MÉDIATUDOMÁNYI KÖNYVTÁR

DIGITÁLIS DILEMMÁK

Nemzeti Média- és Hírközlési Hatóság
Médiatanács • Médiatudományi Intézet

Digitális Dilemmák

Médiatudományi Könyvtár

53.

Sorozatszerkesztő:

Koltay András – Nyakas Levente: 2012–2019
Nyakas Levente – Szadai Károly: 2020–

Digitális Dilemmák

Fiatal kutatók válogatott tanulmányai a közösségi média egyes szabályozási kérdéseiről

Szerkesztette:

Lendvai Gergely Ferenc
Papp János Tamás

Médiatudományi Intézet

2025

A kutatást támogatta:

Nemzeti Média- és Hírközlési Hatóság
Médiatanács • Médiatudományi Intézet

Tartalom

Gondolatok a közösségi média és a jog kapcsolatának tanulmányozásához

Lendvai Gergely Ferenc – Papp János Tamás

A közösségi média platformok megjelenése és gyors térhódítása drámai hatással volt a társadalmi interakciókra, kommunikációra és információáramlásra. A világszerte legnépszerűbb online platformok, mint a Facebook, Instagram, X vagy TikTok több milliárd ember életének, mindennapjainak szerves részévé váltak. Mára már ezek a kijelentések kissé közhelyesnek is tűnnek, ez azonban nem teszi őket kevésbé igazzá. Az online platformok ilyen fokú és mértékű térnyerése rengeteg új kihívást hozott magával, amelyek komoly szabályozási kérdéseket és dilemmákat vetnek fel, és összetett problémák elé állítják a jogalkotót, a jogalkalmazót és a témával foglalkozó tudományos kutatókat egyaránt.

A közösségi média mára már a társadalom jelentős része számára elengedhetetlen eszközzé vált, és ennek hatása minden iparágban érezhető. A marketing, a kommunikáció, a média, a filmművészet, az oktatás, az orvostudomány, a vállalkozások, a katonai szektor: életünk minden területe érintett. A jogi szakma sem kivétel ez alól. A közösségi média megváltoztatta a jogászok munkamódszereit, a bizonyítékszerzést, a kutatási feladatok elvégzésének vagy akár a jogszabályok alkalmazásának módját is.

A közösségimédia-jog – vagy ahogy egyesek hívják, platformjog – egyelőre talán nem önálló jogi terület, mint például a büntetőjog vagy a munkajog, hanem inkább egy olyan terület, amely más jogágak – médiajog, versenyjog, alkotmányjog, polgári jog, hírközlési jog, szerzői jog, adatvédelem, gyermekvédelem, fogyasztóvédelem stb. – metszetén helyezkedik el. E jogágak összefonódása miatt a közösségi média szabályozása különösen összetett és dinamikus terület, amely folyamatosan alkalmazkodik a technológiai fejlődéshez és a társadalmi változásokhoz.

A közösségi média és a médiajog kapcsolata különösen érdekes, a közösségi média megjelenése és elterjedése ugyanis alapvetően alakította át a médiaipart, a sajtót és a kommunikációs szokásokat. A médiajog jellemzően inkább a hagyományos médiumok – mint például a nyomtatott sajtó, a televízió és a rádió – szabályozására koncentrál, azonban úgy tűnik, hogy a közösségi média térnyerése újraértelmezte és kibővítette a médiajog határait. A közösségi oldalakon megszokott decentralizált tartalomgyártás és -terjesztés alapvetően eltér a hagyományos média működésétől, ahol a tartalom előállítása és terjesztése szigorúan szabályozott és központosított, ennek következtében a médiajog alkalmazása a közösségimédia-platformokra számos új kérdést, valamint kihívást vet fel. Ami azonban közös pont a közösségi média és a médiajog kapcsolatában, az a tartalom szabályozása és moderálása. Míg a hagyományos médiumok szigorú szerkesztési és ellenőrzési folyamatokon mennek keresztül, addig a közösségimédia-platformokon a felhasználók által létrehozott tartalom gyakran ellenőrizetlenül kerül közzétételre. Ez a szabadság lehetőséget ad a kreativitásra és az önkifejezésre, ugyanakkor növeli a káros, félrevezető vagy illegális tartalmak megjelenésének kockázatát. A médiajogi szabályozásoknak tehát ki kell terjedniük a közösségimédia-platformok tartalommoderálási gyakorlatainak felügyeletére és szabályozására is.

Egy másik kulcsfontosságú közös terület a szólásszabadság és az egyéni önkifejezés szabadsága közötti egyensúly megtalálása. A közösségimédia-platformok lehetőséget biztosítanak a felhasználók számára, hogy szabadon kifejezzék személyiségüket, gondolatokat osszanak meg az egész világgal, vagy változatos formában kifejezhessék véleményüket társadalmi, szociális vagy politikai kérdésekben is – akár szélsőségesnek mondható formában is. Ennek garantálása társadalmi elvárás, ám szintúgy az is, hogy a platformok biztosítsák a tartalomfogyasztáshoz kötődő biztonságos környezetet, vagyis azt, hogy ne terjedjenek káros, gyűlöletkeltő, kirekesztő vagy félrevezető tartalmak. A jogi szabályozásnak tehát olyan egyensúlyt kell teremtenie, amely védi a szólásszabadságot, miközben hatékonyan lép fel a káros tartalmakkal szemben. Ez a feladat azonban nem könnyű, mivel a közösségi média dinamikus és gyorsan változó jellege megnehezíti a hatékony szabályozás kialakítását. A platformok moderálási gyakorlata és a jogi szabályozók által előírt korlátozások gyakran konfliktusba kerülnek egymással, vagy akár a tagállamok saját, szólásszabadsággal kapcsolatos alkotmányos alapelveivel.

1. Miért kell vizsgálni a közösségi média szabályozását?

Talán nem túlzás azt mondani, hogy az elmúlt évek fejlődése eredményeként a közösségi média és a jog kapcsolatának tanulmányozása szépen lassan egy új tudományággá (de mindenképpen egy új tudományterületté) nőtte ki magát. Ez a tudományág számos tudományterületet integrál, nem csupán a jogi szabályozásokra és azok hatásaira fókuszál, hanem interdiszciplináris megközelítést alkalmaz, bevonva a szociológia, a kommunikációtudomány, a pszichológia, az informatika és a politikatudomány eredményeit is. Ennek a komplexitásnak köszönhetően világossá válik, hogy a jogi eszközök önmagukban nem mindig elegendők a felmerülő problémák megoldására. A közösségi média dinamikus és gyorsan változó jellege megnehezíti a hatékony szabályozás kialakítását, és gyakran előfordul, hogy a jogi megoldások nem tudnak lépést tartani a technológiai fejlődéssel.

A közösségi média szabályozása mint kutatási téma több szempontból is komoly kihívások elé állítja a témával foglalkozó tudományos szakembereket. Egyrészt mindenképpen fel kell idéznünk Koltay András Kőműves Kelemen-hasonlatát, mely szerint a médiajoggal foglalkozó kutatók a jogtudomány Kőműves Kelemenjei, kiknek írásai szinte hónapok alatt jogtörténeti művé nemesednek.[1] A közösségi médiával kapcsolatos tudományos diskurzusok kapcsán ez hatványozottan igaz, a technológia, a platformok működése vagy akár a társadalmi folyamatok is olyan gyorsan változnak a közösségi média világában, hogy minden, a témával foglalkozó értekezés szükségszerűen csupán pillanatfelvételként szolgálhat az aktuális helyzetről.

Másrészt a terület szabályozásának kérdése körül kialakuló viták a mai napig nem jutottak nyugvópontra. Abban talán már egyértelmű konszenzus van, hogy mindenképp beszélhetünk szabályozási szükségességről a közösségi média területén,[2] ennek miléntje azonban továbbra

1 Koltay András: Hol van a médiajog szelleme? Rendhagyó recenzió a *European Media Law* című kötetről. *Iustum Aequum Salutare*, 2009/3., 6.

2 Jack M. Balkin: How to Regulate (and Not Regulate) Social Media. *Journal of Free Speech Law*, vol. 71., no. 1. (2021) 71–96.

is rengeteg kérdést vet fel. Az Európai Unió témában született – a kötetben szereplő tanulmányok többsége által alaposan elemzett – jogalkotási tevékenysége ugyanis nem tett pontot a közösségi média és az online platformok szabályozásával kapcsolatos viták végére, csupán a számos lehetséges út közül kijelölte az egyiket, mint az uniós joggyakorlat által követendő irányt. S bár az EU gyakran szigorúbb szabályozásokat vezet be a fogyasztóvédelem, az adatvédelem és a versenyjog területén, mint más régiók – és ugyanezek a szabályozások a fogyasztók védelmét szolgálják és megpróbálják biztosítani a tisztességes versenyt a vállalatok számára –, mégis ezek sokszor pont ellenkező hatást váltanak ki, mert a kisebb cégek számára megnövekedett költségeket és adminisztratív terheket jelentenek, melyek különösen hátrányosak lehetnek az európai kis- és középvállalkozások számára.[3] Emellett a túlzottan szigorú szabályozás gátolhatja az innovációt és a technológiai fejlődést, a rugalmas és támogató szabályozási környezet hiánya ugyanis nagymértékben akadályozhatja az új technológiák és üzleti modellek kifejlesztését. A nagy technológiai vállalatok monopolhelyzetének visszaszorítása érdekében bevezetett intézkedések rövid távon a verseny növelését szolgálhatják, azonban hosszú távon a túlzott szabályozás elriaszthatja a befektetőket és csökkentheti a versenyképességet.[4]

Végezetül a kihívások közül ki kell emelnünk az egyik legfontosabbat, mely magából a kutatási terület természetéből adódik. A közösségi média szociális és társadalmi hatásai ugyanis rendkívül szerteágazóak, ami megnehezíti azok teljes körű feltérképezését és a megfelelő szabályozás kialakítását. A megfelelő szabályozási keretrendszer kialakításához, vagy az arról szóló tudományos diskurzus megalapozott alakításához szükséges a szabályozni kívánt cél pontos meghatározása, amihez elengedhetetlen a közösségi média által keltett negatív társadalmi hatások azonosítása. Ezeket empirikus kutatások alapján pedig még csak most kezdjük igazán feltérképezni. Ráadásul mindehhez hozzáadódik az is, hogy a közösségi média dinamikusan változik, folyamatosan jelennek meg új platformok és trendek, melyek társadalmi hatásai nem ismertek, az egyes országok eltérő társadalmi és kulturális normái szintén megnehezítik az egységes szabályozás kialakítását, valamint a nagy techcégek hatalmas gazdasági és politikai befolyása is korlátozza a hatékony szabályozás lehetőségeit.

