

Zanathy Anna

A képmáshoz való jog az online platformokon

A képmáshoz való jog az online platformokon

Avagy megvédte volna-e az európai platformszabályozás
Hillary Clintont a #Pizzagate-ügy kapcsán

Sorozatszerkesztő:

Koltay András – Nyakas Levente: 2012–2019

Nyakas Levente – Szadai Károly: 2020–2026

ZANATHY ANNA

A képmáshoz való jog az online platformokon

Avagy megvédte volna-e az európai platformszabályozás
Hillary Clintont a #Pizzagate-ügy kapcsán

Médiatudományi Intézet

2026

A kutatást támogatta:



Minden jog fenntartva.

© Zánthy Anna, 2026

© Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézete, 2026

Tartalom

Rövidítésjegyzék	9
1. Bevezetés	13
1.1. A #PizzaGate összeesküvés-elmélet	14
1.2. Módszertan	19
1.2.1. Az adatgyűjtés módszerei	19
1.2.2. Elemzés és értelmezés	20
2. Az internet kialakulása	21
3. Az internet szabályozására vonatkozó elméletek	29
3.1. Nemzetközi kontra állami szabályozás	29
3.2. Az internetszabályozás versengő irányzatai	32
3.2.1. Kiberlibertarizmus, avagy a jogmentes tér mítosza	32
3.2.2. Kiberpaternalizmus	34
3.2.3. Az integrált szabályozás, avagy 'a ló joga'	36
3.2.4. Az önszabályozás, az állami szabályozás és a társszabályozás	38
3.3. Kód-jog, avagy <i>Code is law</i>	39
4. A tartalommoderáció és a platformszabályozás közelmúltbeli fejlődése	45
5. A képmáshoz való jog	49
5.1. A személyiségi jogokról általában	49
5.2. A képmáshoz való jog	52
5.3. A képmáshoz való jog megsértése	53
5.4. A képmáshoz való jog korlátai	55
5.4.1. A jogosulti hozzájárulás	55
5.4.2. Tömegfelvétel	58
5.4.3. Közszereplő	59
6. A képmáshoz való jog érvényesülése az online térben	63
6.1. Az egyén hozzájárulásának érvényesülése a közösségimédia-oldalakon	63
6.1.1. A tagelés jogi megítélése a képmáshoz való jog szempontjából	64

6.1.2. A képmáshoz való jog megsértésének tipikus online esetei	65
6.1.3. Néhány fontosabb online platform szabályai és megoldási javaslatai	66
6.2. A képmáshoz való jog érvényesülése a manipulált képek világában	68
6.2.1. A deepfake fogalma és eredete	68
6.2.2. A deepfake mint a képmáshoz való jog tárgya	70
6.2.3. A deepfake mint a képmáshoz való jog megsértésének esete	72
6.3. Attól, hogy hamis, egyúttal jogellenes is?	76
6.3.1. A deepfake megítélése az Alkotmánybíróság joggyakorlata alapján	76
6.3.2. A deepfake megítélése az EJEB joggyakorlata alapján	79
7. A tárhelyszolgáltatói felelősség szabályozása	89
7.1. A tárhelyszolgáltatók az Eker. irányelv tükrében	90
7.2. A tárhelyszolgáltatók felelősségének megítélése az EUB joggyakorlata szemszögéből	92
7.3. Az Eker. irányelv elavulása és a növekvő igény egy új jogszabály iránt	94
8. A platformok jogi felelőssége a DSA alapján	99
8.1. A DSA céljai	99
8.2. A platformok meghatározása a DSA alapján	101
8.3. A közvetítő szolgáltatók felelősség alóli mentesülése	105
8.3.1. A DSA által teremtett felelősségi rendszer semlegessége az üzleti dimenziókra, vállalatokra és termékekre nézve	105
8.3.2. A felelősség alóli mentesség csak akkor alkalmazható, ha az érintett tartalmat a szolgáltatást igénybe vevője biztosítja	107
8.3.3. A közvetítő szolgáltatónak semlegesnek kell lennie a felhasználó által generált tartalmat érintően	109
8.4. A platformok felelősség alóli mentessége	110
8.5. A platformok felelőssége az EJEB ítélkezési gyakorlata szerint	113
8.5.1. A hozzászólások tartalma és kontextusa	114
8.5.2. A kérelmező által a jogellenes tartalom eltávolítása vagy megakadályozása érdekében alkalmazott intézkedések	115
8.5.3. A hozzászólások szerzőinek felelősségre vonásának lehetősége a közvetítő szolgáltatók felelősségének alternatívájaként	116
9. A DSA által a platformokkal szemben előírt kellő gondossági kötelezettségek	117
9.1. A platformok tartalommoderálásával összefüggésben előírt kellő gondossági kötelezettségek	120
9.1.1. A tartalommoderálás meghatározása és a DSA szerinti irányadó eljárás	120
9.1.2. A platformok tartalommoderálására vonatkozó kellő gondossági kötelezettségek és a jogellenes tartalomért való felelősségük közötti összefüggés	126
9.2. A platformok ajánlórendszereivel összefüggésben előírt kellő gondossági kötelezettségek	127
9.2.1. Az ajánlórendszerek működése	128
9.2.2. Az ajánlórendszerek definíciója a DSA alapján	129
9.2.3. Az ajánlórendszerek átláthatósága	130
9.2.4. Kilépés az ajánlórendszerekből	134

10. Hatékony védelmet nyújtana-e a DSA Hillary Clinton számára a hamisított képmásának hozzájárulása nélküli terjesztésével szemben?	137
10.1. A platformok szerepe Hillary Clinton hamisított képmásának nyilvánosság felé való terjesztésében	137
10.1.1. A közösségimédia-platformok (rejtett) pénzügyi érdekeltsége az álhírek és a deepfake-ek terjesztésében	138
10.1.2. A közösségimédia-platformok tartalomoptimalizálása eredményez-e egyfajta szerkesztőségi ellenőrzést?	141
10.1.3. Az óriásplatformok azonban – definíciójuk szerint – passzív szerepet töltenek be tartalom nyilvánosság felé való terjesztésében	143
10.2. Felelősségre vonható-e a DSA alapján azok a platformok, amelyek Hillary Clinton hamisított képmását hozzájárulása nélkül a nyilvánosság felé terjesztették?	144
10.3. A DSA szerinti kellő gondossági kötelezettségek elegendő védelmet nyújthatnak-e a #PizzaGate összeesküvés-elmélet ellen?	148
10.3.1. A visszhangkamrák negatív következményei	149
10.3.2. A DSA által nyújtott védelem a visszhangkamrákkal szemben	151
11. Összefoglalás és javaslatétel egy hatékonyabb platformszabályozásra	155
11.1. A főbb kutatási eredmények összefoglalása	156
11.1.1. A képmáshoz való jog tömeges megsértése az interneten	156
11.1.2. A jelenlegi platformszabályozás alkalmatlan hatékony jogorvoslat biztosítására a képmáshoz való jogában megsértett egyén számára	157
11.2. Javaslatétel egy hatékonyabb platformszabályozásra	161
Források és irodalom	167
Irodalomjegyzék	167
Hivatkozott jogszabályok, jogi dokumentumok	183
Hivatkozott jogesetek	184

Rövidítésjegyzék

AB	Alkotmánybíróság
CDA	Kommunikációs tisztességről szóló törvény
Charta	Európai Unió Alapjogi Charta
DSA	Digitális szolgáltatásokról szóló rendelet (2022/2065)
EB	Európai Bizottság
EFF	Electronic Frontier Foundation
EJEB	Emberi Jogok Európai Bírósága
EJEE	Emberi Jogok Európai Egyezménye
Eker. irányelv	Elektronikus kereskedelemről szóló irányelv (2000/31/EK)
EU	Európai Unió
EUB	Európai Unió Bírósága
EUMSZ	Az Európai Unió működéséről szóló szerződés
GDPR	Általános adatvédelmi rendelet (2016/679)
ISP	Internetszolgáltató
ISSP	Információs társadalommal összefüggő szolgáltató
korábbi Ptk.	1959. évi IV. törvény a Magyar Köztársaság Polgári Törvénykönyvéről
P2B	Az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló rendelet (2019/1150)
P2B Iránymutatás	Iránymutatás a rangsorolási átláthatóságról (2020/C 424/01, C/2020/8579)
Ptk.	2013. évi V. törvény a Polgári törvénykönyvről

*Férjemnek, Jonathan Kletzkine-nek,
szüleimnek, Zánathy Jánosnak és Zánathyné Martin Györgyinek,
valamint mentoromnak és barátomnak, Gosztonyi Gergelynek.*

Nélkülük ez a könyv sohasem születhetett volna meg.

1. Bevezetés

Az elmúlt évtizedben a hírfogyasztás jelentősen átalakult. A Reuters Intézet évente kiadott tanulmányai rendre arra világítanak rá, hogy a megkérdezettek többsége már nem a hagyományos médiát tekinti elsődleges hírforrásnak, hanem jóval inkább a közösségimédia-platformokat.¹ A 2024-es jelentés szerint a válaszadók mindössze körülbelül egyötöde (22%) jelölte meg a klasszikus híroldalakat vagy alkalmazásokat fő hírforrásként, míg a többség már közösségi médiát, keresőmotorokat vagy híraggregátorokat használ az online hírekhez való hozzáféréshez.²

Mivel azonban a közösségimédia-platformoknak nincs szerkesztői felelősségük, felmerül a kérdés, hogy miként biztosítható az ezen felületeken megosztott tartalmak megbízhatósága. A Reuters Intézet által megkérdezettek 60%-a például komoly aggodalmát fejezte ki amiatt, hogy az interneten megjelenő hírek valóságtartalma nem mindig ellenőrizhető. A válaszadók szerint különösen nagy bizonytalanság tapasztalható a TikTok és az X platformokon megosztott tartalmak esetében, ahol a megbízható és megbízhatatlan hírek közötti megkülönböztetés nehézségei legszembetűnőbbek.³

Az elmúlt évek tapasztalatai továbbá arra is rávilágítottak, hogy a tartalomhitelesség kérdése nem csupán a szöveges hírek, hanem a képek esetében is felmerülnek: az elmúlt években például a deepfake-ek száma fél évente megduplázódott. Előrejelzések szerint 2025-ben már 8 millió deepfake kerül majd megosztásra, míg 2023-ban ez a szám mindössze félmillió volt.⁴ Bár a mesterséges intelligencia által létrehozott felvételek sok esetben kizárólag a szórakoztatás célját szolgálják, azok könnyen a társadalmi visszaélések eszközeivé válhatnak – gondoljunk csak a választásokat befolyásoló deepfake felvételekre⁵ vagy Angela Raynerről, illetve Taylor Swiftről megosztott digitálisan manipulált szexuális képekre.⁶

¹ Paul CHADWICK: How fares trust in journalism amid a sea of fake news? *The Guardian*, 2017. július 9., <https://www.theguardian.com/commentisfree/2017/jul/09/how-fares-trust-in-journalism-amid-a-sea-of-fake-news>

² NEWMAN et al. (2024): 10.

³ Uo., 11–12.

⁴ NEGREIRO (2025): 2.

⁵ Sarah KREPS: Artificial Intelligence and elections: premature threats? *Diálogo Político*, 2025. február 4., <https://dialogopolitico.org/special-edition-2025-artificial-democracy/artificial-intelligence-elections-premature-threats>

⁶ Lucia OSBORNE-CROWLEY: Let's go after deepfake pornography sites – and the social media giants that peddle them. *The Guardian*, 2024. július 10., <https://www.theguardian.com/commentisfree/article/2024/jul/10/lets-go-after-deepfake-pornography-sites-and-the-social-media-giants-that-peddle-them>

Bár az Európai Unió több kísérletet is tett az utóbbi években a deepfake-ek platformokon keresztül való terjedésének megakadályozására, a valóságban ezen probléma továbbra is számos jogi és gyakorlati kihívást vet fel. Egyrészt a deepfake-felvételek sok esetben sértik a rajtuk 'szereplő' egyének képmáshoz való jogát – és így jogellenes tartalomnak minősülnek –, másrészt az Emberi Jogok Európai Bíróságának joggyakorlata értelmében az Emberi Jogok Európai Egyezményének 10. cikke által garantált véleménynyilvánítás szabadsága a hamis véleményekre is vonatkozik, ezért a szabályozás nem vezethet a szólásszabadság korlátozásához (*chilling effect*),⁷ és nem gátolhatja az információk szabad áramlását. Harmadrészt pedig a szabályozásnak képesnek kell lennie arra, hogy a jogellenes deepfake-ek terjedését megakadályozza, miközben egyidejűleg figyelembe veszi a platformoknak a tartalomterjesztésében betöltött egyedi szerepét.

Jelen monográfia célja annak átfogó értékelése, hogy vajon az online platformokat szabályozó jelenlegi (európai) szabályozási keret⁸ a gyakorlatban hatékony védelmet nyújt-e a képmáshoz való jogában megsértett egyéneknek. E fő kutatási kérdés megválaszolása érdekében az alábbi alkérdéseket kívánom monográfiámban részletesen elemezni:

A jog jelenleg milyen megközelítés alapján szabályozza az internetet, illetve ezen belül az online platformokat?

A #PizzaGate összeesküvés-elmélet keretében Hillary Clintonról terjesztett hamisított képmás sértette-e a volt külügyminiszter képmáshoz való jogát?

A DSA hatékony védelmet biztosít-e a képmáshoz való jogában megsértett Hillary Clinton számára akár a hamisított képmás tárolásában és nyilvánosság felé való terjesztésében közreműködő platformok felelősségre vonása, vagy ezen platformokkal szemben előírt kellő gondossági kötelezettségek kikényszerítése útján?

1.1. A #PizzaGate összeesküvés-elmélet

Bár még ma sem teljesen világos, hogy pontosan hogyan is kezdődött a #PizzaGate összeesküvés-elmélet, a legtöbben 2016. október 28. napjára teszik annak megjelenését. Ezen a napon James B. Comey, az amerikai Szövetségi Nyomozóiroda akkori igazgatója bejelentette, hogy újranyitja a nyomozást Hillary Clinton ellen a külügyministersége alatt használt magán e-mail-szerverrel összefüggésben.⁹ Anthony Weiner volt kongresszusi demokrata képviselő¹⁰ elektronikus eszközein ugyanis több Hillary Clinton szerveréről származó adatot találtak, amikor azokat egy 15 éves lánynak küldött szeméremértő üzenetek miatt megvizsgálták.¹¹

⁷ GOSZTONYI–LENDVAI (2026)

⁸ Monográfiámban a szabályozás (*regulation*) fogalma alatt az írott szabályokat (különösen jogszabályokat) értem, amelyek *ex ante* módon, a jövőre nézve állapítanak meg és érvényesítenek kötelező normákat.

⁹ Marc FISHER – John WODROOW COX – Peter HERMANN: Pizzagate: From rumor, to hashtag, to gunfire in D.C. *The Washington Post*, 2016. december 6., https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html

¹⁰ Hillary Clinton közeli segítőjének, Huma Abedinnak a férje.

¹¹ Amanda ROBB: Anatomy of a fake-news scandal. *The Rolling Stone*, 2017. november 16., <https://www.rollingstone.com/politics/politics-news/anatomy-of-a-fake-news-scandal-125877>

Két nappal később, 2016. október 30-án jelent meg az első tweet a #PizzaGate összeesküvés-elmélettel kapcsolatban, amikor egy ismeretlen személy egy New York-i ügyvéd, David Goldberg fantomfiókja alatt az alábbi bejegyzést tette közzé: „a New Yorki-rendőrségen az a hír járja, hogy Huma emailjei pedofil hálózatra mutatnak, és @Hillary Clinton áll a középpontban.” A tweet emellett egy hiperlinket is tartalmazott Carmen Katz azon Facebook-bejegyzésére, amely azzal vádolta Hillary Clintont, hogy „dokumentáltan előszeretettel viselkedik a kiskorú lányok iránt.”¹² A tweetet (beleértve az azt tartalmazó hiperlinket) több mint 6000-szer retweetelték.¹³ Az összeesküvés-elmélet futótűzként kezdett terjedni névtelen vagy álnevesített hozzászólásokon keresztül más közösségimédia-platformokon (Reddit, 4chan), valamint más összeesküvés-elméleti oldalakon (GoodLike Productions, InfoWars, YourNewsWire).

A #Pizzagate kifejezés először a Twitteren jelent meg 2016. november 7-én. A következő hetekben naponta több ezer #Pizzagate-ről szóló tweetet osztottak meg világszerte, főként a Cseh Köztársaságból, a Vietnámi Szocialista Köztársaságból és Ciprusról. Ekkor már nemcsak a jobboldali aktivisták és összeesküvés-elméleteket vallók vettek részt a terjesztésben, hanem botok (bizonyos hírek és információk felerősítésére szolgáló programok) és kincsvadászok (*treasure hunters*) is, mint például a macedón tinédzserek, akik élvezték a közösségi oldalak *trending news* hirdetési és díjazási rendszere miatt az ezen álhírek által biztosított gazdasági előnyöket.

Míg a hozzászólások egy része a részletek egyszerű megismétlése volt, a többi még tovább ment a megalapozatlan vádakkal, azt terjesztve, hogy Hillary Clinton gyermekkereskedelemben és a pedofiliában vett részt. Alex Jones, az InfoWars nevű (egyébként összeesküvés-elméletekről és dezinformáció-terjesztésről hírhedt) weboldal alapítója egy 2016. november 4. napján közzétett YouTube-videóban például kijelentette, hogy amikor arra a sok gyermekre gondolt, akiket Hillary Clinton személyesen gyilkolt meg, aprított fel és erőszakolt meg, egyáltalán nem fél kiállni ellene. A SubjectPolitics.com pedig egy virálisan terjedő (hamis) cikket közölt az alábbi főcímmel: „VÉGE: Az NYPD házkutatást tartott Hillary Clinton ingatlanán. Amit találtak, TÖNKRETESZI AZ ÉLETÉT.”

Közben a botrány egy másik szála is elkezdett kibontakozni. Októberben a WikiLeaks kiszivárogtatta John Podesta, Hillary Clinton kampányfőnökének meghekkelt e-mailjeit, amelyek közül néhányban John Podesta és testvére, a lobbista Tony Podesta vacsoratervekről, pizzákról és egy bizonyos északnyugat-dakotai pizzériáról, a Comet Ping Pongról beszéltek. Az egyik e-mailben a két testvér még a Comet Ping Pong tulajdonosát, James Alefantist is meghívta, hogy főzzön Clinton adománygyűjtésére.¹⁴ Alefantis számára nem volt ismeretlen az amerikai politika, mivel korábban a Cometben Clinton kampányának adománygyűjtő esteket rendezett, kapcsolatban állt David Brockkal, valamint számos (vásárlói és baráti) kapcsolata volt a Demokrata Párttal.¹⁵

¹² Azt a mai napig nem lehet tudni, hogy pontosan ki állt David Goldberg és Carmen Katz fantomfiókjai mögött.

¹³ Craig SILVERMAN: How The Bizarre Conspiracy Theory Behind „Pizzagate” Was Spread. *BuzzFeed News*, 2016. december 5., <https://www.buzzfeed.com/craigsilverman/fever-swamp-election>

¹⁴ James ALEFANTIS: What happened when ‘Pizzagate’ came to my restaurant. *The Washington Post*, 2017. április 19., https://www.washingtonpost.com/opinions/pizzagate-taught-us-the-value-of-community/2017/04/19/92cae67c-23b0-11e7-bb9d-8cd6118e1409_story.html

¹⁵ Marc FISHER – John WODROOW COX – Peter HERMANN: Pizzagate: From rumor, to hashtag, to gunfire in D.C. *The Washington Post*, 2016. december 6., https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html

Mindezek alapján a Clinton-ellenes összeesküvés-elméleteket vallók és a Reddit és a 4chan oldalakon gyülekező online trollok elkezdtek a sajtos pizza (*cheese pizza*) kifejezést a pedofilokkal összekapcsolni, mivel a chatforumokon a 'c.p.' kezdőbetűket használják a gyermekpornográfia (*child pornography*) jelölésére.¹⁶ Hamarosan Hillary Clinton mellett más prominens demokrata politikusokat is megvádoltak azzal, hogy a Comet Ping Pong pincéjéből koordináltak egy gyermekkereskedő hálózatot.¹⁷ Ráadásul a továbbgyűrűző #Pizzagate-elméletek szerint egy egész földalatti alagutat építettek ki titkos szobákkal, ahol sátáni, sőt kannibalista rituáléknak adtak otthont.¹⁸

A #Pizzagate-elmélet számos válfaja ekkor már futótűzként terjedt az interneten. Az étterem tulajdonosa naponta kapott halálos fenyegetéseket, a Comet Ping Pong Facebook- és Yelp-oldalait elárasztották obszcén 'kritikákkal', az étterem tulajdonosának és személyzetének képeit, személyes adatait pedig közzétették az interneten.¹⁹ Emellett az étterem háztömbjében lévő többi üzlet tulajdonosait is kapcsolatba kezdték hozni az alagutakkal, rövidesen ők is fenyegető telefonhívások és e-mailek áldozataivá váltak.²⁰

A hazugságok odáig fajultak, hogy 2016. december 4-én az amerikai Edgar Maddison Welch egy puskával felfegyverkezve besétált a Comet Ping Pongba, az alkalmazottakra fogta a fegyverét, és többször belelőtt egy zárt ajtóba. A rendőrségi nyomozás során kiderült, hogy a fegyverest a #Pizzagate álhír motiválta, és az állítólagos gyermekkereskedelem ügyében akart nyomozni.²¹ Welch személyesen elismerte, hogy nem találta semmilyen nyomát illegális tevékenységnek, és Alex Jones is kijelentette egy 6 perces 'bocsánatkérő' videóban,²² hogy Alefantis és étterme nem vett részt semmilyen emberkereskedelemben, ahogy azt a #Pizzagate-ról szóló elméletek állították.

Mindezen cáfolatok ellenére a történet csak ideiglenesen halkult el, sokan még mindig megszállottan hisznek ezekben a hazugságokban. 2017 márciusában több tucat ember tüntetett a Fehér Ház előtt a #PizzaGate kivizsgálását követelve. 2019 januárjában letartóztattak egy 22 éves férfit, miután felgyújtotta a Comet Ping Pong éttermet.²³ 2020-ra a történet

¹⁶ Gregor AISCH – Jon HUANG – Cecilia KANG: Dissecting the #PizzaGate Conspiracy Theories. *The New York Times*, 2016. december 10., <https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html>

¹⁷ David O. KLEIN – Joshua R. WUELLER: Fake News: A Legal Perspective. *KMT*, 2017. május 1., <https://kleinmoynihan.com/fake-news-a-legal-perspective>

¹⁸ Gregor AISCH – Jon HUANG – Cecilia KANG: Dissecting the #PizzaGate Conspiracy Theories. *The New York Times*, 2016. december 10., <https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html>

¹⁹ James ALEFANTIS: What happened when 'Pizzagate' came to my restaurant. *The Washington Post*, 2017. április 19., https://www.washingtonpost.com/opinions/pizzagate-taught-us-the-value-of-community/2017/04/19/92cae67c-23b0-11e7-bb9d-8cd6118e1409_story.html

²⁰ Marc FISHER – John WODROOW COX – Peter HERMANN: Pizzagate: From rumor, to hashtag, to gunfire in D.C. *The Washington Post*, 2016. december 6., https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html

²¹ N/A: Washington gunman motivated by fake news 'Pizzagate' conspiracy. *The Guardian*, 2016. december 5., <https://www.theguardian.com/us-news/2016/dec/05/gunman-detained-at-comet-pizza-restaurant-was-self-investigating-fake-news-reports>

²² Paul FARHI: The conspiracy theory-obsessed host of InfoWars apologizes for promoting 'Pizzagate'. *Centre Daily Times*, 2017. március 26., <https://www.centredaily.com/news/nation-world/national/article140722218.html>

²³ N/A: Suspect charged for setting fire to 'Pizzagate' restaurant. *CBS News*, 2019. február 14., <https://www.cbsnews.com/news/ryan-jaselskis-suspect-charged-for-setting-fire-to-comet-ping-pong-pizzagate-restaurant-2019-02-14>

kicsit módosult is: Justin Bieber amerikai énekes *Yummy* című számáról hiszik sokan, hogy az „egy segélykiáltás, a titkos zeneipari pedofilhálózat leleplezése, a #Pizzagate-bili borítása.”²⁴

A módosulások ellenére az eredeti történeteszl is fennmaradt az interneten. 2020 augusztusában a Facebookon és más közösségi oldalakon egy digitálisan módosított (jelen esetben: hamisított) fénykép kezdett keringeni Hillary Clintonról.²⁵ A képen Hillary Clinton tengerparti kutyasétáltatás közben egy nyomkövetőt visel a bokáján (1. ábra). A volt amerikai külügyminiszterről készült hamis képet összekapcsolták a #PizzaGate összeesküvés-elmélettel, ezzel azt sugallva, hogy házi őrizetben van gyermekkereskedelemmel kapcsolatos vádak miatt.²⁶



1. ábra: A Hillary Clintonról készült digitálisan módosított felvétel a #Pizzagate alátámasztására²⁷

²⁴ BOLCSÓ Dániel: Visszatért a Pizzagate, és jobban terjed, mint valaha. *Index*, 2020. július 2., https://index.hu/techtud/2020/07/02/pizzagate_tiktok_amerika_elnokvalasztas_osszeeskues_elmelet_konteo_pedofil_pedofilia_justin_bieber

²⁵ N/A: Fact check: Altered photo shows ankle monitor on Hillary Clinton. *Reuters*, 2020. augusztus 17., <https://www.reuters.com/article/idUSKCN25D1UW>

²⁶ Uo.

²⁷ Forrás: <https://www.facebook.com/photo?fbid=3007323229329585&set=a.1237089659686293>

Az eredeti fényképet (2. ábra), amelyen Hillary Clinton nyomkövető nélkül sétáltatja kutyáját a New York-i Amagansett strandján Bill Clinton és egy titkosszolgálati ügynök társaságában, Matt Agudo készítette 2014-ben az INFphoto.com számára. Az eredeti fényképet digitálisan módosították (manipulálták), hogy azon nyomkövető is szerepeljen.



2. ábra: A Hillary Clintonról készült eredeti felvétel²⁸

Bár már közel 10 év telt el azóta, hogy a #Pizzagate összeesküvés-elmélet először megjelent az interneten, még mindig nem tűnt el a közösségi médiából. Éppen ellenkezőleg. Számos olyan – nemrég megjelent – technológia vagy alkalmazás széles körű elterjedésével, amelyek lehetővé teszik a felhasználók számára, hogy a mesterséges intelligencia segítségével bármilyen (hamis vagy nem hamis) tartalmat létrehozzanak, a #Pizzagate körüli kitalált történetek egyre örültebbek, az alátámasztó ‘bizonyítékok’ pedig egyre valóságosabbak lettek.

²⁸ Forrás: https://i.dailymail.co.uk/i/pix/2014/08/08/article-2720212-205E771500000578-434_634x762.jpg

Például 2023 novemberében a TikTokon keringett egy mesterséges intelligencia által generált videó, amelyben egy férfi arról beszélt, hogy Donald Trump amerikai elnök Guantanamo Bay-t, Guamot és Tierra del Fuegot jelölte ki olyan katonai perek lefolytatására, amelyekben többek között Hillary Clintont és John Podestát is bíróság elé állítják.²⁹

A fentebb leírtak ellenére – a rendelkezésre álló nyilvános információk alapján – úgy tűnik, hogy Hillary Clinton sosem kezdeményezett jogi eljárást becsületsértésért, jóhírnév megsértésért vagy rágalmazásáért sem a fotót készítő vagy megosztó felhasználók, sem pedig az online platformok ellen.

1.2. Módszertan

Az első kutatási alkérdés megválaszolása érdekében a monográfia alapvetően történeti-leíró és elemző módszertant alkalmaz. Ezt követően a második és harmadik alkérdés vizsgálatához a monográfia egy hipotetikus esettanulmány módszerével él: a #PizzaGate összeesküvés-elmélet keretében a Hillary Clintonról készült hamisított képmás megosztásának jogi vonatkozásait vizsgálja úgy, mintha az Európában, azon belül pedig Magyarországon történt volna. A #PizzaGate összeesküvés-elmélet mint a monográfia alapját képező esettanulmány az alábbi szempontok alapján került kiválasztásra:

- a) annak ellenére, hogy a #PizzaGate összeesküvés-elmélet nyilvánvalóan abszurd és valótlan, mind a mai napig jelen van az amerikai köztudatban, és jelentős számú követője akad;
- b) a #PizzaGate összeesküvés-elmélet azon kevés álhírek közé tartozik, amelyek súlyos, a valós életben is megnyilvánuló következményekkel jártak;
- c) a #PizzaGate-ügy az egyik leginkább dokumentált álhírként vizsgálható;
- d) a #PizzaGate összeesküvés-elmélet alátámasztására számos deepfake-felvétel készült.

1.2.1. Az adatgyűjtés módszerei

Jelen monográfia elkészítéséhez két nagyobb adatcsoportra volt szükség:

- a) A #Pizzagate összeesküvés-elmélet ténybeli hátterére vonatkozó tényadatok. Mivel a #Pizzagate összeesküvés-elmélet keretében megosztott eredeti tartalmak már nem elérhetők az interneten, a ténybeli hátteret újságcikkek alapján volt szükséges megállapítani.
- b) A platformok technikai hátterére vonatkozó adatok. Ezeket az információkat a következő forrásokból gyűjtöttem össze: i) a platformok magyarázó és oktató videóit; ii) személyes interjú Robert van Eijkel, a holland adatvédelmi hatóság vezető felügyeleti tisztviselőjével; iii) az érintett platformok használatakor szerzett személyes megfigyeléseim; és iv) a Hollandiában, a nagy közösségimédia-oldalak ellen indított adatvédelmi kollektív igényérvényesítéssel kapcsolatos ügyvédi munkám során szerzett tapasztalataim.

²⁹ N/A: Fact check: Hillary Clinton, Podesta were not tried by US military at Guantanamo. Reuters, 2023. december 6., <https://www.reuters.com/fact-check/hillary-clinton-podesta-were-not-tried-by-us-military-guantanamo-2023-12-06>

1.2.2. Elemzés és értelmezés

A #PizzaGate összeesküvés-elmélet keretében Hillary Clintonról terjesztett hamisított képmás megosztásának jogi elemzése során a következő logikai lépéseket követtem:

- a) Meghatároztam az alkalmazandó jogszabályokat, amelyek EU-s és magyar szinten szabályozzák a szóban forgó jogi kérdést (pl. nemzetközi szerződések, irányelvek, rendeletek, törvények).
- b) Ha az azonosított jogszabály rendelkezései nem voltak egyértelműek vagy elégségesek, az azt értelmező joggyakorlatot (pl. az EJEB, az EUB, a magyar bíróságok és az AB ítélkezési gyakorlatát) is megvizsgáltam.
- c) Ha a jogszabály értelmezése ezek után sem volt egyértelmű, másodlagos forrásokra támaszkodtam (pl. tudományos szakirodalom, könyvek, szaktanulmányok, kommentárok), hogy megtaláljam a választ a tárgyalt jogi kérdésre.

2. Az internet kialakulása

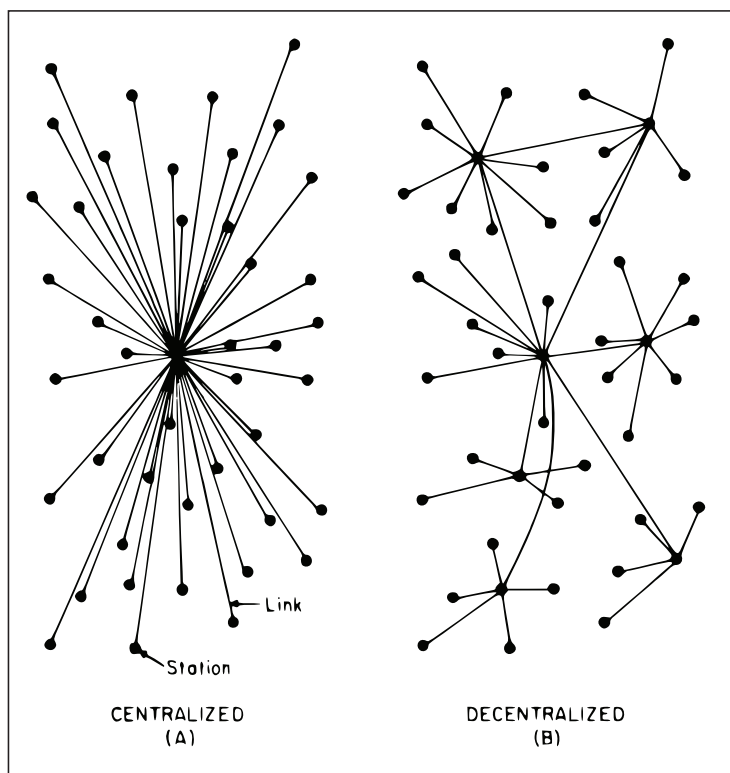
Az internet szükségessége a hidegháború egyik legfeszültebb pillanatában, a Szputnyik-1 műhold sikeres űrbe juttatásának idején merült fel. Eisenhower elnök – attól félve, hogy a szovjetek már az űrből is képesek lesznek Amerikára atomcsapást mérni – egy olyan hálózat létrehozását kezdeményezte, amely az esetleges pusztítás után is tovább működik. A Védelmi Minisztérium által 1958-ban megalapított Advanced Research Projects Agency (ARPA) kutatói megoldásként létrehozták az ARPANET-et, amely néhány amerikai egyetem számítógépét egy ‘központi’ számítógép használata nélkül kötötte össze, így biztosítva, hogy valamely gép megsemmisülése esetén is tovább élhessen a hálózat.¹

Az ARPANET kialakítása során a tudósoknak mindenekelőtt egy új hálózati struktúrát kellett kitalálniuk, amelyben nincs olyan központi elem, amelynek elpusztítása az egész hálózat leállításához vezethet. Egy ilyen hálózat felépítése azonban nem volt magától értő, mivel az ARPANET megteremtése előtt a tudósok a kommunikációs hálózatoknak ekkor még csak két alapvető fajtáját ismerték: (i) centralizált hálózat; és (ii) decentralizált hálózat.² A centralizált hálózat esetén valamennyi pont egyetlenegy központi elemhez csatlakozik, így a hálózat bármely két pontja közötti kommunikáció esetén a továbbítandó információnak szükségszerűen ezen középponton kell áthaladnia. A decentralizált hálózat ezzel szemben több centralizált hálózat összességeként épül fel, így annak nincsen egyetlen középpontja sem.³

¹ BARTÓKI-GÖNCZY-POGÁCSÁS (2019): 721.

² DeNARDIS (2014): 113.

³ LODDER-ZWENNE (2014): 2–3.



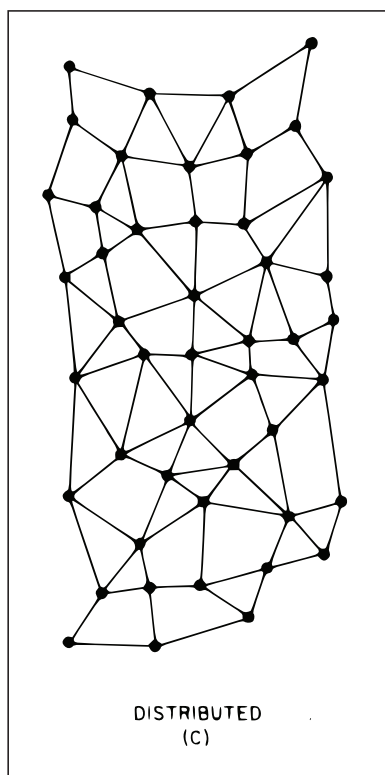
3. ábra: A centralizált és a decentralizált hálózat modellje⁴

Ahogy azonban az a 3. ábrából is egyértelműen kitűnik, sem a centralizált, sem pedig decentralizált hálózat nem volt alkalmas egy olyan rendszer kialakítására, amelynek nincsen központi eleme, és így az bármely pontjának megsemmisítése esetén is képes tovább működni. Mind a centralizált, mind pedig a decentralizált modell gyengesége ugyanis a hálózat teljes egészét vagy egy részét összekapcsoló középpont(ok)ban rejtett.

A centralizált és decentralizált hálózatok gyengeségének kiküszöbölésére, valamint egy stabil kommunikációs rendszer kiépítésére Paul Baran kínált megoldást, aki egy harmadik kommunikációs hálózat, a disztributív hálózat (4. ábra) kiépítésére tett javaslatot. Paul Baran ötlete ugyanis egy olyan rendszer kiépítése volt, amelyben valamennyi pont kapcsolatban áll a vele szomszédos pontokkal, anélkül, hogy a hálózat egyetlenegy középpontot is tartalmazna.⁵ Tekintettel arra, hogy a disztributív hálózat bármely két pontja között áramló információ több kommunikációs csatornán is továbbítható a címzettnek, Paul Baran rendszere alkalmas volt arra, hogy a hálózat annak bármely pontjának megsemmisülése esetén is hibátlanul működjön.

⁴ Forrás: BARAN (1964).

⁵ Yoo (2018): 165.



4. ábra: A disztributív hálózat modellje⁶

A fentebb leírtak ellenére Lawrence Roberts, az ARPANET kialakításáért felelős projekt vezetője végül a decentralizált, és nem a disztributív hálózat mellett döntött. Ennek elsődleges okai azok voltak, hogy a disztributív hálózat nem tette lehetővé az információ 0.2 másodpercen belül való továbbítását (amely az ARPANET-tel szemben támasztott egyik alapvető követelmény volt), és kiépítése túlságosan drága lett volna.⁷

Az ARPANET abból a szempontból is forradalmi áttörést jelentett az infokommunikáció terén, hogy az információt két számítógép között csomagkapcsolt technológiával közvetítette. A csomagkapcsolt adattovábbítás megjelenése előtt a távközlés elsősorban vonalkapcsolt technológiát alkalmazott, amely két kommunikáló számítógép között lévő állandó kapcsolat (vonal, csatorna) fenntartásán alapult.⁸ Ezen megoldás azonban nem tette lehetővé a kapcsolat gyors kiépítését, illetve az információ gyors továbbítását, és könnyen sebezhető volt.

⁶ Forrás: BARAN (1964).

⁷ Uo.

⁸ WALDEN (2018)

Míg maga a csomagkapcsolt technológia szintén Paul Baran nevéhez fűződik, a technológia ARPANET-ben történő felhasználása Leonard Kleirock munkásságára⁹ vezethető vissza.¹⁰ A csomagkapcsolt adattovábbítás lényege, hogy az információ nem egyben, hanem csomagokra bontva került továbbításra. A továbbítandó információ még a küldését megelőzően részinformációkra, csomagokra (*package*) bomlik, amelyek különböző útvonalakon továbbításra kerülnek a címzett számítógép részére, ahol végezetül ezen adatcsomagok ismételt összeállnak az eredetileg kézbesítendő információvá.¹¹

Az ARPA kutatói számára a harmadik kihívást annak a kérdésnek a megválaszolása jelentette, hogy miként biztosítható a hálózathoz kapcsolódó számítógépek egymással való kompatibilitása. A 60-as években ugyanis még nem létezett olyan standard protokoll, amely a számítógépek közötti kommunikációt biztosította volna. Mivel egy ilyen protokoll kidolgozása rengeteg időbe, befektetett energiába és anyagi forrásba került volna, az ARPA kutatóinak másfelől kellett a problémát megközelíteniük. E kérdésre végezetül Wes Clark szolgált válasszal, akinek elgondolása szerint szükségtelen a számítógépeket közvetlenül a hálózathoz csatlakoztatni; elegendő, ha az ARPANET és a számítógép közé egy olyan minikomputert, IMP-t (*interface message processor*) építenek be, amely interfészként funkcionál a számítógép és az ARPANET hálózat között. Az ARPANET tehát egy olyan többretegű hálózatként működött, ahol a számítógépek (1. szint) az azonos programnyelvet beszélő IMP-kből álló hálózathoz (2. szint) kapcsolódtak.¹²

Az ARPANET kiépítésére vonatkozó elképzelések végezetül 1969. október 29. napján a Bolt, Beranek és Newman nevű cég mérnöki segítségével valósultak meg, amikor Charley Kline a Stanfordi Egyetem kutatóintézetének SDS 940-es számú számítógépéhez csatlakozott a UCLA-n található Sigma 7-es számú számítógépen keresztül. Az ARPANET eredetileg négy amerikai egyetem (Stanford, University of California Los Angeles, University of California és University of Utah) számítógépeit kapcsolta össze.¹³ Az ARPANET hosszú ideig egy szigorúan ellenőrzött katonai projektként működött, 1983-ban azonban a hálózatról MILNET néven leválasztották annak hadászati szegmensét.¹⁴ Az ARPANET roham-szerű fejlődését jól szemléltetik az 5–8. ábrák, amelyek a hálózat komplexitását mutatják be.

⁹ Leonard Kleirock az ARPA csapatában arra a kérdésre kereste választ, hogy a számítógépek miként köthetők össze drága kábelek lefektetése nélkül.

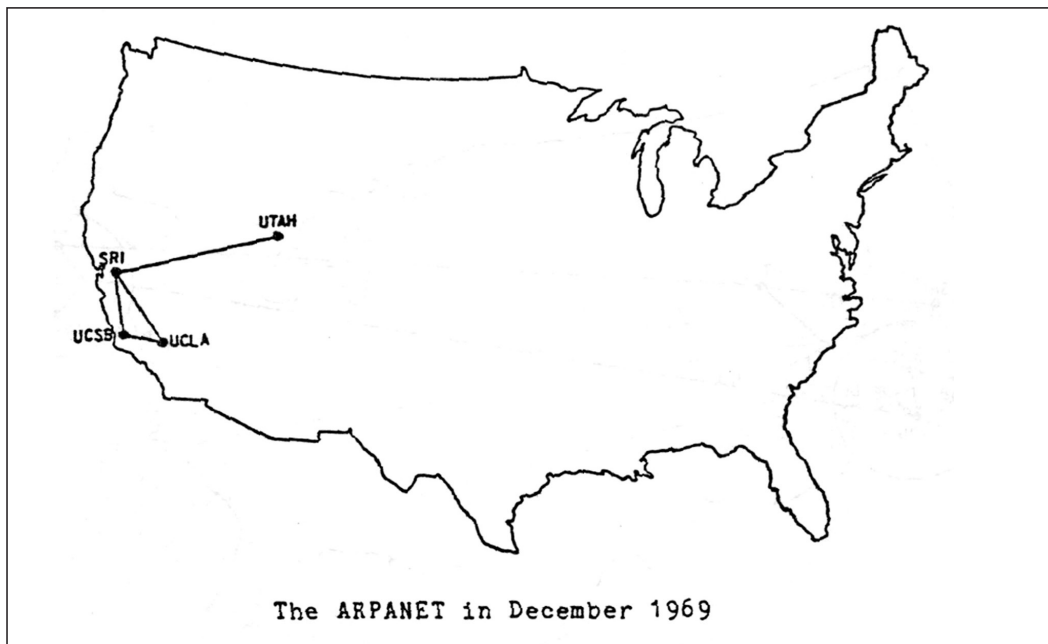
¹⁰ MURRAY (2023): 18.

¹¹ Uo.

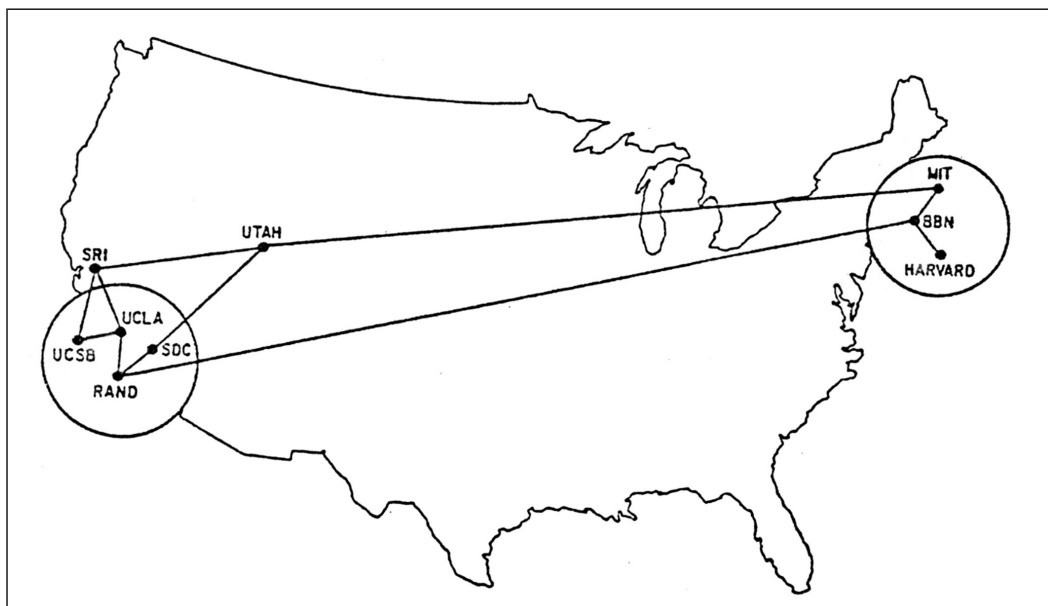
¹² MURRAY (2023): 19.

¹³ PACKARD (2023)

¹⁴ BARTÓKI-GÖNCZY-POGÁCSÁS (2019): 721.



5. ábra: Az ARPANET 1969 decemberében¹⁵



6. ábra: Az ARPANET 1970 júniusában¹⁶

¹⁵ Forrás: ARPANET Technical Information: Geographic Maps, <http://mercury.lcs.mit.edu/~jnc/tech/arpageo.html>

¹⁶ Forrás: Uo.

Az ARPANET azonban sok szempontból különbözött a mai, általunk ismert internettől. Az ARPANET ugyanis egyrészt egy hálózat volt és nem hálózatok hálózata, másrészt pedig zárt hálózatként működött, vagyis egy számítógép csak akkor tudott az ARPANET-hez csatlakozni, ha a felhasználó rendelkezett a megfelelően konfigurált, a Bolt, Beranek és Newman cég által biztosított IMP-vel.¹⁹

Mivel az ARPANET bebizonyította, hogy lehetséges egy olyan működő számítógéphálózatot létrehozni, amelyben valamennyi számítógép képes a többi számítógéppel kommunikálni, az ARPANET-et számos további számítógéphálózat megjelenése követte. Példának okáért, miközben Angliában és Franciaországban a helyi vezetékes internet alapjait fektették le, addig az Egyesült Államok Angliával és Norvégiával együtt létrehozta a SATNET-et, amely lehetővé tette, hogy a hálózathoz kapcsolódó számítógépek vezeték nélkül, szatelliten keresztül kommunikáljanak. Mivel azonban ezen hálózatok egymástól függetlenül alakultak ki, így a különböző hálózatokhoz csatlakozó számítógépek közötti kommunikáció továbbra is lehetetlen volt.²⁰

Bob Kahn, aki az IMP tervezésében működött közre a Bolt, Beranek és Newman cégnél, ezen különböző hálózatok egymással való összekapcsolását, és így a hálózatok hálózatának megteremtését tűzte ki céljául. Ezen cél elérése érdekében néhány társával együtt 1972-ben megalapította a Vincent Cerf által vezetett International Network Working Group nevű szervezetet, majd ugyanezen évben csatlakozott az IPTO Internetting Projektjéhez. Kahn felismerte, hogy a hálózatok összekapcsolásához egy újabb réteg (az *Internet-working Architecture Layer*) kialakítása szükséges, amelyen keresztül a hálózatok egymás között tudnak kommunikálni. Ez a megoldás tehát lehetővé tette, hogy a különböző számítógéphálózatok megőrizték a hálózatokon belüli egyedi kommunikációs nyelveket, miközben biztosította az egymástól teljesen függetlenül kialakított hálózatok közötti interoperabilitást. Összességében tehát Kahn elmélete azon az ötleten alapult, hogy az ARPANET zárt rendszerét kell nyílt hálózati rendszerré átalakítani. Mivel azonban az ARPANET által ismert programozási nyelv (Network Control Protocol, NCB) az IMP-n kívül más hálózattal vagy eszközzel nem volt kompatibilis, Kahnnak módosítania kellett az NCB szabályain, aminek eredményeként kialakította az Internetnetwork Protocol (IP) új szabályait.²¹

Ezt követően Kahnnak – Vincent Cerf segítségével – arra a problémára kellett megoldást találnia, hogy miként lehetséges a különböző interfészeket alkalmazó, különböző továbbítási sebességgel működő és így különböző méretű információcsomagok továbbítására alkalmas hálózatok közötti információtovábbítást biztosítani. A kérdésre a választ Cerf a való világban találta meg, amikor rájött, hogy a szállítóknak teljesen mindegy, mit szállítanak, mivel a konténerek egységesített mérete és formája lehetővé teszi, hogy azokban bármi (pl. csokoládé vagy TV) bármilyen formában (pl. hajón vagy repülőgépen) továbbítható két pont között. Cerf e felismerést a digitális világra alkalmazva megalkotta a Trans-

¹⁹ MURRAY (2023): 19.

²⁰ Uo., 20.

²¹ Uo., 20–21.

mission Control Protocol-t (TCP). A TCP/IP²² bemutatására 1973-ban az International Network Working Group nemzetközi találkozóján került sor a Sussex Egyetemen.²³

A napjainkban általunk ismert internet kialakulása szempontjából végezetül fontos megemlíteni a Sir Timothy John ('Tim') Berners-Lee által kitalált programozási nyelvet (HTML),²⁴ aminek folyományaként 1992-ben megszületett a World Wide Web.²⁵ Míg ugyanis a 80-as években az internethasználat jellemzően az akadémiai szférára korlátozódott,²⁶ addig az úgynevezett hiperlinkek megjelenésével az internet bárki által könnyedén használható hálózattá alakult, amelyen a hiányos informatikai ismeretekkel rendelkező felhasználó is könnyedén 'szörfölhetett'.²⁷

²² A TCP/IP olyan protokollok, amelyek a számítógépek között továbbítandó információcsomagok formázását, címzését és továbbítását szabályozzák, lehetővé téve így az interneten történő adattovábbítást. Az IP az információcsomag fejlécének a felépítésére, tartalmára vonatkozóan állapít meg univerzális szabályokat, így biztosítva, hogy az információ a megfelelő címzetthez érkezzon meg. A TCP arra vonatkozóan ír elő szabványokat, hogy az információ kézbesítését követően a címzett számítógép hogyan, milyen tartalommal küldjön vissza a feladó számítógép számára egy válaszüzenetet, az információ megérkezésére vonatkozó megerősítést. Egyszerű példára lefordítva az IP a boríték címzését, a TCP a tértivevény visszaküldését szabályozza (DeNARDIS [2014]: 67–68.; LODDER–ZWENNE [2014]: 3.).

²³ MURRAY (2023): 22.

²⁴ BARTÓKI-GÖNCZY-POGÁCSÁS (2019): 721.

²⁵ PINTÉR (2007): 116.

²⁶ Uo.

²⁷ BARTÓKI-GÖNCZY-POGÁCSÁS (2019): 721.

3. Az internet szabályozására vonatkozó elméletek

Az internethasználat kilencvenes évek közepén történő exponenciális terjedésével – amelyet az 1. táblázat szemléltet – egyidejűleg felmerült az internet szabályozása iránti igény is.

1. táblázat: **Az internetfelhasználók számának növekedése 1995 és 2000 között¹**

Dátum	Felhasználók száma (fő)
1995. december	16 millió
1996. december	36 millió
1997. december	70 millió
1998. december	147 millió
1999. december	248 millió
2000. december	361 millió

A szabályozással kapcsolatban több olyan kérdés is megfogalmazódott, amelyekre egyáltalán nem volt egyértelmű a válasz. Lehetséges-e egyáltalán egy földrajzi határokat nem ismerő, fizikailag kézzel nem megfogható hálózatot szabályozni, és ha igen, akkor azt milyen eszközökkel, milyen formában lehet megvalósítani, illetve a szabályok követését miként lehet ellenőrizni?²

3.1. Nemzetközi kontra állami szabályozás

Az államoknak mindenekelőtt azt kellett eldönteniük, hogy az internetet nemzetközi vagy állami szinten kívánják-e szabályozni. A nemzetközi szabályozás képviselői ugyan eltérő álláspontokat fogalmaztak meg a szabályozás forrását és eszközeit (pl. önszabályozás, nemzet-

¹ Forrás: <https://www.globalpolicy.org/component/content/article/109-tables-and-charts/27519-internet-users.html>

² PINTÉR (2007): 116.

közi egyezmény) illetően, azonban abban kivétel nélkül valamennyien egyetértettek, hogy az internetnek a területi alapon megvalósuló állami szabályozása sem elméletben, sem gyakorlatban nem működik.³

A nemzetközi szabályozást elsősorban a technológiai, illetve a telekommunikációs iparban működő cégek karolták fel, akiknek – az internet területi alapon megvalósuló állami szabályozása következtében – egyszerre majdnem 200 különböző jogrendszernek kellett (volna) megfelelniük. Steve Case például az internettel összefüggésben felmerülő biztonsági, adatvédelmi és adójogi kérdések nemzetközi rendezésének szorgalmazása mellett több alkalommal is nyíltan kritizálta a nemzeti jogalkotóknak a telekommunikáció és az adójog területén érvényesülő ‘államközpontú’ szabályozásait, mivel azok szükségszerűen gátat szabtak az internet természetes fejlődésének.⁴ A nemzetközi szabályozás képviselői elsősorban abból indultak ki, hogy az internet nem az első olyan globális jelenség (pl. tengerjog, légi jog, nemzetközi kereskedelem stb.), amely nemzetközi együttműködést igényel az államok részéről. Ahmad Kamal például az internet jogi szabályozását a nemzetközi vizek szabályozásához hasonlította, és így amellet foglalt állást, hogy globális tárgyalásokat kell kezdeményezni az internet átfogó és összehangolt jogi szabályozása, valamint egy, a nemzetek felett álló szabályozóhatóság kialakítása érdekében.⁵

Az internet nemzetközi szabályozása mellett szólt tehát egyrészt a joghatósági konfliktusok megszüntetése, másrészt pedig a ‘*patchwork*-szabályozás’ felszámolása következtében az internetfelhasználók életének és az internetet működtető cégek működésének megkönnyítése. Az internetre vonatkozó egyetlen nemzetközi szabályozás ugyanis minden bizonnyal lehetővé tette volna mind a felhasználók, mind pedig az IT-cégek számára, hogy a cselekedeteik következményeit biztosan előre láthassák. Az internet ily módon megvalósuló szabályozása azonban nemcsak az internetfelhasználók és az IT-cégek, hanem a kormányok számára is több szempontból kedvező lett volna.⁶ Jean-Pierre Chevenement volt francia belügyminiszter például amellet foglalt állást, hogy a globális szabályozás kialakítása a bűnözők számára menedéket nyújtó ‘digitális rejtékely’ felszámolása érdekében elkerülhetetlen.⁷

A fentebb leírtakkal szemben azonban számos jogtudós (pl. Polyák Gábor,⁸ Jack Goldsmith és Tim Wu⁹) úgy vélte, hogy a hálózat kulturális sokszínűségére, az interneten megjelenő értékek és azok védelme iránti igények különbözőségére tekintettel az egységes nemzetközi jogi szabályozás megvalósíthatatlannak látszik.¹⁰ 2001. március 15-én Vincent Cerf, az internet egyik alapító atyja a *New York Times*-nak adott interjújában akként nyilatkozott, hogy az internet az államhatároktól tekintet nélkül lett kialakítva, és így az azon keresztül megvalósuló adatforgalom is független a földrajzi határoktól.¹¹ Bár Vincent Cerfnek

³ GOLDSMITH–WU (2006): 27.

⁴ STEVE CASE: Remarks Prepared for Delivery (via satellite) Israel ‘99 Business Conference’ (1999. december 13.), idézi: GOLDSMITH–WU (2006): 194.

⁵ KAMAL (2005): 255., 260.

⁶ GOLDSMITH–WU (2006): 26.

⁷ McCULLAGH (2000)

⁸ POLYÁK (2001): 169.

⁹ GOLDSMITH–WU (2006): 149.

¹⁰ POLYÁK (2001): 169.; GOLDSMITH–WU (2006): 149.

¹¹ LISA GUERNSEY: Welcome to the World Wide Web. Passport, Please? *The New York Times*, 2001. március 15., <https://www.nytimes.com/2001/03/15/technology/welcome-to-the-world-wide-web-passport-please.html>

kétségtelenül igaza volt abban, hogy az internet egy földrajzi határokat nem ismerő globális hálózatként lett megtervezve, az elmúlt harminc év tapasztalatai azonban mégis azt igazolják, hogy az államhatárok az interneten is kirajzolódtak.¹²

Jack Goldsmith és Tim Wu három okra vezették vissza az államhatároknak az interneten való kirajzolódását. A szerzők elsőként arra hívták fel a figyelmet, hogy az államhatárok egyben nyelvi határok, amelyek szükségszerűen kisebb csoportokra tagolják az internet felhasználóit.¹³ A 90-es években széles körben elterjedt gondolat volt, hogy ahogy a TCP/IP lett az Internet protokollnyelve, úgy az angol lesz az interneten elérhető tartalom univerzális nyelve. Ezen prófécia azonban, elsősorban a nemzeti kormányok által kifejtett ellenállás következtében, rövid időn belül megdőlni látszott. A nemzeti kormányok ugyanis hamar felismerték, hogy mivel a következő generációk életének az internet elválaszthatatlan részét fogja képezni, az angol konyhanyelvűvé válva komoly fenyegetést jelenthet az egyéb nyelvekre és kultúrákra. Így míg a 90-es évek végén az interneten elérhető tartalom 80%-a angol nyelven íródott, addig 2023-ban az interneten elérhető tartalom 55%-a volt angol.¹⁴

Az internetfelhasználók nyelvi sokszínűsége önmagában még nem lenne elég indok az internet nemzetközi szabályozásának elvetésére. Az államhatárok azonban nem csak nyelvi, hanem egyben kulturális határok is, amelyek mögött különböző kultúrák, társadalmi berendezkedések, valamint politikai/jogi rendszerek húzódnak. Ebből egyrésztől az következik, hogy a különböző országok polgárai különböző tartalmak iránti igényeket támasztanak az internettel szemben.¹⁵ Egy tokiói lakos például nyilvánvalóan a tokiói időjárásra, a Tokióban elérhető fodrászok telefonszámára kíváncsi, nem pedig az egyiptomi közlekedési hírekre.

A különböző kulturális, történelmi hagyományokat tükröző politikai, jogi rendszerek továbbá különböző elvárásokat támasztanak az állampolgárokkal, a területükön élő/tartózkodó vagy tevékenykedő személyekkel szemben.¹⁶ Ezen eltérések azonban nem csupán az egymástól drasztikusan eltérő politikai rendszerek (pl. egy demokratikus és egy diktatórikus berendezkedésű állam) között érzékelhetők. Így például a szólásszabadság területén a Hollandiában jogszerű tartalom Tennessee-ben obscénnek; a japán anime az Egyesült Államokban gyermekpornográfiának, és a New York-i Disney-mese Bajorországban gyermekekre káros tartalomnak minősül.¹⁷ Két demokratikus állam jogrendszerének a szólásszabadságról kialakult eltérő felfogását legjobban talán a *Yahoo!, Inc. kontra La Ligue Contre Le Racisme et l'Antisemitisme (LICRA)* eset szemlélteti. Az ügy tényállása szerint a francia Rasszizmus és Antiszemitizmus Elleni Liga, valamint a Franciaországi Zsidó Diákok Uniója a francia bíróság előtt keresetet nyújtott be a Yahoo! ellen azon az alapon, hogy az amerikai székhelyű böngésző megsértette a francia jogot azáltal, hogy a honlapján keresztül tiltott náci relikviákat lehetett vásárolni. A bíróság a jogerős döntésében a Yahoo! felelősségének

¹² GOLDSMITH–WU (2006): 58.

¹³ Az anyanyelv jelentőségét a Windows első kézből tapasztalhatta meg, amikor az izlandi kormány az alábbi ultimátumot ajánlotta az amerikai cégnek: vagy lefordítják izlandi nyelvre a Windows operációs rendszert, vagy a kormány más operációs rendszer (pl. az izlandi nyelven is elérhető Apple operációs rendszer) alkalmazását teszi kötelezővé.

¹⁴ Internet Society Foundation: What are the most used languages on the Internet? *ISF.org*, 2023. május 15., <https://www.isocfoundation.org/2023/05/what-are-the-most-used-languages-on-the-internet>

¹⁵ GOLDSMITH–WU (2006): 59.

¹⁶ Uo., 51. és 151.

¹⁷ LESSIG–RESNICK (1999): 395.

megállapítását követően arra kötelezte az alperest, hogy a vitatott tartalmakat a francia állampolgárok számára tegye elérhetetlenné.¹⁸ „A Yahoo! azonban az amerikai bírósághoz fordult, kérve annak megállapítását, hogy az ítélet az Egyesült Államokban nem bír kötelező erővel és nem végrehajtható. A kaliforniai bíróság a Yahoo!-nak adva igazat kijelentette, hogy a francia ítélet nem végrehajtható, mivel az sértené az első alkotmánykiegészítésben foglalt szólásszabadsághoz való jogot.”¹⁹

Ahogy ez az ügy is szemlélteti, az internet centralizált nemzetközi szabályozásának egyik legnagyobb hátránya, hogy az képtelen az országok kultúrájában, történelmi hagyományokban és jogi gondolkodásában rejlő különbségek érvényesülését biztosítani. Még abban az esetben is, ha az internetet szabályozó egyezmény – Cairncross javaslata alapján – pusztán ‘*best practice*-en’ alapuló rendelkezéseket tartalmazna, statisztikailag valószínűsíthető, hogy a közel hatmilliárd emberre irányadó egyetlen normaszöveggel legalább egymilliárd ember nem lenne elégedett.²⁰ Végezetül azt is látni kell, hogy amennyiben az államok mégis egy egységes nemzetközi egyezmény mellett döntenének, az nem csak hogy hosszú ideig nem kerülne elfogadásra, de feltehetően – a konszenzus érdekében – túl általános megfogalmazású lenne ahhoz, hogy a rohamosan változó internet problémáira valódi megoldást tudjon nyújtani.

3.2. Az internetszabályozás versengő irányzatai

Az internetszabályozás kérdéseire számos versengő irányzat kínált különböző megoldásokat.²¹ Tekintettel azonban arra, hogy jelen fejezet célja az internetszabályozás alapjainak ismertetése, illetve a képmáshoz való jog interneten történő szabályozásának kontextusba helyezése, jelen alfejezet ezen versengő elméletek közül csupán a három legfontosabbat (kiberlibertarizmus, kiberpaternalizmus, integrált szabályozás elmélete) kívánja bemutatni.

3.2.1. Kiberlibertarizmus, avagy a jogmentes tér mítosza

A kiberlibertarizmus (*cyberlibertarianism*) az internet kialakulásával egyidőben fejlődött ki, és a 80-as években, valamint a 90-es évek elején élte fénykorát. A kiberlibertarizmus az internet korai korszakának szellemét tükrözte, és így az internetre vadnyugatként tekintett, ahol a szólásszabadság és a véleménynyilvánítás szabadsága szabadon szárnyalhatott bármilyen állami szabályozás vagy jogi korlátozás nélkül.²² A kiberlibertarizmus – ahogy arra az elmélet neve is utal – elutasította bármely állam vagy nemzetközi szervezet beavatkozását, és a hangsúlyt kizárólag a felhasználók önszabályozására helyezte.²³ Az elmélet képviselői

¹⁸ DUH (2002)

¹⁹ BARTÓKI-GÖNCZY-POGÁCSÁS (2019): 735.

²⁰ GOLDSMITH-WU (2006): 27., 152.

²¹ PINTÉR (2007): 116.

²² ZANATHY (2021)

²³ PINTÉR (2007): 116–117.

abból indultak ki, hogy mivel az interneten nem érvényesülnek a fizikai, földrajzi határok, így a kibertér természeténél fogva *de facto* alkalmatlan a tradicionális értelemben vett jogi szabályozásra (jogmentes tér mítosza).²⁴

A kiberlibertarizmus értelmében azonban az internet nem csupán *de facto*, hanem *de lege* is alkalmatlan volt a szabályozásra. A nemzetközi jog egyik legfontosabb alapelve, hogy egy állam a szuverén hatalmát kizárólag a területi határain belül gyakorolhatja: a területi határok tehát valójában az állam végrehajtási jogának, az állami kényszer gyakorlásának tényleges határait határozzák meg. Mivel azonban a kiberlibertarizmus szerint az internet egy olyan, szuverén határokat nem ismerő virtuális tér, amely az országok felett ‘lebeg’, és így az lehetetlenné teszi az államok számára, hogy kizárólag a saját területükön gyakoroljanak kontrollt, a jogmentes tér mítosza értelmében bármilyen állami beavatkozás, szabályozás illegitim.²⁵ A kiberlibertarizmus elmélete mögött tehát valójában az a jogi érvelés húzódott, hogy mivel egy országnak sincs kizárólagos joghatósága az internet felett, így valójában egyetlen országnak sem állapítható meg joghatósága.²⁶

A jogmentes tér mítoszának képviselői közé tartoztak többek között David Jhonson, David Post és John Perry Barlow. Utóbbi volt az első, aki az internetet – a William Gibson 1984-es science-fiction novellájából, a *Neurománcból* ismert fogalommal – a kibertér (*cyberspace*) elnevezéssel írta le.²⁷ Másrészről, Barlow 1990. július 10. napján Mitch Kaporral (a Lotus 1-2-3 alapítójával) és Jhon Gilmore-ral (a Sun Microsystem első programozójával) együtt megalapította az Electronic Frontier Foundation-t (EFF), egy alapítványt, amelynek elsődleges célja azon elképzelés, szabályozási koncepció minél szélesebb körben történő érvényre juttatása volt, hogy a kibertér a való világtól független, és így nem tűr semmilyen kormányzati beavatkozást.²⁸ Az EFF-et az alapítók tehát kettős szándékkal hozták létre: (i) az internetfelhasználók szabad véleménynyilvánításhoz, szólásszabadsághoz, gondolatszabadsághoz való jogának, valamint az új technológiák (pl. internet és World Wide Web) használatához való jogosultságának garantálása; és (ii) a kibertér és a való világ között felmerülő konfliktusok békés úton való rendezése.²⁹ Az EFF az alapítását követően rövid időn belül hatalmas támogatásra tett szert, nem túl meglepő módon, elsősorban a Szilícium-völgy elitjének körében. Az alapítvány támogatóinak neve között szerepelt például Bill Joy (a Sun Microsystems egyik alapítótagja), Rob Glaster (a Microsoft korábbi igazgatója), Bruce Katz, a Microsoft, valamint a Hewlett-Packard. A támogatók személyének és anyagi támogatásának köszönhetően a kiberlibertarizmus meghatározó lobbitevékenységet folytatott Washingtonban az internet külső állami beavatkozásaitól (elsősorban az amerikai kormánytól) való védelmének kiépítése érdekében.³⁰ Végezetül, szintén Barlow nevéhez kapcsolódik az 1996. február 8. napján kihirdetett Kibertér-függetlenségi Nyilatkozat (Declaration of Independence of Cyberspace), amely többek között hangsúlyozta a kibertér szuverenitását és az államok internet szabályozási törekvéseinek feltétel nélküli elutasítását.³¹

²⁴ MURRAY (2011): 198.

²⁵ MURRAY (2011): 199.

²⁶ PINTÉR (2007): 116–117.

²⁷ MURRAY (2007): 5.

²⁸ GOLDSMITH–WU (2006): 18.

²⁹ NHAN–CARROLL (2012): 390–391.

³⁰ GOLDSMITH–WU (2006): 19.

³¹ BARLOW (1996)

Az internet állami szabályozásának elutasítása azonban semmiképpen sem jelentett egy anarchikus társadalmi rend interneten való kiépítése iránti elköteleződést.³² Ezen elmélet képviselői ugyanis az internetet egy olyan térként képzelték el, ahol szabályrendszerként a felhasználók által kialakított etikai normarendszer, az úgynevezett netikett érvényesült volna.³³ David Jhonson és David Post az interneten érvényesülő netikettet a kereskedők által a középkorban alkalmazott *Lex Mercatori*ához hasonlították. A *Lex Mercatori*át a kereskedők ugyanis pontosan azon problémára adott válaszként fogadták el, miszerint a kereskedők a jogvitáikkal nem tudtak és nem is akartak a kereskedelmet nem ismerő és az iránt egyáltalán nem érdeklődő földesurakhoz fordulni.³⁴

A kiberlibertarizmus értelmében tehát az internet polgárai (*netizens*) egy olyan önszabályozáson alapuló rendszert alakítottak volna ki,³⁵ amelyben (i) az internetfelhasználók és szolgáltatók alkotják a szabályokat; (ii) az így közösen kialakított etikai kódexek megszegése egyeztető fórumon kerül elbírálásra;³⁶ (iii) a közösség által elfogadott szankciókat pedig technikai eszközökkel (pl. felhasználói fiók megszüntetése, feltöltött tartalom törlése stb.) rendszeroperátorok (*system operators*) hajtják végre.³⁷

Az önszabályozás mellett szólt egyrészt, hogy a szabályokat olyanok alkotják, akik a legközelebből ismerik mind az igényeket, mind a szabályozandó viszonyokat. Másrészt, hogy egyedül ez a szabályozási mód képes az internet gyors változásával lépést tartani azáltal, hogy a demokratikus alapelveket úgy juttatja érvényre, hogy közben az általa megalkotott norma rugalmas marad.³⁸ Végezetül pedig az önszabályozás harmadik előnye, hogy a joghatósági kérdések, konfliktusok hiányában önszabályozás esetén nem kérdőjelezhető meg az elfogadott normák és végrehajtott szankciók legitimitása.³⁹

3.2.2. Kiberpaternalizmus

A kiberpaternalizmus (*cyberpaternalism*) a kiberlibertarizmus által felvetett kérdések megválaszolására, illetve a kiberlibertarizmus által hirdetett eszmékkel szembeni kritika megfogalmazására jött létre. Felismerve az interneten megvalósuló jogsértések, bűncselekmények felfezhetetlen terjedését, a kiberpaternalizmus mindenekelőtt tagadta az interneten keresztül felmerülő jogviszonyok pusztán önszabályozás útján való rendezését. A kiberpaternalizmus ugyanis – a kiberlibertarizmussal ellentétben – az internetet nem a szólásszabadság fellegváraként látta, hanem sokkal inkább egy fertőként, ahol olyan súlyos bűncselekmények, mint például gyermekpornográfia, csalás, személyiséglopás, terrorizmus és drogkereskedelem, büntetlenül virágozhatnak.⁴⁰ A kiberpaternalizmus továbbá elutasította a kiberlibertarizmus

³² JOHNSON–POST (1996): 1389.

³³ PINTÉR (2007): 116–117.

³⁴ JOHNSON–POST (1996): 1389–1390.

³⁵ Uo., 1388.

³⁶ BAYER (2002): 451.

³⁷ JOHNSON–POST (1996): 1388.

³⁸ BAYER (2002): 451.

³⁹ JOHNSON–POST (1996): 1387.

⁴⁰ MURRAY (2011): 199.

képviselői által hirdetett azon gondolatot, miszerint mivel a kibertérben nem érvényesülnek az államhatárok, így az internet természeténél fogva immunis bármilyen állami szabályozásra.⁴¹

A szakirodalom a kiberpaternalizmusnak két alágát különbözteti meg: (i) kiberrealizmus (*cyberrealism*) és (ii) technodeterminizmus (*technodeterminism*).⁴² A kiberrealizmus értelmében az interneten konfrontálódó jogrendszerek következtében felmerülő joghatósági kérdések egyáltalán nem újszerű problémák a nemzetközi jogban. A közlekedés, kommunikáció területén bekövetkezett fejlődés ugyanis már jóval korábban arra kényszerítette az államokat, hogy szakítsanak a területi elven alapuló joghatóság elméletének kizárólagos alkalmazásával, valamint, hogy ismerjék el az idegen jogrendszerek extraterritoriális érvényesülését.⁴³

A kiberrealizmus szerint a kiberlibertarizmus képviselői akkor követtek el kibertérrel kapcsolatban logikai hibát (*cyberspace fallacy*), amikor az internetre olyan szuverén határokat nem ismerő önálló jogrendszerként gondoltak, amely kizárólag a virtuális térben létezik. A fizikai megtestesülés hiányából – a kiberrealizmus szerint tévesen – a kiberlibertarizmus képviselői azt a következtetést vonták le, hogy az mind *de facto*,⁴⁴ mind pedig *de lege*⁴⁵ alkalmatlan a tradicionális értelemben vett jogi szabályozásra.

A kiberrealizmus képviselői ezen kibertérrel kapcsolatos logikai hibát az alábbi érveléssel igyekeztek orvosolni. Mivel az internet végső soron nem más, mint egy kábelekkal összekötött számítógép-hálózat, így a kibertér több ponton is összekapcsolódik a való világgal (pl. az internetfelhasználók tartózkodási helye, a számítógépek, kommunikációs eszközök fekvése stb). A kibertérnek ezen, való világban megjelenő leképeződései különböző államok joghatóságai alá tartoznak, így az internetet valójában nem hogy nulla, hanem egyszerűen több, egymással versengő jogrendszer is szabályozza.⁴⁶ Mivel azonban az internet pontosan csak annyira globális jelenség, mint bármelyik másik nemzetközi együttműködést igénylő terület, így annak állami szabályozása nem okozhat problémát pusztán a különböző jogrendszerek összeütközése miatt.

A kiberpaternalizmus keretében kialakult második irányzat, a technodeterminizmus (vagy más néven Berkman-iskola) Lawrence Lessig munkássága következtében vált ismerté, noha ezen elmélet kialakulása Joel Reidenberg *Lex Informatica: The Formulation of Information Policy Rules through Technology* című szakcikkében foglaltakra vezethető vissza.⁴⁷

⁴¹ MURRAY (2023): 66.

⁴² GOSZTONYI (2022a)

⁴³ GOLDSMITH (1999): 1206.

⁴⁴ A kiberlibertarizmus képviselői abból indultak ki, hogy mivel az interneten nem érvényesülnek a fizikai, földrajzi határok, így a kibertér természeténél fogva *de facto* alkalmatlan a tradicionális értelemben vett jogi szabályozásra [GOSZTONYI–ZANATHY (2025): 79.].

