

# Az online dezinformáció jogi kezelésének nemzetközi mintái az internet és az online média szabályozásában

VIKMAN LÁSZLÓ\*

A tanulmány célja áttekintést adni a dezinformáció elleni fellépési lehetőségekről az Európai Unió és az Egyesült Nemzetek Szervezete néhány kezdeményezésének és három EU-n kívül ország – a beavatkozás mértékében eltérő – szakpolitikai megközelítésének példáin keresztül. A véleménynyilvánítás és a sajtó szabadsága mint alapvető jog érvényesülése, az online médiumok mint gazdasági vállalkozások nagyrészt önszabályozó tartalomszűrése vagy a tartalomért viselt korlátozott felelőssége, valamint az online dezinformáció esetleges célpontjai, sértettjei érdekeinek kiegyensúlyozásakor az állami szabályozó komoly dilemmákkal szembesül. Fenntartható megoldást nemzetközi egyezmények, nemzeti szabályozási keretek, az online média- és sajtószabadság, a véleménynyilvánítás szabadsága mátrixában lehet megtalálni, úgy, hogy abban felelősséget vállal az állam mellett a média- és a techszektor, valamint a tartalomfogyasztó állampolgár is.

---

**Kulcsszavak:** dezinformáció, fake news, internetszabályozás, médiaigazgatás, közösségi média, a véleménynyilvánítás szabadsága

---

## *International practices in the legal approach of online disinformation in internet and online media regulation*

The aim of this paper is to provide an overview of the options for action against disinformation, using examples of some initiatives of the European Union and the United Nations and policy approaches in three non-EU countries, which vary in the degree of intervention. There are serious dilemmas for public regulators in balancing the interests of freedom of expression and freedom of the press as a fundamental human right, the largely self-regulatory content filtering or limited responsibility for content by online media as economic enterprises, and the potential targets and victims of online disinformation. A sustainable solution can be found in a matrix of international conventions, national regulatory frameworks, online media and press freedom, freedom of expression, where the responsibility is shared between the state, the media and tech sector and the content-consuming citizen.

---

**Keywords:** disinformation, fake news, internet regulation, media governance, social media, freedom of expression

---

---

\* Tudományos segédmunkatárs, Nemzeti Közszerzői Egyetem Hadtudományi és Honvédtisztviselői Kar; PhD-hallgató, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola; hivatásos tiszt, Magyar Honvédség.

## 1. Bevezetés

Az alapvető emberi jogokat tisztelőben tartó demokratikus államok igyekeznek tisztességes nyíltsággal kijelölni az emberek közötti kommunikáció tartalmi és formai tilalomfáit, mivel a szervezett társadalom egyik alappillérenek is tekinthető, szabad és valós tényeken alapuló párbeszéd elengedhetetlen a jogállami igazgatáshoz, gazdasághoz, kereskedelemhez, a békés társadalmi együttéléshez és a magánélethez egyaránt. A 21. századi infokommunikációs környezet összetett, sokszínű, sokcsatornás, igény szerint anonim működése, a hamisítást lehetővé tevő egyre olcsóbb és hatékonyabb eszközök (*deepfake* technológiák),<sup>1</sup> a mesterséges intelligencia egyes alkalmazásai, a felhasználókról rendelkezésre álló tömeges személyes adatok alapján skálázható, célozható és a modern marketing teljes repertoárját felvonultató befolyásoló dezinformációs kampányok a hétköznapijaink részei.<sup>2</sup> Ezek a kampányok mindenki számára szembetűnő formát és különösen kirívó mértéket a globális pandémia során értek el, ezzel 2020 környékén sok államot új szabályok megalkotására ösztönöztek.<sup>3</sup>

A közbeszéd, a közvélemény, az uralkodó narratíva, a figyelem és mindezek irányítása, terelése eddig is minden kiterjedt konfliktusos szituáció része volt a történelemben, azonban az internet, a számítógépek, a mindenhol elérhető távközlés és mobilkommunikáció, valamint a közösségimédia-platformok<sup>4</sup> precedens nélküli, államhatárokat, nyelvi korlátokat sem ismerő befolyást biztosítanak az üzeneteiket elég tervezetten és kitaróan közvetíteni kívánók számára. Márpedig a szereplők sokszínűsége sem igazán ismer határokat, hiszen állami és nem állami szereplők, a gazdasági és a nonprofit szféra, a közigazgatás és a civil társadalom szervezetei mind igyekeznek célzottan eljuttatni üzeneteiket a közönségükhöz, ezen keresztül reputációjukat, befolyásukat és hatókörüket növelve.<sup>5</sup>

Az igazmondás etikai parancsa, a ragaszkodás a tényekhez, az objektív valósághoz néha másodlagossá válhat fontosabbnak vélt értékek, célok miatt, aminek a következményei is sokfélék lehetnek a közlőtől, a hamisság mértékétől, a közönség méretétől és a torzítás okozta károktól függően, amire szélsőséges és káros esetekben a jognak – a jogalkotó által kezelendő mértékűnek értékelt hamisság esetén – az államiság kezdetei óta van eszközrendszere, léteznek kidolgozott válaszai. Egy korszerű jogrendszer többek közt az alkotmányos alapjogi szabadságjogok korlátaival (sajtószabadság, véleménynyilvánítás), a versenyjog (fogyasztók megtévesztése), a médiaigazgatás (terrorista tartalmak) és a reklámjog (gyermekvédelmi szempontból tiltott reklámok) szabá-

<sup>1</sup> Lásd GOSZTONYI Gergely – LENDVAI Gergely: Deepfake és dezinformáció. Mit tehet a jog a mélyhamisítással készített álhírek ellen? *Médiakutató*, 2024/1., <https://doi.org/10.55395/MK.2024.1.3>, 41–49.

<sup>2</sup> Lásd LUKÁCS Bence: Dezinformációs támadások társadalmi hatásai, lehetséges ellenintézkedések azonosítása. *Katonai Jogi és Hadijogi Szemle*, 2023/3–4., 52–64.; FALYUNA Nóra: Az online dezinformáció és hatásai – a dezinformációs hálózatok kialakulásának bemutatása a tudományos dezinformáció és az államtagadó összeesküvéselemletek kapcsolatán keresztül. *In Medias Res*, 2024/1., <https://doi.org/10.59851/imr.13.1.3>, 42–74.

<sup>3</sup> Lásd KISS Máté Attila: Álhírek büvöletében – a dezinformációk elleni fellépés kilátásai. *Nemzetbiztonsági Szemle*, 2021/2., 20–28., <https://doi.org/10.32561/nisz.2021.2.2>.