2. A kötet céljai és tartalma

A közösségi média jogi vizsgálata tehát kihívásokkal teli, viszont közel sem új jelenség. Egyszerű tudománymetriai számításokat követve 2010 és 2013 között a Scopus adatbázisa szerint 14.654 dokumentum foglalkozik közvetve vagy közvetlenül a közösségi média generális vagy specifikus szabályozásával a társadalomtudományok – így a jogtudomány – területén.[5]

3 Georgios Gryllos: The new digital landscape: Interaction between the DMA and rules of national and EU law governing the conduct of gatekeepers. *Concurrences* 2024/1. 40–56.

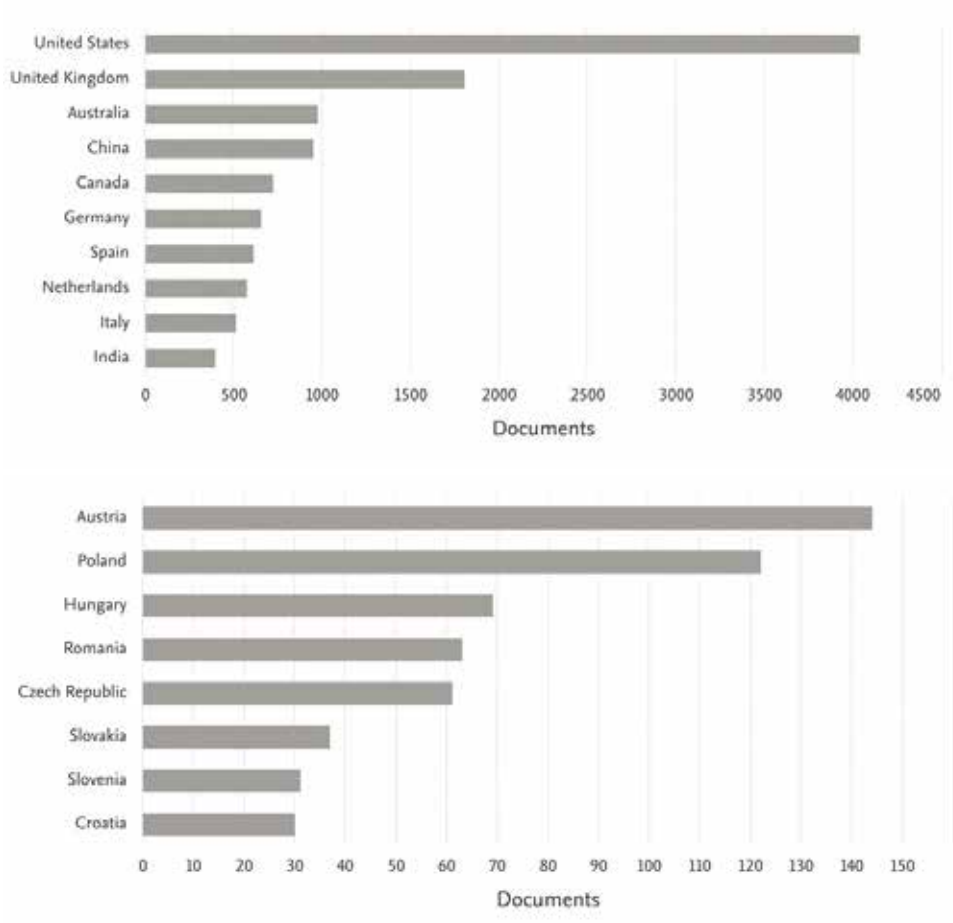
4 Mariateresa Maggiolino: Is the DMA (Un)fair? *Journal of Antitrust Enforcement*, vol. 12., no. 2. (2024) 267–272. https://doi.org/10.1093/jaenfo/jnae022

5 Használt search string: (TITLE-ABS-KEY ('legal regulation' OR 'law' OR 'legislation' OR 'policy' OR 'governance' OR 'compliance' OR 'regulatory framework' OR 'legal framework' OR 'legal standards' OR 'legal aspects' OR 'jurisprudence' OR 'statutory regulation' OR 'legal control') AND TITLE-ABS-KEY ('social media' OR 'social networks' OR 'online platforms' OR 'digital media' OR 'internet platforms' OR 'social networking sites' OR 'web 2.0' OR 'social media platforms' OR 'online social networks')) AND PUBYEAR > 2009 AND PUBYEAR < 2024 AND (LIMIT-TO (SUBJAREA , 'SOCI')).

Ez az adat egyszerre két dolgot bizonyít. Egyfelől a közösségi média, az online platformok és az új digitális felületek szabályozása a kutatókat érdeklő, a tudományágakat 'megmozgató' és a társadalomtudományokat gazdagító témakör. Sőt, mint globális jelenség a közösségi média számos ország kutatóit foglalkoztatja (ld. *1. ábra*), legyen szó a nyugati 'Óriásokról' (így az Egyesült Államok, Egyesült Királyság, Németország, Hollandia), a gyorsan fejlődő Globális Délről (Brazília, Kína, Irán) vagy akár a Föld lakossága által talán alig ismert mikro-országokról (lásd a vanuatui Toby Ley munkásságát, aki elsősorban az online médiaszabadságot kutatja a csendes-óceáni szigetek országaiban).[6]

1. ábra

A közösségi médiához kapcsolódó szabályozási kérdések tudományos feldolgozása a legnagyobb országok és a tágan értelmezett kelet-közép-európai országok viszonylatában a Scopus adatbázisban 2010 és 2023 között.



Forrás: Saját szerkesztés Scopus adatok alapján. Magyarország (n=69).

6 Toby Ley: Policy, papers and pages: Improving media engagement in the Pacific. *Pacific Journalism Review*, vol. 19., no. 1. (2013) 58. https://doi.org/10.24135/pjr.v19i1.238

Másfelől, ami talán még fontosabb a hazai kutatók számára, a közösségi média szabályozása közel sem 'megoldott' kérdés; jóval inkább egy napról napra fejlődő, egyszerre uniformizálódó és fragmentálódó, hol dinamikus, hol lomha fejlődést mutató, egyszerre interdiszciplinaritást és a jog sajátos specifikusságát megkövetelő kutatási témáról beszélhetünk. E 'nem-megoldott' helyzet viszont feladat is; feladat arra nézve, hogy a hazai jogirodalomban is szükség (sőt, talán kényszer) van arra, hogy a közösségi média szabályozását és annak változását aktívan, értően és alaposan feldolgozzák a kutatók.

Jelen tanulmánykötetben három kiemelt cél elérésére tettünk kísérletet. Egyfelől, a fenti aktív tudományos diskurzust szerettük volna gyarapítani olyan hazai fiatal kutatók gondolataival, akik bár pályájuk elején vannak, szakértelmük, tudományos karrierjük és ambíciózus célkitűzéseik alapján képesek 'lefordítani' a hazai tudomány nyelvére a már meglévő joganyagot és irodalmat, továbbá olyan új témák feltérképezésére vállalkoztak, amelyekre eddig kevesen – legyen szó az adatvédelem vagy a versenyjog új kérdéseiről, vagy egy 'mérföldkőnek' számító jogeset kritikai elemzéséről. A tanulmányok ennek fényében igen szigorú átvizsgáláson mentek keresztül. A Szimpóziumra készülő és ott előadó hallgatóknak eleve egy közel kész kézirattal kellett érkezniük, amelyet aztán többször át kellett dolgozniuk a hazai, e témában kutató vezető és legmagasabban idézett jogtudósok véleményei alapján, ezt követően pedig két turnusban bírálták is a kéziratokat. Célunk ezzel elsősorban az volt, hogy diszkussziót kezdeményezzünk a már tapasztalt és a tapasztalatokat gyűjtő kutatók között; szabadon, de tudományos keretek között meg lehessen vitatni a gondolatokat és elinduljon egy olyan szakmai együttműködés, amelynek eredménye egy magas színvonalú, a hazai tudományban és akár jogalkotásban használható '*output*'.