⁴⁵ A nemzetközi jog egyik legfontosabb alapelve, hogy az állam a szuverén hatalmát kizárólag a területi határain belül gyakorolhatja. A területi határok tehát valójában az állam végrehajtási jogának, az állami kényszer gyakorlásának tényleges határait határozzák meg. Mivel azonban a kiberlibertarizmus szerint az internet olyan, szuverén határokat nem ismerő virtuális tér, amely az országok felett 'lebeg', és így az lehetetlenné teszi az államok számára, hogy kizárólag a saját területükön gyakoroljanak kontrollt, a jogmentes tér mítosza értelmében bármilyen állami beavatkozás, szabályozás illegitim. A kiberlibertarizmus elmélete mögött tehát valójában az a jogi érvelés húzódott, hogy mivel egy országnak sincs kizárólagos joghatósága az internet felett, így valójában egyetlen országnak sem állapítható meg joghatósága [GOSZTONYI–ZANATHY (2025): 79.].

⁴⁶ MURRAY (2023): 66.

⁴⁷ MURRAY (2011): 201.

Reidenberg a jogmentes tér mítosza és a Berkman-iskola közötti kapcsolatot alakította ki azáltal, hogy elismerte a kiberlibertarizmus azon elgondolását, miszerint az internet szabályozása annak struktúrája miatt szükségszerűen csak a területi határok figyelmen kívül hagyása mellett valósítható meg; ugyanakkor azt is hangsúlyozta, hogy a kibertér szabályozásával összefüggésben az államot és a jogszabályokat egy újfajta ‘szabályozás’ (*Lex Informatica*) váltotta fel, amelynek értelmében az internetfelhasználókat egyrészt az internetszolgáltatók közötti szerződések, másrészt az internet technológiai felépítése szabályozza.⁴⁸

Reidenberg az internetszabályozás alapjainak lefektetése érdekében – Thomsonhoz és Posthoz hasonlóan – a *Lex Mercatoria*ából, a középkorban a kereskedelmi viszonyokat rendező önszabályozás keretében elfogadott és alkalmazott nemzetközi szabályzatból indult ki.⁴⁹ Felismerve, hogy a jogszabályok csak pontosan körülhatárolt, az államok kizárólagos szuverén hatalma alatt álló területeken belül érvényesíthetők,⁵⁰ Reidenberg egy, a *Lex Mercatoria*hoz hasonló, az interneten felmerülő jogviszonyok rendezésének elsődleges forrásként alkalmazandó soft law, a *Lex Informatica* elfogadására tett javaslatot.⁵¹ Elképzelése szerint a *Lex Informatica* technológiai sztenderdek összessége, amely a technológiai lehetőségek és a rendszerek struktúráinak szabályozása útján közvetve rendezi az internetfelhasználók magatartásait.⁵² A *Lex Informatica* tehát lényegében maga a hálózat, így a *Lex Informatica* közőmbös az államhatárok miatt felmerülő joghatósági konfliktusokra. Ahogy arra már fentebb utaltunk, a *Lex Informatica* tartalmát egyrészt a technológiai lehetőségek, másrészt pedig a fogyasztók (internetfelhasználók) által kialakított gyakorlat határozza meg. A *Lex Informatica* elsődleges forrásai tehát az interneten keresztül működő technológiák fejlesztői; míg a *Lex Informatica* ‘rendelkezései’ automatikusan, önmaguktól kerülnek végrehajtásra.⁵³

A Reidenberg által leírt *Lex Informatica* tehát az alábbi három előnnyel rendelkezett: (i) a *Lex Informatica* alkalmazását nem befolyásolják a nemzethatárok; (ii) a *Lex Informatica* rugalmas és egyszerre valamennyi állam jogszabályainak megfelelő szabályozást biztosít; valamint (iii) a *Lex Informatica* betartásának felügyelete és végrehajtása automatikusan valósul meg.

3.2.3. Az integrált szabályozás, avagy ‘a ló joga’

1996-ban a Chicagói egyetemen megrendezett ‘A kibertér joga’ című konferencián Frank H. Easterbrook fellebbviteli bíró hatalmas botrányt keltett az előadásával, amelyben a kibertér jogát (kiberjog, *cyberlaw*) a lovakat szabályozó joghoz (*law of horse*)⁵⁴ hasonlí-

⁴⁸ MURRAY (2023): 66.

⁴⁹ MURRAY (2011): 201.

⁵⁰ REIDENBERG (1997–1998): 570.

⁵¹ MURRAY (2011): 201.

⁵² REIDENBERG (1997–1998): 555.

⁵³ Uo., 570–572.

⁵⁴ A ló joga kifejezés utalás a Chicagói egyetem korábbi dékánjának, Gerhard Gaspernek elgondolására, miszerint a jogi kar nem dilettáns majmokat képez, így szükségtelen a jogszabályi rendelkezések speciális esetekre történő alkalmazását külön tárgyként tanítani. Gerhard Gasper szerint tehát a jogi karnak nem feladata a lovakkal összefüggésben felmerülő jogviták (pl. ló által okozott kár megtérítése iránti jogvita) rendezésére szolgáló speciális jogot (‘a ló joga’) oktatni, helyette a diákoknak az általános jogelveket, jogszabályi rendelkezéseket (pl. kötelmi jog, kártérítési jog stb.) kell elsajátítani.

totta.⁵⁵ Easterbrook bíró tehát – a konferencián megjelent IT-jogászok dilettánsoknak nyilvánítását követően – amellet foglalt állást, hogy a kiberjog mint önálló jogág – a ló jogához hasonlóan – nem létezik, hiszen az valójában nem más, mint a már létező és hatályos jogszabályok kibertérben történő alkalmazása.⁵⁶ Ebből következőleg Easterbrook az interneten felmerülő jogviszonyok szabályozásával összefüggésben többek között az alábbiakat tanácsolta a konferencián megjelent hallgatóság számára:

„Folytasd tovább, amit eddig csináltál!” Az interneten felmerülő jogviszonyok nagy része a hatályos jogszabályok megfelelő alkalmazásával könnyen azonosítható és rendezhető. Szükségtelen tehát újabb jogszabályok elfogadása pusztán azért, mert a jogviszony nem a való világban, hanem a kibertérben keletkezett.⁵⁷

„Tedd világosabbá a jogszabályokat!” Tagadhatatlan, hogy a kibertér – természeténél fogva – megnehezítette egyes jogszabályok értelmezését. Abban az esetben tehát, amennyiben egy jogszabályi rendelkezés alkalmazása nem egyértelmű, az adott jogszabályi előírás módosítása szükséges a világos jogalkalmazás és a jogbiztonság biztosítása érdekében. A jogalkotónak azonban tartózkodnia kell az internet *ex ante* szabályozásától, vagyis attól, hogy az interneten potenciálisan kialakuló jogviszonyokat valós vagy vélt érdekek mentén előzetesen rendezze.⁵⁸

„Teremts tulajdoni viszonyokat ott, ahol még nincsenek!” Az internetet a fizikai világhoz hasonlóan egy olyan világgá kell alakítani, ahol a ‘mindennapi életet’ elsősorban a tulajdonjog rendezi.⁵⁹

Ugyan kétségtelenül vitatható Easterbrooknak az IT-jogászok dilettantizmusával, illetve a kiberjog létének teljes megalapozatlanságával kapcsolatos véleménye, valójában csak az internetszabályozás egyik legelterjedtebb elméletének, az integrált szabályozásnak az alapjait ismertette. Az integrált szabályozás értelmében ugyanis az interneten keletkező jogviszonyok a társadalmi struktúra integráns részei. Az irányzat képviselői tehát az internetszabályozás módját a már létező jogszabályok kisebb-nagyobb átalakításában látták. Az internet elterjedésével és az azon megvalósuló viszonyok számának növekedésével ugyanis egyre világosabbá vált, hogy az internet nem vonható ki a létező büntetőjogi, polgári jogi vagy egyéb jogterületi szabályozás alól.⁶⁰ Nyilván elképzelhetetlen lenne egy olyan világ, amelyben ugyanazon termék vevőjét eltérő jogok és kötelezettségek illethetik meg illetve terhelhetik, attól függően, hogy az interneten vagy a valós, fizikai életben kötött adásvételi szerződést.

Ezen elmélet értelmében tehát az internetnek egyetlen egy olyan területe sincs, amely jogon kívül állna. Ebből következően az interneten, pontosabban annak segítségével elkövetett jogsértésekre a jogsértés időpontjában hatályos jogszabályok irányadók.⁶¹ Így például, ha egy közösségi oldalon valakinek a képmáshoz való jogát megsértették, akkor ugyanúgy a Polgári törvénykönyvről szóló 2013. évi V. törvény (Ptk.) az irányadó, mintha a jogsértést nem a virtuális, hanem a való világban követték volna el.

⁵⁵ EASTERBROOK (1996): 207.

⁵⁶ MURRAY (2007): 9.

⁵⁷ EASTERBROOK (1996): 210.

⁵⁸ Uo., 210–211.

⁵⁹ Uo., 212.

⁶⁰ PINTÉR (2007): 117.

⁶¹ BARTÓKI-GÖNCZY-POGÁCSÁS (2019): 730–731.

3.2.4. Az önszabályozás, az állami szabályozás és a társszabályozás

A fentiekből következik, hogy míg a kiberlibertarizmus az önszabályozás mellett foglalt állást, addig a kiberpaternalizmus és az integrált szabályozás elmélete az állami beavatkozás bizonyos fokát szükségesnek tekintette. Az állam szabályozásban betöltött szerepének mértékétől függően két fő megközelítés különböztethető meg: (i) a teljes állami szabályozás; és (ii) a társszabályozás.⁶²

Teljes állami szabályozás alatt az a megközelítés értendő, amikor az állam kizárólag kötelező erejű jogi eszközökkel, szankciókkal és végrehajtási mechanizmusokkal igyekszik a jogalanyok magatartását befolyásolni. Ezt a szabályozási modellt a jogalkotó tipikusan olyan esetekben alkalmazza, amikor a jogalanyokat (elsősorban vállalatokat) olyan normák betartására kell kötelezni, amelyek a közérdeket szolgálják, ugyanakkor nem feltétlenül állnak összhangban a jogalanyok saját érdekeivel (például a vállalati profit maximalizálásával). Fontos ugyanakkor hangsúlyozni, hogy bár a teljes állami szabályozás elve szerint a szabályozás kizárólag jogszabályok útján valósul meg, a jogalkotó ezen belül többféle szabályozási stratégiát alkalmazhat: a klasszikus, azaz utasításon és ellenőrzésen alapuló (*command and control*) modelltől kezdve egészen a 'piacformáló' szabályozási megközelítésig.⁶³ Bár az érintett iparág bizonyos mértékben jogosult és képes a jogalkotási folyamat során releváns visszajelzést adni, a teljes állami szabályozás legnagyobb hátránya, hogy a szabályozást elsősorban olyan szervek és személyek alakítják, akik nem ismerik és nem értik kellő mélységben az iparág sajátosságait. Ennek következtében fennáll a kockázata, hogy a jogszabályok nem tükrözik megfelelően az adott iparág sajátos működését és dinamikáját.⁶⁴

Társszabályozás alatt az állami szervek és a szabályozott jogalanyok együttműködésén alapuló szabályozási módszer értendő, amelyben tehát keverednek az önszabályozás és a jogi szabályozás elemei.⁶⁵ A koregulációs modell mellett az szól, hogy képes az önszabályozás azon gyenge pontját orvosolni, amelynek értelmében az így kialakított normák nem kikényszeríthetők. Abban az esetben tehát, ha valaki kilép az önszabályozás keretéből, a jogi szabályozás továbbra is képes az esetleges jogsértést megakadályozni vagy a már bekövetkezetteket orvosolni. Társszabályozásról azonban csak akkor beszélhetünk, ha az állam az önszabályozást elismeri, azaz deklarálja, hogy ezt a fajta 'joghatóságot' az államéval teljeskörűen és alapjaiban azonosnak tekinti a saját törvényszerűségein belül. E feltétel teljesülése érdekében az államnak a következőket kell biztosítania:

- a) pontosan kerüljön rögzítésre az állami szerepvállalás tartalma, keretei, valamint az önszabályozás területei, és
- b) az állami feladatok 'kiszervezése', azok megvalósításához szükséges jogok és kötelezettségek civil társadalomra való átruházása (ideértve a szükséges anyagi források rendelkezésre bocsátását is).⁶⁶

⁶² GORWA (2024): 59.

⁶³ BALDWIN–CAVE–LODGE (2012): 106–107.

⁶⁴ GORWA (2024): 59–61.

⁶⁵ MENYHÁRD (2021)

⁶⁶ ROZGONYI (2003): 647–648.

A társszabályozásnak számos előnye és hátránya van. Előnyei közé tartozik, hogy költséghatékony, mivel kevesebb szabályozási erőforrást és kompetenciát igényel a jogalkotó és a végrehajtó szervektől. Hátránya viszont, hogy végrehajtási erő hiányában hatástalan lehet olyan esetekben, amikor a szabályozott jogalanyok nem áll érdekében a szigorú, a közérdeket előtérbe helyező szabályozás betartása.⁶⁷

3.3. Kód-jog, avagy *Code is law*

Valamennyi fentebb ismertetett elmélet azon kérdésre kívánt választ találni, hogy a jogi eszközökkel megvalósuló szabályozás (jelen alfejezetben a továbbiakban: jog) miként képes az internetet, illetve az interneten keresztül megvalósuló emberi magatartásokat szabályozni. A teljesség érdekében azonban szükséges megjegyezni, hogy Lawrence Lessig szerint a jog csupán egy a négy szabályozási eszköz közül, amely egy személy online viselkedését meghatározza. Annak érdekében, hogy az internet működéséről és szabályozásáról átfogó képet kaphassunk, elkerülhetetlen Lessig ezen elméletének, illetve az azzal összefüggésben megfogalmazott kritikák és alternatív javaslatok részletes bemutatása.

Lessig elképzelése értelmében valamennyi szabályozás középpontjában a szabályozni kívánt alany, az úgynevezett ‘szánalmas pont’ (*pathetic dot*) áll, amelyet az alábbi négy erő szabályoz: a jog, a társadalmi normák, a piac, valamint a fizikai környezet.⁶⁸ Ezen erők azonban természetesen nem egymástól függetlenül fejtik ki hatásukat, hiszen azok egymást erősíthetik, gyengíthetik vagy pusztán egyéb indirekt módon befolyásolhatják (9. ábra).⁶⁹ Példának okáért a jogi norma közvetlenül befolyásolja a piacot, amikor az adásvétel tárgyát szabályozza (pl. szervkereskedelem tilalma), a piacon érvényesülő árak továbbá meghatározzák a fizikai környezetünket (pl. az olcsó építőanyagok az épületek számának növekedéséhez vezetnek), a fizikai környezetünk pedig hatást gyakorol a társadalmi normákra (pl. a nagy számban elérhető épületek megerősítik a magánszféra iránti igényünket).⁷⁰ Lessig szerint tehát valamennyi szabályozás ezen négy erő összessége, illetve az általuk kifejtett hatások, bennük megtestesülő értékek közötti kereskedelem.⁷¹

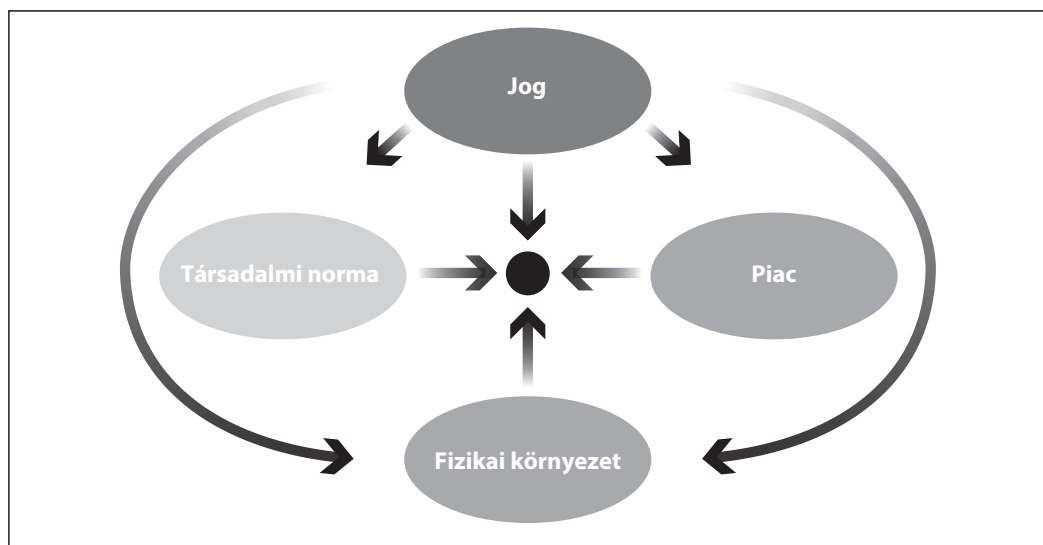
⁶⁷ GORWA (2024): 61–64.

⁶⁸ LESSIG (2006): 122–123.

⁶⁹ LESSIG (1999): 509–510.

⁷⁰ Uo., 509. és 511.

⁷¹ ZÓDI (2020); HASSAN – DE FILIPPI (2017).



9. ábra: A Lessig-modell⁷²

Lássuk most ezt a négy erőt egyenként:

1. A jog – Lessig definíciója értelmében – a legitim jogalkotó által elfogadott előírás, amely a száználmas pont magatartását azáltal szabályozza, hogy meghatározza a megengedett tevékenység kereteit, illetve szankciókat állapít meg ezen határok átlépése, jogsértés esetén.⁷³ A szabályozni kívánt alany tehát azért nem fogyaszt kábítószer Magyarországon, mert tudja, hogy az szabadságvesztéssel büntetendő cselekmény.
2. Lessig elgondolása értelmében a társadalmi norma a joghoz hasonlóan, negatív következmények kilátásba helyezésével, *ex post* módon korlátozza az emberi magatartást. A társadalmi normák azonban a jogszabályi rendelkezésektől eltérő módon kerülnek kikényszerítésre, hiszen ezen normák megsértése esetén fenyegető szankciók decentralizáltak, illetve azok végrehajtásáért nem a kormány, hanem a közösség felel. Példának okáért tehát a száználmas pont azért nem szív el egy cigarettát egy csecsemő jelenlétében, mert tudja, hogy az rosszallást (megvető tekinteteket, akár egy-két szúrós megjegyzést is) váltana ki a társadalom részéről.⁷⁴
3. Lessig elméletében a harmadik szabályozó erő a piaci erő, amely a piaci szereplők magatartását az árakon keresztül határozza meg. A szabályozni kívánt alany például a gázolajárak egekbe emelkedése esetén az autó helyett inkább a tömegközlekedési eszközt veszi igénybe.⁷⁵

⁷² Saját szerkesztés.

⁷³ LESSIG (1999): 508; LESSIG (2006): 124.

⁷⁴ LESSIG (2006): 122.

⁷⁵ JIMÉNEZ GONZÁLEZ (2021)

4. Végezetül a kibertérben érvényesülő negyedik erő a fizikai környezet, vagyis – ahogy Lessig nevezi – a kód (*code*).⁷⁶ A kód, illetve a szoftver és hardver az, ami a kibertérrel olyanná teszi, amilyennek azt mi, felhasználók érzékeljük.⁷⁷ Az ugyanis, hogy az e-mail-fiókunkhoz csak jelszó megadása után férhetünk hozzá, hogy a WhatsApp-beszélgetések titkosítottak, vagy, hogy milyen személyes adatok megadása kötelező egy Facebook-profil létrehozásához, kizárólag annak az informatikusnak a döntésétől függ, aki ezen programok kódját megírta. A programozók tehát valójában, *de facto* törvényalkotók, hiszen ők döntenek el, hogy a kibertérben mit és hogyan szabad. Lehet arról jogszabályi rendelkezés ugyanis, hogy a személyes adatok kezeléséhez szükséges hozzájárulás nem köthető ki a szolgáltatás nyújtásának feltételeként, ha ezzel egyidejűleg csak úgy lehet egy Facebook-profil létrehozni, hogy a felhasználó a közösségi oldal által megvalósítandó adatkezelési műveletekhez hozzájárul.⁷⁸

Az internet szabályozása szempontjából Lessig elmélete azért jelentett hatalmas áttörést, mert az amerikai professzor érvelése szerint ezen négy szabályozási erő nem csak a fizikai világban, hanem a kibertérben is épp ugyanúgy érvényesül.⁷⁹ A jog – hol hatékonyan, hol kevésbé sikeresen ugyan, de – tagadhatatlanul befolyásolja a kibertérben tanúsított magatartásunkat. A jog által kilátásba helyezett jogkövetkezmények miatt ugyanis nem lopunk személyazonosságot, nem sértjük meg más becsületét, és nem törjük fel a rendőrség biztonsági rendszerét. A társadalmi normák a joghoz hasonlóan szintén keretet szabnak az interneten folytatott tevékenységünknek. Beszéljen valaki túl sokat a Facebookon, és rövid időn belül a 'barátainak' a blokkolt ismerősei között találja magát. Ezen hozzáállás egyébként nem teljesen idegen a modern jogalkotótól. A GDPR például bevezette a beépített adatvédelem (*privacy by design*) követelményét, amelynek értelmében valamennyi adatkezelő már az adatkezelési műveletei korai fázisainak tervezése során köteles olyan technikai és szervezési intézkedéseket bevezetni, amelyek kezdettől fogva szavatolják a magánélet védelmére irányuló és az adatvédelmi alapelvek érvényesülését.⁸⁰

Egyetértek Lessiggel abban, hogy a kibertér valójában nem más, mint a programozók által kialakított környezet, és ebből közvetlenül következik, hogy azon feltevés, miszerint a kibertér annak természetéből adódóan nem szabályozható, hibás gondolat. Ezen hibás gondolat alapja egyrészt, hogy a kibertér jellege fix, másrészt pedig, hogy ezen állandó, örök adottságok a jogalkotó által nem befolyásolhatók. Ha azonban elfogadjuk Lessig fentebb leírt elméletét, és a kibertérre egy olyan, a programozók elképzelése szerint kialakított környezetként tekintünk, amelyet a többi három szabályozási eszköz közvetve vagy közvetlenül képes befolyásolni, akkor könnyen beismerhető, hogy az internet szabályozásának korai

⁷⁶ KOLLÁR-SZÖKE (2023): 32–33.

⁷⁷ LESSIG (1999): 508.

⁷⁸ Lessig a *Code 2.0* című könyvében pontosan ezen felismerés következtében különbözteti meg a keleti part kódexét, az úgynevezett East Coast Code-ot (Washingtonban elfogadott és a US Code-ban kihirdetett jogszabályi rendelkezés) a nyugati part kódjától, az úgynevezett West Coast Code-tól (a Szilícium-völgyben vagy Redmondban írt és műanyagba égetett bitek útján kihirdetett kódok). LESSIG (2006): 136.

⁷⁹ LESSIG (1999): 507.; LESSIG (2006): 124.

⁸⁰ VÁRADI (2019): 49.

megközelítése már alapjaiban volt téves.⁸¹ Az tagadhatatlan ugyan, hogy az internet jelenlegi felépítése számtalan jogszabályi rendelkezés érvényesülését teszi lehetetlenné vagy legalább is nehezíti meg, ez azonban nem jelenti azt, hogy a kibertér ne lenne szabályozható. Abban az esetben ugyanis, ha a jogalkotó a jogot a felhasználók közvetlen szabályozása helyett arra használja, hogy a programozókra vonatkozóan ír elő kötelező szabályokat és így befolyásolja a kódot, akkor közvetve egy olyan kiberteret, környezetet teremt, amelyben a további jogszabályi rendelkezések már szabadon és hatékonyan érvényesülhetnek.⁸²

Az internet közvetett jogi szabályozásának kiváló példái a DRM (Digital Rights Management) technológiai megoldások. Az internet használatának elterjedésében sokan a szerzői jogok halálát látták, mivel az internet a szerzői jogi oltalom alatt álló művek gyors és ingyenes terjesztését, sokszorosítását tette lehetővé.⁸³ Az érdekképviselői szervek, illetve a jogalkotók nyomására azonban a programozók rövid időn belül kifejlesztették a DRM technológiai megoldásokat, amelyek lehetővé tették a digitális tartalmaknak az interneten történő elérhetővé tételét, oly módon, hogy azok engedély nélküli másolása vagy terjesztése technikailag lehetetlen volt. Ilyen DRM technológiai megoldást használ például az Apple iTunes, amely biztosítja a jogszerűen megvásárolt dalok meghatározott számú eszközre történő másolását, de nem teszi lehetővé ezen daloknak szélesebb körben való terjesztését.⁸⁴ A jogszabályi rendelkezéseknek programozás útján történő érvényre juttatásának másik példája az internetszolgáltatók által használt szűrők működése, amelyek egyes tartalmaknak az interneten való elérhetőségét lehetetlenítették el.⁸⁵

A Lessig által kidolgozott modell a '90-es évek végétől a 2000-es évek végéig élte a fénykorát. A 2000-es évek végén azonban mind a jogalkotóknak, mind a jogtudósoknak be kellett látniuk, hogy programozáson alapuló szabályozás önmagában nem elegendő. A DRM technológiai megoldások ellenére tömegesen valósultak meg szellemi tulajdonbitorlások az interneten (elsősorban az illegális fájlmegosztó portálokon), illetve az internetfelhasználók is rövid időn belül megtanulták kijátszani az internetszolgáltatók által alkalmazott szűrőket (pl. proxy, VPN, IP-cím-*spoofing* útján).⁸⁶

Ahogy arra Andrew Murray is rámutatott, a Lessig-modell és így programozáson alapuló szabályozás gyengesége ugyanis abban rejlett, hogy a modell középpontjában egyetlenegy pont állt, annak ellenére, hogy a szabályozandó individuum semmilyen körülmények között sem tekinthető elszigeteltnek, hiszen az minden esetben egy közösség részét képezi. Murray tehát művében a Lessig-modell tovább gondolásaként egy új modellre, az aktív mátrix-modellre (10. ábra) tett javaslatot.⁸⁷

⁸¹ DAVIDSON (2009): 11–24.

⁸² NORDELL (2021): 2.

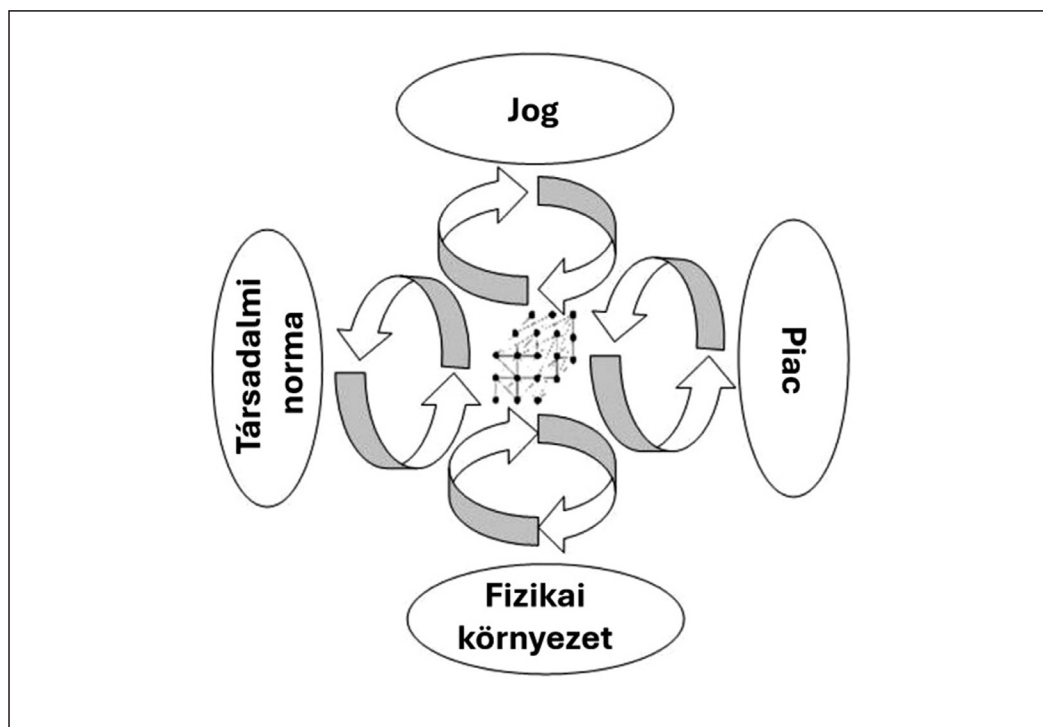
⁸³ LESSIG (1999): 522–523.

⁸⁴ LESSIG (2006): 116.

⁸⁵ MURRAY (2011): 209–210.

⁸⁶ Uo., 205.

⁸⁷ MURRAY (2007): 53–54.



10. ábra: Az aktív mátrix-modell⁸⁸

Ez a módosított modell két szempontból jelentett újdonságot Lessig modelljéhez képest. Egyrészt, ahogy arra már fentebb utaltunk, az aktív mátrix-modellben a szánalmas pont sosem szánalmas, és végképp nem egy izolált pont, hanem egy közösség, egy kapcsolathálózat része, amelynek tagjai állandó diskurzusban vannak egymással.⁸⁹ A modell középpontjában lévő egyetlen pontot tehát egy pontrendszer váltotta fel. Másrészt Murray felismerte, hogy a szabályozás tárgyára ható erők közül három (a jog, a piac és a társadalmi normák) a társadalom által közvetített korlátok, és így azok a társadalomból eredeztetik a legitimitásukat. A jog ugyanis a szavazók által megválasztott jogalkotók által elfogadott norma, a piaci erők a piaci szereplők által megtestesített keresletnek és kínálatnak a tükörképei, a társadalmi normák pedig a közösség által elfogadott értékrendek. Következésképpen ezen három erő által megvalósított szabályozás minden esetben egy, a pontokból felépülő társadalom és a szabályozó erő közötti párbeszéd eredménye.⁹⁰ Murray elmélete értelmében tehát Lessig modellje azért futott zátonyra a valóságban, mert abból a téves feltevésből indult

⁸⁸ Forrás: MURRAY (2011): 207.

⁸⁹ Uo., 206.

⁹⁰ Uo., 207–208.

ki, hogy a szabályozás a szabályozó hatalom monológja, nem pedig szabályozó és a szabályozott közötti párbeszéd. Murray továbbá amellett foglalt állást, hogy minden, ami az ember által teremtett, az ember által módosítható is – így a kibertér és a szűrőprogramok is.⁹¹ Ezért amennyiben a programozáson alapuló szabályozással a szabályozott közösség nem ért egyet, ezen közösség tagjai előbb vagy utóbb megtalálják a programnak azon gyengeségét (pl. *zero-days*), amellyel a kódon keresztül megvalósuló szabályozás megkerülhető.

Tökéletes példa az aktív mátrix-modell működésére mindaz, ami a Pirate Bay felszámolására irányuló kísérlettel összefüggésben volt tapasztalható.⁹² Mivel a Pirate Bay egy illegális fájlmegosztó honlap volt, a különböző országok jogalkotói számtalan módon igyekeztek azt felszámolni, többek között úgy, hogy az internetszolgáltatókat az oldal blokkolására kötelezték. Az internetfelhasználók azonban a jogalkotók e kísérletére tett válaszként tömegével hozták létre a Pirate Bay úgynevezett tükrözött oldalait (másolatait), amelyek, mivel különböző IP-címekkel rendelkeztek, nem kerültek az internetszolgáltatók által blokkolásra, és így elérhetőek voltak az internetezők számára.

A teljesség érdekében szükséges megjegyezni, hogy Andrew Murray aktív mátrix-modelljét saját maga fejlesztette tovább a későbbiekben. Egyrésztől azért, mert felismerte, hogy az internetfelhasználók közössége nem egy nagy közösségből, hanem számos kisebb, egymást lefedő csoportból épül fel. Másrésztől pedig azért, mert belátta, hogy a kisebb csoportok sem homogének, hanem éppen ellenkezőleg, valamennyi kapcsolatháló egy vagy több kapuőrt (*gatekeeper*⁹³) ölel fel, akik meghatározzák a közösség többi tagja irányába folyó információ mennyiségét és minőségét.⁹⁴

⁹¹ Uo., 210.

⁹² OBERHOLZER-GEE–STRUMPF (2010)

⁹³ BARTÓKI-GÖNCZY (2018)

⁹⁴ REED–MURRAY (2018): 140–143.

4. A tartalommoderáció és a platformszabályozás közelmúltbeli fejlődése

Amint fentebb említettük, az 1990-es években és a 2000-es évek elején az önkéntes moderálás volt az uralkodó norma a korai közösségi hálózatokban.¹ A vállalatok önkéntesen (i) szabályokat fogadtak el arra vonatkozóan, hogy mi számít elfogadható tartalomnak; és (ii) intézkedéseket hoztak saját szabályaik betartatására. A ‘korai *boomer*’ vállalatok között például széles körben elfogadott gyakorlat volt a pornográf anyagok eltávolítása a ‘család-barát’ vagy egyébként moderált szolgáltatások nyújtására való törekvés jegyében.²

A tartalom önkéntes moderálása és kurátori tevékenysége miatt azonban ezek a korai platformok elkerülhetetlenül ki voltak téve számos jogi kihívásnak. Az Amerikai Egyesült Államok Alkotmányának véleménynyilvánítás szabadságára vonatkozó Első Kiegészítésére tekintettel – amely egyébként az európai megközelítéshez képest szokatlanul széles körben nyújt védelmet a szólás valamennyi formájának³ – az alacsonyabb szintű bíróságok az Egyesült Államokban a platformok ilyen jellegű tartalommoderálását a kiadók vagy terjesztők kurátori felelősségének egy formájaként értelmezték. Következésképpen az önkéntes tartalommoderálást végző platformok felelősségre vonhatók voltak a felhasználók által közzétett tartalmakért.

Nem meglepő, hogy a fentiek miatt (a tartalom moderálásával kapcsolatos méretbeli, gyakorlatiassági, megbízhatósági és pénzügyi kérdések mellett) egyre több platform döntött úgy, hogy eltávolodik az önkéntes tartalommoderálástól. Válaszul két kongresszusi képviselő egy záradékot illesztett be egy távközlési jogszabályba, amely mentesítette a platformokat a tárhelyszolgáltatásért és a jogellenes tartalom eltávolításáért való felelősségük alól.⁴ Ez volt a Communication Decency Act 230. cikke (közismert nevén a CDA 230), amely kimondta, hogy „[a]z interaktív számítógépes szolgáltatás egyetlen szolgáltatóját vagy felhasználóját sem lehet más információtartalom-szolgáltató által nyújtott információk kiadójaként vagy előadójaként kezelni.”⁵ Bár a CDA 230 eredetileg arra volt hivatott, hogy a vállalatokat arra ösztönözze, hogy ne féljenek önkéntesen fellépni az illegális tartalmak ellen,⁶ a gyakorlatban mégis egyhamar a platformok lényegében korlátlan mentességéhez és elképzelhetetlen

¹ GORWA (2024): 20.

² Uo., 33.

³ SMUK (2019): 48–49.

⁴ BALENDRA (2024): 61.

⁵ Communications Decency Act (CDA), Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996).

⁶ GORWA (2024): 44.

túlhatalmához vezetett.⁷ Jack M. Balkin ezt a következőképpen fogalmazta meg: „a digitális véleménynyilvánítás (*speech*) magánkézben lévő, kifinomult kommunikációs infrastruktúrán keresztül folyik. Napjainkban a magánkézben lévő infrastruktúrák tulajdonosainak döntései határozzák meg a tényleges lehetőségeinket a megnyilvánulásra, ők irányítják azokat a digitális tereket, amelyekben az emberek egymással kommunikálnak. Ez a véleménynyilvánítás magánszabályozásának (*private governance*) problémája.”⁸

A CDA 230 nem csupán az Amerikai Egyesült Államok szabályozására gyakorolt mindmáig jelentős hatást, de számos más nemzetközi jogi megközelítést is befolyásolt az online szolgáltatások széles körének szabályozása vonatkozásában. 2000-ben az Európai Parlament és a Tanács elfogadta a 2000/31/EK irányelvet (E-kereskedelmi irányelv),⁹ amely úgyszintén mentességet biztosított a tárhelyszolgáltatók számára az általuk tárolt tartalmakért való jogi felelősség alól, feltéve, hogy (i) nem volt tudomásuk a jogellenes tartalomról, és (ii) a jogellenes tartalmat, amint arról tudomást szereztek eltávolították.¹⁰

A technológia fejlődésével és az online platformok mindennapi életünkben betöltött kiemelkedő szerepével egyre nagyobb szükség van az online szféra további szabályozására. Az európai politikai döntéshozók mind tagállami szinten, mind az EU-n belül aktívan részt vettek az online közvetítők tartalomszabályozási gyakorlatának alakításában, nem kötelező erejű jogszabályok (*soft law*), informális tárgyalások és társszabályozási eszközök alkalmazásával.¹¹ Az ilyen erőfeszítések egyik figyelemre méltó példája a Bizottság által 2011-ben indított ‘CEO Coalition to make the Internet a better place for kids’ elnevezésű kezdeményezés, amelyet olyan jelentős iparági szereplők támogattak, mint az Apple, a Facebook, a Google, a Microsoft, különböző uniós távközlési vállalatok, hardvergyártók és más cégek.¹² Ez a kezdeményezés munkacsoportok üléseinek sorozatából állt, amely öt alapelv kidolgozásában csúcsosodott ki: „egyszerű és megbízható jelentési eszközök a felhasználók számára, életkornak megfelelő adatvédelmi beállítások, a tartalomosztályozás szélesebb körű alkalmazása, a szülői felügyelet szélesebb körű elérhetősége és használata, valamint a gyermekek szexuális zaklatását tartalmazó anyagok hatékony visszaszorítása.”¹³

Az elmúlt években a felhasználók által generált tartalom platformjainak informális szabályozása egyre inkább intézményesült, formalizálódott és átláthatóvá vált. A 2010-es évek közepére az európai politikai döntéshozók e szabályozási folyamatok eredményeként nyilvános eredményeket és iránymutatásokat kezdtek követelni. Ez az elmozdulás olyan jelentős szabályozási keretek létrehozását eredményezte, mint (i) a jogellenes online gyűlöletbeszédre vonatkozó magatartási kódex, amely az aláíró cégeket arra kötelezi, hogy haladéktalanul távolítsák el a terrorista anyagokat és a szélsőségesnek ítélt, potenciálisan problémás tartalmak más formáit,¹⁴ és (ii) a dezinformációra vonatkozó uniós gyakorlati kódex, amely

⁷ GOSZTONYI (2023): 49.

⁸ BALKIN (2018): 199.

⁹ Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (elektronikus kereskedelemről szóló irányelv), HL L 178, 17/07/2000, 0001–0016.

¹⁰ Részletesen lásd: 7. fejezet.

¹¹ MARSDEN (2011): 139.

¹² LIVINGSTONE–O’NEILL (2014): 32.

¹³ GORWA (2024): 47.

¹⁴ HIETANEN–EDDEBO (2022)

az aláíró cégeket a dezinformáció visszaszorítására és online politikájuk fejlesztésére kötelezi.¹⁵ Amint azt Lános Petra Lea kifejtette: „a nem kötelező erejű jogi eszközök választása stratégiai jelentőségű, mivel így a tagállamok számára referencia-keretet biztosít anélkül, hogy az intervenció intézkedések területéhez tartozó szektorban a harmonizáció irányába tennének lépéseket.”¹⁶

Az EU és a tagállamok társszabályozásra irányuló erőfeszítései ellenére a 2010-es években bekövetkezett események sorozata teljesen nyilvánvalóvá tette, hogy informális menetrend-meghatározási és irányítási kísérleteik nem bizonyultak hatékonyak. „A platformszabályozásról szóló vita 2014-től felpezsdül[t]. Először is a Facebook/WhatsApp ügylet kiesésével,¹⁷ amely nyilvános vitát indított el a digitális platformok fúzióiról és felvásárlásairól.”¹⁸ Emellett a közösségimédia-platformokon szervezett több társadalmi mozgalom is hangsúlyozta, hogy jelentős szerepet játszanak a nyilvános viták alakításában. Nevezetesen például erre a 2011 eleji arab tavasz, a 2011-es londoni zavargások és az Occupy Wall Street mozgalom.¹⁹ Ezek az események megmutatták a közösségi média erőteljes befolyását a közhangulatra és a cselekvés mozgósítására.²⁰

Az európai jogalkotók nem engedhették meg maguknak, hogy továbbra is passzívak maradjanak. A kezdetben inkább tanácsadói megközelítést alkalmazó államok egyre inkább hajlandóságot mutattak arra, hogy a kormányzás közvetlenebb formái felé forduljanak.²¹ Egyre több szakpolitika célozza meg kifejezetten a nagy platformcégeket, és igyekszik eljárási szabályokat megállapítani a politikailag és társadalmilag vitatott tartalmak kezelésére vonatkozóan. Ezek a szabályozási törekvések nem pusztán az internetszolgáltatókra vagy általában az online közvetítőkre vonatkozó általános szabályok, hanem célzott beavatkozások, amelyek célja a felhasználók által generált tartalmakkal foglalkozó platformok által alkalmazott szabályalkotási és végrehajtási mechanizmusok alakítása. Bár a platformspecifikus szabályozások alkalmazási és végrehajtási körükben eltérőek, egyre inkább találhatók az oldalakon olyan kulcsfontosságú jellemzők, mint a kötelező bejelentési eljárások, a panaszkezelési mechanizmusok, valamint a megfelelő eljárás és az átláthatóság követelményeinek betartása.²²

E szabályozási váltás egyik legjelentősebb megnyilvánulása az EU digitális egységes piaci stratégiája, amely – mint Angyal Zoltán megjegyezte – három fő célkitűzést követ: (i) az online termékek és szolgáltatások hozzáférhetőbbé tétele az európai fogyasztók számára; (ii) a digitális hálózatok és innovatív szolgáltatások virágzásához szükséges feltételek és egyenlő versenyfeltételek megteremtése; és (iii) a digitális gazdaság növekedési potenciáljának maximalizálása.²³ A jelen monográfia szempontjából a digitális egységes piaci stratégia

¹⁵ MONTI (2020): 219.

¹⁶ LÁNCOS (2022): 60.

¹⁷ ALISON L. DEUTSCH: WhatsApp: The Best Facebook Purchase Ever? *Investopedia*, 2021. június 26., <https://www.investopedia.com/articles/investing/032515/whatsapp-best-facebook-purchase-ever.asp>

¹⁸ ABATE (2020)

¹⁹ GOSZTONYI (2023): 44.

²⁰ ABATE (2020)

²¹ GORWA (2024): 50.

²² Uo., 48.

²³ ANGAL (2020): 6.

gia legfontosabb pillére a Digitális szolgáltatásokról szóló rendelet,²⁴ amely szabályozza a tárhelyszolgáltatók felelősségét, és előírja a platformok számára a kellő gondossági kötelezettségeket, hogy biztonságos, kiszámítható és megbízható online környezetet hozzon létre, amely elősegíti az innovációt, és amelyben a Chartában rögzített alapvető jogok érvényesülnek.²⁵

Következésképpen a platformszabályozás árnyaltabb és összetettebb jogi keretté fejlődött, ami jelentős kihívások elé állítja az érintett vállalatokat. Ez a pálfordulás a szabályozás tekintetében máris feszültségekhez vezetett a túlnyomórészt amerikai platformok – amelyeket a szólásszabadságot erősen előtérbe helyező jogi hagyományok alakítanak – és az európai szabályozási megközelítés között, amelyet elsősorban az Emberi Jogok Európai Bíróságának ítélkezési gyakorlata és az uniós jogszabályok határoznak meg. Míg az Egyesült Államokból származó internet a véleménynyilvánítás szabadságának és a magánélet védelmének alappilléreire épült, az európai jogi hagyományok – miközben hasonlóan védik ezeket a jogokat – lehetővé teszik a korlátozásokat, feltéve, hogy ezek a korlátozások megfelelnek a szükségeség és az arányosság kritériumainak.²⁶

²⁴ Részletesen lásd: 8. és 9. fejezetek.

²⁵ DSA 1. cikk (1) bekezdés.

²⁶ GOSZTONYI (2023): 44.

5. A képmáshoz való jog

Az előző fejezetekben láthattuk, hogy a jelenleg uralkodó internetszabályozási elmélet az integrált szabályozás elmélete, miszerint a kibertérben létrejövő jogviszonyokra a meglévő jogszabályokat kell alkalmazni. Ahogyan arra már korábban kitértem, ezen szabályozási megközelítés hatékonyságának vizsgálata érdekében a monográfiámban a továbbiakban a #PizzaGate összeesküvés-elméletet kívánom elemezni.

A #PizzaGate összeesküvés-elmélet jogi elemzése során az első kérdés, amelyre választ kívánok találni, hogy vajon a #PizzaGate összeesküvés-elmélet keretében Hillary Clintonról terjesztett hamisított képmás sértette-e a volt külügyminiszter képmáshoz való jogát. Ezen kérdés megválaszolásához azonban elengedhetetlen a képmáshoz való jog szabályozásának rövid áttekintése. Továbbá tekintettel arra, hogy a képmáshoz való jog egy nevesített személyiségi jog, először a személyiségi jogok általános kereteiről kell röviden szólnunk.

5.1. A személyiségi jogokról általában

Székely László a személyiségi jogokat úgy határozta meg, mint „azok a nem vagyoni jellegű jogok, amelyek a polgári jogviszonyok alanyait azért illetik meg, hogy biztosítsák önálló, a többi jogalannal egyenlő jogi helyzetüket.”¹ A személyiségi jogokkal tehát a jogalanyt (természetes és jogi személyt egyaránt), és annak minden olyan tulajdonságát védjük, amely őt azzá teszi, aki vagy ami. Arra a kérdésre, hogy mi teszi indokolttá a személyiségi jogok védelmét, Személyi Kálmán² úgy felelt, hogy „minden jogtárgy meg kell, hogy találja védelmét a magánjogban.”³

A személyiségi jogok jogrendszerben betöltött helye kapcsán meg kell állapítanunk, hogy a Ptk.-ban kifejezetten megfogalmazott, vagy az általános személyiségi jog elemeként érvényesülő személyhez fűződő jogok elkülönülnek mind az emberi jogoktól, mind pedig az alkotmányos alapjogoktól. Hiszen míg az előbbi magánjogi jellegű, és így védelmére polgári

¹ SZÉKELY (2007): 144.

² SZEMÉLYI (1915): 4.

³ SZÉKELY (2011): 145.

jogi eszközök szolgálnak, addig az utóbbi kettő közjogi jogintézmény, és így érvényesítésükre az állam alapvetően közjogi eszközöket biztosít.⁴ Sólyom László ezt úgy fogalmazta meg, hogy „a személyiségi jogok az ember jogállásának alapvető kifejezői közé tartoznak.”⁵

Mivel a személyiségi jogok által védett jogtárgyat, a személyiséget nem lehet pontosan meghatározni, a személyiségi jognak sem lehet egy pontosan és tökéletesen körülhatárolt fogalma. A törvény e probléma áthidalása érdekében olyan általános védelmet alkot meg, amely a természetes és jogi személyek személyiségére és valamennyi egyéni adottságaira kiterjed.⁶ A Ptk. (2013. évi V. törvény a Polgári Törvénykönyvről) a személyiségi jogok szabályozása során tehát mindenekelőtt azok általános védelméről rendelkezik. Az 1959. évi IV. törvénytől (korábbi Ptk.) eltérően a személyiségi jogi generálklauszult két elemből felépítve fogalmazza meg: a Ptk. 2:42. § (1) bekezdése a személyiségi jogok lényegét és rendeltetését kifejező általános szabályt fogalmaz meg, míg a (2) bekezdés lényegében a korábbi Ptk. 75. § (1) bekezdését ismétli meg.⁷

A Ptk. – a korábbi Ptk. nem kielégítő szabályozásából tanulva – két újítást hozott. Egyrészt a korábbi szabályozástól eltérően a Ptk. 2:42. § (1) bekezdése a személyiségi jogok aktív oldalát hangsúlyozza. Másrészt pedig azáltal, hogy a 2:42. § (2) bekezdése a személyiségi jogok anyajogaként tekint az emberi méltóságra, feloldja a korábbi szabályozás azon ellentmondását, amelynek értelmében egy, a személyiségi jogoknál jóval tágabb fogalom – az emberi méltóság – nevesített személyiségi jogként került meghatározásra.⁸

A védelemre jogosultak körénél meg kell állapítanunk, hogy az mind a természetes, mind pedig a jogi személyekre kiterjed. A Ptk. 3:1. § (3) bekezdése értelmében ugyanis a jogi személy személyéhez fűződő jogaira a személyiségi jogokra vonatkozó szabályokat kell alkalmazni, kivéve, ha a védelem jellegénél fogva csupán az embert illetheti meg. Meg kell azonban jegyeznünk, a Ptk. 3:1. § (3) bekezdése nem véletlenül a jogi személy személyéhez fűződő jogairól, és nem pedig személyiségi jogokról rendelkezik, így utalva arra, hogy személyisége csak az embernek van.

A Ptk. tehát elismeri, hogy az ember személyiségi jogai között vannak olyanok, amelyek a jogi személyekkel szemben is értelmezhetők, amelyek gyakorlása a jogi személyek számára is jelentőséggel bírhat és amelyek megsértése esetén a jogi személy az emberhez hasonlóan a személyiségi jogok megsértésének valamennyi szankciójára is igényt tarthat.⁹ A Legfelsőbb Bíróság például a Pfv.IV.22.623/1999. számú ügy kapcsán hozott ítéletében mondta ki, hogy a jogi személy jóhírneve is megsérthető.¹⁰

Meg kell említenünk, hogy személyiségi jogai természetesen csak létező jogalanyoknak lehetnek, vagyis a személyiségi jogképesség az általános polgári jogi jogképességnek felel meg.¹¹ A természetes személyt a személyiségi jogok tehát élve születése esetén fogamzásától haláláig, a jogi személyt pedig megalakulásától kezdve jogutód nélküli megszűnéséig illetik meg.¹²

⁴ VÉKÁS (2013): 57.

⁵ SÓLYOM (1983): 10.

⁶ PETRIK (2001): 59.

⁷ VÉKÁS (2013): 56.

⁸ Uo., 56.

⁹ Uo., 83–84.

¹⁰ KECSKÉS (2007): 419.

¹¹ LENKOVICS–SZÉKELY (2001): 105.

¹² PETRIK (2001): 4937.

A személyiségi jogi generálklauzula jellegéből adódóan kellően absztrakt ahhoz, hogy nyugodt szívvel állíthassuk, hogy a Ptk. a személyiség minden megnyilvánulását jogi védelem alá helyezi,¹³ és így annak bármilyen sérelme esetén a törvényben szabályozott valamennyi védelmi eszköz igénybe vehető.¹⁴ A jogalkotó tehát a személyiségi jogok összességét, azok valamennyi formáját – a 2:43. §-ban nevesítetteket és nem nevesítetteket egyaránt – védi.¹⁵ Az általános személyiségi jog anyajogi jellegét az Alkotmánybíróság több határozatában is megfogalmazta: az Alkotmánybíróság például a 8/1990. (IV. 23.) AB határozatában kiemelte, hogy az általános személyiségi jogra mind az Alkotmánybíróság, mind a bíróságok hivatkozhatnak az egyén autonómiájának védelmére abban az esetben, ha az adott tényállásra a konkrét, nevesített alapjogok egyike sem alkalmazható.

Fontos megjegyezni, hogy a személyiségi jogok – a tulajdonjoghoz hasonlóan – abszolút szerkezetű jogviszonyt teremtenek a jogosult és mindenki más között, akik alapvetően tartózkodásra, a jogosult személyes sférájának tiszteletben tartására kötelesek.¹⁶ A relatív jogviszony pedig akkor keletkezik, ha és amikor valakinek a személyiségi jogát megsértik. A jogosult tehát ebben a jogviszonyban követelheti a jogsértő magatartás befejezését és a jogsértés jóvátételét, illetve ebben a jogviszonyban lehet olyan körülményekre hivatkozni (pl. közszereplés, a jogosult hozzájárulása), amelyek a jogkövetkezmények alkalmazását kizárják vagy korlátozzák.¹⁷ A Ptk. tehát kimondatlanul állítja fel azt a vélelmet, amelynek értelmében egy személy személyiségi jogainak bármilyen fajta megsértése jogellenes, kivéve, ha a sértő ennek ellenkezőjét bizonyítja, vagyis a jogsértő cselekedeteinek feljogosítottságát (pl. az érintett hozzájárulását) bizonyítja.¹⁸

Korábban már utaltunk rá, de nem árt még egyszer külön is hangsúlyozni, hogy a nevesített személyiségi jogok semmiképpen sem tekinthetők a személyhez fűződő jogok taxációjának, amire a Ptk. 2:43. §-ban a 'különösen' kifejezéssel is utal. A személyiségi jogok számbavehetetlenek, csak a legfontosabbak emelhetők ki közülük, lehetővé téve így, hogy a jövőben újak keletkezzenek, amelyekre a védelem a generálklauzula folytán mindig ki fog terjedni.¹⁹ Érdemes megjegyezni, hogy a Ptk. – a korábbi Ptk.-beli szerkezetet módosítva – a személyiségi jogok példálózó felsorolását követően csak azokat szabályozza érdemben, amelyek esetében normatív szabályt kíván adni.²⁰

Végül, de nem utolsó sorban szólunk kell a személyiségi jogok korlátairól. Mivel azonban a képmáshoz való jog kapcsán erről a kérdésről hamarosan részletesen fogunk beszélni, így most csak röviden, általánosságban ejtünk pár szót a témáról. Korlátnak minősül mindenekelőtt az a szabály, aminek értelmében a személyiségi jog nem haladhatja meg a polgári jog hatókörét, vagyis nem tekinthető totális védelmi eszköznek. Más jogágak is biztosítanak a személyeknek egy bizonyos szintű védelmet, de azt más okból, más célból teszik.

¹³ LENKOVICS–SZÉKELY (2001): 102.

¹⁴ PETRIK (2011): 66.

¹⁵ Uo., 34.

¹⁶ LENKOVICS–SZÉKELY (2001): 102.

¹⁷ PETRIK (2001): 28., 53. és 58.

¹⁸ LENKOVICS–SZÉKELY (2001): 102.

¹⁹ SZIKORA (2024a): 29.

²⁰ VÉKÁS (2013): 57.

További korlátot jelent az egyén önrendelkezési joga, vagyis nem tekinthető jogsértésnek az az egyébként jogi normával ellentétes magatartás, amelyhez az egyén hozzájárult.²¹

A Ptk. 2:44. §-a értelmében a közügyek szabad vitatását biztosító alapjogok gyakorlása érdekében a közéleti szereplő személyiségi jogainak védelme szükséges és arányos mértékben, az emberi méltóság sérelme nélkül korlátozható. A személyiségi jogok korlátját jelenti tehát a – lentebb részletesen tárgyalt – közéleti szereplés, amely az alkotmányos értékek érvényesülése miatt szükséges.

A fentiek mellett az idő is további határt szab a személyiségi jogoknak, mivel azok a személyt csak élete végéig illetik meg.²² Mindezekén túl a jogellenesség is korlátot képez azáltal, hogy a személyiségi jogok csak a jogszabályok keretei között, és csak addig részesülnek védelemben, ameddig más személyek jogát nem sértik. Az azonban, hogy hol húzódik a személyiségi jogi védelem határa, minden ügyben esetenként dönthető el. Emellett természetesen jogos védelem és szükséghelyzet esetén sem beszélhetünk a személyiségi jogok jogellenes megsértéséről.²³

Végezetül pedig ilyen korlátot jelenthet a jogszabály engedélye, amelynek kapcsán a Ptk. szerkesztői úgy vélték, hogy ennél részletesebb szabályozásra nincs is szükség, mivel az alkotmányossági kérdés, hogy a jogszabály mely esetekben korlátozhatja a személyhez fűződő jogokat.²⁴ Éppen ezen megfontolásból került ki például a Ptk.-ból a korábbi Ptk. 80. § (3) bekezdése, amelynek értelmében az eltűnt vagy súlyos bűncselekmény miatt büntetőeljárás alatt álló személyről készült képmás nyomós közérdekből vagy méltánylást érdemlő magánérdekből a hozzájárulása nélkül felhasználható.

5.2. A képmáshoz való jog

Képmáson az ember külső megjelenésének bármilyen tárgyi eszközzel készített olyan rögzítését, közvetítését, ábrázolását, utánpépszerűsét és többszörözését kell érteni, amely alkalmas az egyén testi jellegzetességeinek kifejezésére és így az ábrázolt személy azonosítására, egyediesítésére.²⁵ A képmáshoz való jog védelme tehát valójában az egyén külső megjelenésnek, képének a jogi védelme.²⁶ Mivel azonban az egyén külső megjelenése elválaszthatatlan a személyiségtől, így e védelemnek a polgári jogban a személyiségi jogok keretében történő szabályozása könnyen megérthető.²⁷ Vitathatatlan ugyanis, hogy az emberi test jellegzetességei – így például a bőre, a haja, a szeme, sőt akár az alakja is – az egyénnek olyan elidegeníthetetlen sajátosságai, amelyek megkülönböztetik, kiemelik őt a társadalom többi tagja közül.²⁸ Véleményem szerint az egyén külső megjelenése egyben lelkének, személyiségének

²¹ SZÉKELY (2007): 56.

²² Uo., 57.

²³ LENKOVICS–SZÉKELY (2001): 103.

²⁴ KECSKÉS (2007): 420.

²⁵ TÖRÖ (1979): 512.

²⁶ SZEGHALMI (2014): 54.

²⁷ TATTAY (2004): 3.

²⁸ TÖRÖ (1979): 507., 509.

pillanatnyi tükörképe. Ebből következően tehát egy személyről készült képmás maradóan azonosítja mind az ember egyszeri és megismételhetetlen külső megjelenését,²⁹ mind változó belső személyiségét.

Mindenekelőtt a képmáshoz való jog alanyát érdemes tisztázni. Nem szorul különösebb magyarázatra, hogy a képmással kapcsolatos személyiségi jogok csak az embert illethetik meg,³⁰ így a védelemnek is csak természetes személy lehet az alanya. Ember és ember között azonban nyilvánvalóan nem lehet különbséget tenni. Az EJEB az Egeland és Hanseid kontra Norvégia ügyben mondta ki például, hogy még egy háromszoros gyilkosságért elítélt bűnelkövető is jogosult a magánszférájának védelmére.³¹ A sajtó által közölt kép ugyanis az elítéltet az ítélethirdetés után, letörtén ábrázolta, ahogyan a rendőrautóba beültetik. Az EJEB megállapította, hogy bár a bűncselekmény súlyára és az elítélés körülményeire tekintettel a sajtószabadságot megalapozó közérdek fennállt, és így felvétel az elítélt hozzájárulása nélkül is elkészíthető, illetve felhasználható volt, a konkrét képek azonban a jogosultat olyan élethelyzetben mutatták be, amelyre már kiterjedt a bűnelkövető magánszférájának védelme.³²

5.3. A képmáshoz való jog megsértése

A képmáshoz való jog tartalmát illetően elkerülhetetlen, hogy pár szót szóljunk Törő Károly azon elméletéről, miszerint az ember személyiségi jogi védelmének egyaránt ki kell terjednie az egyén külső megjelenésére, az ezeket tárgyasult formában tükröző képmásra, valamint a képmás és a hangfelvétel egységére, integritására. Véleménye szerint – mivel az emberi kép és hang, illetve a képmás az egyéni személyiség kifejezésének eszköze – a jogi védelemnek is szükségszerűen kétirányúnak kell lennie. Egyrésztől mindenki számára lehetővé kell tenni, hogy személyisége a társadalomban érvényesülhessen, másrésztől pedig biztosítani kell valamennyi egyén számára önkifejezésének kizárólagosságát, egyedüli rendelkezési jogosultságát. Törő Károly ezt úgy fogalmazta meg, hogy „senkit sem lehet kötelezni arra, hogy ezt a jogát mikor és hogyan érvényesítse.”³³ A fentebb leírtak például a képmás esetében azt jelentik, hogy bárki bármikor jogosult magáról képet készíteni vagy készíttetni, ugyanakkor senki nem kötelezhető annak tűrésére, hogy engedélye nélkül róla felvétel készüljön.³⁴

Ahogy arra már korábban utaltunk, a személyiségi jogok szabályozása kapcsán elterjedt a jogirodalomban az a nézet, miszerint a negatív megközelítés helyett helyesebb lenne a személyhez fűződő jogok aktív alanyi jogokként való meghatározása.³⁵ Míg azonban a jogalkotó a személyiségi jogok generálklauzulájának kodifikálása során e követelménynek sikeresen eleget tett, addig a képmáshoz való jogot szabályozó rendelkezés aligha tükrözi ezen álláspontot. A képmás védelmét tehát előnyösebb lenne úgy megfogalmazni, mint a személyek

²⁹ JOBBÁGYI (2009): 86.

³⁰ LENKOVICS–SZÉKELY (2001): 126.

³¹ Egeland és Hanseid kontra Norvégia, App. no. 34438/04 (2009. április 16.).

³² KOLTAY (2025): 137.

³³ TÖRŐ (1979): 515.

³⁴ Uo., 520.; SZEGHALMI (2014): 54.

³⁵ KECSKÉS (2007): 418.

azon alanyi jogát, melynek alapján mindenkinek joga van eldönteni egyrészről, hogy róla vagy hangjáról felvétel készüljön-e, másrészről pedig, hogy az miként kerüljön felhasználásra.³⁶

A képmáshoz való jog alapja tehát nem más, mint az az alanyi jog, amelynek értelmében mindenki a saját életvitelének és erkölcsi érzetének megfelelően maga állapíthatja meg azt a határt, amelyen túl róla jogszerűen felvételt készíteni vagy nyilvánosságra hozni nem lehet.³⁷ (Természetesen e jogosultságnak is megvannak a maga – mind írott, mind íratlan – korlátai.) A védelem célja tehát az egyén döntési autonómiájának biztosítása abban, hogy róla képmás csak akkor készülhessen és az csak olyan nyilvánosság elé kerülhessen, amelyhez ő maga hozzájárult.

Fontos megjegyezni, hogy a jelenleg hatályos Ptk. – a korábbi Ptk. megfogalmazását orvosolva – már nem használja a visszaélés kifejezést. Ez a nem túl szerencsés megfogalmazás ugyanis könnyen azt a látszatot kelthette, hogy csak az sértheti más képmáshoz való jogát, aki felróhatóan nem úgy jár el, ahogy az az adott helyzetben általában elvárható. Ez a feltételezés azonban sem a korábbi, sem a mostani szabályozás esetében sem állhatna távolabb a valóságtól, mivel a tényállás teljes egészében objektív jellegű, és független a jogosulatlan beavatkozó aktuális tudatállapotától. A képmáshoz való jog tehát bármilyen magatartással, így vétlen, fel nem róható cselekedettel is megsérthető.³⁸

A korábbi Ptk. esetén a képmás oltalmával kapcsolatban elterjedt nézet volt, hogy a védelem kétszintű. Az 1959. évi IV. törvény 80. § (1) bekezdése ugyanis általánosságban tiltotta a képmással kapcsolatos bármiféle visszaélést, a 80. § (2) bekezdése pedig a jogsértés egy speciális esetéről, a képmás nyilvánosságra hozataláról rendelkezett.³⁹ Annak ellenére, hogy a jelenleg hatályos Ptk. a korábbi Ptk. személyiségi jogi fejezetének szerkezetét – álláspontom szerint helyesen – megváltoztatta, véleményem szerint továbbra is fennmaradt a képmás védelmének kétszintű szabályozása. Ennek értelmében a Ptk. 2:43. § g) pontja egy általános tilalmat, a képmáshoz való jog megsértésének tilalmát deklarálja. A Ptk. 2:48. § (1) bekezdése pedig a jogsértés két speciális esetét, a felvétel jogosult hozzájárulása nélküli elkészítését, valamint annak hozzájárulás nélküli felhasználását szabályozza. Ebből következően tehát elsődlegesen azt kell vizsgálni, hogy a jogsértés valamely formája megvalósult-e, és ha igen, akkor vajon a felvétel jogellenes elkészítése, illetve felhasználása útján vagy más módon történt-e.

Természetesen az az álláspont is elfogadható, hogy a Ptk. egyszintű szabályozást teremtett azért, hogy a jogsértésnek két esetköréről, a felvétel jogosulatlan elkészítéséről és jogosulatlan felhasználásáról rendelkezik. Ezt a nézetet támasztja alá, hogy a képmás felhasználása olyan tág kifejezés, amely a felvétel elkészítésén kívül valamennyi lehetséges jogsértő cselekményt felölel.⁴⁰

Attól függően, hogy melyik álláspontot fogadjuk el, vagy a képmáshoz való jog megsértését, vagy pedig a felvétel felhasználását kell kiterjesztően értelmeznünk. Eredményét tekintve azonban a két nézet között nincs jelentős eltérés, mivel a jogsértés mindkét esetben

³⁶ SZEGHALMI (2014): 55.

³⁷ JOBBÁGYI (2009): 86.

³⁸ LENKOVICS–SZÉKELY (2001): 125–126.

³⁹ JOBBÁGYI (2009): 86.; TATTAY (2004): 4.

⁴⁰ KOVÁCS Helga (2024): 281–283.

számtalan módon megvalósulhat, így például a felvétel engedély nélküli sokszorosításával, forgalmazásával, kiállításával, az érintett hozzájárulásától eltérő célú felhasználásával⁴¹ vagy torzításával.⁴² Petrik FerencTörő Károly például azt hangsúlyozta, hogy a jogsértés minden olyan esetben megvalósul, amikor a felvétel a jogosult érdekköréből a hozzájárulása nélkül kikerül – függetlenül attól, hogy az bárki számára hozzáférhetővé válik-e.⁴³

Ahogy arra már a képmás definíciója kapcsán utaltunk, a külső megjelenés rögzítése bármilyen tárgyi eszközzel megvalósítható. A védelem szempontjából tehát teljesen közömbös a rögzítés technikai eszköze,⁴⁴ így a képmáshoz való jog védelme alá tartozik például a fénykép, a fénymásolat, a videofelvétel, a mém, a gif, a festmény, a rajz, sőt még a karikatúra is.

5.4. A képmáshoz való jog korlátai

A képmáshoz való jog korlátain olyan körülményeket értünk, amelyek fennállása esetén nem beszélhetünk a képmáshoz való jog jogellenes megsértéséről. Az ember külső megjelenésével kapcsolatos jogosultságokat egyrészt a jog társadalmi rendeltetése és a társadalmi érdekek megfelelő gyakorlásának követelménye, másrészt pedig a közérdeket érvényesítő egyéb jogszabályok rendelkezései korlátozzák. Természetesen a személyiségi jogok lentebb külön nem nevesített, általános korlátai (pl. idő) is kizárják a képmáshoz való jog jogellenes megsértését.

5.4.1. A jogosulti hozzájárulás

A Ptk. 2:48. § (2) bekezdése értelmében a képmás elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges. A Ptk. szövegéből egyértelműen kitűnik, hogy mind a felvétel elkészítéséhez, mind pedig annak felhasználáshoz a jogosult engedélye szükséges. „A hozzájárulásban megnyilvánuló rendelkezési jogosultság tehát önálló, a felvétel készítésétől független jog.”⁴⁵ Ez a gondolat azonban korábban egyáltalán nem volt nyilvánvaló, hiszen az 1959. évi IV. törvény 80. §-a nem rendelkezett a felvétel elkészítéséről, így az ahhoz való hozzájárulást sem tette szükségessé. A szabály eredetileg a bírói gyakorlatban került kidolgozásra, és csak az új Ptk. rögzítette azt.⁴⁶

A Fővárosi Ítéltábla például a 2.Pf. 20.922/2007/5. számú ítéletében állapította meg, hogy a „fényképfelvétel készítéséhez való hozzájárulás nem jelenti egyben a felhasználás engedélyezését is, mivel a felhasználásra vonatkozó rendelkezési jog önálló, független a felvételkedészítés engedélyezésétől.”⁴⁷ Az egyénnek ugyanis jogában áll eldönteni, hogy a róla készített kép milyen körben, milyen módon, hol és milyen összefüggésben jelenjen meg.

⁴¹ KECSKÉS (2007): 440.

⁴² PETRIK (2001): 135.

⁴³ TÖRÖ (1979): 522.

⁴⁴ LENKOVICS-SZÉKELY (2001): 126.

⁴⁵ KECSKÉS (2007): 440.

⁴⁶ VÉKÁS (2013): 68.

⁴⁷ 2.Pf. 20.922/2007/5.

A képmás elkészítéséhez, illetve annak felhasználásához adott hozzájárulás elkülönültségét mondta ki továbbá a Fővárosi Bíróság a 48.Pf. 29.878/2001/3. és a Fővárosi Ítéltábla a 2.Pf. 20.271/2006/4. és a 2.Pf. 21.008/2013/6. számú ítéleteiben is.

Főszabály szerint tehát a jogszerűen elkészített felvételt jogszerűtlenül is fel lehet használni, ha például a felvétel készítője az érintett hozzájárulása nélkül kívánja a felvételt nyilvánosságra hozni.⁴⁸ Ezen elvi tétel mögött pedig az a gondolat húzódik meg, hogy a saját személyiségi értékei felett mindenki saját maga rendelkezik,⁴⁹ és ezért a védelemnek a felvétel felhasználásának lehetőségét megteremtő cselekményre is ki kell terjednie. Az, akiről jogosulatlanul, akár tudta nélkül felvételt készítenek, nyilvánvalóan a jövőben sem lesz abban a helyzetben, hogy annak felhasználását ellenőrizni tudja.

Törő Károly a fentebb leírtakat kiegészítve megállapítja, hogy létezhetnek olyan kivételes esetek, amikor a felvétel elkészítéséhez adott hozzájárulás különösen a társadalmi szokásokra, a készítő és az ábrázolt személy kapcsolatára, valamint a felvételek készítés céljára tekintettel magában foglalja a felhasználáshoz való jogot is.⁵⁰ Így például, ha valaki nem tiltakozik az ellen, hogy baráti társaságában róla fénykép készüljön, nyilván a felvételnek szűk baráti, családi körben való felhasználását sem sérelmezi.⁵¹ Törő Károssal szemben úgy gondolom, ezekben az esetekben nem arról van szó, hogy a képmás elkészítéséhez adott hozzájárulás miatt szükségtelenné válik a felvétel felhasználásához való engedély, hanem a kép elkészítéséhez adott hozzájárulással mint ráutaló magatartással engedélyezem annak bizonyos körben való felhasználását is. A képmás szélesebb körben való terjesztésével azonban a felhasználás köre meghaladja józan ész által kialakított határokat, és így az ábrázolt személy újból igényt tarthat a jogi védelemre.⁵² Így például a családi körben jogszerűen készített felvételnek a televízióban történő felhasználására a kép készítője már nem jogosult.⁵³

Felmerülhet azonban a kérdés, hogy vajon milyen formában adhatja meg az érintett a hozzájárulását. Erre egyértelmű választ nehéz adni, mivel mind a szakirodalomban, mind pedig a joggyakorlatban két egymást kizáró vélemény alakult ki. Az egyik álláspont értelmében a hozzájárulásnak kifejezettnek és egyértelműnek kell lennie, míg mások úgy gondolják, hogy a hozzájárulás ráutaló magatartással is megadható. Kecskés László,⁵⁴ Koltay András,⁵⁵ vagy Petrik Ferenc⁵⁶ szerint – elsősorban a joggyakorlatra alapozva – a személyiségi jog megsértését kizáró hozzájárulásnak kifejezettnek kell lennie, és azt nem lehet kiterjesztően értelmezni. Ezzel szemben Lenkovics Barnabás és Székely László,⁵⁷ Vékás Lajos,⁵⁸ vagy Jobbágyi Gábor⁵⁹ álláspontja szerint a hozzájárulás történhet írásban, szóban vagy ráutaló magatartással is. Ellenkező esetben ugyanis a mindennapi élet ellehetetlenülne, hiszen

⁴⁸ LENKOVICS–SZÉKELY (2001): 127.

⁴⁹ PETRIK (2001): 28.

⁵⁰ TÖRŐ (1979): 522–523.

⁵¹ LENKOVICS–SZÉKELY (2001): 127.

⁵² TÖRŐ (1979): 523–524.

⁵³ PETRIK (2001): 136.

⁵⁴ KECSKÉS (2007): 440.

⁵⁵ KOLTAY (2009): 395.

⁵⁶ PETRIK (2001): 136.

⁵⁷ LENKOVICS–SZÉKELY (2001): 127.

⁵⁸ VÉKÁS (2013): 68.

⁵⁹ JOBBÁGYI (2009): 87.

a hétköznapiakban a tiltakozás, az elhárítás hiánya ráutaló magatartással adott hozzájárulásként értékelhető.⁶⁰ Petrik Ferenc szerint a hallgatással megvalósuló hozzájárulás azonban csak akkor fogadható el, ha az ábrázolt személy tudott róla, hogy fényképezik.⁶¹ Így például, ha valaki olyan eseményen vesz részt, ahol felvétel készül, megjelenésével, mint ráutaló magatartással megadja a kép elkészítéséhez, illetve a körülményekből adódóan akár a felhasználáshoz is a hozzájárulását.

Úgy vélem, a hallgatolagos hozzájárulás akkor is megállapítható, ha az érintett nem tudta, hogy róla felvétel készül, de arra alapos okkal számíthatott volna. Ilyenkor nyilvánvalóan mérlegelni kell az eset valamennyi körülményét, így például az ábrázolás módját, körülményeit. Példának okáért, ha a valaki a wimbledoni tenisztornán Venus Williams mellett foglal helyet, akkor – annak ellenére, hogy ő nem közszereplő –, nem kifogásolhatja, hogy róla fénykép készül, és azt újságban közzé is teszik.