<sup>4</sup> Lásd INÁNCSI Máttyás: Közösségi média és dezinformáció. *Military and Intelligence Cybersecurity Research Paper*, 2023/7., 1–17.

<sup>5</sup> Lásd SELJÁN Péter: A jelen kiberbiztonsági fenyegetései és a jövő kihívásai – a nemzetállami aktorok tevékenysége és a dezinformációk terjedése. *Nemzet és Biztonság*, 2021/4., <https://doi.org/10.32576/nb.2021.4.2>, 41–65.

lyával, a büntetőjogban kriminalizált tényállásokban található korlátozásokkal (rágalmazás, rémhírterjesztés, gyűlöletbeszéd) igyekeznek a társadalmi kohézió és a köz érdekét szolgáló biztonságos és megbízható kommunikáció megőrzésére, az ezeket kikezdő tartalmak szűrésére.

Mindazonáltal a véleménynyilvánítás szabadságának és a sajtószabadságnak mint a társadalmi működés alapvető demokratikus jogainak korlátozása hatalmas felelősség, és bármely ezeket érintő újabb szabályozás – szolgálja bár a közrend, a közbiztonság és -nyugalom szintén magasztos céljait – ki kell állja a potenciálisan korlátozottak kritikáját és a jogállamiság tesztjeit. Ezeket az intézkedéseket alapos mérlegeléssel, az adott társadalom politikai kultúrájához, médiafogyasztási tudatosságához, médiakörnyezetéhez, veszélyeztetettségéhez igazítottan kell – az elérhető legnagyobb társadalmi konszenzus mellett – kodifikálni.

A jelen tanulmány második pontjában a hazánk szempontjából talán leginkább fontos két nemzetközi szervezet – az Európai Unió (EU) és az Egyesült Nemzetek Szervezete (ENSZ) – néhány intézkedésén keresztül mutatunk be olyan szakpolitikai és szabályozási irányokat, amelyek várhatóan formálják, meghatározzák majd a jelentős részben jogon túli aspektusai miatt nehezen megragadható dezinformáció elleni küzdelmet. A következő fejezetben három EU-n kívüli ország szabályozási megközelítéseit mutatjuk be, amelyek a szabályozás drasztikussága, az alkalmazható állami intézkedések vonatkozásában az enyhébb, a tudatosítást-nevelést előtérbe helyező megoldásoktól a komoly bírságokon át egészen a büntetőjogig terjednek. A célunk ezzel bemutatni egyrészt azt, hogy a kulturálisan és a jogrendszerükben is nagyon különböző országok számára univerzális probléma a kérdés definiálása, kezelése, másrészt azt, hogy milyen komoly feladat a jogalkotásban megragadni ezt a közbizalmat kikezdő jelenséget, amelynek értékelése, megítélése, azonosítása a gyakorlatban korántsem rutinszerű, kézenfekvő, és minden esetben alapvetően függ az ország biztonsági helyzetétől, fenyegetettségétől is. A negyedik fejezetben a dezinformáció védelmi-biztonsági vonatkozásait, valós fenyegetés jellegét mutatjuk be a capitoliumi lázadás esettanulmányként használható példáján keresztül, végül a jogalkotó mellett a társadalom és a techszektor felelősségére, szerepére térünk ki.

## 2. Az Európai Unió és az Egyesült Nemzetek Szervezete néhány kapcsolódó intézkedése

Az EU-ban<sup>6</sup> a digitális szolgáltatásokról szóló rendeletnek (DSA)<sup>7</sup> a nagy szolgáltatókra alkotott kockázatkezelési szabályozása már jól jelzi, hogy milyen irányvonalak várhatók az *acquis communautaire*-ben az online dezinformáció elleni küzdelemben, de a nemzeti szabályozások még

<sup>6</sup> Az európai szabályozás elemzését lásd például Marius DRAGOMIR – José RÚAS-ARAÚJO – Minni HOROWITZ: Beyond Online Disinformation: Assessing National Information Resilience in Four European Countries. 11(1) *Humanities and Social Sciences Communications* (2024), <https://doi.org/10.1057/s41599-024-02605-5>; MEZEI Kitti – SZENTGÁLI-TÓTH Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In CHRONOWSKI Nóra – SZENTGÁLI-TÓTH Boldizsár – SZILÁGYI Emese: *Demokrácia-dilemmák – alkotmányjogi elemzések a demokráciaelv értelméről az Európai Unióban és Magyarországon*. Budapest, ELTE Eötvös, 2022, 241–261.

<sup>7</sup> 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.



A jelentés szerint a dezinformáció fogalmának nincs általánosan elfogadott, egyértelmű meghatározása, közös értelmezése.<sup>13</sup> A kifejezést a nemzetközi távközlési unió (ITU) és az ENSZ Nevelésügyi, Tudományos és Kulturális Szervezete (UNESCO) 2020 szeptemberi jelentésében olyan hamis vagy félrevezető tartalmak leírására használta, amelyek konkrét károkat okozhatnak, függetlenül a motivációktól, a tudatosságtól vagy a viselkedéstől.<sup>14</sup> A főtítok szerint a véleménynyilvánítás szabadsága természetesen kiterjed a hatalom szempontjából kritikus beszédre is, beleértve a társadalmi normákat megkérdőjelező beszédet, a humor különböző formáit vagy akár a tévedés lehetőségét is ki. Azok a szabályozási megközelítések, amelyek egyszerű megoldásokat keresnek erre az összetett problémára, vagy szándékosan, vagy a komplex gondolkodás hiánya miatt az indokolt mértéken felül korlátozhatják a nemzetközi emberi jogi egyezmények által védett közlési formákat és tovább fokozhatják a meglévő társadalmi feszültségeket, a demokratikus intézményekkel szembeni bizalmatlanságot és az elidegenedést. A jelentésben mind az államok, mind a globális információcserében kulcsszerepet játszó technológiai cégek felé – a nemzetközi legjobb gyakorlatok figyelembevételével is – ajánlásokat fogalmaztak meg.<sup>15</sup>

Ez alapján az állampolgárok és a kormányaik közötti bizalom javítása érdekében az államok részéről célszerű lenne elismerni, hogy a dezinformáció elleni küzdelemhez elengedhetetlen egy olyan sokoldalú megközelítés, amely az emberi jogok, különösen a véleménynyilvánítás szabadságának védelmén és tiszteletben tartásán alapul. Erősíteni kellene a társadalom minden szintjén az inkluzivitást, és minimalizálni kellene a belső feszültségekhez vezető polarizáltságot, bevonva a civil társadalmat. Alapvető támasz lehet ebben a közérdekű információkhoz való hozzáférés erősítése, és az is, hogy az dezinformáció elleni állami intézkedéseket az alapvető emberi jogok keretein belül maradván (az általános tilalmak mellőzése, a korlátozások elismert jogos érdeket szolgáljanak és kiállják a szükségesség-arányosság tesztjét), átlátható és megismerhető módon, független felügyelet mellett hajtsák végre.