Második célunk a közösségi média kutatásának sokszínű természetének bemutatása volt. Hogy e célkitűzést elérjük, olyan kéziratokat helyeztünk előtérbe, amelyek valamiféle nóvumot, új megközelítést, paradigmát kínálnak. Így mindösszesen tíz tanulmány megismerésére invitáljuk az olvasót igen szerteágazó és nagy érdeklődésre számot tartó témákban. A témákat három nagy csoportba rendeztük, amelyek a következők: I. szólásszabadság és alapjogok a közösségi média szabályozásának tükrében, II. adatvédelem és digitális technológiák, és III. a versenyjog és a szerzői jog dilemmái. Az I. fejezetben Szakálné Szabó Zita: #áldás vagy #átok? című tanulmányában azt vizsgálja, hogy a közösségi média által kialakított új médiakörnyezet és az ezáltal kialakuló és formálódó új médiaszokások miképpen változnak, és kérdéseket vet fel arra nézve, hogy ez az átalakulás miképpen értékelhető a társadalom egésze szempontjából. A szerző saját szerkesztésű ábrákkal illusztrált, statisztikai adatokkal és gazdag irodalmi áttekintéssel dolgozó tanulmányában igyekszik a médiatudatosság, az online gyerekvédelem és a médiába vetett bizalom bemutatására. A társadalmi tényezők alapjogi kontextusba helyezéséhez a szabályozási kérdéseket alapjogi megközelítésen keresztül vizsgálja Vitkovics Bálint és Botos Mihály Bálint. Vitkovics dolgozatában a becsülethez és a jó hírnévhez való jog megsértését elemzi különös tekintettel azokra az esetekre, amelyek a közösségi média felületein történnek. A szerző alaposan ismerteti a platformok konceptualizálásának kihívásait, bemutatja a vonatkozó hazai szabályozási környezetet, különös tekintettel a Ptk.-ban foglalt személyiségi jogokra, majd az alapjogok kollízióját többek között a kommentek státusza és a digitális nyilvánosság polémiája mentén járja körül jogesetek bemutatásán keresztül. Botos az online szólásszabadság egy másik igen népszerű fejezetét dolgozza fel; a szerző a közösség elleni uszítás jogalkalmazási gyakorlatát ismerteti a Fővárosi Főügyészség ötven kapcsolódó eljárásának ügyiratain keresztül. A kézirat az ügyek részletes ismertetésén és a főbb hasonló-

ságok feltárásán keresztül nyújt betekintést a hazai joggyakorlatba, az írást pedig egy kritikai analízisre támaszkodó 'új mérce' bevezetésével zárja. A fejezet lezárásaként egy, a hazai és a külföldi jogirodalomban is igen kezdetlegesen feldolgozott téma bemutatását olvashatjuk Kovács Andrea tollából. Kovács a *botokat*, azaz a közösségi médiában megjelenő automatizált fiókokat vizsgálja a szólásszabadság szemszögéből: szólásnak minősülhet-e valami, amit egy automatizált bot 'mond'? Az írás alapos alapjogi áttekintéssel és a jelenlegi (talán pontosabban: alakuló) szabályozási irányok ismertetésével, valamint összehasonlításával kíván válaszolni a kérdésre.

A II. fejezetben az adatvédelmet és a digitális technológiákat, továbbá az azokhoz kapcsolódó szabályozási kérdéseket három szerző munkáján keresztül ismerhetjük meg. Bálint János azt taglalja, hogy melyek az adatvédelem általános kérdései az online platformokon. Bálint tanulmányában – amely részletességét, szerkezetét és átláthatóságát tekintve akár az adatvédelemmel foglalkozó szakemberek és szakjogászok számára is jelentős segítség lehet, fontos iránymutatásként szolgálhat – kiemelkedő szerepet játszanak az iránymutatások értékelései, amelyeket a szerző mind elméleti, mind gyakorlati szempontból értékel. Ezt követően Mozsonyi Norbert írását olvashatjuk a magánszféra és az adatvédelem témakörében. Mozsonyi az online adatvédelem holisztikus megközelítését proponálja és részletekbe menően elmélkedik arról, hogy 'halott-e a *privacy*', azaz, hogy milyen hatékony eszköztár lenne megfelelő szabályozási szemszögből a magánszféra teljesebb körű védelme biztosításáért. A harmadik tanulmányt Kálmán Kinga jegyzi, aki az Európai Unió Bíróságának egyik új és nagy horderejű esetét ismerteti kritikai megközelítésben. Alkalmazva a jogesetelemzések strukturális és metodikai megfontolásait, Kálmán aprólékosan elemzi a Meta kontra Bundeskartellamt ítéletet, amely elsősorban a közösségimédia-platformokat felhasználók személyes adatainak üzletszerzésből történő, személyre szabott felhasználását érinti.

A III. fejezetben a versenyjog és a szerzői jogok kerülnek a középpontba. Az utolsó szekciót Beyer Fülöp és Csillik Kristóf írása nyitja. A szerzők a versenyjog szerepét vizsgálják, különösen a Digital Markets Act (DMA) tükrében. Az írás kiemelt erőssége, hogy a szerzők gondolataik közvetítésére nem csupán jogi normákra és jogirodalmi művekre építkeznek, hanem értő módon építik bele a közgazdaságtan tudományát is, különösen közgazdasági modellek és szabályok alkalmazásán keresztül. Huszár Daniella az algoritmusok szerepét tanulmányozta a közösségi média platformokon alkalmazott *dark patterns* tekintetében. A *dark patterns*, amelyet a magyar szakirodalom, talán kissé szimplifikált szemantikai megfontolásokat követve sokszor 'sötét mintázatoknak', szerencsésebb esetekben – ahogy Huszár is teszi – 'sötét megoldásoknak' fordít, általánosságban véve a platformok felhasználókat manipuláló eszköztárát takarja és számtalan kérdést felvet mind a versenyjog, mind a platformszabályozás területén. A szerző rendkívül gazdag irodalomra építi munkáját, amelyben többek között teoretikus összehasonlítások vannak a sötét megoldások lehetőségeiről, illetve egy alaposan felépített táblázatból a legnagyobb közösségimédia-platformok által alkalmazott sötét megoldásokat is megismerheti az olvasó. A szerzői jogi kérdéseket a fejezet, egyben pedig a tanulmánykötet lezárásaként Kovács György vizsgálja. Kovács tanulmányában két kiemelt jelentőségű uniós jogszabály, a digitális egységes piacról szóló szerzői jogi irányelv (CDSM) és a digitális szolgáltatásokról szóló rendelet (DSA) szabályait elemzi összehasonlító kritikai eszközökkel. A tanulmány fontos látképet ad a jelenlegi szabályozásokról és a szerzői jog jelenlegi helyzetéről a két instrumentum kontextusában.

A fenti témák feldolgozásának egyik különösen fontos aspektusa az alapja a harmadik célunknak is. Valljuk ugyanis, hogy a fiatal kutatók gondolatainak, munkáinak látványos és hozzáférhető megjelenése alapvető fontosságú annak érdekében, hogy a hazai jogtudomány lépést tudjon tartani a nemzetközi jogirodalom dinamikus fejlődésével. E körben őszintén reméljük, hogy az Olvasó hasznosnak és inspirálónak tartja majd a válogatott tanulmányokat, és ösztönözni szeretnénk minden olvasót, érdeklődőt, elismert kutatót, oktatót, szakembert – és leginkább a sokszor viszontagságokkal teli, türelmet és tartást megkívánó, ugyanakkor szellemileg páratlanul pezsdítő, sőt élethosszon át kitartó tudományos pályára aspiráló fiatal kollégát és hallgatót –, hogy bizalommal keressék meg a szerzőket, illetve akár a szerkesztőket is, alakuljon ki egy újfajta, modern és *output*orientált tudományos együttműködés, amelynek eredményét nemcsak pár napos konferenciákon, hanem akár kezünkben forgatva is megismerhetjük. Bizalommal ajánljuk tehát a kötet tanulmányozását és barátsággal javasoljuk annak ajánlását is!

Jelen tanulmánykötet és a vonatkozó szimpózium nem jöhetett volna létre a kéziratszerzők opponenseinek és bírálóinak szaktudása, valamint segítsége nélkül, így külön szeretnénk hálánkat és köszönetünket kifejezni Dr. Pogácsás Anettnek, Dr. Bartóki-Gönczy Balázsnak, Dr. Koltay Andrásnak, Dr. Pünkösty Andrásnak, Dr. Szilágyi Pálnak és Dr. Török Bernátnak. Őszintén bízunk benne, hogy a jövőben folytathatjuk a közös munkát és hasonló kötetekkel gyarapíthatjuk a 'közösségi média és jog' kérdésköreit feldolgozó hazai irodalmat.

I. Szólásszabadság és alapjogok

#áldás vagy #átok?

– avagy a közösségi média társadalmi hatásainak vizsgálata

Szakálné Szabó Zita

„Szeretjük azt hinni, hogy az információ szabaddá tesz minket, és hogy az internet-hozzáférés a tekintélyelvűek által elnyomottakat elvezeti a demokrácia fényéhez. [...] időről időre blokkolhatják ugyan az internetet, de ki is használhatják azt, nemcsak a másképp gondolkodók felderítésére, hanem arra is, hogy propagandát terjesszenek általa."[1]

(Torie Bosch)

A 21. században a közösségi média teljesítette ki az internetet, és mint egy hatalmas virtuális állam, saját maga határozza meg követendő normáit, maga értelmezi saját tartalmát, az azzal kapcsolatos döntéseket és azok későbbi esetleges felülvizsgálatát. Tehát mondhatjuk, hogy a részvétel kultúrájában a közösségi média egyértelműen a legmeghatározóbb kommunikációs eszközzé nőtte ki magát. De milyen mértékben szolgálhat ez az új médiakörnyezet inkább arra, hogy bevonja a társadalmat a közügyekbe, mint azt a 'régi' média tette? És milyen lehetőségek rejlenek a közösségi médiában, azokat pedig a társadalmi változásokban hogyan és miképpen lehet előre mozdítani? Végső soron áldás vagy átok a társadalmi változásokban a közösségi média léte, figyelembe véve, hogy a közösségi média platformjainak megjelenése óta azok társadalmi mozgalmakat szervező és kiváltó szerepe folyamatos vitatéma tárgyát képezi, és nemegyszer a történések középpontjába került már? A közösségi oldalak leginkább egy hatalmas virtuális államra hasonlítanak, és fejlődésükben sincs megjelenésük óta egyetlen pillanatra sem megállás. Nagyon nehéz megjósolni, hogy a rohamléptekkel való fejlődés milyen irányba tart, ugyanakkor a jogi szabályozására is általában jellemző, hogy a bekövetkező változásokat pár lépéssel lemaradva követi. A közösségi média a kibertér által biztosított lehetőségeknek köszönhetően a társadalmi folyamatokban nagyon fontos szerepet játszik, gondoljunk csak a vezetők és kormányzatok világszerte alkalmazott digitális platformokon való megnyilvánulásaira, vagy éppen a világon zajló – és a közösségi médiában közvetített – fegyveres konfliktusok frontjairól történő, első kézből való tájékoztatásokra.

