713 irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról

Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról

Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály)

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról

Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

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

Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv)

Az Európai Parlament és a Tanács 2011/92/EU irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

Az Európai Parlament és a Tanács 2021/1232 rendelete a 2002/58/EK irányelv bizonyos rendelkezéseitől a technológiáknak a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó szolgáltatók által a gyermekek online szexuális bántalmazása elleni küzdelem céljából a személyes és egyéb adatok kezelésére történő használata tekintetében való ideiglenes eltérésről

Az Európai Parlament és a Tanács 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről

Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata 2012/C 326/01

Az irodalmi és a művészeti művek védelméről szóló 1886. szeptember 9-i Berni Egyezmény

Child Pornography Prevention Act (CPPA), 1996

Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

Code of Practice on Disinformation

Code pénal

Communications Act, 2003

Communications Decency Act, 1996
Comprehensive Crime Control Act, 1984
Computer Abuse Act, 1990
Computer Fraud and Abuse Act (CFA), 1986
Copyright Designs and Patents Act, 1988
Criminal Justice and Courts Act, 2015
Criminal Justice Court Act, 2015
Data Protection Act, 2018
Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act (DEEPFAKES Accountability Act), 2019
Digital Millenium Copyright Act
Egyezmény a Tanács által az Európai Unióról szóló szerződés 34. cikkének megfelelően létrehozott, az Európai Unió tagállamai közötti kölcsönös bűnügyi jogsegélyről
Emberi Jogok Európai Egyezménye
Ending Nonconsensual Online User Graphic Harassment Act (ENOUGH)
Espionage Act, 1917
Fair and Accurate Credit Transactions Act (FACTA), 2003
Federal Rules of Criminal Procedure
Federal Rules of Evidence
Florida Computer Crimes Act, 1978
Forgery and Counterfeiting Act, 1981
Fraud Act, 2006
H.R.5566 – Animal Crush Video Prohibition Act, 2010
Identity Theft and Assumption Deterrence Act (ITADA), 1998
Identity Theft Enforcement and Restitution Act, 2008
Identity Theft Penalty Enhancement Act, 2004
Indecency with Children Act, 1960
Interinstitutional agreement on better law-making (2003/C 321/01). The European Parliament, the Council of the European Union and the Commission of the European Communities
Investigatory Powers Act, 2016
Javaslat: Az Európai Parlament és a Tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról
Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (2007/C 306/01)
LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique
LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet

Malicious Communications Act, 1988
National Information Infrastructure Protection Act, 1996
Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352)
Obscene Publications Act, 1959
Online Safety Act, 2023
Prosecuting Intellectual Property Crimes, 2006
Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT), 2003
Protection of Children Act, 1978
Protection of Children Against Sexual Exploitation Act, 1977
Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries
Recommendation No. R (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems. Strasbourg, 1990
Sexual Offences Act, 2003
Stop Online Piracy Act
Strafgesetzbuch
T/10307. számú törvényjavaslat a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról
Terrorism Act, 2000
The EU Code of Conduct on Countering Illegal Hate Speech Online.
The Malicious Deep Fake Prohibition Act (MDFPA)
The Protection from Harassment Act, 1997
Trade Marks Act, 1994
United States Code

Jogesetek, hatósági döntések

13/2014. (IV. 18.) AB határozat
14/2000. (V. 12.) AB határozat
15/2020. (VII. 8.) AB határozat
15/2022. (VII. 14.) AB határozat
18/2000. (VI. 6.) AB határozat
2/2007. (I. 24.) AB határozat
30/1992. (V. 26.) AB határozat
36/1994. (VI. 24.) AB határozat
46/2013. (II. 21.) AB határozat