A bírói joggyakorlatban e kérdés megítélése a következőképp alakult: a Legfelsőbb Bíróság a Pfv. IV. 22.415/1999. számú ítéletében kimondta, hogy a személyhez fűződő jogok megsértését kizáró hozzájárulásnak kifejezettnek kell lennie, azt a jogosult terhére nem lehet kiterjesztően értelmezni. A Fővárosi Ítéltábla a 2.Pf. 20.271/2006. számú ügyben hozott ítéletében szintén leszögezte, hogy mind a felvétel elkészítéséhez, mind pedig annak felhasználásához az ábrázolt személy kifejezett és határozott hozzájárulása szükséges, mivel a Ptk. 6:8. § (3) bekezdése [akkor az 1959. évi IV. törvény 207. § (4) bekezdése] alapján a jogról lemondó jognyilatkozatot nem lehet kiterjesztően értelmezni. A hozzájárulás kifejezett jellegének és célhoz kötöttségének követelményét a Fővárosi Ítéltábla ismételten hangsúlyozta a 2.Pf. 21.008/2013. számú ügyben hozott ítéletében, amelynek indokolásában kimondta, hogy a képmás felhasználására kizárólag akkor kerülhet sor, ha a jogosult ehhez határozott, pontosan megjelölt célra szóló hozzájárulását adja. Az ítélet jelentősége továbbá abban rejlik, hogy a Fővárosi Ítéltábla ezen döntésében külön hangsúlyozta a felhasználás céljának jelentőségét, amely ismeretének hiányában a jogosult nem tud megfelelően dönteni, és így a felhasználás jogszerűségéhez sem tud hozzájárulni. Másrészt a Fővárosi Ítéltábla például a 2.Pf. 20.271/2006/4. számú ítéletében egyértelműen kimondta, hogy a képmás készítéséhez való hozzájárulás ráutaló magatartással is megadható. Ilyen ráutaló magatartásnak minősül, ha az érintett személy tudja, hogy abban a helyiségben, ahová belép felvétel készül vagy felvétel készülhet. Az Ítéltábla az alperes ellenkérelmében foglaltakat megerősítve kiemelte, hogy a hozzájárulás kifejezése nincs alakszerűséghez kötve, így az szóban, írásban vagy akár ráutaló magatartással is megadható.

Álláspontom szerint a hozzájárulás ráutaló magatartással is megadható. Az az ember, aki belemosolyog a kamerába, nyilvánvalóan érzékeli, hogy róla képet készítenek, és az ellen nyilvánvalóan semmilyen ellenvetése nem volt, annak ellenére, hogy ezt kifejezetten nem mondta ki. Természetesen mindkét nézettel könnyen lehet azonosulni, de az biztos, hogy égető szükség lenne a jövőben egy jogegységi határozatra az egységes ítélkezési gyakorlat biztosítása érdekében.

Végül, de nem utolsó sorban szólunk kell a megadott hozzájárulás visszavonásának kérdéséről, amely kapcsán szintén nem alakult ki még egységes álláspont. Egyesek a jogosult akaratát tartják kizárólagosnak, és így korlátozás nélkül elismerik a hozzájárulás egyoldalú

⁶⁰ LENKOVICS–SZÉKELY (2001): 127.

⁶¹ PETRIK (2001): 140.

visszavonását mindaddig, míg az engedélyezett cselekvést el nem végezték. Mások szerint azonban a hozzájárulás csak fontos okból, így például az érintett személy megtevesztése miatt vonható vissza. Képmás közzétételéhez adott hozzájárulás például akkor vonható vissza, ha kiderül, hogy a feljogosított nem az előre közölt célra kívánja a felvételt felhasználni. Ezen álláspont képviselői tehát inkább arra helyezik a hangsúlyt, hogy az érintett hozzájárulása a másik fél számára egyfajta jogosultságot keletkeztet.⁶²

5.4.2. Tömegfelvétel

Mivel a képmáshoz való jog védelme során is érvényesül a társadalmi rendeltetésnek megfelelő joggyakorlás általános követelménye, így kizárt az ábrázolt személy rendelkezési joga a tömegfelvételek esetén.⁶³ A Ptk. 2:48. § (2) bekezdése értelmében nincs szükség a jogosult hozzájárulására a felvétel elkészítéséhez vagy annak felhasználásához tömegfelvétel esetén. A törvény azonban már nem határozza meg a tömegfelvétel fogalmát, így azt a korábbi Ptk. kapcsán kialakult bírói joggyakorlat tölti meg tartalommal.

A BH 1985.17 számon közétett ítéletben a Legfelsőbb Bíróság kimondta, hogy az olyan nyilvános eseményről, rendezvényről, táj- és utcarészletről készült felvétel minősül tömegfelvételnek, amely összhatásában örökíti meg a nyilvánosság előtt lezajlott eseményeket, vagyis az ábrázolás módja nem egyéni. Abban az esetben azonban, ha megállapítható a felvétel egyedisége, egyéni képmás jellege, a kép nyilvánosságra hozatalához a jogosult hozzájárulása szükséges. A nyilvános helyen (pl. utcán, kiállításon, sporteseményen) megjelenő személy tehát nem sérelmezheti alaposan azt, hogy tudósításban (riportfilmben vagy tévéhíradóban) a közönség körében az ő képmását is felveszik és vetítik.⁶⁴ Hasonlóan foglalt állást a Fővárosi Törvényszék a P. 22.699/2016/4. számú ítéletében, amelyben megállapította, hogy az érintett hozzájárulása szükséges egy olyan tömegfelvétel nyilvánosságra hozatalához, amelyen az egyén egyedileg került ábrázolásra.⁶⁵ Ezen bírói ítélkezési gyakorlat alkotmányosságát egyébként az Alkotmánybíróság is megerősítette a 28/2014. (IX. 29.) AB határozatában, amely szerint a sajtószabadság biztosítása érdekében a képmás engedély nélküli nyilvánosságra hozatalának tilalma nem vonatkozhat az olyan nyilvános eseményekről, rendezvényekről, táj- és utcarészletekről készült felvételekre, amelyek esetén a felvétel összhatásában örökíti meg a nyilvánosság előtt lezajlott eseményeket, és így az az ábrázolás módja nem egyéni.⁶⁶

A tömegfelvételt tehát úgy fogalmazhatjuk meg, mint egy olyan képmás, amely valamely „rendezvényen résztvevő tömeget ábrázol, és a képen az egyes résztvevők azonosíthatósága csak véletlenszerű, a kép nem az egyes konkrét személyek megörökítése céljából készült.”⁶⁷

A fentebb leírtak alapján tehát megállapíthatjuk, hogy a tömegfelvételen résztvevők azért nem részesülhetnek védelemben, mert a felvétel nem egy személy kifejezését, megkü-

⁶² PETRIK (2001)

⁶³ TÖRÖ (1979): 546.

⁶⁴ BH 1985.17.

⁶⁵ P. 22.699/2016/4.

⁶⁶ 28/2014. (IX. 29.) AB határozat, 48.

⁶⁷ KOLTAY (2009): 396.

lönböztetését, hanem egy eseményen megjelenő tömeg ábrázolását szolgálja. A képmás ugyanis akkor tekinthető tömegfelvételnak, ha „az egyének fel nem ismerhetők vagy felismerésük véletlen”.⁶⁸ Nyilván a ‘tömeg’ kifejezés pontosan nem számszerűsíthető, de alapvetően leszögezhető, hogy ha a képen ábrázolt személyeket nem külön-külön, hanem egy sokaság egy-egy elemeként látjuk, akkor tömegfelvételtől beszélhetünk.⁶⁹ Nem jogsértő tehát például egy utcai eseményt a háttérből figyelő járókelőről készült fénykép. Meg kell azonban jegyeznünk, hogy a tömegfelvétel csak célja által indokoltan, így elsősorban tájékoztatás céljából használható fel.⁷⁰ Abban az esetben azonban, ha az ábrázolás módja egyéni, vagyis meghaladja a tömegfelvétel kereteit, a rögzített személy jogosult a személyiségi jogi védelemre.⁷¹ Ugyanez igaz akkor is, ha az egyént kiemelik a tömegből és így a képmást újra individualizálják.⁷²

Az egyéni ábrázolás kapcsán két fontosabb gondolatot kell megemlítenünk. Egyrészt, hogy az egyéni ábrázolást nem csak akkor lehet megállapítani, ha valaki egymaga szerepel a felvételen. Több személy együttes ábrázolása is egyéni jellegű, ha a tömegszerűség hiányzik, azaz a felvétel mindegyik szereplőt egyedileg mutatja be.⁷³ Véleményem szerint azonban az is jogsértő, ha a felvétel több szereplő közül legalább egyet egyedileg ábrázol. Másrészt a tömegfelvétel nem egyenlő a tömegek által látogatott helyszínen készült felvétellel. Senki sem köteles ugyanis tűrni, hogy róla engedélye nélkül felvételt készítsenek, pusztán azért, mert tömegesen látogatott helyen jelent meg. Így például a strandon feltűnő bikiniben megjelenő hölgyről hozzájárulása nélkül nem lehet felvételt készíteni.⁷⁴

Említést kell tennünk Petrik Ferenc azon elméletéről, miszerint tömegfelvételnak minősül az olyan eseményről (pl. sportesemény) készült felvétel, ahol a résztvevőnek számolnia kell azzal, hogy róla képmás készülhet.⁷⁵ Véleményem szerint azonban az ilyen eseményekről készült képek nem feltétlenül tömegfelvételek, hiszen sok esetben azokról éppen a tömegszerű hatás hiányzik, és egy-egy személyt ragadnak ki a sokaságból. Ez azonban nem jelenti azt, hogy az ilyen eseményen készült felvételek jogsértők lennének, mivel valamennyi ábrázolt személy ráutaló magatartással, az eseményen való részvétellel hozzájárul a képmások elkészítéséhez (lásd: 2.Pf. 20.271/2006. számú ügy).

5.4.3. Közszerelő

A Ptk. 2:48. § (2) bekezdése értelmében nincs szükség az érintett hozzájárulására a felvétel elkészítéséhez és annak felhasználásához nyilvános közéleti szereplésről készült felvétel esetén. A törvényszövegből tehát egyértelműen kitűnik, hogy sem a képmás elkészítéséhez, sem pedig annak felhasználáshoz nincs szükség a közszerelő engedélyére.⁷⁶ A közszerelő tehát,

⁶⁸ KOLOSVÁRY Bálint: *Az arckép és a jog*. Szeged. 1927. Idézi TÖRÖ (1979): 546.

⁶⁹ NAGY Csilla (2021)

⁷⁰ PETRIK (2001): 140.

⁷¹ TÖRÖ (1979): 547.

⁷² LENKOVICS-SZÉKELY (2001): 127.

⁷³ TÖRÖ (1979). 547.

⁷⁴ Uo., 547.

⁷⁵ PETRIK (2001): 140.

⁷⁶ LENKOVICS-SZÉKELY (2001): 127.

mivel önként vállalva kilép a magánélet köréből, köteles tűrni, hogy képmását az újságok, a televízió és más elektronikus hírközlési eszközök közvételegyék. Természetesen a Ptk. ezen rendelkezése a Ptk. 2:44. §-ban deklarált, a közéleti szereplők csökkentett személyiségvédelmét megállapító generálklauzulával együtt értelmezendő.⁷⁷ Ennek értelmében tehát a közéleti szereplő képmáshoz való joga a közügyek szabad vitatását biztosító alapjogok gyakorlását szükségtelenül nem korlátozhatja, egyensúlyt teremtve így a sajtószabadság és a nevesített személyiségi jog között.⁷⁸

Mivel sem a korábbi, sem a hatályos Ptk. nem határozza meg sem a közszereplő, sem pedig a nyilvános közszereplés fogalmát, bírói körökben eltérő gyakorlat alakult a tekintetben, hogy vajon a Ptk. 2:48. § (2) bekezdésének hatálya alá pontosan kik tartoznak. Az egységes jogalkalmazás biztosítása érdekében a Kúria héttagú jogegységi tanácsa az 1/2012. számú BKMPJE határozatában a közszereplés *sui generis* fogalmát alkotta meg, amelynek értelmében a nyilvános közszereplés az egyén önkéntes elhatározásán, autonóm döntésén alapuló olyan politikai, társadalmi, művészeti tevékenység, megnyilvánulás, amelyet egy meghatározott cél, szűkebb vagy tágabb értelemben a helyi közösség vagy a társadalom életének befolyásolása érdekében fejt ki. A Kúria gondolkodásában tehát a közszereplés a közterületen zajló eseményeken való részvételnél szűkebb kategória, mivel az előbbi a közszereplő szándékát is feltételezi. Így a nyilvános helyen szolgálati kötelezettségét teljesítő vagy munkát végző személy – pl. rendőr, büntetés-végrehajtási-intézet alkalmazottja – e tevékenysége során közéleti szerepléshez szükséges szándék hiányában nem minősül közszereplőnek, és így a Ptk. 2:48. § (2) bekezdése értelmében a felvétel elkészítéséhez és annak felhasználásához a hozzájárulása szükséges.⁷⁹

Meg kell azonban jegyeznünk, hogy a bírói gyakorlat értelmében a nyilvános közszereplés megállapításához nem szükséges országos szintű megjelenés, és nem csak a köz érdekében eljáró, hanem a közszereplés szándékával, a nyilvánosság előtt való szereplés célzatával fellépő személy is közszereplőnek minősül.⁸⁰

A közelmúltban a közszereplő fogalmán közvetve az Alkotmánybíróság is alakított, azáltal, hogy a rendőrök képmásának jogszerűsége kapcsán a Kúriával eltérő álláspontra helyezkedett. Az Alkotmánybíróság ugyanis a 28/2014. (IX. 29.) AB határozatban megállapította, hogy a közterületen intézkedő rendőrökről készült képfelvétel hozzájárulásuk nélkül is nyilvánosságra hozható, ha a nyilvánosságra hozatal tájékoztatásnak, a közügyeket érintő képi tudósításnak minősül.⁸¹ Az Alkotmánybíróság a határozatában nem az eljárás alapjául szolgáló ügyben felmerült polgári jogi kérdést, hanem azt vizsgálta, hogy a sajtószabadság rendőrök arcának kitakarásával megvalósuló korlátozása szükséges és arányos-e az emberi méltóság védelme érdekében, vagyis hogy a megtámadott jogerős bírói ítélet egyensúlyt teremtett-e a szabad tájékoztatás és az emberi méltóságra visszavezethető képmásvédelem között.⁸² Az Alkotmánybíróság határozatában mindenekelőtt leszögezte, hogy a sajtószabadság kettős: szubjektív alanyi jogi jellege mellett a demokratikus közvélemény megteremtését és

⁷⁷ SZÉKELY (2011): 177. Lásd még: 7/2014. (III. 7.) AB határozat.

⁷⁸ KOLTAY (2009): 396.

⁷⁹ TÓTH J. (2017): 116–118.

⁸⁰ BORONKAY (2013)

⁸¹ 28/2014. (IX. 29.) AB határozat, 43.

⁸² 28/2014. (IX. 29.) AB határozat, 27. és 35.

fenntartását szolgálja. A saját képmáshoz való jog kapcsán az Alkotmánybíróság megállapította, hogy az a polgári jog része, amely Európában az önrendelkezési jogból és az emberi méltóságból vezethető le. A személyiségi jogok eme kifejeződésének célja pedig, hogy valamenyny ember számára biztosítsa a döntési jogosultságot, hogy róla milyen képet és milyen összefüggésben hozzanak nyilvánosságra.⁸³ E két alapjog jelentőségének egymáshoz való aránya kapcsán az Alkotmánybíróság leszögezte, hogy a közhatalmat gyakorló személyek esetében a személyiségvédelem korlátozottsága mindenki máshoz képest szélesebb körben minősül indokoltnak a szólás- és sajtószabadság érdekében.⁸⁴ Következésképp a személyiségi jogok sérelmére való hivatkozás nem alapozza meg a sajtószabadság gyakorlásának a korlátozását, feltéve, hogy a tájékoztatás nem visszaélészerű.⁸⁵

Érdekességgé kell megemlítenünk, hogy mind az elméletben (pl. Jobbágyi Gábor szerint⁸⁶), mind pedig a gyakorlatban létezik olyan felfogás, miszerint a tömegfelvételek szereplői nyilvános közszereplőnek minősülnek. Koltay András szerint például a nyilvános események aktív résztvevői (pl. a felszólaló) egyértelműen közszereplők, míg a rendezvényen részt vevő passzív hallgatók nem minősülnek annak, bizonyos esetekben (pl. tömegfelvétel alanyaként) azonban még az ő képmásuk is jogszerűen nyilvánosságra hozható.⁸⁷ Én Petrik Ferencsel értek egyet abban, hogy a nyilvánosság előtt zajló események résztvevői nem közszereplők, mert nem céljuk a társadalmi viszonyok befolyásolása. Egy sporteseményen készült felvétel jogszerűen felhasználható akár a szurkoló hozzájárulása nélkül, ha ő egy tömegfelvétel alanya, vagy pedig – ahogy azt már korábban kifejtettem – hozzájárulásával, amelyet ráutaló magatartással – a belépőjegy megvásárlásával – adott meg.

Hasonlóan foglalt állást az EJEB a Peck kontra Egyesült Királyság-ügy kapcsán hozott ítéletében is.⁸⁸ Az EJEB ugyanis kimondta, hogy nem válik valaki közszereplővé pusztán azért, mert közterületen tartózkodik. Az ügy tényállása értelmében Mr. Peck az utcán öngyilkossági kísérletét követően zavarodottan, késsel a kezében sétált, amelyet az ott elhelyezett térfigyelő kamera oly módon rögzített, hogy Mr. Peck felismerhetővé vált. Az önkormányzat a kamerarendszer kiépítésének alátámasztása érdekében Mr. Peck akarata ellenére nyilvánosságra hozta a felvételeket. Az EJEB végül Mr. Peck magánélethez fűződő jogának megsértését állapította meg arra hivatkozva, hogy a kérelmező képmásának nyilvánosságra hozatalával a privát szférája olyan mértékben sérült, amely túlmegy az adott helyzetben szokásosan elvárható korlátozásnál.⁸⁹

Fontos megjegyezni, hogy a közéletben részt vevő személynek nem lehet minden megnyilvánulását közszereplésnek tekinteni, és így a nyilvános szereplés körén kívül a közszereplőnek is joga van a magánéletre.⁹⁰ Nem alkalmazható tehát a Ptk. 2:48. § (2) bekezdése akkor, amikor a közszereplő szabadidejét tölti, magánemberként szórakozik (pl. üzletben vásárol).⁹¹

⁸³ Uo., 22–23.

⁸⁴ SZILÁGYI (2018): 12.

⁸⁵ 28/2014. (IX. 29.) AB határozat, 36. és 42.

⁸⁶ JOBBÁGYI (2009): 87.

⁸⁷ KOLTAY (2009): 396–397.

⁸⁸ Peck kontra Egyesült Királyság, App. no. 44647/98 (2003. január 28.)

⁸⁹ KOLTAY (2009): 407–408.

⁹⁰ TÖRÖ (1979): 549.

⁹¹ PETRIK (2001): 138.; LENKOVICS–SZÉKELY (2001): 128.

A Legfelsőbb Bíróság a Pfv. IV. 21.553/2004. számú ügyben azt állapította meg, hogy a közszereplő képmása csak közszerepléseivel összefüggésben, a közéleti megnyilvánulásai által meghatározott keretben, annak bemutatására használható fel az érintett hozzájárulása nélkül. A közszereplő képmása tehát nem szabad felhasználás tárgya, nem szolgálhat különböző, a közszereplő konkrét megnyilvánulásaitól független gondolati tartalmak, vélemények illusztrálására. A Legfelsőbb Bíróság elvi élel szögezte le, hogy az érintett hozzájárulása nélkül a róla készült fénykép más célból történő felhasználására a sajtó nem lehet jogosult pusztán azon az alapon, hogy a felperes korábban közszereplőként lépett a nyilvánosság elé.

Korábban már említettük, hogy a Ptk. 2:44. §-át és a 2:48. § (2) bekezdését együtt kell alkalmazni. Ennek alapján azonban jogosan feltételezhető, hogy a Ptk. a korábbi bírói gyakorlattal szembemelve lehetővé teszi a közéleti szereplők magánéletének olyan szegmenseiről való felvétel készítését, amelyek ugyan nem minősülnek nyilvános közéleti szereplésnek, de az érintett közszereplő megítélését lényegesen befolyásolják, és így a demokratikus közvélemény kialakításához is hozzájárulnak.⁹² Végezetül pedig le kell szögeznünk, hogy a közszereplőről képmás készítése vagy annak felhasználása akkor is jogsértő lehet, ha az más személyiségi jogot, például emberi méltóságot vagy személyes titkot sért.⁹³

⁹² BORONKAY (2013)

⁹³ PETRIK (2001): 139.

6. A képmáshoz való jog érvényesülése az online térben

Az előző fejezetben a képmáshoz való jognak ‘rendes’ körülmények között való érvényesülését, megsértését és korlátait vizsgáltuk részletesen. A képmás védelmét biztosító komplex szabályozás ismertetését követően azonban meg kell vizsgálnunk, hogy vajon ezen szabályok miként jutnak érvényre, vagy egyáltalán érvényre jutnak-e az interneten. Ezen kérdések megválaszolása érdekében jelen fejezet (i) a képmáshoz felhasználásához adott hozzájárulás közösségimédia-oldalakon való érvényesülését, valamint (ii) a deepfake képmáshoz való jog szempontjából való elemzését vizsgálja.

6.1. Az egyén hozzájárulásának érvényesülése a közösségimédia-oldalakon

Egy magánszemély képmásának nyilvánosságra hozatalához szükséges hozzájárulás közösségimédia-oldalakon való érvényesülését érdemes eseti példákon keresztül bemutatni. Bár az egyes közösségimédia-oldalak által nyújtott funkciók bizonyos mértékben eltérnek egymásól, azok alapjaiban ugyanazokon a működési alapelveken nyugszanak. Mindezek alapján a képmáshoz való jog érvényesülését először a Facebookon, a közösségimédia-oldalak egyik legkiemelkedőbb példáján keresztül fogom vizsgálni. A mai napig ugyanis a Facebook rendelkezik a legtöbb (kicsit több mint 3 milliárd) felhasználóval,¹ akik percenként (!) 136 000 képet publikálnak.² Ezt követően a képmás megosztásához szükséges hozzájárulás kérdését más közösségimédia-platformokon (YouTube, TikTok és Instagram) is vizsgálom, annak igazolása érdekében, hogy a képmáshoz való jog tömeges megsértése nem kizárólag a Facebookra, hanem a közösségi média egészére jellemző probléma.

¹ Stacy Jo DIXON: Most popular social networks worldwide as of February 2025, by number of monthly active users. Statista.com, 2025. március 26., <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users>

² Szélesebbre nyitva a képet: napi szinten 14 milliárd kép kerül megosztásra a különböző közösségimédia-oldalakon keresztül. Matic BROZ: Photo statistics: How many photos are taken every day? *Photutorial*, 2025. május 21. <https://photutorial.com/photos-statistics>

6.1.1. A tagelés jogi megítélése a képmáshoz való jog szempontjából

A felhasználó az általa feltöltött tartalom – legyen szó szövegről, fényképről vagy videofelvételről – egy másik Facebook-felhasználót megjelölhet (angolul: *to tag*), ezáltal egy olyan hivatkozást (hiperlinket) létrehozva, amely közvetlenül az érintett felhasználó profiljához vezet. Bár a közösségi média jellegéből adódóan a felhasználók a feltöltött képeken az esetek többségében megjelölik az ismerőseiket, ez egyáltalán nem törvényszerű hiszen a kép megosztójának nem kötelessége a kép alanyait megneveznie. A tagelésnek³ tehát kulcsfontosságú szerepe van a képmáshoz való jog közösségi oldalakon való érvényesülésében. Enélkül ugyanis az ábrázolt személynek esélye sem lenne tudomást szerezni arról, hogy róla olyan képet raktak fel a világhálóra, amelyet akár a világ összes internetkapcsolattal rendelkező embere megtekinthet, ellehetlenítve így az őt megillető jogi védelem érvényesítésének lehetőségét.

A tagelés eredményeként, a feltöltött fénykép a tagelt felhasználó profiloldalán is megjelenik.⁴ Ezen felvételt a tagelt felhasználó profiloldalán a beállításaitól függően (i) bárki; (ii) a tagelt személy valamennyi Facebook-ismerőse; (iii) a tagelt személy valamennyi Facebook-ismerősének ismerőse; (iv) a tagelt személy által pontosan meghatározott Facebook-ismerősök köre; vagy (v) kizárólag a tagelt személy láthatja.⁵ Az azonban, hogy a megosztott kép más a tagelt személy profiloldalán kinek érhető el, nem azonos azzal, hogy ki láthatja az érintett tartalmat a Facebookon. A megosztott fotó célközönsége elsődlegesen ugyanis a bejegyzés létrehozójának beállításaitól függ. A tagelt személy ezen 'alapcélközönséget' kizárólag bővíteni tudja.⁶ Így, ha a fényképet megosztó felhasználó beállításai szerint a fénykép publikus (vagyis azt bárki megtekintheti), a tagelt személynek nem áll módjában a nyilvánosság körét csökkenteni. A tagelt személy autonómiája csupán arra terjed ki, hogy a kérdéses fénykép az ő saját profiloldalán milyen személyi kör számára lehet elérhető. Ráadásul a tagelt személynek még ezen autonómiája sem korlátlan: a tartalmat megosztó ugyanis jogosult a feltöltött kép célközönségét kizárólag a saját ismerőseire és a tagelt személyre korlátozni, esetlegesen felülírva így a tagelt személynek a tartalom saját profilján keresztül való elérhetőségére vonatkozó döntését.

Mindebből azonban az is következik, hogy a Facebook a képmás felhasználására (megosztására) vonatkozó döntési jogosultságot elsődlegesen a megosztó kezébe helyezi. Ezen megközelítés azonban szöges ellentétben áll a képmáshoz való jog esszenciájával. Amint korábban részletesen kifejtettem, a képmáshoz való jog az egyént megillető alanyi jog, amely alapján az érintett jogosult meghatározni, hogy a róla készült felvétel milyen módon kerüljön felhasználásra.⁷ A képmáshoz való jog kétirányú védelme értelmében senki nem kötelezhető annak tűrésére, hogy a róla készült felvételt az általa kívánttól eltérő nyilván-

³ A legelterjedtebb magyarázást, a tagelés kifejezést használom. Ugyanakkor Veszelszki Ágnes álláspontja szerint a tagelés kifejezés is elfogadható lenne. VESZELSZKI (2012): 325.

⁴ Facebook Súgóközpont: Mi az a megjelölés a Facebookon, és hogyan működik? <https://www.facebook.com/help/124970597582337>

⁵ Facebook Súgóközpont: A Facebook-oldalak megjelöléseinek kezelése, https://www.facebook.com/help/186837828030552/?helpref=related_articles

⁶ Facebook Súgóközpont: Hogyan állíthatod be, ki láthatja a Facebook-bejegyzéseket, amelyekben meg vagy jelezve? <https://www.facebook.com/help/454185581308206/>

⁷ LENKOVICS–SZÉKELY (2001): 126.

nosság előtt tárják fel.⁸ Ezzel szemben a Facebookon a megosztó jogosult a képen szereplő, tagelt személy által meghatározottnál mind kisebb, mind pedig nagyobb célközönséget beállítani.

Érdekes kérdést vet fel továbbá a tagelés jogi megítélése a képmáshoz való jog szemszögéből. Vajon tekinthető-e a tagelés az érintett személy hozzájárulása iránti kérelemnek, vagy egyszerűen csak egy informális tájékoztatás arról, hogy róla képet hoztak nyilvánosságra? Mivel a tagelésre a felvétel megosztása után kerül sor, véleményem szerint a tagelés semmiképpen sem értékelhető engedélykéresként, hiszen a hozzájárulásnak előzetesnek, és nem utólagosnak szükséges lennie.

Ugyanakkor ki kell emelni, hogy egyes felhasználói adatvédelmi beállítások mellett a tagelés nem vezet automatikusan a tagelt személy profiloldalára mutató hiperlink létrejöttéhez. Ilyen esetekben az érintett egy értesítést kap a Facebookon, amelyen keresztül jóváhagyhatja vagy elutasíthatja a megjelölést. Amennyiben a tagelt személy a jóváhagyást megtagadja, a Facebook nem hoz létre kapcsolatot a fénykép és az érintett profilja között. Fontos ugyanakkor hangsúlyozni, hogy a kép ebben az esetben is elérhető marad a platformon, a feltöltő által meghatározott célközönség számára. Ezért a tagelés ezen esetekben sem tekinthető az érintett személy hozzájárulására irányuló kérelemnek, mivel annak elutasítása nem jár az érintett felvétel törlésével.

6.1.2. A képmáshoz való jog megsértésének tipikus online esetei

A tagelés jogi elemzése már önmagában bizonyítéka annak, hogy a Facebook megközelítése az egyén képmáshoz való jogához alapjaiban téves, mivel az nem tükrözi a személyiségi jog alanyi jogi jellegét. A képmáshoz való jog azonban nem csak a tagelésre vonatkozó szabályok hibás mivolta következtében, hanem számos egyéb módon is sérülhet (és álláspontom szerint sérül is) a Facebookon keresztül. Mivel azonban lehetetlen az összes elképzelhető jogsértő esetet ismertetni, így a probléma szemléltetése érdekében jelen alfejezet azok közül csak a fontosabbakra tér ki.

Tételezzük fel, hogy egy közszereplőnek nem minősülő magánszemély (a továbbiakban: A) magáról és szintén nem közszereplő barátnőjéről (a továbbiakban: B) készült fényképet oszt meg a Facebookon. Ebben az esetben nyilvánvalóan az érintett személy hozzájárulása vizsgálendő annak megállapítása érdekében, hogy mikor beszélhetünk a képmáshoz való jog megsértéséről.

Főszabály szerint, ha B megadja a hozzájárulását a kép megosztásához (azaz a felvétel nyilvánosságra hozatalához), B képmáshoz való joga nem sérül. Jogellenesen jár el azonban A, ha a képet B hozzájárulásánál szélesebb körben terjeszti. Így például, ha B megengedi, hogy a képmását A úgy töltsse fel, hogy azt valamennyi ismerőse láthatja, de A beállításai alapján az mindenki által megtekinthető, B újból igényt tarthat a jogi védelemre. Abban az esetben, ha A nem kérte előzetesen B hozzájárulását, és beállítása alapján a közös képüket mindenki láthatja, B képmáshoz való joga sérül, hiszen képmását engedélye nélkül hozták nyilvánosságra.

⁸ Uo., 126.; TÖRÖ (1979): 520.

B képmáshoz való joga továbbá akkor is sérül, ha a képet engedélye nélkül töltötte fel A, de azt csak az utóbbi ismerősei láthatják. Ennek a helyzetnek a jogi minősítése azonban már vita tárgyát képezheti, hiszen felmerülhet annak a lehetősége, hogy a kép elkészítéséhez adott hozzájárulás magában foglalja azt a jogot, hogy a felvételt A ismerősei is láthassák. Véleményem szerint azonban ez az érvelés jelen esetben nem fogadható el. Egy felhasználónak ugyanis átlagosan 338 ismerőse van a Facebookon, aminek következtében a felhasználás köre jóval meghaladja a józan ész által kialakított határokat.

Nem ez a helyzet áll fenn akkor, ha a képet csak az A által meghatározott szűkebb baráti kör láthatja. Ebben ez az esetben a kép elkészítéséhez adott hozzájárulás ugyanis a felvétel felhasználásához való engedélyt is felöleli.

Hasonlóan ítélandók meg azok a tényállások is, amikor egy idegenről osztunk meg képet, azzal az eltéréssel, hogy hozzájárulása nélkül valamennyi esetben sérül a képmáshoz való joga. További problémát jelentenek azok az esetek, amikor nem felhasználókról töltenek fel képeket, úgy, hogy azokat csak az ismerősök láthatják. Ez ugyanis azt jelenti, hogy az ábrázolt személyek a felvételekről – és így a jogsértésekről – valószínűleg sosem fognak tudomást szerezni. És végül a jog szempontjából talán a legnehezebben kezelhető kérdés – amelyre még maga a Facebook is külön figyelmeztet – hogy bármi, amit valaki megoszt, másolható és újra feltölthető azok által, akik az eredeti tartalmat megtekinthették.⁹

Összességében tehát elmondható, hogy főszabály szerint bárki bárkiről – tekintet nélkül arra, hogy az illető a Facebookon felhasználó-e, vagy sem, ismerős-e, vagy sem – tölthet fel képet, azon bárkit megjelölhet, és ezek közül egyikhez sem kell az érintett hozzájárulása.

6.1.3. Néhány fontosabb online platform szabályai és megoldási javaslatok

Az előző alfejezetekben a képmáshoz való jog Facebookon való megsértésének tipikus eseteit vizsgáltam. A probléma széleskörű vizsgálata érdekében azonban elkerülhetetlen, hogy a fenti szempontokból a képmáshoz való jog érvényesülését más jelentős közösségi oldalakon (YouTube, TikTok, Instagram) is elemezzem (2. táblázat). Vizsgálatom bebizonyítja, hogy a képmással kapcsolatos probléma hasonlóképpen jelentkezik az összes közösségimédia-platformon.

⁹ Meta Adatvédelmi Központ: Adatvédelmi szabályzat, https://www.facebook.com/privacy/policy/?entry_point=-data_policy_redirect&entry=0

2. táblázat: A képmáshoz való jog szabályozása (YouTube, Instagram, TikTok)¹⁰

	YouTube	Instagram	TikTok
A közösségi oldal működésének alapszabályai	3 féle nyilvánosság van: a feltöltött tartalmat (i) mindenki láthatja; (ii) csak azok láthatják, akiket a videó linkét ismerik; vagy (iii) csak azok láthatják, akiket a megosztó kiválaszt.	– 3 féle nyilvánosság van: (i) minden Instagram felhasználó; (ii) a tartalmat megosztó által kiválasztott követők láthatják a feltöltött tartalmat. ^a – A tartalmat kizárólag az azt feltöltő személy tagelheti. Privát fiók esetén a megosztó csak a követői tagelheti. ^b – A taget csak telefonra letöltött applikáción keresztül lehet törölni. ^c – A felhasználó előzetes engedélyéhez kötheti a tagelt képének profiloldalán való megjelenését. Ez azonban nem akadályozza meg a kép Instagramon való megosztását. ^d	– 4 féle nyilvánosság van: (i) mindenki; (ii) a felhasználó követői; (iii) felhasználó azon követői, akiket az érintett visszakövetett; (iv) csak a tartalommegosztó láthatja a feltöltött tartalmat. ^e – Amennyiben a tartalommegosztó profilja publikus, akkor a feltöltött tartalmat a megosztó által meghatározott személyek továbboszthatják. ^f – Az egyént beállításaitól függően (i) bárki; (ii) az illető követői; (iii) az egyén azon követői, akit visszakövetett; vagy (iv) senki nem tagelheti. ^g – A tény, hogy egy felhasználó senki számára nem teszi lehetővé, hogy őt tagelje, nem akadályozza meg a tartalommegosztót a videó feltöltésében.
A képmáshoz való jog megsértésének típusos esetei	Ha másról engedélye nélkül videót töltenek fel, feltéve, hogy azt vagy mindenki, vagy csak azok láthatják, akik a linket ismerik.	– Ha másról engedélye nélkül videót töltenek fel (annak függvényében, hogy hány, a tartalmat megosztó által kiválasztott személy láthatja, lehetséges, hogy a kép megosztása nem sérti az egyén képmáshoz való jogát). – A tagelés törlése, vagy a tageléshez való hozzáférés megtagadása nem vezet a kép megosztásának megakadályozásához.	– Ha másról engedélye nélkül videót töltenek fel (annak függvényében, hogy hány, a tartalmat megosztó által kiválasztott személy láthatja, lehetséges, hogy a kép megosztása nem sérti az egyén képmáshoz való jogát). – A tagelés törlése, vagy a tageléshez való hozzáférés megtagadása nem vezet a kép megosztásának megakadályozásához.

¹⁰ Saját szerkesztés.^a Instagram Sugóközpont: A nyilvános és a privát Instagram-fiókok közötti különbségek, <https://help.instagram.com/517073653436611>^b Instagram Sugóközpont: Hogyan tudok embereket megjelölni a bejegyzéseimben az Instagramon? <https://help.instagram.com/174635396025538>^c Instagram Sugóközpont: Hogyan tudod eltávolítani magadat, ha valaki megjelölt egy fényképen a Threadsben? <https://help.instagram.com/1241952293692588>^d Instagram Sugóközpont: Olyan Instagram-bejegyzések manuális engedélyezése, amelyeken meg vagy jelölve, <https://help.instagram.com/496738090375985>^e TikTok Support: Adatvédelmi beállítások, <https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/video-visibility>^f Uo.^g TikTok Support: Megjelölések a TikTok-on, <https://support.tiktok.com/en/using-tiktok/messaging-and-notifications/mentions-on-tiktok>

6.2. A képmáshoz való jog érvényesülése a manipulált képek világában

Ahogy arra a jelen monográfia tárgyát képező fiktív jogeset is rávilágít, a mai világunkban a legnagyobb társadalmi veszélyt valószínűleg nem a jogszerűen (vagy jogszerűtlenül) elkészített fényképek interneten való terjesztése, hanem a valamilyen úton-módon manipulált, hamisított fényképek és videók abszolút igazságként való megosztása jelenti. Utóbbi alatt értem mind a létező, de valamilyen technikai eszközzel (pl. Photoshoppal) módosított, mind pedig a mesterséges intelligencia által létrehozott, korábban meg nem lévő fényképeket is. Elég utalni például a Twitteren terjedő, Vlagyimir Putyint ábrázoló videóra, amelyben az orosz elnök békét 'hirdetett',¹¹ vagy az ukrán elnök, Volodimir Zelenszkij 2022. márciusi 'beszédére', amelyben felszólítja az ukrán katonákat a fegyverek letételére.¹² Mindkét videó a deepfake tökéletes mintapéldánya.

6.2.1. A deepfake fogalma és eredete

Deepfake alatt olyan mesterséges neurális hálózatokon alapuló úgynevezett mélytanulás által létrehozott, meghamisított videó-, kép- vagy hangfelvétel értendő, amely meggyőzően azt a téves látszatot kelti, hogy a meghamisított tartalomban ábrázoltak és/vagy elhangzottak valójában megtörténtek.¹³ Maga a deepfake elnevezés a *deep learning* (mélytanulás) és a *fake* (hamis) kombinációjából ered.¹⁴ A deepfake létrehozásának két klasszikus módja létezik: a Generatív Ellenséges Hálózatok és az Autóenkóder.

A Generatív Ellenséges Hálózatok (Generative Adversarial Networks, GAN) működése két párban álló mesterségesintelligencia-rendszeren alapszik. Az egyik (generátor) elkészíti a képet, hangot vagy videót, míg a másik (diszkriminátor) értékeli a generátor valamennyi próbálkozását és mindaddig, ameddig valósnak nem tartja az elkészített tartalmat, visszaküldi a generátor próbálkozásait.¹⁵ Tegyük fel például, hogy egy Picasso-képet szeretnénk készíteni egy GAN-alapú gépi tanulással működő mesterséges intelligencia segítségével. Miután az AI-tervező csapatok feltöltötték Picasso összes festményét, a generátor a feltöltött műalkotások jellemző vonásai alapján megkísérli utánozni Picasso munkáját azáltal, hogy ezernyi új képet készít Picasso stílusában. A diszkriminátor értékeli a generátor valamennyi próbálkozását abból a szempontból, hogy az mennyire hasonlít Picasso stílusához. A nem meggyőző próbálkozásokat a diszkriminátor visszaküldi a generátornak abból a célból, hogy az tovább javítson a próbálkozásán. Végül miután a generátor és a diszkriminátor milliányi alkalommal oda-vissza küldte egymásnak próbálkozásokat, a generátor sikeresen készít egy olyan Picasso képet, amelyet a diszkriminátor valósnak fogad el.¹⁶

¹¹ KUŹNICKA-BŁASZKOWSKA-KOSTYUK (2025): 3.

¹² HAIG (2022): 126.

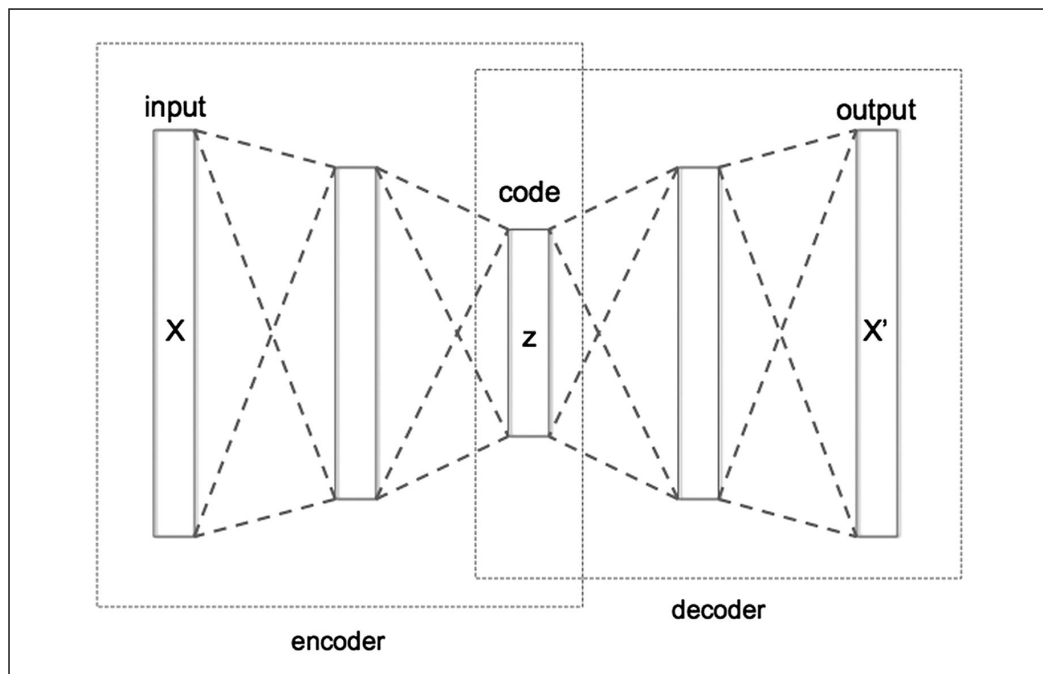
¹³ MRÁZ (2022): 249.

¹⁴ GOSZTONYI-LENDVAI (2023c)

¹⁵ HERKE (2023): 159.

¹⁶ A példa forrása: POMÁZI Krisztián: GAN (Generative Adversarial Network) alapú gépi tanulási feladat elvégzése. Aut.bme, 2021, <https://www.aut.bme.hu/Task/20-21-tavaszi/GAN-Generative-Adversarial>

Az autoenkóder (*autoencoder*) azon az elméleten alapul, hogy „egy jó reprezentációból minimális veszteséggel visszaállítható az eredeti egyed”.¹⁷ Az autoenkóderen alapuló gépi tanulás szintén két mesterségesintelligencia-rendszert (hálózatot) használ: a kódolót és a dekódolót. Először a kódoló a bemeneti képet (videót, hangot) kis vektorként kódolja, azaz tömöríti a nyersanyagot,¹⁸ majd utána ebből a reprezentációból a dekóder minimális veszteséggel megpróbálja helyreállítani a bemenetet. Ezen gépi tanulási módszert – példa helyett – legjobban a 11. ábrával lehet illusztrálni.



11. ábra: Autoenkóder-alapú gépi tanulási folyamat¹⁹

A deepfake-technológia megjelenésének pontos időpontja nehezen határozható meg. Az arccserélő (*face swap*) technológia, amely a deepfake elődjének tekinthető, 2004-ben ‘született meg’,²⁰ de csak 2016-ban terjedt el széles körben az olyan applikációk – mint a MSQRD, Face Swap Live és Face Stealer – megjelenésével, amelyek lehetővé tették az arcok kicserélését pusztán pár kattintással.²¹ Maga a deepfake alapjául szolgáló neurális hálózati architektúra megjelenése 2014-re tehető, amikor Ian Goodfellow társaival együtt a Generatív

¹⁷ FARKAS Róbert: Gépi tanulás a gyakorlatban. <https://www.inf.u-szeged.hu/~rfarkas/ML>

¹⁸ HERKE (2023): 159.

¹⁹ Forrás: Wikipedia, Autoencoder, https://en.wikipedia.org/wiki/Autoencoder#/media/File:Autoencoder_structure.png

²⁰ SCHEIRER (2023): 87.

²¹ GOSZTONYI–LENDVAI (2024): 43.

Ellenséges Hálózatok kiépítéséről és felhasználásáról szóló cikkét publikálta.²² A következő jelentős lépésre 2017-ben került sor, amikor lehetővé vált az egyének arcképének egyszerű és gyors módon történő mozgóképes monitorozása.²³ Ennek eredményeként tömegével jelentek meg az olyan pornófilmek, amelyekben a színésznők arcát hírességek arcával cserélték ki.²⁴ Mára már tucatjával érhetők el az olyan ingyenesen letölthető applikációk, amelyek lehetővé teszik deepfake készítését meglévő filmek, képek felhasználásával (pl. ZaoApp, Jiggy és FaceMagic) vagy akár szimpla szöveg alapján (pl. DALL-E, Midjourney és GPT-4o).

Annak ellenére, hogy a deepfake-technológia már több évtizede létezik, és a különböző applikációknak köszönhetően tömeges jelenséggé vált, a deepfake magyar jogi vonatkozását elemző szakirodalmak száma még igen csekély. Továbbá, ezen elérhető szakirodalom is elsősorban alkotmányjogi (szólásszabadság²⁵) és büntetőjogi (rágalmazás és bosszúpornó²⁶) szempontból elemzi a deepfake-et. Azzal a kérdéssel azonban, hogy a deepfake miként értékelendő a képmáshoz való jog szempontjából, egy tanulmány sem foglalkozik, bár – Veszelszki Ágnes szavait felhasználva – „igazi nehézfégyverzetről”²⁷ beszélhetünk.

Ezen ür kitöltése (vagy legalább is a hiány csökkentése) érdekében jelen monográfia az alábbi két kérdésre kíván választ találni:

- a) A képmáshoz való jog tárgya lehet-e egyáltalán a mesterséges intelligencia által létrehozott fénykép?
- b) A deepfake a képmáshoz való jog megsértésének minősül-e?

6.2.2. A deepfake mint a képmáshoz való jog tárgya

Noha eddig nem született olyan bírósági ítélet, amely kifejezetten kimondaná, hogy a deepfake-technológiával előállított tartalom a képmáshoz való jog tárgyi hatálya alá esne, a meglévő ítélkezési gyakorlat analógia útján történő alkalmazása alapján megalapozottan állítható, hogy ezek a tartalmak a jogvédelmi körbe tartoznak.²⁸

Több olyan ítélet is ismert ugyanis, amelyben a bíróság az arccserélés jogi következményeit elemezte. A Kúria például a Pfv. 21.267/2018/17. számú ítéletében arra a kérdésre kereste a választ, hogy sérült-e a felperes képmáshoz való joga azáltal, hogy az alperes a felperes arcát hozzájárulása nélkül egy szexuális tartalmú cselekvést végző meztelen női testhez montírozta.²⁹ Hasonlóan a Fővárosi Ítéletábrla a Pf. 21.277/2008/3. számú döntésében azt az esetet elemezte, amikor egy nő arcát egy férfi testére másolták. A bíróság mindkét esetben kiterjesztette a képmáshoz való jog védelmi körét a hamisított fényképekre is, és megállapította a képmáshoz fűződő jog megsértését.

²² PAWELEC (2025): 5.

²³ James VINCENT: AI tools will make it easy to create fake porn of just about anybody. *The Verge*, 2017. december 12., <https://www.theverge.com/2017/12/12/16766596/ai-fake-porn-celebrities-machine-learning>

²⁴ HERKE (2023): 159.

²⁵ GOSZTONYI–LENDVAI (2024); G. KARÁCSONY (2022); MRÁZ (2022).

²⁶ HERKE (2023); SORBÁN (2020).

²⁷ VESZELSZKI (2022): 33.

²⁸ RAD–CHRISTIE (2024)

²⁹ Pfv. 21.267/2018/17.

Tekintettel arra, hogy a képmáshoz való jog tárgya bármi lehet, amely képes az egyén testi jellegzetességeinek kifejezésére és így az ábrázolt személy egyediesítésére³⁰ (pl. rajz, karikatúra, festmény, szobor, videófelvétel), így logikusnak tetszik, hogy az egyén bármilyen digitális ábrázolása ugyanúgy képmásnak minősül.³¹ Az, hogy a képmáshoz való jog kiterjed valamennyi olyan mesterséges intelligencia által létrehozott fényképre, amely az egyén azonosítására alkalmas, összhangban áll a szakirodalomban kialakult azon elmélettel, miszerint a védelem szempontjából a rögzítés technikai eszköze lényegtelen.³²

A teljesség érdekében azonban szükséges megjegyezni, hogy bár mostanra a deepfake-technológia elérte azt a szintet, hogy befogadók már több mint a fele nem tudja megkülönböztetni a deepfake-et a valóságtól,³³ a deepfake ‘hitelessége’ még mindig nagyon eltérő lehet az alkalmazott technológia függvényében. Érdekes kérdést vet fel tehát azon deepfake-képek megítélése, amelyek bár nem ábrázolnak egy konkrét személyt egyértelműen azonosítható módon, mégis magas fokú hasonlóságot mutatnak egy valós személy arcvonásaival vagy megjelenésével. Vegyük például az alábbi, a CNN által bemutatott fotó alapján a GPT-4o által generált képet (13. ábra). Míg a GPT-4o által generált képen látható személy meglepő hasonlóságot mutat Julia Roberts valódi képével (12. ábra), – és első ránézésre egy átlagos befogadó könnyen azt hiheti, hogy a képen maga a színésznő látható –, részletesebb és alaposabb vizsgálat után ezen befogadó feltehetően és remélhetően meg tudja állapítani, hogy a kép valójában nem az amerikai színésznőt ábrázolja.



12. ábra:
Julia Roberts valódi fényképe³⁴



13. ábra:
GPT-4o által generált kép Julia Robertsról

Egyrészt a képmáshoz való jog mind a bírói joggyakorlat³⁵ mind pedig a szakirodalom³⁶ szerint kiterjed a karikatúrarajzra, amely – szemben például egy fényképpel – természetéből adódóan torzított módon ábrázolja a valóságot. Másrészt a képmás fent említett definíciójából következik, hogy a képmáshoz való jog kizárólag az olyan felvételekre terjed ki, amelyek alapján az érintett személy egyértelműen beazonosítható. Ezen álláspontot erősítette

³⁰ TÖRÖ (1979): 512.

³¹ KRISTON–TÓTH (2023): 88.

³² LENKOVICS–SZÉKELY (2001): 126.

³³ KÖBIS–DOLEŽALOVÁ–SORAPERLA (2021): 10–11.

³⁴ Forrás: Lisa RESPERS FRANCE: Julia Roberts has discovered she's not actually a Roberts. *CNN*, 2023. január 12., <https://edition.cnn.com/2023/01/12/entertainment/julia-roberts-roots/index.html>

³⁵ Pf. 21.001/2010/4.

³⁶ PETRIK (2001): 131.

meg például a Fővárosi Törvényszék P. 20.544/2014/4. számú ítéletében, amelyben a bíróság a képmáshoz való jog előfeltételeként azt vizsgálta, hogy a vitatott felvételen az egyén egyértelműen beazonosítható és felismerhető-e.

A fentebb leírtak alapján tehát álláspontom szerint egy mesterséges intelligencia által létrehozott fénykép, amely az érintetthez hasonló – de vele nem azonos – személyt ábrázol, kizárólag abban az esetben sértheti meg az érintett képmáshoz való jogát, amennyiben vagy a hasonlóság mértéke vagy egyéb körülmény (pl. kép alatti magyarázó szöveg) alapján egy átlagos ember arra a következtetésre jutna, hogy a deepfake-képen ténylegesen az érintett szerepel.³⁷

6.2.3. A deepfake mint a képmáshoz való jog megsértésének esete

Ahogy azt korábban kifejtettem, a Ptk. az egyén képmáshoz való jogát két szinten szabályozza: (i) a Ptk. 2:42 § (1) bekezdése a 2:43 § g) pontjában nevesített képmáshoz való jog bármely módon való megsértésének tilalmát állítja fel; míg (ii) a Ptk. 2:48 § (1) bekezdése a képmáshoz való megsértésének két speciális esetét (a felvétel jogosult hozzájárulása nélküli elkészítését, valamint annak hozzájárulás nélküli felhasználását) szabályozza.

A képmáshoz való jog deepfake útján történő megsértésének két esetét érdemes elkülöníteni: (i) egy már meglevő kép deepfake elkészítése céljából való felhasználása; és (ii) az eredeti kép meghamisítása.³⁸ Előbbire példa Hillary Clinton valamennyi fényképének felhasználása egy középkorú, szőke, fehér bőrű nő arcképének elkészítésére, míg az utóbbi kategóriába például a jelen monográfiában részletesen vizsgált, Hillary Clinton-kép tartozik.

A magyar bírói joggyakorlat következetesen foglal állást a tekintetben, hogy „egy meghatározott célból adott hozzájárulás alapján készült és nyilvánosságra hozott fénykép újbóli – eltérő célú és hozzájárulás nélküli – felhasználása önmagában is jogsértést valósít meg.”³⁹ Ezen érvelés alapján állapította meg a képmáshoz való jog megsértését például (i) a Kúria (akkori nevén Legfelsőbb Bíróság) a ‘polgárrá fogadási’ ünnepségen magánszemélyekről (felperesekről) készült fényképeknek az alperes kampányszórólapjain való közzététele miatt,⁴⁰ vagy (ii) a Szegedi Ítéltábla egy modellről naptárhoz készült fényképnek valamely termék csomagolására szolgáló dobozon a hozzájárulása nélkül történő felhasználása miatt.⁴¹ Mindebből azonban az is következik, hogy magánszemélyekről már elkészült fényképeknek deepfake készítése céljából való engedély nélküli felhasználása (pl. mesterséges intelligencia által történő elemzése hasonló fényképek elkészítés céljából, vagy a feltöltött fényképek mesterséges intelligencia általi másolása) a képmáshoz való jog megsértésének minősül a Ptk. 2:48. § (1) bekezdése alapján.

³⁷ Meg kell ugyanakkor említeni, hogy Cristian Vaccari és Andrew Chadwick 2020-as kutatásból az derült ki, hogy egy 4 másodperces deepfake-videó a kutatásban részt vevők közel 15 százalékát tévesztette meg, míg 35 százalékuk bizonytalan volt azzal kapcsolatban, hogy a tartalom, amelyet láttak, ‘valós’ volt-e (VACCARI–CHADWICK: [2020]).

³⁸ MRÁZ (2022): 271.

³⁹ BH 1995.632 és Pfv. 20.801/2007/7.

⁴⁰ Pfv. 20.801/2007/7.

⁴¹ BDT 2015.3312. (Pf. 20.092./2013/2.).

A Pécsi Ítéltábla ítéletében továbbá azt is leszögezte, hogy „a képmáshoz való jog megsértése szempontjából nincs különbség a Facebook-oldalon található fénykép és a bármely más forrásból származó felvétel felhasználásának feltételei és megítélése között”.⁴² Így a képmáshoz való jog megsértésének fentebbi bekezdésben ismertetett esete akkor is megvalósul, amikor a jogsértő személy kizárólag a közösségimédia-oldalakon nyilvánosan megosztott fényképeket használja fel a deepfake elkészítése céljából. Az ugyanis, hogy valaki az interneten képet tesz közzé magáról, nem jelenti azt, hogy ezzel hozzá is járul a fényképe mások általi felhasználásához.⁴³ Az ábrázolt személy jogosult annak meghatározására, hogy képmását ki, milyen módon és körben használja fel.⁴⁴

Fontos megjegyezni, hogy a képmásfelhasználás ‘célhoz kötöttségének’ követelménye (vagyis, hogy a jogszerűen készített és valamely célból felhasznált fénykép kizárólag ezen céllal összeegyeztethető más célból használható fel) a bírói joggyakorlat értelmében a közszereplőkről készített képmások esetén is alkalmazandó. A Fővárosi Ítéltábla elvi döntésében például akként foglalt állást, hogy a „közéleti szerepet vállaló személyek közéleti szereplése alkalmával készült képmás csak a közszereplésükkel összefüggésben, a közéleti megnyilvánulásuk által meghatározott körben, annak bemutatására használható fel hozzájárulás nélkül”.⁴⁵ Hasonlóan, a Kúria a BH 2006.282. (Pfv. IV. 21.553/2004.) számú döntésében kimondta, hogy a közszereplő képmása, hozzájárulása nélkül kizárólag közszerepléseivel összefüggésben, a közéleti megnyilvánulásai által meghatározott keretben, annak bemutatására használható fel.⁴⁶ A Szegedi Ítéltábla BDT 2020.4222. (Pf. III.20.010/2020.) számú ítélete még tovább szigorította a közszereplőről készült képmás felhasználhatóságának körét: a bíróság ugyanis akként rendelkezett, hogy a közéleti szereplésről készült felvétel az érintett személy hozzájárulása nélkül kizárólag arról az eseményről szóló tudósításban használható fel, amelyről a felvétel készült, tekintettel arra, hogy a Ptk. 2:48 § (2) bekezdésében meghatározott, a hozzájárulás beszerzésének kötelezettsége alóli kivételek nem értelmezhetők kiterjesztően.⁴⁷

A közszereplő képmása tehát nem szabad felhasználás tárgya, az nem szolgálhat különböző, a közszereplő konkrét megnyilvánulásaitól független gondolati tartalmak, vélemények illusztrálására.⁴⁸ Mindebből azonban azt is következik, hogy a közszereplő képmása az érintett személy külön hozzájárulása nélkül csak szűk körben, kizárólag olyan deepfake készítésére használható fel, amely összefüggésbe hozható azzal a tárgykörrel, amellyel kapcsolatban a közszereplő közéleti szerepvállalás során a felvétel készült.⁴⁹

⁴² BDT 2020.4126. (Pf. III.20.101/2019/4.).

⁴³ PJD 2016.21. (I.Pf. 21.458/2015/4/II.).

⁴⁴ Így például a Clearview AI, amely közel hárommilliárd képmásból álló adatbázist hozott létre különböző közösségimédia-oldalakon megosztott fényképek letöltésével egy mesterséges intelligencián alapuló arcfelismerő program létrehozása céljából, többmilliárd személy képmáshoz való jogát sértette meg. GRC World Forums: Privacy advocacy groups challenges Clearview AI. *GRC World Forums*, 2021. május 28., <https://www.grcworldforums.com/global/privacy-advocacy-groups-challenges-clearview-ai/1873.article>

⁴⁵ PJD 2016.21. (I.Pf. 21.458/2015/4/II.).

⁴⁶ BH 2006.282. (Pfv. IV. 21.553/2004.).

⁴⁷ BDT 2020.4222. (Pf. III.20.010/2020.).

⁴⁸ BH 2006.282. (Pfv. IV. 21.553/2004.).

⁴⁹ PJD 2016.21. (I.Pf. 21.458/2015/4/II.).

Ezen következtetés azonban véleményem szerint egyes esetekben sértheti az Alkotmánybíróság, illetve az EJEB szólásszabadsággal összefüggésben kialakított joggyakorlatát. Ahogyan azt fentebb részletesen kifejtettem, a közszereplő képmáshoz való joga szükséges és arányos mértékben korlátozható a szólásszabadság és a véleménynyilvánítás biztosítása érdekében, azonban példának okáért a Barack Obama közoktatásról szóló sajtótájékoztatóján készült fényképek nem használhatók fel egy olyan fakevideó készítésére, amelyben ugyanő a COVID oltás szükségességéről beszél, hiszen ez a közügyek szabad megvitatásának sérelméhez, és így közvetve a szólásszabadság aránytalan korlátozásához vezethet.

A képmáshoz való jog deepfake útján megvalósuló megsértésének másik esete a már meglévő képfelvétel meghamisítása. Ezzel kapcsolatban mindenekelőtt le kell szögeznünk, hogy (a hiányzó szakirodalmon felül) olyan bírói döntés sem létezik, amely egy deepfakevideót vagy -képet elemezne egy egyén képmáshoz való joga szempontjából. Ugyanakkor több olyan ítélet is ismert, amely egy eredeti fénykép torzítását, montírozását, illetve meghamisítását elemzi a Ptk. 2:42 §-a, valamint a 2:48 §-a alapján. Jelen esetben ezen ítéletek véleményem szerint (korlátozott) analógiaként alkalmazandók, hiszen a meghamisított felvételek jogi megítélése szempontjából az alkalmazott technológia majdhogynem lényegtelen.

A Kúria a PJD 2019.18. (Pfv. 20.955/2017/9.) számú döntésében elvi éllal mondta ki, hogy amennyiben az egyén képmását olyan formában teszik közzé, hogy azáltal az érintett képmása torzítottan, vagy hamis látszat keltésére használják fel, úgy a felvétel közzététele sérti a Ptk. 2:48 §-át.⁵⁰ Noha az ítélet alapjául szolgáló tényállás szerint az alperes a szóban forgó képet semmilyen technikai eszközzel nem módosította, azt pusztán egy létező videóból kivágta az eredeti felvételtől le nem vonható következtetés alátámasztása érdekében, a bíróság megközelítése megfelelően alkalmazandó a deepfake jogi elemzése során is. Döntésében a Kúria ugyanis a jogsértés elbírálása során először összevetette az eredeti és a kifogásolt képet annak megállapítása érdekében, hogy az utóbbi a felperest érintően hamis látszatot kelt-e. Mivel megállapította, hogy az alperes a kifogásolt kép kontextusból való kiragadásával olyan mértékű torzítást idézett elő, amely megtévesztő üzenetet sugallt a nyilvánosság számára, a Kúria a képmáshoz fűződő jog megsértését állapította meg. Hasonló megállapításra jutott a Kúria egy másik ítéletében is, amely szerint a felperes képmásának egy szexuális tartalmú cselekvést végző meztelen női testhez montírozása a felperes képmással való visszaélésnek minősül.⁵¹ Mindebből tehát az következik, hogy az eredeti kép meghamisításából álló deepfake-tartalmak többsége a képmáshoz való jog megsértésének minősül.

Általánosságban elmondható, hogy a bírói joggyakorlat ezen megközelítést alkalmazza a közszereplőkről készült felvételek meghamisítása esetén is. Így például a Győri Ítéltábla az egyik ügyében akként rendelkezett, hogy a közszereplés során készült felvételt sem lehet torzított, az eredeti jelentéstartalomtól eltérő módon felhasználni.⁵² Hasonlóan a Fővárosi Bíróság egy előadóművész családtagjainak képmáshoz való jogának megsértését állapította meg ítéletében azért, mert az alperes az érintettek arcát hozzájárulásuk nélkül más

⁵⁰ PJD 2019.18. (Pfv. 20.955/2017/9.). Lásd továbbá: BH 1994.127. (Pfv. IV. 21.327/1993.) és BH 1997.578. (Pfv. IV. 20.118/1996.).

⁵¹ Pfv. 21.267/2018/17.

⁵² Pf. 20.138/2019/6.

személyek testére montírozta, és azt újságjában közzétette. Az ügyben az alperes az egyik felperes arcát egy férfi meztelen felsőtestére montírozta az alábbi szöveggel: „[...] valaha férfi volt – lapunknak elárulta, hogy valójában [...] néven fiúként látta meg a napvilágot – később több műtéttel operáltatta magát át, s a hormonkezelések olyan jól sikerültek, hogy két egészséges lánynak is életet adhatott.” Felismerve a felperesek közszereplői minőségét, a bíróság ítéletében mindenekelőtt leszögezte, hogy a felperesek közszereplőként vállalták képmásuk különböző újságokban való megjelenését. A bíróság ítéletében ugyanakkor azt is megállapította, hogy a felperesek pusztán azért, mert egy műsorban szerepelnek, illetve a műsort reklámozzák, nem adták hozzájárulásukat ahhoz, hogy őket nevetségessé tegyék vagy megalázzák.⁵³

Másrészről azonban a közszereplőket megillető képmáshoz való jog nem abszolút és így bizonyos esetekben a képfelvételük módosítható, torzítható, sőt akár hamisítható is.⁵⁴ Emellett foglalt állást például a Fővárosi Ítéltábla a Pf. 20.750/2021/15. számú ítéletében, amely kimondta, hogy az alpolgármester (felperes) képmáshoz való joga nem sérült azáltal, hogy egy újság (alperes) egy olyan fényképmontázst tett közzé, amelyen a felperes fényképe egy két politikus által átkarolt alakra lett montírozva. Indokolásában a bíróság arra a következtetésre jutott, hogy a gunyoros képmontázs a felperes vélt politikai nézeteinek illusztrálását szolgálja, ezáltal a manipulált felvétel a felperes politikai tevékenységével hozható összefüggésbe. Mivel azonban a közszereplők esetében fokozott tűrési kötelezettség érvényesül, a felperesnek tűrnie kellett a vélt politikai álláspontját szemléltető, torzított képfelvétel nyilvánosságra hozatalát is.⁵⁵ Hasonló következtetésre jutott a Fővárosi Ítéltábla egy másik ítéletében is, amely szerint nem sérült azon közszereplőnek a képmáshoz való joga, akinek az arcképét egy „Együtt a Maffiabaloldal” feliratú fotómontázssra másolták. Ezen döntésében a bíróság elsősorban arra helyezte a hangsúlyt, hogy a fotómontázson feltüntetett szöveg (amely mindkét fél szerint jogszerű véleménynyilvánításnak minősült) és az azon látható képfelvételek egymással összefüggésben álltak.⁵⁶ Ugyanezen ügyben a Kúria továbbá azt is hozzátette, hogy „adott esetben a fotómontázson feltüntetett fényképfelvételek csoportosítása egy adott kormányzati ciklusban az érintett személyek kifejezetten közéleti tevékenységével összefüggésben készült, amely a feliratokkal együtt a vélemény kinyilvánításának egy sajátos formája volt.”⁵⁷ Így bár a képmontázs negatív tartalmat hordozott, azt az I. rendű felperes mint volt miniszter és a II. rendű felperes mint volt országgyűlési képviselő köteles volt eltűrni.⁵⁸

⁵³ Pf. 21.277/2008/3.; P. 20.239/2008/3.

⁵⁴ Ezzel kapcsolatban lásd: KOVÁCS–SORBÁN (2024).

⁵⁵ Pf. 20.750/2021/15.

⁵⁶ Pf. 20.537/2014/3.

⁵⁷ Pfv. 21.245/2015/4.

⁵⁸ Pf. 20.537/2014/3.

6.3. Attól, hogy hamis, egyúttal jogellenes is?

Amint arra már korábban utaltunk, a deepfake (akár pozitív, akár negatív értelemben) tagadhatatlanul kiemelkedő szerepet tölt be a demokratikus közvélemény alakításában.⁵⁹ Bár valamennyi deepfake természeténél fogva hamis, ez nem jelenti feltétlenül azt, hogy az mind jogellenes is, és nem védi őket a véleménynyilvánítás szabadsága.⁶⁰ De hol húzzuk meg a határt a védett és a tiltott beszéd között? Mi különbözteti meg a jogszerű deepfake-et a jogellenestől?

Ezen kérdések megválaszolása érdekében elkerülhetetlen a deepfake mint közlés szó-lásszabadság szempontjából való elemzése. Jelen fejezet célja tehát annak vizsgálata, hogy vajon a deepfake mely esetekben tekinthető jogszerű véleménynyilvánításnak az Alkotmány-bíróság, valamint az EJEB joggyakorlata szerint.

6.3.1. A deepfake megítélése az Alkotmánybíróság joggyakorlata alapján

Az Alkotmánybíróság jelenleg uralkodó joggyakorlata értelmében a szólásszabadság védel-mének keretei között a hazugság általános értelemben nem tiltott.⁶¹ Annak megállapítása érdekében, hogy mely hamis közlés esik a szólásszabadság védelme alá, mindenekelőtt kü-lönbséget kell tennünk a tényállítások és a vélemények között.⁶² A véleménynyilvánítás sza-badsága ugyanis valamennyi véleményre kiterjed,⁶³ függetlenül attól, hogy az értékes vagy értéktelen, igaz vagy hamis, érzelmen vagy észérveken alapul.⁶⁴ A véleménynyilvánítás sza-badsága azonban nem ilyen feltétlen a tényállítások tekintetében. Ahogy arra több Alkot-mánybírószági döntés is rámutatott, „a véleménynyilvánítás szabadsága nem terjed ki a be-csületsértésre alkalmas valótlan tények közlésére”,⁶⁵ feltéve, hogy a nyilatkozó személy kifejezetten tudta a közlés valótlanosságát (tudatosan hamis közlés), vagy foglalkozása, hivatá-sa gyakorlásának szabályai szerint elvárható lett volna tőle a tények valóságtartalmának viz-sgálata.⁶⁶ Ezzel szemben a véleménynyilvánítás szabadsága kiterjed a valós tények, infor-mációk közlésére még akkor is, ha azok becsületsértésre alkalmasak.⁶⁷ Koltay András ugyanakkor megjegyzi, hogy „a tények és a vélemények elválasztása olykor igen nehéz, sőt egyenesen lehetetlen.”⁶⁸ Ahogyan arra maga az Alkotmánybíróság is rámutatott, „a tényállí-tást tartalmazó megnyilvánulások szintén részei a szólásszabadságnak. Egyrészt valamely tény közlése is kifejezhet személyes véleményt, másrészt tényközlések nélkül a véleményfor-málás is ellehetetlenülne.”⁶⁹

⁵⁹ MRÁZ (2022): 252.

⁶⁰ LENDVAI (2023): 125.

⁶¹ KOLTAY (2020): 239.

⁶² KOLTAY (2019): 12.

⁶³ 36/1994. (VI. 24.) AB határozat, 1.1.

⁶⁴ 3100/2017. (V. 8.) AB határozat, 32.

⁶⁵ 36/1994. (VI. 24.) AB határozat, III.2.

⁶⁶ SZILÁGYI (2018): 6.; HERMÁN (2024): 78.

⁶⁷ 36/1994. (VI. 24.) AB határozat, III.2.; VITKOVICS (2025): 55–56.

⁶⁸ KOLTAY (2009): 413.

⁶⁹ 7/2014. (III. 7.) AB határozat, 49.

Az Alkotmánybíróság hosszú ideig egy szemantikai megközelítést alkalmazott,⁷⁰ amelynek értelmében tényállításnak kizárólag az olyan közlés minősült, amelynek „igazságtartalma legalább részben ellenőrizhető”⁷¹ volt. Tényállításnak tehát csak az olyan közlések minősültek, amelyek objektíve valóság vagy valótlanok voltak.⁷² Ezen megközelítés azonban – úgy tűnik – mára már meghaladottá vált. Az Alkotmánybíróság jelenlegi gyakorlata sokkal pragmatikusabb utat választott: a közlés ellenőrizhető igazságtartalma csupán szükséges, de nem elégséges feltétele annak, hogy a közlés tényállításnak minősüljön.⁷³ Ezen új felfogást tükrözi például a 3107/2018. (IV. 9.) AB határozat:

„Erre utalt az Alkotmánybíróság akkor, amikor a mérlegelés alkotmányos követelményeként mondta ki, hogy a szóban forgó kijelentés értékelése nem történhet csupán »megragadva a kijelentés direkt tartalmánál« (...), hanem a mérlegelést a választási kampány felfokozott helyzetét és az ügy összes körülményét figyelembe véve, valamint arra tekintettel kell elvégezni, hogy a jelöltek egymás programját és alkalmasságát minél szabadabban kritizálhassák (...).”⁷⁴

Az Alkotmánybíróság legutóbbi döntései értelmében a tényállítás alkotmányjogi fogalmát megszorítóan kell értelmezni,⁷⁵ míg a véleménynyilvánítás szélesebb értelmezést kíván.⁷⁶ A tényállítás és a véleménynyilvánítás elkülönítése érdekében szükséges a közlés körülményeinek, tárgyának és céljának figyelembevétele.⁷⁷ A közlés kontextusának vizsgálatával összefüggésben az Alkotmánybíróság kifejezetten hangsúlyozta, hogy a közlés mögöttes jelentését vizsgálni szükséges:⁷⁸

„Ha a megnyilatkozásnak a közügyek vitája, kiváltképp a kampány sajátosságaira tekintettel észszerűen tulajdonítható olyan jelentés, amely szerint a közlést a választók az érintett múlt- vagy jövőbeli politikájára vagy a jelölt alkalmasságára vonatkozó politikai véleményként (nem pedig szó szerint) értelmezik, akkor a közéleti vita legintenzívebb szférájának szabad alakulása érdekében ebből kell kiindulni. (...) Szintén védelem alá tarthat a kritika túlzó, meghökkentő megfogalmazása, akkor is, ha a túlzás esetleg ténybeli kérdést is érint.”⁷⁹

A fentebb leírtakból következően tehát a deepfake kizárólag abban az esetben részesülhet(ne) alkotmányjogi védelemben, ha az hamis információn alapuló véleménynek és nem hamis tényállításnak minősül. Ahogyan azonban arra számos szerző rámutatott, a deepfake a tényállítás és véleménynyilvánítás között helyezkedik el.⁸⁰ Egyrészt, a deepfake fentebb

⁷⁰ MRÁZ (2022): 261.

⁷¹ 13/2014. (IV.18.) AB határozat, 37.

⁷² KOLTAY (2020): 236.

⁷³ MRÁZ (2022): 261.

⁷⁴ 3107/2018. (IV. 9.) AB határozat, 27.

⁷⁵ Uo.

⁷⁶ MRÁZ (2022): 262.

⁷⁷ 9/2015. (IV. 23.) AB határozat, 43.

⁷⁸ 3107/2018. (IV. 9.) AB határozat, 28.

⁷⁹ Uo.

⁸⁰ Lásd például: MRÁZ (2022): 261.

említett definíciója szerint – azaz, hogy meghamisított videó, kép vagy hangfelvétel, amely meggyőzően azt a téves látszatot kelti, hogy a meghamisított tartalom valójában megtörtént – hamis tényállítás. Másrészről azonban, ahogyan azt a korábbi fejezetekben ismertetett jogesetek esetében is láthattuk, a hamisított, torzított fényképek számos esetben a véleménynyilvánítás eszközeként szolgálnak.