1. Bevezetés

A tanulmány elsőként annak megválaszolására törekszik, hogy áldás vagy átok a társadalmi változások előmozdításában a közösségi média léte, amely kérdés megválaszolása során szükséges kitérni arra, hogy melyek azok a társadalmi változások, amelyekre a közösségi média hatást gyakorolhat, valamint, hogy a közösségimédia-platformok a digitális korunkban milyen szerepvállaláson mentek keresztül, és milyen irányba tartanak jelenleg.

1 Torie Bosch: Tangled Web. *Slate*, 2011. február 1. https://slate.com/culture/2011/02/evgeny-morozov-s-net-delusion-social-media-are-tools-for-oppressors-not-just-activists.html

1.1. Társadalmi változások: gondolkodásmód megkonstruálása varázsütésre?

A társadalmi változások[2] előmozdításában a közösségi médiának óriási szerepe van, hiszen az információkhoz, valamint a különféle kommunikációs csatornákhoz való hozzáférésnek is hatalmas mozgatóereje van, amely a megmozdulások sikerességéhez hozzájárul, azonban azok impulzusát végső soron mégsem a világháló, hanem az eszmék és azok követői adják.

A közösségi média elsődleges és legfontosabb szerepe az információ elérhetősége és terjesztése, ami sokkalta gyorsabb és hatékonyabb módszer, mint az újságok vagy a televízió. Másodlagos szerepe az emberek összekapcsolása, és a közös célok felé mozdítása. Segít a társadalmi változásokra való felhívásban és mobilizációban, hiszen az embereknek lehetőségük van kifejezni elégedetlenségüket, kritikát és véleményt tudnak formálni a társadalmi kérdésekről, ami által erős véleménykinyilvánítással párhuzamosan akár jelentős politikai hatást is ki tudnak váltani. Az utóbbi évtizedben az online diskurzusok vezető platformjává[3] a Facebook, a Google és a Twitter váltak,[4] amelyek kétségkívül szélesítik az egyén megszólalási lehetőségeit, de torzíthatják is a valóságot[5] – erre a későbbiekben ki is térünk –, és a társadalmi párbeszéd alakulására döntő hatást gyakorolva alapjaiban rajzolhatják át a nyilvánosság szerkezetét. Jack Dorsey a Twitter egykori vezérigazgatója, reagálva a közösségi médiában terjedő félretájékoztatással kapcsolatosan növekvő aggodalmakra, 2019. október 20-án az alábbiak szerint *tweet*elt: „Véleményünk szerint a politikai üzeneteket a választóknak maguknak kell

2 Társadalmi változások alatt olyan változásokat értünk, amelyek a társadalom szélesebb rétegeit érintik, és hatással vannak az emberek viselkedésére, hozzáállására, akár az életmódjukra vagy életkörülményeikre is. Ezek a változások többféle területet is érinthetnek, mint a gazdaság, politika, és származhatnak különféle forrásokból, mint a politikai mozgalmakból, társadalmi aktivizmusból, technológiai fejleményekből, demográfiai változásokból. A társadalmi változások hosszú távú folyamatok, tehát nem egyik napról a másikra következnek be, és céljuk legtöbbször a pozitív változások előmozdítása és a társadalom jobbítása. Ahhoz, hogy a társadalmi változások segítségével előremozdítsák a kitűzött közös célt, az abban résztvevő embereknek együttműködniük szükséges, és szükséges továbbá összefogniuk a változáshoz vezető erőfeszítések megtételében. A közösségi média által nyújtott platformok lehetőséget adnak, hogy az emberek kapcsolatba lépjenek, kommunikáljanak egymással, és a közös célok elérése érdekében közösen cselekedjenek. *'We are social'*. Az embereknek lehetőségük van továbbá tudatosságot ébreszteni, véleményüket megvitatni, és összefogni másokkal a közös cél, ügyeik érdekében. A társadalmi változások összetett folyamatában a közösségi média mint az információáramlás és a kapcsolatépítés egyik legfontosabb eszköze lehetőséget ad arra, hogy az általuk fontosnak tartott ügyekben cselekedjenek, és mozgósítsanak másokat az elégedetlenségük, vagy a változásra való törekvésük érdekében.

3 Az Európai Parlament és Tanács a digitális szolgáltatások egységes piacáról szóló 2022/2065 rendelet és annak módosításáról szóló 2000/31/EK (digitális szolgáltatásokról szóló rendelet) irányelve az online platform fogalmát az alábbiak szerint definiálja: „az online platform olyan tárhelyszolgáltatás, 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 funkcionalitása, amely 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."

4 Kate Klonick: The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review*, vol. 131. (2018).

5 Koltay András: Trump elnök Twitter-fiókja és a szabadság halványodó amerikai álma. *Index.hu,* 2021. január 18. https://index.hu/velemeny/2021/01/18/trump_elnok_twitter-fiokja_es_a_szabadsag_halvanyodo_amerikai_alma/

keresniük, és nem az orruk alá kell tolni őket."[6] A Twitter a politikai reklámok kitiltásával[7] kívánt elhatárolódni az olyan kényes területektől, mint például a politika.

> „[A]z új (közösségi) média egy adott történelmi pillanatban akár a formálódó, angeluszi értelemben vett látens közvéleményt aktivizáló fórummá is válhat."[8]

Fontos azonban megjegyezni, hogy a közösségi média a felsoroltakon kívül másfajta változásokat is magával hozott, mint például az adatvédelem, vagy tájékozottság hiányában keltett poláris vélemények egy olyan közegben, ahol minden leírt szónak nyoma van. A tanulmány a jelenlegi és jövőbeni szabályozási megoldásokkal, valamint a felmerülő jogi problémákkal nem foglalkozik. A szabályozási rendszer nem egy könnyen körülhatárolható, elkülönített szabályozási forma része, hiszen a jog folyamatosan változik, és a közösségi média által felvetett ilyen irányú kérdések külön téma tárgyát képezik.

1.2. Közösségi média vagy 'közösségi média'? Technikai módszerek a világhálón, avagy aktív részvétel és szerepvállalás a digitális korban

A kilencvenes évek elején az internet megjelenése csakúgy meglepte a világot, mint egykor a számítógépek megjelenése. Az internet egyrészről egy utolérhetetlenül gyors és rugalmas információs szolgáltatások gyűjtőhelyévé, másrészről pedig a hagyományos postai és telefonszolgáltatásokkal versenyre kelő kommunikációs médiummá vált.[9] De miben rejlik a népszerűsége, és hogyan jelentett további fellendülést a közösségi média megjelenése, amelynek felhasználói száma évről évre egyre csak gyarapszik?

> „A közösségi média (*social media*) a felhasználói interaktivitásra építő, online médiaeszközök összefoglaló neve, amelyek különféle céllal létrejött felületeket foglalnak magukba."[10]

A hazai médiajog tekintetében a közösségi média megnevezés ilyen tekintetben azonban félrevezető, ugyanis a hazai jogirodalom a fogalmat leginkább a közösség tájékoztatási, vagy kulturális igényeket kielégítő médiaszolgáltatásra alkalmazza. Hazánkban az angol *social media* kifejezés magyar megfelelőjeként egy fogalom, a közösségi média fogalma honosodott meg, azonban a klasszikus közösségi média, valamint az új, Web 2.0-ás közösségi média angol megfelelői a *community media* és a *social media*.[11] A meglévő fogalmi zavarra számos szerző már rámutatott, és ebből kifolyólag a két kifejezés pontos meghatározása okán célszerűbb lenne az online platformok körében inkább a *social media* kifejezést használnunk.[12]

6 Kate Conger: Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says. *The New York Times,* 2019. október 30. https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html

7 2023 januárjában oldotta fel Elon Musk a politikai és társadalmi témájú hirdetésekre vonatkozó tilalmat, amely lépéssel megpróbálta a cég bevételeit növelni.

8 Iványi Márton: Közösségi média: a nyilvánosság elektronikus agorája vagy posztmodern panoptikum? Hatalmi válaszok a közösségi média kihívásaira. *Médiakutató,* 2014/2. [a továbbiakban: Iványi (2014a)] 120.

9 Iványi Márton: A közösségi média és a társadalmi mozgalmak. *Iskolakultúra: Pedagógusok szakmai-tudományos folyóirata,* 2014/2. [a továbbiakban: Iványi (2014b)] 68.

10 Kepe Nóra: *A közösségi média önimádó embere.* Budapest, L'Harmattan, 2022. 43.

11 Gosztonyi Gergely: Az alternatív média a(z európai) médiaszabályozásban. *In Medias Res,* 2013/1. 133.

12 Ld. Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Medias Res,* 2019/1.

Tekintettel arra, hogy a legtöbben a közösségi média fogalma alatt elsősorban a *social media* felületeit[13] értjük, jelen tanulmányban én is ebben az értelemben alkalmazom a közösségi média kifejezését.