Az államoknak érdemes lenne ösztönözni a techcégeket tartalommoderálási politikáik és gyakorlatuk nyilvánosságra hozatalára, valamint arra, hogy ezek működtetése során végezzenek emberi jogi szempontok szerinti hatásvizsgálatokat és tegyék kutathatóvá – a felhasználók jogos érdekeinek tiszteletben tartása mellett – vonatkozó adataikat. Úgyszintén állami feladat a sokszínű és szabad médiakörnyezet védelme, az újságírók és a jogvédők tevékenységét is ideértve. Az akár köztisztviselőktől származó gyűlöletbeszédtől és dezinformációtól való tartózkodás mellett fontos tartózkodni az olyan intézkedések bevezetésétől is, amelyek megakadályozzák vagy megzavarják az információterjesztéshez való általános hozzáférést, online és offline, beleértve az internet leállítását. Végül fontos lenne befektetni olyan oktatási rendszerekbe, amelyek elősegítik a médiáról és az információról való kritikus gondolkodást, valamint a digitális írástudást, többek között a civil társadalommal és a tudományos körökkel való együttműködés révén, hogy az egyéneknek eszközöket biztosítsanak az információk és a források azonosításához és értékeléséhez.

<sup>13</sup> Az EBESZ hasonló anyagához lásd Andrey RIKHTER: *International Law and Policy on Disinformation in the Context of Freedom of the Media*. Wien, OSCE, 2021.

<sup>14</sup> Kalina BONTCHEVA – Julie POSETTI (szerk.): *Balancing Act: Countering Digital Disinformation while Respecting Freedom of Expression*. International Telecommunication Union, Geneva, 2020, <https://bit.ly/3ZuKOzS>.

<sup>15</sup> Report of the Secretary General (12. lj.) 17–18.

A jelentés az államok mellett a globális információáramlásban központi szerepet játszó, kontinenseken átívelő befolyással bíró<sup>16</sup> média- és technológiai vállalkozások szerepét felismerve ezek vonatkozásában is fontos irányelveket fogalmaz meg.<sup>17</sup> A cégeknek nyilvánosságra kellene hozniuk a dezinformáció elleni küzdelemmel kapcsolatos politikáikat és gyakorlatukat (például eltávolítás, címkézés, fiókok felfüggesztése, demonetizáció és a tartalom erősítésmentesítése), és részletes tájékoztatást kellene nyújtaniuk arról, hogy ezeket az intézkedéseket földrajzi területekre és nyelvekre lebontva hogyan hozzák meg, ahogyan biztosítaniuk kellene hatásuk független nyomon követését és mérését is. Szükség lenne arra is, hogy nyilvánosan számoljanak be a dezinformáció terjedésével kapcsolatos tartalommal vagy adatokkal kapcsolatos kormányzati megkeresésekről, ezzel biztosítva az átláthatóságot, amit erősítene az összegyűjtött és felhasznált felhasználói adatokkal kapcsolatos adatok közzététele is, különös tekintettel a politikai hirdetésekre és a kapcsolódó finanszírozásra.

A techcégeknek a platformjaikon hatékonyabban kellene fellépniük az összehangolt támadásokkal szemben, beleértve a kritikus hangokat és az újságírókat célzó támadásokat is, ezek kapcsán be kellene számolniuk a nyilvánosságnak, különösen a kulcsfontosságú politikai események, például a választási időszakok, a béketárgyalások, a tiltakozó megmozdulások vagy a globális összejövetelek idején. Szintén a prudens működésük igazolása érdekében sokat jelentene, ha hozzáférést biztosítanának a kutatók számára a releváns adataikhoz és információikhoz, hogy a szakértők megérthessék a dezinformációval kapcsolatos dinamikákat és megalapozottan tájékoztathassák a bizonyítékokon alapuló szakpolitikákat. Működésük során független panasz-felülvizsgálati mechanizmusokat és a felhasználók számára hatékony jogorvoslati lehetőségeket kell biztosítaniuk, továbbá kellő gondossággal kell eljárniuk a termékeik, a politikáik és a működésük hatásaival kapcsolatban, többek között emberi jogi hatásvizsgálatok elvégzésével, független felülvizsgálók bevonásával és üzleti modelljeik felülvizsgálatával. Fontos lenne, hogy kellő figyelmet fordítsanak az államok közötti potenciális emberi jogi hatásokra, és biztosítsák, hogy a dezinformációs politikák végrehajtása következetes és kellő erőforrással ellátott legyen a működésük szerinti államokban azért, hogy az ilyen politikák a helyi nyelvekre és kontextusokra reagáljanak.

### 3. Néhány Európai Unió kívüli ország szakpolitikai intézkedései

Az egyes országok dezinformáció ellen hozott intézkedéseiről több áttekintő projekt keretében is készült már összegzés és adatbázis,<sup>18</sup> amelyekből az egyes országok tevékenységei nagy vona-

<sup>16</sup> Elrettenítő példa erre a befolyásra a 2017-es mianmari vérengzés, amelyek során a rohingya népcsoport elleni gyűlölködő tartalmak hatását a Facebook algoritmusai sokszorozta meg, ezzel jelentős mértékben hozzájárulva a bekövetkezett vérengzésekhez és több mint 700 ezer ember kényszerű meneküléséhez, lásd *Myanmar: Facebook's systems promoted violence against Rohingya; Meta owes reparations – new report*, Amnesty International, 2022, <https://bit.ly/4ipZckD>.

<sup>17</sup> Report of the Secretary General (12. lj.) 19.

<sup>18</sup> Lásd *A guide to anti-misinformation actions around the world*, <https://bit.ly/3CNvplf>; *Law and Disinformation in the Digital Age. A Project of the Georgetown University Law Center Global Law Scholars*, Georgetown, 2022, <https://bit.ly/4g4zqRn>.

lakban megismerhetők. Mindezek áttekintésére a jelen keretek közt nincs lehetőség, de három ország konkrét szabályozási példája – a *soft* eszközöket alkalmazóktól a súlyosabb szankciókkal fenyegető megközelítésekig – kellően cizellált képet adhat a szabályozási opciókról, azok fogadtatásáról és esetleges korlátairól az egyes megközelítések, perspektívák és sajátos problémákra adott nemzeti válaszok alapján.