Álláspontom szerint az Alkotmánybíróság joggyakorlatára tekintettel a deepfake főszabály szerint hamis tényállításnak minősül. A deepfake ugyanis természetéből adódóan meggyőzően kelti azt a látszatot, hogy a meghamisított tartalom valójában megtörtént. Nightingale és Farid által 2022-ben végzett kutatásából például nem csupán az derül ki, hogy a résztvevők csak 48%-os pontossággal tudták a valódi személyeket azonosítani, de az is, hogy a mesterséges intelligencia által 'létrehozott' személyek 8%-kal magasabb bizalmi indexet értek el.⁸¹ Látható tehát, hogy az egyének mára már sokszor nem tudnak különbséget tenni valós és valótlan tartalmak között.⁸² A deepfake-nek a hitelesség ilyen magasfokú imitálására való képességéből azonban az is következik, hogy egy átlagos befogadó az esetek többségében a deepfake-et már nem véleményként, hanem szó szerint, tényállításként fogja értelmezni. A 3107/2018. (IV. 9.) AB határozatban foglaltakra tekintettel tehát ezen esetekben a deepfake-ek tényállításnak minősülnek.

Természetesen mindez nem zárja ki annak lehetőségét, hogy bizonyos esetekben – a körülményektől és a közlés kontextusától függően – egyes deepfake tartalmak véleményként legyenek értelmezhetők. Amennyiben például a felvétel hamis volta egyértelműen kitűnik magából a képi anyagból, vagy a közlés környezetéből kétséget kizáróan megállapítható, hogy a manipulált képmás kizárólag a közlő véleményének illusztrálására szolgál, úgy az adott deepfake véleménynek tekinthető. A jelen monográfia tárgyát képező Hillary Clinton-felvétel azonban véleményem szerint nem tartozhat ezen kivételes esetkörbe, hiszen az semmilyen véleményt nem tükröz, pusztán egy már korábban többszörösen megcáfolt álhírt próbál alátámasztani.

Végezetül külön említést érdemel a 15/2020. (VII. 8.) AB határozat, amelyben az Alkotmánybíróság a rémhírterjesztés új tényállásának⁸³ alkotmányosságát állapította meg. Bár a szakirodalom ezen alkotmánybíróági döntéssel kapcsolatban számos (megalapozott) kritikát is megfogalmazott,⁸⁴ a határozat alábbi rendelkezései véleményem szerint előrevetíti az Alkotmánybíróság deepfake-ekkel kapcsolatos jövőbeni (várható) álláspontját:

„Az Alaptörvény a véleménynyilvánítás szabadságát a sajtó szabadságához, sokszínűségéhez, a demokratikus közvélemény kialakulásához szükséges szabad tájékoztatáshoz köti. Ehhez a hamis közlés önmagában nem járul hozzá, noha annak a cáfolata már igen.”⁸⁵

⁸¹ MEZRICZKY (2023): 44.

⁸² KELEMEN (2023): 35.

⁸³ Büntető Törvénykönyvről szóló 2012. évi C. törvény 337. § (2) bekezdés: 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 megghiúsítsa, büntetett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.

⁸⁴ Például Bencze Máttyás és Ficsor Krisztina amellet foglaltak állást, hogy a Btk. ezen módosítása a jogbiztonság alapvető elveit sértette meg (BENCZE–FICSOR [2020]).

⁸⁵ 15/2020. (VII. 8.) AB határozat, 52.

A különleges jogrendi állapot⁸⁶ célja az állam normális működésének helyreállítása, így nem lehet szükségtelen az olyan közlések tiltása, amelyek e célt akadályozzák vagy megghiúsítják.⁸⁷ Így különös jogrend idején a tudottan hamis (vagy elferdített) tényeken alapuló olyan véleménynyilvánítás, amely a járványügyi védekezést akadályozhatja a hallgatóságra gyakorolt hatásánál fogva korlátozható jogrendet kiváltó ok kezelése érdekében.⁸⁸

Az egyes intézkedések kritikáinak tilalma a véleménynyilvánítás aránytalan korlátozásának minősülne.⁸⁹

Az Alkotmánybíróságnak a fentebb hivatkozott megállapításai arra engednek következtetni, hogy a hamis tényeken alapuló vélemény a közbiztonság érdekében korlátozható, feltéve, hogy az nem vezet a közéleti vita korlátozásához. A Hillary Clintonról készült deepfake-felvétel vonatkozásban ez pedig azt jelentené, hogy még abban az esetben is, amennyiben a felvétel nem tényállításnak, hanem véleménynek minősülne, akkor sem részesülhetne a szólásszabadság védelmében.

6.3.2. A deepfake megítélése az EJEB joggyakorlata alapján

A véleménynyilvánítás szabadsága és a magánélet tiszteletben tartásához való jog közötti kompromisszum

Az EJEB ítélkezési gyakorlata szerint az államoknak pozitív kötelezettségük, hogy biztosítsák a magánülethez való jog tiszteletben tartását még a magánfelek között is,⁹⁰ valamint, hogy pozitív intézkedéseket hajtsanak végre a véleménynyilvánítás szabadságának védelme érdekében.⁹¹ A szólásszabadsághoz való jog és a magánülethez való jog egyenlő tiszteletet érdemel, ezért ezen emberi jogok között nem létezik absztrakt hierarchia.⁹² Következésképpen, mivel egyik jog nem írhatja felül automatikusan a másik jogot, a jogalkotónak a jóhírnév sérelme szabályozásakor, valamint a bírói hatalomnak az ilyen ügyek elbírálásakor méltányos egyensúlyt kell teremtenie ezen egymással versengő jogok között.⁹³

Bár a nemzeti jogalkotók és a nemzeti hatóságok széles mérlegelési jogkörrel rendelkeznek annak meghatározásában, hogy hol található a megfelelő egyensúly a véleménynyilvánítás szabadsága és az államnak az egyén jóhírnevének védelmére vonatkozó kötelezettsége között, mégis tiszteletben kell tartaniuk az emberi jogi bíróságok által meghatározott

⁸⁶ KELEMEN (2022)

⁸⁷ DRINÓCZI (2021): 5.

⁸⁸ 15/2020. (VII. 8.) AB határozat, 52.

⁸⁹ Uo., 52–53.

⁹⁰ Bédar kontra Svájc, App no. 56925/08 (2016. március 29.), 73.; Lozovyye kontra Oroszország, App no. 4587/09 (2018. április 24.), 36.

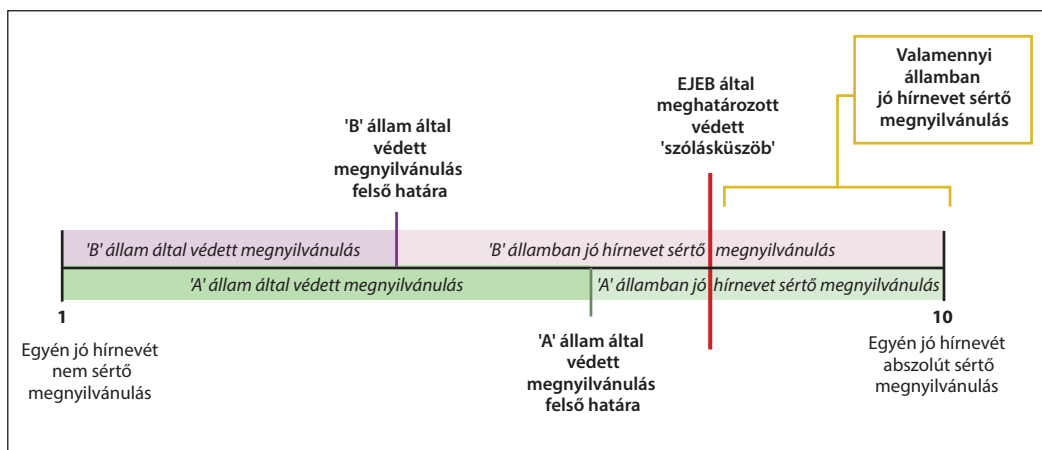
⁹¹ Appleby és társai kontra Egyesült Királyság, App. no. 44306/98 (2003. július 5.), 39.; Melnychuk kontra Ukrajna, App. no. 28743/03 (2005. július 28.), 2.

⁹² Von Hannover kontra Németország (2. sz.), App. no. 40660/08 és 60641/08 (2012. február 7.), 106.; Axel Springer AG kontra Németország, App. no. 39954/08 (2012. február 7.), 87.; ANGELOPOULOS–SMET (2016).

⁹³ Mosley kontra Egyesült Királyság, App. no. 48009/08 (2011. május 10.), 111.; Couderc és Hachette Filipacchi Associés kontra Franciaország, App. no. 40454/07 (2015. november 10.), 91.; Bédar kontra Svájc, App no. 56925/08 (2016. március 29.), 52.

határokat.⁹⁴ Az EJEB kijelöli a védett szólás határait, ami azt jelenti, hogy az EJEB határozza meg azoknak a kijelentéseknek a körét, amelyek annyira sértik az egyén jóhírnevét, hogy azokat az EJEE részes államai nem tűrhetik el, és ezért azokat ezen országokban a jóhírnév sérelmének kell tekinteni.

Az EJEE 8. cikkében foglalt,⁹⁵ a magánélet tiszteletben tartásához való jog védelmére vonatkozó állami kötelezettség szempontjából az EJEB szerepe a védett 'szólásküszöb' meghatározásában a következő példán keresztül szemléltethető. Vegyünk egy 1-től 10-ig terjedő skálát, ahol az 1 olyan tartalomra utal, amely egyáltalán nem rágalmazó, a 10 pedig olyan tartalomra, amely teljes mértékben sérti az egyén jóhírnevét. Ezen a skálán az EJEB megállapítja a védett szólás határát, meghatározza, hogy mi az a maximális mérték, ameddig az államok eltűrhetik a sértő tartalmakat. Az államok a skálán az EJEB által meghatározott határ előtt húzhatják meg a határokat, de azon túl már nem. Mindebből azonban az is következik, hogy egy olyan közlés, amely az EJEB joggyakorlata értelmében sérti az EJEE 8. cikkét,⁹⁶ nem tartozhat a véleménynyilvánítás oltalma alá Magyarországon.



14. ábra: Az EJEB kontra az egyes államok által meghatározott 'szólásküszöb'⁹⁷

A jóhírnév sérelmét érintő ügyben ha az egyik fél úgy véli, hogy a jogerős ítélet megsértette alapvető jogát (a szerző esetében a véleménynyilvánítás szabadságát, a sértett esetében a magánélet tiszteletben tartásához való jogot), a jogerős határozat meghozatalától számított hat hónapon belül (feltéve hogy a kérelmező kimerítette az összes, rendelkezésére álló hazai jogorvoslati lehetőséget) eljárást kezdeményezhet az állam ellen azon az alapon, hogy az állam megsértette a kérelmező alapvető jogának védelmére vonatkozó kötelezettségét.⁹⁸

⁹⁴ Lingens kontra Ausztria, App. no. 9815/82 (1986. július 8.), 39.; Janowski kontra Lengyelország, App. no. 25716/94 (1999. január 21.), 30.; Tammer kontra Észtország, App. no. 41205/98 (2001. február 6.), 60.; Lautsi és társai kontra Olaszország, App. no. 30814/06 (2011. március 18.), 70.; Chauvy és társai kontra Franciaország, App. no. 64915/01 (2004. június 29.), 64.

⁹⁵ MENYHÁRD (2017)

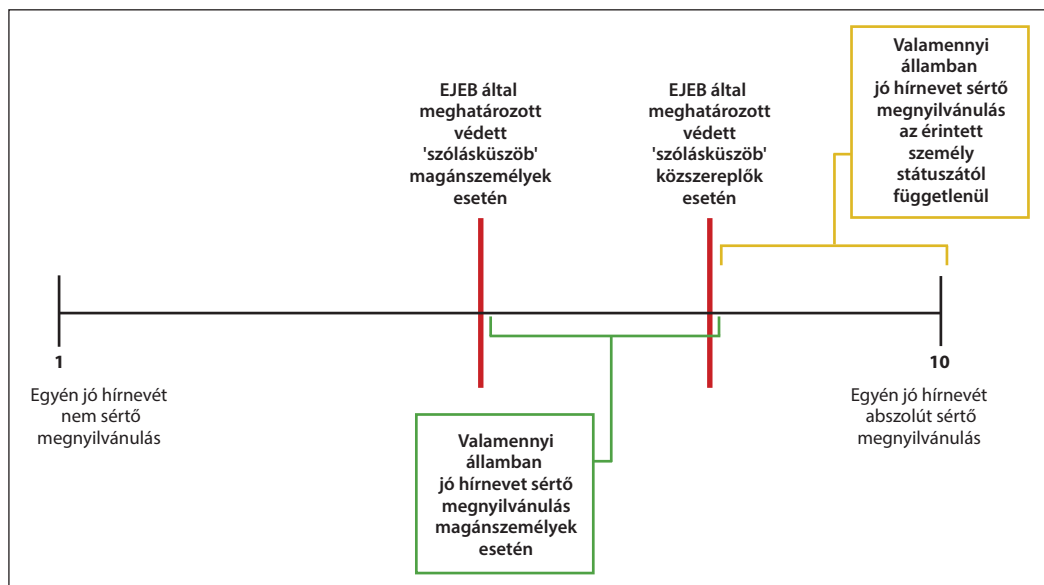
⁹⁶ SÜLYÖK (2021)

⁹⁷ Saját szerkesztés.

⁹⁸ EJEE, 34–35. cikk.

A fentebb leírtak alapján tehát elsősorban nem azt szükséges eldönteni, hogy a Hillary Clintonról készített deepfake a magyar jog szerint a jóhírnév megsértésének minősülne-e, hanem elegendő annak értékelése, hogy a hamisított felvétel olyannyira megalázó-e, hogy azt az EJEB ítélkezési gyakorlata értelmében egyetlen állam sem tudná védett közlésnek minősíteni. Amennyiben e kérdésre a válasz pozitív, úgy a deepfake Hillary Clinton jóhírnévének megsértéseként értékelendő mind Magyarországon, mind pedig valamennyi olyan államban, amely ratifikálta az EJEE-t.

Az EJEB a véleménynyilvánítás szabadságának felső határát eltérően állapította meg az érintett személy státusza, illetve beszéd jellege alapján.⁹⁹ Az EJEB következetes joggyakorlata szerint a politikai beszéd és a politikusokkal szembeni kritika szélesebb körű védelmet élvez, mivel a politikusok tudatosan és elkerülhetetlenül teszik ki magukat annak, hogy a sajtó és a nyilvánosság minden szavukat és tetteiket fokozott figyelemmel nyomon kövesse és bírálja.¹⁰⁰ Továbbá „a magánszemélyek hírneve fokozottabb védelmet érdemel, mint a politikusoké vagy a köztisztviselőké, de ez kevésbé igaz, ha a jogsértés közérdekű ügyet érint.”¹⁰¹ Végül a vállalkozásokkal kapcsolatos véleménynyilvánítás a legkevésbé védett, mivel az EJEB széles mérlegelési mozgásteret biztosít az országoknak a jóhírnév és az üzleti gyakorlat védelmére ilyen esetekben.¹⁰² Következésképpen az EJEB a védett közlés felső mércéjét a legmagasabbra a közszereplők esetében tette. A korábbi ábrát tehát a következőképpen kell módosítani:



15. ábra: Az EJEB kontra az egyes államok által meghatározott 'szólásküszöb' közszereplők esetén¹⁰³

⁹⁹ KOZŁOWSKI (2006): 140.

¹⁰⁰ Lingens kontra Ausztria, App. no. 9815/82 (1986. július 8.), 26.

¹⁰¹ KOZŁOWSKI (2006): 141.

¹⁰² Uo., 141.

¹⁰³ Saját szerkesztés.

A #Pizzagate-ügyben több személy hírneve is érintett, így Hillary Clinton, John Podesta, Tony Podesta, a Demokrata Párt más jelentős tagjai, James Alefanti, más étteremtulajdonosok és boltosok, sőt a Comet Ping Pong és a botrányban érintett más helyi vállalkozások is. Ami a Hillary Clintonnal kapcsolatban kialakult kifejezéseket illeti, azok a legvédelettebbek. Ha tehát a Hillary Clintonnal kapcsolatos történeteket annyira sértőnek találták, hogy azok egyetlen országban sem élvezhetnek politikai szólásként védelmet, akkor a többiekkel kapcsolatban megfogalmazott valamennyi jóhírnevet sértő megjegyzés sem tartozik majd a védett szólás körébe.

Jelen alfejezetnek tehát a következő kérdésre kell választ adnia: ha a nemzeti bíróság jóhírnevet sértőnek találná a Hillary Clintonra vonatkozó #Pizzagate-történeteket, és a szerzők az EJEB előtt eljárást kezdeményeznének az állam ellen a véleménynyilvánítás szabadságához való joguk megsértése miatt, akkor az EJEB helyt adna-e keresetüknek, és megállapítaná-e az EJEE 10. cikkének megsértését.

A deepfake, mint az EJEE 10. cikke által nem védett megnyilvánulás

Az Axel Springer AG kontra Németország és a Von Hannover kontra Németország (2. sz.) ügyekben az EJEB több olyan kritériumot is meghatározott, amelyet figyelembe kell venni a véleménynyilvánítás szabadságához való jog és a magánélet tiszteletben tartásához való jog egymással szemben való mérlegelése során. Ezen kritériumok közé – többek között – az alábbiak tartoznak:

- a) a hozzájárulás mértéke egy közérdekű társadalmi vitához;
- b) az érintett személy közszereplői mivolta;
- c) a publikáció tartalma, formája és következményei; és
- d) az információ megszerzésének módja és annak valóságtartalma.¹⁰⁴

a) A hozzájárulás mértéke egy közérdekű társadalmi vitához

A közérdekű vagy politikai kérdésekkel kapcsolatos megnyilvánulások főszabálya szerint a véleménynyilvánítás szabadságának magas fokú védelmét élvezik,¹⁰⁵ mivel a közérdekű és politikai kérdésekkel összefüggő információk és gondolatok szabad közlése és megosztása elengedhetetlen egy demokratikus társadalom működéséhez. Ebből következően ezen esetekben a nemzeti bíróságoknak és hatóságoknak biztosított mérlegelési szabadság különösen szűk. Az, hogy egy megnyilvánulás közérdekű kérdést érint-e, vagy sem, az érintett téma és a közlés tartalmának szélesebb körű értékelésétől függ.¹⁰⁶ A közbeszéd (*public discourse*)

¹⁰⁴ Axel Springer AG kontra Németország, App. no. 39954/08 (2012. február 7.), 89–95., Von Hannover kontra Németország (2. sz.), App. no. 40660/08 és 60641/08 (2012. február 7.), 108–113.

¹⁰⁵ Axel Springer AG kontra Németország, App. no. 39954/08 (2012. február 7.), 90.; Morice kontra Franciaország, App. no. 29369/10 (2015. április 23.), 125.

¹⁰⁶ Tønsbergs Blad AS és Haukom kontra Norvégia, App. no. 510/04 (2007. március 1.), 87.; Fressoz és Roire kontra Franciaország, App. no. 29183/95 (1999. január 21.), 50.; Bladet Tromsø és Stensaas kontra Norvégia, App. no. 29183/95 (1999. május 20.), 50.; Björk Eiðsdóttir kontra Izland, App. no. 46443/09 (2012. július 10.), 67.; Medžlis Islamske Zajednice Brčko és társai kontra Bosznia és Hercegovina, App. no. 17224/11 (2017. június 27.), 92.

magában foglalja a közérdekű ügyek szabad megvitatását, különösen, de nem kizárólagosan a hatalom gyakorlóinak, illetve az ilyen pozíciókért indulóknak bírálatát.¹⁰⁷ Az EJEB joggyakorlata értelmében továbbá a választások során létfontosságú valamennyi vélemény (annak tartalmától függetlenül) szabad áramlásának biztosítása. A véleménynyilvánítás szabadsága ugyanis az egyik alapfeltétel annak biztosításához, hogy a nép a véleményét szabadon kifejezhesse a parlamenti választások során.¹⁰⁸

Különbség van azonban a közérdekű vitához hozzájáruló közlés és az olyan megnyilvánulás között, amely kizárólag a nyilvánosság kíváncsiságát hivatott kielégíteni az egyén magánéletének részleteivel kapcsolatban.¹⁰⁹ Az EJEB ítélkezési gyakorlata szerint ahhoz, hogy egy közlés az EJEE 10. cikke szerinti védelemben részesüljön, nem elegendő, hogy annak tárgya közérdekű, ugyanis a közlés tartalmának alkalmasnak kell lennie arra is, hogy hozzájáruljon az adott kérdésről folytatott nyilvános vitához.¹¹⁰ A Stoll kontra Svájc ügyben az EJEB amellet foglalt állást, hogy a hamis állítások nem járulnak hozzá az általános vitához, következésképpen nem tartoznak a közérdekűség körébe.¹¹¹ Ezzel összefüggésben az EJEB azt is kimondta továbbá, hogy minél súlyosabb vagy komolyabb egy állítás, annak annál szilárdabb ténybeli alapokon kell nyugodnia.¹¹²

Felmerül tehát a kérdés, hogy vajon a Hillary Clintont ábrázoló deepfake mekkora mértékben járul hozzá a közérdekű társadalmi vitához. A #Pizzagate eredetileg a 2016-os amerikai elnökválasztás során jelent meg. A nyilvánosságnak joga van tudni arról, hogy egy elnökjelölt érintett-e bármilyen bűncselekményben annak érdekében, hogy a választás napján valamennyi választó megalapozott döntést hozhasson. Egy amerikai elnökjelöltet bűncselekmény elkövetésével vádoló megnyilvánulás tehát vitathatatlanul hozzájárul a közérdekű társadalmi vitához még abban az esetben is, ha a bűncselekmény elkövetése nem bizonyított. A kérdéses felvétel azonban a választások után évekkel később jelent meg, mikorra Hillary Clinton nem csupán visszavonult már a politikai élettől, de a #Pizzagate történet is megcáfolásra került. A felvétel célja tehát kizárólag a valóság manipulálása lehetett, amely nemhogy nem járul hozzá a közérdekű társadalmi vitához, hanem – álláspontom szerint – épp ellenkezőleg: tudatosan rombolja azt.

¹⁰⁷ KOZŁOWSKI (2006): 142.; Feldek kontra Szlovákia, App. no. 29032/95 (2001. július 12.), 74.; Brasilier kontra Franciaország, App. no. 71343/01 (2006. április 11.), 41.; Gutiérrez Suárez kontra Spanyolország, App. no. 16023/07 (2010. június 1.), 26.

¹⁰⁸ Bowman kontra Egyesült Királyság, App. no. 24839/94 (1998. február 19.), 42.; Incal kontra Törökország, App. no. 22678/93 (1998. június 9.), 46.; TV Vest AS és Rogaland Pensjonistparti kontra Norvégia, App. no. 21132/05 (2008. december 11.), 61.

¹⁰⁹ Von Hannover kontra Németország (1. sz.), App. no. 59320/00 (2004. június 24.), 65.; Société Prisma Presse kontra Franciaország, App. no. 66910/01 és 71612/01 (2003. július 1.); Mosley kontra Egyesült Királyság, App. no. 48009/08 (2011. május 10.), 11.

¹¹⁰ Bédat kontra Svájc, App. no. 56925/08 (2016. március 29.), 64.; Uitz (2021): 248–258.

¹¹¹ Stoll kontra Svájc, App. no. 69698/01 (2007. december 10.), 103.; Fressoz és Roire kontra Franciaország, App. no. 29183/95 (1999. január 21.), 54–55.

¹¹² Pedersen és Baadsgaard kontra Dánia, App. no. 49017/99 (2004. december 17.), 78.; Ólafsson kontra Izland, App. no. 58493/13 (2017. március 16.), 53.; Björk Eiðsdóttir kontra Izland, App. no. 46443/09 (2012. július 10.), 71.

b) Az érintett személy közszereplői mivolta

Az EJEB a magyar joggyakorlathoz hasonlóan elismeri, hogy az elfogadható kritika határai tágabbak a közszereplőkkel kapcsolatban, mint a magánszemélyek esetében. „Az utóbbival ellentétben az előbbi elkerülhetetlenül és tudatosan kiteszi magát annak, hogy minden szavát és tettét alaposan megvizsgálják mind az újságírók, mind a nagyközönség, és így következőképpen nagyobb fokú toleranciát kell tanúsítania.”¹¹³ A politikai beszéd tehát az EJEB értelmezése szerint „kiemelt védelmet élvez”, mivel a politikai vélemények szabad kifejtése a demokratikus társadalom egyik alapköve.¹¹⁴

A közszereplők nyilvános sértegetése vagy gúnyolása szintén az EJEE 10. cikke által védett, mivel a véleménynyilvánítás szabadsága nemcsak a kedvezően fogadott vagy nem sértőnek vagy közömbösnek tekintett megnyilvánulásokra vonatkozik, hanem azokra is, amelyek sértőek, megdöbbsentőek vagy zavaróak.¹¹⁵ Követkézőképpen a túlzás, a közszereplők provokálása vagy akár a határokat nem ismerő kijelentések is megengedettek, de csak bizonyos mértékig.¹¹⁶ Amint azt az EJEB a Jon Gaunt kontra Egyesült Királyság-ügyben megállapította, bizonyos fokú túlzás, sőt provokáció is megengedett, amennyiben az nem terjed ki „nyilvánvalóan sértő nyelvezetre” vagy „indokolatlan személyes támadásra”.¹¹⁷

A fentebb leírtakból következően tehát az EJEE 8. cikke csak akkor alkalmazható, ha a személy jóhírnevét sértő támadás súlyossága elér egy bizonyos küszöböt,¹¹⁸ és oly módon valósul meg, amely ténylegesen sérti az érintett személy magánéletének tiszteletben tartásához való jog élvezetét.¹¹⁹ Az EJEB ezen megállapítását a Tamiz kontra Egyesült Királyság-ügyben is megismételte,¹²⁰ amikor kimondta, hogy bár az online hozzászólások között sok sértő vagy akár rágalmazó tartalom is előfordulhat, ezek túlnyomó többsége valószínűsíthetően túlságosan jelentéktelen, illetve olyan korlátozott közönséghez jut el, hogy nem képes jelentős kárt okozni egy másik személy jóhírnevében.¹²¹

Azonban az, hogy a közszereplőknek nagyobb fokú toleranciát kell tanúsítaniuk, nem jelenti azt, hogy hírnevük nem érdemel semmiféle védelmet az EJEE 8. cikke alapján. A Lingens kontra Ausztria-ügyben az EJEB például kiemelte, hogy a jóhírnév védelme a politikusokra is kiterjed, még akkor is, ha nem magánszemélyként járnak el.¹²² Az ilyen védelem követelményeit azonban a politikai kérdések nyílt megvitatásához fűződő érdekekkel

¹¹³ KOZŁOWSKI (2006): 142.

¹¹⁴ Uo., 142.

¹¹⁵ Handyside kontra Egyesült Királyság, App. no. 5493/72 (1976. december 7.), 49.; Oberschlick kontra Ausztria (2. sz.), App. no. 20834/92 (1997. július 1.), 29.; Lopes Gomes Da Silva kontra Portugália, App. no. 37698/97 (2000. szeptember 28.), 101.

¹¹⁶ Willem kontra Franciaország, App. no. 10883/05 (2009. július 16.), 33.

¹¹⁷ Jon Gaunt kontra Egyesült Királyság, App. no. 26448/12 (2016. szeptember 6.), 10.

¹¹⁸ Axel Springer AG kontra Németország, App. no. 39954/08 (2012. február 7.), 83.; Tamiz kontra Egyesült Királyság, App. no. 3877/14 (2017. szeptember 19.), 80.

¹¹⁹ Axel Springer AG kontra Németország, App. no. 39954/08 (2012. február 7.), 83.; Medžlis Islamske Zajednice Brčko és társai kontra Bosznia és Hercegovina, App. no. 17224/11 (2017. június 27.), 112.

¹²⁰ Tamiz kontra Egyesült Királyság, App. no. 3877/14 (2017. szeptember 19.), 80.

¹²¹ European Court of Human Rights Registry: Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence. Strasbourg, Council of Europe/European Court of Human Rights, 2025, 61. o.

¹²² Lingens kontra Ausztria, App. no. 9815/82 (1986. július 8.), 26.

szemben kell mérlegelni.¹²³ Az Egill Einarsson kontra Izland-ügyben ugyanis az EJEB megállapította, hogy még a közéleti vitákban aktívan részt vevő, ellentmondásos megítélésű közszereplőknek sem kell elviselniük, hogy őket nyilvánosan erőszakos bűncselekményekkel, például nemi erőszakkal vádolják anélkül, hogy ezeket az állításokat tényekkel alátámasztanák.¹²⁴

Mindezek alapján tehát megállapítható, hogy bár Hillary Clintonnak mint közszereplőnek kötelessége volt eltűrni a túlzó, vagy akár provokatív kritikát is, ezen kötelezettsége nem terjedt ki arra, hogy őt szándékosan hamisított 'bizonyítékokon' nyugvó gyermekkereskedelemmel és pedofilhálózat működtetésével vádolják. Az Emberi Jogok Európai Egyezménye 8. cikkének védelmi köre ilyen esetekben kiterjed a közszereplők jóhírnevének védelmére is, még akkor is, ha ez szükségszerűen a véleménynyilvánítás szabadságának korlátozásához vezet.

c) A publikáció tartalma, formája és következményei

A magyar AB gyakorlatához hasonlóan az EJEB joggyakorlata szerint is különbséget kell tenni a tények (*facts*) és az értékítéletek (*valuable judgements*) között, mivel a tények léte bizonyítható, míg az értékítéletek igazságtartalma nem. Ezért a jóhírnevet sértő értékítélet igazságtartalmának bizonyítása nem követelhető meg, hiszen az a véleménynyilvánítás szabadságát sértené.¹²⁵

Ez azonban nem jelenti azt, hogy az értékítélet abszolút védelem alatt állna. Az EJEB döntései értelmében pusztán az, hogy egy értékítélet igazságtartalmát nem kell bizonyítani, nem jelenti azt, hogy az alaptalan vádak a szólásszabadság védelme alatt állnának. Amint azt az EJEB többször megismételte, még abban az esetben is, ha egy kijelentés értékítéletnek minősül, a véleménynyilvánítás szabadsága arányosan korlátozható annak függvényében, hogy a kifogásolt kijelentésnek van-e elegendő ténybeli alapja. Nem élvezhet ugyanis védelmet az olyan túlzó értékítélet, amelynek semmilyen ténybeli alapja nincs.¹²⁶

Bár az értékítélet ténybeli alapját feltétlenül figyelembe kell venni, az annak tulajdonítandó súlya a megjegyzés jellegétől és az értékítélet kontextusától függ. Például a Thorgeirson kontra Izland-ügyben az EJEB úgy ítélte meg, hogy „bár a cikkek nagymértékben támaszkodtak mások pletykáira, történeteire és nyilatkozataira, azok fontos közérdekű ügyre (azaz a rendőri brutalitásra) vonatkoztak, és így az újságírótól nem lehet megkövetelni, hogy bizonyítsa ezen állítások ténybeli alapját.”¹²⁷ Másrészt a Salumäki kontra Finnország-ügyben az EJEB arra a következtetésre jutott, hogy egy olyan újságcikk, amely egy ismert üzletembert minden tényszerű alap nélkül egy gyilkossággal hozott összefüggésbe, nem részesülhet az EJEE 10. cikke szerinti védelemben, mivel az érintett állítás hamis volt, ellentmondásos információkra épült, és súlyosan sértette az üzletember jóhírnevét.¹²⁸

¹²³ MACOVEI (2004): 50.

¹²⁴ Egill Einarsson kontra Izland, App. no. 24703/15 (2017. november 7.), 52.

¹²⁵ Lingens kontra Ausztria, App. no. 9815/82 (1986. július 8.), 46.

¹²⁶ Jerusalem kontra Ausztria, App. no. 26958/95 (2001. február 27.), 43.; De Haes és Gijssels kontra Belgium, App. no. 19983/92 (1997. február 24.), 47.; Veraart kontra Hollandia, App. no. 10807/04 (2006. november 30.), 55.

¹²⁷ McGONAGLE (2016): 27.

¹²⁸ Salumäki kontra Finnország, App. no. 23605/09 (2014. április 29.), 59.

Ahogy az korábban már részletesen kifejtettem, álláspontom szerint, a Hillary Clintonról készített deepfake hamis tényállításnak minősül. Még abban az esetben is, ha az EJEB a kérdéses felvételt értékítéletnek tekintené, az mint a közrend megzavarása érdekében gyártott hamis közlés, feltehetően nem részesülne az EJEE 10. cikke által biztosított védelemben.

A véleménynyilvánítás szabadsága magában foglalja a túlzások vagy akár a provokáció megengedett mértékét is. A Ziembinski kontra Lengyelország (2. sz.)-ügyben az EJEB például kimondta, hogy bár a közérdekű nyilvános vitában részt vevő egyén nem léphet túl bizonyos határokat, mégis megengedett számára, hogy olyan véleményt formáljon, amely túlzásnak, provokációnak vagy akár mértéktelen kijelentéseknek minősül.¹²⁹ „A túlzás és a provokáció a szatíra tipikus jellemzői, amelyet a Bíróság a művészi kifejezés és a társadalmi kommentár egyik formájának tekint, és a valóság eltúlzására és elferdítésre való hajlama révén provokációra és felzaklatásra törekszik, tehát hozzájárul a nyilvános vitához.”¹³⁰

Az EJEB elismeri, hogy mind a szatíra, mind pedig az ironia fontos szerepet játszik a közérdekű kérdések nyílt megvitatásában, ami egy demokratikus társadalom nélkülözhetetlen jellemzője.¹³¹ Következésképpen a tiszteletlen szatíra és az ironikus kifejezésmód, amely nem minősül sértésnek, illetve nem tekinthető indokolatlanul sértőnek,¹³² minden bizonynyal az EJEE védelmét élvezi.

A szatirikus tartalom elfogadható és elfogadhatatlan tartalma közötti egyensúly azonban esetről esetre vizsgálendő. A méltányos egyensúly megteremtése érdekében az EJEB például figyelembe veszi a szatíra stílusát, valamint azt is, hogy a szatíra hozzájárul-e a közérdekű vitához, vagy sem. A Tusalp kontra Törökország-ügyben például az EJEB megállapította, hogy bár a sértő kifejezésmód kívül eshet a véleménynyilvánítás szabadságának védelmén, ha az szándékos becsmérésnek minősül, vagy ha a sértő kijelentés kizárólagos célja a sértés, a vulgáris kifejezések használata önmagában nem döntő a sértő kifejezés megítélése szempontjából, mivel az akár pusztán stilisztikai célokat is szolgálhat.¹³³ Továbbá az EJEE 8. cikkének alkalmazását csak akkor válthatja ki a szatirikus tartalom, ha a személyes becsület és jóhírnév elleni támadás eléri egy bizonyos súlyossági szintet, és olyan módon, hogy az sérti a magánélet tiszteletben tartásához való jog személyes élvezetét.¹³⁴ A Nikowitz és Verlagsgruppe News Gmh kontra Ausztria-ügyben hozott ítéletében az EJEB bevezette az átlagos olvasó fogalmát is, hogy különbséget tegyen a különböző típusú szatirikus anyagok között.¹³⁵ Az átlagos olvasónak képesnek kell lennie felfogni a szöveg szatirikus jellegét és különösen a történet humoros elemét, hogy a tartalom szatírának minősüljön.¹³⁶

¹²⁹ Dąbrowski kontra Lengyelország, App. no. 18235/02 (2006. december 19.), 35.; Uj kontra Magyarország, App. no. 23954/10 (2011. július 19.), 24.; Novaya Gazeta és Borodyanskiy kontra Oroszország, App. no. 14087/08 (2013. március 28.), 29.; Marian Maciejewski kontra Lengyelország, App. no. 34447/05 (2015. január 13.), 79.

¹³⁰ McGONAGLE (2016): 21.

¹³¹ Vereinigung Bildender Künstler kontra Ausztria, App. no. 68354/01 (2007. április 5.), 33.; European Court of Human Rights Research Division (2015): 20.; GODIOLI et al. (2025).

¹³² Riolo kontra Olaszország, App. no. 42211/07 (2008. július 17.), 68.

¹³³ Tusalp kontra Törökország, App. no. 32131/08 (2012. február 21.), 48.

¹³⁴ Sousa Goucha kontra Portugália, App. no. 70434/12 (2016. március 22.), 25.

¹³⁵ Nikowitz és Verlagsgruppe News GmbH kontra Ausztria, App. no. 5266/03 (2007. február 22.), 24–26.

¹³⁶ Uo., 25.

A szóban forgó deepfake nem minősülhet szatírának, és túlzó és provokatív jellege nem tekinthető csupán valamely művészi kifejezés lényeges elemének. A #Pizzagate-ügy nem járult hozzá az általános társadalmi vitához, és indokolatlanul sértő jellege meghaladta a szatírával szemben támasztott stilisztikai követelményeket. Továbbá az a körülmény, hogy a #Pizzagate-elméletet terjesztő kijelentések végső soron fegyveres erőszakhoz vezettek, azt támasztja alá, hogy a közlés potenciális szatirikus vagy ironikus jellege a befogadók számára nem volt felismerhető.

d) Az információ megszerzésének módja és annak valóságtartalma

Az EJEB gyakorlata szerint az információ megszerzésének módja és annak valóságtartalma is fontos tényező, amelyet figyelembe kell venni az EJEE 8. és 10. cikke közötti méltányos egyensúly megteremtése során.¹³⁷ Ebben a tekintetben ki kell emelni, hogy a #Pizzagate-történetek mind hamisak voltak, és megbízható forrás hiányában csak keresztreferenciát adtak egymásnak.

Összefoglalva, az EJEB joggyakorlata szerint a Hillary Clintonról készített deepfake-kép nem minősülhetne a véleménynyilvánítás szabadsága által védett közlésnek mivel az (i) nem járult hozzá az általános közérdekű vitához, (ii) annyira sértő volt, hogy azt még egy közszereplő sem volt köteles eltűrni, (iii) nem minősült értékítéletnek, csak hamis tényállításnak, és (iv) a valóságot hamis színben tüntette fel, megbízható forrás nélkül.

¹³⁷ Axel Springer AG kontra Németország, App. no. 39954/08 (2012. február 7.), 93.

7. A tárhelyszolgáltatói felelősség szabályozása

A 6. fejezet részletesen vizsgálta, hogy a képmáshoz való jog miként érvényesül az online térben. A 6.1. alfejezet rámutatott arra, hogy a közösségimédia-platformok strukturálisan alkalmatlanok a képmáshoz való jog védelmére, hiszen úgy ösztönöznek a fényképek és videók tömeges megosztására, hogy a képmás feletti rendelkezési jogosultságot nem a felvételen szereplő, hanem az érintett tartalmat megosztó felhasználó kezébe helyezik. A 6.2. és 6.3. alfejezetek továbbá a képmáshoz való jog megsértésének egy másik tipikus esetét, a deepfake-et is részletesen vizsgálták a volt amerikai külügyminiszter hamisított képének jogi elemzésén keresztül.

A Ptk. 6:2. § (1) bekezdése értelmében a személyiségi jog megsértése kötelelemkeletkeztető tény. A Ptk. 2:51–2:53. §-ai továbbá felsorolják a személyiségi jogsérelem – így a képmáshoz való jog megsértése – esetén az érintett megillető követelések körét (pl. sérelemdíj, kártérítés, jogsértés megállapítására irányuló kérelem). Jogosan merülhet fel tehát a kérdés, hogy vajon a képmáshoz való jog megsértése miatt felmerülő kártérítési igény vajon kivel szemben érvényesíthető.

Első ránézésre logikusnak tűnhet, hogy a képmáshoz való jog megsértéséért elsődlegesen a tartalom szerzője vonható felelősségre. A szerzők felelősségrevonása azonban számos okból kifolyólag jelentős nehézségekbe ütközhet. A sértettnek ugyanis, mielőtt érdemben bármilyen jogi igényt érvényesíthetne a szerzővel szemben, sikeresen meg kell küzdenie az alábbi akadályokkal:

- az alperes azonosításának problematikája (anonimitás);
- több potenciális szerző/jogsértő létezése;
- a több ország joghatóságának összeütközése és a kollíziós jog problémája;
- az alperesek vagyonának hiánya a megfelelő kártérítés nyújtásához; és
- az a kihívás, hogy ha egy illegális tartalom egyszer már felkerült az internetre, akkor szinte lehetetlen azt véglegesen eltávolítani.¹

Emily Laidlaw munkájában ezt a jelenséget nagy volumenű, alacsony értékű problémának (*high-volume, low-value problem*) nevezi, amelyen azt érti, hogy nagy mennyiségű jogellenes online tartalom van, de a legtöbb igényt nem éri meg peresíteni, tekintettel az alacsony potenciális kártérítésre és a jogi bonyolultságra.²

¹ LAIDLAW (2017): 17–18.

² Uo., 19.

Mivel az elsődleges jogsértők, a szerzők perlése az esetek jelentős részében nem reális megoldás a felperes számára, a jogi felelősség kiterjesztése a jogellenes tartalmat közvetítőkre, a másodlagos jogsértőkre logikusan következik a hatékony jogorvoslat biztosítására irányuló jogpolitikai igényből:³

- a közvetítő szolgáltatók megkönnyítik a jogellenes tartalmak terjesztését, és nélkülük a szerzők, illetve a megosztók (*reposters*) nem tudnának a jogsértő magatartásban részt venni, kárt okozni;
- a közvetítő szolgáltatók esetében az anonimitás nem jelent valódi problémát, mivel a felhasználókkal ellentétben ezen szolgáltatók jól ismert és elérhető entitások;
- a jogérvényesítési költségek sokkal alacsonyabbak, mivel nincs szükség a szerzők azonosítására, és ahelyett, hogy több száz eljárást kellene kezdeményezni több száz szerző, megosztó ellen, a felperes egyetlen ügyben kaphat megfelelő kártérítést;
- az alperes pénzügyi helyzetével kapcsolatos aggályok általában nem merülnek fel közvetítő szolgáltatók esetében; és
- a magánszemélyektől eltérően a közvetítő szolgáltatók nem csak a felperes által kért jogorvoslatot (pl. valamennyi képmáshoz való jogot sértő tartalom törlését) tudnák garantálni, hanem hatékony megoldást is tudnának nyújtani a jövőbeli jogsértések megelőzésére.⁴

Másrészről azonban a közvetítő szolgáltatók (ahogyan arra a nevük is utal) nem vesznek részt a jogsértő tartalmak elkészítésében, azokat pusztán tárolják, illetve a nyilvánosság felé közvetítik. Ebből következően ezen másodlagos jogsértők felelősségre vonása a gyakorlatban elérhetetlen és/vagy aránytalan megoldásnak bizonyulhat. Mindezekon felül a közvetítő szolgáltatók felelősségre vonása az általuk közvetített tartalmakért súlyos következményekkel járhat a szólásszabadságra nézve.⁵

Jelen fejezet célja tehát annak vizsgálata, hogy a közvetítő szolgáltatók felelősségre vonhatók-e az általuk tárolt és nyilvánosság felé közvetített jogsértő tartalmakért, és ha igen, akkor milyen szabályozás alapján, milyen szólásszabadsági keretek között. Ezen cél elérése érdekében a felmerülő jogi kérdéseket a Hillary Clintonról készült deepfake jogi elemzése keretében fogom megválaszolni.

7.1. A tárhelyszolgáltatók az Eker. irányelv tükrében

Az Eker. irányelvet 2000. június 8-án fogadták el, és 2000. július 17-én lépett hatályba. Az irányelv elfogadásának több célja volt: (i) egy világos és kellően átfogó szabályozási keret biztosítása az elektronikus kereskedelem belső piacon megvalósuló aspektusainak rendezése érdekében; és (ii) jogi keret megteremtése az információs társadalommal összefüggő szolgáltatások tagállamok közötti szabad mozgásának biztosítása érdekében.⁶ Az Eker. irányelv

³ SCOTT (2017): 228.

⁴ RIORDAN (2016): 57.

⁵ Uo., 228.

⁶ Eker. irányelv, 1. cikk.

„az akkori problémák megoldására törekedett, amelyeket a digitalizáció egyre gyorsabb fejlődése váltott ki. Miközben a modern társadalom úgynevezett információs társadalommá alakult át, ennek megfelelően gazdasági tevékenységek új formái, például az online kereskedelem és az online kutatási eszközök, amelyeket együttesen »információs társadalmi szolgáltatásoknak« nevezünk, alakultak ki.”⁷

Az Eker. irányelv volt az első olyan európai uniós szinten elfogadott jogi aktus, amely az információs társadalommal összefüggő szolgáltatók (*information society service provider*, ISSP) magatartását szabályozta. Az ISSP státusz minden olyan természetes vagy jogi személyre vonatkozott, aki vagy amely valamilyen szolgáltatást nyújtott, általában díjazás ellenében, távolról, elektronikus úton és a szolgáltatás igénybe vevőjének egyéni kérésére. Az információs társadalommal összefüggő szolgáltatások közé tartoztak azok a szolgáltatások is, amelyekért a szolgáltatókat nem maguk a felhasználók, hanem a honlapokon elhelyezett hirdetésekkel származó bevételekkel fizettek.⁸

Az Eker. irányelv 4. szakasza az úgynevezett közvetítő szolgáltatók felelősségét szabályozta.⁹ Az Eker. irányelv szerkezete és megfogalmazása, valamint az EUB ítélkezési gyakorlata¹⁰ értelmében a közvetítő szolgáltatók az ISSP-k egy alkategóriáját képezték, és három információs társadalommal összefüggő szolgáltatást öleltek fel: (i) egyszerű továbbítás (*mere conduit*); (ii) tárhelyszolgáltatás (*hosting*); és (iii) gyorsítótárolóban történő rögzítés (*caching*). A *cachingszolgáltatók* olyan ISSP-kre utaltak, amelyek a szolgáltatás igénybe vevője által küldött információnak hírközlő hálózaton keresztül történő továbbítását biztosították.¹¹ Tárhelyszolgáltatókon olyan ISSP-k voltak értendők, amelyek információs társadalommal összefüggő szolgáltatásai a szolgáltatás címzettje által biztosított információk tárolásából álltak.¹² A *mere conduit* kategóriában pedig olyan ISSP-k voltak, amelyek információs társadalommal összefüggő szolgáltatásai a szolgáltatás igénybe vevője által küldött információnak hírközlő hálózaton keresztül történő továbbítását, vagy a hírközlő hálózathoz való hozzáférés biztosítását foglalták magukban.¹³

Az Eker. irányelv (42) preambulumbekzdése az Eker. irányelv 4. szakaszának rendelkezéseit „az irányelvben megállapított felelősség alóli mentességekként” említette.¹⁴ Az Eker. irányelv tehát egy olyan bináris felelősségi rendszert hozott létre, amely különbséget tesz egy részről a közvetítő szolgáltatók (amelyek a harmadik személyek által rendelkezésre

⁷ SCHULTE-NÖLKE et al. (2020): 14.

⁸ C-291/13, Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi és Giorgos Sertis, ECLI:EU:C:2014:2209, 30.; C-352/85, Bond van Adverteerders és társai kontra Holland Állam, EU:C:1988:196, 16.; C-51/96 és C-191/97, Christelle Delière kontra Ligue francophone de judo et disciplines associées ASBL, Ligue belge de judo ASBL, Union européenne de judo (C-51/96) és François Pacquée, EU:C:2000:199, 56.; C-484/14 Tobias, Mc Fadden kontra Sony Music Entertainment Germany GmbH, EU:C:2016:689, 41–42.

⁹ WENDEHORST (2016)

¹⁰ C-291/13, Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi és Giorgos Sertis, ECLI:EU:C:2014:2209, 45.

¹¹ Eker. irányelv 13. cikk (1) bek.

¹² Eker. irányelv 14. cikk (1) bek.

¹³ Eker. irányelv 12. cikk (1) bek.

¹⁴ MONTI (2024): 444.

bocsátott továbbított, ideiglenesen tárolt vagy tárolt tartalom tekintetében mentesülnek a felelősség alól), másrészt pedig az egyéb ISSP-k (amelyek főszabály szerint felelősségre vonhatók a jogellenes tartalomért) között.¹⁵ Ezen értelmezést az EUB többször is megerősítette: például a Google France és Google-ügyben a bíróság megállapította, hogy „annak ellenőrzése céljából, hogy a reklámszolgáltatás nyújtójának felelőssége korlátozható-e (...), meg kell vizsgálni, hogy az említett információs társadalommal összefüggő szolgáltatás nyújtója”¹⁶ közvetítő szolgáltatóként járt-e el. Amennyiben igen, úgy a közvetítő szolgáltató főszabály szerint nem tartozott felelősséggel az általa közvetített jogellenes tartalomért, kivéve, ha az Eker. irányelv 12–14. cikkeiben meghatározott feltételek fennálltak. A tárhelyszolgáltatók esetében például ez azt jelentette, hogy a tárhelyszolgáltató nem tartozott felelősséggel az általa tárolt jogellenes tartalomért, kivéve, ha (i) arról tényleges tudomása volt; vagy (ii) a jogellenes tartalomról való tudomásszerzést követően nem intézkedett haladéktalanul annak eltávolítása érdekében.¹⁷

A kétezres években tehát az ISSP-k felelőssége a besorolásuktól függött. A közösségi-média-platformok tekintetében azonban e bináris rendszer gyakorlati alkalmazása kiemelkedően nehézkesnek bizonyult, mivel az irányelv nem definiálta e szolgáltatókat és nem rendelkezett azok egyértelmű besorolásáról.¹⁸

7.2. A tárhelyszolgáltatók felelősségének megítélése az EUB joggyakorlata szemszögéből

Mivel az Eker. irányelv hallgatott a platformok besorolásáról, az EUB-ra maradt azon feladat, hogy véleményt alkosson és így útmutatást adjon a tekintetben, hogy a platformok a tárhelyszolgáltatók közé sorolhatók-e – ahogyan azt a közösségi-média-szolgáltatók kezdettől fogva állították.¹⁹

Az EUB a helyzet jogi értékelése során egy jelentős dilemmával szembesült. Egyrésztől az Eker. irányelv (42) preambulumbekzdése szerint az ISSP csak akkor tekinthető tárhelyszolgáltatónak, ha tevékenysége pusztán technikai, automatikus és passzív jellegű, és ezért az internetszolgáltató nem ismeri a tárolt információkat, és nem is ellenőrzi azokat. Az ISSP tehát csak akkor tartozhat az Eker. irányelv 14. cikkének hatálya alá, ha tevékenysége nem terjed túl a tároláson. Másrésztől azonban a gyakorlatban a közvetítő szolgáltatók tevékenysége ritkán korlátozódik pusztán harmadik személyek által rendelkezésre bocsátott adatok tárolására (pl. számítógépes adathordozón történő rögzítésére), hiszen ezen szolgáltatók általában a tároláson túl hozzáférést és keresési funkciókat is biztosítanak a felhasználók számára. Ezen túlmenően a közvetítő szolgáltatók általában lehetővé teszik a felhasználók

¹⁵ GOSZTONYI (2021)

¹⁶ Google France SARL és Google Inc. kontra Louis Vuitton Malletier SA (C-236/08), Google France SARL kontra Viaticum SA és Luteciel SARL (C-237/08) és Google France SARL kontra Centre national de recherche en relations humaines (CNRRH) SARL és társai (C-238/08), ECLI:EU:C:2010:159, 114.

¹⁷ GOSZTONYI (2022c): 21–22.

¹⁸ VALCKE–LENAERTS (2010): 125.

¹⁹ Ezzel kapcsolatban kiemelendő, hogy a magyar joggyakorlattal összefüggésben Szikora Tamás megállapítja, hogy a személyiségi jogi perekben sem az Ekv. tv., sem a Ptk. „alkalmazása nem tekinthető egységesnek és következetesnek” (SZIKORA [2024b]).

számára a tartalom megosztását, értékelését és/vagy szerkesztését, valamint személyre szabott szolgáltatásokat nyújtának azáltal, hogy azonosítják és optimalizálják a látogatók számára releváns tartalmakat.²⁰

Mivel az Eker. irányelv technológiasemleges szemlélettel készült, az EUB tágan értelmezte a tárolás fogalmát, és ezért a hálózati szintű szolgáltatás bizonyos formáit is mentesítette.²¹ A felelősséget kizáró tárolás és a felelősséget magával vonó tartalmamegosztás közötti határvonalat annak megítélésével lehetne azonosítani, hogy az ISSP aktív vagy passzív szerepet vállalt-e az információ terjesztésében. Az EUB szerint két fő tényezőt kell figyelembe venni a tárhelyszolgáltatók egyéb ISSP-ktől való megkülönböztetése érdekében: (i) a közvetítő szolgáltató által nyújtott szolgáltatás karakterjegyeit,²² és (ii) a szolgáltató tudattartamát.²³

A Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd és társai-ügyben az EUB kimondta, hogy pusztán az a tény, hogy egy információs társadalommal összefüggő szolgáltatás fizetéshez kötött, hogy a szolgáltató határozza meg a fizetési feltételeket vagy hogy általános tájékoztatást nyújt ügyfeleinek, nem eredményezheti azt, hogy a platformok nem minősülnek tárhelyszolgáltatóknak.²⁴ Ugyanebben az ügyben az EUB ugyanakkor arra a következtetésre is jutott, hogy az a tény, hogy a szóban forgó ISSP egy újságkiadó vállalat volt, amely elektronikus formátumban tette közzé az újságjának online változatát, elegendő ahhoz, hogy az ISSP tudomása az általa közzétett információkról feltételezhető legyen.²⁵

A L'Oréal és társai-ügyben meghozott EUB ítélet azt is megállapította, hogy mivel az eBay részletes segítséget nyújtott az eladóknak eladásaik optimalizálásához, saját online áruházai létrehozásához, illetve az értékesítések előmozdításához és növeléséhez [beleértve a piacterén értékesített termékek egy részének keresőmotor-üzemeltetők (pl. Google) segítségével történő reklámozását],²⁶ az eBay nem volt olyan közvetítő szolgáltatónak tekinthető, amely semleges pozíciót foglalt el az érintett, eladóként tevékenykedő ügyfelei és a lehetséges vásárlók között. Az eBay tehát aktív szerepet játszott, és ismerte, valamint kezelte az eladási ajánlatokra vonatkozó adatokat.²⁷ Az EUB döntése tehát arra utalt, hogy egy olyan technikai és automatikus folyamat, amelynek célja bizonyos tartalmak népszerűsítése vagy optimalizálása, nem tekinthető tárolási tevékenységnek, függetlenül attól, hogy ezen folyamatot semlegesen alkalmazzák a tárolt információkra.

Az EUB ugyanakkor az újabb döntéseiben már akként foglalt állást, hogy a tárolt információkra semlegesen alkalmazott technikai és automatikus folyamatokat tárolási tevé-

²⁰ RIORDAN (2016): 401.

²¹ Uo.

²² C-521/17, Coöperatieve Vereniging SNB-REACT U.A. kontra Deepak Mehta, ECLI:EU:C:2018:639, 44.

²³ RIORDAN (2016): 403.

²⁴ C291/13, Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi és Giorgos Sertis, ECLI:EU:C:2014:2209, 42. Lásd továbbá Google France SARL és Google Inc. kontra Louis Vuitton Malletier SA (C-236/08), Google France SARL kontra Viaticum SA és Luteciel SARL (C-237/08) és Google France SARL kontra Centre national de recherche en relations humaines (CNRRH) SARL és társai (C-238/08), ECLI:EU:C:2010:159, 116.; C-324/09, L'Oréal SA és társai kontra eBay International AG és társai, ECLI:EU:C:2011:474, 115.

²⁵ C291/13, Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi és Giorgos Sertis, ECLI:EU:C:2014:2209, 45.

²⁶ C-324/09, L'Oréal SA és társai kontra eBay International AG és társai, ECLI:EU:C:2011:474, 31.

²⁷ Uo., 116.

kenységnek kell tekinteni.²⁸ Például a Google France és Google-ügyben az EUB megállapította, hogy a Google-t nem lehet megfosztani a tárhelyszolgáltatói címtől pusztán azon az alapon, hogy (i) a reklámszolgáltatás fizetéshez kötött; (ii) a Google határozta meg a fizetési feltételeket; és hogy (iii) a Google általános tájékoztatást nyújtott ügyfeleinek. Ezen túlmenően a kiválasztott kulcsszó és az internetfelhasználó által bevitt keresőkifejezés közötti egyezés sem volt elégséges annak megállapításához, hogy a Google ismerte vagy kezelte a hirdető által a rendszerébe bevitt és a szerverén tárolt adatokat.²⁹

Hasonlóképpen a Frank Peterson kontra Google LLC, YouTube Inc. és társai, valamint az Elsevier Inc. kontra Cyando AG egyesített ügyekben az EUB azt is megállapította, hogy azok a tények, hogy egy online tartalommegosztó platform üzemeltetője automatikusan indexálja a platformra feltöltött tartalmakat, hogy a platform rendelkezik keresési funkcióval és hogy a felhasználók profilja vagy preferenciái alapján videókat ajánl, nem elegendők annak a következtetésnek a levonására, hogy az említett üzemeltető tudott az e platformon végzett jogellenes tevékenységekről vagy az ott tárolt jogellenes információkról.³⁰ E tekintetben az EUB egyértelművé tette, hogy a szolgáltató absztrakt tudása (azaz általános értelemben vett tudása arról, hogy a platformot olyan tartalmak megosztására is használják, amelyek sérthetik a szellemi tulajdonjogokat) nem elegendő a szolgáltató aktív szerepének megalapozásához.³¹

7.3. Az Eker. irányelv elavulása és a növekvő igény egy új jogszabály iránt

Bár az Eker. irányelv kétségtelenül az egyik legsikeresebb uniós jogszabály volt, és óriási szerepet játszott az online szolgáltatások fejlődésében, a 2020-as évek elejére már jócskán elavulttá vált az elmúlt húsz év technológiai, gazdasági és társadalmi fejlődésének fényében.³² Az Eker. irányelv elfogadása óta számos olyan új szolgáltatás és tevékenység jelent meg, amelyeket a jogalkotók nem láthattak előre, mint például a videómegosztó platformok, az értékesítési platformok, a közösségi hálózatok és a *peer-to-peer* szolgáltatások.³³ Ennek eredményeképpen az irányelv rendelkezéseinek értelmezése és alkalmazása egyre nagyobb kihívást jelentett a gyakorlatban. Ez pedig tagállami szinten eltérő ítélkezési gyakorlat kialakulásához vezetett. Mindez együttesen szabályozási bizonytalanságot eredményezett, ami szükségszerűen akadályt gördített az információs társadalommal összefüggő szolgáltatások EU-beli fejlődésének útjába.³⁴

²⁸ WILMAN (2023): 40.

²⁹ Google France SARL és Google Inc. kontra Louis Vuitton Malletier SA (C-236/08), Google France SARL kontra Viaticum SA és Luteciel SARL (C-237/08) és Google France SARL kontra Centre national de recherche en relations humaines (CNRRH) SARL és társai (C-238/08), ECLI:EU:C:2010:159, ECLI:EU:C:2010:159, 116–117.

³⁰ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 114.

³¹ Uo., 111.

³² PAPP (2022); KLEIN (2023): 123–124.

³³ KOLTAY–SZIKORA–LAPSÁNSZKY (2024): 13.

³⁴ Commission Staff Working Document Online services, including e-commerce, in the Single Market {SEC(2011) 1641 final}, 43.

Az Európai Bizottság szerint a szabályozási bizonytalanság egyik fő oka az volt, hogy a közvetítő szolgáltatók számára az Eker. irányelv által kialakított felelősségi rendszer gyakorlatban való alkalmazása nem volt mindig egyértelmű.³⁵ A Bizottság különösen az Eker. irányelv 12–14. cikkeinek az ott nem említett szolgáltatókra való alkalmazhatóságot nevezte meg az egyik legfontosabb problémaként.³⁶ Az Eker. irányelv 12–14. cikkeinek hatályával kapcsolatos tisztázatlanságot több technológiai cég is felvetette a digitális szolgáltatásokról szóló rendelethez kapcsolódó előzetes hatásvizsgálat során. Az Ebay visszajelzésében például kijelentette, hogy „jelentős széttagoltságot tapasztaltunk az uniós nemzeti bíróságok között az Eker. irányelv értelmezését illetően. Ez a jogbizonytalanság rendkívül káros az információs társadalommal összefüggő szolgáltatások működésére és fejlődésére.”³⁷

Az EB az Eker. irányelvvel kapcsolatban egy másik kulcsproblémát is azonosított, mégpedig a felelősség alóli mentesülés anyagi feltételeinek tagállami szinten eltérő értelmezését.³⁸ Például a jogellenes tartalomról való tényleges tudomásszerzés követelményét, amely az Eker. irányelv 14. cikke értelmében az ilyen tartalom eltávolítására vagy az ahhoz való hozzáférés megakadályozására vonatkozó kötelezettséget keletkeztette, az EU-ban a tagállami hatóságok nem értelmezték egységesen.³⁹ A gyakorlatban általánossá vált, hogy a közvetítő szolgáltatók a jogellenes tartalomról szóló értesítést elegendőnek tekintik a tényleges ismeret megállapításához.⁴⁰ Harmonizált értesítési és eltávolítási eljárások hiányában azonban a tagállamok eltérő normákat fogadtak el arra vonatkozóan, hogy a bejelentésnek milyen részletesnek kellett lennie ahhoz, hogy a szolgáltató tényleges ismeretének küszöbértékét elérje.⁴¹ Ezt a kérdést több technológiai óriásvállalat is felvetette az EB fent említett nyilvános konzultációja során. A Facebook⁴² például kijelentette, hogy

³⁵ Uo., 25.

³⁶ Jelentésében az EB több példát is hozott az Eker. irányelv 12–14. cikkének hatályával kapcsolatban kialakult jelentősen eltérő nemzeti joggyakorlatra. Az EB utalt például a különböző tagállamokban a videómegosztó oldalak minősítésével kapcsolatban kialakult, egymásnak ellentmondó nemzeti ítélkezési gyakorlatra. Amint azt a tanulmány részletesen kifejti, Franciaországban a videómegosztó oldalak a tárhelyszolgáltatói tevékenységekre vonatkozó felelősség alóli menteséget élvezték (lásd például a Magdane kontra Dailymotion-ügyben hozott ítéletet). Ezzel szemben Németországban a hamburgi bíróság a Peterson kontra Google Inc. és társai-ügyben megakadályozta, hogy a YouTube az Eker. irányelv 14. cikke szerinti mentességre hivatkozzon, megállapítva, hogy a harmadik személyek által feltöltött videók megosztására szolgáló videómegosztó oldal nem részesülhet a mentességben, ha a feltöltött tartalmat saját tartalmaként tünteti fel. Uo., 25–26.

³⁷ eBay’s feedback on the Inception Impact Assessment for a Digital Services Act: Deepening the internal market and clarifying responsibilities for digital services, 2020. június 30., 2. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F535644_en

³⁸ SEC(2011) 1641 final, 25.

³⁹ COLE–ETTELDORF–ULLRICH (2021): 170–171.

⁴⁰ Uo.

⁴¹ Uo., 172.

⁴² Hasonlóképpen a Google beadványa is tartalmazta, hogy „a hivatalos értesítésnek legalább a következő követelményeket kell tartalmaznia: a kérdéses tartalom egyértelmű azonosítása URL-cím, videó időbélyegző vagy más egyedi azonosító alapján; a jog és a jogi igény alapjának feltüntetése; az értesítés feladójának egyértelmű azonosítása, amennyiben az igényelt jogok jellege megköveteli a jogtulajdonos azonosítását; és a követelés jóhiszeműségének és érvényességének igazolása. Ez segíti a felülvizsgálati csoportokat az információk hatékonyabb és felelősségteljesebb feldolgozásában, valamint védelmet nyújt a család vagy rosszhiszemű bejelentésekkel való visszaélésekkel szemben.” Google’s feedback on the Inception Impact Assessment for a Digital Services Act: Deepening the internal market and clarifying responsibilities for digital services, 2020. június 30., 8. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F535584_en

„a jelenlegi szabályozási keretből hiányzik az egyértelműség és a következetesség azzal kapcsolatban, hogy hogyan kell kinézniük ezeknek a bejelentéseknek, ami a szükségességnél hosszabb feldolgozási időhöz vezet. (...) Kíváncsú lenne meghatározni azokat a minimális információkat, amelyek szükségesek ahhoz, hogy egy értesítés jogkövetkezményekkel járjon (pl. az egyedi URL, az állítólagos jogsértés típusa vagy jogellenessége, valamint a bejelentő státusza).”⁴³

A fentiekben túlmenően az értesítéseknek az illegális tartalomról való tényleges tudomásszerzés elégséges bizonyítékeként való elismerése arra is vezetett, hogy az online platformok az illegális tartalmak kezelésében nagyrészt reaktív megközelítést alakítottak ki, mivel aktív tevékenységükkel a felelősség alóli mentesség elvesztését kockáztatták volna.⁴⁴

Ez végeredményben a felhasználókat fokozott veszélynek tette ki, és alapvető jogaik fokozott megsértéséhez vezetett.⁴⁵ Vagy ahogyan azt a Google az EB-hez benyújtott beadványában kifejtette:

„sok olyan szürke zónás esettel találkozunk, amelyek esetében megfelelő időre van szükség a jog és a kontextus értékeléséhez, és továbbra is aggódunk a közelmúltbeli jogszabályok miatt, amelyek lehetővé teszik nagy összegű büntetések kiszabását, ha a rövid, rögzített átfutási idő nem teljesül. (...) Az ilyen követelmények túlzott tartalomtörléshez vezethetnek. (...) Ez aláássa a véleménynyilvánítás és a kommunikáció szabadságát olyan módon, amely nem szükséges, nem igazodik hozzá és nem arányos.”⁴⁶

A fentiekből következik, hogy bár az Eker. irányelv sikeresen megteremtett egy egységes jogi keretet annak a valóságnak a szabályozására, amely húsz évvel ezelőtt létezett, ez a jogszabályi terület ismét széttöredezetté vált. Az Eker. irányelv elfogadása óta új digitális szolgáltatások jelentek meg, amelyek alakították és átalakították az európai polgárok mindennapi életét, beleértve a kommunikációt, a kapcsolattartást, a fogyasztást és az üzletkötés módját. Ezen szolgáltatások új kockázatokat és új kihívásokat jelentenek mind a társadalom egésze, mind pedig az egyének számára.⁴⁷

Néhány tagállam (pl. Németország és Franciaország) a saját kezébe vette az ügyet, és különböző nemzeti jogszabályok elfogadásával igyekezett az új kihívásokat jogi úton rendezni.⁴⁸ Ezen tagállami jogszabályok elsősorban a közvetített jogellenes tartalmak (pl. gyű-

⁴³ Facebook’s feedback on the Inception Impact Assessment for a Digital Services Act: Deepening the internal market and clarifying responsibilities for digital services, 2020. június 30., https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F535593_en

⁴⁴ GOSZTONYI (2023): 60.

⁴⁵ COLE–ETTELDORF–ULLRICH (2021): 170–171.

⁴⁶ Google’s feedback on the Inception Impact Assessment for a Digital Services Act: Deepening the internal market and clarifying responsibilities for digital services, 2020. június 30., https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F535584_en

⁴⁷ Javaslat az Európai Parlament és a tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, 2020/0361(COD), COM(2020) 825 final, 1.

⁴⁸ KÉRINGER (2023); GOSZTONYI–LENDVAI (2023a): 4–5.; SZŐKE (2021): 113–114.

löletbeszéd⁴⁹), valamint az online dezinformáció kezelésére vonatkozó gondossági követelményeket írtak elő a közvetítő szolgáltatókkal szemben. A nemzeti jogszabályokon alapuló gondossági kötelezettségek között szerepeltek többek között a szolgáltatók jelentéstételi (*reporting*) és átláthatósági (*transparency*) kötelezettségei. Ezek az eltérő nemzeti jogszabályok azonban magukban hordozták a belső piac torzításának kockázatát. Az EUMSZ⁵⁰ 26. cikke értelmében a belső piac egy olyan határok nélküli térség, amelyben biztosított az áruk és szolgáltatások szabad mozgása és a letelepedés szabadsága. Mivel azonban a különböző tagállamok eltérő módon szabályozták az új, határokon átnyúló, digitális szolgáltatásokat, félő volt, hogy egy adott tagállamban (tipikusan Írországban) letelepedett közvetítő szolgáltató nem lesz képes a szolgáltatásait ugyan olyan feltételek mellett valamennyi tagállamban biztosítani.

Annak ellenére, hogy a közvetítői szolgáltatókra vonatkozó szabályok harmonizálására irányuló igény fokozatosan nőtt, az uniós jogalkotó kizárólag az ágazati kérdések rendezésére fókuszált,⁵¹ így 2018-ban elfogadta az az audiovizuális médiaszolgáltatásokról szóló irányelv módosítását,⁵² majd 2019-ben a szerzői és szomszédos jogoknak a digitális egységes piacon való védelméről szóló irányelvet.⁵³ A fordulópont 2017–2018 környékén érkezett el, a Cambridge Analytica botrány, valamint az Egyesült Államok elnökválasztásába való orosz beavatkozás megállapítása eredményeként.

2022. október 19. napján az uniós jogalkotó az 'Európa digitális jövőjének alakítása' elnevezésű program részeként⁵⁴ elfogadta a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló 2022/2065 EU Rendeletet (DSA).⁵⁵ A jogszabály meg kívánja teremteni a legjobb feltételeket az innovatív digitális szolgáltatások nyújtásához a belső piacon, fokozni kívánja az online biztonságot, védeni az alapvető jogokat, valamint létrehozni egy átfogó és tartós irányítási keretet a közvetítő szolgáltatók hatékony felügyeletére. A DSA ezeket a célkitűzéseket több kulcsfontosságú mechanizmuson keresztül valósítja meg, mint például: (i) egyértelmű felelősségek, kötelezettségek és elszámoltathatóság megállapítása a közvetítő szolgáltatók, különösen az online platformok számára; és (ii) felelős és kellően gondos magatartási követelmények bevezetése bizonyos közvetítő szolgáltatásokra (beleértve az illegális tartalmakra vonatkozó értesítési és intézkedés iránti eljárásokat), valamint a felhasználók számára a tartalom moderálására vonatkozó döntések megtámadására szolgáló mechanizmusokat.

⁴⁹ BUKOR–TRÄGER (2024): 2.

⁵⁰ Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, HL C 202., 2016.6.7., 1–388.

⁵¹ POLYÁK (2020): 114–115.

⁵² Az Európai Parlament és a Tanács 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, PE/33/2018/REV/1, HL L 303, 28.11.2018, 69–92.

⁵³ Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, PE/51/2019/REV/1, HL L 130., 2019.5.17., 92–125.

⁵⁴ A Tanács következtetései Európa digitális jövőjének alakításáról, 2020/C 202 I/01, ST/8711/2020/INIT, HL C 202I., 2020.6.16., 1–12.

⁵⁵ 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 (digitális szolgáltatásokról szóló rendelet), PE/30/2022/REV/1, HL L 277., 2022.10.27., 1–102.

8. A platformok jogi felelőssége a DSA alapján

Thierry Breton, a belső piacért felelős biztos 2019 és 2024 között a DSA elfogadásával kapcsolatban úgy nyilatkozott, hogy a jogszabály jelzi annak a korszaknak a végét, amikor a nagy online platformok úgy működhettek, mint „amikor az online óriásplatformok úgy érezhetik, »túl nagyok« ahhoz, hogy utolérjék őket a következmények.”¹ Ursula von der Leyen, az EB elnöke is csatlakozott ehhez a véleményhez, hangsúlyozva, hogy a DSA korszerűsíti az EU-n belüli valamennyi online szolgáltatás szabályozási keretét, biztosítva, hogy a digitális tér biztonságos maradjon, miközben védi a véleménynyilvánítás szabadságát és támogatja a digitális üzleti növekedést. A DSA középpontjában az az elv áll, hogy „amit hagyományosan jogellenesnek tekintünk, annak internetes formában is jogellenesnek kell lennie,”² és a nagyobb platformok fokozott felelősséggel tartoznak. Ez a digitális piacokkal kapcsolatos politikai megállapodás határozott üzenetet közvetít minden európai polgárnak, valamennyi uniós vállalkozásnak és nemzetközi partnereinknek.

8.1. A DSA céljai

A DSA 1. cikkének (1) bekezdése szerint a rendelet célja, hogy „hozzájáruljon a közvetítő szolgáltatások belső piacának megfelelő működéséhez, az olyan biztonságos, kiszámítható és megbízható online környezetre vonatkozó harmonizált szabályok meghatározásával, amely elősegíti az innovációt, és amelyben a Chartában rögzített alapvető jogok, köztük a fogyasztóvédelem elve hatékony védelmet élveznek.” A DSA céljából következik, hogy a rendelet a közvetítő szolgáltatások nyújtását szabályozó általános szabályozási keretrendszer létrehozására korlátozódik, anélkül, hogy a digitális platformok működésének minden egyes aspektusát szabályozni kívánná. A DSA nem terjed ki olyan konkrét területekre, mint a szerzői jog, az adatvédelem vagy a büntetőjog.³ Ehelyett harmonizált szabályok meghatározására összpontosít:

¹ A digitális szolgáltatásokról szóló jogszabály: a Bizottság üdvözli a biztonságos és elszámoltatható online környezet létrehozását célzó jogszabályokról született politikai megállapodást. 2022. április 23. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545

² Uo.

³ NOVÓVIC (2024): 3.

- olyan részletes szabályok bevezetésével, amelyek a közvetítő szolgáltatások nyújtását a szolgáltatások teljes életciklusa során szabályozzák (pl. közös szabványok az olyan kulcsfontosságú kötelezettségekre vonatkozóan, mint az értesítésekre való reagálás, a hatóságok felszólítására az illegális tartalom eltávolítására, bejelentési és cselekvési mechanizmusok bevezetése, átlátható felhasználási feltételek biztosítása és a DSA-nak való megfelelés kommunikálása a nyilvánosság felé);
- a meglévő jogi követelmények, különösen az EUB ítélezési gyakorlatából származó követelmények tisztázása és beépítése; és
- a korábban vitatott és kevésbé megalapozott elv világos jogalapjának megteremtése.

A platformok magatartásának tagállamok közötti harmonizálásával a DSA növeli a jogi kiszámíthatóságot és biztosítja, hogy a platformok előre láthassák tetteik következményeit,⁴ így válaszolva a platformok által az EB Eker. irányelvvel kapcsolatban folytatott nyilvános konzultáció során megfogalmazott legfőbb aggályokra.