A digitális világnak köszönhetően ma már olyan adatokhoz juthatunk hozzá pár kattintással, amelyek éppen az adott, aktuális munkánkhoz szükségesek. A DataReportal[14] évente olyan statisztikákat, elemzéseket és jelentéseket készít, amelyeket szerte a világon több, mint 230 országban több millióan olvasnak és használnak, ezzel is segítve a digitális világban dolgozó embereket, és szervezeteket. Az általuk készített elemzéseket, és jelentéseket felhasználva nyilvánvalóvá válik, hogy a közösségimédia-felületek alkalmazása a kezdeti lassú bővülés után dinamikus fejlődésen ment keresztül, „miközben az oldalak tevékenységükben is egyre változatosabbá váltak."[15]

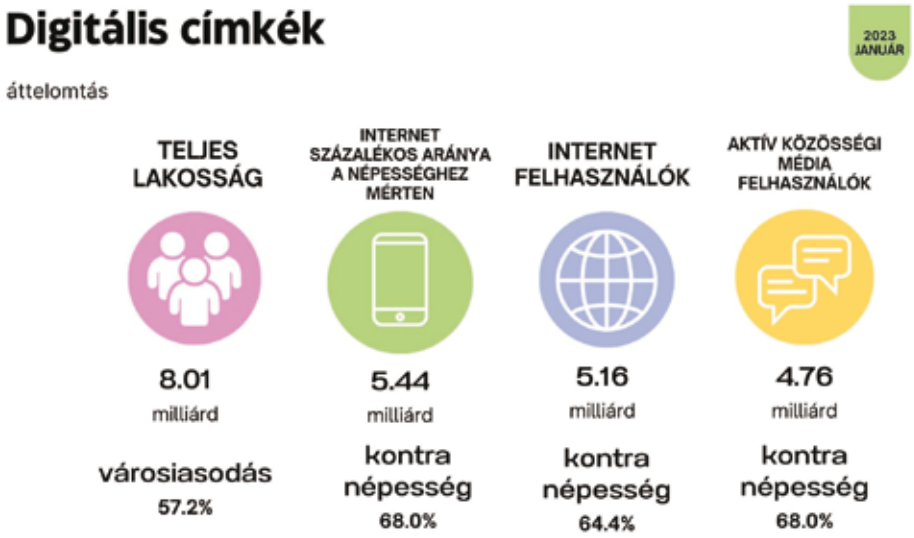
A világ teljes lakossága által használt digitális eszközök és a közösségi média felhasználására vonatkozó adatok döbbenetes számokat mutatnak. Az alábbi két ábrán egyrészről a 2023. évi januári mutatók, másrészről a több mint tíz évvel korábbi, 2012. évi januári mutatók hasonlíthatók össze.

13 Az első közösségimédia-oldalt, a SixDegrees oldalát 1997-ben az Egyesült Amerikai Államokban hozták létre, és az személyes profil létrehozására és kapcsolattartásra volt alkalmas. A Facebookot 2004-ben hozták létre, és napjainkban is a legnagyobb felhasználói létszámmal rendelkezik, 2017-ben már több mint 2 milliárd felhasználója volt világszerte. A lista második helyén 1,5 milliárd felhasználóval a YouTube, harmadik helyén pedig 1,3 milliárd felhasználóval holtversenyben a WhatsApp és a Facebook Messenger áll. 2019-ben üstökösként tört be a piacra az első kínai okostelefonra fejlesztett alkalmazás, a TikTok, , és azt világszerte a kínai letöltőkön kívül 1 milliárdan töltötték le. Ezeken túl a WeChat, Instagram, QQ, QZone felületek is több mint félmilliárd regisztrált taggal rendelkeznek. Marketer: Facebook felhasználók száma Magyarországon. *ROIHacks.hu,* 2023. május 10. https://roihacks.hu/facebook-felhasznalok-szama-magyarorszagon

14 A DataReportal minden jelentését Simon Kemp és csapata készíti, az adatokat pedig közvetlenül, megbízható harmadik felektől szerzi be, amelyeknek a felsorolása minden elemzésben külön megtörténik. Simon Kempet globális szaktekintélyként tartják számon, aki az emberek internetfelhasználásával kapcsolatos kutatásokat végez. Munkáját a londoni Accenture vállalatnál kezdte, ahol egy vezető szupermarketlánc e-kereskedelmi tevékenységét segített felépíteni, majd olyan nagynevű cégeknek dolgozott, mint a Google, Coca-Cola, Nestlé, vagy éppen a Diageo. Munkája mellett pedig a világ számos legprogresszívebb marketinggel foglalkozó szervezetének a tanácsadó testületében tevékenykedik. https://datareportal.com/

15 Kepe i. m. 43.

1. ábra Digitális címkék áttekintése, 2023. január



Saját szerkesztés. Az adatok forrása: DataReportal[16]

2. ábra Felhasználói számok, 2012. január

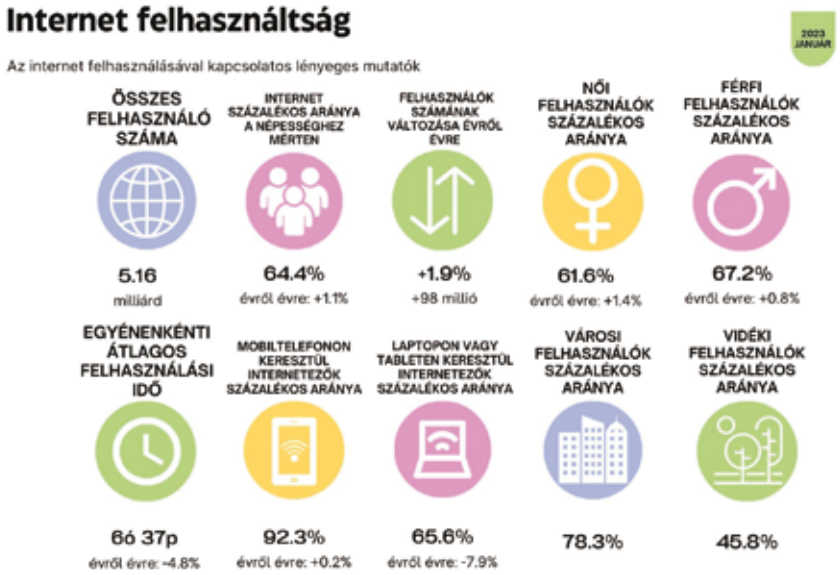
Saját szerkesztés. Az adatok forrása: DataReportal[17]

16 Simon Kemp: Digital 2023: Global overview report. *Datareportal.com,* 2023. január 26. https://datareportal.com/reports/digital-2023-global-overview-report

17 Simon Kemp: Digital 2012: Global digital overview. *datareportal.com,* 2012. január 17. https://datareportal.com/reports/digital-2012-global-digital-overview

Érdemes megvizsgálni, hogy az internetet használók hogyan és miként alkalmazzák a *részvétel kultúrájá*ban[18] a kezükbe adott elektronikus hírközlési szolgáltatás által adott lehetőségeket. Az alábbi ábrán láthatjuk az internet felhasználásával kapcsolatos mutatókat, továbbá érdemes megvizsgálni az átlagos felhasználási időre vonatkozó adatokat is. A képernyőidőnket – vagyis, hogy mennyi időt töltünk a telefonunk nyomkodásával – mi is bármikor ellenőrizhetjük. A KSH adatai szerint a 16 és 74 év közötti magyar lakosság körében a világhálót rendszeresen felkereső személyek száma 2021-ben 89 százalék volt, míg ez a szám a 2000-es évek elején alig érte el a 37 százalékot. Az okostelefonok segítségével bármikor bárhonnan[19] megnézhetjük a világ aktuális történéseit, így a közösségimédia-oldalakat is.

3. ábra Az internet felhasználásával kapcsolatos lényeges mutatók, 2023. január



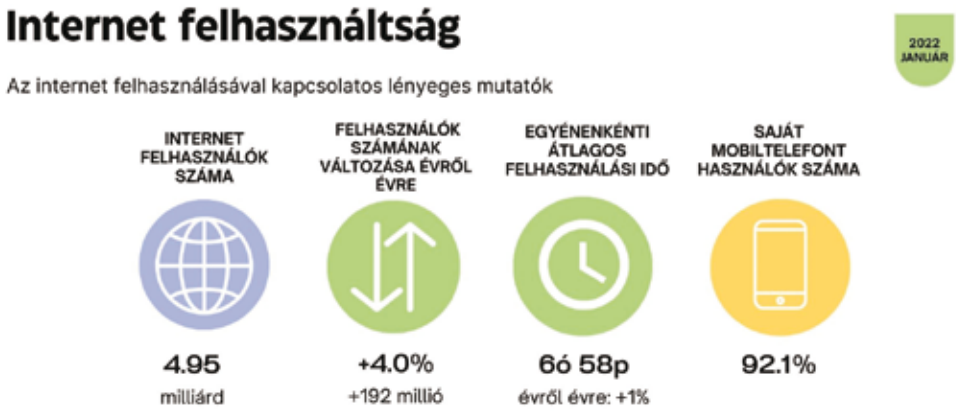
Saját szerkesztés. Az adatok forrása: DataReportal[20]

18 A részvételi kultúra elmélete a 2000-es évek elején vált divatos kifejezéssé, és egyszerre hordozta magában az egyének közötti kapcsolatok megerősítését, valamint a közösségek építését és a demokrácia tökéletesítésének lehetőségét. Ennek helyébe lépett a kapcsolódás kultúrája, amely azonban erős kritikai potenciállal rendelkezik. Glózer Rita: *Részvétel, média, kultúra – videóblogok a részvételi kultúrában.* Budapest–Pécs, Gondolat, 2022. 156.

19 *Fear of Missing Out* (FOMO), vagyis a kimaradástól való félelem; a közösségi média térnyerése és mindent behálózó jelenléte a jelenség – különösen a fiatalok körében történő – terjedésének oka.

20 Kemp (2023) i. m.

4. ábra Az internet felhasználásával kapcsolatos lényeges mutatók, 2022. január



Saját szerkesztés. Az adatok forrása: DataReportal[21]

Az előző évhez, 2022 évéhez képest három lényeges változást emelnék ki, ami a fenti ábrán is jól látszik: az első a felhasználók számának növekedésében való lényeges eltérés: 2021 évről 2022 évre a felhasználók száma 4 százalékos növekedést mutatott, ez a százalékos arány azonban 2022 évről 2023 évre 1,9 százalékra csökkent. Ez közel 100 millióval kevesebb felhasználót jelent. Másik lényeges csökkenő mutató az átlagos felhasználási időben jelentkezik, mivel a 2022 év januárjában mért átlagos közel 7 órás felhasználási idő 6 és fél órára csökkent. A két év mutatóinak összehasonlítása során a már korábban említett mobiltelefonon keresztüli internetezés népszerűtlensége (?) is jól látszik az elenyésző, két tized százalékos emelkedésből.