### 3.1. Nagy-Britannia

Nagy-Britanniában 2021 júliusában széles körű stratégiát jelentettek be az online dezinformáció ellen (Online Media Literacy Strategy).<sup>19</sup> A brit médiahatóság, az Office of Communications (Ofcom) adatai szerint a felnőtt internetezők 40%-a nem rendelkezik az online tartalmak kritikus értékeléséhez szükséges készségekkel. A 15 éves kor alatti gyermekek különösen veszélyeztetettek: mindössze 2%-uk rendelkezik az ahhoz szükséges kritikai gondolkodással, hogy megkülönböztesse a tényeket és a fikciókat az interneten.

A stratégia keretében a brit tanárok, könyvtári dolgozók, ifjúságsegítők és gondozók médiatudatossági képzése (Train the Trainer program) segítheti a fellépést az online dezinformáció elleni küzdelemben.<sup>20</sup> A résztvevőket felkészítik arra, hogy megtanítsák másoknak megérteni, hogyan működik az online környezet, beleértve azt is, hogyan születnek, működnek és fizetnek az online hírcikkek és a közösségi médiában megjelenő posztok és hogyan elemazzék kritikusan az általuk fogyasztott tartalmakat.

A következő lépés a 2023 folyamán elfogadott Online Safety Act volt,<sup>21</sup> amely az uniós DSA-val párhuzamosan alakult ki. A törvény hatálya alá tartozó szolgáltatóknak intézkedéseket kell bevezetniük annak megakadályozására, hogy szolgáltatásaikat illegális tevékenységre használják, valamint a megjelenő illegális tartalmak eltávolítására. Az új norma kategorizálja az online tartalomszolgáltatókat, ahol az 1. kategória a legtöbb kötelezettséggel járó, gyakorlatilag a globális elérésű vállalkozások szintje, amelyeknek a saját maguk által megalkotott szűrési szabályok, felhasználási feltételek mentén kell eltávolítani a legális, de nem kívánt, valamint a káros tartalmakat, ezzel elkerülve a kormányzati cenzúrát. Ebben a kategóriában szintén kötelező a felhasználók számára olyan eszközök biztosítása, amelyek lehetőséget adnak az őket elérő tartalmak meghatározására (ideértve más felhasználók blokkolását is). A törvény kimondottan tiltó szabályait az illegális tartalmak elleni küzdelem és gyermekvédelmi szempontok alapján határozták meg, az Ofcom pedig kifejezetten a dezinformációval foglalkozó tanácsadó testületet hoz létre, amely várhatóan a kérdéses helyzetek mérlegelésében kap majd szerepet.

A Center for Strategic and International Studies értékelése szerint a tartalomszűrésnek a szolgáltatókra telepítésével a brit megoldás a digitális platformokra – és nem egy kormányzati végrehajtó szervre – hárítja a felelősséget a konkrét tartalmak megjelöléséért vagy eltávolításáért.<sup>22</sup> Mivel a tartalommoderálás eseti döntés a nagyon különböző típusú kifejezések és kontextusok között, az Ofcom számára valószínűleg nehéz lesz objektíven megállapítani, hogy a

<sup>19</sup> *Minister launches new strategy to fight online disinformation*, 2021, <https://bit.ly/49atRy3>.

<sup>20</sup> *Online Media Literacy Strategy. Policy paper*, 2021, <https://bit.ly/3COKtzn>.

<sup>21</sup> *Online Safety Act 2023*, <https://bit.ly/4ieaGHy>.

<sup>22</sup> *The United Kingdom's Online Safety Bill Exposes a Disinformation Divide*, 2022, <https://bit.ly/3CS6Zr1>.

vállalatok következetesen alkalmazzák-e a szolgáltatási feltételeiket – a félretájékoztatás és a dezinformáció esetében pedig mind a kormányzat, mind a digitális platformok elkerülhetetlenül szembesülnek majd erősen szubjektív helyzetekkel.

### 3.2. Ausztrália

Az ausztrál megközelítés szintén az ön- és az állami szabályozás sajátos keveréke. Az illetékes hatóság (Australian Communications and Media Authority, ACMA)<sup>23</sup> felügyeli a Digital Industry Group (DIGI) elnevezésű ausztrál iparági szervezet által kidolgozott gyakorlati kódex megvalósulását.<sup>24</sup> Azonban az állam is tett lépéseket: a Combatting Misinformation and Disinformation Bill törvénytervezet társadalmi egyeztetése tavaly június és augusztus között lezajlott, és jelenleg második körben tárgyalja a parlament.<sup>25</sup> A törvényjavaslat hatáskörrel ruházná fel az ACMA-t arra az esetre, ha a félretájékoztatás és a dezinformáció elleni küzdelemben az iparág erőfeszítései nem lennének megfelelők. A javasolt hatáskörök lehetővé tennék a hatóság számára, hogy

- információkat gyűjtsön a digitális platformszolgáltatóktól, továbbá megkövetelje, hogy a félretájékoztatással és a dezinformációval kapcsolatos ügyekről bizonyos nyilvántartásokat vezessenek;
- felkérje az iparágot, hogy dolgozzon ki a digitális platformokon történő félretájékoztatás és dezinformáció elleni küzdelemre vonatkozó gyakorlati kódexet, amelyet az ACMA nyilvántartásba vehetne és érvényesíthetne;
- a szabályozás erősebb formáját: ágazati szabványt hozzon létre és érvényesíthessen, ha a gyakorlati kódex nem bizonyulna hatékonynak a digitális platformokon történő félretájékoztatás és dezinformáció elleni küzdelemben.

A törvényjavaslat a következő fogalom meghatározásokat használja:

- a félretájékoztatás olyan hamis, félrevezető vagy megtévesztő online tartalom, amelyet a megtévesztés szándéka nélkül osztanak meg vagy hoznak létre, de az súlyos károkat okozhat vagy hozzájárulhat azokhoz;
- a dezinformáció olyan félretájékoztatás, amelyet szándékosan, megtévesztés vagy súlyos károkozás szándékával terjesztenek;
- a súlyos kár olyan kár, amely az ausztrál lakosság, gazdaság vagy környezet jelentős részét érinti vagy aláássa az ausztrál demokratikus folyamat integritását.

Az ACMA-nak nem lesz hatásköre arra, hogy konkrét tartalmak vagy bejegyzések eltávolítását kérje a digitális platformok szolgáltatásairól. A kódex és a szabványalkotási hatáskörök nem vonatkoznak az engedélyezett választási, népszavazási, valamint más típusú tartalmakra, például a szakmai hírekre, és az azonnali üzenetküldő szolgáltatásokon küldött magánüzenetek és a satíra szintén kivételt képeznének.

<sup>23</sup> ACMA: Online misinformation, <https://bit.ly/4g9dWCq>.