Nem titok, hogy a határokon átnyúló szolgáltatásokra alkalmazandó jogszabályok harmonizálása elősegíti a szolgáltatások szabad mozgását az EU-n belül, még akkor is, ha ez bizonyos szabályozási korlátozások bevezetésével jár együtt. A harmonizációra a belső piac széttöredezettségének elkerülése és megszüntetése, valamint a jogbiztonság biztosítása érdekében van szükség, így csökkentve a fejlesztők bizonytalanságát és elősegítve az interoperabilitást.⁵ A DSA-t mindezekből következően az EU egységes piacát szem előtt tartva fogadták el: azaz a jogszabály az EU egységes piacát igyekszik kiépíteni azáltal, hogy biztosítja a feltételeket az innovatív digitális szolgáltatások megjelenéséhez és a belső piacon való elterjedéséhez.⁶

A közvetítő szolgáltatókra vonatkozó szabályok harmonizálása a DSA másik fő céljának eléréséhez is szükséges, nevezetesen a szolgáltatás valamennyi igénybe vevője biztonságának, bizalmának és jogainak fokozott garantálásához, beleértve különösen a gyűlöletbeszéd, szexuális zaklatással vagy diszkriminációval szemben kiszolgáltatott csoportok magas szintű védelmét.⁷ Amint azt a DSA (3) preambulumbekkezdése tovább részletezi:

„a közvetítő szolgáltatók felelősségteljes és kellően gondos magatartása elengedhetetlen a biztonságos, kiszámítható és megbízható online környezethez, illetve ahhoz, hogy az uniós polgárok és más személyek gyakorolhassák a Chartában biztosított alapvető jogokat, különösen a véleménynyilvánítás és a tájékozódás szabadságát, a vállalkozás szabadságát, a megkülönböztetésmentességhez való jogot és a fogyasztóvédelem magas szintjének elérését.”

⁴ SZÖKE (2021): 115–117.

⁵ DSA (4) preambulumbekkezdés.

⁶ ZÓDI (2023): 182–184.; PÜNKÖSTY (2022b).

⁷ DSA (9) preambulumbekkezdés.

8.2. A platformok meghatározása a DSA alapján

A DSA (5) preambulumbekzdése és 2. cikkének (1)–(2) bekezdése szerint a rendelet kizárólag a közvetítő szolgáltatókra, az információs társadalommal összefüggő szolgáltatók egy bizonyos típusára vonatkozik. Ebből következik, hogy a DSA az Eker. irányelvhez hasonlóan különbséget tesz a közvetítő szolgáltatók és az ilyen szolgáltatásokat nem nyújtó, egyéb információs társadalommal összefüggő szolgáltatók között.

Hasonlóan az Eker. irányelvben található struktúrához, a DSA megtartotta a közvetítő szolgáltatások három különböző kategóriába való besorolását: (i) egyszerű továbbítás (*mere conduit*); (ii) tárhelyszolgáltatás (*hosting*); és (iii) gyorsítótárolóban történő rögzítés (*caching*). Ezen túlmenően a DSA ezeket a kategóriákat az Eker. irányelv 12–14. cikke alapján határozza meg:

- egyszerű továbbítás (*mere conduit*): olyan szolgáltatás, amely a szolgáltatás igénybe vevője által küldött információnak hírközlő hálózaton keresztül történő továbbításából vagy a hírközlő hálózathoz való hozzáférés biztosításából áll;⁸
- gyorsítótárazás (*caching*): olyan szolgáltatás, amely a szolgáltatás igénybe vevője által küldött információnak hírközlő hálózaton keresztül történő továbbításából áll, együtt jár az információ automatikus, közbenső és átmeneti tárolásával, és amelyet azzal a kizárólagos céllal hajtanak végre, hogy az információ későbbi továbbítását a szolgáltatás más igénybe vevői számára azok kérésére hatékonyabbá tegye;⁹
- tárhelyszolgáltatás (*hosting*): olyan szolgáltatás, amely a szolgáltatás igénybe vevője által küldött és a szolgáltatás igénybe vevőjének kérésére tárolt információ tárolásából áll.¹⁰

A DSA által bevezetett egyik legfontosabb újítás a platformok szerepének tisztázása, ezáltal nagyobb jogbiztonságot nyújtva az online platformok számára.¹¹ A platformot a DSA olyan tárhelyszolgáltatóként határozza meg, amely

„a szolgáltatás igénybe vevőjének kérésére információkat tárol és nyilvánosan terjeszt, kivéve, ha ez a tevékenység egy másik szolgáltatás kisebb vagy kizárólag kiegészítő eleme, vagy a fő szolgáltatás kisebb funkcionálisága, amely objektív és technikai okokból nem használható az említett másik szolgáltatás nélkül, és az ilyen elem vagy funkcionáliság másik szolgáltatásba való integrációja nem a rendelet alkalmazhatóságának elkerülésére szolgál.”¹²

A platformok ezért a tárhelyszolgáltatók egy sajátos alcsoportját alkotják, amelyeket az különböztet meg más tárhelyszolgáltatóktól, hogy funkciójuk nem csupán az információk tárolása,

⁸ DSA 3. cikk g) i.

⁹ DSA 3. cikk g) ii.

¹⁰ DSA 3. cikk g) iii.

¹¹ TÓTH (2022): 79.

¹² DSA 3. cikk i).

hanem azok nyilvánosság számára való hozzáférhetőségének megkönnyítése is.¹³ A DSA szerint a platformokat a többi tárhelyszolgáltatótól megkülönböztető kulcsfontosságú tényező az, hogy a tárolt információt széles és potenciálisan korlátlan számú közönség számára hozzáférhetővé teszik, amit nyilvános terjesztésnek neveznek. A nyilvános terjesztés fogalma tehát döntő fontosságú annak meghatározásában, hogy egy tárhelyszolgáltató platformnak minősül-e. A DSA 3. cikkének k) pontja a nyilvános terjesztés fogalmát úgy határozza meg, mint „az információk elérhetővé tétele potenciálisan korlátlan számú harmadik fél számára a szolgáltatás információt biztosító igénybe vevőjének kérésére”. Amint ezt a DSA (14) preambulumbekzdése tovább pontosítja, a nyilvános terjesztés azokra az esetekre korlátozódik, amikor az információt a címzettek számára hozzáférhetővé teszik anélkül, hogy az információt nyújtó szolgáltatás igénybe vevője további intézkedést kérne, függetlenül attól, hogy az említett személyek ténylegesen hozzáférnek-e a szóban forgó információhoz. Ennek megfelelően, ha az információhoz való hozzáféréshez regisztrációra vagy a szolgáltatás igénybe vevőinek egy csoportjába való felvételre van szükség, az információ csak akkor tekinthető a nyilvánosság számára terjesztettnek, ha a szolgáltatás igénybe vevőit, akik az információhoz kívánnak hozzáférni, automatikusan regisztrálják vagy felveszik, anélkül, hogy emberi döntés vagy kiválasztás alapján döntenének arról, hogy kinek biztosítanak hozzáférést. Amint azt a DSA (14) preambulumbekzdése kifejti, a nyilvános terjesztés fogalma azért kerül ily módon korlátozásra, hogy az olyan személyközi kommunikációs szolgáltatások, mint az e-mailek vagy a magánüzenet-szolgáltatások ne tartozzanak a platformok hatálya alá. Ezen szolgáltatásokat ugyanis az üzenet küldője az általa meghatározott, korlátozott számú személlyel történő kommunikációra használja fel.

Bár mindez elsőre logikusnak tűnhet, a valóságban a DSA (14) preambulumbekzdése számos kérdést vet fel. Például, a DSA (14) preambulumbekzdéséből következik-e, hogy a Facebook privát csoportjai vagy a Reddit privát oldalai (*subreddit*) nem minősülnek platformnak tekintettel arra, hogy azok (i) csak korlátozott számú felhasználó számára hozzáférhetőek; és (ii) a belépés a csoport házigazdájának vagy szervezőjének döntésétől függ. Amennyiben igen, úgy felmerül továbbá a kérdés, hogy vajon egy tárhelyszolgáltató minősülhet-e egyes szolgáltatásai vonatkozásában platformnak, míg a többi esetében csak tárhelyszolgáltatónak (vagy akár más közvetítő szolgáltatónak). E kérdésekre ma még nincsen pontos jogi válaszunk, ám a közeljövőben bizonyosan el kell a joggyakorlatnak mozdulnia valamelyik irányba.

A DSA 'online platform' fogalommeghatározásának másik lényeges eleme az olyan tevékenység kizárása, amely csak „egy másik szolgáltatás kisebb vagy kizárólag kiegészítő eleme”, vagy „a fő szolgáltatás kisebb funkcionalitását” jelenti.¹⁴ Ezek a tevékenységek nem tartoznak a platformok DSA szerinti definíciójának hatálya alá, feltéve, hogy a főszolgáltatás

¹³ Ezt a DSA (13) preambulumbekzdése is megerősíti, amely szerint „az e rendeletben meghatározott tárhelyszolgáltatók tágabb kategóriáján belül meg kell különböztetni az online platformok alkategóriáját. Az online platformokat ... olyan tárhelyszolgáltatókként kell meghatározni, amelyek nemcsak a szolgáltatás igénybe vevői által a szolgáltatás igénybe vevőinek kérésére megadott információkat tárolják, hanem a szolgáltatás igénybe vevőinek kérésére ezeket az információkat a nyilvánosság számára is terjesztik.”

¹⁴ HOFMANN–RAUE (2025): 72–73.

kisebb eleme vagy funkciója „objektív és technikai okokból nem használható az említett másik szolgáltatás nélkül, és az ilyen elem vagy funkcionalitás másik szolgáltatásba való integrációja nem a rendelet alkalmazhatóságának elkerülésére szolgál.”¹⁵

Ez a kivétel jelenti a platformok és az egyéb tárhelyszolgáltatók közötti egyértelmű különbséget, ahol a platformszerű funkciók csupán mellékesen kapcsolódnak az elsődleges szolgáltatáshoz.¹⁶ Ezáltal a DSA elkerüli, hogy szükségtelenül széles körű kötelezettségeket rójon azokra a tárhelyszolgáltatókra, amelyek csak kisebb interaktív elemeket tartalmaznak.¹⁷ A DSA példaként említi egy online újság kommentárszekcióját, amely kiegészítő szolgáltatásnak minősülhet, mivel az elsődleges szolgáltatás a kiadó szerkesztői ellenőrzése alatt álló hírek közzététele. Ebben az esetben a hozzászólási lehetőség másodlagosnak minősül, és nem alakítja át a szolgáltatást platformmá.¹⁸ Mindezek után a DSA azt is kifejezetten tisztázza, hogy a közösségi hálózaton a kommentek tárolása nem kezelhető pusztán kiegészítő funkcióként, mivel az egyértelműen nem a kínált szolgáltatás mellékes jellemzője – még akkor sem, ha kiegészíti a felhasználói hozzászólások közzétételét.¹⁹ Ilyen esetekben az interaktív elemek a szolgáltatás szerves részét képezik, és így a közösségi hálózat továbbra is online platformnak minősül, amelyre a DSA szerinti kötelezettségek teljes köre vonatkozik.

Végül a teljesség kedvéért meg kell jegyezni, hogy a DSA a platformok egy speciális kategóriáját (az online óriásplatformokat²⁰) külön nevesíti és szabályozza. Az online óriásplatformok olyan platformok, amelyek esetében a szolgáltatás havi átlagos aktív felhasználóinak száma az EU-ban eléri vagy meghaladja a 45 milliót, és amelyeket az EB online óriásplatformoknak minősített. Az online óriásplatformok közé tartozik például a Facebook, az Instagram, a LinkedIn, a Pinterest, a Snapchat, a TikTok, a Twitter és a YouTube.²¹ Az EU elismerte az online óriásplatformok gazdaságra és társadalomra gyakorolt erőteljes hatását. Erre tekintettel a DSA olyan rendelkezéseket tartalmaz, amelyek az átláthatóság és az elszámoltathatóság magasabb szintű normáinak előírásával tükrözik e platformok egyedülálló szerepét. Ezek a fokozott kötelezettségek a tartalom moderálási gyakorlatokra, a hirdetések átláthatóságára és az algoritmikus folyamatok használatára vonatkoznak, biztosítva, hogy az ilyen platformok szolgáltatói szigorúbb szabályozási követelményeket tartsanak be.²²

Összefoglalva, a DSA a közvetítő szolgáltatók három kategóriáját különbözteti meg: (i) egyszerű továbbító szolgáltatók (*mere conduit*); (ii) gyorsítótárazási szolgáltató (*caching*); és (iii) tárhelyszolgáltató (*hosting*). A tárhelyszolgáltatók egy speciális alcsoportját képezik az online platformok, amelyek lehetővé teszik a felhasználók számára, hogy az általuk nyújtott tartalmakat a nyilvánosság felé terjesszék. A DSA megkülönbözteti továbbá a platformok

¹⁵ DSA 3. cikk i).

¹⁶ ZÓDI (2023): 186.

¹⁷ DSA (13) preambulumbekkezdés.

¹⁸ ZANATHY (2025): 198.

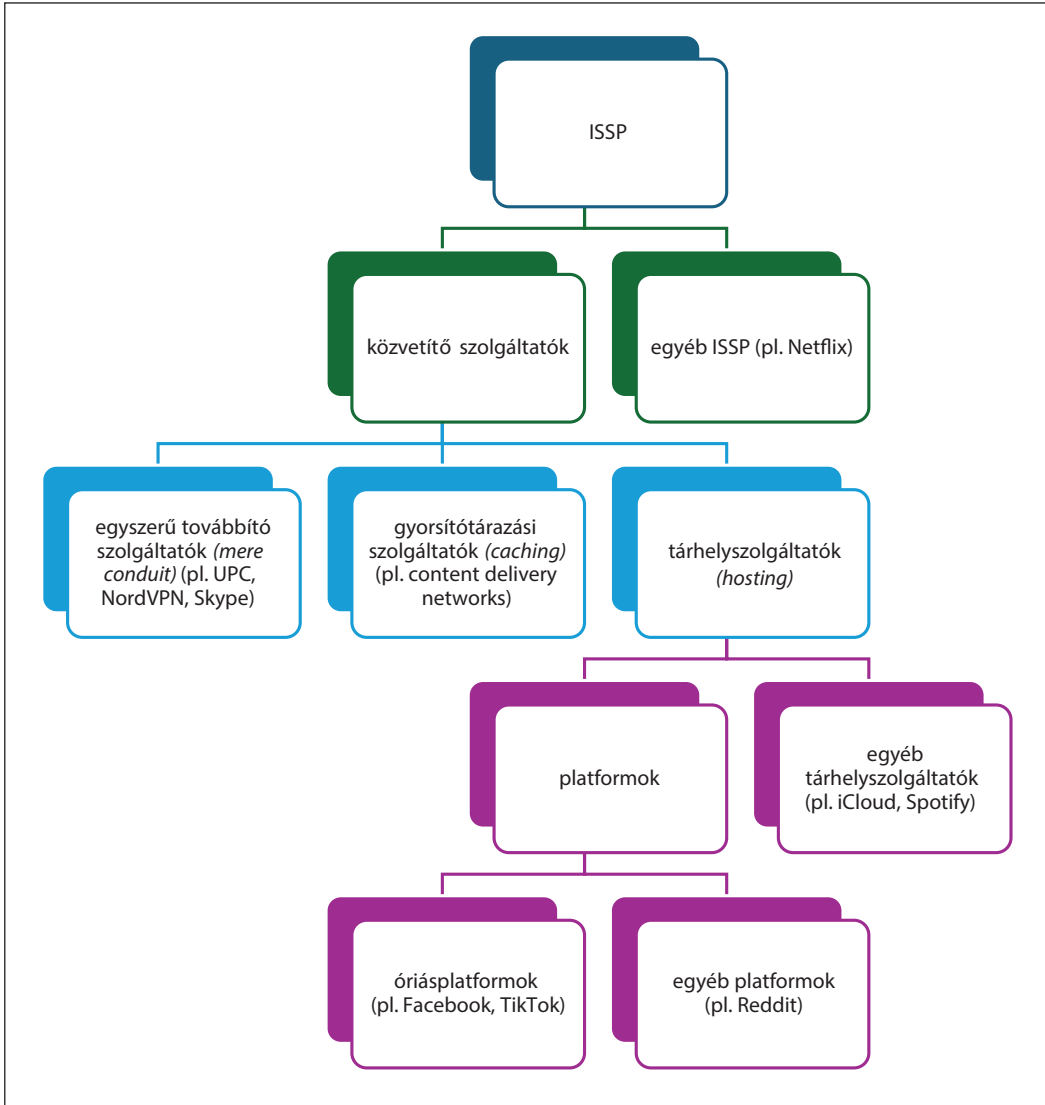
¹⁹ DSA (13) preambulumbekkezdés.

²⁰ Az angol terminus technicus (*very large online platform*) miatt a szakirodalom a legtöbbször a VLOP mozaikszót használja rájuk.

²¹ A digitális szolgáltatásokról szóló jogszabály alapján kijelölt online óriásplatformok és keresőmotorok felügyelete. Az információkat utoljára 2025. május 15-én frissítették. <https://digital-strategy.ec.europa.eu/hu/policies/list-designated-vlops-and-vloses>

²² HUSOVEC (2024): 19–32.

egy egyedi kategóriáját – az online óriásplatformokat –, amelyeket jelentős felhasználói bázisuk és az online ökoszisztémában betöltött meghatározó szerepük különböztet meg a többi platformtól.²³ A közvetítő szolgáltatók előbb ismertetett csoportosítását a 16. ábra szemlélteti.



16. ábra: A közvetítő szolgáltatók a DSA alapján²⁴

²³ MONTI (2024): 447.

²⁴ Saját szerkesztés.

8.3. A közvetítő szolgáltatók felelősség alóli mentesülése

Ahogy arra a DSA (17) preambulumbekzdése is rávilágít, a DSA a közvetítő szolgáltatók felelőssége vonatkozásában kizárólag arra a kérdésre ad választ, hogy a közvetítő szolgáltatók milyen feltételek mellett nem vonhatók felelősségre a szolgáltatás igénybe vevői által rendelkezésre bocsátott jogellenes tartalom miatt. A DSA azonban önmagában nem teremt jogalapot a közvetítő szolgáltatók felelősségre vonására, ez ugyanis továbbra is a hatályos nemzeti, illetve más uniós jogszabályokra marad.

8.3.1. A DSA által teremtett felelősségi rendszer semlegessége az üzleti dimenziókra, vállalatokra és termékekre nézve

Gyakran hangoztatott tévhit az online világgal kapcsolatban, hogy a DSA felelősségi rendszerét – és így a tárhelyszolgáltatók fogalom meghatározását is – bizonyos típusú szolgáltatásokra vagy vállalatokra tekintettel alakították ki. Ez azonban nem így van. Amint azt a DSA (29) preambulumbekzdése kifejti, a felelősség alóli mentességet élvező közvetítői szolgáltatások háromféleképpen nyújthatók:

- önállóan,
- más típusú közvetítői szolgáltatás részeként, vagy
- más közvetítői szolgáltatásokkal egyidejűleg.

A tárhelyszolgáltatás kifejezés például számos kategóriát felölel, ideértve a felhőalapú számítástechnikát, a webtárhelyet, a fizetett hivatkozási szolgáltatásokat, az információk és tartalmak online megosztását lehetővé tevő szolgáltatásokat (pl. videómegosztó platformok, közösségimédia-szolgáltatások), az alkalmazásboltokat és a felhőalapú számítástechnikai szolgáltatásokat.

Az, hogy egy adott szolgáltatás egyszerű továbbításnak, tárhelyszolgáltatásnak vagy gyorsítótárazásnak minősül-e, kizárólag annak technikai funkcióitól függ, amelyek idővel fejlődhetnek, és amelyeket eseti alapon kell értékelni.²⁵ Ez azt is jelenti, hogy a DSA-nak a tárhelyszolgáltatókat szabályozó rendelkezései a szolgáltatás konkrét műszaki tevékenységei alapján alkalmazandók, nem pedig az üzleti modell, vagy az e szolgáltatást integráló termék típusa alapján. Más szóval az értékelés attól függ, hogy a tevékenységek technikai leírása megfelel-e a DSA-ban meghatározott felelősségi mentességeknek.²⁶

Felmerülhet azonban a kérdés, hogy a DSA mely rendelkezései vonatkoznak egy olyan közvetítő szolgáltatóra, amely többféle közvetítő szolgáltatást kombinál egyidejűleg. A kérdés megválaszolásához vegyük példaként a Facebookot. Egyrészt a Facebook a felhasználók által generált tartalmakat, például kommenteket és képeket tárol, ami alapján tárhelyszolgáltatónak minősül. Másrészt a Facebook Messenger, amely a Facebook integrált részét képezi, *mere conduit* szolgáltatás, hiszen az megkönnyíti a kommunikációs hálózathoz

²⁵ DSA (29) preambulumbekzdés.

²⁶ DSA 6.2.1.

való hozzáférést a felhasználók számára. Véleményem szerint – és ez összhangban áll a tudományos szakirodalommal²⁷ – az ilyen hibrid közvetítőket funkcióink szerint kell értékelni. Így amikor a jogalkalmazónak arra a kérdésre kell válaszolnia, hogy a Facebook felelőssége vonható-e a felhasználó által az idővonalán megosztott jogellenes tartalomért, úgy a jogalkalmazónak a DSA 6. cikkére kell támaszkodnia.²⁸ Ezzel szemben amennyiben a Facebook felelőssége a Facebook Messengeren keresztül elküldött jogsértő tartalom vonatkozásában merül fel, úgy a jogalkalmazónak a Facebook felelősségét a DSA 4. cikke alapján kell megállapítania. Mindebből azonban az is következik, hogy a hibrid szolgáltatások nem tarthatnak kizárólagosan a közvetítő szolgáltatók egyetlen alkategóriájába.

Bár ez a megközelítés elsőre logikusnak tűnhet, a hibrid közvetítő szolgáltatók felelőségének kérdése a gyakorlatban jelentős kihívásokat támaszthat. Példaként említendő:

- A műszaki funkciók szolgáltatásba való integrálásának módja, amely befolyásolhatja, hogy a DSA-nak mely felelősségi alakzata alkalmazandó.
- A hibrid szolgáltató által nyújtott különböző közvetítő szolgáltatások közötti kapcsolat, amely további kérdéseket vethet fel. Logikus lenne például, hogy ha az egyik közvetítő szolgáltatás pusztán kiegészítő szolgáltatás, amely szorosan kapcsolódik a másik közvetítő szolgáltatáshoz, akkor a szolgáltató felelősségét a fő szolgáltatásra vonatkozó szabályok szerint kelljen értékelni. Mind a DSA, mind pedig a joggyakorlat hallgat azonban arról, hogy milyen feltételek mellett tekinthető egy szolgáltatás tisztán járulékosnak, illetve, hogy mikor tekinthető két szolgáltatás olyan mértékben összefonódottnak, hogy a két szolgáltatás iránti jogi felelősséget már nem lehet (vagy nem érdemes) elválasztani.

Fontosnak tartom azonban megjegyezni, hogy a DSA platformra vonatkozó meghatározása – a fentebb leírtakkal ellentétben – nem semleges az üzleti dimenziókra, a vállalati profilokra és a terméktípusokra nézve. Ez különösen nyilvánvaló az online óriásplatformok definíciójából, amely a teljes szolgáltatás felhasználóinak összlétszámán alapszik, és semmilyen különbséget sem tesz a termék egyes jellemzői vagy funkciói között. Ezt a megközelítést támasztják alá az EB határozatai is,²⁹ amelyek az olyan online termékeket, mint például a Facebook, a YouTube, az AliExpress és az Amazon Store, az online óriásplatformok közé sorolják, anélkül, hogy a termék egyes funkcióira külön-külön figyelemmel lennének.

Amint fentebb említettük, a platformokat a DSA a tárhelyszolgáltatók egy speciális részhalmazaként határozza meg. A DSA üzleti dimenziókkal szembeni semlegességéből az következne, hogy a felhasználók számára kizárólagosan tárhelyszolgáltatást nyújtó közvetítő szolgáltatások sorolhatók a platformok kategóriájába. A platform definíciójának második része azonban azt sejteti, hogy a platformok magukban foglalhatják a hibrid szolgáltatásokat is, feltéve, hogy a tárhelyszolgáltatás nem „egy másik szolgáltatás kisebb vagy kizárólag kiegészítő eleme”, vagy „a fő szolgáltatás kisebb funkcionalitása”.³⁰

²⁷ WILMAN–KALÉDA–LOEWENTHAL (2024)

²⁸ HOFMANN–RAUE (2025): 72–73.

²⁹ A digitális szolgáltatásokról szóló jogszabály alapján kijelölt online óriásplatformok és keresőmotorok felügyelete. Az információkat utoljára 2025. május 15-én frissítették. <https://digital-strategy.ec.europa.eu/hu/policies/list-designated-vlops-and-vloses>

³⁰ DSA 3. cikk i).

Az EB 2023. április 25. napján a Facebookot az elsők között jelölte ki online óriásplatformként. Az EB határozatában kijelentette: „A Facebook az (EU) 2022/2065 [DSA] rendelet 3. cikke g) pontjának iii. alpontja értelmében olyan tárhelyszolgáltatás, amely a szolgáltatását igénybe vevők kérésére információkat tárol és terjeszt a nyilvánosság számára. Ezért az (EU) 2022/2065 [DSA] rendelet 3. cikkének i) pontja értelmében online platformnak minősül.”³¹ Ez a határozat az EB egyértelmű mulasztását tükrözi a Facebook sokrétűségének értékelésében, ugyanis figyelmen kívül hagyta a Facebook azon jellemzőit, amelyek nem minősülnek ‘nyilvános terjesztésnek’ (pl. tartalom privát csoportban való megosztása), vagy amelyek egyáltalán nem tartoznak a tárhelyszolgáltatás körébe (pl. Facebook Messenger).

A fentebb leírtakból két alternatív következtetés vonható le:

- a DSA felhagyott azzal a megközelítéssel, hogy egy hibrid szolgáltató felelőssége az alapján állapítható meg mely funkciója érintett az adott jogvitában, vagy
- az EB már megkezdte a platform DSA szerinti definíciójának kiterjesztő értelmezését azáltal, hogy abba már nem csupán a kizárólagosan tárhelyszolgáltatást nyújtó közvetítő szolgáltatók, hanem azon szolgáltatók is beletartoznak, amelyek csak részben nyújtanak tárhelyszolgáltatást (feltéve, hogy a tárhelyszolgáltatás nem egy másik szolgáltatás kisebb jelentőségű és pusztán kiegészítő eleme, vagy a főszolgáltatás kisebb jelentőségű funkciója.)

Bármely következtetés legyen is a helyes, az elkerülhetetlenül komoly kihívásokat fog támasztani a joggyakorlatban. Véleményem szerint a középpontban elsősorban a hibrid szolgáltatók által kínált különböző közvetítői szolgáltatások közötti kapcsolat megítélése fog állni. Ezen kérdés megválaszolása ugyanis szükséges lesz annak megállapításához, hogy (i) a hibrid szolgáltató mely közvetítő szolgáltató kategóriájába tartozik kizárólagosan, és így a DSA mely rendelkezései alapján vonható felelősségre; vagy (ii) az adott hibrid szolgáltató platformnak minősülhet-e.

8.3.2. A felelősség alóli mentesség csak akkor alkalmazható, ha az érintett tartalmat a szolgáltatást igénybe vevője biztosítja

A közvetítő szolgáltatások meghatározásából következik, hogy a DSA által biztosított felelősség alóli mentesség csak akkor alkalmazható, ha az információt a szolgáltatás igénybe vevője szolgáltatja. Ezt a DSA (18) preambulumbekkezdése is megerősíti, amely kimondja, hogy a felelősség alóli, a DSA-ban megállapított mentességet nem lehet alkalmazni, amennyiben a közvetítő szolgáltató szolgáltatása nem korlátozódik a szolgáltatás igénybe vevője által biztosított információk pusztán technikai és automatikus kezelésére.

³¹ Commission decision of 25.4.2023 designating Facebook as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council, (1) preambulumbekkezdés.

De mi minősül a szolgáltatás igénybe vevője által biztosított információnak? Bár a DSA nem határozza meg ezt a fogalmat, a DSA (18) preambulumbekzdése legalább tisztázza, hogy mi nem minősül annak. A DSA (18) preambulumbekzdése kimondja, hogy a mentesség „nem adható meg a nem a szolgáltatás igénybe vevője, hanem maga a közvetítő szolgáltató által nyújtott információkért való felelősség tekintetében, beleértve azt az esetet, amikor az információt a szolgáltató szerkesztőségi felelőssége mellett állították elő.”

A DSA (18) preambulumbekzdése a tárhelyszolgáltatók felelőssége tekintetében a korábban (*common law* alatt) kialakult megközelítést tükrözi. A DSA egyszerűen megismétli, hogy amennyiben a közvetítő szolgáltató szerkesztői ellenőrzést gyakorol, a felelősség alóli mentesség nem alkalmazható. Ennek eredményeképpen leszögezhető, hogy továbbra sem világos, hogy pontosan mikor is gyakorol szerkesztői ellenőrzést a közvetítő szolgáltató.

A hagyományos értelemben vett szerkesztői ellenőrzés a tartalom létrehozását, kiválasztását vagy szerkesztését jelenti a közzététel előtt.³² A platformok ilyen tevékenységet azok szó szoros értelmében nyilvánvalóan nem végeznek. Ugyanakkor a közösségimédia-platformok – mint például a Facebook és az X – fejlett technológiákat (pl. mesterséges intelligencia, gépi tanulás és a kiterjesztett valóság) alkalmaznak a tartalom önkéntes moderálása érdekében. A platformok tehát nemcsak az elfogadható tartalom határait határozzák meg, hanem e szabályok betartatása érdekében széles köben alkalmaznak különböző eljárásokat, posztokat távolítanak el, illetve fiókokat törölnek. Emellett a platformok algoritmusok, illetve mesterséges intelligencia segítségével személyre szabott tartalmakat mutatnak a felhasználóknak a róluk,³³ valamint a korábbi interakcióikról gyűjtött adatok alapján.³⁴ A platformok tevékenysége tehát effektíve ahhoz hasonlítható, mint amikor egy szerkesztő/kiadó valamennyi olvasó számára személyre szabott újságot készít.

A DSA-hoz fűzött kommentárok szerint³⁵ a felhasználók által a digitális platformokra ‘pusholt’ (azaz feltöltött) információkat a felhasználók által generált tartalomnak kell minősíteni, még abban az esetben is, ha a felhasználók által tett erőfeszítés minimális. Ezzel szemben, amikor a szolgáltatók külső forrásokból ‘húzzák’ (azaz összegyűjtik és átdolgozzák) az információkat, az ilyen szolgáltatások nem tartoznak a DSA által megállapított felelősségi mentességek hatálya alá.

Azonban még a ‘pusholt tartalom’ kategóriáján belül is nehéz egyértelmű határokat húzni. A legtöbb jogi szakértő például a Spotifyt az általa válogatott zenék kurátorának és közvetítőjének minősítené, míg ugyanezek az emberek mellett foglalnának állást, hogy az Apple Store kizárólag a felhasználók (programozók) által készített tartalmat közvetíti a nyilvánosság felé. Ez a megkülönböztetés azonban meglehetősen önkényes.

Egyrészt mind a Spotify, mind pedig az Apple Store minimális felügyeletet gyakorol a feltöltött tartalmak felett, másrészt mind a Spotify, mind pedig az az Apple Store harmadik felektől – azaz a tartalmat feltöltő zenészek ügynökeitől, illetve az applikációkat feltöltő fejlesztőktől – származó tartalmakat forgalmaz.³⁶

³² OSTER (2015): 58.

³³ HUSZÁR (2025): 215–217.

³⁴ SCHWEMER (2023)

³⁵ KOLTAY (2024b): 43–44.; HUSOVEC (2024): 98.

³⁶ HUSOVEC (2024): 98.

A technológiai fejlődéssel párhuzamosan nem valószínű, hogy eltűnik annak nehézsége, hogy mikor tekinthető az információ a szolgáltatás címzettje által szolgáltatottnak, sőt, a kihívás valószínűleg egyre összetettebbé válik majd a közeljövőben. A *'pull'* és a *'push'* közötti hagyományos kettősség valószínűleg még inkább elmosódik, amint azt a közösségi médiában a generatív chatbotok megjelenése mutatja.³⁷ Ezek az eszközök képesek homályossá tenni a felhasználók tényleges hozzájárulását. Azokban az esetekben, amikor a felhasználók részvétele nem nyilvánvaló, felmerül a kérdés: tekinthető-e a tartalom még mindig felhasználó által generáltnak.³⁸

8.3.3. A közvetítő szolgáltatónak semlegesnek kell lennie a felhasználó által generált tartalmat érintően

A harmadik feltétel, amelyet a közvetítő szolgáltatóknak teljesíteniük kell annak érdekében, hogy a felelősség alól mentesüljenek, az EUB-nek az Eker. irányelv (42) preambulumbekkezdésével és 12–15. cikkével kapcsolatban kialakított ítélkezési gyakorlatából³⁹ következik. Eszerint a közvetítő szolgáltatók csak akkor nem vonhatók felelősségre a tárolt/továbbított információkért, ha szerepük semleges a felhasználó által generált tartalommal kapcsolatban, azaz magatartásuk pusztán technikai, automatikus és passzív, és nem ismerik vagy ellenőrzik az általuk tárolt/továbbított adatokat.

A DSA megtartotta ezen 'semlegességi doktrínát'.⁴⁰ A DSA a (18) preambulumbekkezdésben újfogalmazta az Eker. irányelv (42) preambulumbekkezdését – amely eredetileg a semlegességi doktrínát kialakította –, és megismételte az EUB ítélkezési gyakorlatában szereplő kritériumokat.⁴¹ Ennek eredményeképpen azonban – álláspontom szerint – több jogértelmezési kérdés továbbra is megválaszolatlan marad.

Tekintettel arra, hogy az EUB ítélkezési gyakorlata korábban részletesen ismertetésre került, a jelen alfejezet kizárólag a YouTube-ügyben hozott ítélet és a főtanácsnoki indítvány főbb megállapításait foglalja össze.

Az EUB megállapította, hogy az algoritmikus kategorizálás, személyre szabás, rangsorolás vagy keresés biztosítása nem jelenti azt, hogy a szolgáltatónak tudomása lenne a jogellenes tartalomról. Nem elegendő, hogy a szolgáltatónak absztrakt tudomása van arról (azaz általános jelleggel tudatában van annak), hogy szolgáltatása jogsértő tartalmat hordoz.⁴²

³⁷ Kovács Andrea (2025).

³⁸ Husovec (2024): 99.

³⁹ Lásd például: Google France SARL és Google Inc. kontra Louis Vuitton Malletier SA (C-236/08), Google France SARL kontra Viaticum SA és Luteciel SARL (C-237/08) és Google France SARL kontra Centre national de recherche en relations humaines (CNRRH) SARL és társai (C-238/08), ECLI:EU:C:2010:159; C-324/09, L'Oréal SA és társai kontra eBay International AG és társai, ECLI:EU:C:2011:474; C-521/17, Coöperatieve Vereniging SNB-REACT UA kontra Deepak Mehta, ECLI:EU:C:2018:639; C-682/18; C-683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503.

⁴⁰ Wagner (2023): 6–7.

⁴¹ Gosztonyi (2022b): 67.

⁴² C-682/18. és C-683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 111. és 114.

Mindebből következően tehát a modern digitális szolgáltatások leggyakoribb tevékenységei nem fosztják meg a szolgáltatókat őket megillető felelősség alóli mentességtől, hiszen:

- a jogsértő tartalmak felderítését segítő tartalomfigyelő eszközök telepítése nem minősül olyan aktív beavatkozásnak, amely kizárja őket a semlegességből,⁴³ és
- a közvetítő szolgáltató szerepe semleges, ha csupán a szolgáltatást igénybe vevője által biztosított információk feldolgozásában, kezelésében vesz részt. A szolgáltató aktív szerepéről csak akkor beszélhetünk, ha a szolgáltató „ismeri vagy ellenőrzi” azokat az információkat, tartalmakat, amelyeket a szolgáltatást igénybe vevő kérésére tárol. Az aktív szerep tehát megköveteli a szolgáltatótól, hogy megszerezze a felhasználó által létrehozott tartalom feletti szellemi ellenőrzést. Ez a helyzet akkor áll fenn, ha a szolgáltató választja ki a tárolt információkat, ha valamilyen más módon aktívan részt vesz az információk tartalmának kialakításában, vagy ha az információkat úgy tárja a nyilvánosság elé, hogy azok a sajátjának tűnnek.⁴⁴

8.4. A platformok felelősség alóli mentessége

A DSA nem rendelkezik külön arról, hogy a platformok milyen feltételek mellett mentesülhetnek az általuk nyilvánosság felé közvetített jogsértő tartalmakért való felelősség alól. Tekintettel azonban arra, hogy a platformok a tárhelyszolgáltatók egy speciális típusának minősülnek, erre valójában nincs is szükség. Elegendő ugyanis annak vizsgálata, hogy a tárhelyszolgáltatók milyen felételek mellett élvezhetik a felelősség alóli mentességet a DSA 6. cikke alapján. Jelen alfejezet célja tehát ennek a kérdésnek a megválaszolása.

Az Eker. irányelv által létrehozott – korábban bemutatott – értesítési és eltávolítási felelősségi rendszer⁴⁵ (különösen felelősség korlátozására vonatkozó rendelkezések horizontális jellege) döntő szerepet játszott abban, hogy az újszerű digitális szolgáltatások villámgyorsasággal terjednek el az EU belső piacán.⁴⁶ Az Eker. irányelv által kialakított szabályozási környezetben jelent meg például 2003-ban a Facebook, 2005-ben a YouTube vagy 2006-ban a Twitter.⁴⁷ Az európai digitális piac növekedésének biztosítása érdekében az európai jogalkotó – nem meglepő módon – e jogi keret megőrzése mellett döntött.⁴⁸ A DSA ezért az Eker. irányelv 12–15. cikkeit lényegében szó szerint átültette a DSA 4–8. cikkeibe. Mivel azonban az Eker. irányelv képtelen volt számos olyan (jogi) problémát kezelni, amelyek az elfogadása után elterjedt digitális szolgáltatásokkal (pl. a közösségi médiával) összefüggésben merültek fel, a DSA szükségszerűen igyekezett ezeket a szabályozási hiányosságokat betölteni részben az EUB ítélkezési gyakorlatának beépítésével, részben pedig az Eker. irányelv 12–15. cikkeinek finomhangolásával.

⁴³ Uo., 109.

⁴⁴ Uo., 152.

⁴⁵ DE STREEL et al. (2020): 10.

⁴⁶ DSA (16) preambulumbekzdés.

⁴⁷ HUSOVEC (2024): 94.

⁴⁸ DSA (16) preambulumbekzdés.

A DSA 6. cikkének (1) bekezdése szerint a tárhelyszolgáltató nem felelős a szolgáltatás igénybe vevőjének kérésére tárolt információkért, ha (i) a tárhelyszolgáltatónak nincs tényleges tudomása a jogellenes tevékenységről vagy jogellenes tartalomról, és nincs tudomása olyan tényekről vagy körülményekről, amelyekből a jogellenes tevékenység vagy jogellenes tartalom nyilvánvalóvá válik; vagy (ii) a tárhelyszolgáltató a tudomásszerzést követően haladéktalanul intézkedik a jogellenes tartalom eltávolításáról vagy az ahhoz való hozzáférés megszüntetéséről. A tárhelyszolgáltató tehát csak akkor mentesülhet a felelősség alól, ha bizonyítani tudja, hogy nem volt tudomása a jogellenes tartalomról, vagy haladéktalanul intézkedett ezen jogellenes tartalom eltávolításáról.⁴⁹

A jogellenes tartalomról vagy tevékenységről való tényleges tudomásszerzés többféle módon történhet. A közösségimédia-platformok esetében a leggyakoribb módszer a felhasználó által küldött értesítés. Az ilyen értesítésnek kellően konkrétnek kell lennie, azaz lehetővé kell tennie egy gondosan eljáró gazdasági szereplő számára, hogy a jogellenes tartalmat azonosítsa, értékelje és azzal szemben fellépjen.⁵⁰ A tárhelyszolgáltató kellően konkrét értesítés hiányában is felelősségre vonható a jogellenes tartalom tárolásáért, ha „valamilyen módon tudomást szerzett olyan tényekről vagy körülményekről, amelyek alapján egy gondos gazdasági szereplőnek fel kellett volna ismernie a jogellenességet.”⁵¹ Ebből azonban az is következik, hogy a tárhelyszolgáltató akkor is felelősségre vonható az általa tárolt jogellenes tartalomért, ha a felhasználó értesítése ugyan nem volt elég konkrét vagy kellően megalapozott, de a tárhelyszolgáltató az általa lefolytatott vizsgálat során képes volt azonosítani a jogellenes tevékenység vagy információ fennálltát.⁵² A tárhelyszolgáltató tényleges tudásának megállapításához azonban soha nem elegendő annak általános ismerete, hogy a szolgáltatást jogellenes tartalom tárolására használják.⁵³

A fentiekkel kapcsolatban a gyakorlatban leggyakrabban felmerülő kérdés az, hogy a szolgáltató önkéntes vizsgálata során szerzett információk alapján megállapítható-e a tárhelyszolgáltató tényleges vagy vélelmezett tudomásszerzése. Az EUB erre a kérdésre egyértelmű igennel válaszolt. A YouTube-ügyben például az EUB úgy ítélte meg, hogy a tárhelyszolgáltató „a saját kezdeményezésére folytatott vizsgálat eredményeként” elegendő ismeretet szerezhet a jogellenes tevékenységről.⁵⁴

A tárhelyszolgáltató abban ez esetben is mentesülhet a felelőssége alól, ha tényleges tudomást szerzett a jogellenes tartalomról vagy tevékenységről, feltéve, hogy „haladéktalanul intézkedik [intézkedett] a jogellenes tartalom eltávolításáról vagy az ahhoz való hozzáférés megszüntetéséről.”⁵⁵ Noha több tárhelyszolgáltató az Eker. irányelv hiányosságaként

⁴⁹ NOVÓVIC (2024): 82.

⁵⁰ HOFMANN–RAUE (2025): 331–332.

⁵¹ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 115.

⁵² DSA (22) preambulumbekkezdés.

⁵³ Uo.

⁵⁴ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 115.

⁵⁵ DSA 6. cikk (1) b).; ZÖDI (2023): 189.

emelte ki, hogy az nem határozta meg egyértelműen a ‘haladéktalanul’ követelmény pontos tartalmát, a DSA e tekintetben szintén nem ad iránymutatást. A DSA ezen döntését azzal indokolta, hogy a haladéktalanul *terminus technicus* estenként értékelendő elsősorban a bejelentett jogellenes tartalom típusának és az intézkedés sürgősségének figyelembevételével, hiszen „az ilyen szolgáltatóktól például elvárható, hogy késedelem nélkül cselekedjenek, ha olyan állítólagos jogellenes tartalomról érkezik bejelentés, amely személyek életét vagy biztonságát veszélyezteti.”⁵⁶ Mindezek eredményeképpen a jogellenes tartalom eltávolítására nyitva álló idő tagállamonként továbbra is eltérő marad.

Fontos kiemelni, hogy bár a DSA 6. cikke mentesíti a tárhelyszolgáltatókat a felelősség alól a jogellenes tartalmak tárolása esetén, ez nem jelenti azt, hogy nem kötelesek részt venni a jogsértés megszüntetésében vagy megelőzésében.⁵⁷ Ezt a DSA 6. cikkének (4) bekezdése is megerősíti, amely szerint a 6. cikk nem érinti a bíróság vagy közigazgatási hatóság azon lehetőségét, hogy a szolgáltatót a jogsértés megszüntetésére vagy megakadályozására kötelezze. A gyakorlatban az ilyen (bírósági vagy közigazgatási) döntés a szolgáltatót a jogellenes tartalom eltávolítására vagy az ahhoz való hozzáférés megakadályozására kötelezi.⁵⁸ A tárhelyszolgáltatókkal szemben elfogadható végzések köre azonban nem korlátlan. Az EUB ítélkezési gyakorlata szerint a jogsértés megszüntetésére irányuló végzés csak akkor áll összhangban az uniós joggal, ha (i) figyelembe veszi az alapvető jogok védelméből eredő követelményeket,⁵⁹ és (ii) méltányos egyensúlyt teremt a szóban forgó jogok és érdekek között (beleértve az ilyen intézkedések által érintett egyének alapvető jogait is).⁶⁰ A Scarlet Extended SA kontra SABAM-ügyben például az EUB úgy ítélte meg, hogy egy olyan végzés, amely az ISP hálózatán keresztül folytatott valamennyi elektronikus kommunikációt, időbeni korlátozás nélkül figyelő, szűrőrendszer telepítését írja elő, aránytalanul korlátozza:

- az ISP üzletvitelhez való jogát (mivel az ISP-nek saját költségén complex számítógépes rendszert kellene telepítenie);
- az ISP ügyfeleinek a magánélethez és az adatvédelemhez való jogát (mivel beszélgetéseiket folyamatosan figyelnék és szisztematikusan elemeznék); és
- az ISP ügyfeleinek az információ fogadásához vagy továbbításához való jogát (mivel a szűrőrendszer potenciálisan a jogszerű kommunikáció blokkolásához is vezethetne).⁶¹

Az EUB többször elutasította a szolgáltatókat nem konkrét intézkedések végrehajtására fel szólító végzések és ítéletek helybenhagyását, vagy úgy, hogy azokat érvénytelennek minősí-

⁵⁶ DSA (52) preambulumbekkezdés.

⁵⁷ Novovic (2024): 84.

⁵⁸ DSA (25) preambulumbekkezdés.

⁵⁹ C-70/10, Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771, 41.

⁶⁰ C-70/10, Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771, 44–46.; C-275/06, Productores de Música de España (Promusicae) kontra Telefónica de España SAU, ECLI:EU:C:2008:54, 68.

⁶¹ C-70/10, Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771, 48. és 50–53.

tette,⁶² vagy úgy, hogy azokat nem találta eléggé konkrétnek.⁶³ A jogsértés megszüntetésére irányuló felszólításnak ezért kellően konkrétnek kell lennie, lehetővé téve a szolgáltató számára a jogellenes tartalom azonosítását és felkutatását.

Végezetül fontos kiemelni, hogy a DSA 8. cikke – az Eker. irányelv 15. cikkéhez hasonlóan – az általános monitorozás előírásának tilalmát fogalmazza meg.⁶⁴ Vagyis a tárhelyszolgáltatókkal szemben nem állapítható meg olyan kötelezettség, amely alapján (i) az általuk tárolt információkat nyomon kellene követniük; vagy (ii) a jogellenes tevékenységre utaló tényeket vagy körülményeket ki kellene vizsgálniuk.⁶⁵ Az általános monitoring tilalma (a gyakorlati kivitelezhetetlenségének nehézsége mellett) elsősorban arra vezethető vissza, hogy „annak bevezetése gyakorlatilag internetes cenzárt valósítana meg”.⁶⁶ Az EUB az általános nyomon követés fogalmát hagyományosan tágan értelmezte. Így az alá tartozott minden olyan előírás, „amely az online platformokat arra kívánta kötelezni, hogy a jogsértések kiszűrése érdekében a szolgáltatás valamennyi felhasználójának valamennyi tartalmát ellenőrizték.”⁶⁷ 2019-re azonban az EUB már meghaladta a korábban kialakított joggyakorlatát. Felismerve annak tényleges veszélyét, hogy a korábban jogellenesnek minősített információt más felhasználó ismét létrehozhatja, illetve megoszthatja, az EUB a Glawischnig-Piesczek-ügyben már akként foglalt állást, hogy a nemzeti bíróság jogszerűen kötelezheti a szolgáltatót arra, hogy a korábban jogellenesnek nyilvánított információval azonos tartalmú, tárolt információt törölje, vagy az ahhoz való hozzáférést megakadályozza.⁶⁸

8.5. A platformok felelőssége az EJEB ítélkezési gyakorlata szerint

A korábbiakban részletesen elemeztem, hogy a platformok milyen feltételek mellett vonhatók felelősségre az általuk tárolt és nyilvánosság felé közvetített jogellenes tartalmakért a DSA alapján. A platformok felelősségre vonása a platformok számára az EJEE 10. cikke által biztosított véleménynyilvánítás szabadságába való beavatkozásnak minősül,⁶⁹ így elkerülhetetlen, hogy röviden szóljak arról, hogy a platformok véleménynyilvánítás-szabadsága milyen feltételek mellett korlátozható jogszerűen az EJEB joggyakorlata szerint.

⁶² Lásd például: C-70/10, Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771.

⁶³ Lásd például: C-314/12, UPC Telekabel Wien GmbH kontra Constantin Film Verleih GmbH és Wega Filmproduktionsgesellschaft mbH, ECLI:EU:C:2014:192; C-484/14 Tobias, Mc Fadden kontra Sony Music Entertainment Germany GmbH, EU:C:2016:689; C-18/18, Eva Glawischnig-Piesczek kontra Facebook Ireland Limited, ECLI:EU:C:2019:821.

⁶⁴ KOLTAY (2024a): 244.

⁶⁵ GOSZTONYI–GALEWSKA–ŠKOLKAY (2024)

⁶⁶ GYETVÁN (2021)

⁶⁷ SZIKORA (2024c): 305.

⁶⁸ C-18/18, Eva Glawischnig-Piesczek kontra Facebook Ireland Limited, ECLI:EU:C:2019:821, 53.

⁶⁹ Magyar Jeti Zrt. kontra Magyarország, App no. 11257/16 (2018. december 4.), 56.; Magyar Tartalom-szolgáltatók Egyesülete és Index.hu Zrt. kontra Magyarország, App no. 22947/13 (2016. február 2.), 45.

A platformok véleménynyilvánítás-szabadságának korlátozása csak akkor lehet jogszerű, ha a beavatkozást jog írja elő, az EJEE 10. cikkének (2) bekezdésére tekintettel jogszerű célt szolgál, és egy demokratikus társadalomban szükséges.⁷⁰ Annak megítéléséhez, hogy a beavatkozás szükséges-e egy demokratikus társadalomban, az EJEB a következő vizsgálandó tényezőket határozta meg:

- a hozzászólások tartalma és kontextusa;
- a kérelmező által a jogellenes tartalom eltávolítása vagy megakadályozása érdekében alkalmazott intézkedések;
- a hozzászólások szerzőinek felelősségre vonásának lehetősége a közvetítő szolgáltatók felelősségének alternatívájaként; és
- a nemzeti eljárás során alkalmazott jogkövetkezmények.⁷¹

8.5.1. A hozzászólások tartalma és kontextusa

A jogellenes tartalom jellege alapvető szerepet játszik annak eldöntésében, hogy a véleménynyilvánításhoz való jog korlátozása arányos-e. Ha a tartalom gyűlöletbeszédnek és az egyének testi épségét közvetlenül fenyegető fenyegetésnek minősül, mások és a társadalom egészének jogai és érkei indokolhatják a közvetítő szolgáltató felelősségre vonását az ilyen tartalomért, ha az „nem hozott intézkedéseket az egyértelműen jogellenes megjegyzések haladéktalan eltávolítása érdekében, még az állítólagos sértett vagy harmadik fél értesítése nélkül is”.⁷² Másrészt az EJEB megállapította, hogy az olyan rágalmozó tartalom, amely ‘csupán’ sérti valakinek a jóhírnevét, nem tekinthető egyértelműen jogellenesnek (*clearly unlawful*),⁷³ és ezért a közvetítő szolgáltatóknak a jogellenes tartalom előzetes szűrésére való kötelezése aránytalan korlátozást jelentene a közvetítő szolgáltatók véleménynyilvánítási szabadságában.⁷⁴

A hozzászólások tartalmával és kontextusával kapcsolatban az EJEB továbbá azt is vizsgálja, hogy (i) az online közvetítő szolgáltatóknak gazdasági érdeke fűződik-e a megjegyzések tárolásához, illetve közzétételéhez; (ii) a közvetítő szolgáltatók milyen mértékű ellenőrzést gyakorolnak a megjegyzések felett; és (iii) a közvetítő szolgáltatók a tartalom illetve kommentek nyilvánosság számára való terjesztésében betöltött szerepe túlmutatott-e a passzív, pusztán technikai szolgáltatói szerepvállaláson.⁷⁵

Az utóbbi kritériummal kapcsolatban érdemes megjegyezni, hogy az EJEB és az EUB joggyakorlata eltér abban a tekintetben, hogy milyen feltételek mellett minősülhet a közvetítő szolgáltató szerepe passzív, pusztán technikai jellegűnek. Így például, a Sanchez kontra

⁷⁰ GOSZTONYI–PRIBULA–LENDVAI (2025)

⁷¹ Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 142–143.; Magyar Tartalomszolgáltatók Egyesülete és Index.hu Zrt. kontra Magyarország, App no. 22947/13 (2016. február 2.), 69.

⁷² Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 159.; Magyar Tartalomszolgáltatók Egyesülete és Index.hu Zrt. kontra Magyarország, App no. 22947/13 (2016. február 2.), 91.

⁷³ Magyar Jeti Zrt. kontra Magyarország, App no. 11257/16 (2018. december 4.), 82.; WIŚNIEWSKI (2021): 125–126.

⁷⁴ KÓCZIÁN (2016)

⁷⁵ Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 144–146. o.; Magyar Tartalomszolgáltatók Egyesülete és Index.hu Zrt. kontra Magyarország, App no. 22947/13 (2016. február 2.), 73.

Franciaország-ügyben, az EJEB a kérelmező felelősségét állapította meg a Facebook-oldalán elhelyezett – és el nem távolított – jogsértő kommentekért, többek között azon az alapon, hogy tudta, vagy legalábbis előre láthatta, hogy a Facebook-falán mások által megosztott kommentek jogsértőek lehetnek.⁷⁶ Ezzel szemben, ahogyan azt fentebb részletesen kifejtettem, az EUB joggyakorlata értelmében a tárhelyszolgáltató nem tartozik felelősséggel az általa tárolt jogellenes tartalomért pusztán azért mert absztrakt tudomása van arról (azaz általános jelleggel tudatában van annak), hogy szolgáltatása jogsértő tartalmat hordoz.⁷⁷

8.5.2. A kérelmező által a jogellenes tartalom eltávolítása vagy megakadályozása érdekében alkalmazott intézkedések

A megfelelő intézkedések terjedelme több tényezőtől függ, és azt eseti alapon kell meghatározni. Ha például egy tartalom nem egyértelműen jogellenes, akkor egy gyors reagálást lehetővé tevő, hatékony eljárásokkal kísért értesítési és eltávolítási eljárás is elégségesnek bizonyulhat. Egyértelműen jogellenes tartalom esetén azonban a közvetítő szolgáltatóknak további intézkedéseket kell bevezetniük, amelyek lehetővé teszik az általános, megelőző monitorozást.⁷⁸

Az EJEB a közvetítő szolgáltató szerepét és tulajdonságait is figyelembe veszi, amikor a szükséges intézkedések köréről dönt. Egyrészt az EJEB elismerte, hogy a nagy weboldalak, platformok fontos szerepet játszanak „a nyilvánosság hírekhez való hozzáféréseinek előmozdításában és általában az információ terjesztésének megkönnyítésében”.⁷⁹ Másrészt az EJEB azt is elismerte, hogy az interneten megjelenő tartalmak és a kommunikáció kárt is képesek okozni.⁸⁰ Az EJEB megállapította továbbá, hogy egy potenciális sértett számára korlátozott lehetőségek állnak a rendelkezésére az internet folyamatos monitorozása, a jogellenes tartalmak beazonosítása és eltávolítása érdekében. Ezzel szemben a közvetítő szolgáltatók sokkal gyorsabban képesek a jogsértő kommenteket, azok megosztása után eltávolítani.⁸¹

Az EJEB joggyakorlata értelmében a közvetítő szolgáltatók által alkalmazott intézkedések hatékonyságát is figyelembe kell venni. Például a Delfi AS kontra Észtország-ügyben az EJEB megállapította, hogy bár a Delfi nem hanyagolta el teljes mértékben a jogellenes tartalmak szűrésére és ezáltal a harmadik felek megkárosításának megelőzésére vonatkozó kötelezettségét, intézkedései mégsem teljesítették a céljukat, mivel az egyértelműen jogellenes kommentek hat hétig elérhetők maradtak.⁸²

⁷⁶ GOSZTONYI–LENDVAI (2023b): 47.

⁷⁷ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 111. és 114.

⁷⁸ Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 159.

⁷⁹ Ahmet Yildirim kontra Törökország, App. no. 3111/10 (2012. december 18.) 48.; Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 157.

⁸⁰ Editorial Board of Pravoye Delo és Shtekel kontra Ukrajna, App. no. 33014/04 (2011. május 5.), 63.

⁸¹ Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 153. és 158.

⁸² Megelőző intézkedésként a Delfi automatikus, szóalapú szűrőt és egy értesítési és eltávolítási rendszert vezetett be, továbbá külön moderátorcsoportot is létrehozott, valamint megtiltotta az olyan kommentek közzétételét, amelyek „ellentételek a jó gyakorlattal, vagy fenyegetést, sértést, obszcén kifejezéseket vagy trágárságokat tartalmaznak, illetve ellenségeskedésre, erőszakra vagy illegális tevékenységre buzdítanak.” PAPP (2017).

8.5.3. A hozzászólások szerzőinek felelősségre vonásának lehetősége a közvetítő szolgáltatók felelősségének alternatívájaként

A legnagyobb akadály, amellyel a sértettnek várhatóan szembe kell néznie, a szerzők anonimitása. Bár az anonimitás hatékony eszköz az eszmék és az információk szabad áramlásának biztosítására az interneten, az egyben súlyosbítja a jogellenes beszéd gyors terjedését: szükséges mindezért a más jogokkal és érdekekkel szembeni egyensúlyra való törekvés. Bár az anonimitás különböző fokozata áll az internetfelhasználók rendelkezésére és a teljes és állandó anonimitás nehezen elérhető, a sérelmet szenvedő számára még mindig szinte lehetetlen, hogy a hozzászólások szerzőivel szemben hatékonyan fellépjen.⁸³

⁸³ Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 147–148. és 151.; GOSZTONYI–HUSZÁR (2022).

9. A DSA által a platformokkal szemben előírt kellő gondossági kötelezettségek

Felismerve a platformok társadalomban betöltött központi szerepét és az egyén szabadságára és jogaira gyakorolt jelentős hatását, a DSA – az Eker. irányelvben korábban foglaltakon túlmenően – számos kellő gondossági kötelezettséget ír elő a platformokkal szemben. A DSA egy úgynevezett bináris rendszert vezetett be: egyrészt a platformok főszabály szerint mentesülnek a jogellenes tartalmak tárolásáért, illetve nyilvánosság részére történő terjesztéséért való felelősség alól, másrészt azonban – a jogellenes tartalomért való felelősségüktől függetlenül – a platformok kötelesek a DSA III. fejezetében előírt kellő gondossági kötelezettségeket betartani.¹ Az EU láthatóan egy finom egyensúlyt kívánt megteremteni a platformok vonatkozásában, amelynek értelmében a platformok ugyan nem vonhatók felelősségre a rajtuk elhelyezett jogellenes tartalomért, de elszámoltathatók a szolgáltatásaik által kiváltott társadalmi hatások, illetve a szolgáltatásaikban rejlő kockázatok kezeléséért.²

Fontos azonban megjegyezni, hogy a platformok felelősségére és a kellő gondossági kötelezettségeikre vonatkozó rendelkezések a DSA-ban bizonyos átfedéseket mutatnak. A DSA 16. cikke szerint például olyan mechanizmusokat kell a tárhelyszolgáltatóknak létrehozniuk, amelyek lehetővé teszik, hogy bárki értesítse őket a szolgáltatásukon található jogellenes tartalmakról.³ Ha az ilyen értesítés eredményeként a tárhelyszolgáltató a DSA 6. cikke szerinti tényleges tudomást szerez a jogellenes tartalomról, úgy a szolgáltató felelősséggel tartozik annak tárolásáért és nyilvánosság részére való terjesztéséért, kivéve, ha haldéktalanul intézkedik az adott tartalom eltávolítása érdekében.

¹ BUITEN (2021): 373.

² Érdeességként érdemes megjegyezni, hogy a DSA az EU és a nagy technológiai vállalatok között kötött alku – hosszú tárgyalások eredményeként született meg. Az Európai Parlament ugyanis hosszú ideig ragaszkodott ahhoz, hogy a platformok jogellenes tartalom tárolásáért való felelősségük alóli mentességét a kellő gondossági kötelezettségek betartásához kössék. Így a DSA III. fejezet bármilyen módon való megsértése a DSA 6. cikke szerinti felelősség alóli mentesség elvesztéséhez vezetett volna. Az Európai Parlament azzal érvelt ugyanis, hogy a felelősség alóli mentesség olyan kiváltság, amely csak azoknak jár, akik a törvényt teljes egészében tiszteletben tartják. Ez a szigorú megközelítés azonban nem került be a DSA végleges normaszövegébe.

³ LENDVAI (2024a): 79–80.

A DSA az alkalmazandó kellő gondossági kötelezettségek körét a szolgáltató típusának függvényében határozza meg. A DSA 11–15. cikkeiben előírt kellő gondossági kötelezettségek valamennyi közvetítő szolgáltatóra vonatkoznak, míg a 16–18. cikkeiben foglaltak csak a tárhelyszolgáltatók, a 19–32. cikkeiben meghatározottak csak a platformok, míg a 33–43. cikkeiben felsoroltak csupán az online óriásplatformok számára állítanak fel kötelezettségeket.

A DSA által előírt kellő gondossági kötelezettségek az általuk elérni kívánt célkitűzések alapján három kategóriába sorolhatók:

- tartalommoderálás, amely elsősorban a platform tartalommal összefüggő döntéseinek meghozatalának folyamatára vonatkozik;
- átláthatóság, amely a szolgáltatás átláthatóságát hivatott biztosítani; és
- kockázatkezelés, amely arra vonatkozó kötelezettségeket foglal magában, hogy a platformnak hogyan kell kezelnie és csökkentenie a szolgáltatás működéséből és használatából eredő kockázatokat.

3. táblázat: A DSA által előírt kellő gondossági kötelezettségek⁴

Kellő gondossági kötelezettségek	Valamennyi közvetítő szolgáltatóra alkalmazandó	Valamennyi tárhelyszolgáltatóra alkalmazandó	Valamennyi platformra alkalmazandó	Kizárólag online óriásplatformokra alkalmazandó
Tartalom-moderálással összefüggő kötelezettségek	14. cikk (tisztességes szerződési feltételek)	16. cikk (bejelentési és cselekvési mechanizmusok) 17. cikk (indokolás) 18. cikk (bűncselekmények gyanújának bejelentése)	20. cikk (belső panaszkezelési rendszer) 21. cikk (peren kívüli vitarendezés) 22. cikk (megbízható bejelentők) 23. cikk (visszaélésekkel szembeni intézkedések és védelem) 30-32. cikkek (speciális rendelkezések a B2C szolgáltatások kapcsán)	38. cikk (ajánlórendszerek) 34-35. cikkek (kockázatkezelés) 45-48. cikkek (magatartási kódexek)

⁴ Forrás: HUSOVEC (2024): 184.

Kellő gondossági kötelezettségek	Valamennyi közvetítő szolgáltatóra alkalmazandó	Valamennyi tárhelyszolgáltatóra alkalmazandó	Valamennyi platformra alkalmazandó	Kizárólag online óriásplatformokra alkalmazandó
Kockázatkezeléssel összefüggő kötelezettségek	N/A		25. cikk (online interfész tervezése és kialakítása) 26. cikk (3) bek. (profilozáson alapuló hirdetés az online platformokon) 27. cikk (ajánlórendszerek átláthatósága) 28. cikk (kiskorúak online védelme) 30. cikk (kereskedők nyomonkövethetősége) 31. cikk (beépített megfelelés a kialakítás által)	
Átláthatósággal összefüggő kötelezettségek	11. cikk (hatóságok kapcsolattartó pontjai) 12. cikk (kapcsolattartó pontok a szolgáltatásokat igénybe vevők számára) 13. cikk (jogi képviselők) 15. cikk (átláthatósági jelentési kötelezettségek)	N/A	22. cikk (megbízható bejelentők) 24. cikk (átláthatósági jelentési kötelezettségek) 26. cikk (hirdetés az online platformokon)	37. cikk (független ellenőrzés) 39. cikk (online hirdetések átláthatósága) 40. cikk (adatokhoz való hozzáférés és az adatok vizsgálata) 41. cikk (megfelelést támogató szervezeti egység) 42. cikk (átláthatósági célú jelentéstételi kötelezettség)

Bár valamennyi kellő gondossági kötelezettség önmagában megérdemelne egy külön fejezetet, monográfiámban kizárólag a vizsgált fiktív Hillary Clinton-jogeset szempontjából legfontosabb kötelezettségeket kívánom bemutatni. Így a következőkben a platformok tartalom-moderálását és a platformok ajánlórendszereivel összefüggésben elfogadott gondossági kötelezettségeket elemzem.

9.1. A platformok tartalommoderálásával összefüggésben előírt kellő gondossági kötelezettségek

9.1.1. A tartalommoderálás meghatározása és a DSA szerinti irányadó eljárás

A DSA 3. cikkének t) pontja a tartalommoderálást a következőképpen határozza meg:

„a közvetítő szolgáltató olyan automatizált vagy nem automatizált tevékenysége, amely különösen a szolgáltatás igénybe vevője által közzétett jogellenes tartalom vagy a közvetítő szolgáltató szerződési feltételeivel összeegyeztethetetlen információ észlelésére, azonosítására és kezelésére szolgál, ideértve az ilyen jogellenes tartalom vagy információ elérhetőségét, láthatóságát és hozzáférhetőségét érintő intézkedéseket, például annak hátrасorolását, a demonetizálását, az ahhoz való hozzáférés megszüntetését vagy annak eltávolítását, vagy a szolgáltatás igénybe vevője általi információközlés lehetőségét érintő intézkedéseket, például a fiókja megszüntetését vagy felfüggesztését.”

A DSA – az Eker. irányelv által létrehozott értesítési és eltávolítási rendszerre építve – saját tartalommoderálásra irányadó eljárást, bejelentési és cselekvés mechanizmust alakít ki,⁵ amely egyrészt biztosítja a jogellenes tartalmakra időben adott megfelelő válasz adását, másrészt pedig – garanciális elemként⁶ – védi a tartalomkészítők alapvető jogait (pl. szólásszabadság) és érdekeit. Fontosnak tartom megjegyezni, hogy az uniós jogalkotó tudatosan a *‘notice-and-action’* és nem a *‘notice-and-stay-down’* eljárást⁷ választotta, így a DSA alapján platform jelenleg nem köteles a jelentett és törölt tartalom ismételt megosztását megakadályozni.⁸ Felmerül azonban a kérdés, hogy vajon miként értékelendő a DSA szempontjából az EUB-nek a Glawischnig-Piesczek-ügyben hozott ítélete, amely azt sejteti, hogy a platformokat terhelő tartalommoderálási kötelezettség közelebb áll a *‘notice-and-stay-down’* megközelítéshez, mint a *‘notice-and-action’* megoldáshoz. Vajon a jogalkotó (az EUB többi, Eker. irányelvvel összefüggésben elfogadott ítéleteivel szemben) tudatosan nem implementálta az EUB döntését?

A DSA tartalommoderálásra irányadó eljárása a következő lépésekből áll:

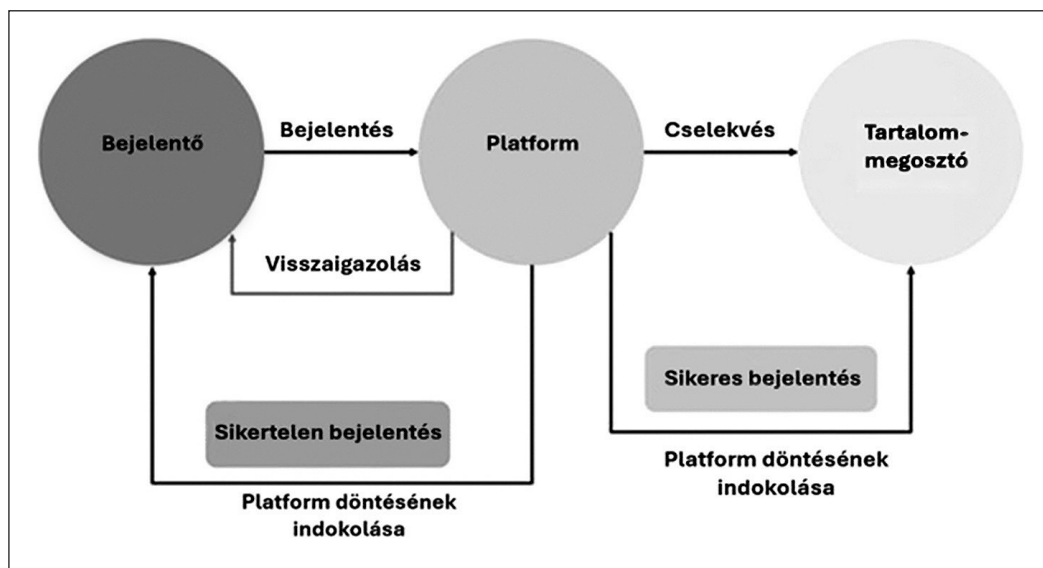
1. lépés: a platform értesítése az állítólagosan jogellenes tartalomról (azaz a bejelentés),
2. lépés: a bejelentés értékelése és szükség esetén a tartalom valamiféle korlátozásához szükséges intézkedések elfogadása (azaz a cselekvés),
3. lépés: a platform döntésének felülvizsgálata, és
4. lépés: a jogorvoslat.

⁵ DSA 16. cikk.

⁶ GYETVÁN–GOSZTONYI (2025)

⁷ KUCZERAWY (2018)

⁸ BUITEN (2021): 374.



17. ábra: A DSA bejelentési és cselekvési eljárása⁹

A platform értesítése a vélt jogellenes tartalomról (azaz a bejelentés)

Mivel a tárhelyszolgáltatók nem kötelesek proaktívan ellenőrizni a felhasználók által feltöltött információkat a jogellenes tartalmak szűrése érdekében,¹⁰ a tartalom moderálásának sarokköve (és egyben első lépése) az állítólag jogellenes tartalomról szóló bejelentés. A bejelentési és cselekvési mechanizmusokat uniós szinten harmonizálni kellett annak érdekében, hogy az értesítések időben, egységes, átlátható és egyértelmű szabályok alapján történjenek, az összes érintett fél jogainak és jogos érdekeinek védelme mellett.¹¹ Ezen konkrét okok miatt a DSA – elődjével ellentétben – szigorúbban szabályozza a bejelentési eljárásokat.

A DSA a platformokat méretüktől függetlenül arra kötelezi, hogy könnyen hozzáférhető és felhasználóbarát bejelentési és cselekvési mechanizmusokat vezessenek be, amelyek megkönnyítik a bejelentő fél által jogellenes tartalomnak tekintett konkrét információknak platformokhoz való eljuttatását.¹² Ezen mechanizmusoknak egyértelműen azonosíthatónak kell lenniük, a kérdéses információ közelében kell elhelyezkedniük, és legalább olyan könnyen megtalálhatónak és használhatónak kell lenniük, mint a tárhelyszolgáltató szerződési feltételeit sértő tartalomra vonatkozó bejelentési mechanizmusoknak.¹³ A DSA 16. cikkének (1) bekezdése azt is tisztázza, hogy a felhasználóknak lehetőséget kell biztosítani arra, hogy

⁹ Forrás: HUSOVEC (2024): 212.

¹⁰ DSA 8. cikk.

¹¹ DSA (52) preambulumbekkezdés.

¹² BALENDRA (2024): 64.

¹³ DSA (50) preambulumbekkezdés.

bejelentéseiket kizárólag elektronikus úton (pl. e-mailben, elektronikus űrlapok kitöltésével vagy a platformok által kifejlesztett kifinomultabb alkalmazási interfészek használatával) tehessék meg. Ezenfelül a felhasználóknak képesnek kell lenniük arra, hogy egyetlen bejelentésen keresztül több jogellenesnek vélt tartalmat is bejelentsenek, ezáltal biztosítva a mechanizmusok hatékony működését.¹⁴

Fontos kiemelni, hogy a DSA csak a jogellenes tartalom (azaz pontosabban uniós vagy tagállami jogot sértő tartalom) bejelentésének folyamatát szabályozza: ez nem vonatkozik azonban a platform által szerződéses jogviszony keretében meghatározott tiltott tartalmak szűrésére. A DSA megalkotásakor az európai jogalkotó tudatosan döntött úgy, hogy nem legitimálja és nem ösztönzi a magánjogi szabályok nyilvános érvényesítését, mivel külön csatornákat kíván fenntartani a „közjogi szabályok” nyilvános érvényesítésére (pl. hatósági végzések) és a „magánjogi szabályok” magánjogi érvényesítésére.¹⁵

A DSA ugyanakkor nem tisztázza egyértelműen, hogy ki tehet bejelentést. Következésképpen bejelentést bárki tehet, függetlenül attól, hogy természetes vagy jogi személy vagy a kérdéses szolgáltatás felhasználója-e. Általános szabályként a bejelentéseket ahhoz a platformhoz kell intézni, akitől észszerűen elvárható, hogy rendelkezik az ilyen konkrét elemek elleni fellépéshez szükséges technikai és működési képességekkel.¹⁶

A platform a véleménynyilvánítás és a tájékoztatás szabadságával összeegyeztethető, megalapozott döntést csak úgy tud hozni, ha a bejelentés kellően pontos és megfelelően indokolt.¹⁷ Ennek biztosítása érdekében a DSA szabályozza a közlés minimális tartalmát. Ezek a minimális elemek a következő pontokban foglalhatók össze:

- Kellően megalapozott magyarázat arra, hogy a szóban forgó információ miért jogellenes. A DSA értelmében a magyarázat megkövetelt szintje a jogellenes tartalom típusától függően változik. Az önmagában jogellenes tartalom esetében minimális magyarázatra van szükség, míg azon információk esetében, amelyek jogellenessége a további körülmények fennállásától függ, a bejelentés részletesebb indoklást igényel. Például egy rasszista megjegyzés (általában) nem igényel hosszabb indoklást, míg egy képmáshoz való jogot sértő felvétel esetén indokolt lehet a jogellenesség körülményeinek részletesebb magyarázata. A bejelentők számára lehetővé kell tenni továbbá azt is, hogy állításaik alátámasztására bizonyítékokat töltsenek fel.¹⁸
- A vélhetően jogellenes tartalom pontos elektronikus helyének egyértelmű megjelölése. A bejelentéseknek tartalmazniuk kell minden olyan szükséges információt, amellyel a szolgáltató számára a jogellenes tartalom beazonosítható. A jogellenes tartalom pontos elektronikus helyének egyértelmű megadása ugyanakkor az érintett tartalom, illetve az adott platform típusától függően változhat: a bejelentő például megadhatja a jogellenes tartalomhoz vezető linket (URL) vagy akár a jogellenes tartalom helyéről képernyőfelvételt is készíthet. A szolgáltatóknak a 16. cikk (2) bekezdésében előírtaknak megfelelően meg kell könnyíteniük a kellően pontos

¹⁴ HOFMANN–RAUE (2025): 333.