„Állandóan vitatkozunk az internetnek a változásban játszott szerepéről. Vannak, akik azt gondolják, az internet virtuális világ, amelynek a valóságra kevés hatása van, míg szerintem kulcsfontosságú eszköz a változás elindításához. Az internet nem virtuális világ, amelyet avatárok laknak. Olyan kommunikációs eszköz, amelynek segítségével a fizikai világban élő emberek szervezkedhetnek, cselekedhetnek, gondolatokat terjeszthetnek, és felhívhatják a figyelmet valamire."[22]

A digitális aktivizmusról alkotott felfogásunk most kezd kiteljesedni, tekintettel arra, hogy valójában egy absztrakt fórumról beszélünk, amikor a közösségi média színterét említjük. A közösségi oldalak olyan új kommunikációs eszközzé váltak, és lettek a mindennapjaink részesei, amely módosította a nyilvánosság erőtanát, és a véleménynyilvánítás lehetőségeit példátlan módon gazdagította. Digitális vagy online aktivizmusnak nevezzük azt a folyamatot, amikor valaki digitális eszközökkel – mint például a közösségi média – kíván valamilyen változást elérni, akár politikai hatást kiváltani. A közösségi média szerepével és a felhasználók tömeges befolyásolásával, akár manipulálásával hatalmas hatást

21 Simon Kemp: Digital 2022: Global overview report. *datareportal.com,* 2022. január 26. https://datareportal.com/reports/digital-2022-global-overview-report

22 Váil Ghoneim: *Forradalom 2.0.* Budapest, Gabo, 2013. 70.

tud gyakorolni a nyilvánosságra.[23] Kérdésként merülhet fel, hogy ezek a platformok mekkora hatalommal is rendelkeznek a demokratikus nyilvánosság alakítására tekintettel. „Az aktív médiabeli részvétel fejleszti az írás, olvasás, szerkesztés, filmkészítés és -terjesztés, az önkifejezés készségeit, sőt az állampolgári szabadságjogok iránti érzékenységet is, melyek egy új médiaműveltség, és erre épülve a teljes jogú társadalmi (politikai, gazdasági, kulturális) részvétel alapját jelentik."[24]

5. ábra A közösségi média felhasználóinak számában való változás nyomon követése (millió/év)[25]

Lényeges, hogy lássuk az összefüggést az internetfelhasználás, valamint a közösségimédia-platformok térnyerése között, valamint, hogy a közösségi média önmagában nem vezet forradalmakhoz, de nagymértékben segíti azok kibontakozását, ahogyan az Arab Tavasz[26]

23 2014-ben a Facebook több mint félmillió felhasználót érintő kísérletet végzett abból a vizsgálódási célból, hogy a felhasználók miként reagálnak hírfolyamuk manipulálására. A célcsoport egyik részének az algoritmus pozitív tartalmakat, másik részének azonban éppen ellenkezőleg, negatív, demoralizáló posztokat dobott fel. A kísérletből kiderült, hogy a hírfolyam típusa az érintettek hangvételét, és érzelmi állapotát is nagyban befolyásolta, így akik sok negatív hírrel találkoztak hírfolyamukban, azokon eluralkodott a pesszimizmus, a pozitív posztokkal szembesülő fogyasztók viszont sokkal jobb szellemi és mentális állapotba kerültek. A Facebook célja ezzel a kísérlettel az volt, hogy növelje a felhasználók elégedettségét a minél relevánsabb tartalmak megjelenítésével, és nem utolsó sorban, hogy lehetővé tegyék a vállalat számára a hírfolyamok tartalmának bármikori megváltoztatását is. Digital Hungary: Hogyan manipulál a Facebook? *DigitalHungary.hu,* 2016. augusztus 14. https://www.digitalhungary.hu/kultura/Hogyan-manipulal-a-Facebook/3175/

24 Glózer i. m. 160.

25 Kemp (2023) i. m. t

26 Az elmúlt évek során nagyon sok cikk és tanulmány született az 'Arab Tavasznak', vagy más néven a 'tavaszi Facebook-forradalomnak' is nevezett jelenségről. 2010 végén a jázminos forradalom vette kezdetét Tunéziában, amikor is az utcára vonult tüntetők követelték a korrupció felszámolását, az élelmiszerárak és a munkanélküliség csökkentését, valamint a politikai szabadságjogok megadását. Ezt követően aztán az arab világ több országában is forrongások törtek ki, amelyeknek egy részét sikeresen elfojtották a helyi kormányok, de több helyen a tüntetők megdöntötték az évtizedek óta uralkodó despotikus vezetők hatalmát, erőszakos tüntetéssorozatok eredményeként.

esetében is tette. Mert vajon internet nélkül milyen szerepet játszhattak volna a Nobel-békedíj elnyerésére jelölt bloggerek, Váil Ghoneim vagy Leyla Ben Mortada?

A közösségi médiát az interaktivitás konstituálja, tehát az online teret a felhasználók töltik meg tartalommal. A rendelkezésre álló eszközök sokfélesége, azok mozgathatósága, valamint a megfigyeltség érzésének hiánya a felhasználók egyre szélesebb körét bírja közreműködésre. De mi az, ami még nagyobb hajlandóságot vált ki a felhasználók további közreműködésében? Az önkifejezés. Az internetes online platformok az élet minden területét lefedik, „[a] kapcsolódásoknak köszönhetően egyszerre keletkeztetnek tudást a rendszer több pontján, amely tudások halmozódása az egyéni közreműködés miatt korlátlan".[27] A közösségi felületekhez való kapcsolódás melletti fő érv pedig nem más, mint a (látszólagos) önkéntesség, hiszen ez inkább kiváltságként jelenik meg a felhasználók szeme előtt, és ez a kivételesség, és az önmegmutatás iránti vágy az, ami leginkább hozzájárul a bevonódás és a tartós elköteleződés létrejöttéhez.

2. Digitális utópizmus egy szabadelvű, egyenlő társadalom megteremtésében

A digitális utópizmus ideológiája szerint egy szabadelvűbb és egyenlőbb társadalom kialakításában az elektronikus médiumok segítségül szolgálhatnak, a mindennapi életben pedig ennek megfelelően a világpolitika színterén intenzíven is megjelennek. Az internet és világháló használata a kommunikációs környezetet egyszerre szélesítette ki és törte darabokra, így a diktatórikus berendezkedésű államok esetében a világhálóban rejlő potenciál sem úgy jelenik meg, mint egy liberális demokrácia kontextusában:

> „[...] a horizontális, nem hivatalos kommunikációs hálózatok összekapcsolódása gyengíti a hagyományos média által elért eredményeket. Az ár, amelyet az egalitarizmus internet által biztosított, örömteli növekedéséért fizetünk, a decentralizált hozzáférés szerkesztetlen történetekhez."[28]

Az új média differenciált közönséget vonz, ami többé már nem tekinthető tömegközönségnek, hiszen a beérkező üzenetek és források sokasága miatt maga a közönség is jobban szelektál, saját maga választja ki a hozzá érkező üzeneteket, ezzel erősítve az individuális kapcsolatok szegmentálódását.[29] A szabadelvűbb, egyenlőbb társadalom lehetőséget teremt arra, hogy mindenki, aki szólni kíván mindenféle erős érdek közvetítése nélkül, az megteheti. A közösségi média szépsége tehát magában a hozzáférhetőségében rejlik.[30] Ugyanakkor működésében benne van az is, hogy nem csak egyéneket, de akár csoportokat is elszigetelhet egymástól, amely elszigetelődés gyakorlati következményeként az úgynevezett *echo chamber*,

27 Kepe i. m. 60.

28 Der Standard: Ein avantgardistischer Spürsinn für Relevanzen. *Der Standard*, 2006. március 10. https://www.derstandard.at/story/2372764/ein-avantgardistischer-spuersinn-fuer-relevanzen

29 Manuel Castells: Az új média és a tömegközönség diverzifikációja. In: Angelusz Róbert – Tardos Róbert – Terestyéni Tamás (szerk.): *Média, nyilvánosság, közvélemény – Szöveggyűjtemény.* Budapest, Gondolat, 2011. 952.

30 Iványi (2014a) i. m. 123.

vagyis a 'visszahanghatás' jelensége[31] jön létre. Tehát a közösségi médiában elfoglalt pozíció az egyén gondolkodásmódjára és véleményére nagy hatással bír.