<sup>24</sup> DIGI: Disinformation Code, <https://bit.ly/3Oxpeo2>.

<sup>25</sup> Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023. Fact sheet, <https://bit.ly/3VeA6uY>.



Az információgyűjtési és nyilvántartási szabályok, kódexek vagy szabványok be nem tartása esetén a hatóság többféle hivatalos végrehajtási intézkedés közül választhat. Ezeket az intézkedéseket általában fokozatosan, az okozott kártól vagy a kár kockázatától függően alkalmaznák (szélsőséges esetben akár súlyos pénzbírságot is). Büntetőjogi szankciók csak azokra a digitális platformokra vagy egyénekre vonatkoznának, amelyek vagy akik a nyilvántartás vezetésére vonatkozó rendelkezések alapján tudatosan hamis vagy félrevezető nyilvántartást vezetnek vagy tartanak fenn, vagy hamis vagy félrevezető információt adnak.

A tervezet aránylag szofisztikált megközelítése ellenére komoly kritikákat kapott az ausztrál emberi jogi bizottságtól.<sup>26</sup> Jelenlegi formájában az előzetes törvénytervezet azzal a kockázattal jár, hogy aránytalanul nagy terhet ró a véleménynyilvánítás szabadságára. Azon túlmenően, hogy a félretájékoztatás és a dezinformáció fogalmát nehezen megragadhatónak és némiképp önkényesnek érzik, kulcsfontosságú, hogy megtalálják a megfelelő egyensúlyt az ezek elleni küzdelem és a véleménynyilvánítási szabadság védelme között. Miközben egyértelműen szükség van az online félretájékoztatás és dezinformáció elleni küzdelemre, fennáll annak a veszélye, hogy a különböző nézőpontok és ellentmondásos vélemények célkeresztbe kerülnek. Lehetnek eltérések abban, hogy pontosan hol kell meghúzni a határt, de szilárd garanciák nélkül maguk a dezinformáció elleni intézkedések is veszélyeztethetik a demokráciát és a demokratikus értékeket. A félretájékoztatás és a dezinformáció elleni küzdelmet célzó bármilyen törvénynek az emberi jogok köré kell épülnie, és szilárd átláthatósági és ellenőrzési biztosítékokat kell tartalmaznia, emellett intézkedéseket kell tenni a digitális kultúra és ellenállóképesség szintjének emelésére a felhasználók körében.

### 3.3. Törökország

Törökország szakértői értékelések szerint rendkívüli mértékben kitett a dezinformációnak, aminek az egyik oka, hogy az elitek kommunikációs eszközként tekintenek rá a társadalmi folyamatok uralása érdekében, ezzel egyébként felértékelve a külföldi médiát mint tájékoztatói forrást.<sup>27</sup> 2022 október elején a török parlament elfogadott egy javaslatot a dezinformáció elleni küzdelem jegyében, amelyet az elnök október 18-án alá is írt. A büntető törvénykönyv módosításának kritikusi szerint a szövegezés nem volt elég egyértelmű, így elfogadása alkalmas lehet a véleménynyilvánítás szabadságának aránytalan korlátozására. A PACE Monitoring Bizottság még a tervezet elfogadása előtt felkérte az Európa Tanács emberi jogokért felelős szaktestületét, a Velencei Bizottságot, hogy készítsen véleményt a tervezetről. A bizottság „sürgős véleménye”<sup>28</sup> szerint az új 217/A § bünteti azokat a személyeket, akiket nyilvánosan „hamis vagy félrevezető információk” terjesztésében bűnösnek találunk, egy és három év közötti börtön

<sup>26</sup> Australian Human Rights Commission: *Finding balance: combatting misinformation and disinformation without threatening free expression*, <https://bit.ly/3Veyhhy>.

<sup>27</sup> PÉNZVÁLTÓ Nikolett: *Dezinformáció és külső információs befolyás Törökországban*. Stratégiai Védelmi Kutatóintézet Elemzések, 2019, <https://bit.ly/3Bh3Xfg>.

<sup>28</sup> Türkiye – Comments submitted by the Turkish authorities on 6 October 2022 regarding the draft urgent joint opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft amendments to the Penal Code regarding the provision on „false or misleading information”, Velencei Bizottság, 2022, <https://bit.ly/3AUcCo1>.

tönbüntetéssel sújtaná őket, ami a büntetési tétel felével növelhető azok esetében, akik eltitkolják személyazonosságukat vagy egy szervezet nevében járnak el. A rendelkezés bármely személyre vonatkozik, legyen az újságíró, politikus, aktivista, szakmabeli vagy állampolgár. A rendelkezés egyének csoportjaira is vonatkozik (szervezetekre, médiaorgánumokra, online platformokra vagy más közvetítőkre).

A Velencei Bizottság – elismerve a dezinformáció mint súlyos probléma jelentőségét – megállapította, hogy a rendelkezés az Emberi Jogok Európai Egyezménye 10. cikkében szabályozott véleménynyilvánítási szabadságba ütközik, és azt az álláspontot fogalmazta meg, hogy sokkal pontosabban kell meghatározni a törvény alkalmazási körét. Korábbi ajánlásaival összhangban megőrzendő értékként jelölte meg az interneten az anonimitáshoz való jog megerősítését és védelmét, a felhasználók személyes adatainak védelmét, valamint hozzáférési lehetőségeiket a szolgáltatók által róluk kezelt információkhoz. Rámutatott, hogy a kriminalizációhoz képest alternatív intézkedések is eredményeket érhetnek el a dezinformációval szemben, és kétségesnek értékelte, hogy ilyen drasztikus büntetőjogi válasza lenne szükség.

Egy gazdasági szempontú értékelés szerint a törvény szigorítja a közösségimédia-platformok és az online híroldalak ellenőrzését.<sup>29</sup> Ezenkívül súlyosan érinti a véleménynyilvánítási szabadságát Törökországban, és az ország már amúgy is csökkenő demokratikus hitelét jelzi, ami gazdasági következményekkel is járhat, mivel a kis- és a középvállalkozások a tevékenységük során nagymértékben támaszkodnak a közösségimédia-platformokhoz való zavartalan hozzáférésre, és ez a jogszabály mindegyiket érintheti. Ugyanez vonatkozik a társadalom egészére is, mivel Törökországban a digitalizáció igen magas fokon áll. A digitális trendeket nyílt forrású adatokon keresztül tanulmányozó Kepios cég 2022-es tanulmánya szerint a török lakosság 82%-a kapcsolódik az internethez, és átlagosan napi nyolc órát tölt online, ami meghaladja a hétórás globális átlagot. Ez természetesen egyrészt nagy kitettséget jelent a sok potenciális „célpont” miatt, másrészt a drákói szabályozás tömeges kriminalizációhoz vezethet.