¹⁵ HUSOVEC (2024): 209.

¹⁶ DSA 16. cikk (1); DSA (51) preambulumbekkezdés.

¹⁷ DSA (53) preambulumbekkezdés.

¹⁸ HUSOVEC (2024): 213–214.

és megfelelően indokolt bejelentések benyújtását¹⁹ – ellenkező esetben ugyanis nem csupán az eljárás válna hosszabbá és költségesebbé, de a felhasználók is könnyebben elrettennének bejelentések megtételétől.

- A bejelentést tevő személy neve és elektronikus e-mail-címe.
- A bejelentést tevő azon nyilatkozata, miszerint ő jóhiszeműen járt el, és a bejelentésben szereplő információk és állítások pontosak és hiánytalanok.²⁰

Érdekes módon, míg a DSA 16. cikke (2) bekezdésének c) pontja egyértelműen előírja, hogy az értesítésnek tartalmaznia kell az értesítést benyújtó személy vagy szervezet nevét és e-mail-címét, az (50) preambulumbekkezdés szerint „az értesítési mechanizmusnak lehetővé kell tennie, de nem kell megkövetelnie az értesítést benyújtó személy vagy szervezet azonosítását”.²¹ Véleményem szerint a DSA-n belüli ellentmondás feloldható lenne azzal, ha a bejelentőktől nevük és elérhetőségük feltüntetését abban az esetben követelnék meg, ha ez az információ nélkülözhetetlen annak megállapításához, hogy a szóban forgó közlés jogellenes tartalomnak minősül-e.

A bejelentés értékelése és szükség esetén a tartalom valamiféle korlátozásához szükséges intézkedések elfogadása (azaz a cselekvés)

A bejelentés ‘kézhezvételét’ követően a tárhelyszolgáltatónak vissza kell igazolnia a bejelentőnek az átvételt, feltéve, hogy az értesítésben szerepelnek a bejelentő elérhetőségei. Ezt követően a tárhelyszolgáltató az értesítés alapján észszerű időn belül, kellő gondossággal, nem önkényesen és tárgyilagosan eljárva dönt arról, hogy egyetért-e a bejelentővel, és el kívánja-e távolítani vagy le kívánja-e tiltani az adott tartalomhoz való hozzáférést (cselekvés).²² Egyértelmű tehát, hogy a DSA nem kötelezi a platformokat a bejelentett tartalom automatikus eltávolítására. Ez a jogalkotó tudatos döntése volt, mivel el akarta kerülni, hogy a tartalmak túlzottan széles körű eltávolítására ösztönözzön, és ezzel a tartalomkészítők szólásszabadsághoz való alapvető jogának megsértését kockáztassa.²³

A platformoknak észszerű időn belül kell feldolgozniuk a bejelentéseket. A DSA – az Eker. irányelvet végrehajtó egyes nemzeti jogszabályokkal ellentétben – ismételten sem tisztázza, hogy mit jelent az ‘időben’ *terminus technicus*. A norma mintha inkább azt jelezné, hogy a fogalmat eseti alapon kell értékelni, mivel az több körülménytől (pl. a bejelentett jogellenes tartalom típusától és az intézkedés sürgősségétől) függ. Végezetül, a platformoknak indokolatlan késedelem nélkül kell tájékoztatniuk a bejelentést tevőt a bejelentéssel összefüggésben hozott döntésükről, valamint arról, hogy azzal szemben milyen jogorvoslati lehetőségek állnak a bejelentő rendelkezésére.²⁴

¹⁹ Uo., 212–213.

²⁰ DSA 16. cikk (2).

²¹ DSA (50) preambulumbekkezdés.

²² DSA (50) preambulumbekkezdés; DSA 16. cikk (6).

²³ Vö.: Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 67.: „az óvatosság javára tévedni, hogy elkerülje a későbbi esetleges felelősséget”.

²⁴ DSA (52) preambulumbekkezdés.

Annak megítélése, hogy a bejelentés alapján intézkedés megtétele szükséges-e, vagy sem, a platformnak mérlegelnie kell (i) egyrészt a bejelentőnek a jogellenes tartalom eltávolítására irányuló jogos érdekét, illetve a társadalmi közérdeket; (ii) másrészt pedig a tartalom létrehozójának szólásszabadsághoz, véleménynyilvánításhoz való jogát.²⁵

A DSA 17. cikk (1) bekezdése alapján következtetni lehet arra, hogy a platformok milyen intézkedéseket tehetnek a bejelentések alapján: (i) a szolgáltatás igénybe vevője által szolgáltatott konkrét információk láthatóságának korlátozása (pl. a tartalom eltávolítása, a tartalomhoz való hozzáférés megszüntetése vagy a tartalom hátrасorolása); (ii) a pénzbeli kifizetések felfüggesztése, megszüntetése vagy más módon történő korlátozása; (iii) a szolgáltatás nyújtásának teljes vagy részleges felfüggesztése vagy megszüntetése; és (iv) a szolgáltatás igénybe vevője fiókjának felfüggesztése vagy megszüntetése.²⁶ Mivel a DSA 17. cikk a platformok döntéseire vonatkozó indokolási kötelezettséget ír elő, így véleményem szerint az nem tartalmazza a platformok rendelkezésére álló intézkedések taxatív listáját. Ennek következtében a tárhelyszolgáltatók a DSA 17. cikkben felsoroltakon túl további intézkedéseket is hozhatnak (pl. elősegíthetik a bejelentő és az állítólagosan jogellenes tartalom feltöltője közötti egyezség elérését).

A platform döntésének indoklása

Amint fentebb említettük, a DSA 17. cikkének (1) bekezdése előírja a szolgáltatók platformok számára, hogy egyértelmű és konkrét indoklást nyújtsanak minden érintett felhasználónak (azaz a tartalom létrehozójának és a bejelentés tevőnek egyaránt), ha a DSA 17. cikk (1) a)–d) pontjaiban felsorolt intézkedések valamelyikére kerül sor a tartalom jogellenességére tekintettel.

Kérdéses, hogy amennyiben az a)–d) pontokban fel nem sorolt intézkedésre kerülne sor, ezekre is kiterjed-e az indokolási kötelezettség. A DSA céljai és alapelvei, valamint a jogorvoslati jog biztosítása érdekében erre a kérdésre pozitív választ célszerű adni. Ellenkező esetben ugyanis a platform az e pontokban nem felsorolt intézkedéssel megkerülhetné indokolási kötelezettségét. Véleményem szerint ezzel összhangban nem tekinthető kimerítő jellegűnek a panaszkezelési rendszerre vonatkozó – DSA 20. cikkben szereplő – intézkedésekkel kapcsolatos felsorolás sem.²⁷

A tájékoztatásnak egyértelműnek és konkrétnek kell lennie annak biztosítása érdekében, hogy az érintett felhasználók élni tudjanak a DSA alapján rendelkezésükre álló jogorvoslati jogukkal. A platform indokolási kötelezettsége legalább az alábbi információkat foglalja magában:

²⁵ DSA (52) preambulumbekkezdés.

²⁶ LENDVAI (2024b): 83–84.

²⁷ Figyelemre méltó, hogy ez az indokolási kötelezettség akkor is felmerül, ha a tárhelyszolgáltató azon az alapon jár el, hogy a tartalom nem egyeztethető össze az általános szerződési feltételeivel; a DSA 17. cikk hatálya tehát túlmutat a bejelentési és cselekvési keretrendszeren. Tekintettel azonban arra, hogy jelen monográfia arra a kérdésre keresi a választ, hogy a DSA milyen jogorvoslati megoldásokat kínál a képmáshoz való jogában megsértett egyén számára, a DSA 17. cikkének ezen aspektusát nem fogom a továbbiakban vizsgálni.

- információ arról, hogy a platform döntése maga után vont-e bármilyen intézkedést. Amennyiben igen, úgy az indokolásnak ki kell terjednie az intézkedés területi és időbeli hatályára;
- a döntés alapjául szolgáló tények és körülmények;
- a döntés meghozatala során esetlegesen alkalmazott automatizált eszközök;
- a tartalom jogsértő jellegének jogalapra, valamint arra vonatkozó magyarázat, hogy az információ miért tekinthető jogellenesnek; és
- tájékoztatás a felhasználó számára a döntéssel kapcsolatban rendelkezésre álló jogorvoslati lehetőségekről.

A platformnak csak akkor kell felfednie a bejelentő személyazonosságát, ha az feltétlenül szükséges, így például, ha az tartalom jogellenességének megállapításához elengedhetetlen (pl. rágalmozás vagy jóhírnév megsértése).²⁸ A jogalkotási folyamat során jelentős vita folyt arról, hogy a bejelentő személyazonosságát minden esetben fel kell-e fedni, ugyanis míg a kötelező nyilvánosságra hozatal egyrészt elriaszthatja a bejelentőket a megtorlástól való félelem miatt, másrészt elrettentő hatással is lehet a rendszerrel visszaélni kívánó felhasználókkal szemben.

Jogorvoslat

A DSA többféle jogorvoslati lehetőséget biztosít azon érintett felhasználók számára, akik a platformoknak a bejelentések alapján hozott döntéseit kívánják megtámadni. Ezen jogorvoslati eszközök bevezetése különösen fontos szerepet játszik a bejelentési és cselekvési mechanizmusban, hiszen a DSA lehetővé teszi a platformok számára, hogy a döntéseiket automatizált folyamatok révén, kötelező emberi beavatkozás nélkül hozzák meg. Felismerve ezen automatizált eljárásoknak az alapvető jogokat érintő kockázatait, a DSA célja annak biztosítása, hogy a felhasználók könnyen hozzáférhető és hatékony módon támadhassák meg a platformok döntéseit.²⁹

Amint azt a Bizottság hatásvizsgálata is megerősítette, a különböző jogorvoslati eszközök bevezetését elsősorban a tévesen eltávolított tartalmakkal kapcsolatos hatékony védelem iránti igény indokolta.³⁰ E célból a DSA három különböző jogorvoslati lehetőséget biztosít:

- DSA 20. cikke szerinti panasz, amely lényegében a platform rendszerén belül elérhető jogorvoslati fórum;
- bíróságon kívüli vitarendezési mechanizmusok, amelyet a DSA 21. cikke rendez; és
- az adott tagállam nemzeti joga szerint elérhető bírósági fórum.

²⁸ DSA (54) preambulumbekzdés.

²⁹ DSA (58) preambulumbekzdés.

³⁰ Commission staff working document. Impact assessment. Accompanying the document proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, {COM(2020) 825 final} – {SEC(2020) 432 final} – {SWD(2020) 349 final}, 186.

Ezek a mechanizmusok nem csupán egymástól függetlenül érhetők el a felhasználók számára, de azok egymástól függetlenül is működnek.³¹ Ezen elsősorban azt értem, hogy a felhasználónak nem kötelesek valamelyik jogorvoslati eszközt kimeríteni annak érdekében, hogy a másikat igénybe vehessék. Sőt, a DSA 20. cikke szerinti panasz eljárás és a DSA 21. cikke szerinti bíróságon kívüli vitarendezés még egymással párhuzamosan is történhetnek.

9.1.2. A platformok tartalommoderálására vonatkozó kellő gondossági kötelezettségek és a jogellenes tartalomért való felelősségük közötti összefüggés

Különös figyelmet kell fordítani a platformok tartalommoderálására vonatkozó kellő gondossági kötelezettségek és a jogellenes tartalomért való felelősségük közötti összefüggésre.³² A DSA 16. cikkének (3) bekezdése szerint a bejelentés megalapozhatja a platform DSA 6. cikk szerinti tényleges tudomását a jogellenes tartalomról, feltéve, hogy a bejelentés lehetővé teszi egy megfelelő gondossággal eljáró platform számára, hogy részletes jogi vizsgálat nélkül is megállapítsa az adott tartalom jogellenességét.

Így még ha a platform eleget is tesz a kellő gondossági kötelezettségeinek, és a DSA-nak megfelelően dolgozza fel a bejelentést, akkor is felelősségre vonható a jogellenes tartalom tárolásáért, ha bejelentés eredményeként téves döntést hoz. Megfordítva ezt, kijelenthető, hogy az a szolgáltató, amely a bejelentés alapján haladéktalanul törli a jogellenes tartalmat, és így a DSA 6. cikke alapján mentesül a jogellenes tartalom tárolásáért való felelőssége alól, a DSA 52. cikke alapján mégis felelősségre vonható és pénzbírsággal büntethető a kellő gondossági kötelezettségének megszegése miatt, ha nem megfelelően jár el a bejelentés feldolgozásával kapcsolatban.

Martin Husovec azzal érvel, hogy csak egy érvényes bejelentés válthat ki tényleges tudomásszerzést a tárhelyszolgáltató részéről.³³ A DSA 16. cikk (3) bekezdése valóban úgy rendelkezik, hogy „az e cikkben említett bejelentések” tényleges tudomásszerzést eredményezhetnek, azonban – álláspontom szerint – e rendelkezés szigorú értelmezése azzal a kockázattal járna, hogy az ellentmondásba kerülne a DSA 6. cikkében foglalt szélesebb körű felelősséget megalapozó elvekkel. A tényleges tudomásszerzés különböző eszközökkel történhet, és még akkor is, ha a bejelentés nem felel meg a DSA 16. cikk (2) bekezdésében meghatározott valamennyi formai követelménynek – például az állítások pontosságát megerősítő nyilatkozat hiánya miatt –, a szolgáltató a gyakorlatban mégis szerezhethet tényleges tudomást a tartalom jogellenes jellegéről. Ilyen esetekben a tárhelyszolgáltató felelőssége megállapítható, hacsak nem távolítja el a bejelentett tartalmat.

Fontos kiemelni, hogy egy olyan értesítés, amely nem alapozza meg egyértelműen a bejelentett tartalom jogellenességét, önmagában nem eredményezheti a szolgáltató tényleges tudomásszerzését. Ahogy fentebb láthattuk, a DSA előírja, hogy az érvényes értesítésnek

³¹ HOFMANN–RAUE (2025): 391–469.

³² PÜNKÖSTY (2022a)

³³ HUSOVEC (2024): 219.

elegendő információt kell tartalmaznia ahhoz, hogy a szolgáltató részletes jogi elemzés nélkül is döntést hozhasson: ez pedig összhangban van az EUB ítélkezési gyakorlatával.³⁴ Ha azonban a vizsgálat során olyan további információk kerülnek napvilágra, amelyek nyilvánvalóvá teszik a tartalom jogellenességét, akkor a tényleges tudomásszerzést vélemezni kell.

További kérdésként merül fel, hogy a szolgáltató szerezhet-e tényleges tudomást, ha az bejelentés és cselekvés folyamata teljesen automatizált. Mivel a DSA nem tiltja a tartalom-moderálás automatizálását, így jogosan merülhet fel a kérdés, hogy egy ilyen automatizált döntéshozatal eredményezhet-e a DSA 6. cikke szerinti tényleges tudomásszerzést. Bár a tudományos szakirodalom még nem vizsgálta mélyrehatóan ezt a kérdést, álláspontom szerint erre a kérdésre pozitív válasz adható. Először is, mivel a tartalom moderálásának automatizálására vonatkozó döntés a platform tudatos döntése, ezért viselnie kell az ahhoz kapcsolódó kockázatokat is (nevezetesen azt, hogy bizonyos jogellenes tartalmak esetleg észrevétlenül maradnak, ami így megalapozhatja a platform felelősségét.) Másodszor, ez az értelmezés összhangban van az EUB-nek az Eker. irányelvvel összefüggésben kialakított joggyakorlatával is.³⁵ Miközben az EUB elismerte, hogy a platform tartalommal kapcsolatos automatizált folyamatai – például az indexelés vagy az ajánlások – önmagukban nem jelentenek elegendő alapot a platform tényleges tudomásának megállapításához, az EUB azt is megerősítette, hogy a tényleges tudás különböző eszközökkel is létrejöhet. Különösen akkor tekinthető úgy, hogy a szolgáltatónak tényleges tudomása van, ha olyan tényekről vagy körülményekről szerez tudomást, amelyek alapján egy gondos gazdasági szereplőnek fel kellett volna ismernie a tartalom jogellenességét.³⁶ Ha a szolgáltató értesítést kap egy konkrét tartalomról, akkor a tudásának jellege az arra vonatkozó absztrakt tudatosságból, hogy szolgáltatását jogellenes tevékenységekre használhatják, a potenciálisan jogellenes tartalom konkrét esetének tényleges ismeretévé válik. Ilyen esetekben a platform már nem az általános vagy absztrakt ismeretek állapotában van, hanem tényleges tudomást szerez egy adott tartalomról, ami azonban a DSA szerinti felelősségét megalapozza.³⁷

9.2. A platformok ajánlórendszereivel összefüggésben előírt kellő gondossági kötelezettségek

Az ajánlórendszerek jelentős hatást gyakorolnak a felhasználók interneten elérhető információkkal való interakciójára. Egyrészt az ajánlórendszerek elősegítik az információk gyors és széles körű terjedését, valamint a szolgáltatás igénybe vevői számára releváns információk megtalálását, így javítva a felhasználói élményt. Másrészt azonban az az ajánlórendszerek

³⁴ Lásd például: C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 116.

³⁵ ZEYBEK – VAN HOBOKEN – BURI (2022)

³⁶ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 14–15.

³⁷ WOLTERS–GELLERT (2023): 414–416.

meghatározott szerepet töltenek be bizonyos üzenetek felerősítésében és így (közvetve) különböző online viselkedésformák kialakításában is.³⁸ Például a YouTube esetében a megtekintett tartalmak mintegy 70%-át,³⁹ míg a TikTok platformon az esetek 90-95%-át⁴⁰ az ajánlórendszerek által közvetített tartalmak teszik ki.

9.2.1. Az ajánlórendszerek működése

A tartalomoptimalizálás az online platformok egyik legfontosabb funkciója, amely elsősorban azt foglalja magában, hogy az információk milyen rangsorban jelennek meg az érintett online felületen. Erre például „az információk algoritmikus javasolásával, rangsorolásával és prioritizálásával, a szöveges és egyéb vizuális megjelenítések révén történő különbségtétellel vagy a szolgáltatás igénybe vevője által biztosított információk egyéb feldolgozása révén kerül sor.”⁴¹ Ahogyan arra a DSA (70) preambulumbekzdése is utal, ez a folyamat nagymértékben támaszkodik az ajánlórendszerekre, amelyek gyakran gépi tanuláson alapuló mester-séges intelligenciával egészülnek ki.⁴²

Az ajánlórendszerek működésnek alapja a felhasználók személyes adatainak gyűjtése és tovább kezelése felhasználói profil létrehozása érdekében, amely alapján az érintett számára személyre szabott, célzott tartalom nyújtható.⁴³ Az ajánlórendszer tehát valójában nem más, mint egy algoritmikus tartalomszűrési eszköz, amely az egyén számára nagy valószínűséggel tetsző információt szelektálja ki és jeleníti meg.⁴⁴

Az ajánlórendszer alapjául szolgáló algoritmikus modellnek az alábbi három fő kategóriája különböztethető meg (amelyek a gyakorlatban sokszor egymással keverednek):

- Tartalomalapú modell: lényege, hogy a felhasználó által korábban kedvelthez hasonló tartalmat jelenít meg az érintett számára. A tartalomalapú ajánlórendszer működésének előfeltétele a tartalmak kategorizálása és címkézése, ami lehetővé teszi tartalmak rendszerszintű azonosítását és összehasonlítását. Az algoritmus lényegében a felhasználó által korábban kedvelt tartalmak címkéit (*description*) hasonlítja össze a többi tartalom címkéivel hasonló tartalom azonosítása céljából.⁴⁵ Így például, ha egy felhasználó a Netflixen megnézi a Forrest Gump című filmet, a Netflix algoritmus további olyan filmeket fog javasolni, amelyeket a Netflix Tom Hanks nevével köt össze.

³⁸ DSA (70) preambulumbekzdés.

³⁹ Joan E. SOLSMAN: YouTube's AI is the puppet master over most of what you watch. *CNET*, 2018. január 10., <https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/>, 10.

⁴⁰ N/A: Investigation: How TikTok's Algorithm Figures Out Your Deepest Desires. *Wall Street Journal*, 2021. július 21., https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796?mod=trending_now_video_3

⁴¹ DSA (70) preambulumbekzdés.

⁴² DSA (70) preambulumbekzdés.

⁴³ MAGRANI – DA SILVA (2024): 144.

⁴⁴ MAZEH–SHMUELI (2020): 1.

⁴⁵ APÁTHY Sándor: Ajánlórendszerek a gyakorlatban. *Onespire*, d.n. <https://onespire.hu/ajanlorendszerek-a-gyakorlatban>

- Kollaboratív modell: egy csoport viselkedésének elemzése útján gyűjtött információkat használja fel annak érdekében, hogy az érintett számára tetsző tartalmat mutasson. A csoportnak tetsző tartalmat azon felhasználók számára jeleníti meg az algoritmus, akik a közösségbe tartozó egyének profiljával hasonlóságot mutatnak.⁴⁶ A Facebook ajánlórendszere például részben ilyen algoritmuson alapszik: a platform elemzi, hogy például a 30 éves, házasságos nőt milyen tartalmak érdeklí, majd az így azonosított minták alapján minden 30 éves nőnek hasonló jellegű reklámokat jelenít meg.
- Tudásalapú modell: a felhasználóról gyűjtött (csekély) adatot egy adott terület (pl. marketing vagy értékesítés) ismereteivel kombinálja – ilyen modellt használnak például hiteltermékek, biztosítások vagy autók értékesítése során.⁴⁷

9.2.2. Az ajánlórendszerek definíciója a DSA alapján

A DSA az ajánlórendszer fogalmát tágran határozza meg. A DSA 3. cikkének s) pontja szerint az ajánlórendszer olyan „teljes mértékben vagy részben automatizált rendszer, amelyet az online platform arra használ, hogy az online interfészén konkrét információkat javasoljon vagy ezeket az információkat rangsorolja a szolgáltatás igénybe vevője számára, többek között a szolgáltatás igénybe vevője által indított keresés alapján vagy egyéb módon meghatározva a megjelenített információk relatív sorrendjét vagy elsőbbségét.”⁴⁸ Ajánlórendszer tehát valójában nem más, mint az az algoritmus, mesterséges intelligencia, amely meghatározza például a Google keresési eredményeit, a közösségi média hírfolyamain megjelenő tartalmakat, sőt még a társkereső alkalmazásokban javasolt potenciális partnerek sorrendjét is.⁴⁹

Némi párhuzamot lehet vonni a rangsorolásnak az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló 2019/1150 EU Rendeletben (P2B)⁵⁰ szereplő meghatározásával, bár az ajánlórendszerek a rangsorolásnál sokkal többre terjednek ki.⁵¹ A P2B jóval a DSA előtt, 2020. július 12. napján lépett hatályba az online közvetítő szolgáltatások üzleti felhasználói és az online keresőprogramok tekintetében a kereskedelmiweboldal-használók számára megfelelő átláthatóság, tisztességesség és a hatékony jogorvoslati lehetőségek biztosítása érdekében.⁵² A P2B értelmében a rangsorolás az online közvetítő szolgáltatáson keresztül kínált áruknak és szolgáltatásoknak biztosított viszonylagos kiemelés, illetve az online keresőprogramok által a keresési eredményekhez rendelt relevancia, ahogyan azt az online közvetítő szolgáltatók,

⁴⁶ JANNACH et al. (2011): 13.

⁴⁷ GOWDER (2023): 33–35.

⁴⁸ DSA 3. cikk s).

⁴⁹ HUSOVEC (2024): 288.; NOVOVIC (2024): 58.

⁵⁰ 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 (P2B), PE/56/2019/REV/1, HL L 186., 2019.7.11., 57–79.

⁵¹ A rangsorolás az áruk és szolgáltatások kiemelésének sorrendjére korlátozódik, ellentétben az ajánlórendszerrel, amely a felhasználó által megadott bármely információ kiemelésére vonatkozik. FIRNIKSY (2021): 168.; POLYÁK et al. (2021): 159–160.

⁵² P2B Preambulum 1.

illetve az online keresőprogram-szolgáltatók megjelenítik, strukturálják vagy kommunikálják, tekintet nélkül az ilyen megjelenítéshez, strukturáláshoz vagy kommunikációhoz használt technológiai eszközökre.

Ezzel összefüggésben az EB nem kötelező érvényű iránymutatásokat⁵³ is kiadott a rangsorolás átláthatóságáról (P2B Iránymutatás), de ezek korlátozott információt nyújtanak arról, hogy hogyan kell értelmezni a rangsorolás fogalmát. A P2B Iránymutatás alapján kijelenthető, hogy a rangsorolást alapvetően az „adatvezérelt, algoritmus-alapú döntéshozatal egy formájának” kell tekinteni. Bár a P2B Iránymutatás megerősíti, hogy az, hogy mi minősül rangsorolási rendszernek, esetről esetre vizsgálendő, a rangsorolási rendszerek P2B Iránymutatásban használt példái (pl. keresési funkciók, meta-keresőprogramok) némi egyértelműséget nyújthatnak e tekintetben. A P2B Iránymutatás például azt is megállapítja, hogy a rangsorolás magában foglalhatja az áruk és szolgáltatások alapértelmezett sorrendjét is, amelyek között a fogyasztók keresőkérdések használata nélkül navigálhatnak, a különböző online közvetítő szolgáltatások zökkenőmentes használata révén, vásárlási gombok, vizuális megjelenítés (beleértve a térképek vagy könyvtárak formájában működő online közvetítő szolgáltatásokat), kiemelés, leadgenerálás és szerkesztői beavatkozások révén.

Tekintettel a DSA technológiaiailag semleges keretrendszerére, valószínű, hogy a P2B Iránymutatásban felvázolt megközelítés hasonlóan fog érvényesülni a jövőben: az ajánlórendszer fogalmát tágan fogják értelmezni, míg a végrehajtó hatóságok a konkrét kontextus alapján fogják értékelni, hogy mi minősül ajánlórendszernek. Következésképpen a platformoknak óvatosságot célszerű tanúsítaniuk, és abból kell kiindulniuk, hogy minden olyan tartalomszervezési rendszer, amely a felhasználó kifejezett inputja nélkül, egyéni felhasználói paraméterekre támaszkodik, a DSA értelmében feltehetőleg ajánlórendszernek fog minősülni.⁵⁴

9.2.3. Az ajánlórendszerek átláthatósága

A DSA 27. cikkének (1) bekezdése kimondja, hogy „az online platformot üzemeltető azon szolgáltatók, amelyek ajánlórendszereket használnak, szerződési feltételeikben – világos és közérthető nyelvezettel – meghatározzák az ajánlórendszerükben használt fő paramétereket, valamint a szolgáltatás igénybe vevői számára az e fő paraméterek módosítására vagy befolyásolásra rendelkezésre álló lehetőségeket.”

A DSA 27. cikke szerinti kötelezettség tehát egy átláthatósági kötelezettség, amely kétrétű. A platformoknak el kell magyarázniuk (i) az ajánlórendszerükben használt fő paramétereket, és (ii) az e fő paraméterek módosításának vagy befolyásolásának lehetőségét és módszerét.⁵⁵ Már most fontos kiemelni, hogy az online óriásplatformok és a nagyon nagy online keresőmotorok kivételével a platformok nem kötelesek alternatív lehetőséget kínálni

⁵³ A Bizottság közleménye: Iránymutatás a rangsorolási átláthatóságról az (EU) 2019/1150 európai parlamenti és tanácsi rendeletnek megfelelően (P2B Iránymutatás), 2020/C 424/01, C/2020/8579, HL C 424., 2020.12.8., 1–26, 11.

⁵⁴ NOVOC (2024): 59.

⁵⁵ DECAROLIS–LI (2023): 6.

a felhasználóknak az ajánlórendszerükhöz. A DSA 27. cikkének célja nem az ajánlórendszerek használatának korlátozása vagy tiltása, hanem az átláthatóság előmozdítása, amely lehetővé teszi a felhasználók számára, hogy megértsék, hogyan befolyásolják az ilyen rendszerek az információk megjelenítését.⁵⁶

Bár a DSA 27. cikk (1) bekezdése szerinti átláthatósági kötelezettségek első látásra magától értetődőnek tűnhetnek, e rendelkezés végrehajtása számos összetett problémát vet fel a gyakorlatban.

Először is, a DSA korlátozott iránymutatást nyújt a platformok által az ajánlórendszereikről közzeendő információk körére vonatkozóan. Konkrétan, bár a 27. cikk (1) bekezdése előírja az ajánlórendszerükben használt fő paraméterek közzétételét, a DSA nem ad pontos meghatározást arra vonatkozóan, hogy mit is jelentenek ezek a fő paraméterek.⁵⁷ A DSA (70) preambulumbekkezdése és a DSA 27. cikk (2) bekezdése egyértelművé teszi, hogy az ilyen paramétereknek tartalmazniuk kell: (i) a szolgáltatás igénybe vevőjének javasolt információk meghatározásakor legfontosabb kritériumokat, és (ii) a fontosságukra vonatkozó információkat (beleértve azt is, ha az információkat profilalkotás és az online viselkedés alapján rangsorolják). A 2016/679 EU Rendelet⁵⁸ (GDPR) szerinti profilalkotással és automatizált döntéshozatallal kapcsolatos ítélkezési gyakorlat azonban azt mutatja, hogy a fő paraméterek és azok relatív fontosságának meghatározása ritkán egyszerű feladat – különösen a mesterséges intelligenciával működtetett ajánlórendszerek esetében, amelyeket az óriásplatformok kivétel nélkül alkalmaznak.

A gyakorlat általában a P2B Iránymutatáshoz fordul annak további tisztázása érdekében, hogy hogyan kell értelmezni a fő paraméterek kifejezést. Ennek fő oka, hogy a P2B 5. cikk (1) bekezdése a DSA 27. cikkével megegyező terminológiát használ, amikor kimondja, hogy „az online közvetítő szolgáltatók szerződési feltételeikben rögzítik a rangsorolást meghatározó fő paramétereket és e fő paraméterek más paraméterekhez képest meglévő viszonylagos jelentőségének okait.” A P2B Iránymutatás szerint a szolgáltatóknak a rangsorolás szempontjából külön-külön vagy együttesen a legjelentősebb fő paraméterek meghatározásakor különösen a következőket kell figyelembe venniük:

- az algoritmusuk célja, amely azok megalkotását vezette;⁵⁹
- információ, amelyet az érintettek számára a leghasznosabb lenne tudni;⁶⁰
- a kérdéses mechanizmus alapján az információ, amely meghatározza a rangsorolást;⁶¹
- azok a paraméterek, amelyek személyre szabják az eredményeket (azaz azok az előre meghatározott paraméterek, amelyek alkalmazása azt eredményezi, hogy az egyik fogyasztó más rangsort kap, mint egy másik fogyasztó, aki ugyanazt az online közvetítő szolgáltatást vagy online keresőmotort használja) –⁶² e tekintetben a P2B

⁵⁶ HOFFMANN-RAUE (2025): 557.

⁵⁷ LEERSSEN (2023): 10.

⁵⁸ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), HL L 119., 2016.5.4., 1–88.

⁵⁹ P2B Iránymutatás 41.

⁶⁰ P2B Iránymutatás 45.; BUSCH (2024).

⁶¹ P2B Iránymutatás 47.

⁶² P2B Iránymutatás 49.; RUTGERS-SAUTER (2021).

Iránymutatás felsorolja azokat a tényezőket (pl. a megcélzott felhasználók összetétele, a felhasználó előzményei, a felhasználó keresési magatartása és a felhasználó aktivitása vagy jelenléte harmadik fél szolgáltatásainál), amelyeket figyelembe kell venni, ha bármelyikük hatással van a rangsorolásra;⁶³

- információ arra vonatkozóan, hogy hogyan befolyásolja a személyre szabás a rangsorolást, beleértve az eredmények változékonyságát vagy eltérését a különböző felhasználók esetében.⁶⁴

A fent említett pontokon kívül a P2B Iránymutatás I. melléklete a fő paraméterek példáinak nem kimerítő felsorolását tartalmazza. Ezek a paraméterek közé tartozik például az ár, a fogyasztói vélemények, az internetes forgalom, a keresési teljesítmény és a kulcsszavak megjelenése.

Fontos azonban megjegyezni, hogy a P2B a közvetítők és az üzleti felhasználók közötti kapcsolatot hivatott szabályozni. Ez a különbségtétel a rendelet és a DSA alapján eltérő értelmezéshez vezethet, mivel az üzleti felhasználók esetében az általános elvárhatóság szintje lényegesen magasabb, mint ami egy átlagos fogyasztótól elvárható. Ezért álláspontom szerint a 'fő paraméterek' kifejezés értelmezése során érdemesebb lenne a GDPR 13–14. cikkei által előírt, az adatkezelőknek a profilozásról, illetve automatizált döntéshozatalról való tájékoztatási kötelezettségét értelmező normaszöveget alapul venni a gyakorlatban. A GDPR 13. cikk (2) bekezdés f) pontja és 14. cikk (2) bekezdés g) pontja értelmében ugyanis az adatkezelők kötelesek az érintetteknek (azoknak a személyeknek, akiknek az adatait kezelik) érdemi tájékoztatást nyújtani az automatizált döntéshozatalban alkalmazott logikáról, valamint az ilyen feldolgozás jelentőségéről és az érintettre gyakorolt várható következményeiről. Az ajánlórendszerek használata, amely a felhasználó személyes adatainak feldolgozásával jár, profilalkotásnak minősül.⁶⁵ Ha pedig a személyre szabott tartalmat kizárólag az ajánlórendszer határozza meg emberi közreműködés nélkül, és az jelentősen érinti az egyént, az automatizált döntéshozatalnak is minősülhet.⁶⁶

A – ma már nem hatályos – 95/46/EK irányelv⁶⁷ 29. cikke alapján létrehozott, az adatvédelem és a magánélet védelmével foglalkozó független európai tanácsadó testület, a WP29 iránymutatása szerint az adatkezelőknek nem kell komplex magyarázatot adniuk az alkalmazott algoritmusokról, illetve nem kell nyilvánosságra hozniuk a teljes algoritmust. Ehelyett az adatkezelőnek egyszerű, átfogó módot kell találnia arra, hogy tájékoztassa az érintettet a döntés indoklásáról vagy a döntés meghozatalakor figyelembe vett kritériumokról.⁶⁸

⁶³ P2B Iránymutatás 48–75.

⁶⁴ P2B Iránymutatás 50.

⁶⁵ GDPR 4. cikk (4).

⁶⁶ GDPR 22. cikk (1).

⁶⁷ Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, HL L 281., 1995.11.23., 31–50.

⁶⁸ WP29: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN, WP251rev.01, 25.

Az EUB előtt zajló Dun & Bradstreet Austria-ügyben a főtanácsnok tovább pontosította, hogy miként kell értelmezni az automatizált döntéshozatalban alkalmazott logikára vonatkozó érdemi információ fogalmát. A főtanácsnok funkcionális megközelítést követett, és az automatizált döntéshozatalban részt vevő logikára vonatkozó érdemi tájékoztatás fogalmát e kötelezettség célja szempontjából értelmezte. Indítványában megállapította, hogy „automatizált döntéshozatal» alapjául szolgáló logikára vonatkozó érthető információknak« lehetővé kell tenniük az érintett számára, hogy gyakorolhassa [a GDPR] (...) által biztosított jogait»⁶⁹ és különösen, hogy ellenőrizhesse az automatizált döntéshozatal pontosságát, valamint azt, hogy „fennáll-e objektíven ellenőrizhető összhang és okozati összefüggés egyrészt az alkalmazott módszer és kritériumok, másrészt az automatizált döntés által elért eredmény között.»⁷⁰ Az adatkezelő által nyújtott információknak tehát lehetővé kell tenniük az érintett számára annak ellenőrzését, hogy azok megfelelnek-e a tényeknek, és így a szóban forgó automatizált döntés valóban pontos (*accurate*) információkon alapul-e.

A főtanácsnok azt is megállapította továbbá, hogy az adatkezelő azon kötelezettsége, hogy az automatizált döntéshozatalra vonatkozó átláthatóságot biztosítsa, csak akkor teljesítheti célját, ha a nyújtott tájékoztatás tömör, könnyen hozzáférhető, könnyen érthető, átlátható és az egyén számára jelentőséggel bír.⁷¹ E tekintetben a főtanácsnok indítványában azt is megjegyezte, hogy az automatizált döntéshozatalban használt algoritmusok természetüknél fogva túlságosan technikai jellegűek és olyan összetettek, hogy azokat egy átlagos személy nem értheti meg. Ennek megfelelően a főtanácsnok úgy ítélte meg, hogy az adatkezelők nem kötelesek nyilvánosságra hozni az algoritmusait, ehelyett tájékoztatást kell nyújtaniuk az automatizált döntéshez vezető folyamatról, a döntés eredményének okairól. Az érdemi tájékoztatás fogalma tehát magában foglalja (i) az alkalmazott módszert; (ii) a figyelembe vett kritériumokat; és (iii) azok súlyozását.⁷²

A főtanácsnok indítványa elismeri, hogy bizonyos esetekben az érintettnek a döntéshozatalban alkalmazott logikáról való érdemi tájékoztatáshoz való jogát felülírhatják mások jogai és érdekei, mivel a személyes adatok védelme nem abszolút jog, és az arányosság elvével összhangban más alapvető jogokkal szemben kell mérlegelni.⁷³ Bár a DSA nem mondja ki kifejezetten, hogy a platformok átláthatósági kötelezettségei az ajánlórendszereikkel kapcsolatban korlátozottak lehetnek, az EUB ítélezési gyakorlatából következik, hogy a felhasználók átláthatósághoz való jogát egyensúlyba lehet (és kell) hozni mások jogaival és szabadságaival, beleértve a platform szellemi tulajdonjogait is. Ezt az értelmezést a DSA (153) preambulumbekzdése is alátámasztja, amely szerint a rendelet

„tiszteltben tartja a Charta által elismert alapvető jogokat és az uniós jog alapelveinek minősülő alapvető jogokat. Ennek megfelelően ezt a rendeletet ezekkel az alapvető jogokkal összhangban kell értelmezni és alkalmazni, ideértve a véleménynyilvánítás szabadságát, a tájékozódás szabadságát, valamint a tömegtájékoztatás szabadságát és sokszínűségét. Az ebben a rendeletben meghatározott hatáskörök gyakorlása során az

⁶⁹ C-203/22, Dun & Bradstreet Austria, ECLI:EU:C:2024:745, 71.

⁷⁰ Uo., 71.

⁷¹ Uo., 65–66.

⁷² NNAWUCHI–GEORGE (2025): 13.

⁷³ C-203/22, Dun & Bradstreet Austria, ECLI:EU:C:2024:745, 82.

érintett hatóságoknak – azokban a helyzetekben, amikor az alapvető jogok ütköznek egymással – megfelelő egyensúlyra kell törekedniük az érintett jogok között az arányosság elvének megfelelően.”

Nem egyértelmű azonban a jogalkotási szándék a platformokra vonatkozó azon követelmény mögött, hogy az általános szerződési feltételeikben nyilvánosságra kell hozniuk az ajánlórendszerek főbb paramétereit.⁷⁴ Az egyik lehetséges értelmezés szerint az ilyen közzététel szerződéses kötelezettséget teremt, ami azt jelenti, hogy a közzétett információtól való bármilyen eltérés szerződésszegésnek minősül. Bár ez az értelmezés ösztönözheti a platformokat arra, hogy átfogó tájékoztatást nyújtsanak, a gyakorlatban nem valószínű, hogy elfogadják azt, mivel figyelmen kívül hagyja az ajánlórendszerek folyamatosan változó, dinamikus jellegét. Ráadásul mivel a gyakorlatban a platformok folyamatosan fejlesztik és frissítik ezeket a rendszereket, ez a megközelítés az általános szerződési feltételek túl gyakori módosítását tenné szükségessé, ami nehezen tűnik kivitelezhetőnek.

A fent említettek szerint a DSA 27. cikke azt is előírja, hogy amennyiben a szolgáltatás igénybe vevőinek nyújtott információk relatív sorrendjének meghatározására több lehetőség is rendelkezésre áll, a platformoknak lehetővé kell tenniük a felhasználók számára, hogy bármikor kiválaszthassák és módosíthassák az általuk preferált lehetőséget. Ennek a funkciónak közvetlenül és könnyen elérhetőnek kell lennie a platform felületén. Ezen gondossági kötelezettség célja nem csupán az ajánlórendszerek gyakorlati átláthatóságának biztosítása, hanem az is, hogy a felhasználók kezébe adja a döntést a részükre megjelenített tartalom rangsorolásával összefüggésben (beleértve azt is, hogy hajlandóak-e egy információs buborékban maradni, vagy sem).⁷⁵

9.2.4. Kilépés az ajánlórendszerekből

A DSA 27. cikkében meghatározott követelményeken túlmenően a DSA 38. cikke egy olyan tartalommoderálási kötelezettséget ír elő, amely megköveteli az online óriásplatformoktól, hogy ajánlórendszereikhez legalább egy olyan alternatívát biztosítsanak, amely nem támaszkodik a felhasználói profilalkotásra.⁷⁶ E rendelkezés célja, hogy a felhasználóknak választási lehetőséget biztosítson a személyre szabott ajánlások mellőzésére, ezáltal enyhítve a túlzott személyre szabás lehetséges negatív következményeit, például az úgynevezett információs buborékok kialakulását.⁷⁷ Másképp megfogalmazva a DSA 38. cikke lehetővé teszi a felhasználók számára, hogy a profilozáson alapuló ajánlási rendszerből kilépjenek (*opt-out*).⁷⁸

⁷⁴ DSA 27. cikk (1).

⁷⁵ NOVOC (2024): 229.

⁷⁶ PAPP (2024a): 137.

⁷⁷ PAPP (2024b)

⁷⁸ LENDVAI (2024c): 176.

Ki kell emelni, hogy a DSA nem kötelezi az óriásplatformokat arra, hogy alapértelmezett beállításként a profilalkotás nélküli alternatívát alkalmazzák, helyett csak azt írja elő, hogy a felhasználók számára elérhetővé kell tenni ezt az alternatívát, és hogy – amint azt korábban tárgyaltuk – a felhasználóknak lehetőségük legyen könnyen elérni és aktiválni ezt a lehetőséget.

A DSA nem határozza meg pontosan, hogy mi tekinthető a profilozáson alapuló ajánlórendszer alternatívájának.⁷⁹ A Facebook és Instagram például alternatívaként a tartalom kronologikus megjelenítését ajánlja fel a felhasználóik számára.⁸⁰ A Panoptykon alapítvány pedig olyan moderált személyre szabást javasolna alternatívaként, amely az adott felhasználó kifejezett visszajelzései és szabadon megadott információi alapján működne.⁸¹

Fontosnak tartom megjegyezni, hogy a DSA 38. cikke által előírt gondossági kötelezettség – álláspontom szerint – könnyen kontraproduktívá válhat. Az óriásplatformok által preferált kronologikus vagy betűrendes elrendezése ugyanis olyan felületet eredményezhet, amely nem praktikus vagy nehezen navigálható, elriasztva így a felhasználókat attól, hogy a nem személyre szabott ajánlásokat válasszák, ezzel pedig a szabályozás – szándékaival ellentétben – közvetve erősíti a profilozáson alapuló ajánlórendszerek használatát.

⁷⁹ HOFMANN–RAUE (2025): 730.

⁸⁰ CLEGG (2023)

⁸¹ SZYMIELEWICZ (2023): 9.

10. Hatékony védelmet nyújtana-e a DSA Hillary Clinton számára a hamisított képmásának hozzájárulása nélküli terjesztésével szemben?

A #PizzaGate összeesküvés-elmélet (beleértve Hillary Clinton hamisított képmását is) futótűzként terjedt mind a legnagyobb (Facebook, X, YouTube), mind pedig a kisebb (Reddit, 4chan) közösségi oldalakon. Kétségtelen, hogy mindezeket az oldalakat tárhelyszolgáltatóknak, azon belül is online platformoknak kell tekinteni (bár nem mindegyik online óriásplatform). Így a jogellenes tartalmak befogadásáért való felelősségüket a DSA 6. cikkének (1) bekezdése alapján kell értékelni.

10.1. A platformok szerepe Hillary Clinton hamisított képmásának nyilvánosság felé való terjesztésében

Ahogy az korábban részletesen bemutattam a tárhelyszolgáltató nem vonható felelősségre a tárolt adatokért, ha szolgáltatását semlegesen, a szolgáltatás igénybe vevője által megadott adatok pusztán technikai és automatizált feldolgozásával nyújtja. Az EUB-nek a YouTube-ügyben hozott döntése azt az álláspontot támasztja alá, hogy az algoritmikus kategorizálás, a személyre szabás, a rangsorolás és az egyéniesített keresési funkciók biztosítása önmagában nem zárja ki, hogy a tárhelyszolgáltató semleges szerepet töltsön be, vagy hogy a felelősség alóli mentességben részesüljön. Ez azt sugallja, hogy az EUB álláspontja szerint a tartalomoptimalizálási eszközök a „platform pusztá rendelkezésre bocsátásának”¹ körébe tartoznak.

Véleményem szerint azonban a Google France és Google-ügyben, valamint a YouTube-ügyben az EUB tévesen feltételezte, hogy az érintett tartalom automatizált kezelése, az algoritmus általános alkalmazása a tárhelyszolgáltató semleges szerepét vonná maga után. A valóságban egy olyan algoritmus hatása, amelyet automatizált módon alkalmaznak minden felhasználó által generált tartalomra, nem feltétlenül semleges. A tartalom moderálására használt algoritmusok például a platformok beléjük kódolt értékeit képviselik, ezért az ilyen algoritmusok által vizsgált minden egyes poszt a platformok jóváhagyását vagy elutasítását

¹ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 108.

tükrözi.² De ha a platformok nem azért szűrik a pornográfiát, mert az illegális, hanem mert nem felel meg az irányelveiknek, akkor hogyan állíthatnánk, hogy a platformok semleges szerepet vállalnak az információ terjesztésében?

A semleges platformok koncepciója véleményem szerint inkább egyfajta mítosz, ugyanis a platformok a kollektív kreativitás 'pártfogóiként' működnek. Felkérjük, sőt ösztönzik felhasználóikat, hogy vegyenek részt a tartalom létrehozásában, és ezáltal meghatározzák a kreatív tartalom előállításának feltételeit.³ Ahogy Tarleton Gillespie megfogalmazta: „ezek a feltételek gyakorlati, technikai, gazdasági és jogi jellegűek, és messze elrugaszkodnak a platform retorikája által sugallt semlegességtől.”⁴ Ebben a fejezetben bemutatom, hogy az, hogy a közösségimédia-platformok pusztán automatikus, passzív módon alkalmazzák algoritmusait a felhasználók által generált tartalmak optimalizálására, ez nem jelenti azt, hogy nem vesznek részt aktívan az információ terjesztésében, és így annak gyakorlati kontrollálásában.

10.1.1. A közösségimédia-platformok (rejtett) pénzügyi érdekeltsége az álhírek és a deepfake-ek terjesztésében

A #PizzaGate összeesküvés-elmélet, valamint Hillary Clinton hamisított képmásának terjesztésében részt vevő platformok valamilyen mesterséges intelligenciát vagy algoritmust használnak arra, hogy az embereknek a számukra legmegfelelőbb történeteket mutassák meg. Ezek az algoritmusok olyan tartalmakat választanak ki és ajánlanak, amelyek megfelelnek a felhasználók érdeklődési körének, amelyek népszerűek más felhasználók körében, és/vagy amelyek több interakciót generálnak a felhasználók között annak érdekében, hogy növeljék a megtekintések számát, a felhasználói figyelmet és ezáltal (óhatatlanul) a közösségi hálózatok reklámbevételét.⁵

A Facebook⁶ egy úgynevezett rangsorolási folyamatot használ annak érdekében, hogy „személyre szabott és sokszínű bejegyzések folyamatát kínálja olyan emberek, hírforrások, vállalkozások és közösségek bejegyzéseiből”,⁷ akikkel a felhasználó a Facebookon kapcsolatban állt. A felhasználó által a hírfolyamában látható bejegyzések sorrendjét több körülmény határozza meg, amelyeknek különböző súlyozási tényezői lehetnek. A rangsorolás során a Facebook algoritmus a következőket veszi figyelembe:

- a poszt szerzőjével (barátok, csoportok vagy oldalak) való interakciók gyakorisága (pl. „Ön többször like-olta XY bejegyzését, mint másokét”);
- hogy a poszt olyan tartalom-e, amellyel a felhasználó gyakran interakcióba lép (pl. „Ön többször megnyitott a QZ oldal linkjeit tartalmazó posztokat, amikor azok az Ön hírfolyamában voltak”);

² GILLESPIE (2018): 210–211.

³ GILLESPIE (2010): 358.

⁴ GILLESPIE (2018): 188.

⁵ MARTENS et al. (2018): 22.

⁶ Mivel az algoritmus lényege minden közösségimédia-oldal esetében ugyanaz, jelen monográfia csak egy példán (Facebook) keresztül értékeli a tartalomelosztási mechanizmust.

⁷ Facebook Súgóközpont, Hogyan működik a hírfolyam? https://www.facebook.com/help/1155510281178725/?helpref=hc_fnav&cms_id=1155510281178725

- a hozzászólások, kedvelések, reakciók és megosztások száma, amelyeket egy poszt kap más felhasználóktól (pl. „Önnek a WZ felhasználótól származó poszt népszerűbb a többi megjelenített poszthoz képest”);
- a közzététel időpontja, illetve a tartalom relevanciája.⁸

De ne engedjük magunkat megtéveszteni, a közösségi oldalak nem (vagy legalábbis nem csak) azért optimalizálják a tartalmat, mert jobb szolgáltatást szeretnének nyújtani a felhasználóik számára, hanem mert anyagilag érdekeltek abban, hogy a felhasználókat minél pontosabban megcélozzák az egyénre szabott preferenciák alapján. Mára már egyértelmű, hogy a platformok szlogenjei „közelebb hozza egymáshoz a világot”, „otthont ad több ezer közösségnek, végtelen beszélgetésnek és hiteles emberi kapcsolatnak”, „mindenkinek hangot ad és megmutatja a világot”) jól hangzanak a véleménynyilvánítás szabadsága szempontjából, de ugyanilyen fontos, hogy ezen platformok az online hirdetési piac főszereplői is. A digitális reklámparban „a hirdetési bevételek 259 milliárd dollárra nőttek, ami 15%-os növekedést jelent 2023-hoz képest.”⁹

A platformok bevételeinek leggyakoribb forrásai az automatizált hirdetésárverések (más néven a hirdetési licitfolyamatok), amelyek során a hirdetőik licitálnak egy hirdetés platformon való elhelyezésére.¹⁰ A hirdetésárverések lényege egyszerű: a hirdetőik célközönsége között általában átfedésben van, és mivel a reklámok számára rendelkezésre álló helyek száma korlátozott, így csak a legmagasabb összértékű hirdetés (*total value*) jelenhet meg a felhasználók számára.¹¹

Bár az összértéket meghatározó tényezők platformonként változhatnak, a hirdetőik által egy adott kampányért fizetni hajlandó összeg mindig meghatározó tényező. Például a Facebook esetében a teljes érték három tényező (licitösszeg, becsült végrehajtási arányok¹² és a hirdetés minősége) kombinációja, míg az X esetében a hirdetési pontszám (*ad score*) a minőségi pontszám (amelyet a hirdetés rezonanciája,¹³ relevanciája és naprakészsége alapján számolnak) és a licitösszeg szorzata.¹⁴

A licitösszeg az a monetáris összeg, amelyet a hirdetőik hajlandóak fizetni a kívánt eredmény eléréséért – ez azonban nem feltétlenül azonos azzal az összeggel, amelyet a hirdetőiknek ténylegesen ki kell fizetniük. A hirdetőik ugyanis főszabály szerint a hirdetéseikre való kattintások vagy megjelenések száma alapján fizetnek. Mindezeket felül további díjazás ellenében a hirdetőik egyéb szolgáltatásokat is igénybe vehetnek a platformoktól (a hirdetés népszerűsítése a kívánt célközönség elérésének maximalizálása érdekében, a hirdetésnek

⁸ Uo.

⁹ IAB/PwC: Internet Advertising Revenue Report. Full-year 2024 results. IAB.com, 2025. április 17., https://www.iab.com/wp-content/uploads/2025/04/IAB_PwC-Internet-Ad-Revenue-Report-Full-Year-2024.pdf

¹⁰ BRAUN–EKLUND (2019): 2.

¹¹ Facebook Üzleti Súlyközpont, Tudnivalók a hirdetési licitfolyamatról, https://www.facebook.com/business/help/430291176997542?id=561906377587030&ref=fbb_ads

¹² Vagyis annak megbecslése, hogy a hirdetés adott személynek történő megjelenítése kiváltja-e a hirdető által kívánt eredményt.

¹³ Vagyis a hirdető egyéb hirdetéseivel való interakciók száma.

¹⁴ X Business: Bidding and auctions FAQs, <https://business.x.com/en/help/troubleshooting/bidding-and-auctions-faq#what-pricing-options-are-available-on-twitter-ads>

megfelelő cékközönség előtt való elhelyezése a megtekintettség növelése érdekében, valamint a hirdetés – át nem ugorható reklámként való – elhelyezése egy a platformon megosztott videó legelején.¹⁵

A személyre szabás előnyei a reklámozás szempontjából tehát egyértelműek. Egyrészt a platformok garantálják, hogy minden egyes felhasználó számára személyre szabott hirdetés jelenjen meg, így növelve a hirdetésre történő kattintások számát – és ezzel közvetve a hirdetőknél kiszámlázható összeget. Másrészt a platformok algoritmusai optimalizálják a tartalmat annak érdekében, hogy nagyobb forgalmat (kattintásokat és megtekintéseket) generáljanak, így biztosítva, hogy a hirdetésárverés során magasabb összeget tudjanak kérni a hirdetések oldalukon való elhelyezése ellenében. A közösségimédia-oldalak tartalomoptimalizálás keretében olyan tartalmakat népszerűsítnek, amelyek valószínűleg felkeltik a felhasználók figyelmét, következésképpen növelik a megtekintéseket, kattintásokat, és végső soron a hirdetési bevételt.

Ami azonban nem feltétlenül nyilvánvaló, hogy az álhírek készítői, a hamis híreket tartalmazó weboldalak működtetői és más rosszindulatú szereplők parazitaként élőködnek ezen a hirdetési ökoszisztémán. Egyes jelentések szerint az álhírek készítői például könnyen kereshettek már tíz éve is havi 10 000 és 30 000 dollár közötti összeget.¹⁶ Ennek az álhír-ökoszisztémának (*fake news ecosystem*) a legkiemelkedőbb szereplői a paraziták (*parasite*), amelyek működési modellje alapján először a parazita „pénzt fizet egy vagy több szolgáltatónak, akik megígérik, hogy látogatókat irányítanak az oldalára.”¹⁷ Ezen szolgáltatók néhány, a parazita weboldalára irányító hiperlinket tartalmazó hirdetést tesznek közzé a közösségi oldalakon. A parazitaoldal forgalmának növelése érdekében a szolgáltatók elsődleges célja olyan célzott hirdetések megosztása, amelyekre, illetve a bennük elhelyezett hiperlinkekre, a közösségi oldal felhasználói nagy valószínűséggel rákattintanak. Fontos azonban megjegyezni, hogy bár a szolgáltatók által megosztott hirdetések valódi emberi látogatókat is vonzanak, az általuk generált forgalom többnyire ‘érvénytelen forgalom’, azaz botok és kattintásmunkások által generált oldalmegtekintések. Ezután a parazita a közösségimédia-oldalokról áramló javarészt érvénytelen forgalmat eladja a hirdetőknél, és „automatizált rendszereket csábít arra, hogy hamis felhasználók figyelméért licitáljanak.”¹⁸ Másként megfogalmazva a parazita az oldalára érkező érvénytelen forgalmat valódi látogatottsággént tünteti fel a hirdetők számára, akik így hatalmas összegeket fizetnek azért, hogy a hirdetéseiket a parazita weboldalán elhelyezhessék. E hirdetések azonban a valóságban csak egy nem létező, képzeletbeli közönség számára jelennek meg.

Fontos mindazonáltal megjegyezni, hogy a paraziták fentebb ismertetett modelljében a valódi látogatók által generált forgalom elengedhetetlen szerepet tölt be. Az ugyanis nem csupán a parazita weboldalának forgalmát – és így a hirdetők számára a parazitaoldal értékét – növeli, de a botok és kattintásmunkások által generált oldalmegtekintéseket is álcázza, ezáltal nehezítve a parazita weboldalak hirdetői által való azonítását. Pontosan ezért, a kö-

¹⁵ X Business: X Ads campaigns 101, <https://business.x.com/en/help/campaign-setup/campaigns-101>

¹⁶ Laura SYDELL: We Tracked Down A Fake-News Creator In The Suburbs. Here's What We Learned. *NPR*, 2016. november 23., <https://www.npr.org/sections/alltechconsidered/2016/11/23/503146770/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs>

¹⁷ BRAUN–EKLUND (2019): 7.

¹⁸ Uo., 10.

zösségi oldalakon megosztott, a parazita weboldalára irányító hirdetések, illetve egyéb tartalmak legtöbbször álhírek, amelyek kattintásvadász tartalomként (*clickbait content*) ideális esetben futótűzként terjednek az interneten – de legalábbis elegendő valódi látogatottságot generálnak ahhoz, hogy az érvénytelen forgalmat legitimálják. Andrew Guess és munkatársai tanulmányukban például azt találták, hogy az álhíroldalakra irányuló látogatások több mint egyötöde a Facebookról származik.¹⁹

Sajnos azonban nem csak rosszindulatú külső szereplőknek áll érdekében a platform hirdetési ökoszisztémáján keresztül dezinformációt terjeszteni. A nyugtalanító valóság ugyanis az, hogy maguk a közösségi platformok is érdekelték az álhírek terjesztésében. Ahogy arra már fentebb részletesen kitértem, a közösségi oldalak ajánlórendszerei előnyben részesítik és a felhasználók profiloldalain kiemelt helyen tüntetik fel azon tartalmakat, amelyek a legtöbb megtekintést, kattintást generálják, így növelve az adott tartalomhoz tartozó hirdetés helyének értékét. Mivel az álhírek a közösségi médiában a legszélesebb körben megosztott tartalmak közé tartoznak, a platformoknak jelentős pénzügyi érdekeltsége van azok terjesztésében. A platformok tehát anyagi hasznot húznak az álhírek sikeres reklámozásából, amelyet az emberi és a gépi intelligenciát ötvöző különböző hirdetési technológiák alkalmazása garantál. Ezek az eszközök teljesen legálisak, de mivel teljes mértékben automatizáltak, így ajtót nyitnak a visszaélések és a rossz gyakorlatok előtt is, amelyek célja jobb esetben a meg nem érdemelt bevétel megszerzése, rosszabb esetben pedig akár a demokrácia aláásása.²⁰

10.1.2. A közösségimédia-platformok tartalomoptimalizálása eredményez-e egyfajta szerkesztőségi ellenőrzést?

A fentebb leírtak ellenére az ajánlórendszerek alkalmazása és a tartalom személyre szabása természetesen nem ördögtől való. Az online elérhető információk mennyisége olyan hatalmas, hogy megfelelő szűrés nélkül a felhasználók teljesen elvesznének a weboldalakon. A Facebook esetében például 60 másodpercenként 510 000 kommentet tesznek közzé,²¹ míg az X-en ugyanennyi idő alatt átlagosan több mint 350 000 tweet kerül megosztásra.²²

Jelenleg úgy fest, hogy a közösségimédia-platformok által alkalmazott ajánlórendszerek óhatatlanul is információs buborékba zárják a felhasználókat. Vegyük például az álhíreket, amelyek – mint az egyik legszélesebb körben megosztott tartalomtípus – többször a felhasználók hírfolyamának tetején jelennek meg. Ha egy felhasználó interakcióba lép az ilyen tartalommal – például rákattint egy linkre –, az algoritmus a felhasználó valódi érdeklődésétől vagy eredeti szándékától függetlenül a jövőben a hasonló tartalmakat fog előnyben részesíteni. A platform rangsorolási mechanizmusa ugyanis az ilyen tartalmakat nemcsak népszerűek, hanem a felhasználó ismételt elköteleződése miatt relevánsnak is fogja tekinteni.

¹⁹ GUESS et al. (2018): 3.

²⁰ GHOSH–SCOTT (2018): 25.

²¹ N/A: Facebook users, stats, data & trends for 2025. *Datareportal*, 2025. március 12., <https://datareportal.com/essential-facebook-stats>

²² N/A: Twitter Usage Statistics. *Internet Live Stats*, 2025. május 26., <https://www.internetlivestats.com/twitter-statistics>

Ez elkerülhetetlenül egy olyan öngerjesztő folyamatot indít el, amely fokozatosan elszigeteli a felhasználót, végül pedig egy információs buborékba zárja anélkül, hogy arra az adott felhasználó ráeszmélne.

A probléma ezekkel az információs buborékokkal az, hogy az emberek többnyire nem racionális lények. Ritkán férnek hozzá teljes körű információkhoz, sőt, gyakran nem is keresik a teljes körű információkat. Nem céljuk, hogy maximalizálják viselkedésük relatív hasznosságát, és nem kívánják kiszámítani a kockázatot, mielőtt online cselekednének. Ehelyett korlátozott számú heurisztikus elvre támaszkodnak, azaz inkább egyszerű szabályokat (hüvelykujj-szabályokat) használnak döntéseik meghozatalához, semmint, hogy alaposan megvizsgálják az összes rendelkezésre álló információt.²³

A platformok szűrési technológiai három fő mentális hiányosságunkat használják ki:

- az emberek hajlamosak elhinni azokat a történeteket, amelyeket gyakran hallanak, mivel az ismétlés igazolja a hitelességet (ismétlési heurisztika);²⁴
- az emberek hajlamosak figyelmen kívül hagyni az álláspontjukat megkérdőjelező információkat, mivel jobban motiválja őket az, hogy megerősítsék a kialakult hozzáállásukat és hasonlóan gondolkodó információkat keressenek, mint hogy pontos következtetésre jussanak;²⁵ és
- az emberek hajlamosak megbízhatóbbnak tekinteni azokat az információkat, amelyek abból az online közösségből származnak, amellyel szorosan azonosulnak, amelynek részét képezik.²⁶

A platformok ajánlórendszerei tehát nem csak információs buborékba zárják be a felhasználókat, hanem folyamatosan megerősítik azt az elképzelést, amelyre a buborék eredetileg épült, mivel a felhasználó természeténél fogva nem ösztönözhető arra, hogy teljes körű információt keressen, különösen olyan adatokat, amelyek ellentmondanak a meggyőződésének. Ennek eredményeként, hogy az emberek elzárkóznak a hitrendszerüket megkérdőjelező véleményektől és információktól, visszhangkamrák (*echo chambers*) alakulhatnak ki.²⁷ Ezek a visszhangkamrák alapvetően párhuzamos, de különálló univerzumok, amelyek egymás létezéséről nem is tudva léteznek egymás mellett.

A felhasználó által generált tartalmak és az általuk létrehozott visszhangkamrák már több mint egy évtizede a tudományos irodalom vizsgálati tárgyát képezik. Amit azonban a szakirodalom gyakran nem említ, az az, hogy a tartalom személyre szabása Richard Thaler és Cass R. Sunstein szavaival élve egy *'nudge'*. Ahogyan azt kifejtették: ez „a választási architektúra bármely olyan aspektusa, amely kiszámítható módon megváltoztatja az emberek viselkedését anélkül, hogy megtiltana a választási lehetőségeket vagy jelentősen megváltoztatná a gazdasági ösztönzőket.”²⁸ Mivel a platformok ajánlórendszerei egyénre szabott weboldalakat hoznak létre, amelyek felhasználónként eltérőek, így a *nudge*-elmélet alapján a

²³ LEISER (2016): 200–202.

²⁴ LEISER (2017): 3–4.

²⁵ KAAKINEN et al. (2020): 29.

²⁶ Uo., 27–29. o.

²⁷ SEARGEANT–TAGG (2019): 42.

²⁸ THALER–SUNSTEIN (2009): 6.

közösségimédia-platformok választási architektúráknak tekinthetők. Ezen választási architektúrák pedig olyan egyénre szabott viselkedési és döntési kontextusok, amelyek a felhasználókat arra ösztönzik, hogy folyamatosan interakcióba lépjenek a honlapokkal azáltal, hogy olyan tartalmakat kínálnak, amelyek leginkább érdeklik őket. Ez azt is jelenti, hogy ez – definíció szerint – magába foglalja az emberek választásának manipulálását is.²⁹

A tartalomoptimalizálás mellett a #Pizzagate terjesztésében résztvevő platformok mind alkalmaznak önkéntes, automatizált és legfőképpen megelőző komplex tartalommoderálást is. A Facebook például fejlett, gépi tanuláson alapuló mesterséges intelligenciát alkalmazó technológiákat használ azért, hogy előzetesen ellenőrizze, felismerje és eltávolítsa a visszaélészerű és veszélyes tevékenységeket, tartalmakat. A Facebook emellett nemcsak meghatározza a megengedett tartalmak határait, hanem a megfelelő intézkedésekkel (pl. tartalmak eltávolítása, fiókok letiltása stb.) érvényre is juttatja azokat.³⁰ Ehhez nagyon hasonlóan az X is heurisztikus és gépi tanulási algoritmusok kombinációját alkalmazza annak érdekében, hogy automatikusan felismerje és törölje a platform szabályzatát sértő tartalmakat.³¹

Felmerül tehát a kérdés, hogy vajon az ilyen jellegű, a platformok által önként vállalt tartalomoptimalizálás és megelőző tartalmi moderálás szerkesztői ellenőrzésnek tekinthető-e. A szerkesztői ellenőrzés a szerkesztett tartalom ismeretét jelenti,³² ez a tudati elem azonban egyértelműen hiányzik a platformok algoritmikus kurátori tevékenységéből. Ezt erősítette meg a főtanácsnok a Frank Peterson kontra Google LLC, YouTube Inc. és társai, valamint az Elsevier Inc. kontra Cyando AG egyesített ügyekben elfogadott indítványa, amely indítvány szerint a keresési és indexelési funkciók – amelyek elengedhetetlenek a tartalomajánlás-hoz – automatizáltak, és ezért pusztán technikai és automatikus információfeldolgozásról van szó. Ennek következtében a főtanácsnok szerint a szolgáltató nem rendelkezik a keresett információ tartalma felett, annak ellenére, hogy ő volt az, aki a mögöttes eszközöket és az algoritmust kifejlesztette, és ezért ő ellenőrzi a feldolgozott információt.³³ Úgy tűnik tehát, hogy a szerkesztői ellenőrzés gyakorlásáról csak abban az esetben beszélhetünk, ha a platform a vitatott tartalmat előzetesen ismerte. Tagadhatatlan azonban, hogy a #Pizzagate terjesztésében részt vevő platformok közül egyik sem rendelkezett ilyen előzetes ismerettel Hillary Clinton hamisított képmása tekintetében.

10.1.3. Az óriásplatformok azonban – definíciójuk szerint – passzív szerepet töltenek be tartalom nyilvánosság felé való terjesztésében

Korábban részletesen tárgyaltam, hogy számos platform meglehetősen aktív szerepet vállalt a #Pizzagate összeesküvés-elmélet terjesztésében a tartalmak optimalizálásával és moderálásával saját anyagi haszonszerzése érdekében.

²⁹ Uo., 82. és 239.

³⁰ Facebook, Felhasználási feltételek, Áttekintés, <https://www.facebook.com/legal/terms>

³¹ X, DSA Transparency Report, 2024, <https://transparency.x.com/dsa-transparency-report.html>

³² ONG (2015): 135.

³³ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 160. és 162.

Az EB által közzétett, az óriásplatformokat tartalmazó lista³⁴ szerint a Facebook, az X és a YouTube is mind óriásplatformoknak minősül, és így a platform – illetve a tárhelyszolgáltató – definíciója értelmében passzív szerepet tölt be a rajta elhelyezett tartalom tárolásában és nyilvánosság felé való terjesztésében.

Mindez azonban arra enged következtetni, hogy a platformoknak a tartalom tárolásában és nyilvánosság felé való terjesztésében a gyakorlatban betöltött szerepe és a DSA által elképzelt szerepe szöges ellentétben áll egymással. A DSA platformdefiníciója tehát nem tükrözi a valóságot, hiszen a platformok minden esetben a passzív tárhelyszolgáltatók egy típusának minősülnek, függetlenül a valóságban betöltött szerepüktől.

10.2. Felelősségre vonhatók-e a DSA alapján azok a platformok, amelyek Hillary Clinton hamisított képmását hozzájárulása nélkül a nyilvánosság felé terjesztették?

Tekintettel arra, hogy a DSA önmagában nem teremt jogalapot a platformok felelősségre vonására, hanem kizárólag a platformok felelősség alóli mentesülését szabályozza,³⁵ így álláspontom szerint annak a kérdésnek a megválaszolása, hogy felelősségre vonhatók-e azok a platformok, amelyek Hillary Clinton hamisított képmását hozzájárulása nélkül a nyilvánosság felé terjesztették két feltételnek kell teljesülni:

- a nemzeti (jelen esetben magyar) jogszabályok alapján a platformok polgári jogi (pl. kártérítési) felelőssége megállapítható; és
- a platform nem mentesül a felelősség alól a DSA 6. cikke alapján, vagyis a platformnak tényleges tudása van a jogellenes tartalomról és nem intézkedett haladéktalanul a jogellenes tartalom eltávolítása érdekében.

Ebből azonban az is következik, hogy a magyar polgári jogi szabályozás részletes elemzése jelen monográfia keretein belül nem szükséges, amennyiben a platform a DSA 6. cikke alapján egyébként is mentesülne a felelőssége alól.

Az előző alfejezetben levonhattuk azt a következtetést, hogy bár a közösségi platformok aktív szerepet játszottak a #Pizzagate összeesküvés-elmélet terjesztésének elősegítésében, ennek ellenére a DSA által adott definíciójuk értelmében passzív tárhelyszolgáltatóknak minősülnek. A DSA 6. cikkének (1) bekezdése értelmében az ilyen szolgáltatók mentesülnek a harmadik fél által megosztott tartalomért való felelősség alól, amennyiben bizonyítani tudják, hogy (i) vagy nem volt tényleges tudomásuk a kérdéses jogellenes tartalomról; vagy (ii) a tudomásszerzést követően haladéktalanul intézkedtek az adott tartalom eltávolítása vagy az ahhoz való hozzáférés megszüntetése érdekében.³⁶

Amint azt már korábban említettük, a platformok leggyakrabban a bejelentőrendszeiken keresztül benyújtott felhasználói bejelentések révén szereznek tényleges tudomást az

³⁴ A digitális szolgáltatásokról szóló jogszabály alapján kijelölt online óriásplatformok és keresőmotorok felügyelete. Az információkat utoljára 2025. május 15-én frissítették. <https://digital-strategy.ec.europa.eu/hu/policies/list-designated-vlops-and-vloses>

³⁵ DSA (17) preambulumbekkezdés.

³⁶ Novovic (2024): 82.

illegális tartalomról. A felhasználói bejelentés azonban nem az egyetlen módszer, amellyel a tudomásszerzés történhet. A #Pizzagate-ügy különösen érdekes kérdést vet fel ezzel kapcsolatban a DSA alapján.

A 2016-os amerikai választások idejére az összeesküvéssel kapcsolatos tartalmak széles körű terjedése a főbb közösségimédia-platformokon már közismert volt. Sőt, a neves hírportálok, mint például a *The Washington Post*,³⁷ a *The Independent*³⁸ vagy a *The Washington Times*³⁹ már nagy terjedelemben írtak a #Pizzagate összeesküvés-elméletéről és annak főbb közösségimédia-platformokon való terjedéséről. Emellett a Comet Ping Pong étterem tulajdonosa a Twittert, a Redditet, a Facebookot és a YouTube-ot is megkérte, hogy segítsenek neki megállítani az összeesküvés-elmélet terjedését.⁴⁰ Ez felveti azt a kérdést, hogy a közösségimédia-platformok szereztek-e olyan mértékű tudomást a #Pizzagate illegális tartalmáról, amely elegendő volt ahhoz, hogy a DSA szerinti felelősséget megalapozza, még a felhasználók formális értesítésének hiányában is.