9/2012. számú büntető elvi döntés
21.B.480/2019/20
3.Bf.1080/2013/12
B.687/2012/11
Abrams v. United States, 250 U.S. 616
Ahmet Yıldırım v. Turkey, App. no. 3111/10
American Council on Education v. FCC, 451 F.3d 226, 233 (D.C. Cir. 2006)
Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002)
Bethel School District v. Frazer, 478 US 675 (1986)
Bf.III.1.548/2014
Bfv.II.74/2008/5
BH 2010.2.33: Legf. Bír. Bfv. II. 74/2008. I
BH 2017.8.252: Kúria Bfv. III. 1.291/2016
BH1990.540
BH2000.285
BH2004.71
BH2009.135
BH2011.302
BH2012.143
BH2012.87
BH2014.169
BH2019.68
BJD 7330
Brandenburg v. Ohio, 395 U.S. 444 (1969)
C-293/12 és C-594/12, a Digital Rights Ireland Ltd. kontra Írország és Kärntner Landesregierung kontra Michael Seitlinger és társai egyesített ügyekben hozott 2014. április 8-i ítélet
C-320/16, az Uber France ügyben hozott 2018. április 10-i ítélet
C-347/14, a New Media Online GmbH kontra Bundeskommunikationssenat és Der Bundeskanzler. A Verwaltungsgerichtshof ügyben hozott 2015. február 21-i ítélet
C-390/18, az Airbnb Ireland ügyben hozott 2019. december 19-i ítélet
C-434/15, az Asociación Profesional Elite Taxi ügyben hozott 2017. december 20-i ítélet
C-62/19, a Star Taxi App SRL ügyben hozott 2020. december 3-i ítélet
Capitol Records, Inc v. Thomas (2008) U.S. District Court for the District of Minnesota (2008 WL 4405282)
Catt v. the United Kingdom, App. no. 43514/15
Cengiz and Others v. Turkey, App. nos. 48226/10 and 14027/11
Ceylan v. Turkey, App. no. 23556/94

Chaplinsky v. New Hampshire, 315 U.S. 568 (1942)
Commission Decision of 03/10/2014 declaring a concentration to be compatible with the common market (Case No COMP/M.7217 – Facebook / Whatsapp) according to Council Regulation (EC) No. 139/2004
Cour de cassation, criminelle, Chambre criminelle, 16 mars 2016, 15-82.676
Debreceni Ítélőtábla, Bf.597/2017/76
Debreceni Ítélőtábla, Bhar.I.625/2020/32
Debreceni Járásbíróság, 44.B.221/2020/65
Décision n° 2020-801 DC du 18 juin 2020
DELFI AS v. Estonia, no. 64569/09. 2015. június 16-i ítélet
Dennis v. United States, 341 U.S. 494, 509, 515, 516 (1951)
DPP v. Jones [1997] 2 Cr App R 155 HL
DPP v. Mcmahon 1984 ILRM 461
EBH2017.B.17
EBH2019.B.2
EBH2009.2033
EBH2014.B.16
Elonis v. United States, 575 U.S. 723 (2015)
Fővárosi Ítélőtábla, 5.Bf.300/2016/40
Fővárosi Ítélőtábla, Bf.12/2021/11
Fővárosi Ítélőtábla, Bf.136/2020/47
Fővárosi Ítélőtábla, Bf.204/2015/13
Fővárosi Ítélőtábla, Bf.392/2016/113
Fővárosi Ítélőtábla, Bf.492/2013/19
Fővárosi Ítélőtábla, Bhar.136/2018/6
Fővárosi Ítélőtábla, Bhar.186/2018/8
Fővárosi Ítélőtábla, Bhar.51/2015/9
Fővárosi Ítélőtábla, Bhar.60/2014/4
Fővárosi Törvényszék, Bf.10387/2013/7
Fővárosi Törvényszék, Bf.6036/2015/15
Fővárosi Törvényszék, Bf.7671/2015/5
Fővárosi Törvényszék, Bf.12455/2015/6
Fővárosi Törvényszék, 14.B.454/2016/62A
Fővárosi Törvényszék, 28.B.436/2011/56
Fővárosi Törvényszék, 42(II.)Kb.1327/2015
Gertz v. Robert Welch Inc., 418 U.S. 323 (1974)