#### 4. Esettanulmány a dezinformáció védelmi-biztonsági jelentőségéről

Az ellenfél ellenállásának megtörésére, a hátország támogatásának gyengítésére a rémhírek, megtévesztő információk terjesztése a hadviseléssel egyidős eszköz. Megjelenési formái, közvetítői csatornái, kifinomultsága és célzott jellege a rendelkezésre álló kommunikációs technológiákkal együtt szintén fejlődött. „Rendszertanilag” az alkalmazása és az elhárítása szempontjából is leginkább nemzetbiztonsági, titkosszolgálati feladat, bár tény, hogy nem mindig egyszerű elhatárolni a rokon – sőt „összefgyvernemi” szemlélettel komplementer – területnek tekinthető kognitív és pszichológiai hadviseléstől és a stratégiai kommunikációtól. Ezekről nem feltétlenül az eszköztára – napjainkban leginkább, de nem kizárólagosan a kiberműveletek alkalmazása – különbözteti meg, hanem közvetített üzenetének a valóságtól eltérő, torzított, manipulált tartalma.

<sup>29</sup> *Turkey's New Disinformation Law Affects More Than Meets the Eye*, 2022, <https://bit.ly/3Zxw963>.

A 21. századi biztonsági környezet kihívásainak leírására jellemzően használt hibrid fenyegetések<sup>30</sup> fogalomkörében kiemelt szerepet játszó, katonai kifejezéssel „nem kinetikus” módszer a felmerült költségekhez képest nagy hatások kiváltására lehet képes. Közvetlen attribúcióját az esetleg beazonosítható elkövetők affiliációjának letagadhatósága teszi nehezzé, így kívánatos megoldás lehet az ellenérdekelt állam belső stabilitásának bomlasztására álhírek terjesztésével (például választási manipulációkról) vagy meglévő belső feszültségek felkorbácsolására, azok kihasználására.<sup>31</sup>

Esettanulmányként felhozhatók a 2021. január 6-án Washingtonban történt események. Ezen a napon online szerveződő, különböző internetes felületeken és alkalmazásokon egymással közös véleménybuborékba kerülő emberek tömegei (sokan az alkotmányos fegyverviseléshez való jogukat is demonstratívan gyakorolva) jelentek meg a washingtoni Fehér Házhoz közel több helyszínen. A gyűléseket és a nyugtatóknak nem nevezhető beszédeket követően a rendezvények feletti kontroll kicsúszott a szervezők kezéből, az irányítás megszűnt, és zavargások alakultak ki a Capitoliumnál, több halott és rengeteg sérült áldozattal. Donald Trump elnök és a zavargásokban, rongálásokban, erőszakos cselekményekben tevőlegesen is részt vevő – és a rengeteg videó- és fényképfelvétel segítségével tömegesen azonosított – személyek ellen jelenleg is eljárások folynak.

Az eseményekhez vezető utat a kibertérben az Amerikai Egyesült Államokban alapított, de globális aktivista civil szervezet, az Avaaz vizsgálta, arról részletes jelentést készített, amelyben ajánlásokat is megfogalmazott.<sup>32</sup> Vizsgálata szerint a Facebook kb. 10,1 milliárd dezinformációs hír és egyéb tartalom egyéni megtekintését akadályozhatta volna meg a 2019. október (havi 97 millió) és 2020. október (havi 278 millió) közötti időszakban. Ez a milliárdos nagyságrendű forgalom, felhasználói elérés az Egyesült Államok top 100 médiaszervezetének (online, elektronikus és hagyományos médiumok) hírforgalma szempontjából is jelentősnek minősíthető. A QAnon, a Stop the Steal, a Boogaloo, a Proud Boys milícia és más csoportok és kapcsolódó oldalak közül 267-et azonosítottak, ezek 32 millió követőt értek el. A Facebook saját deklarált szabályainak megsértése ellenére ezek közül 118 oldal elérhető volt a tanulmány publikálásakor is, 27 millió követővel. Egy 2020. októberi felmérés szerint a regisztrált választók 44%-a találkozott a postán beküldött szavazatokra vonatkozó top 100 legnépszerűbb félrevezető történettel. Ezek negyedét a Facebook nem is jelölte hamisként, pedig akkor már együttműködött tényellenőrző szervezetekkel.

<sup>30</sup> Lásd BERTALAN Dávid: A hibrid hadviselés és az álhírek néhány összefüggése. *Felderítő Szemle*, 2019/3., 23–38.; HÉREGI Erika: Információs műveletek mint a hibrid hadviselés eszközei. *Felderítő Szemle*, 2019/3., 187–202.; DOBÁK Imre: A dezinformáció – napjaink kiemelt kihívása. *Katonai Jogi és Hadijogi Szemle*, 2020/1., 93–124.; KELEMEN Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog – Állam – Politika*, 2021/3., 76.; FARKAS Ádám – KELEMEN Roland: *Nemzeti biztonság és kibertér*. Budapest, Média tudományi Intézet, 2023, 44.

<sup>31</sup> Lásd Sebastian BAY: Countering Hybrid Threats to Elections: From Updating Legislation to Establishing Collaboration Networks. *Hybrid CoE Research Report 12*, Helsinki, Hybrid COE, 2024, <https://bit.ly/3D2CMW0>; Jon HASSAIN: *Disinformation in Democracies: Improving Societal Resilience to Disinformation*. Riga. NATO StratCom COE, 2022, <https://bit.ly/3ZfmuR8>.

<sup>32</sup> Facebook: From Election to Insurrection, 2021, <https://bit.ly/415vz1F>.

Az Avaaz a jelentésében az alábbi fontosabb javaslatokat tette:

- a közösségi oldalak működésének transzparenciáját biztosító szabályozásra van szükség;
- a közösségi médiumok tartalomirányítását szabályozó algoritmusokat rendszeresen „detoxikálni” kell a fogyasztói érzelmek felkorbácsolásának elkerülése érdekében;
- meg kell teremteni a valós, tényleges és hatékony helyreigazítás lehetőségét;
- meg kell reformálni a tartalomszolgáltatók felelősségi szabályait (Communications Decency Act 1996, 230. cikk<sup>33</sup>);
- nemzeti dezinformáció elleni stratégiát kell kiadni;
- kormányzati felelőst kell kijelölni a kormányzati ellenlépések koordinációjára;
- együtt kell működni az EU-val.