Erre a kérdésre a válasz feltehetőleg negatív lesz, minden bizonnyal két fő okból. Először is, pusztán a jogellenes tartalom lehetséges létezésének absztrakt ismerete nem minősül tényleges ismeretnek a DSA 6. cikke (1) bekezdésének a) pontja értelmében.⁴¹ Ezt alátámasztja az EUB ítélkezési gyakorlata, amely szerint – ahogy fentebb láthattuk – a tárhelyszolgáltatók felelősségének kiváltásához nem elegendő pusztán az a tény, hogy a platform tudott arról, hogy olyan tartalmakat tárol, amelyek jogellenesnek minősülhetnek.⁴² Míg a tudományos vita nagyrészt arra összpontosított, hogy a tényleges ismeret megköveteli-e a felhasználók által létrehozott konkrét tartalmak jogellenességének tudatosítását, viszonylag kevés figyelmet fordítottak arra a kérdésre, hogy az ilyen ismeretnek a tartalom konkrét eseteire kell-e vonatkoznia, nem pedig az absztrakt tartalomra. Úgy tűnik, az uralkodó tudományos nézet az, hogy a tárolt tartalom pusztán létezésének ismerete nem elegendő, ehelyett a szolgáltatónak inkább olyan információkkal kell rendelkeznie, amelyek egyértelműen jelzik a kérdéses tartalom jogellenességét. Ez az érvelés – álláspontom szerint – hasonlóképpen alkalmazandó annak vizsgálatakor is, hogy a tudásnak konkrétan kell-e lennie. Ennek

³⁷ Abby OHLHEISER: Fearing yet another witch hunt, Reddit bans 'Pizzagate'. *The Washington Post*, 2016. november 24., <https://www.washingtonpost.com/news/the-intersect/wp/2016/11/23/fearing-yet-another-witch-hunt-reddit-bans-pizzagate>

³⁸ Lizzie DEARDEN: Donald Trump's transition team dismisses CIA findings Russia attempted to influence US election in his favour. *The Independent*, 2016. december 10., <https://www.independent.co.uk/news/world/americas/donald-trump-russia-us-election-intervene-hacks-cyberattacks-dnc-podesta-emails-leak-help-victory-denies-transition-team-a7466986.html>

³⁹ Andrew BLAKE: Alex Jones, Infowars founder, appeals to Trump for aid over fears of 'fake news' crackdown. *The Washington Times*, 2016. december 9., <https://www.washingtontimes.com/news/2016/dec/9/alex-jones-conspiracy-theorist-appeals-trump-aid-o>

⁴⁰ Abby OHLHEISER: Fearing yet another witch hunt, Reddit bans 'Pizzagate'. *The Washington Post*, 2016. november 24., <https://www.washingtonpost.com/news/the-intersect/wp/2016/11/23/fearing-yet-another-witch-hunt-reddit-bans-pizzagate>

⁴¹ WILMAN–KALÉDA–LOEWENTHAL (2024): 170.

⁴² Google France SARL és Google Inc. kontra Louis Vuitton Malletier SA (C-236/08), Google France SARL kontra Viaticum SA és Luteciel SARL (C-237/08) és Google France SARL kontra Centre national de recherche en relations humaines (CNRRH) SARL és társai (C-238/08), ECLI:EU:C:2010:159; C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503.

megfelelően a potenciálisan jogellenes tevékenység általános ismerete – például a #Pizzagate összeesküvés-elmélethez kapcsolódó tartalom létezésének ismerete – nem elegendő. Ahhoz, hogy a felelősség felmerüljön, a tárhelyszolgáltatónak tudnia kell a konkrét, azonosítható, törvénytörtő tartalomról.

Másodszor, ez az értelmezés összhangban van a DSA 8. cikkével, amely kifejezetten előírja, hogy a tárhelyszolgáltatókra nem vonatkozik általános ellenőrzési kötelezettség, és nem kötelesek aktívan keresni a jogellenes tevékenységre utaló tényeket vagy körülményeket. Következésképpen a platformok jogilag nem voltak kötelesek proaktívan megvizsgálni a felhasználók által generált hatalmas mennyiségű tartalmat annak érdekében, hogy felderítsék és eltávolítsák a #Pizzagate összeesküvés-elmélethez kapcsolódó tartalmakat. Ha azonban ezek a platformok önkéntesen saját vizsgálatokat végeztek volna (pl. az étterem tulajdonosának kérésére), és ennek során konkrét #Pizzagate tartalmakat azonosítottak volna, akkor ezáltal tényleges tudomást szereztek volna az ilyen tartalmakról, és így felelősségük is felmerült volna.

A fentiekből következik, hogy a legtöbb esethez hasonlóan a #Pizzagate-tel kapcsolatban is a platform tényleges tudomásszerzése és így potenciális felelőssége csak egy DSA szerinti bejelentéssel alapozható meg.⁴³ Eltekintve attól a tényről, hogy a platformok ajánlórendszerei a #Pizzagate-et csak olyan felhasználók számára jelenítették meg, akiket az feltehetően érdekelt, és így azt nagy valószínűséggel nem is jelentették, a monográfiában szereplő jogi vizsgálat végigfuttathatósága érdekében tételezzük fel, hogy legalább az egyik óriásplatform (pl. az X vagy a Facebook) kapott ilyen értesítést.

A fentiek szerint a bejelentés – önmagában, a platformok további vizsgálata nélkül – a jogellenes tartalom tényleges ismeretéhez akkor vezethet, ha az megfelel meghatározott jogi követelményeknek.⁴⁴ Az egyik ilyen követelmény, hogy a bejelentés elegendő információt tartalmaz ahhoz, hogy egy gondos tárhelyszolgáltató részletes jogi vizsgálat nélkül is egyértelműen megállapíthassa, hogy a bejelentett tartalom jogellenes.⁴⁵ Ez az EUB ítélezési gyakorlatából következik, amely szerint az értesítésnek elegendő információt kell tartalmaznia ahhoz, hogy „az adott platform üzemeltetője részletes jogi vizsgálat nélkül is meggyőződhesen arról, hogy az említett közlés jogellenes, és hogy az említett tartalom eltávolítása összeegyeztethető a véleménynyilvánítás szabadságával.”⁴⁶ Vitathatatlan, hogy amikor egy tárhelyszolgáltató egy bejelentés alapján döntést hoz, gyakorlatilag arról dönt, hogy mások jogainak és/vagy érdekeinek védelme érdekében korlátozza-e valaki véleménynyilvánítási szabadságát. Ennek az egyensúlynak az elérése gyakran kihívást jelent még a képzett jogászok és tapasztalt bíróságok számára is. Vegyük például az EJEB-et, amelynek elemzései gyakran hosszan elemzik azokat a körülményeket, amelyekre tekintettel a véleménynyilvánítás szabadsága jogszerűen korlátozható. Ezért az EUB helyesen állapította meg azon követelményt, hogy a bejelentett tartalom jogellenességének elég egyértelműnek kell lennie ahhoz, hogy a jogi képzettséggel nem rendelkező tárhelyszolgáltató képes legyen a versengő jogok közötti méltányos egyensúlyt megteremteni. Jogosan merülhet fel azonban a kérdés,

⁴³ DSA 16. cikk (2).

⁴⁴ WILMAN–KALÉDA–LOEWENTHAL (2024): 172.

⁴⁵ DSA (53) preambulumbekzdés; DSA 16. cikk (3).

⁴⁶ C-682/18. és C683/18. egyesített ügyek, Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503, 116.

hogy vajon az olyan technológiai óriáscégek, mint például a Meta vagy a TikTok milyen mértékben tekinthetők ‘jogi végzettséggel nem rendelkező’ tárhelyszolgáltatóknak, hiszen ezen cégeknek nyilvánvalóan hatalmas, globális jogi osztályaik vannak, és tucatnyi ügyvédi irodával dolgoznak együtt napi szinten a jogellenes tartalmak megítélésével összefüggésben. Az EJEB már a Delfivel kapcsolatban is megállapította, hogy a Delfi professzionális kiadóként nem hivatkozhat arra, hogy a vonatkozó jogszabályokat és a kapcsolódó bírói gyakorlatot nem ismerte.⁴⁷ Véleményem szerint ugyanakkor még ha a platformok jogi végzettséggel nem rendelkező tárhelyszolgáltatóknak minősülnének is, a tartalom jogellenessége számos esetben (pl. a Hillary Clintonról közzétett felvétel esetén) nem egyértelmű.

De most térjünk vissza a hipotetikus esetünkhöz, amelyben egy felhasználó a #Pizzagate-tartalmat – konkrétan azt a képet, amelyen állítólag Hillary Clinton bokáján nyomkövetőt visel – bejelenti.

A fenti bekezdés fényében az első kérdés, amellyel a platformnak az ilyen bejelentés kézhezvételekor foglalkoznia kell, hogy a bejelentés elegendő mértékben specifikus-e ahhoz, hogy a platform részletes jogi értékelés nélkül dönthessen a bejelentett tartalom jogellenes voltáról. Ha ez nem így van, akkor nem tekinthető úgy, hogy a platform tényleges tudomást szerzett a jogellenes tartalomról, és ezért nem lép életbe a DSA 6. cikke.

A DSA 16. cikkének (3) bekezdése kifejezetten a bejelentés tartalmára vonatkozó követelményeket állapít meg, nem pedig a bejelentett tartalom egyértelmű jogellenességének bizonyítására vonatkozó érdemi kötelezettséget ír elő. A DSA tehát nem írja elő, hogy a tartalom jogellenességének azonnal nyilvánvalónak kell lennie; inkább azt követeli meg, hogy a bejelentő kellően részletes információkat szolgáltatson ahhoz, hogy a tárhelyszolgáltató azt meg tudja állapítani. Ez sok esetben teljesen észszerű. Vegyünk például egy olyan helyzetet, amelyben egy felhasználó bejelent egy tízperces, animált rajzfilmet a YouTube-on: további kontextus hiányában a bejelentett tartalom elsőre nem tűnhet jogsértőnek. Ha azonban a bejelentő jelzi, hogy ő az eredeti szerzője a rajzfilmnek, és a videót a hozzájárulása nélkül töltötték fel, akkor a platformnak lehetősége van arra, hogy a tartalom esetleges jogellenességét anélkül értékelje, hogy bonyolult jogi elemzésbe bocsátkozna.

Ugyanakkor azt is ki kell emelnem, hogy vannak olyan esetek is, amikor a tartalom nem egyértelműen jogellenes, és azt még egy kellően részletezett bejelentés sem tudja orvoslani. Tökéletes példa erre a jelen ügy, azaz maga a ‘nyomkövetőt viselő’ Hillary Clintonról készült fotó. Kétségtelen, hogy a fotó hamisítvány volt. Azonban, mint fentebb tárgyaltuk, csak mert egy kép hamisítvány, az nem jelenti automatikusan azt, hogy jogellenes, és azt sem, hogy kétségtől jogellenes. A korábbi fejezetek hosszasan tárgyalták azokat a körülményeket, amelyek fennállása esetén az álhírek még a védett szólás körébe tartozhatnak. Ha például egy felhasználó jelentené a #Pizzagate-történetet (vagy még inkább a Hillary Clintonról készült képet), akkor a platformnak hasonlóan árnyalt jogi értékelést kellene végeznie annak megállapításához, hogy a tartalom valóban jogellenes-e. Ez azt jelenti, hogy ilyen esetben a kép pusztá jelentése nem feltétlenül váltaná ki a platform tényleges tudomásszerzését a DSA 16. cikkének (3) bekezdése alapján, mivel a jogellenesség további jogi elemzés nélkül nem lenne nyilvánvalóan megállapítható.

⁴⁷ Delfi AS kontra Észtország, App no. 64569/09 (2015. június 16.), 129.

Másrészt, ha a platform tényleges tudomását minden kellően részletezett bejelentés megalapozná – még akkor is, ha maga a bejelentett tartalom nem egyértelműen jogellenes –, akkor a platformnak minden egyes alkalommal hosszas jogi elemzést kellene végeznie annak eldöntése érdekében, hogy szükséges-e bármilyen intézkedés megtétele a felelősség alóli mentesülése érdekében. Egy ilyen elemzés magában foglalná annak értékelését, hogy a tartalom eltávolítása a véleménynyilvánítás szabadságához való alapvető jog szükséges és arányos korlátozásának minősülhet-e. Ha a DSA-nak ez az értelmezése helyes lenne, akkor ez azt jelentené, hogy a rendelet „alapvető jogokat érintő kötelezettségeket ró a magánszemélyekre”⁴⁸ azáltal, hogy a platformokat a hagyományosan a nemzeti bíróságok számára fenntartott feladattal bízta meg, vagyis, hogy találják meg az egymással versengő alapvető jogok, például a véleménynyilvánítás szabadsága és az emberi méltóság közötti finom egyensúlyt.

Ennek eredményeképpen a platformok a szólásszabadság határainak döntőbíróivá válnának, ami nem csak ellentmondásos, de jelentős kockázatot is jelent.⁴⁹ Ahogy Natalie Alkiviadou kifejti, a közösségimédia-platformok „magáncégek, amelyekre nem vonatkoznak a nemzetközi emberi jogi kötelezettségek, és amelyekre nem vonatkozik a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 19. cikke szerinti kötelezettség. Ráadásul a cégek a (...) DSA-hoz hasonló jogszabályok értelmében súlyos bírságokkal szembesülnek, és feladatuk a gyűlöletkelzőnek ítélt tartalmak ellenőrzése és eltávolítása.”⁵⁰

Mindezek mellett, mivel a platformok csak akkor mentesülhetnek a felelősségük alól, ha haladéktalanul cselekednek a jogellenes tartalom eltávolítása érdekében, nem meglepő, ha inkább óvatosságra törekednek, és a lehetséges jogi vagy reputációs következmények miatt inkább a kétséges megítélésű tartalmak eltávolítása mellett döntenek. A Future of Free Speech 2024-es jelentése például kimutatta, hogy Franciaországban, Németországban és Svédországban a Facebookról és a YouTube-ról eltávolított kommentek 88–98%-a valójában jogilag védett megnyilvánulás volt.⁵¹

A fentiekből következik, hogy bár a platformok aktív szerepet játszottak a #PizzaGate összeesküvés-elmélet terjesztésében, főszabály szerint mégis mentesülnek a potenciális felelősség alól a DSA 6. cikke alapján. Ebből egyúttal az is következik, hogy a magyar polgári jogi szabályozás részletes elemzése a továbbiakban szükségtelen.

10.3. A DSA szerinti kellő gondossági kötelezettségek elegendő védelmet nyújthatnak-e a #PizzaGate összeesküvés-elmélet ellen?

A fentiekből tehát az következik, hogy bár a platformok a tartalom terjesztésében aktív szerepet töltenek be, a DSA alapján az általuk tárolt jogellenes tartalomért csak szűk körben vonhatók felelősségre. A DSA által bevezetett bináris rendszer fényében ugyanakkor joggal vetődik fel a kérdés: amennyiben a DSA a platformok aktív szerepének negatív következmé-

⁴⁸ CHAKRAVORTI–TRACHTMAN (2025): 226.

⁴⁹ Ez még akkor is így van, ha például Mark Zuckerberg 2025-ben a véleménynyilvánítási szabadság élharcosaként tetszeleg [BRUTTIN (2025)].

⁵⁰ ALKIVIADOU (2024): 210.

⁵¹ VIGEN SMOLARZ – VINTHER-JENSEN (2024): 41.

nyeit (például az információs buborékok kialakulását) nem a felelősségi szabályok útján kívánja kezelni, vajon a platformokkal szemben előírt kellő gondossági kötelezettségek alkalmasak-e arra, hogy hatékony védelmet biztosítsanak?

E kérdés megválaszolása érdekében először a platformok tartalomterjesztésben betöltött aktív szerepének negatív következményeit szükséges bemutatni, majd ezt követően arra kell kitérni, hogy a platformokkal szemben előírt kellő gondossági kötelezettségek képesek-e hatékony védelmet biztosítani ezen negatív következményekkel szemben.

10.3.1. A visszhangkamrák negatív következményei

Amint azt korábban kifejtettük, a platformok ajánlórendszerei viselkedési profilokat hoznak létre minden egyes felhasználó számára, ezáltal személyre szabva a szolgáltatást a felhasználók valós vagy feltételezett preferenciái alapján.⁵² A közösségimédia-platformok tehát nem pusztán egy objektív világképet mutatnak be, hanem az egyéni preferenciákhoz igazított környezetet alakítanak ki. Ennek eredményeképpen visszhangkamrák és szűrőbuborékok (*filter bubbles*) alakulnak ki, amelyekben a hasonló nézeteket valló egyének összegyűlnek és erősítik egymás nézeteit és prioritásait ahelyett, hogy a különböző nézőpontokat ütköztetnének saját álláspontjuk csiszolása érdekében. Ez azonban egyúttal ahhoz is vezet, hogy a szűrőbuborékokban lévő felhasználókban az a téves elképzelés alakul ki, hogy a világnak ez a moderált változata maga a valóság.⁵³

Az egyéni autonómia magában foglalja az önrendelkezési képességet és a jogot, hogy az egyén saját meggyőződése, az általa gyűjtött információk és értékek alapján alakítsa ki a saját álláspontját. Ez döntően azt igényli, hogy az egyénnek valódi lehetősége legyen arra, hogy tájékozottan, önkéntesen, kényszerítéstől, indokolatlan korlátozásoktól vagy aránytalan külső befolyástól mentesen hozza meg döntéseit.⁵⁴ Úgy tűnik azonban, hogy a platformok ajánlórendszerei pontosan ezt az autonómiát veszik el a felhasználóktól, mivel egy szűk buborékba kényszerítik őket, ahol a rendelkezésre álló információk az egyetlen igazságként jelennek meg. Ahogy Eduardo Magrani és Paula Guedes Fernandes da Silva kifejtették, az ajánlórendszerek „beavatkoznak az emberek autonómiájába mindenféle tartalom ajánlása formájában, a zenétől és a filmekről kezdve a munkalehetőségekig, a felhasználókat egy bizonyos irányba ösztökélve, általában a profiljukból levont preferenciáikhoz kapcsolódóan, megpróbálva őket bizonyos típusú tartalmakra rászoktatni, vagy korlátozni a lehetőségek körét, amelyeknek ki vannak téve.”⁵⁵

Mivel az ajánlórendszerek – pontosabban az általuk létrehozott információs buborékok – elszigetelik a felhasználókat a különböző nézőpontoktól, nem meglepő, hogy a személyre szabottságra és annak a demokráciára leselkedő veszélyeire már több mint egy évtizede rámutat a tudományos irodalom. Cass R. Sunstein például már 2001-ben a *Republic.com* című könyvében kiemelte, hogy a személyre szabás a fragmentációig fokozódik,⁵⁶ ami

⁵² MAGRANI – DA SILVA (2024): 147.

⁵³ KHOSRAVINIK (2017): 67.

⁵⁴ MAGRANI – DA SILVA (2024): 147.

⁵⁵ Uo., 148.

⁵⁶ Vö.: LEMLEY (2021): 1418.

végül negatív hatással lesz a demokratikus vitákra.⁵⁷ Hasonlóképpen mutatták azt is ki, hogy az információs buborékok „erősítik a diszkriminatív előítéleteket és az egyéni előítéleteket, növelve a polarizációra, a gyűlöletbeszédre és a nyilvános beszéd manipulálására való fogékonyságot”.⁵⁸ Seth Flaxman és munkatársai 2016-ban végeztek egy empirikus vizsgálatot 50 000, az Egyesült Államokban található internetfelhasználó online böngészési szokásait elemezve. A vizsgálat során kimutatták, hogy „a közösségi médián vagy webes keresőmotorokon keresztül talált cikkek valóban magasabb ideológiai szegregációval járnak, mint azok, amelyeket az egyén közvetlenül a híroldalak látogatásával olvasott.”⁵⁹ Az ilyen ideológiai szegregáció azonban elkerülhetetlenül további negatív következményekkel jár, mint például:

- a sokszínűségnek való kitettséggel ellentétben nem növeli a toleranciát az egyén sajátjától eltérő attitűdökkel és meggyőződésekkel szemben;
- elkerülhetetlenül torzítja egy vélemény valódi népszerűségét, és ezért az emberek, különösen a kisebbségben lévők hajlamosak lehetnek túlbecsülni nézeteik népszerűségét, nehezen fogadva így el egy olyan eredmény legitimitását, amely nem felel meg a meggyőződésüknek; és
- társadalmi polarizálódást eredményez, és az emberek szélsőségesebb nézeteket vallhatnak, mint amilyenekkel eredetileg rendelkeztek.⁶⁰

A szűrőbuborék tehát közvetlen veszélyt jelent a véleménynyilvánítás szabadságára, különösen arra az aspektusára, hogy az egyén mindenféle információt és eszmét szabadon, határok nélkül kereshessen, megismerhessen és terjeszthessen, akár szóban, írásban vagy nyomtatásban, művészeti formában, vagy bármely más, szabadon választott médiumon keresztül.⁶¹

Az algoritmikus személyre szabás funkciójával kapcsolatos másik aggály, hogy közvetett módon más alapvető jogokat is veszélyeztet, például a gondolat-, a lelkiismereti és a vallásszabadságot, a gyülekezési és egyesülési szabadságot, valamint a választások szabadságát. A kettős folyamat elmélete (*dual process theory*) szerint az emberi gondolkodás két fajtája közül az egyik a reflektív gondolkodás, amely „az információk szándékos és tudatos feldolgozásával társul”.⁶² De ha az emberek az igazságnak csak egy kis, egyénre szabott szeletét látják, amelyet algoritmikusan hoztak létre az eredeti elképzeléseik érvényesítésére, akkor hogyan tudnak megalapozott döntéseket hozni az életük más területein? A korlátozott információ elkerülhetetlenül torz döntésekhez vezet.

Ahogy korábban láthattuk, Thaler és Sunstein szerint a tartalom személyre szabása is egy *‘nudge’* azaz az emberek döntéseinek manipulálása. Az algoritmikus személyre szabással azonban az a fő probléma, hogy nem nevezhető *‘positive nudge’*-nak, mivel nem felel meg az előírt követelményeknek:

⁵⁷ SUNSTEIN (2001); SUNSTEIN (2007).

⁵⁸ MAGRANI – DA SILVA (2024): 149.

⁵⁹ FLAXMAN–GOEL–RAO (2016): 304.

⁶⁰ GARRETT–RESNICK (2011): 108–109.

⁶¹ Polgári és Politikai Jogok Nemzetközi Egyezségokmánya 19. cikk (2); Emberi Jogok Európai Egyezménye 10. cikk (1).

⁶² HANSEN–JESPERSEN (2013): 13.

- A közösségimédia-platformok nem úgy szervezik az architektúrát, hogy az a felhasználók választásait és viselkedését az ő érdekeiknek megfelelően befolyásolja. Ehelyett a döntéshozatali összefüggéseket a profit határozza meg, mivel az a szándék húzódik meg mögötte, hogy növeljék a weboldal forgalmát és ezáltal a hirdetési bevételeket.
- A tartalom személyre szabása nem átlátható, mivel nem világos a mögötte álló valódi szándék, valamint, hogy milyen eszközökkel kívánnak viselkedésbeli változást elérni.
- A tartalom személyre szabása nem őrzi meg a szabadságot, mivel a felhasználóknak nincs lehetőségük arra, hogy ne legyenek profilalkotás tárgyai, és így ne kényszerüljenek egy személyre szabott szűrőbuborékba.⁶³

10.3.2. A DSA által nyújtott védelem a visszhangkamrákkal szemben

A DSA elfogadásának idején már széles körben ismert volt mind az ajánlórendszerekből eredő információs buborékok létezése, mind pedig azok negatív társadalmi hatása. A DSA mégsem tesz egyetlen utalást sem az információs buborékokra vagy a visszhangkamrákra.⁶⁴ Ugyanakkor – ahogy azt korábban láthattuk – bizonyos mértékig mégiscsak szabályozza az online platformok ajánlórendszereit. Felmerül azonban a kérdés, hogy a DSA ezen rendelkezései milyen mértékben nyújtanak hatékony védelmet a visszhangkamrákkal szemben.

Korábban arra a két fő kötelezettségre összpontosítottam, amelyet a DSA az ajánlórendszerek tekintetében a platformokra ró. Először is, a DSA 27. cikke előírja, hogy a platformoknak tájékoztatniuk kell a felhasználókat az ilyen rendszerek használatáról. Másodszor, a 38. cikk arra kötelezi az óriásplatformokat, hogy az alapértelmezett ajánlórendszerük mellett legalább egy alternatív lehetőséget kínáljanak a felhasználók számára.

Bár a DSA 27. cikke növelheti a felhasználók tudatosságát azzal kapcsolatban, hogy miért látnak bizonyos tartalmakat egy bizonyos sorrendben, ez nem akadályozza meg a felhasználók információs buborékokba való zárását. Így a visszhangkamrák káros hatásait csak csekély mértékben mérsékeli. Ezzel szemben a DSA 38. cikke érdemibb kísérletet tesz az említett aggályok kezelésére, mivel megköveteli az óriásplatformoktól, hogy érdemi választási lehetőséget biztosítsanak a felhasználóknak. Álláspontom szerint azonban a DSA 38. cikkének potenciális előnyei a gyakorlatban valószínűleg nem fognak teljes mértékben megvalósulni.

Először is azért, mert a DSA 38. cikk csak az óriásplatformokkal foglalkozik. Bár tagadhatatlan, hogy e platformok ajánlórendszereinek hatása a legnagyobb, a kisebb platformok ajánlórendszerei is igen jelentősek lehetnek.⁶⁵ A monográfia tárgyát képező hipotetikus esetünk kiváló példa erre. Amint azt korábban tárgyaltuk, a #Pizzagate összeesküvés-elmélet kezdetben olyan platformokon nyert teret és terjedt gyorsan, mint a Reddit és a

⁶³ Uo., 17.

⁶⁴ PAPP (2023): 146.

⁶⁵ GÖSSL (2023): 23.

4chan. E platformok egyike sem minősül óriásplatformnak, így nem kötelesek a felhasználók számára az alapértelmezett ajánlómechanizmusaik mellett alternatív tartalomszervezési rendszert biztosítani.

A második oka a DSA 38. cikkében foglaltak megvalósulási nehézségeinek, hogy a vonatkozó jogszabályhely csak egy kilépési mechanizmust biztosít, így a felhasználóknak aktívan dönteniük kell, hogy nem használják a platform ajánlórendszerét. Ahogy Susanne Lilian Gössl kifejti, ezzel a jogalkotási döntéssel az a probléma, hogy „az *opt-out* lehetőség (...) kevésbé hatékony, mint az *opt-in*, és arra ösztönzi a felhasználókat, hogy csak azt használják, amit már biztosítanak számukra.”⁶⁶ Ennek egyik oka az lehet, hogy a felhasználók egyszerűen nincsenek tisztában a platformon lévő ajánlórendszerek letiltásának lehetőségével, hiszen hajlamosak nem elolvasni a regisztráció során megadott információkat, és egyszerűen csak átkattintanak rajta.⁶⁷ Még ha a felhasználók tisztában is lennének azzal, hogy hogyan válhatnak át nem személyre szabott tartalomra, akkor sem valószínű, hogy élnek ezzel a funkcióval. Mindazokon túl, hogy a profilozáson alapuló ajánlórendszerek növelik a platform-szolgáltatás hatékonyságát és a felhasználói élményt, a tanulmányok azt is kimutatták, hogy a felhasználók elutasítják a személyes, objektív információkat, amelyek egyébként elmentnédnek a felfogásuknak.⁶⁸ És mivel kevesen akarnak olyan tartalmakat látni, amelyeket helytelennek vagy akár ellenségesnek tartanak, valószínűtlen, hogy a felhasználók önként választanának olyan szolgáltatást, amely következetesen ilyen tartalmakat jelenít meg.

Harmadik érvem, hogy mind a DSA 27. cikke, mind pedig a DSA 38. cikke legfeljebb az átláthatóság előmozdítását célozza,⁶⁹ nem pedig a tartalomsemlegesség kikényszerítését. A DSA nem kötelezi az online óriásplatformokat arra, hogy objektív vagy kiegyensúlyozott információkat nyújtsanak a felhasználóknak, és nem tiltja az olyan ajánlórendszerek alkalmazását sem, amelyek a szélsőséges álláspontokat helyezik előtérbe vagy erősítik fel. Ahogy Will Mbíoh fogalmazott: „ha egy ajánlórendszer az ideológiai szélsőségek felé tereli a felhasználókat anélkül, hogy (szükségszerűen) illegális tartalmakkal foglalkozna, akkor (...) a DSA egyetlen rendelkezése sem kényszeríti a platformot a beavatkozásra.”⁷⁰ Hogy ezt a #Pizzagate-üggyel összefüggésben szemléltessük: ha a Reddit algoritmus a #Pizzagate-narratívát minden felhasználó hírfolyamának tetején kiemelten megjelenítette volna, és a többi tartalmat nem szabta volna személyre – vagyis nem mutatott volna profilalkotáson alapuló tartalmat egyes felhasználóknak –, a Redditnek a DSA 38. cikk alapján nem lett volna kötelessége alternatív, nem személyre szabott tartalomszervezési rendszert kínálni.

A negyedik, általánosabb szintű érv, hogy „a DSA-t úgy tervezték, hogy különböző károkat szabályozzon: illegális tartalmakat, azonosítható rossz szereplőket és kifejezett uszítást.”⁷¹ Az algoritmikus moderálás azonban nem tartozik egyik kategóriába sem. A tartalom személyre szabása olyan folyamat, amely káros társadalmi hatásokat eredményezhet anélkül, hogy egyértelműen jogellenes tartalmat vagy azonosítható rosszindulatú szereplőt

⁶⁶ Uo., 24.

⁶⁷ BERGRAM et al. (2020): 188.

⁶⁸ Ez a jelenség az úgynevezett ellenséges hírekkel szembeni elfogultság (*hostile news bias*). PAPP (2023): 148.

⁶⁹ MAGRANI – DA SILVA (2024): 160–161.

⁷⁰ MBÍOH (2024): 206.

⁷¹ Uo., 208.

vonna magába.⁷² Példának okáért, még ha bizonyos #Pizzagate-hez kapcsolódó anyagok a véleménynyilvánítás szabadságához való jog alapján védett megnyilvánulásoknak minősül-nének is (és így a platformok mentesülnének az eltávolításuk kötelezettsége alól), az in-formációs buborék kialakultak volna, a felhasználók továbbra is szembesültek volna ezen összeesküvés-elmélettel, és a #Pizzagate való életben bekövetkezett következményei (pl. a lö-völdözés) is bekövetkeztek volna.

Véleményem szerint a fentiekből az a következtetés vonható le, hogy a DSA nem nyújt elégséges védelmet az információs buborékokkal és a visszhangkamrákkal szemben. Ezzel ért egyet például Papp János Tamás is, aki úgy fogalmazott, hogy a DSA rendelkezései „nem tudnak teljes és közvetlen hatást gyakorolni, ezért nem jelentenek egyszerű megoldást a szűrőbuborék-hatás jelenségére.”⁷³ Will Mbioh még arra a következtetésre is jutott, hogy a DSA nemcsak elégtelen, de „szerkezetileg képtelen kezelni az algoritmikus sodródás jelen-tette kihívást”.⁷⁴

⁷² BADOUARD (2020)

⁷³ PAPP (2023): 146.

⁷⁴ MBIOH (2024): 208.

11. Összefoglalás és javaslatétel egy hatékonyabb platformszabályozásra

Monográfiám 3. és 4. fejezetében részletesen ismertettem, hogy a jog jelenleg milyen megközelítés alapján szabályozza az internetet, illetve ezen belül az online platformokat. A szakirodalom elemzése alapján megállapítottam, hogy napjainkban a jogalkotó az integrált szabályozás elméletét követi, vagyis a meglévő jogszabályoknak a kibertérben létrejövő jogviszonyokra való alkalmazását írja elő.

Monográfiám 5. és 6. fejezetében a képmáshoz való jog interneten való érvényesülését vizsgáltam a #PizzaGate összeesküvés-elméleten keresztül. Ezzel összefüggésben arra a következtetésre jutottam, hogy a Hillary Clintonról terjesztett hamisított képmás a volt külügyminiszter képmáshoz való jogát nyilvánvalóan sértette. A Hillary Clinton képmáshoz való jogát sértő deepfake-felvétel közösségimédia-oldalakon keresztüli terjesztésének vizsgálata továbbá arra is rávilágított, hogy a közösségimédia-oldalaknak az egyén képmáshoz való jogához való hozzáállása a mai napig alapjaiban téves. Mindebből így azt a következtetést vontam le, hogy a képmáshoz való jog tömegesen sérül az interneten, mivel a jog az alapul fekvő technológiát egyáltalán nem – vagy legalábbis nem hatékonyan – szabályozza.

Monográfiám utolsó részében (7–10. fejezetek) arra a kérdésre kerestem a választ, hogy vajon a DSA hatékony védelmet biztosít-e a képmáshoz való jogában megsértett Hillary Clinton számára. Erre a kérdésre nemleges választ tudtam csak adni, mivel (i) főszabály szerint a DSA alapján nem vonhatók felelősségre azok a platformok, amelyek a #PizzaGate összeesküvés-elmélet keretében Hillary Clintonról megosztott hamisított képmás tárolásában és nyilvánosság felé való terjesztésében közreműködtek, és (ii) a DSA által a platformokkal szemben előírt kellő gondossági kötelezettségek sem nyújtanak hatékony védelmet a #PizzaGate összeesküvés-elmélet visszhangzó információs buborékokkal szemben.

A fentebb leírtak alapján a monográfiám fő kérdésére az a válasz adandó, hogy az integrált szabályozás elmélete önmagában nem alkalmas és nem is képes az interneten kialakuló sajátos jogviszonyok hatékony rendezésére. Ezért az utolsó fejezetben – a főbb kutatási eredményeim összefoglalásán túl – javaslatot fogalmazok meg arra vonatkozóan, hogy milyen eszközökkel és módszerekkel lehetne a platformok működését a jelenleginél hatékonyabban és eredményesebben szabályozni.

11.1. A főbb kutatási eredmények összefoglalása

11.1.1. A képmáshoz való jog tömeges megsértése az interneten

Több példán keresztül bemutattam, hogy a képmáshoz való jog miként nem tud megfelelő módon érvényesülni az interneten. Monográfiámban bebizonyítottam, hogy noha napi szinten 14 milliárd képet osztanak meg a közösségi médián keresztül, a közösségimédia-oldalaknak az egyén képmáshoz való jogához való hozzáállása – álláspontom szerint – a mai napig alapjaiban téves.

Egyrészről a tagelés a jogi szempontból való elemzése kapcsán láthattuk, hogy a közösségimédia-oldalakon keresztül megosztott fénykép célközönsége elsődlegesen a bejegyzés létrehozójától, és nem pedig a képen szereplő egyén beállításaitól függ. A közösségimédia-oldalak tehát a képmás feletti rendelkezési jogosultságot elsősorban nem a képen szereplő egyén, hanem a képet megosztó számára biztosítják. Így arra a következtetésre jutottam, hogy a közösségimédia-oldalaknak a képmás felhasználásához való hozzáállása szöges ellentétben áll a képmáshoz való jog kétoldalú védelmével, amelynek értelmében mindenki jogosult eldönteni, hogy a róla készült felvétel milyen módon kerüljön felhasználásra, és senki nem kötelezhető annak tűrésére, hogy a róla készült felvételt az általa kívánttól eltérő nyilvánosság előtt tárják fel.

Másodrésről a fényképek közösségimédia-oldalakon való felhasználása tipikus eseteinek vizsgálata arra is rámutatott, hogy főszabály szerint bárki bárkiről – tekintet nélkül arra, hogy az illető Facebook-felhasználó-e, vagy sem, illetve a megosztó ismerőse-e, vagy sem – tölthet fel képet, azon bárkit megjelölhet, és ezek közül egyikhez sem kell az érintett hozzájárulása. Ezen megállapításom tovább erősítette azt a következtetésemet, miszerint a képmáshoz való jog közösségi médiában való sérelmének elsődleges oka abban keresendő, hogy e platformok működési elvei nem állnak összhangban a képmáshoz való jogra vonatkozó bírói gyakorlat alapvető elvárásaival.

Harmadrészről, bár eddig még nem született olyan magyarországi bírósági ítélet, amely a deepfake-felvételek jogi vonatkozását vizsgálná, a jelenlegi ítélkezési gyakorlat analógia útján történő alkalmazása útján azt is bebizonyítottam, hogy a deepfake-felvételek a képmáshoz való jog védelme alá tartoznak. Monográfiámban a képmáshoz való jog deepfake útján való megsértésének két esetét különböztettem meg:

Egy már meglévő képnek az érintett hozzájárulása nélkül való felhasználása a deepfake-felvételt létrehozó mesterséges intelligencia tanítása – és ezzel végső soron egy teljesen új, az eredetitől különböző (deepfake) felvétel elkészítése – céljából sérti a Ptk. 2:48. § (1) bekezdésében foglalt célhoz kötöttségét a képmás felhasználásához szükséges engedélynek.

- Egy már meglévő kép meghamisítása a Ptk. 2:42 §-át, valamint a Ptk. 2:48 §-át is sérti a fényképek torzításával/montírozásával kapcsolatban elfogadott joggyakorlat szerint.
- A képmáshoz való jog deepfake útján történő megsértésének két esetét érdemes elkülöníteni: (i) egy már meglévő kép deepfake elkészítése céljából való felhasználása; és (ii) az eredeti kép meghamisítása.

Utóbbival kapcsolatban azonban arra is rávilágítottam, hogy a közszereplőket megillető képmáshoz való jog nem abszolút, így a róluk készült felvétel bizonyos esetekben módo-

sítható, torzítható, sőt akár hamisítható is. Ebből azonban arra a követeltetésre jutottam, hogy csak azért, mert a deepfake természeténél fogva hamis, nem feltétlenül jelenti azt, hogy az mind jogellenes is, és nem védi a véleménynyilvánítás szabadsága.

Annak megállapítása érdekében, hogy a deepfake-felvételek mikor részesülhetnek a véleménynyilvánítás szabadságának védelmében, monográfiámban részletesen vizsgáltam az AB joggyakorlatát. Ennek értelmében a deepfake kizárólag abban az esetben részesülhet(ne) alkotmányjogi védelemben, ha az hamis információn alapuló véleménynek – és nem pedig hamis tényállításnak – minősül. Noha rámutattam, hogy a deepfake a tényállítás és véleménynyilvánítás között helyezkedik el, végezetül amellett foglaltam állást, hogy főszabály szerint a deepfake inkább tekintendő hamis tényállításnak, mintsem véleménynek. A deepfake ugyanis természetéből adódóan meggyőzően kelti azt a látszatot, hogy a meghamisított tartalom valójában megtörtént. A deepfake-nek a hitelesség ilyen magasfokú imitálására való képességéből azonban az is következik, hogy egy átlagos befogadó az esetek többségében a deepfake-et már nem véleményként, hanem szó szerint, tényállításként fogja értelmezni.

11.1.2. A jelenlegi platformszabályozás alkalmatlan hatékony jogorvoslat biztosítására a képmáshoz való jogában megsértett egyén számára

Monográfiám második felében arra a következtetésre jutottam, hogy annak, akinek képmáshoz való jogát az interneten megsértették, nem áll hatékony jogi védelem a rendelkezésére.

Egyrészt a szerzők és a képmáshoz való jogot sértő tartalmak megosztóinak felelőségre vonása számos okból kifolyólag nem egy valós alternatíva. A sértettnek ugyanis, mielőtt érdemben bármilyen jogi igényt érvényesíthetne a szerzővel szemben, legalább az alábbi akadályokkal kell megküzdenie: (i) az alperes azonosításának problematikája (anonimitás); (ii) több potenciális szerző/megosztó/jogsértő létezése; (iii) a több ország joghatóságának összeütközése és a kollíziós jog problémája; és (iv) az a kihívás, hogy ha egy illegális tartalom egyszer már felkerült az internetre, akkor szinte lehetetlen azt véglegesen eltávolítani.

Másodrészt a platformok nyilvánosság felé közvetített jogellenes tartalomért való felelősségét szabályozó DSA szintén nem biztosít hatékony jogorvoslatot a képmáshoz való jogában sértett számára. Ezen következtetésemet az alábbi megállapításaimra alapítottam:

- A platform fogalma több szempontból is téves, önellentmondó, és nem tükrözi az alapul fekvő technológia valódi adottságait. Például a platform definíciójának meghatározó eleme, hogy a szolgáltató funkciója nem csupán az információk tárolására, hanem az azon tárolt információk széles és meghatározatlan számú (valójában potenciálisan korlátlan számú) közönség számára való hozzáférhetővé tételére is kiterjed. A DSA alapján tehát nem tekinthető platformnak az a tárhelyszolgáltató, amely az általa tárolt információhoz való hozzáférést regisztrációhoz vagy a szolgáltatás igénybe vevőinek egy csoportjához való csatlakozáshoz köti, feltéve, hogy az nem automatikusan történik. Ahogyan arra rámutattam, ez azonban azt is jelenti, hogy a Facebook privát csoportjai vagy a Reddit privát oldalai (subreddit) nem minősülnek platformoknak tekintettel arra, hogy azok (i) csak korlátozott számú

felhasználó számára hozzáférhetőek, és (ii) a belépés a csoport házigazdájának vagy szervezőjének döntésétől függ. Ezzel szemben azonban a Facebookot az EB az elsők között minősítette online óriásplatformnak, anélkül, hogy a privát Facebook-csoportok jogi helyzetéről rendelkezett volna.

- A DSA továbbá nem foglal egyértelműen állást abban a tekintetben, hogy a DSA mely felelősségi alakzata alkalmazandó az olyan közvetítő szolgáltatókra, amelyek többféle közvetítő szolgáltatást kombinálnak egyidejűleg, azaz hibrid közvetítő szolgáltatóknak tekinthetők. Például a Facebook egyrészt a felhasználók által generált tartalmakat tárol, ami alapján tárhelyszolgáltatónak minősül, másrészt viszont a Facebook integrált részét képező Facebook Messenger *mere conduit* szolgáltatás, hiszen csak megkönnyíti a kommunikációs hálózathoz való hozzáférést a felhasználók számára. Amellett foglaltam állást, hogy az ilyen hibrid közvetítőket funkcióink szerint kell értékelni. Így amikor a jogalkalmazónak arra a kérdésre kell válaszolnia, hogy a Facebook felelősségre vonható-e a felhasználó által az idővonalán megosztott jogellenes tartalomért, úgy a jogalkalmazónak a DSA 6. cikkére kell támaszkodnia. Ezzel szemben amennyiben a Facebook felelőssége a Facebook Messengeren keresztül elküldött jogsértő tartalom vonatkozásában merül fel, úgy a jogalkalmazónak a Facebook felelősségét a DSA 4. cikke alapján kell megállapítania. Mindebből azonban az is következik, hogy a hibrid szolgáltatások nem tartozhatnak kizárólagosan a közvetítő szolgáltatók egyetlen alkategóriájába. Ezzel szemben az EB-nek a Facebookot óriásplatformként kijelölő határozatában figyelmen kívül hagyta a Facebook azon jellemzőit, amelyek nem minősülnek nyilvános terjesztésnek (pl. tartalom megosztása privát csoportban), vagy amelyek egyáltalán nem tartoznak a tárhelyszolgáltatás körébe (pl. Facebook Messenger). Ebből azonban két alternatív következtetés vonható le: (i) a DSA felhagyott azzal a megközelítéssel, hogy egy hibrid szolgáltató felelőssége az alapján állapítható meg mely funkciója érintett az adott jogvitában, vagy (ii) az EB már megkezdte a platform DSA szerinti definíciójának kiterjesztő értelmezését azáltal, hogy abba már nem csupán a kizárólagosan tárhelyszolgáltatást nyújtó közvetítő szolgáltatók, hanem azon szolgáltatók is beletartoznak, amelyek csak részben nyújtanak tárhelyszolgáltatást (feltéve, hogy a tárhelyszolgáltatás nem egy másik szolgáltatás kisebb jelentőségű és pusztán kiegészítő eleme vagy a főszolgáltatás kisebb jelentőségű funkciója).
- Álláspontom szerint a DSA teljes mértékben félreértette a közösségimédia-oldalak tartalom terjesztésében betöltött szerepét. A platformok definíciója értelmében passzív szerepet töltenek be a rajtuk elhelyezett tartalom tárolásában és nyilvánosság felé való terjesztésében. Ezen megközelítés az EUB-nek azon a – Google France és a Google, valamint a YouTube-ügyekben megállapított – téves feltételezésén alapul, hogy az érintett tartalom automatizált kezelése, az algoritmus általános alkalmazása a tárhelyszolgáltató semleges szerepét vonja maga után. Monográfiámban azonban amellett foglaltam állást, hogy a platformoknak a tartalom terjesztésében betöltött szerepe igenis aktív, még akkor is, ha a platformok az algoritmusait automatizált módon alkalmazzák valamennyi felhasználó által generált tartalomra. A semleges platformok koncepciója véleményem szerint inkább egyfajta mítosz, ugyanis a platformok a kollektív kreativitás ‘pártfogóiként’ működnek. Felkérlek,

sőt ösztönzik felhasználóikat, hogy vegyenek részt a tartalom létrehozásában, és ezáltal meghatározzák a kreatív tartalom előállításának feltételeit. Ezen következtetésemet az alábbi megállapításaim alapján vontam le:

- = A tartalom moderálására használt algoritmusok a platformok beléjük kódolt értékeit képviselik, ezért az ilyen algoritmusok által vizsgált minden egyes poszt a platformok jóváhagyását vagy elutasítását tükrözi.
- = A platformoknak anyagi érdeke is fűződik ahhoz, hogy az algoritmusaik olyan tartalmakat válasszanak ki és ajánljanak, amelyek megfelelnek a felhasználók érdeklődési körének, amelyek népszerűek más felhasználók körében, és/vagy amelyek több interakciót generálnak a felhasználók között, így növelve a megtekintések számát, a felhasználói figyelmet és ezáltal (óhatatlanul) a közösségi hálózatok reklámbevételét. Minél magasabb ugyanis az adott tartalom megtekintésének száma, annál magasabb összeg kérhető a tartalomhoz fűződő reklámhely hirdetésárverés keretében való értékesítése során. Mivel azonban az álhírek és a deepfake a közösségi médiában a legszélesebb körben megosztott tartalmak közé tartoznak, a platformoknak így jelentős pénzügyi érdekeltsége van azok terjesztésében.
- = A platformok tartalomoptimalizálásának eredményeként információs buborékok jönnek létre, amelyek korlátozzák a felhasználók szólásszabadságát. A platformok algoritmusai a reklámbevételek maximalizálása érdekében elsősorban olyan tartalmak megjelenítésére törekednek, amelyeket az adott felhasználó számára relevánsnak ítélnék. Ez a szelekciós mechanizmus szükségszerűen egy olyan öngerjesztő folyamatot indít el, amely fokozatosan izolálja a felhasználót más, a platformon elérhető és más felhasználók számára közvetített tartalmaktól, még mielőtt a felhasználó e korlátozás tényét tudatosítaná. Azt is bizonyítottam, hogy a platformok ajánlórendszerei nem csak információs buborékba zárják be a felhasználókat, hanem folyamatosan megerősítik azt az elképzelést, amelyre a buborék eredetileg épült. Ennek eredményeként úgy nevezett visszhangkamrák alakulnak ki, amelyek lényegében különálló univerzumok: egymás létezéséről szinte nem is tudva, párhuzamosan léteznek egymás mellett. Amint azt a korábbi fejezetekben részletesen kifejtettem, az algoritmusok által így létrehozott információs buborékok, illetve visszhangkamrák szükségképpen a felhasználók azon alapvető jogának sérelméhez vezetnek, amely szerint az egyén jogosult mindenféle információt és eszmét szabadon, határok nélkül megismerni.
- A DSA a tartalommoderálással összefüggésben megfogalmazott rendelkezései (különösen a bejelentési és cselekvési mechanizmus), valamint a DSA platformok felelősségére vonatkozó szabályai közötti joghézag miatt a lehetséges jogi vagy reputációs következmények elkerülése érdekében a platformok hajlamosak a kétséges megítélésű tartalmak eltávolítása mellett dönteni. Ennek oka, hogy a DSA 16. cikk (3) bekezdése értelmében a bejelentés a platform felelősségét megalapozó, a jogellenes tartalomról való tényleges tudomásszerzéshez vezet, amennyiben a bejelentés elegendő specifikus információt tartalmaz ahhoz, hogy a platform részletes jogi értékelés nélkül dönthessen a bejelentett tartalom jogellenes voltáról. A DSA 16. cikk (3) bekezdése azonban kifejezetten a bejelentés tartalmára vonatkozó követelményeket állapít meg, nem pedig a bejelentett tartalom egyértelmű jogellenességének

bizonyítására vonatkozó érdemi kötelezettséget ír elő. A DSA tehát a felelősség megállapításához nem írja elő, hogy a tartalom jogellenességének azonnal nyilvánvalónak kell lennie; inkább azt követeli meg, hogy a bejelentő kellően részletes információkat szolgáltatson ahhoz, hogy a tárhelyszolgáltató azt meg tudja állapítani. Ahogyan azonban azt bemutattam, vannak olyan esetek is, amikor a tartalom nem egyértelműen jogellenes, és azt még egy kellően részletezett bejelentés sem tudja orvosolni. Tökéletes példa erre a monográfiámban használt ügy, azaz maga a 'nyomkövetőt viselő' Hillary Clintonról készült fotó. Kétségtelen, hogy a fotó hamisítvány volt. Azonban az, hogy egy kép hamisítvány, nem jelenti automatikusan azt, hogy jogellenes, és azt sem, hogy nyilvánvalóan jogellenes. Mivel azonban a DSA nem egyértelmű a tekintetben, hogy ilyen esetekben a bejelentés megalapozza-e a platform tényleges tudását és így a felelősségét, a platformok inkább eltávolítják a bejelentett tartalmakat, mint hogy a jogi felelősségük megállapítását kockáztassák.

- Miután monográfiámban levontam azt a következtetést, hogy a platformok a tartalom terjesztésében betöltött aktív szerepük ellenére csak szűk körben vonhatók felelősségre a DSA alapján az általuk tárolt jogellenes tartalomért, és így a DSA felelősségi rendszere nem rendezi a platformok által létrehozott információs buborékokat és visszhangkamrákat, végezetül azt is megállapítottam, hogy a DSA által előírt kellő gondossági kötelezettségek sem nyújtanak hatékony védelmet a felhasználók számára az algoritmusok ezen negatív hatásával szemben.
- = Egyrészt, a DSA 27. cikke által platformokkal szemben előírt átláthatósági kötelezettség nemcsak, hogy elégtelen, hanem annak tartalma és hatálya sem egyértelmű. A DSA 27. cikke értelmében a platformoknak el kell magyarázniuk (i) az ajánlórendszerükben használt fő paramétereket és (ii) az e fő paraméterek módosításának vagy befolyásolásának lehetőségét és módszerét. A DSA azonban nem határozza meg, hogy pontosan mik volnának a főbb paraméterek. A DSA 27. cikkének célja tehát nem az ajánlórendszerek használatának korlátozása vagy tiltása, hanem az átláthatóság előmozdítása, ami lehetővé teszi a felhasználók számára, hogy megértsék, hogyan befolyásolják az ilyen rendszerek az információk megjelenítését.
- = Másrészt, a DSA 38. cikke által a felhasználók számára biztosított jogosultság hatálya túl szűk. A DSA 38. cikke, amely lehetővé teszi a felhasználók számára, hogy az online óriásplatformok profilozáson alapuló ajánlási rendszeriből kilépjenek, pusztán egy *opt-out* és nem egy *opt-in* jogosultságot biztosít a felhasználók számára. A DSA ugyanis még az óriásplatformokat sem kötelezi arra, hogy alapértelmezett beállításként a profilalkotás nélküli alternatívát alkalmazzák, vagy hogy egyes tartalmak tekintetében a profilozáson alapuló ajánlórendszereket egyáltalán ne alkalmazzák. Ahogyan arra részletesen kitértem, a DSA 38. cikke által előírt gondossági kötelezettség továbbá könnyen kontraproduktívá válhat: az óriásplatformok által preferált alternatív megoldások (például kronologikus vagy betűrendes elrendezés) ugyanis olyan felületet eredményezhetnek, amely nem praktikus vagy nehezen navigálható, elriasztva így a felhasználókat attól, hogy a nem személyre szabott ajánlásokat válasszák.

11.2. Javaslattétel egy hatékonyabb platformszabályozásra

A fentebb leírtakból következik, hogy az integrált szabályozás elmélete nem alkalmas és nem is képes az interneten keletkező jogviszonyokat rendezni. Ha azonban egy szabályozás nem teszi lehetővé önmagunk, érdekeink, jó hírünk, nevünk, tisztességünk, képmásunk védelmét, úgy az a szabályozás nem csupán hatástalan, de – Verebics János szavaival élve – „érvénytelen” is.¹ Jogosan merülhet fel tehát a kérdés, hogy vajon a platformszabályozásnak milyen alternatív módja tenné lehetővé, hogy:

- a képmáshoz való jog az interneten megfelelően érvényesüljön,
- a képmáshoz való jogában megsértett egyén hatékony védelemben részesüljön mások véleménynyilvánításához való jogának szükségtelen és aránytalan korlátozása nélkül, és
- a felhasználók az ajánlórendszerek által kialakított információs buborékok és visszahangkamrák negatív hatásaival szemben hatékony védelemben részesüljenek.

Monográfiám utolsó fejezetében – mintegy keretes szerkezetbe foglalva a könyv elején bemutatott szabályozási megoldásokat – erre a kérdésre igyekszem választ adni. Fontosnak tartom azonban leszögezni, hogy e problémára jelen pillanatban az egész világon nincsen jó megoldás, csak versengő javaslatok. Annak érdekében, hogy megválaszolható legyen a kérdés, miként lehetne a platformokat hatékonyabban szabályozni, mindenekelőtt szükséges beazonosítani azokat a problémákat, amelyek a jelenlegi szabályozás hatástalanságához vezetnek. Monográfiámban a hatályos szabályozás alábbi hiányosságait azonosítottam.

Egyrészt a jelenlegi platformszabályozás – így a DSA is – az úgynevezett utasításon és ellenőrzésen alapuló szabályozási stratégián (*command and control*) alapul. E szabályozási megközelítés az egyén jogkövető magatartását részletes jogszabályi rendelkezésekkel és azok megszegéséért kiszabható szankciókkal kívánja kikényszeríteni, így az a jogkövetkezményektől való félelmen és nem a jogkövetésre való ösztönzésen alapul. Ahogyan azonban azt a #Pizzagate összeesküvés-elmélet elemzése során láthattuk, ez a többértelmű, tág jogszabályi rendelkezések alkotta környezet könnyen ahhoz vezethet, hogy az érintett személy, szerv inkább a szigorúbb jogértelmezést választja az esetleges szankciók elkerülésének reményében, függetlenül attól, hogy annak milyen további következményei lehetnek másokra nézve. A DSA platformokra vonatkozó felelősségi rendszerének vizsgálata során például láthattuk, hogy a platformok a potenciális jogi felelősség elkerülése érdekében gyakran inkább a nem egyértelműen jogsértő tartalmak eltávolítása mellett döntenek, ami azonban az esetek többségében más felhasználók szólásszabadságának szükségtelen és aránytalan korlátozásához vezethet.

Másrészt, a DSA egyes rendelkezéseinek gyakorlatban való alkalmazása arra is rámutatott, hogy a jelenleg hatályos platformszabályozás nem igazán értette meg az általa szabályozni kívánt területet, illetve technológiát. Gondoljunk például csak arra, hogy a DSA alapján a platformok definíciójuk szerint passzív szerepet töltenek be az általuk tárolt tartalom nyilvánosság felé történő terjesztésében annak ellenére, hogy a gyakorlatban a platformok szerepe nagyon is aktív. Másik kiváló példa, hogy a DSA a platformokat a tárhelyszolgáltatók egy speciális kategóriájaként határozza meg, míg a gyakorlatban a platformok ritkán nyújtanak kizárólagosan tárhelyszolgáltatói tevékenységet.

¹ VEREBICS (1998): 44.

Harmadrésről a monográfiámban több példán keresztül azt is szemléltettem, hogy a probléma sok esetben nem a jogszabály szövegezésében rejlik, hanem maga a technológia, illetve annak kialakítása nem teszi lehetővé a jog érvényesülését. Láthattuk például, hogy a képmáshoz való jog az interneten azért nem tud megfelelően érvényesülni, mert a közösségi-média-oldalak nem a képmáshoz való jog elvei alapján alakították ki a felületüket. Hasonlóan a deepfake-felvételek – az alapul fekvő technológia gyors fejlődésen túl – azért képesek mára már a befogadók felét megtéveszteni, mert azokon semmi nem jelzi a képek, videók hamis jellegét.

Ezen hiányosságok kiküszöbölése érdekében véleményem szerint a *command and control* szabályozási megközelítés helyett érdemesebb lenne a platformokat egy koregulációs modell keretében szabályozni, amelyben az állam jogszabályokon keresztül történő szabályozása és a platformokat működtető technológiai cégek önszabályozása keverednének. A szabályozás alapja tehát a jogalkotó/jogalkalmazó és a jogszabály alanya közötti együttműködés, állandó kommunikáció és a kölcsönös bizalom lenne. A jogkövetést a hatóságok jogértelmezési gyakorlatát tükröző publikációk, valamint a jogszabályértelmezéssel kapcsolatos megkeresésekre adott hivatalos válaszok segítenék. A jogkövetés iránti bizalom növelése érdekében célszerű lenne továbbá, ha a hatóságok eljárásaik során előnyben részesítenék a jogkövetési szint emelésére tett ajánlásokat, illetve az érintett szervezetek vagy személyek által önként tett kötelezettségvállalásokat a szankcionálással, különösen a bírságok kiszabásával szemben.

Ezen koregulációs modellen belül a jogi szabályozásnak az elvi alapú szabályozási megközelítést (*principles-based regulation*) kellene alkalmaznia. A jogszabályoknak tehát elsősorban a szabályozással elérni kívánt célokat, értékeket és követendő elveket kellene meghatározniuk, míg a jogalanyok e normatív kereteken belül önállóan alakíthatnák ki a jogszabályoknak való megfelelésük módját. Ezen elvi alapú szabályozás tehát nem részletszabályok megalkotásán és betartatásán alapulna, hanem a jogszabály alanyai számára biztosított autonómián, amely lehetővé tenné az előírt elveknek és értékrendnek megfelelő, a releváns kockázatokat hatékonyan kezelő, egyénre szabott megoldások kialakítását. A koregulációs modellen belül az önszabályozás elsősorban magatartási kódexek elfogadása útján valósulna meg, amelyek a technológiai cégek által magukra nézve kötelezőnek elismert normákat, sajátos szankciókat és vitarendezési formákat tartalmaznának.²

Álláspontom szerint egy ilyen koregulációs modell az alábbi főbb előnyökkel járna:

- a jogszabályok képesek lennének a folyamatosan és gyorsan változó technológiai fejlődéssel lépést tartani, mivel azok elsősorban elveket, és nem részletszabályokat fogalmaznának meg;
- a magatartások részletes szabályozása az adott technológiát értő és részleteiben ismerő személyek, technológiai cégek kezében maradna;
- az adott szervezetek a jogkövető magatartásukat a saját működésük, felépítésük, és szolgáltatásuk tükrében tudnák kialakítani, megkönnyítve így a globális cégek jogkövetését; és

² Ennek alátámasztására lehet példaként említeni, hogy mind a dezinformációra vonatkozó uniós gyakorlati kódex, mind pedig a jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódex szabályait beépítették a DSA keretrendszerébe 2025-ben.

- a hatóságok jogértelmezési gyakorlatát tükröző publikációk, illetve az eljárásaik során a cégekkel való együttműködés bírsággal szemben való prioritizálása a tág jogszabályi rendelkezések helytelen értelmezésből fakadó következményeket is hatékonyan orvosolná.

A platformok tartalommoderálási gyakorlatának részletes ismertetése során láthattuk, hogy a platformok fontos szerepet játszanak a felhasználók véleménynyilvánításhoz való jogának, valamint más alapvető jogoknak az érvényesülésében. A 10. fejezet azonban arra is rávilágított, hogy a platformoknak anyagi érdeke fűződik a társadalmat megosztó tartalmak terjesztéséhez, illetve a felhasználók információs buborékokba zárásához. Ezen pénzügyi érdekeltségre tekintettel véleményem szerint a platformoknak nem lenne szabad meghatározó szerepet betölteniük az alapvető jogok, különösen a véleménynyilvánítás szabadsága és más alapjogok közötti mérlegelésben és azok érvényesítésében.³ E szerep átvállalása érdekében létre kellene hozni egy olyan hatóságot (vagy a DSA 21. cikk által már amúgy is létrehozott bíróságon kívüli vitarendezési fórumokat kellene korlátozott hatósági jogkörrel felruházni), amely panaszhelyként működne, és ahova a felhasználó illegális tartalom észlelése esetén bejelentéssel fordulhatna. Az interneten megtalálható adatmennyiség nagyságára tekintettel az illegális tartalom felderítésére ugyanis csak akkor kerülhet sor, ha a szabályozás a felhasználókat közreműködésre ösztönzi, és a panasz benyújtására egy egyszerű és gyors eljárást biztosít.

Felmerülhet a kérdés, hogy vajon mi történik azután, hogy a felhasználó panasszal fordult a hatósághoz.⁴ Abban az esetben, ha a hatóság a panaszt nyilvánvalóan alaptalanak találja, a panaszt elutasítja és benyújtót pénzbírsággal sújtja. Akkor, ha a panasz nem nyilvánvalóan alaptalan, és a hatóság jogsértést állapít meg, a szolgáltatót a tartalom törlésére, a megosztó erről való tájékoztatására és a platformon található további, azonos jogsértő tartalom eltávolítására és azonos tartalom feltöltésének megakadályozására kötelezi. Ha a megosztó a tartalom törlését sérelmezi, a tartalom jogszerűségének megállapítása végett meghatározott határidőn belül rendes bírósághoz vagy választottbírósághoz fordulhat, amiről a panaszt benyújtó felet a hatóság értesíti. Az eljárás eredménye alapján a hatóság a szolgáltatót a tartalom visszahelyezésére, és a panaszt benyújtó felet kártérítésre kötelezheti.

Ezen eljárásnak az az előnye, hogy gyors, és az esetlegesen jogellenes tartalommal szemben kellően agresszív. További előny, hogy a szolgáltatót mentesíti a jogsértő tartalomért való felelősség alól, és ezzel egyidejűleg nem kényszeríti a szolgáltatót arra, hogy a tartalom jogellenességéről önkényesen, szakértelem hiányában döntsön. Az eljárással szemben jogos kritikaként merülhet fel, hogy aránytalanul korlátozza a személy szólásszabadságát,

³ Ezen álláspontomat erősíti meg a 2025. augusztus 8. napján hatályba lépett 2024/1083 EU rendelet 18. cikk (4) bekezdése, amely akként rendelkezik, hogy az online óriásplatformok a klasszikus médiaszolgáltatók által szolgáltatott tartalmakat csak sokkal szigorúbb szabályok mellett, szűk körben távolíthatják el. Az Európai Parlament és a Tanács (EU) 2024/1083 rendelete (2024. április 11.) a belső piaci médiaszolgáltatások közös keretének létrehozásáról és a 2010/13/EU irányelv módosításáról (a tömegtájékoztatás szabadságáról szóló európai rendelet), PE/4/2024/REV/1, HL L 2024/1083, 2024.4.17.

⁴ A válaszként lentebb ismertetett eljárás Richard Clayton 4R (*report, remove, respond, replace*) néven ismerté vált eljárásán és saját ötleteimen alapszik. Richard Clayton a 4R nevű eljárását a *Judge and jury? How “notice and take down” gives ISPs an unwanted role in applying the law to the internet* című tanulmányában fejtette ki. https://www.cl.cam.ac.uk/~rnc1/Judge_and_Jury.pdf

hiszen a tartalom már annak potenciális jogsértő jellege esetén is törlésre kerül. Úgy vélem azonban, hogy ha a megosztó nem tiltakozik a tartalom törlése ellen, az azt sugallja, hogy az nem is volt számára fontos, és így a spontán közlését nem kívánja alkotmányos védelemben részesíteni.

Véleményem szerint szükséges lenne továbbá egy az internetes szereplők érdekcsoportjait (pl. tartalomszolgáltatókat, felhasználókat stb.) tömörítő önszabályozó testület kialakítása. Az önszabályozó testület demokratikus elvek alapján működő, az állami szervekkel kooperáló civil szervezet lenne, amely például a magatartási kódexek szakértői munkacsoportok közreműködésével, demokratikus döntéshozatal keretében történő megalkotásával foglalkozna.⁵ Az önszabályozó testület komoly szerepet vállalna továbbá a felhasználók internettel kapcsolatos oktatásában és felvilágosításában, ahol a tájékoztatásnak egyrésről a felhasználók és szolgáltatók jogaira, kötelezettségeire, másrésről pedig a szolgáltatásból eredő veszélyekre és a rendelkezésre álló védelmi lehetőségekre kell kiterjednie.

A fentebb ismertetett javaslatok azonban csak arra adnak választ, hogy a jog miként tudná hatékonyabban szabályozni a platformokat. Arra is rámutattam azonban, hogy sokszor maga a technológia kialakítása nem teszi lehetővé a jog érvényesülését. Ebből azonban – véleményem szerint – az is következik, hogy a platformszabályozásnak nem csupán jogi eszközökre, hanem Lawrence Lessig szabályozási modellje szerinti egyéb szabályozási formákra (társadalmi normák, fizikai környezet, piaci mechanizmusok) is támaszkodnia kellene. Tekintettel arra, hogy a felhasználók képtelenek figyelmen kívül hagyni az online architektúra (kódolás) által meghatározott működési kereteket, álláspontom szerint a platformszabályozást a jog mellett elsősorban a technológiai architektúra és annak kialakítása révén kellene megvalósítani. Ezzel összefüggésben azonban arra is emlékeznünk kell, hogy nem létezik semleges architektúra, vagyis olyan fizikai környezet, amely semmilyen módon nem befolyásolja a felhasználó viselkedését és döntéseit. Mivel azonban egy semleges – Thaler és Sunstein korábban ismertetett kifejezését felhasználva *‘anti-nudge’* – környezet kialakítása lehetetlen, így a jogalkotónak a platformszabályozás során valójában arra a kérdésre kell választ találnia, hogy az internetet mint fizikai környezetet milyen értékek szerint kell felépíteni. Ezen fizikai környezet által tükröződő értékeket pedig a fent említett elvi alapú szabályozáson alapuló jogszabályok határoznák meg.

De vajon mit is jelent ez a gyakorlatban? Vegyük például a platformszabályozás, azon belül is az információs buborékok kérdését. Véleményem szerint a megoldás alapját az képezné, ha a jogalkotó a platformokat a sokszínűség melletti *nudge*-olásra (*nudge for diversity*) kötelezné – létrehozva így John Stuart Mill által elképzelt vélemények piacát.⁶ A platformoknak – mint az online környezet megalkotóinak – tehát társadalmi felelősséget kellene vállalniuk, és választási architektúrájukat Thaler és Sunstein elveinek megfelelően kellene újratervezniük. Azaz, ezen megújított környezeteknek különböző módokon elő kellene segíteniük a nézőpontbéli sokszínűséget, miközben átláthatóak maradnak és megőrzik a felhasználók szabadságát. A környezet felépítését vezérlő elveknek nem csupán egyértelműnek

⁵ SVANTESSON (2020)

⁶ John Stuart Mill szólásszabadsággal kapcsolatban kialakított elméletének alapja az volt, hogy egy vélemény sem értékesebb a másiknál, és így egyik sem érvényesülhet kizárólagosan. Mill szerint az objektív igazság kizárólag az egymásnak ellentmondó vélemények együttes létezésével és ‘belső küzdelmével’ érhető el (MILL [1859]).

kellene lenniük a felhasználók számára, de a felhasználóknak lehetőséget kellene kapniuk arra is, hogy a környezet által ösztönzött választástól eltérő döntést hozhassanak.

Fontosnak tartom hangsúlyozni, hogy álláspontom szerint a társadalmat megosztó, káros – ugyanakkor nem jogellenes – tartalmakkal szembeni hatékony fellépés nem a tartalom szűrésében, hanem az azokat cáfoló vagy megkérdőjelező nézőpontok azonos súlyal történő, mindenki számára hozzáférhető megjelenítésében rejlik. Lessighez hasonlóan úgy gondolom, hogy a szólásszabadság súlyos veszélyeztetésével járna az értékelő- és szűrőrendszerek alkalmazásával megvalósuló tartalomszűrés. E rendszerek alapja ugyanis a PICS technológia, amelynek értelmében a felcímkézett oldalakat a böngészőprogramok és más szoftverek képesek felismerni és a minősítésük alapján megszüntetni. Ezen szűrőprogramok használatából azonban számos probléma adódik, különösen a következők:

- a rendszer nem ismer korlátokat a szűrt vagy szűrhető anyagok skáláján;
- olcsó központi, állami szűrést tesz lehetővé, anélkül, hogy azt a felhasználó érzékelhetné;⁷
- a rendszer hatékony működéséhez minden oldalt minősíteni kell, ellenkező esetben bizonyos tartalmak hozzáférhetetlenné válnak;
- a rendszer semleges, vagyis beállítástól függően nem feltétlenül csak a káros, hanem például a szélsőséges politikai vagy vallási tartalmakat is kiszűri.

Lessig modellje értelmében az információs buborékok felszámolása érdekében igénybe vehető harmadik szabályozási eszköz a piaci erő. E tekintetben álláspontom szerint a legfontosabb lépést a személyre szabás mögötti gazdasági ösztönzés megszüntetése jelentené.⁸ További megoldást jelenthetne például a hirdetésárverések állami szabályozása, vagy a kattintásalapú díjszabásról a fix díjakra való áttérés, aminek következtében a platformoknak már jóval kevésbé állna érdekében a felhasználókat információs buborékokba zárni.

Végezetül annak érdekében, hogy a felhasználó egyáltalán felismerje, hogy egy információs buborékban van, szükséges lenne a társadalom médiaműveltségének, illetve kritikus gondolkodásának növelése. Médiaműveltségen azon ismeretek és készségek összességét értem, amelyek lehetővé teszik az egyén számára a médiakörnyezet tudatos, értő és aktív használatát. Egyetértek Nagy Krisztinával abban, hogy e képességek felvértezik az egyént a kibertérben rejlő kockázatokkal és veszélyekkel szembeni védekezésre, valamint alkalmassá teszik arra, hogy az információs és médiakörnyezetet tanulásra, munkavégzésre, önkifejezésre, illetve a társadalmi életben való aktív részvételre is használja.⁹ A médiaműveltség fejlesztésének számos lehetséges eszköze létezik, ideértve a médiahasználat, az internethasználat, kapcsolatos ismeretek beépítését az alaptantervbe, a társadalom médiaműveltségi szintjének rendszeres felmérését, valamint az internetet és más médiumokat vizsgáló kutatók intézményes támogatását.

A fenti jogi és jogon kívüli eszközök komplex használatával álláspontom szerint lehetséges volna, hogy a bemutatott fiktív jogeset kapcsán az európai platformszabályozás valódi védelmet kínáljon a képmáshoz való jogukban megsértett érintettek számára.

⁷ A PICS-ben nincs semmi, ami előírná, hogy a felhasználóval tudatni kell azt a tényt, hogy a keresőgép szűrést alkalmaz.

⁸ Pontosan ezt ismerte fel a dezinformációra vonatkozó uniós gyakorlati kódex is, amely első számú kötelezettségvállalásként a dezinformáció terjesztéséhez fűződő pénzügyi érdek megszüntetését írta elő.

⁹ NAGY (2018): 228.

Források és irodalom

Irodalomjegyzék

- ABATE (2020) = Serafino ABATE: A Reflection On A Decade of Regulating Digital Platforms – Will 2021 be the Year of Internet Regulation Converging with Media and Telecoms Regulation? In: Emma WRIGHT (Ed.): *International Comparative Legal Guides. Telecoms, Media & Internet 2021* [14th Edition]. Global Legal Group, 2020, 1–3. https://www.acc.com/sites/default/files/resources/upload/TEL21_E-edition.pdf
- ALKIVIADOU (2024) = Natalie ALKIVIADOU: Platform liability, hate speech and the fundamental right to free speech. 34(2) *Information & Communications Technology Law* (2024), 207–217. <https://doi.org/10.1080/13600834.2024.2411799>
- ANGELOPOULOS–SMET (2016) = Christina ANGELOPOULOS – Stijn SMET: Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability. 8(2) *Journal of Media Law* (2016), 266–301. <https://doi.org/10.1080/17577632.2016.1240957>
- ANGYAL (2020) = ANGYAL Zoltán: Úton a digitális egységes piac felé. *Miskolci Jogi Szemle*, 2020/3. különszám, 5–13. https://www.mjsz.uni-miskolc.hu/files/13819/3_angyal_zoltan_t%C3%B6rdelt_jav.pdf
- BADOUARD (2020) = Romain BADOUARD: *Les nouvelles lois du web. Modération et censure*. Paris, Le Seuil, 2020. <http://www.doi.org/10.4000/quaderni.2049>
- BALDWIN–CAVE–LODGE (2012) = Robert BALDWIN – Martin CAVE – Martin LODGE: *Understanding Regulation: Theory, Strategy and Practice*. Oxford, Oxford Academic, 2012. <https://doi.org/10.1093/acprof:osobl/9780199576081.003.0014>
- BALENDRA (2024) = Soorya BALENDRA: *Free Speech in the Puzzle of Content Regulation*. Cham, Springer, 2024. https://doi.org/10.1007/978-3-031-75813-3_4
- BALKIN (2018) = Jack M. BALKIN: Szólásszabadság az algoritmos társadalomban. A big data, a magánszabályozás és a véleménynyilvánítás szabályozásának új iskolája. *In Medias Res*, 2018/2., 197–247.
- BARAN (1964) = Paul BARAN: Rand Memoranda on Distributed Communication. Santa Monica, The Rand Corporation, 1964. https://www.rand.org/pubs/research_memoranda/RM3420.html
- BARLOW (1996) = John Perry BARLOW: *A Declaration of the Independence of Cyberspace*. eff.org, 1996. <https://www.eff.org/cyberspace-independence>
- BARTÓKI–GÖNCZY (2018) = BARTÓKI–GÖNCZY Balázs: *Az online közvetítő szolgáltatók mint az információhoz való hozzáférés kapuőrei*. Pázmány Press, Budapest, 2018.