A digitális utópisták úgy vélik, hogy az új technológiák a demokratikus részvételre, az egyenlőségre és az egyéni szabadságra egyaránt lehetőséget teremthetnek. Ennek irányában több olyan terület is van, amelyben az ideológia segíthet a szabadelvű, egyenlő társadalom alakításában:

1) *Digitális részvétel és demokrácia:* a digitális eszközök lehetőséget teremtenek szélesebb társadalmi réteg részvételére, például a politikai folyamatokban. A demokratikus eszközök és az információs technológia által támogatott részvételi formák a polgárok közvetlen részvételét segíthetik elő a döntéshozatalban, azonban a szak- és nagypolitika ingerküszöbét a közösségi média csak az elmúlt években kezdte elérni. Az állampolgárokat az őket érintő döntésekbe bevonó eljárások, az állampolgári tanács,[32] a részvételi költségvetés, a kooperatív kormányzás és az ezekhez hasonló eljárások világszerte egyre elterjedtebbek. Azonban komoly kihívást jelent, hogy a részvétel mindenki számára lehetséges legyen, és valóban mindenki szóhoz is jusson, ne csak az amúgy is magas érdekérvényesítő képességgel rendelkező csoportok kapjanak újabb lehetőséget az érdekeik képviseletére, továbbá fontos az is, hogy ezek az eljárások ne csak látszatintézkedések legyenek, hanem valóban lehetővé tegyék a mindenki számára nyitott, egyenlő, informált és nem utolsó sorban racionális párbeszédet. A kilencvenes években az internet és a demokrácia kapcsolata közhely lett, de vajon a közösségi média és a demokrácia kapcsolata is erre a sorsra jut az elkövetkező években?
2) *Hozzáférhető oktatás és e-learning:* számos reformpedagógiai irányzat és módszer épül a diákok aktív részvételének ösztönzésére, és mivel a 'részvételi kultúra' maga is a tanulás fontos terepe, az aktív médiabeli részvétel nemcsak az írás, olvasás készségét fejleszti, hanem az önkifejezést, sőt akár az állampolgári szabadságjogok iránti érzékenységet is. „A [...] médiakörnyezet által megkövetelt újfajta felkészültségek között szerepel az információk hitelességének és megbízhatóságának megítélésére, a különféle médiumok közötti navigációra, az információ keresésére, szintetizálására és disszeminációjára való képesség, és a különböző közösségek, nézőpontok, alternatív normák közötti mozgás és

31 A visszahanghatás-jelenség lényege, hogy a közösségimédia-felületet használó számára következetesen csak a sajátjával megegyező véleményeket közvetítenek, és ennek következtében az egyén valóságérzékelése átalakul. A kifejezést 2001-ben először az amerikai társadalomkutató, Cass Sunstein alkalmazta, elsősorban az online felületek létrejöttével egyidőben megjelenő politikai véleménynyilvánítás és -formálás átalakulásának problematikájával kapcsolatban.

32 2021. január 13.-án megkezdte munkáját a „Deutschlands Rolle in der Welt" névre keresztelt állampolgári tanács, amely létrehozásának és felállításának célja, hogy a német társadalmat is bevonják a külpolitika irányításába, és a Bundestag számára ajánlásokat nyújtsanak be a kisorsolt állampolgárokból álló tanácsi üléseken meghozott döntéseikből. A sorsolási eljárás során 160 állampolgárt választanak ki – leképezve ezzel a német társadalom életkori, nemi, képzettségi megoszlását – akik mindannyian kapnak egy témát, amelyet mindig más összetételű kiscsoportban vitatnak meg a többi résztvevővel. A tanácskozások mindegyike professzionálisan moderált és dokumentált, különféle szakértők bevonásával történik. Az állampolgári tanács felállításától elsősorban azt várják, hogy az képes legyen a társadalom és a parlament közötti távolság áthidalására, és a demokráciába vetett bizalom erősítésére. Bürgerrat – Deutschlands Rolle in der Welt: Auftakt für den Bürgerrat „Deutschlands Rolle in der Welt". *Buergerrat.de,* 2021. január 13. https://deutschlands-rolle.buergerrat.de/presse/pressemitteilungen/auftakt-fuer-den-buergerrat-deutschlands-rolle-in-der-welt/

egyeztetés készsége,"[33] amely műveltség egyébként fejleszthető a különböző oktatásban is megjelenő technikáknak és lehetőségeknek köszönhetően.

3) *Digitális egyenlőség:* a fejlett társadalmak tagjai életének a digitalizáció megkerülhetetlen része, a digitális analfabetizmus – a szegénység mellett – önmagában is sokszor a társadalomból való kirekesztettséget okoz. Az internettel való rendelkezés pedig a fejlett országok lakosainak nagy része számára természetes életkörülménnyé vált. A Covid 19-világjárvánnyal azok, akik a digitális térben nem mozogtak kellő magabiztossággal vagy a technológiai vívmányokkal egyáltalán nem barátkoztak meg, hatalmas hátrányba kerültek, hiszen annak következményeként, hogy nem használták a világhálót, nem fejlődtek a digitális készségeik, így hosszú távon a munkavállalás során is csökkentek az esélyeik.
4) *Megosztásgazdaság (megosztott gazdaság):* a digitális utópisták támogatják azokat az elveket, amelyek szerint az új gazdasági modellek lehetővé teszik az erőforrások hatékonyabb felhasználását és az eszközök közös használatát, amely tényezők egy szabadelvű, egyenlő társadalom irányába mutatnak. A *sharing economy*[34] ötletét számos szakosodott online platform segíti, amelyek lehetőséget adnak az eszközök jobb kihasználása által a pozitív környezeti hatások kiváltására és ezzel egy hatékony és fenntartható működés elősegítésére. A megosztott gazdaságban legalább annyiféle negatív, mint amennyi pozitív potenciális jövőkép rejtezhet.[35]
5) *Adatvédelem és önrendelkezés:* A digitális utópisták hangsúlyozzák az egyéni adatvédelem fontosságát és támogatják azokat az intézkedéseket, amelyek az egyének személyes adatainak védelmét szolgálják. Az adatok feletti ellenőrzés, valamint az önrendelkezés lehetőségei a szabadság és egyenlőség értékeivel egyeztethetők össze. „A közösségi oldalak szabályrendszerét akár egyfajta önszabályozásnak is lehetne tekinteni, de ebből hiányzik a külső ellenőrzés bármilyen formája."[36] A közösségi média esetében a szabályozás alanya nem más, mint maga a felhasználó, ezért esik inkább a magánszabályozás formája alá.

A közösségimédia-platformok legmarkánsabb hatása a társadalmi kommunikációra, végső soron pedig a demokratikus nyilvánosság működésének drasztikus átalakítására volt. Az új

33 Glózer i. m. 160.

34 A megosztáson alapuló, közösségi gazdaság fogalma az autómegosztás, a szállásmegosztás révén ismerősen csenghet, azonban ennél jóval bővebb tartalommal bír. A digitalizáció pedig további lehetőséget adott arra, hogy az így kialakuló szívességi hálózatok sok embert kössenek össze, ezzel megnyitva az utat a közösségi megoldások előtt.

35 Koen Frenken, az innovációs tanulmányok kutatóprofesszora 2017-ben megjelent tanulmányában három lehetséges jövőt képzelt el. Az első ezek között az elkapitalizálódás, amelyben a megosztásos gazdaság nem fog különbözni a hagyományostól, a munkavállalók ugyanúgy a kizsákmányolás áldozatai lesznek, a gazdaság zöldülése sem fog bekövetkezni, hiszen a vállalatoknak ez ugyanúgy nem fogja az érdekét szolgálni. A második verzió szerint az állam magára vállalja az újraosztás szerepét a tőkére helyezett nagyobb adókkal és a munkát terhelő járulékok csökkentésével, ami sokszor helyi szintű tervezést igényelne. Ennek a verziónak a célja a teljes körforgásos gazdaság elérése. A harmadik lehetséges jövő pedig az, ami a megosztásos gazdaság valójában lenni akar. Minden a résztvevők kezében van, a profitból is ők részesülnek, és a béreket is ők határozzák meg. Ennek két megvalósulási formája lehetséges: vagy minden a résztvevő tulajdona, vagy a megosztott javakat egyénileg tulajdonolják, de a platform és a profit a közösségé. Koen Frenken: *Political economies and environmental futures for the sharing economy*. Utrecht, The Royal Society Publishing, 2017.

36 Papp János Tamás: *A közösségi média szabályozása a demokratikus nyilvánosság védelmében.* Budapest, Wolters Kluwer Hungary, 2022. 147.

kommunikációs felületek így nemcsak már korábban is érvényes kérdéseket éleztek ki még inkább, hanem teljesen új kihívásokat is magukkal hoztak. A közösségi médiáról szóló értekezések az elmúlt években új szakaszba léptek; míg korábban a demokratikus nyilvánosság formálásában betöltött szerepe, annak pozitív és negatív értelemben megnyilvánuló ereje állt a diskurzus középpontjában, a hangsúly ma már inkább a bevezetett új rendelkezések alkalmazására és hatékonyságára tevődik át. „A különböző kormányok a közösségi oldalakban rejlő lehetőségek kihasználása mellett különböző módon próbálják szabályozni őket."[37] A hatalmi pozíciókban lévők dominanciájának fenntartásában a média is közreműködik, mivel a hierarchikus és hatalmi viszonyokat tartalmazó és igénylő internet átalakítja a társadalmat, és mivel „az emberi kommunikáció új közvetítője jön létre, egy olyan, amelynek hatása a gazdasági és társadalmi életünkben meghaladja az összes korábbi forradalmat – a nyomtatását, telefonét, televízióét és számítógépét."[38] A politikai események alakításában azért is tölt be fontos szerepet az internet és a közösségi média, mert a hagyományos médiumoktól eltérően nem egyirányú tömegkommunikációs eszközről beszélünk, hanem arra is lehetőséget ad, hogy akár tömegek kommunikáljanak egymással, aminek egyértelműen mind politikai, mind társadalmi vonzatai is vannak. A közgazdaságtanból kölcsönzött metafora szerint az internet média világára gyakorolt hatásának három jelentős tényezője van:

– az emberek tömérdek mennyiségű információhoz férhetnek hozzá az internetnek köszönhetően,
– a hétköznapi emberek is lehetőséget kapnak, hogy véleményüket nyíltan hangoztassák, valamint
– csoportok szervezhetik saját tevékenységüket a segítségével.[39]

Az internet a végtelen választások szabadságával és a kötetlenség érzésével szabadítja fel a felhasználókat, amire a közösségi média egalitárius felfogásával még inkább rásegít. A technológia segítségével a társadalmi valóság a vágyott módon alakítható át, az sokféleképpen használható fel, és mivel az internet önmagában semmit nem ír elő, semmi nem következik belőle. És bár a digitális média a társadalmi mozgalmak kibontakozásában valóban elvi lehetőségeket biztosít, azok gyakorlati megvalósulása számos egyéb hatalmi tényező függvényében jelenik csak meg. Az online diskurzusok domináns platformjai voltaképpen privatizálták az interneten rendelkezésre álló közösségi teret, és az ott megengedett megnyilvánulások szabályainak meghatározását is. De mi van akkor, ha „az információ nem érdemli meg a szabadságot"?[40]