## 5. Összegzés

Az Európai Unió törekvésein, az ENSZ-jelentésen és a három ország szabályozási példáján keresztül látható, hogy a félretájékoztatás és a dezinformáció visszaszorítása szabályozási eszközökkel nem leegyszerűsítendő feladat. Mivel egy közzétett tartalom, információ gyakran tűnhet tévedésnek, tartalmazhat részigazságokat vagy tényleges tévedéseket, általános szabályok segítségével a szándékos manipuláció, ferdtítés, torzítás nem mindig azonosítható egyértelműen. Az eddigi jogi megoldások kritikussai a szabadságjogok védelmében fellépve természetesen jogosan követelik a szabályozás egzaktságát, átláthatóságát és értelmezhetőségét, hiszen egy tág, absztrakt definíció – szigorú szankciórendszerrel párosítva – jogosan ébreszt aggodalmakat a demokratikus működés egyik garanciális alapjának tekinthető véleménynyilvánítási szabadság érvényesülésével kapcsolatban.

Felhozhatók érvek a gazdasági szempontok védelmére is. Egy totális szolgáltatói szűrési felelősséget hangsúlyozó, büntetőjogi megoldásokat is felvonultató megközelítés drasztikusan korlátozhatná az érintett szolgáltatásokat, áttérve a felhasználókat kevésbé restriktív joghatóság alatt működő szolgáltatókhoz, ezzel a saját médiagazdaságnak károkat okozva, és a globális internetnek köszönhetően – totális tiltás és blokkoló cenzúra hiányában – nem is feltétlenül elérve a kívánt célt. A határokon átlépő platformok, globális médiavállalkozásnak tekinthető tartalomszolgáltatók vonatkozásában külön nehézséget jelent,<sup>34</sup> hogy számos ország előírásainak kell megfelelniük, liberális demokráciák és autokratikusabb berendezkedésű államok szabályozásainak egyaránt.

Talán ritkábban merül fel érvként, hogy nem csak politikai okai lehetnek annak, hogy egy kormány szabályokat alkotna az interneten megjelenő tartalmak vonatkozásában. Bizton-

<sup>33</sup> Az 1996-os Communications Decency Act 230. cikke korlátozza a közvetítő szolgáltatók felelősségét a harmadik felek által közzétett tartalmakért, nem helyez rájuk szerkesztői felelősséget. A felhasználói figyelmet maximalizáló ajánló algoritmusok használata a különböző platformokon egyre inkább kikezdi ezt a kimentési lehetőséget, ami már több Legfelsőbb Bíróság is eljutó per és törvénymódosítási javaslat tárgya is volt. Lásd Congressional Research Service: Section 230: An Overview, 2024, <https://bit.ly/4gtjkAz>; A Final Bow for Section 230? Latest Plea for Reform Calls for Sunset of Immunity Law. *New Media and Technology Law Blog*, 2024, <https://bit.ly/4g6e12S>.

<sup>34</sup> How to Regulate Misinformation. *The Royal Society Blog*, 2022, <https://bit.ly/4f1mJFC>.

sági szempontból nem hagyhatók figyelmen kívül azoknak az érdekei sem, akiknek az online közegben visszaélnék a személyes adataival, fénykép-, hang- vagy videófelvevételeivel (*doxing*, a zaklatás különböző formái), vagy azoké, akiket súlyosan fenyegetnek vagy kiszorítanak a nyilvánosságból – ideértve a gyerekeket, a nőket, az etnikai, a vallási vagy más kisebbségeket.<sup>35</sup>

Létezik olyan tudományos álláspont,<sup>36</sup> amely kifejezetten javasolja a jogi definíció kerülését, és szakpolitikai céllal határozná meg a dezinformációt: 1. hamis, 2. meghatározott szándékkal terjesztett információ, 3. amely valamely közérdekű károkozásra irányul. Ez kiegészíthető a terjesztés módszerével, csatornáival (például MI, algoritmusok), a platformok fontos szerepének egyértelművé tételével. Nem meglepő, hogy egy ilyen komplex közegben nem csupán a definíciós kihívások miatt támaszkodik több ország is az önszabályozásra, mivel ezzel az állam eltolja magától a cenzúra végrehajtását. Ez a szabályozási logika az Egyesült Államok liberalizált gazdaságára és az internet korai időszakára abszolút jellemző. Ahogy Daniel Rogers, a Global Disinformation Index társalapítója helyesen mutat rá,<sup>37</sup> az online tartalomszolgáltatói felelősség globális mintájaként az amerikai 1996-os Communications Decency Act 230. cikk c) bekezdés (1) pontja szolgált: „Egyetlen interaktív számítógépes szolgáltatás szolgáltatója vagy felhasználója sem tekinthető egy másik információs tartalomszolgáltató által nyújtott információ kiadójának vagy előadójának.” A mai online médiaműködést ismerve ez a modell aligha tartható fenn hosszú távon, a felhasználó ízlésére, figyelmének megkötésére koncentráló és ezzel véleménybuborékokat kialakító platformok már nem sokáig tehetnek úgy, mintha semmi közük nem lenne a társadalmi polarizációhoz, az elidegenedéshez vagy az erre hajlamos egyének esetében a negatív pszichológiai következmények kialakulásához.

Az online média komplex közegében a tartalomszabályozás és ezen belül a dezinformáció elleni küzdelem akkor hozhat eredményeket, ha az erre kialakított nemzeti stratégiában az állam mint szabályozó (amely inkább mozgásteret ad, és csak szélsőséges esetekben tilt), a közgazgatás mint hatóság (amely felügyel, monitoroz, tanácsot ad, és csak szükség esetén büntet), a platformok és a technológiai vállalkozások mint szolgáltatók (amelyek társadalmi és mentálhigiénés szempontokat is mérlegelnek a profitmaximalizálás mellett) és a fogyasztók is mint befogadók (akik növelik saját médiatudatosságukat) felelősséget vállalnak, és a saját eszközeikkel fellépnek a negatív tendenciák ellen.

<sup>35</sup> *European Tech Law Faces Test to Address Interference, Threats, and Disinformation in 2024 Elections*. Council of Foreign Relations, 2024, <https://bit.ly/417Vaa3>.

<sup>36</sup> Ronan Ó FATHAIGH – Natali HELBERGER – Naomi APPELMAN: The Perils of Legally Defining Disinformation. 10(4) *Internet Policy Review* (2021), <https://doi.org/10.14763/2021.4.1584>.

<sup>37</sup> Disinformation Is among the Greatest Threats to Our Democracy. Here Are Three Key Ways to Fight It. *Time*, 2021; <https://bit.ly/3Zem39H>.

<sup>38</sup> 47 U.S. Code § 230 – Protection for private blocking and screening of offensive material.