- BARTÓKI-GÖNCZY-POGÁCSÁS (2019) = BARTÓKI-GÖNCZY Balázs – POGÁCSÁS Anett: A médiatartalom-szolgáltatásnak nem minősülő internetes tartalomszolgáltatások szabályozása. In: KOLTAY András (szerk.): *Magyar és európai médiajog*. Budapest, Wolters Kluwer, 2019, 719–756.
- BAYER (2002) = BAYER Judit: Az internet tartalomszabályozása Magyarországon (Önszabályozás versus állami szabályozás). In: ENYEDI NAGY Mihály – POLYÁK Gábor – SARKADY Ildikó (szerk.): *Magyarország médiakönyve 2002*. Budapest, ENAMIKÉ, 2002.
- BENCZE-FICSOR (2020) = BENCZE Mátyás – FICSOR Krisztina: A koronavírus kihívásai és a jogtudomány: a rémhírterjesztés tényállásának jogalkalmazási kérdései. *JTI Blog*, 2020. április 2. <https://jog.tk.hu/blog/2020/04/a-remhirterjesztes-tenyallasanak-jog-alkalmazasi-kerdesei>
- BORONKAY (2013) = BORONKAY Miklós: A képmáshoz és a hangfelvételhez fűződő jog. In *Medias Res*, 2013/1., 111–132.
- BRAUN-EKLUND (2019) = Joshua A. BRAUN – Jessica L. EKLUND: Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism. 7(1) *Digital Journalism* (2019), 1–21. <https://doi.org/10.1080/21670811.2018.1556314>
- BUITEN (2021) = Miriam BUITEN: The Digital Services Act From Intermediary Liability to Platform Regulation. 12(5) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2021), 361–380. <https://www.jipitec.eu/jipitec/article/view/331/324>
- BUKOR-TRÄGER (2024) = BUKOR Liza – TRÄGER Anikó: Az online gyűlöletbeszéd detektálásának kérdései, különös tekintettel az algoritmikus rendszerekre. *MTA Law Working Papers* 2024/2., 1–14. <https://jog.tk.elte.hu/mtalwp/az-online-gyuloletbeszed-detektalasanak-kerdesei-kulonos-tekintettel-az-algoritmikus-rendszerekre>
- BUSCH (2024) = Christoph BUSCH: Platform regulation beyond DSA and DMA: Which role for the P2B Regulation? 12(2) *Journal of Antitrust Enforcement* (2024), 201–206. <https://doi.org/10.1093/jaenfo/jnae016>
- CHAKRAVORTI-TRACHTMAN (2025) = Bhaskar CHAKRAVORTI – Joel P. TRACHTMAN (Eds.): *Defeating Disinformation: Digital Platform Responsibility, Regulation and Content Moderation on the Global Technological Commons*. Cambridge, Cambridge University Press, 2025. <https://doi.org/10.1017/9781009438636>
- CLEGG (2023) = Nick CLEGG: New Features and Additional Transparency Measures as the Digital Services Act Comes Into Effect. *Meta*, 2023. augusztus 22. <https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect>
- COLE-ETTELDORF-ULLRICH (2021) = Mark D. COLE – Christina ETTELDORF – Carsten ULLRICH: *Updating the Rules for Online Content Dissemination. Legislative Options of the European Union and the Digital Services Act Proposal*. Baden-Baden, Nomos, 2021. <http://doi.org/10.5771/9783748925934>
- DAVIDSON (2009) = Alan DAVIDSON: *The Law of Electronic Commerce*. Cambridge, Cambridge University Press, 2009. <https://doi.org/10.1017/CBO9780511818400>

- DECAROLIS–LI (2023) = Francesco DECAROLIS – Muxin LI: Regulating online search in the EU: From the android case ot he Digital Markets Act and Digital Services Act. 90(különszám) *International Journal of Industrial Organization* (2023), 1–15. <https://doi.org/10.1016/j.ijindorg.2023.102983>
- DE NARDIS (2014) = Laura DE NARDIS: *The Global War for Internet Governance*. New Haven, Yale University Press, 2014. <https://doi.org/10.2307/j.ctt5vkz4n>
- DRINÓCZI (2021) = DRINÓCZI Tímea: Az Alkotmánybíróság határozata a különleges jogrend idején megvalósuló rémhírterjesztésről. *Jogesetek Magyarázata*, 2021/1., 3–13.
- DUH (2002) = Christine DUH: Yahoo! Inc. v. LICRA. 17(1) *Berkeley Technology Law Journal* (2002), 359–378. https://btlj.org/data/articles2015/vol17/17_1_AR/17-berkeley-tech-l-j-0359-0378.pdf
- EASTERBROOK (1996) = Frank H. EASTERBROOK: Cyberspace and the Law of Horse. 1996(1) *University of Chicago Legal Forum* (1996), 207–216. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles
- European Court of Human Rights Research Division (2015) = European Court of Human Rights Research Division: *Internet: case-law of the European Court of Human Rights*. Strasbourg, Európa Tanács, 2015. <https://www.refworld.org/jurisprudence/caselawcomp/echr/2011/83905>
- FIRNIKSZ (2021) = FIRNIKSZ Judit: Rangsorolás – Új szabályozási igény a platformok és az információs túlterheltség korában. In: VALENTINY Pál – ANTAL-POMÁZI Krisztina – BEREZVAI Zombor – NAGY Csongor István (szerk.): *Verseny és szabályozás 2021*. Budapest, MTA KRTK Közgazdaság-tudományi Intézet, 2021, 165–199.
- FLAXMAN–GOEL–RAO (2016) = Seth FLAXMAN – Sharad GOEL – Justin M. RAO: Filter Bubbles, Echo Chambers, and Online News Consumption. 80(S1) *Public Opinion Quarterly* (2016), 298–320. <https://doi.org/10.1093/poq/nfw006>
- G. KARÁCSONY (2022) = G. KARÁCSONY Gergely: „Ideje megváltoztatni” – Az arcfelismerő rendszerek alkalmazásának alapjogi kockázatai a közösségi média és a deepfake korában. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika, 2022, 299–317. https://doi.org/10.36250/01065_16
- GARRETT–RESNICK (2011) = Kelly R. GARRETT – Paul RESNICK: Resisting Political Fragmentation on the Internet. 140(4) *Daedalus* (2011), 108–120. https://doi.org/10.1162/DAED_a_00118
- GHOSH–SCOTT (2018) = Dipayan GHOSH – Ben SCOTT: *#Digitaldeceit. The Technologies Behind Precision Propaganda on the Internet*. Washington, New America, 2018. <https://d1y8sb8igg2f8e.cloudfront.net/documents/digital-deceit-final-v3.pdf>
- GILLESPIE (2010) = Tarleton GILLESPIE: The Politics of ‘platforms’. 12(3) *New Media and Society Volume* (2010), 347–364. <https://doi.org/10.1177/1461444809342738>
- GILLESPIE (2018) = Tarleton GILLESPIE: *Custodians of the Internet. Platforms, Content Moderation and the Hidden Decision that Shape Social Media*. New Haven, Yale University Press, 2018. <https://doi.org/10.12987/9780300235029>

- GODIOLI et al. (2025) = Alberto GODIOLI – Sabine JACQUES – Jennifer YOUNG – Ariadna MATAMOROS-FERNÁNDEZ: *What's in a Joke? Assessing Humor in Free Speech Jurisprudence*. New York, Columbia University, 2025. <http://www.doi.org/10.5281/zenodo.15383543>
- GOLDSMITH (1999) = Jack L. GOLDSMITH: Against Cyberanarchy. 1999(40) *University of Chicago Law Occasional Paper* (1999), 1199–1250. <https://doi.org/10.2307/1600262>
- GOLDSMITH–WU (2006) = Jack GOLDSMITH – Tim WU: *Who controls the internet? Illusion of the Borderless World*. New York, Oxford University Press, 2006. <https://doi.org/10.1093/oso/9780195152661.001.0001>
- GORWA (2024) = Robert GORWA: *The Politics of Platform Regulation. How Governments Shape Online Content Moderation*. Oxford, Oxford University Press, 2024. <http://doi.org/10.1093/oso/9780197692851.001.0001>
- GOSZTONYI (2021) = GOSZTONYI Gergely: Early Regulation of Social Media Liability Issues in the United States of America and the European Union. *Jogtörténeti Szemle*, 2021/5., 21–26.
- GOSZTONYI (2022a) = GOSZTONYI Gergely: Aspects of the History of Internet Regulation from Web 1.0 to Web 2.0. 13(1) *Journal on European History of Law*, (2022), 168–173.
- GOSZTONYI (2022b) = GOSZTONYI Gergely: Az Európai Unió Bírósága hozzájárulása az online platformok felelősségi és monitorozási kérdéseinek alaposabb megértéséhez. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika, 2022, 65–83. https://doi.org/10.36250/01065_05
- GOSZTONYI (2022c) = GOSZTONYI Gergely: Az internetes tartalomszabályozás európai típusú szabályozásának kezdetei, avagy irányelvektől a rendeletekig (TWF, AVMS, E-Comm, DSA, DMA). *Jog-Állam-Politika*, 2022/4., 17–32.
- GOSZTONYI (2023) = GOSZTONYI Gergely: *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices*. Cham, Springer, 2023. <https://doi.org/10.1007/978-3-031-46529-1>
- GOSZTONYI–GALEWSKA–ŠKOLKAY (2024) = GOSZTONYI Gergely – Ewa GALEWSKA – Andrej ŠKOLKAY: Challenges of Monitoring Obligations in the European Union's Digital Services Act. *ELTE Law Journal*, 2024/1., 45–60. <https://doi.org/10.54148/ELTELJ.2024.1.45>
- GOSZTONYI–HUSZÁR (2022) = GOSZTONYI Gergely – HUSZÁR Daniella: Az anonim kommentelés aktuális jogi megítélése az Emberi Jogok Európai Bírósága és az ausztrál legfelső bíróság gyakorlata alapján. In *Medias Res*, 2022/2., 141–152. <https://doi.org/10.59851/imr.11.2.10>
- GOSZTONYI–LENDVAI (2023a) = GOSZTONYI Gergely – LENDVAI Gergely Ferenc: A Skokie-ügy és mai tanulságai a digitális térben. *Infokommunikáció és Jog*, 2023/2., 3–6. https://infojog.hu/wp-content/uploads/pdf/Infokom_202302_3-6o.pdf
- GOSZTONYI–LENDVAI (2023b) = GOSZTONYI Gergely – LENDVAI Gergely Ferenc: Az Emberi Jogok Európai Bíróságának Nagykamara ítélete a Sanchez kontra Franciaország-ügyben, avagy felelős-e egy politikus a Facebook-falára írt kommentekért. *Állam- és Jogtudomány*, 2023/3., 33–51. <https://doi.org/10.51783/ajt.2023.3.03>
- GOSZTONYI–LENDVAI (2023c) = GOSZTONYI Gergely – LENDVAI Gergely Ferenc: Deepfake: A Multifaceted Dilemma in Ethics and Law. 32(2) *Journal of Information Ethics*, (2023), 109–121. <http://www.doi.org/10.2307/JIE.32.2.109>

- GOSZTONYI–LENDVAI (2024) = GOSZTONYI Gergely – LENDVAI Gergely Ferenc: Deepfake és dezinformáció. Mit tehet a jog a mélyhamisítással készített álhírek ellen? *Médiakutató*, 2024/1., 41–49. <http://doi.org/10.55395/MK.2024.1.3>
- GOSZTONYI–LENDVAI (2026) = GOSZTONYI Gergely – LENDVAI Gergely Ferenc: So, what is Chilling Effect? – (Re)Conceptualizing the Phenomenon of Chilling Effect in the context of Legal Doctrine and Social Perception. In: GOSZTONYI Gergely – LENDVAI Gergely Ferenc (szerk.): *Legal and Ethical Issues of Chilling Effect*. Cham, Springer, 2026. http://www.doi.org/10.1007/978-3-032-17654-7_1
- GOSZTONYI–PRIBULA–LENDVAI (2025) = GOSZTONYI Gergely – PRIBULA Eszter – LENDVAI Gergely Ferenc: Az Emberi Jogok Európai Bíróságának szólásszabadsággal kapcsolatosan alkalmazott tesztjei és azok értékelése. In *Medias Res*, 2025/1., 144–165. <https://doi.org/10.59851/imr.14.1.8>
- GOSZTONYI–ZANATHY (2025) = GOSZTONYI Gergely – ZANATHY Anna: Az internet szabályozására vonatkozó korai elméletek. *Jogelméleti Szemle*, 2025/3., 76–88. <https://doi.org/10.59558/jesz.2025.3.76>
- GOWDER (2023) = Paul GOWDER: *The Networked Leviathan for Democratic Platforms*. Cambridge, Cambridge University Press, 2023. <https://doi.org/10.1017/9781108975438>
- GÖSSL (2023) = Susanne Lilian GÖSSL: Recommender Systems and Discrimination. In: Sergio GENOVESI – Katharina KAESLING – Scott ROBBINS (Eds.): *Recommender Systems: Legal and Ethical Issues*. Cham, Springer, 2023. https://doi.org/10.1007/978-3-031-34804-4_2
- GUESS et al. (2018) = Andrew GUESS – Benjamin LYONS – Jacob M. MONTGOMERY – Brendan NYHAN – Jason REIFLER: *Fake news, Facebook ads, and misperceptions*. 2018. <https://bpb-us-e1.wpmucdn.com/sites.dartmouth.edu/dist/5/2293/files/2021/03/fake-news-2018.pdf>
- GYETVÁN (2021) = GYETVÁN Dorina: Az általános nyomon követési kötelezettség mint a közvetítő szolgáltatók felelősségének jövője? *Jogi tanulmányok*, 2021/1., 299–315. <https://edit.elte.hu/xmlui/handle/10831/106570>
- GYETVÁN–GOSZTONYI (2025) = GYETVÁN Dorina – GOSZTONYI Gergely: Garanciális elemek az online platformok véleménynyilvánítást korlátozó moderálási gyakorlatával szemben a digitális szolgáltatásokról szóló rendelet (DSA) előtt és után. *Magyar Jog*, 2025/4., 226–236. <https://doi.org/10.59851/mj.72.04.3>
- HAIG (2022) = HAIG Zsolt: Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle*, 2022/2., 115–128. <http://www.doi.org/10.32563/hsz.2022.2.7>
- HANSEN–JESPERSEN (2013) = Pelle Guldberg HANSEN – Andreas Maaloe JESPERSEN: Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy. 4(1) *European Journal of Risk Regulation* (2013), 3–28. <https://doi.org/10.1017/S1867299X00002762>
- HASSAN – DE FILIPPI (2017) = Samer HASSAN – Primavera DE FILIPPI: The Expansion of Algorithmic Governance: From Code is Law to Law is Code. 2017(Special Issue 17) *Journal of Field Actions* (2017), 88–90. <https://journals.openedition.org/factsreports/4518>
- HERKE (2023) = HERKE Csongor: Deepfake: áldás vagy átok? Jogi szabályozási szempontok. *Pro Futuro*, 2023/1., 157–178. <https://doi.org/10.26521/profuturo/2023/1/13334>

- HERMÁN (2024) = HERMÁN István: A közéleti véleménynyilvánítás fokozott védelmére vonatkozó alkotmányos szempontrendszer érvényesülése a bírósági gyakorlatban. *Ügyészek Lapja*, 2024/3., 73–92. <https://ugyeszeklapja.hu/?p=4608>
- HIETANEN–EDDEBO (2022) = Mika HIETANEN – Johan EDDEBO: Towards a Definition of Hate Speech - With a Focus on Online Contexts. 47(4) *Journal of Communication Inquiry* (2022), 440–458. <https://doi.org/10.1177/01968599221124309>
- HOFMANN–RAUE (2025) = Franz HOFMANN – Benjamin RAUE (Eds.): *Digital Services Act. Article-by-Article Commentary*. Baden-Baden, Nomos, 2025. <https://doi.org/10.5771/9783748931478>
- HUSOVEC (2024) = Martin HUSOVEC: *Principles of the Digital Services Act*. Oxford, Oxford University Press, 2024. <https://doi.org/10.1093/law-ocl/9780192882455.003.0002>
- HUSZÁR (2025) = HUSZÁR Daniella: Az algoritmusok szerepe a közösségimédia-platformokon alkalmazott sötét megoldások tekintetében. In: LENDVAI Gergely Ferenc – PAPP János Tamás (szerk.) *Digitális Dilemmák. Fiatal kutatók válogatott tanulmányai a közösségi média egyes szabályozási kérdéseiről*. Budapest, A Nemzeti Média- és Hírközlési Hatóság Médiatanácsának Médiatudományi Intézete, 2025, 191–222.
- JANNACH et al. (2011) = Dietmar JANNACH – Markus ZANKER – Alexander FELFERNIG – Gerhard FRIEDRICH: *Recommender Systems*. Cambridge, Cambridge University Press, 2011. <https://doi.org/10.1017/CBO9780511763113>
- JIMÉNEZ GONZÁLEZ (2021) = Aitor JIMÉNEZ GONZÁLEZ: Law, Code and Exploitation: How Corporations Regulate the Working Conditions of the Digital Proletariat. 48(2) *Critical Sociology* (2021), 361–373. <https://doi.org/10.1177/08969205211028964>
- JOBÁGYI (2009) = JOBÁGYI GÁBOR: *Személyi és családi jog*. Budapest, Szent István Társulat, 2009.
- JOHNSON–POST (1996) = David R. JOHNSON – David POST: Law and Borders: The Rise of Law in Cyberspace. 48(5) *Stanford Law Review* (1996), 1367–1402. <https://doi.org/10.2307/1229390>
- KAAKINEN et al. (2020) = Markus KAAKINEN – Anu SIROLA – Iina SAVOLAINEN – Atte OKSANEN: Shared identity and shared information in social media: development and validation of the identity bubble reinforcement scale. 23(1) *Media Psychology* (2020), 25–51. <https://doi.org/10.1080/15213269.2018.1544910>
- KAMAL (2005) = Ahmed KAMAL: *The law of cyber-space*. Geneva, United Nations Institute for Training and Research, 2005.
- KECSKÉS (2007) = KECSKÉS László: *Polgári jog. A személyek joga*. Budapest–Pécs, Dialóg Campus, 2007.
- KELEMEN (2022) = KELEMEN Roland: *A kivételes hatalom történeti és elméleti rendszere*. Budapest, Gondolat, 2022.
- KELEMEN (2023) = KELEMEN Roland: Cyberfare State modelljei: A digitális állam lehetséges irányai. In: FARKAS Ádám – KELEMEN Roland (szerk.): *A fejlődés fogságában? Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből*. Budapest, Gondolat, 2023, 13–42.

- KÉRINGER (2023) = KÉRINGER Szabolcs: NetzDG, avagy gyakorlati példa a platform-szabályozás megvalósítására. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Digitalizálódó társadalom. Tanulmányok az új technológiák társadalmi-jogi hatásairól*. Budapest, Ludovika, Budapest, 2023, 175–196. https://doi.org/10.36250/01164_10
- KHOSRAVINIK (2017) = Majid KHOSRAVINIK: Right Wing Populism in the West: Social Media Discourse and Echo Chambers. 19(3) *Insight Turkey* (2017), 53–68. <http://www.doi.org/10.25253/99.2017193.04>
- KLEIN (2023) = KLEIN Tamás: Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Digitalizálódó társadalom. Tanulmányok az új technológiák társadalmi-jogi hatásairól*. Budapest, Ludovika, Budapest, 2023, 117–139. https://doi.org/10.36250/01164_07
- KÓCZIÁN (2016) = KÓCZIÁN Sándor: Az Emberi Jogok Európai Bíróságának ítélete a sértő kommentekről az Index.hu Zrt. kontra Magyarország ügyben. *Jogesetek Magyarázata*, 2016/1–2., 111–116.
- KOLLÁR–SZŐKE (2023) = KOLLÁR Gergő – SZŐKE Gergely László: A „law as a code” koncepció alkalmazási lehetőségei. In: TILK Péter – FEKETE Kristóf Benedek (szerk.): *A jogalkotás digitalizációjának jogi lehetőségei*. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2023, 31–54.
- KOLTAY (2009) = KOLTAY András: *A szólásszabadság alapvonalai – magyar, angol, amerikai és európai összehasonlításban*. Századvég, Budapest, 2009.
- KOLTAY (2019) = KOLTAY András: A közügyek vitáinak szabadsága és a személyiségi jogok védelme. *Pázmány Law Working Papers*, 2019/4., 1–23. <https://publikacio.ppke.hu/id/eprint/2003>
- KOLTAY (2020) = KOLTAY András: A szólásszabadság doktrínája és a fake news jelensége az online platformokon. In: KOVÁCS Éva Margit (szerk.): Ünnepi kötet a 65 éves Imre Miklós tiszteletére. Budapest, Ludovika, 2020, 231–267. https://doi.org/10.36250/00878_19
- KOLTAY (2024a) = KOLTAY András: *Sajtószabadság. Egy közös európai eszme szabályozása*. Budapest, ORAC, 2024.
- KOLTAY (2024b) = KOLTAY András: Tárhelyszolgáltatás. In: KOLTAY András – LAPSÁNSZKY András – SZIKORA Tamás – TÓTH András (szerk.): *Nagykommentár a DSA rendelethez*. Budapest, Wolters Kluwer, 2024, 41–47.
- KOLTAY (2025) = KOLTAY András: A magánélet védelme. In: KOLTAY András (szerk.): *Magyar és európai médiajog*. Budapest, Wolters Kluwer, 2025, 123–140.
- KOLTAY–SZIKORA–LAPSÁNSZKY (2024) = KOLTAY András – SZIKORA Tamás – LAPSÁNSZKY András: Bevezetés. In: KOLTAY András – SZIKORA Tamás – LAPSÁNSZKY András (szerk.): *A vadnyugat vége? Tanulmányok az Európai Unió platform szabályozásáról*. Budapest, ORAC, 2024, 13–17. https://doi.org/10.59851/9789632586328_1
- KOVÁCS Andrea (2025) = KOVÁCS Andrea: Botok a közösségi médiában. In: LENDVAI Gergely Ferenc – PAPP János Tamás (szerk.) *Digitális Dilemmák. Fiatal kutatók válogatott tanulmányai a közösségi média egyes szabályozási kérdéseiről*. Budapest, A Nemzeti Média- és Hírközlési Hatóság Médiatanácsának Médiatudományi Intézete, 2025, 87–108. <https://real.mtak.hu/220575/1/667043a3-95f2-4efb-97f6-d8cdbc4180c4-2.pdf>

- KOVÁCS Helga (2024) = KOVÁCS Helga: A képmáshoz és a hangfelvételhez való jog érvényesítése és a közösséghez tartozással összefüggő személyiségi jog érvényesítése iránt indított perek. In: DZSULA Marianna – KOVÁCS Helga Mariann – SÁNDOR Ottó – TÓTH Gabriella Terézia – RIBAI Csilla (szerk.): *Polgári eljárásjog I–II*. Budapest, Novissima, 2024, 281–211.
- KOVÁCS–SORBÁN (2024) = KOVÁCS Helga – SORBÁN Kinga: A Kúria felülvizsgálati határozata a személyiségi jogok megsértéséről a közösségi médiában. In: KOLTAY András – SZOMORA Zsolt (szerk.): *A hírnév- és becsületvédelem joggyakorlata a polgári és a büntetőjogban*. Budapest, ORAC, 2024, 465–490.
- KOZŁOWSKI (2006) = Dan KOZŁOWSKI: “For the Protection of the Reputation or Rights of Others”. The European Court of Human Rights’ Interpretation of the Defamation Exception in Article 10(2). 11(1) *Communication Law and Policy* (2006), 133–178. https://doi.org/10.1207/s15326926clp1101_4
- KÖBIS–DOLEŽALOVÁ–SORAPERRA (2021) = Nils C. KÖBIS – Barbora DOLEŽALOVÁ – Ivan SORAPERRA: Fooled twice: People cannot detect deepfakes but think they can. 24(11) *iScience* (2021), Art. no. 103364. <http://www.doi.org/10.1016/j.isci.2021.103364>
- KRISTON–TÓTH (2023) = KRISTON Edit – TÓTH Dávid Attila: A képmáshoz és hangfelvételhez való jog aktualitásai, különös tekintettel a gyermekeket érintő „sharenting” jelenségére. *Publicationes Universitatis Miskolcensis Sectio Juridica et Politica* 2023/2., 85–97. <https://doi.org/10.32978/sjp.2023.015>
- KUCZERAWY (2018) = Aleksandra KUCZERAWY: *Intermediary liability and freedom of expression in the EU: from concepts to safeguards*. Cambridge, Intersentia, 2018.
- KUŹNICKA–BŁASZKOWSKA–KOSTYUK (2025) = Dominika KUŹNICKA–BŁASZKOWSKA – Nadiya KOSTYUK: Emerging need to regulate deepfakes in international law: the Russo–Ukrainian war as an example. 11(1) *Journal of Cybersecurity* (2025), Art. no. tyaf008. <https://doi.org/10.1093/cybsec/tyaf008>
- LADILAW (2017) = Emily LAIDLAW: *Are we asking too much from defamation law? Reputation systems, ADR, Industry Regulation and other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age. Proposal for Reform*. Ontario, Law Commission of Ontario, 2017. <https://doi.org/10.2139/ssrn.3059954>
- LÁNCOS (2022) = LÁNCOS Petra Lea: *The Many Facets of EU Soft Law*. Budapest, Pázmány Press, 2022. <https://publikacio.ppke.hu/id/eprint/1474>
- LEERSSEN (2023) = Paddy LEERSSEN: An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. 48(1) *Computer Law & Security Review* (2023), Art. no. 105790. <https://doi.org/10.1016/j.clsr.2023.105790>
- LEISER (2016) = Mark LEISER: The problem with ‘dots’. Questioning the role of rationality in the online environment. 30(3) *International Review of Law, Computers & Technology* (2016), 191–210. <https://doi.org/10.1080/13600869.2016.1145952>
- LEISER (2017) = Mark LEISER: Regulating Fake News. Response to European Commission consultation on Fake News and Online Distribution [Konferenciaelőadás]. *32nd Annual Conference 2017 [BILETA]*, Braga, 2017. <http://www.doi.org/10.13140/RG.2.2.29407.56481>
- LEMLEY (2021) = Mark A. LEMLEY: The Splinternet. 70(6) *Duke Law Journal* (2021), 1397–1427. <https://doi.org/10.2139/ssrn.3664027>

- LENDVAI (2023) = LENDVAI Gergely Ferenc: Deepfake a szólásszabadság tükrében: Reflexiók a jog perspektívájából. In: ACZÉL Petra – VESZELSZKI Ágnes (szerk.): *Deepfake: a valótlanság valóság*. Budapest, Gondolat, 2023, 121–138.
- LENDVAI (2024a) = LENDVAI Gergely Ferenc: Bejelentési és cselekvési mechanizmusok. In: KOLTAY András – LAPSÁNSZKY András – SZIKORA Tamás – TÓTH András (szerk.): *Nagykommentár a DSA rendelethez*. Budapest, Wolters Kluwer, 2024, 77–81.
- LENDVAI (2024b) = LENDVAI Gergely Ferenc: Indokolás. In: Koltay András – Lapsánszky András – Szikora Tamás – Tóth András (szerk.): *Nagykommentár a DSA rendelethez*. Budapest, Wolters Kluwer, 2024, 81–84.
- LENDVAI (2024c) = LENDVAI Gergely Ferenc: Taming the Titans? Digital Constitutionalism and the Digital Services Act. 17(2)(34) *ESSACHESS – Journal for Communication Studies* (2024) 169–184. <https://doi.org/10.21409/0M3P-A614>
- LENKOVICS–SZÉKELY (2001) = LENKOVICS Barnabás – SZÉKELY László: *Magyar polgári jog. A személyi jog vázlata*. Budapest, Eötvös József Könyvkiadó, 2001.
- LESSIG (1999) = Lawrence LESSIG: The Law of the Horse: What Cyberspace Might Teach. *Harvard Law Review* (1999), 501–549. <https://doi.org/10.2307/1342331>
- LESSIG (2006) = Lawrence LESSIG: *Code 2.0*. New York, Basic Books, 2006.
- LESSIG–RESNICK (1999) = Lawrence LESSIG – Paul RESNICK: Zoning Speech on the Internet: A Legal and Technical Model. 98(2) *Michigan Law Review* (1999), 395–431. <https://doi.org/10.2307/1290343>
- LIVINGSTONE–O’NEILL (2014) = Sonia LIVINGSTONE – Brian O’NEILL: Children’s rights online: challenges, dilemmas and emerging directions. In: Simone VAN DER HOF – Bibi VAN DEN BERG – Bart SCHERMER (Eds.): *Minding Minors Wandering the Web. Regulating Online Child Safety*. Berlin, Springer, 2014, 19–38. https://doi.org/10.1007/978-94-6265-005-3_2
- LODDER–ZWENNE (2014) = Arno R. LODDER – Gerrit-Jan ZWENNE (Eds.): *Recht en Computer* (Handbook on ICT Law). Alphen aan den Rijn, Wolters Kluwer, 2014.
- MACOVEI (2004) = Monica MACOVEI: *Freedom of expression. A guide to the implementation of Article 10 of the European Convention on Human Rights*. Strasbourg, Council of Europe, 2004.
- MAGRANI – DA SILVA (2024) = Eduardo MAGRANI – Paula Guedes Fernandes DA SILVA: The Ethical and Legal Challenges of Recommender Systems Driven by Artificial Intelligence. In: Henrique SOUSA ANTUNES – Pedro Miguel FREITAS – Arlindo L. OLIVEIRA – Clara MARTINS PEREIRA – Elsa VAZ DE SEQUEIRA – Luís BARRETO XAVIER (Eds.): *Multidisciplinary Perspectives on Artificial Intelligence and the Law*. Cham, Springer, 2024, 141–168. https://doi.org/10.1007/978-3-031-41264-6_8
- MARSDEN (2011) = Christopher T. MARSDEN: *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*. Cambridge, Cambridge University Press, 2011. <https://doi.org/10.1017/CBO9780511763410>
- MARTENS et al. (2018) = Bertin MARTENS – Luis AGUIAR WICHT – Maria Estrella GOMEZ HERRERA – Frank MULLER-LANGER: The digital transformation of news media and the rise of disinformation and fake news. 2018(02) *JRC Digital Economy Working Paper* (2018). <https://doi.org/10.2139/ssrn.3164170>

- MAZEH–SHMUELI (2020) = Itzik MAZEH – Erez SHMUELI: A personal data store approach for recommender systems: enhancing privacy without sacrificing accuracy. 139(C) *Expert Systems with Applications* (2020), 1–16. <https://doi.org/10.1016/j.eswa.2019.112858>
- MBIOH (2014) = Will MBIOH: Beyond echo chambers and rabbit holes: algorithmic drifts and the limits of the Online Safety Act, Digital Services Act, and AI Act. 33(3) *Griffith Law Review* (2024), 189–208. <https://doi.org/10.1080/10383441.2025.2481544>
- MCGONAGLE (2016) = Tarlach MCGONAGLE: *Freedom of Expression and Defamation*. Strasbourg, Council of Europe, 2016.
- MENYHÁRD (2017) = MENYHÁRD Attila: A magánélet védelme az Emberi Jogi Bíróság gyakorlatában. In: GÖRÖG Márta – MENYHÁRD Attila – KOLTAY András (szerk.): *A személyiség és védelme*. Budapest, ELTE Állam- és Jogtudományi Kar, 2017, 49–63.
- MENYHÁRD (2021) = MENYHÁRD Attila: The Impacts of Technological Revolution on the Role of the State. In: Martin BELOV (Ed.): *The IT Revolution and its Impact on State, Constitutionalism and Public Law*. Oxford, Hart Publishing, 2021, 55–70. <http://www.doi.org/10.5040/9781509940905>
- MEZRICZKY (2023) = MERZICZKY Marcell: Ne higgy a szemének! A deepfake online sajtó-reprezentációja 2018 és 2022 között. In: ACZÉL Petra – VESZELSZKI Ágnes (szerk.): *Deepfake: A valótlan valóság*. Budapest, Gondolat, 2023, 41–55.
- MILL (2020) = John Stuart MILL: *On liberty*. London, John W. Parker, 1859.
- MONTI (2020) = Matteo MONTI: The Eu Code of Practice on Disinformation and the Risk of the Privatisation of Censorship. In: Serena GIUSTI – Elisa PIRAS: *Democracy and Fake News. Information Manipulation and Post-Truth Politics*. London, Routledge, 2020, 214–225. <https://doi.org/10.4324/9781003037385-20>
- MONTI (2024) = Matteo MONTI: Towards a Federal-Type Regulation of Online Public Discourse by the EU? 30(4) *European Public Law* (2024), 441–462. <https://doi.org/10.54648/euro2024012>
- MRÁZ (2022) = MRÁZ Attila: Deepfake, demokrácia, kampány, szólásszabadság. In: Török Bernát – ZÖDI Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai*. Budapest, Ludovika, 2022, 249–277.
- MURRAY (2007) = Andrew MURRAY: *The Regulation of Cyberspace. Control in the Online Environment*. Abingdon, Routledge Cavendish, 2007.
- MURRAY (2011) = Andrew MURRAY: Nodes and Gravity in Virtual Space. 5(2) *Legisprudence* (2011), 195–221. <https://doi.org/10.5235/175214611797885684>
- MURRAY (2023) = Andrew MURRAY: *Information Technology Law: The Law and Society*. Oxford, Oxford University Press, 2023. <https://doi.org/10.1093/he/9780192893529.001.0001>
- NAGY Krisztina (2018) = NAGY Krisztina: *Műveltség – Média – Szabályozás. A médiaműveltség médiapolitikai jelentősége és szabályozási keretei*. Budapest, Gondolat, 2018.
- NAGY Csilla (2021) = NAGY Csilla: A rendezvényeken történő fotózás jogszerűségéről. *Jegyző és Közigazgatás*, 2021/4., 10–12.
- NEGREIRO (2025) = Mar NEGREIRO: *Children and deepfakes*. Brüsszel, Európai Unió, 2025. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf)

- NEWMAN et al. (2024) = Nic NEWMAN – Richard FLETCHER – Craig T. ROBERTSON – Amy ROSS ARGUEDAS – Rasmus Kleis NIELSEN: *Reuters Institute Digital News Report 2024*. Oxford, Reuters Institute for the Study of Journalism, 2024. <http://www.doi.org/10.60625/risj-vy6n-4v57>
- NHAN–CARROLL (2012) = Johnny NHAN – Bruce A. CARROLL: The Offline Defense of the Internet: An Examination of the The Offline Defense of the Internet: An Examination of the Electronic Frontier Foundation. 15(3) *SMU Science and Technology Law Review* (2012), 389–401. <https://scholar.smu.edu/cgi/viewcontent.cgi?article=1180&context=scitech>
- NNAWUCHI–GEORGE (2025) = Uchenna NNAWUCHI – Carlisle GEORGE: Decoding accountability: the importance of explainability in liability frameworks for smart border systems. 28 *Discover Computing* (2025), Art. no. 64. <https://doi.org/10.1007/s10791-025-09559-5>
- NORDELL (2021) = Emmie NORDELL: Code is Law – Deterritorialisation and Reterritorialisation of Law, Law is Code – Cyberspace, Personalisation Algorithms and Human Cognition. 2(1) *Anthropocenes – Human, Inhuman, Posthuman* (2021), Art. no. 10. <https://doi.org/10.16997/ahip.932>
- NOVOMIC (2024) = Milos NOVOMIC: *The EU Digital Services Act (DSA): A Commentary*. Alphen aan den Rijn, Kluwer Law International, 2024.
- OBERHOLZER-GEE–STRUMPF (2010) = Felix OBERHOLZER-GEE – Koleman STRUMPF: File Sharing and Copyright. *Innovation* 10(1) *Policy and the Economy* (2010), 19–55. <https://doi.org/10.1086/605852>
- ONG (2015) = Rebecca ONG: Liability of Internet intermediaries for user-generated content: An examination of Oriental Press Group Ltd v Feaworks Solutions Ltd. 10(1) *Computer Law & Security Review* (2015), 131–138. <https://doi.org/10.1016/j.clsr.2014.11.008>
- OSTER (2015) = Jan OSTER: *Media Freedom as a Fundamental Right*. Cambridge, Cambridge University Press, 2015. <https://doi.org/10.1017/CBO9781316162736>
- PACKARD (2023) = Noel PACKARD: INTERNET Prehistory: ARPANET Chronology. 9(2) *Cogent Social Sciences* (2023), Art. no. 2245237. <https://doi.org/10.1080/23311886.2023.2245237>
- PAPP (2017) = János Tamás PAPP: Liability for Third-party comments before the European Court of Human Rights – Comparing the Estonian Delfi and the Hungarian Index-MTE decisions. In: Marcell SZABÓ – Petra Lea LÁNCOS – Réka VARGA (szerk.): *Hungarian Yearbook of International and European Law* 2016. Hague, Eleven International Publishing, 2017, 315–326. <https://doi.org/10.5553/HYIEL/266627012016004001019>
- PAPP (2022) = PAPP János Tamás: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében*. Wolters Kluwer, Budapest, 2022.
- PAPP (2023) = János Tamás PAPP: Recontextualizing the Role of Social Media in the Formation of Filter Bubbles. *Hungarian Yearbook of International Law and European Law*, 2023/1., 136–150. <http://www.doi.org/10.5553/HYIEL/266627012023011001012>

- PAPP (2024a) = PAPP János Tamás: Ajánlórendszerek. In: KOLTAY András – LAPSÁNSZKY András – SZIKORA Tamás – TÓTH András (szerk.): *Nagykommentár a DSA rendelethez*. Budapest, Wolters Kluwer, 2024, 137–138.
- PAPP (2024b) = PAPP János Tamás: Ajánlórendszerek és szűrőbuborékok. In: KOLTAY András – SZIKORA Tamás – LAPSÁNSZKY András (szerk.): *A vadnyugat vége? Tanulmányok az Európai Unió platform szabályozásáról*. Budapest, ORAC, 2024, 231–259. https://doi.org/10.59851/9789632586328_12
- PAWELEC (2025) = MARIA PAWELEC: *Deepfakes: Manipulation on Demand? Evolution of Deepfake Technology, Social Impact, and the Path Forward*. Tel Aviv, Heinrich Böll Foundation Israel Public Policy Institute, 2025.
- PETRIK (2001) = PETRIK Ferenc: *A személyiség jogi védelme, A sajtó helyreigazítás*. Budapest, HVG-ORAC, 2001.
- PETRIK (2004) = PETRIK Ferenc: A személyiségi jogok az új Polgári Törvénykönyvben. *Magyar Jog*, 2004/5., 257–271.
- PINTÉR (2007) = PINTÉR Róbert (szerk.): *Az információs társadalom. Az elmélettől a politikai gyakorlatig*. Budapest, Új Mandátum, 2007.
- POLYÁK (2001) = POLYÁK Gábor: Az internet az európai médiaszabályozásban. *Studia Iuvenum*, 2001/4., 151–178.
- POLYÁK (2020) = POLYÁK Gábor: A forgalomirányító szolgáltatások médiaszabályozási kérdései. In: POLYÁK Gábor (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – A forgalomirányító szolgáltatások szabályozása*. Budapest, HVG-ORAC, 2020, 108–147.
- POLYÁK et al. (2021) = POLYÁK Gábor – PATAKI Gábor – GOSZTONYI Gergely – SZALAY Klára: Versenyjogi előzmények és piacsabályozási eszközök a Digitális piacokról szóló európai rendelet tervezetében. In: VALENTINY Pál – ANTAL-POMÁZI Krisztina – BEREZVAI Zombor – NAGY Csongor István (szerk.): *Verseny és szabályozás 2021*. Budapest, MTA KRTK Közgazdaság-tudományi Intézet, 2021, 145–164.
- PÜNKÖSTY (2022a) = PÜNKÖSTY András: Egy új digitális etika megalapozásának egyes szempontjai – big data, algoritmusos döntéshozatal és a személy az adatalapú társadalomban. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai*. Budapest, Ludovika, 2022, 43–65.
- PÜNKÖSTY (2022b) = PÜNKÖSTY András: Merre tart az európai szintű platformszabályozás? Áttekintés a platformok szabályozásának versenyjogi ösztönzőiről, valamint a fúziókontroll lehetséges fejlesztéséről. In: TÖRÖK Bernát – ZÖDI Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika, 2022, 176–192. https://doi.org/10.36250/01065_10
- RAD–CHRISTIE (2024) = IRIS RAD – ALEC CHRISTIE: Rolling in the deepfakes: Generative AI, privacy and regulation. *LexisNexis*, 2024. november 6., <https://www.lexisnexis.com/blogs/en-au/insights/rolling-deepfakes-generative-artificial-intelligence-privacy-regulation>
- REED–MURRAY (2018) = CHRIS REED – ANDREW MURRAY: *Rethinking the Jurisprudence of Cyberspace*. Cheltenham, Edward Elgar, 2018. <https://doi.org/10.4337/9781785364297>

- REIDENBERG (1997–1998) = Joel REIDENBERG: *Lex Informatica: The Formulation of Information Policy Rules through Technology*. 76(3) *Texas Law Review* (1997–1998), 553–593.
- RIORDAN (2016) = Janni RIORDAN: *The Liability of Internet Intermediaries*. Oxford, Oxford University Press, 2016. <https://doi.org/10.1093/oso/9780198719779.001.0001>
- ROZGONYI (2003) = ROZGONYI Krisztina: A hálózati médiumok szabályozásának néhány lehetséges szempontja. In: ENYEDI NAGY Mihály – POLYÁK Gábor – SARKADY Ildikó (szerk.): *Magyarország médiakönyve 2003*. Budapest, ENAMIKÉ, 2003, 639–650.
- RUTGERS–SAUTER (2021) = Jacobien RUTGERS – Wolf SAUTER: Promoting Fair Private Governance in the Platform Economy: EU Competition and Contract Law Applied to Standard Terms. In: Emilija LEINARTE – Okeoghene ODUDU – Sophie TURENNE (Eds.): *Cambridge Yearbook of European Legal Studies*. Cambridge, University of Cambridge, 2021, 343–381. <http://doi.org/10.1017/cel.2021.11>
- SCHEIRER (2023) = Walter J. SCHEIRER: *A History of Fake Things on the Internet*. Stanford, Stanford University Press, 2023. <https://doi.org/10.1515/9781503637047>
- SCHULTE-NÖLKE et al. (2020) = Hans SCHULTE-NÖLKE – Ida RÜFFER – Carlos NOBREGA – Aneta WIEWÓROWSKA-DAGALSKA: *The legal framework for e-commerce in the Internal Market*. Luxemburg, Európai Parlament, 2020.
- SCHWEMER (2023) = Sebastian Felix SCHWEMER: Digital Services Act: a reform of the e-Commerce Directive and much more. In: Andrej SAVIN – Jan TRZASKOWSKI (Eds.): *Research Handbook on EU Internet Law*. Cheltenham, Edward Elgar Publishing, 2023, 232–252. <https://doi.org/10.4337/9781803920887.00020>
- SCOTT (2017) = Andrew SCOTT: An unwholesome layer cake: intermediary liability in English defamation and data protection law. In: David MANGAN – Lorna GILLES (Eds.): *The Legal Challenges of Social Media*. Cheltenham, Edward Elgar, 2017, 222–246. <https://doi.org/10.4337/9781785364518.00025>
- SEARGEANT–TAGG (2019) = Philip SEARGEANT – Caroline TAGG: Social media and the future of open debate: A user-oriented approach to Facebook’s filter bubble conundrum. 27(3) *Discourse, Context & Media* (2019), 41–48. <https://doi.org/10.1016/j.dcm.2018.03.005>
- SMUK (2019) = SMUK Péter: A kormány beszéde. Az Első Alkotmánykiegészítés paradigma és a „government speech” alkotmányos korlátai az Egyesült Államokban. *Iustum Aequum Salutare*, 2019/4., 47–68. https://ias.jak.ppke.hu/20194sz/04_SmukP_IAS_2019_4.pdf
- SÓLYOM (1983) = SÓLYOM László: *A személyiségi jogok elmélete*. Budapest, Közgazdasági és Jogi Könyvkiadó, 1983.
- SORBÁN (2020) = SORBÁN Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle*, 2020/10., 81–104. <https://doi.org/10.38146/BSZ.2020.10.4>
- DE STREEL et al. (2020) = Alexandre DE STREEL – Elise DEFREYNE – Hervé JACQUEMIN – Michèle LEDGER – Alejandra MICHEL – Alessandra INNESTI – Marion GOUBET – Dawid USTOWSKI: *Online Platforms’ Moderation of Illegal Content Online. Law, Practices and Options for Reform*. Luxemburg, Európai Parlament, 2020.

- SULYOK (2021) = SULYOK Katalin: A magán- és családi élet tisztelőben tartásához való jog. In: SONNEVEND Pál – BODNÁR Eszter (szerk.): *Az Emberi Jogok Európai Egyezményének kommentárja*. Budapest, HVG-ORAC, 2021, 182–217.
- SUNSTEIN (2001) = Cass R. SUNSTEIN: *Republic.com*. Princeton, Princeton University Press, 2001.
- SUNSTEIN (2007) = Cass R. SUNSTEIN: *Republic.com 2.0*. Princeton, Princeton University Press, 2007.
- SVANTESSON (2020) = Dan Jerker B. SVANTESSON: Internet Jurisdiction and Intermediary Liability. In: Giancarlo FROSIO (Ed.): *Oxford Handbook of Online Intermediary Liability*. Oxford, Oxford University Press, 2020, 691–708. <https://doi.org/10.1093/oxfordhb/9780198837138.013.36>
- SZEGHALMI (2014) = SZEGHALMI Veronika: A képmás polgári jogi védelme és a hazai szabályozás alapvonalaival áttekintése európai példákon át. *Médiakutató*, 2014/1., 53–62. https://www.mediakutato.hu/cikk/2014_01_tavasz/04_kepmas_ptk_europa.pdf
- SZÉKELY (2007) = SZÉKELY László: *Magyar polgári jog. A polgári jog alapjai*. Budapest, Eötvös József Könyvkiadó, 2007.
- SZÉKELY (2011) = SZÉKELY László: *A személyiségi jogok hazai elmélete. A forrásvidék*. Budapest, ELTE Eötvös, 2011.
- SZEMÉLYI (1915) = SZEMÉLYI Kálmán: *A névjog. Tanulmány a személyiségi jogok köréből*. Budapest, Franklin, 1915.
- SZIKORA (2024a) = SZIKORA Tamás: A Polgári Törvénykönyv előírásainak bemutatása. In: KOLTAY András – SZOMORA Zsolt (szerk.): *A hírnév- és becsületvédelem joggyakorlata a polgári és a büntetőjogban*. Budapest, ORAC, 2024, 29–37.
- SZIKORA (2024b) = SZIKORA Tamás: A tárhelyszolgáltató felelőssége. In: KOLTAY András – SZOMORA Zsolt (szerk.): *A hírnév- és becsületvédelem joggyakorlata a polgári és a büntetőjogban*. Budapest, ORAC, 2024, 263–268.
- SZIKORA (2024c) = SZIKORA Tamás: Az általános nyomon követési kötelezettség hiányának gyakorlati érvényesülése a közösségi oldalak vonatkozásában. In: KOLTAY András – SZIKORA Tamás – LAPSÁNSZKY András: *A Vadnyugat vége? Tanulmányok az Európai Unió platformszabályozásáról*. Budapest, ORAC, 2024, 295–310. https://doi.org/10.59851/9789632586328_14
- SZILÁGYI (2018) = SZILÁGYI Emese: A kommunikációs alapjogok általános értelmezése és alkalmazása a rendes bírósági és az alkotmánybírósági gyakorlatban – a bírói kezdeményezések és az alkotmányjogi panaszos ügyek tapasztalatai. *MTA Law Working Papers*, 2018/16. <https://jog.tk.elte.hu/mtalwp/a-kommunikacios-alapjogok-altalanos-ertelmezese-es-alkalmazasa-a-rendes-birosagi-es-az-alkotmanybirosagi-gyakorlatban-a-biroi-kezdemenyezesek-es-az-alkotmanyjogi-panaszos-ugyek-tapasztalatai>
- SZŐKE (2021) = SZŐKE Gergely László: A közösségi oldalak szabályozási problémái. In: KIS Kelemen Bence – MOHAY Ágoston (szerk.): *A technológiai fejlődés jogi kihívásai. Kézikönyv a jogalkotás és jogalkalmazás számára*. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2021, 105–120.
- SZYMIELEWICZ (2023) = Katarzyna SZYMIELEWICZ: *Prototyping User Empowerment. Towards DSA-compliant recommender systems*. Varsó, Panoptykon Foundation, 2023.

- TATTAY (2004) = TATTAY Levente: Gondolatok a képmás védelméről. *Közjegyzők Közlönye*, 2004/9., 3–7.
- THALER–SUNSTEIN (2009) = Richard THALER – Cass R. SUNSTEIN: *Nudge. Improving Decisions about Health, Wealth and Happiness*. New Haven, Penguin Books, 2009.
- TÓTH (2022) = TÓTH András: Az online platformok európai szabályozása. *In Medias Res*, 2022/2., 78–102. <https://doi.org/10.59851/imr.11.2.6>
- TÓTH J. (2017) = TÓTH J. Zoltán: Rendőrképmás: sajtószabadság és képmáshoz való jog a polgári jogi és az alapjogi jogosultságok keresztútján. *Pro Futuro*, 2017/2., 110–128.
- TÖRÖ (1979) = TÖRÖ Károly: *Személyiségvédelem a polgári jogban*. Budapest, Közgazdasági és Jogi Könyvkiadó, 1979.
- UITZ (2021) = UITZ Renáta: A véleménynyilvánítás szabadsága. In: SONNEVEND Pál – BODNÁR Eszter (szerk.): *Az Emberi Jogok Európai Egyezményének kommentárja*. Budapest, HVG-ORAC, 2021, 244–296.
- VACCARI–CHADWICK (2020) = Cristian VACCARI – Andrew CHADWICK: Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. 6(1) *Social Media + Society* (2020), 1–13. <https://doi.org/10.1177/2056305120903408>
- VALCKE–LENAERTS (2010) = Peggy VALCKE – Marieke LENAERTS: Who’s author, editor and publisher in user-generated content? Applying traditional media concepts to UGC providers. 24(1) *International Review of Law, Computers and Technology* (2010), 119–131. <https://doi.org/10.1080/13600861003644533>
- VÁRADI (2019) = VÁRADI Szilvia: A közsférőre vonatkozó adatvédelmi szabályok a GDPR tükrében. *Pro Futuro*, 2019/1., 39–54. <http://www.doi.org/10.26521/Profuturo/1/2019/3877>
- VÉKÁS (2013) = VÉKÁS Lajos (szerk.): *A Polgári Törvénykönyv magyarázatokkal*. Budapest, CompLex, 2013.
- VEREBICS (1998) = VEREBICS János: A tér, a szabadság és a normák – vázlat az Internet jogának fogalmi megközelítéséhez. *Híradástechnika*, 1998/9–10., 39–57.
- VESELSZKI (2012) = VESELSZKI Ágnes: (szerk.): *Netszótár – @-tól a zuckerbergnetig*. Budapest, ELTE Eötvös, 2012.
- VESELSZKI (2022) = VESELSZKI Ágnes: A tudományos influencerektől a deepfake-ig. A legújabb tudománykommunikációs lehetőségek. *Filológia*, 2022/1–4., 27–39.
- VIGEN SMOLARZ – VINTHER-JENSEN (2024) = August VIGEN SMOLARZ – Eske VINTHER-JENSEN: *Preventing “Torrents of Hate” or Stifling Free Expression Online?* Nashville, The Future of Free Speech, 2024. <https://futurefreespeech.org/wp-content/uploads/2024/05/Preventing-Torrents-of-Hate-or-Stifling-Free-Expression-Online-The-Future-of-Free-Speech.pdf>
- VITKOVICS (2025) = VITKOVICS Bálint: A becsülethez és jóhírnévhez való jog megsértése a közösségi platformokon. In: LENDVAI Gergely Ferenc – PAPP János Tamás (szerk.) *Digitális Dilemmák. Fiatal kutatók válogatott tanulmányai a közösségi média egyes szabályozási kérdéseiről*. Budapest, A Nemzeti Média- és Hírközlési Hatóság Média-tanácsának Médiatudományi Intézete, 2025, 45–61.

- WAGNER (2023) = Gerhard WAGNER: Liability Rules for the Digital Age – Aiming for the Brussels Effect. *Forschungsinstitut für Recht und digitale Transformation Working Paper Series*, 2023/10. <https://doi.org/10.2139/ssrn.4320285>
- WALDEN (2018) = Ian WALDEN: *Telecommunications Law and Regulation*. Oxford, Oxford University Press, 2018. <https://doi.org/10.1093/oso/9780198807414.001.0001>
- WENDEHORST (2016) = Christiane WENDEHORST: Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive. 5(1) *Journal of European Consumer and Market Law* (2016), 30–33.
- WILMAN (2023) = Folkert WILMAN: Between Preservation and Clarification. The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law. In: Joris VAN HOBOKEN – João Pedro QUINTAIS – Naomi APPELMAN – Ronan FAHY – Ilaria BURI – Marlene STRAUB (Eds.): *Putting the Digital Services Act into Practice: Enforcement, Access to Justice, and Global Implications*. Berlin, Verfassungsblog GmbH, 2023, 35–49. <https://doi.org/10.17176/20230208-093135-0>
- WILMAN–KALÉDA–LOEWENTHAL (2024) = Folkert WILMAN – Saulius Lukas KALÉDA – Paul-John LOEWENTHAL: *The EU Digital Services Act*. Oxford, Oxford University Press, 2024. <https://doi.org/10.1093/law/9780198892847.001.0001>
- WIŚNIEWSKI (2021) = Adam WIŚNIEWSKI: The European Court of Human Rights and Internet-Related Cases. 26(3) *Białystok Legal Studies*, (2021), 109–133. <http://www.doi.org/10.15290/bsp.2021.26.03.06>
- WOLTERS–GELLERT (2023) = Pieter WOLTERS – Raphaël GELLERT: Towards a better notice and action mechanism in the DSA. 14(3) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2023), 403–419. <https://www.jipitec.eu/jipitec/article/view/392>
- YOO (2018) = S. Christopher Yoo: Paul Baran, network theory, and the past, present, and future of the internet. 17(1) *Colorado Technology Law Journal* (2018), 161–185. <https://doi.org/10.2139/ssrn.3317642>
- ZANATHY (2021) = ZANATHY Anna: „Kiberjog” vagy Netikett: Az internet szabályozására vonatkozó jogtörténeti elméletek. *Joghistoria*, 2021/1–2., 44–52.
- ZANATHY (2025) = ZANATHY Anna: A közösségi média platformok jogi meghatározásának nehézségei a DSA előtt és alatt. *Themis*, 2025/2., 184–203. <https://doi.org/10.55052/themis.2024.2.184>
- ZEYBEK – VAN HOBOKEN – BURI (2022) = Bengi ZEYBEK – Joris VAN HOBOKEN – Ilaria BURI: Redressing Infringements of Individuals' Rights Under the Digital Services Act. *DSA Observatory*, 2022. május 4. <https://dsa-observatory.eu/2022/05/04/redressing-infringements-of-individuals-rights-under-the-digital-services-act>
- ZŐDI (2020) = ZŐDI Zsolt: A jog és a kód. In: POLYÁK Gábor (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog. A forgalomirányító szolgáltatások szabályozása*. Budapest, HVG-ORAC, 2020, 15–35.
- ZŐDI (2023) = ZŐDI Zsolt: *Platformjog*. Budapest, Ludovika, 2023.

Hivatkozott jogszabályok, jogi dokumentumok

Nemzetközi egyezmények

Emberi Jogok Európai Egyezménye
Polgári és Politikai Jogok Nemzetközi Egyezségokmánya

Az Európai Unió jogi aktusai

Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, HL C 202., 2016.6.7.

Rendeletek

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), HL L 119., 2016.5.4.

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 (P2B), PE/56/2019/REV/1, HL L 186., 2019.7.11.

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 (digitális szolgáltatásokról szóló rendelet), PE/30/2022/REV/1, HL L 277., 2022.10.27.

Az Európai Parlament és a Tanács (EU) 2024/1083 rendelete (2024. április 11.) a belső piaci médiaszolgáltatások közös keretének létrehozásáról és a 2010/13/EU irányelv módosításáról (a tömegtájékoztatás szabadságáról szóló európai rendelet), PE/4/2024/REV/1, HL L 2024/1083, 2024.4.17.

Irányelvek

Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, HL L 281., 1995.11.23.

Az Európai Parlament és a Tanács 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, PE/33/2018/REV/1, HL L 303, 28.11.2018

Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, PE/51/2019/REV/1, HL L 130., 2019.5.17.

Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (elektronikus kereskedelemről szóló irányelv), HL L 178, 17/07/2000

Ajánlások, magatartási kódexek, közlemények, előterjesztések, jelentések, döntések

A dezinformációra vonatkozó uniós gyakorlati kódex

A jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódex

A Bizottság közleménye: Iránymutatás a rangsorolási átláthatóságról az (EU) 2019/1150 európai parlamenti és tanácsi rendeletnek megfelelően (P2B Iránymutatás), 2020/C 424/01, C/2020/8579, HL C 424., 2020.12.8.

Commission decision of 25.4.2023 designating Facebook as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council

Commission Staff Working Document Online services, including e-commerce, in the Single Market {SEC(2011) 1641 final}

Commission staff working document. Impact assessment. Accompanying the document proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC {COM(2020) 825 final} – {SEC(2020) 432 final} – {SWD(2020) 349 final}

A Tanács következtetései Európa digitális jövőjének alakításáról, 2020/C 202 I/01, ST/8711/2020/INIT, HL C 202I., 2020.6.16.

European Court of Human Rights Registry: Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence. Strasbourg, Council of Europe/European Court of Human Rights, 2025

Javaslat az Európai Parlament és a tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, 2020/0361(COD), COM(2020) 825 final

WP29: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN, WP251rev.01.

Az Amerikai Egyesült Államok jogi aktusai

Communications Decency Act (CDA), Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996).

Hivatkozott jogesetek

Emberi Jogok Európai Bírósága

Ahmet Yıldırım kontra Törökország, App. no. 3111/10. (2012. december 18.)

Appleby és társai kontra Egyesült Királyság, App. no. 44306/98. (2003. július 5.)

- Axel Springer AG kontra Németország, App. no. 39954/08. (2012. február 7.)
- Bédat kontra Svájc, App. no. 56925/08. (2016. március 29.)
- Björk Eiðsdóttir kontra Izland, App. no. 46443/09. (2012. július 10.)
- Bladet Tromsø és Stensaaas kontra Norvégia, App. no. 29183/95. (1999. május 20.)
- Bowman kontra Egyesült Királyság, App. no. 24839/94. (1998. február 19.)
- Brasillier kontra Franciaország, App. no. 71343/01. (2006. április 11.)
- Chauvy és társai kontra Franciaország, App. no. 64915/01. (2004. június 29.)
- Couderc és Hachette Filipacchi Associés kontra Franciaország, App. no. 40454/07. (2015. november 10.)
- Dąbrowski kontra Lengyelország, App. no. 18235/02. (2006. december 19.)
- De Haes és Gijssels kontra Belgium, App. no. 19983/92. (1997. február 24.)
- Delfi AS kontra Észtország, App. no. 64569/09. (2015. június 16.)
- Editorial Board of Pravoye Delo és Shtetel kontra Ukrajna, App. no. 33014/04. (2011. május 5.)
- Egeland és Hanseid kontra Norvégia, App. no. 34438/04. (2009. április 16.)
- Egill Einarsson kontra Izland, App. no. 24703/15. (2017. november 7.)
- Feldek kontra Szlovákia, App. no. 29032/95. (2001. július 12.)
- Fressoz és Roire kontra Franciaország, App. no. 29183/95. (1999. január 21.)
- Gutiérrez Suárez kontra Spanyolország, App. no. 16023/07. (2010. június 1.)
- Handyside kontra Egyesült Királyság, App. no. 5493/72. (1976. december 7.)
- Incal kontra Törökország, App. no. 22678/93. (1998. június 9.)
- Janowski kontra Lengyelország, App. no. 25716/94. (1999. január 21.)
- Jerusalem kontra Ausztria, App. no. 26958/95. (2001. február 27.)
- Jon Gaunt kontra Egyesült Királyság, App. no. 26448/12 (2016. szeptember 6.)
- Lautsi és társai kontra Olaszország, App. no. 30814/06. (2011. március 18.)
- Lingens kontra Ausztria, App. no. 9815/82. (1986. július 8.)
- Lopes Gomes Da Silva kontra Portugália, App. no. 37698/97. (2000. szeptember 28.)
- Lozovyye kontra Oroszország, App. no. 4587/09. (2018. április 24.)
- Magyar Jeti Zrt. kontra Magyarország, App. no. 11257/16. (2018. december 4.)
- Magyar Tartalomszolgáltatók Egyesülete és Index.hu Zrt. kontra Magyarország, App. no. 22947/13. (2016. február 2.)
- Marian Maciejewski kontra Lengyelország, App. no. 34447/05. (2015. január 13.)
- Medžlis Islamske Zajednice Brčko és társai kontra Bosznia és Hercegovina, App. no. 17224/11. (2017. június 27.)
- Melnychuk kontra Ukrajna, App. no. 28743/03. (2005. július 28.), 2.
- Morice kontra Franciaország, App. no. 29369/10. (2015. április 23.)
- Mosley kontra Egyesült Királyság, App. no. 48009/08. (2011. május 10.)
- Nikowitz és Verlagsgruppe News GmbH kontra Ausztria, App. no. 5266/03. (2007. február 22.)
- Novaya Gazeta és Borodianskiy kontra Oroszország, App. no. 14087/08. (2013. március 28.)
- Oberschlick kontra Ausztria (2. sz.), App. no. 20834/92. (1997. július 1.)
- Ólafsson kontra Izland, App. no. 58493/13. (2017. március 16.)
- Peck kontra Egyesült Királyság, App. no. 44647/98. (2003. január 28.)
- Pedersen és Baadsgaard kontra Dánia, App. no. 49017/99. (2004. december 17.)
- Riolo kontra Olaszország, App. no. 42211/07. (2008. július 17.)
- Salumäki kontra Finnország, App. no. 23605/09. (2014. április 29.)
- Société Prisma Presse kontra Franciaország, App. no. 66910/01. és 71612/01. (2003. július 1.)

Sousa Goucha kontra Portugália, App. no. 70434/12. (2016. március 22.)
 Stoll kontra Svájc, App. no. 69698/01. (2007. december 10.)
 Tamiz kontra Egyesült Királyság, App. no. 3877/14. (2017. szeptember 19.)
 Tammer kontra Észtország, App. no. 41205/98. (2001. február 6.)
 Tønsbergs Blad AS és Haukom kontra Norvégia, App. no. 510/04. (2007. március 1.)
 Tuşalp kontra Törökország, App. no. 32131/08. (2012. február 21.)
 TV Vest AS és Rogaland Pensjonistparti kontra Norvégia, App. no. 21132/05. (2008. december 11.)
 Uj kontra Magyarország, App. no. 23954/10. (2011. július 19.)
 Veraart kontra Hollandia, App. no. 10807/04. (2006. november 30.)
 Vereinigung Bildender Künstler kontra Ausztria, App. no. 68354/0.1 (2007. április 5.)
 Von Hannover kontra Németország (1. sz.), App. no. 59320/00. (2004. június 24.)
 Von Hannover kontra Németország (2. sz.), App. no. 40660/08 és 60641/08. (2012. február 7.)
 Willem kontra Franciaország, App. no. 10883/05. (2009. július 16.)

Az Európai Unió Bírósága

C-18/18. Eva Glawischnig-Piesczek kontra Facebook Ireland Limited, ECLI:EU:C:2019:821.
 C-203/22. Dun & Bradstreet Austria, ECLI:EU:C:2024:745.
 C-275/06. Productores de Música de España (Promusicae) kontra Telefónica de España SAU, ECLI:EU:C:2008:54.
 C-291/13. Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi és Giorgos Sertis, ECLI:EU:C:2014:2209.
 C-314/12. UPC Telekabel Wien GmbH kontra Constantin Film Verleih GmbH és Wega Filmproduktionsgesellschaft mbH, ECLI:EU:C:2014:192.
 C-324/09. L'Oréal SA és társai kontra eBay International AG és társai, ECLI:EU:C:2011:474.
 C-352/85. Bond van Adverteerders és társai kontra Holland Állam, EU:C:1988:196.
 C-484/14. Tobias, Mc Fadden kontra Sony Music Entertainment Germany GmbH, EU:C:2016:689.
 C-51/96. és C-191/97. egyesített ügyek. Christelle Delière kontra Ligue francophone de judo et disciplines associées ASBL, Ligue belge de judo ASBL, Union européenne de judo (C-51/96.) és François Pacquée (C-191/97.), EU:C:2000:199.
 C-521/17. Coöperatieve Vereniging SNB-REACT UA kontra Deepak Mehta, ECLI:EU:C:2018:639.
 C-682/18. és C-683/18. egyesített ügyek. Frank Peterson kontra Google LLC és társai és Elsevier Inc. kontra Cyando AG, ECLI:EU:C:2021:503.
 C-70/10. Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771.
 C-291/13. Sotiris Papasavvas kontra O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi és Giorgos Sertis, ECLI:EU:C:2014:2209.
 C-236/08–C-238/08. egyesített ügyek. Google France SARL és Google Inc. kontra Louis Vuitton Malletier SA (C-236/08), Google France SARL kontra Viaticum SA és Luteciel SARL (C-237/08) és Google France SARL kontra Centre national de recherche en relations humaines (CNRRH) SARL és társai (C-238/08), ECLI:EU:C:2010:159.

Magyar jogesetek

Alkotmánybírósági határozatok

36/1994. (VI. 24.) AB határozat
7/2014. (III. 7.) AB határozat
13/2014. (IV. 18.) AB határozat
28/2014. (IX. 29.) AB határozat

9/2015. (IV. 23.) AB határozat
3100/2017. (V. 8.) AB határozat
3107/2018. (IV. 9.) AB határozat
15/2020. (VII. 8.) AB határozat

Magyar bíróságok döntései

Legfelsőbb Bíróság Pfv. 20.801/2007/7.
Kúria Pfv. 21.245/2015/4.
Kúria Pfv. 21.267/2018/17.

Fővárosi Ítéltábla Pf. 21.001/2010/4.
Fővárosi Ítéltábla Pf. 20.537/2014/3.
Győri Ítéltábla Pf. 20.138/2019/6.

Fővárosi Ítéltábla 2.Pf. 20.271/2006/4.
Fővárosi Ítéltábla 2.Pf. 20.922/2007/5.
Fővárosi Ítéltábla 2.Pf. 21.008/2013/6.
Fővárosi Ítéltábla Pf. 20.750/2021/15.
Fővárosi Ítéltábla Pf. 21.277/2008/3.

Fővárosi Törvényszék P. 22.699/2016/4.

Fővárosi Bíróság P. 20.239/2008/3.
Fővárosi Bíróság 48.Pf. 29.878/2001.

Közzétett eseti döntések

BH 1985.17.
BH 1994.127.
BH 1995.632.
BH 1997.578.
BH 2006.282.

BDT 2015.3312.
BDT 2020.4126.
BDT 2020.4222.

PJD 2016.21.
PJD 2019.18.

A sorozatban eddig megjelent kötetek

1. Apró István (szerk.): *Határon túli magyar nyelvű médiumok 2010/2011* (2012)
2. Dobos Ferenc: *Nemzeti identitás, asszimiláció és médiahasználat a határon túli magyarság körében 1999–2011* (2012)
3. Csink Lóránt – Mayer Annamária: *Variációk a szabályozásra. Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban* (2012)
4. Sarkady Ildikó – Grad-Gyenge Anikó: *A média-értéklánc szerzői jogi vonatkozásai* (2012)
5. Koltay András (szerk.): *A mediaszabályozás két éve (2011–2012)* (2013)
6. Paál Vince (szerk.): *Magyar sajtószabadság és -szabályozás 1914–1989* (2013)
7. Horváth Attila: *A magyar sajtó története a szovjet típusú diktatúra idején* (2013)
8. Koltay András – Nyakas Levente (szerk.): *Összehasonlító médiajogi tanulmányok. A „közös európai minimum” azonosítása felé* (2014)
9. Dobos Ferenc – Megyeri Klára: *Nemzeti identitás, asszimiláció és médiahasználat a határon túli magyarság körében 2.* (2014)
10. Grad-Gyenge Anikó – Sarkady Ildikó: *Közös jogkezelés az audiovizuális médiában* (2014)
11. Apró István (szerk.): *Média és identitás* (2014)
12. Pruzsinszky Sándor: *Halhatatlan cenzúra* (2014)
13. Kóczián Sándor: *Gyermekevédelem a médiajogban* (2014)
14. Apró István – Paál Vince (szerk.): *A határon túli magyar sajtó Trianontól a XX. század végéig* (2014)
15. Kiss Zoltán – Szívi Gabriella: *A közszolgálati mediaszolgáltatás és a szellemi tulajdonjogok kapcsolódási pontjai és szabályozási környezete* (2015)
16. Dobos Ferenc: *A médiahasználat változása az erdélyi, felvidéki, kárpátaljai és vajdasági magyarság körében 2001–2014* (2015)
17. Grad-Gyenge Anikó: *Az audiovizuális archívumok szabályozási kerete – különös tekintettel a médiajogi és szerzői jogi rendelkezésekre* (2015)
18. Dobos Ferenc: *A médiahasználat változása az erdélyi, felvidéki, kárpátaljai és vajdasági magyarság körében 2001–2014/2* (2015)
19. Apró István (szerk.): *Média és identitás 2.* (2016)
20. Mezei Péter: *Jogkimerülés a szerzői jogban* (2016)
21. Koltay András – Andrej Školkay (Eds.): *Comparative media law practice: media regulatory authorities in the Visegrad countries: Vol. 1. Czech Republic and Slovakia* (2016)
22. Koltay András – Andrej Školkay (Eds.): *Comparative media law practice: media regulatory authorities in the Visegrad countries: Vol. 2. Poland and Hungary* (2016)
23. Makkai Béla: *Határon túli magyar sajtó – Trianon előtt* (2016)
24. Grad-Gyenge Anikó: *Film és szerzői jog – A megfilmesítési szerződés* (2016)
25. Köhidi Ákos: *Fájlcsere és felelősség* (2016)
26. Hajdú Dóra: *A törvény által előírt közös jogkezelés a magyar és a francia szerzői jogban* (2016)
27. Tóth J. Zoltán: *A büntetőjogi rágalalmazás és becsületsértés* (2017)
28. Kelemen Roland: *Az első világháború sajtójogi forrásai – Sajtójog a kivételes hatalom árnyékában* (2017)
29. Apró István (szerk.): *Határon túli magyar médiumok 2016* (2017)
30. Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről* (2018)

31. Kiss Zoltán Károly: *A kulturális tevékenységekre, valamint a médiaszolgáltatásra vonatkozó közteherviselési és jogdíjfizetési szabályok* (2018)
32. Merkovity Norbert: *A figyelemalapú politika a közösségi média korában* (2018)
33. Csapody Miklós: *Az „irányított nyilvánosság” és a „szerkezet megváltoztatása” Magyarországon* (2018)
34. Apró István (szerk.): *Média és identitás 3.* (2019)
35. Mák Ferenc: *Sajtó a Birodalom határán. Hírlapok és a nemzeti újjászületés a kiegyezés utáni Délvidéken* (2019)
36. Paál Vince: *Tanulmányok a magyar sajtószabadság történetéhez 1867–1944* (2019)
37. Kiss Zoltán Károly – Kiss Dóra Bernadett: *A vizuális művészetek és a jog – 1. A képzőművészet szabályozása* (2019)
38. Gálik Mihály – Csordás Tamás (szerk.): *A média gazdaságtanának kézikönyve* (2020)
39. Klestenitz Tibor: *Fejezetek az egyházi sajtó történetéből* (2020)
40. Klestenitz Tibor – Paál Vince (szerk.): *Médiatörténeti tanulmányok 2020* (2020)
41. Apró István (szerk.): *Média és identitás 4.* (2021)
42. Kiss Zoltán Károly: *A vizuális művészetek és a jog 2. Az építéset, a fotóművészet és az alkalmazott művészetek jogi szabályozása* (2021)
43. Apró István (szerk.): *Magyar médiaműhelyek a Kárpát-medencében* (2021)
44. Grad-Gyenge Anikó: *Egy modern szerzői jog* (2022) (Online kiadvány!)
45. Szadai Károly (szerk.): *VV10 – Egy valóságshow valósága* (2022)
46. Dobos Ferenc: *Isaurától az 5G-ig. A médiahasználat változása 2001 és 2021 között a határon túli magyarság körében* (2022)
47. Gyulay Dániel: *Becsület csorbitásának vizsgálata a tényállásszerű és jogellenességet nélkülöző cselekmények körében* (2023)
48. Paál Vince (szerk.): *Médiatörténeti mozaikok 2022* (2023)
49. Kiss Zoltán Károly: *A vizuális és az audiovizuális alkotók díjazása* (2023)
50. Farkas Ádám – Kelemen Roland: *Nemzeti biztonság és kibertér* (2024)
51. Szadai Károly (szerk.): *Szabályozott valóságkonstrukció – szerepek, normák, stratégiák a ValóVilág 11-ben* (2024)
52. Apró István (szerk.): *Média és identitás 5.* (2024)
53. Lendvai Gergely Ferenc – Papp János Tamás (szerk.): *Digitális Dilemmák – Fiatal kutatók válogatott tanulmányai a közösségi média egyes szabályozási kérdéseiről* (2025)
54. Borvendég Zsuzsanna – Paál Vince (szerk.): *A nyílt cenzúráról a szabadság illúziójáig – Propagandisták, ügynökök és ellenzékiek a Kádár-rendszer sajtóéletében* (2025)
55. Andok Mónika – Nyakas Levente (szerk.): *„A közvélemény vizsgálódását tehát azzal kell kezdenünk...” – Emlékkötet Walter Lippmann: Public Opinion című művének centenáriuma* (2025)
56. Tóth András – Koltay András (szerk.): *Influenszerek jogi kézikönyve* (2025)
57. Paál Vince – Sz. Nagy Gábor (szerk.): *Médiatörténeti mozaikok 2023* (2025)
58. Velegi Dorottya – Firniksz Judit: *Digitális gazdaság akadályok nélkül – Egyenlő esélyű hozzáférés a digitális piacokon* (2025)
59. Kiss Zoltán Károly: *A művészet, a jog és a tudomány metszéspontjai – Válogatott tanulmányok* (2025)
60. Schultz Márton: *Az információs szabadság magyarázata – A közérdekű adatok megismeréséhez és terjesztéséhez való jog alapintézményei és helye a kommunikációs alapjogok között* (2025)

61. Nyakas Levente (szerk.): *A média hatása a gyermekek pszichés fejlődésére* (2026)
62. Tóth Tamás: *Negatív kampányok, antielitizmus és népcentríkusság* (2026)
63. János Tamás Papp – Levente Nyakas (Eds.): *Understanding Online Disinformation. Concepts, Mechanisms, and Policy Responses* (2026)

Médiatudományi Intézet, Budapest
A kiadásért felel Nyakas Levente
Tördelő: Filei Nikoletta
Megjelent 12 (B/5) év terjedelemben, 300 példányban
Médiatudományi Könyvtár: ISSN 2063-5222
Médiatudományi Könyvtár 64.: ISBN 978-615-5302-61-9