H.Rept. 99-612 11 (1986)
ÍH 2010.97
Jacobellis vs. Ohio, 378 U.S. 184, 197 (1964)
Kablis v. Russia, App. nos. 48310/16 és 59663/17
Karatas v. Turkey, App. no. 23168/94
Kúria, Bfv.219/2020/10
Kúria, Bfv.433/2019/8
Kúria, Bfv.744/2021/20
Kúria, Bfv.III.539/2021/31.
Lakin v. Facebook Inc., No. 12831/15 (N.Y. Sup. Ct. Oct. 26, 2015)
Leroy v. France, App. no. 36109/03
Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007)
Magyar Tartalomszolgáltatók Egyesülete and Index.Hu Zrt v. Hungary, no. 22947/13. 2016. február 2-i ítélet
Miller v. California, 413 U.S. 15, 23 (1973)
New York Times Co. v. Sullivan, 376 U.S. 254 (1964)
Pécsi Ítélőtábla, Bf.31/2016/15
Pécsi Ítélőtábla, Bhar.75/2014/3
People v. Marquan M., 2014 WL 2931482
Perinçek v. Switzerland, App. no. 27510/08
Reed v. Gilbert, 135. S. Ct. 2218, 2227 (2015)
S.Rept. 99-432 7-8 (1986)
Schenck v. United States, 249 U.S. 47 (1919)
Snyder v. Phelps, 131 S. Ct. 1207, 1214 (2011)
State v. Bishop, 2016 WL 3221098
Sürek v. Turkey (No. 1.), 1999-IV. 353, 355
Szegedi Ítélőtábla, Bf. I.505/2014/5
Székesfehérvári Törvényszék, 31.B.18/2019/72
Szekszárdi Járásbíróság, Bpk.362/2021/3
Szekszárdi Járásbíróság, Bpk.392/2021/3
Szekszárdi Járásbíróság, Bpk.520/2021/2
Szombathelyi Törvényszék, B.448/2009/7
Texas v. Johnson, 491 U.S. 397 (1989)
United States v. Czubinski (1997) U.S. Court of Appeals for the First Circuit (106.F.3d 711)
United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)
United States v. Eichman, 496 U.S. 310 (1990)

United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018)
United States v. O'Keefe, 537 F. Supp. 2d 14 (D.D.C. 2008)
United States v. Richards, 755 F.3d 269 5th Circuit (2014)
United States v. Stevens, 559 U.S. 460, 470, 471 (2010)
Virginia v. Black, 538 U.S. 343 (2003)
Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme, 433 F.3d 1199 (9th Cir. 2006)

Vákát oldal

A digitális világ a lehetőségei mellett számos rejtett veszélyt is tartogat, amelyekkel minden internetfelhasználó szembesülhet. A kötet feltárja a virtuális tér modern devianciáit, és a joggyakorlatból kölcsönzött példák segítségül hívásával áttekintő rendszerezést nyújt az interneten előforduló jogsértő, valamint a jogellenesség mezsgyéjén egyensúlyozó ártalmas magatartásokról. Bemutatja mindazokat az ártalmakat, amelyek a digitális világban bármikor érhetik az egyént, az átlagpolgárt, aki gyanútlanul használja az internet infrastruktúráját munkavégzésre, szórakozásra, vagy akár csak a mindennapi életvitelhez szükséges szolgáltatások beszerzése érdekében.

A könyv célja, hogy segítséget nyújtson az internet árnyoldalainak megértésében: a terminológiai alapok lefektetése után ismerteti az informatikai bűnözés európai és amerikai történetét, tárgyalja a vonatkozó uniós, nemzeti és hazai jogforrásokat, s külön fejezetet szentel az informatikai bűncselekményekkel kapcsolatos anyagi jogi szabályoknak. A szerző kitekintést ad a büntetőjog határterületeire is, bemutatva azokat a cselekményeket, amelyek jelenleg a büntetőjog határterületén helyezkednek el. Végül, de nem utolsósorban szól az online platformok felelősségéről és kötelezettségeiről.

Bár elsősorban a joggal, jogalkotással foglalkozó célközönség számára íródott a kötet, más tudományterületek informatikai bűnözés iránt érdeklődő művelői is haszonnal forgathatják; kézikönyv mindazoknak, akik szeretnék megérteni az internet rejtett veszélyeit és felkészülni azokra, esetleg választ keresnek az informatikai bűnözés új kihívásaira.