## Irodalomjegyzék

- BAY, Sebastian: Countering Hybrid Threats to Elections: From Updating Legislation to Establishing Collaboration Networks. *Hybrid CoE Research Report 12*, Helsinki, Hybrid COE, 2024, <https://bit.ly/3D2CMW0>
- BERTALAN Dávid: A hibrid hadviselés és az álhírek néhány összefüggése. *Felderítő Szemle*, 2019/3., 23–38.
- BONTCHEVA, Kalina – POSETTI, Julie (szerk.): *Balancing Act: Countering Digital Disinformation while Respecting Freedom of Expression*. International Telecommunication Union, Geneva, 2020, <https://bit.ly/3ZuKOzS>.
- DOBÁK Imre: A dezinformáció – napjaink kiemelt kihívása. *Katonai Jogi és Hadijogi Szemle*, 2020/1., 93–124.
- DRAGOMIR, Marius – RÚAS-ARAÚJO, José – HOROWITZ, Minni: Beyond Online Disinformation: Assessing National Information Resilience in Four European Countries. 11(1) *Humanities and Social Sciences Communications* (2024). <https://doi.org/10.1057/s41599-024-02605-5>
- FALYUNA Nóra: Az online dezinformáció és hatásai – a dezinformációs hálózatok kialakulásának bemutatása a tudományos dezinformáció és az államtagadó összeesküvéselemletek kapcsolatán keresztül. *In Medias Res*, 2024/1., 42–74. <https://doi.org/10.59851/imr.13.1.3>
- FARKAS Ádám – KELEMEN Roland: *Nemzeti biztonság és kibertér*. Budapest, Médiatudományi Intézet, 2023.
- GOSZTONYI Gergely – LENDVAI Gergely: Deepfake és dezinformáció. Mit tehet a mélyhamisítással készített álhírek ellen? *Médiakutató*, 2024/1., 41–49. <https://doi.org/10.55395/MK.2024.1.3>
- HASSAIN, Jon: *Disinformation in Democracies: Improving Societal Resilience to Disinformation*. Riga. NATO StratCom COE, 2022, <https://bit.ly/3ZfmuR8>.
- HÉREGI Erika: Információs műveletek mint a hibrid hadviselés eszközei. *Felderítő Szemle*, 2019/3., 187–202.
- INÁNCSI Mátyás: Közösségi média és dezinformáció. *Military and Intelligence Cybersecurity Research Paper*, 2023/7., 1–17.
- KELEMEN Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog – Állam – Politika*, 2021/3., 71–85.
- KISS Máté Attila: Álhírek büvöletében – a dezinformációk elleni fellépés kilátásai. *Nemzetbiztonsági Szemle*, 2021/2., 20–28. <https://doi.org/10.32561/nsz.2021.2.2>
- LUKÁCS Bence: Dezinformációs támadások társadalmi hatásai, lehetséges ellenintézkedések azonosítása. *Katonai Jogi és Hadijogi Szemle*, 2023/3–4., 52–64.
- MEZEI Kitti – SZENTGÁLI-TÓTH Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In CHRONOWSKI Nóra – SZENTGÁLI-TÓTH Boldizsár – SZILÁGYI Emese: *Demokrácia-dilemmák – alkotmányjogi elemzések a demokráciaelv értelméről az Európai Unióban és Magyarországon*. Budapest, ELTE Eötvös, 2022, 241–261.

Ó FATHAIGH, Ronan – HELBERGER, Natali – APPELMAN, Naomi: The Perils of Legally Defining Disinformation. 10(4) *Internet Policy Review* (2021).

<https://doi.org/10.14763/2021.4.1584>

PÉNZVÁLTÓ Nikolett: *Dezinformáció és külső információs befolyás Törökországban*. Stratégiai Védelmi Kutatóintézet Elemzések, 2019, <https://bit.ly/3Bh3Xfg>.

RIKHTER, Andrey: *International Law and Policy on Disinformation in the Context of Freedom of the Media*. Wien, OSCE, 2021.

SELJÁN Péter: A jelen kiberbiztonsági fenyegetései és a jövő kihívásai – a nemzetállami aktorok tevékenysége és a dezinformációk terjedése. *Nemzet és Biztonság*, 2021/4., 41–65.

<https://doi.org/10.32576/nb.2021.4.2>

## A HÍRNÉV- ÉS BECSÜLETVÉDELEM JOGGYAKORLATA A POLGÁRI ÉS A BÜNTETŐJOGBAN

**SZERZŐK:** Koltay András, Kovács Helga, Monori Zsuzsanna, Sorbán Kinga, Szikora Tamás, Szomora Zsolt

**SZERKESZTŐK:** Koltay András, Szomora Zsolt

**SOROZATSZERKESZTŐ:** Koltay András

**ÁRA:** 9000 Ft



A hírnév- és becsületvédelem kérdései az alkotmányos jogállam kiépülése óta folyamatosan a nyilvánosság figyelmét élvezik. A magyar társadalom, benne politikusokkal, közéleti személyiségekkel, hírességekkel, újságírókkal, egyéb véleményformálókkal és természetesen a jogalkotókkal, jogalkalmazókkal és tudományos kutatókkal immár több mint három évtizede birkózik azzal a kérdéssel, hogy milyen keretek között lehet valakit bírálni, kritizálni, mit enged meg a szólásszabadság alkotmányos védelme, és meddig terjednek a közügyekben érintettek személyiségi jogai.

A kötet alapjául szolgáló kutatás a 2012-es Btk. és a 2013-as Ptk. hatálya alatt 2021 végéig valamennyi elérhető és legalább a törvényszéki (büntetőügyekben), illetve ítéltótblai (polgári perekben) szintre jutó hírnév- és becsületvédelmi ügyben született döntést megvizsgált. Ez összesen 276 büntető- és 687 polgári ügy elemzését jelentette. A kutatás hangsúlyozottan csak a közügyeket érintő döntésekre fókuszált, tekintettel arra, hogy a hírnév- és becsületvédelem általános megközelítései ezen ügyekben hoznak elő sajátos és nehezen megválaszolható, alapjogi szempontból is kiemelten érzékeny kérdéseket.

A témával foglalkozó tudományos elemzések csak nagyon ritkán hatoltak mélyebbre a vonatkozó alkotmánybírói döntések elemzésénél, illetve a Kúria (Legfelsőbb Bíróság) által közzétett elvi jelentőségű döntések vagy BH-k bemutatásánál. Egy ilyen merítés szükségszerűen a felszínen marad, és nem alkalmas arra, hogy a valóságot – azt, hogy valójában milyen a vizsgált kérdések jogalkalmazói gyakorlata – a maga egészében bemutassa. Érdemes volt tehát nekilátni egy átfogó elemzésnek, amelynek eredményét e kötet foglalja össze.