37 Uo. 216.

38 Don Tapscott: *The Digital Economy.* New York, McGraw-Hill, 1996. XIII.

39 Clay Shirky: The political power of social media. Technology, the Public Sphere and Political Change. *Foreign Affairs*, vol. 90., no. 1. (2011). https://www.foreignaffairs.com/political-power-social-media

40 Jaron Lanier: *You Are Not a Gadget.* New York, Alfred A. Knopf, 2010. 22.

3. Aktív befolyásolás és a közösségi média szerepe a félretájékoztatásban és a kiskorúak védelmében

„Ha tőlem függene, a sajtótörvénynek csak egy paragrafusa volna: hazudni nem szabad."
(Deák Ferenc)[41]

Az utóbbi években a közösségi média demokratikus nyilvánosságra gyakorolt hatásának vonzata az úgynevezett álhírek megjelenésében és egyre nagyobb térnyerésében öltött testet. A közösségi oldalak tömegbefolyásoló hatása, valamint azok tájékoztatásban betöltött szerepének megerősödése nagyban hozzájárult ahhoz, hogy a manipulatív vagy elfogult módon bemutatott hírek – sőt sokszor a minden valóságalapot nélkülöző álhírek – igencsak elterjedtek, és kifejezetten az érzelmek és a személyes hitek befolyásolására irányultak. Megállapíthatjuk, hogy a fiatal korosztály, az alfa generáció az, amelyik a legnagyobb mértékben kapcsolódik a közösségi médiához figyelembe véve természetesen azt is, hogy a közösségi platformok és az internetes hálózatépítés minden korosztály körében egyre népszerűbbé vált az elmúlt években. „Manapság alapvető és létfontosságú készség vagy technika az a képesség, hogy megkülönböztessük a dezinformációt a valóságon alapuló, valódi hírektől."[42] De mivel ennek a tudásnak az elsajátítása hosszú és fáradságos munka hozadéka, amely olykor a felnőtt felhasználók számára is megpróbáltatást jelent, így mit várjunk el a fiatalabb korosztálytól? A közösségi média lényegében ellenőrzés nélkül oszt meg óriási mennyiségű hírtartalmat, ami elvezet egészen az álhírek megjelenéséig, illetve azok gombamódszerű terjedéséig.[43]

A közösségi médiában a kiskorúak védelmével való kapcsolatban az utóbbi időben egyre több és szélesebb körű politikai fórum kezdett foglalkozni.[44] És ami eddig abszurdnak tűnt – hogy egy 18. életévét betöltött személy pert indítson a szülei ellen a 18. életévének betöltését megelőzően kialakult sérelmes helyzet miatt, amelyet a róla nyilvánosságra hozott képek okoztak –, valósággá vált. De a gyermek egyetlen lehetősége, hogy megvárja, amíg nagykorú lesz, és csak akkor léphet fel az őt éveken keresztül sértő, megalázó, vagy bántó helyzet ellen?[45]

Véleményem szerint a fiatalabb felhasználókra hat(hat)nak leginkább a közösségi médiában napjainkban megjelenő álhírek, ami a társadalmi változások előmozdításában rejlő ki-

41 Nógrádi Gábor: *Ide nekem a címlapot is! A médiakapcsolatok művészete.* Budapest, Presskontakt Bt., 2004. 13.

42 Czeglédi Csilla – Veresné Valentinyi Klára – Borsos Eszter – Szira Zoltán – Varga Erika: Az álhírjelenség a közösségi oldalakon. *Acta Carolus Robertus*, 2020/1.

43 Uo. 19.

44 Az Európai Bizottság 2024. május 16-án eljárást indított a Meta ellen annak megállapítására, hogy a közösségi platformokat üzemeltető vállalat a Facebook és az Instagram szolgáltatásai esetében megszegte-e a DSA kiskorúak védelmére vonatkozó fejezeteit. Az eljárás során a Bizottság azt vizsgálja, hogy a Meta eleget tesz-e a digitális szolgáltatásokról szóló jogszabályból folyó, a Facebook és az Instagram online interfészei kialakítása által okozott kockázatok értékelésére és csökkentésére vonatkozó kötelezettségeinek, vagyis, hogy megfelelően csökkenti-e annak a kockázatát, hogy ezek a rendszerek kihasználják a kiskorúak gyengeségeit és tapasztalatlanságát, valamint, hogy függőséget okozó magatartást vonjanak maguk után. Az elkészült értékelés a gyermekek testi és lelki jólétéhez, valamint jogaik tiszteletben tartásához fűződő alapvető jog gyakorlásával kapcsolatos lehetséges kockázatok elhárításához szükséges. Ha pedig az eljárás eredménye az, hogy a Meta mulasztást vétett, akkor az a digitális szolgáltatásokról szóló jogszabály megsértését jelentené.

45 Ennek a témának a mélyebb megismerésére ajánlom Evellei Evelin Molli – Tamás Bianka: A gyermek és a szülő alapjogi versenye online közegben. *Infokommunikáció és Jog,* 2017/Különszám. https://szakcikkadatbazis.hu/doc/9745856

hívásokban hatványozottan is igaz, és mivel a mai fiatalok életét át- és átszövi az internet világa, a folyamatosan változó netes kultúra is hatással van a szokásokra. Fontosnak találom a téma beható vizsgálatát, hiszen a közösségi média aktív befolyásolása, és ezen belül az álhírek jelensége és tömegbefolyásoló hatása a gyermek és kamasz korú felhasználókra, de leginkább a Z és alfa generációkra[46] nézve a legveszélyesebb, éppígy fontos a kiskorúak védelmének érdekében végzett elektronikus média területén eddig véghez vitt szabályozás is.

3.1. Rövid esettanulmány: a háború hatása a közösségi médiára, vagy a közösségi média hatása a háborúra?

> „A média, ha nem is mondja meg, hogy az ember mit gondoljon, azt azonban mindenképp, hogy mire." (Bernard Cohen)[47]

Húsz-harminc évvel ezelőtt a háborúban szenvedő ártatlanok történeteit nagyobb részt profi fotósok és riporterek szemüvegén keresztül láthattuk. Manapság azonban a *részvétel kultúrájá*ban bárki egy kattintással elmondhatja saját történetét, ahogyan azt napjainkban is látjuk az orosz–ukrán, vagy az izraeli háború esetében. Egy olyan közegben, ahol minden írott szónak nyoma van a társadalmi változások előmozdításában, ott a közösségi média is aktívan hat. Sok elemző gondolja úgy, hogy az újonnan kialakult médiakörnyezet sokkal inkább szolgál arra, hogy bevonja a társadalmat a közügyekbe, mint azt a 'régi' média tette. Tegyük hozzá, hogy ezért is játszhat fontos szerepet az internet a politikai események alakításában, mert egész közösségek kommunikációjának ad lehetőséget. „A digitális média eszközei lehetővé teszik a korábban szétszórt közösségek számára, hogy szinkronizálják véleményeiket, koordinálják lépéseiket, és hogy dokumentálják az eseményeket."[48]

Az internet és a közösségi média korlátlan információáramlásának köszönhetően az emberek olyan eseményekről is értesülhetnek, amelyekről korábban nem is hallottak, illetve a már hallott eseményekbe akár részleteiben is beleláthatnak. Az emberek között indult párbeszédek pedig alapot adhatnak, és elősegíthetik az állampolgári részvételt a politikai folyamatok alakulásában. „Az autoriter kormányok is felismerték, hogy egy jól szervezett közösség korlátozhatja a politikai vezetés mozgásterét, s ezért igyekeznek elfojtani az állampolgárok közötti kommunikációt."[49] A közösségi oldalak az álhírek terjedésében egyértelműen hatékonyan közrejátszanak, azonban azok sokféleségéből is adódik, hogy nagyon nehéz egyértelműen meghatározni a hamis hírek körét.

Egészen különleges esettanulmány alapjául szolgálnak a közösségi médiában közvetített fegyveres konfliktusok, hiszen ezek megjelenésével egyidőben a dezinformációk is előtörnek a digi-

46 A Z generációt (Zoomerek) leggyakrabban az 1995 és 2005 közötti időszakra teszik. Ez az első olyan társadalmi generáció, amelynek tagjai fiatal koruk óta hozzáférnek az internethez és a hordozható digitális technológiákhoz. Az alfa generáció a Z generációt követő demográfiai csoport, többnyire 2010-től kezdve számoljuk és 2025-ig fog eltartani. Ennek a generációnak a szórakoztatását egyre inkább az elektronikus technológia, a közösségi hálózatok és a streamingszolgáltatások uralják. A két generációban sok közös vonás fedezhető fel, azonban a leglényegesebb, hogy ennek a két generációnak a tagjai meglehetősen kiszolgáltatott helyzetben vannak, hiszen ők már a digitális világ részeinek tekinthetők, de nincs előttük mintakövetési lehetőség.

47 Iványi (2014b) i. m. 70.

48 Shirky i. m.

49 Iványi (2014b) i. m. 69.

tális térben, és nemcsak a technológia segítő, hanem annak manipulatív oldala is megnyilvánul. „Az információáradat hosszú távon veszélyeztetheti a mentális egészséget és a nem tudatosan használt digitális platformokon keresztül beáramló hírek további káros hatással bírhatnak, főleg, ha azok nem megfelelő forrásból származnak."[50] A digitális térben az országhatárok megszűnnek, hiszen a közösségi média felületei olyan közel hozzák egymáshoz a világ különböző pontjain lévő felhasználókat, hogy a szemlélő számára a saját tapasztalataik szinte kézzelfoghatóvá, közvetlenül átélhetővé válnak. Ennek hozadékaként a közösségi média véleményvezérei a társadalmi hierarchiát szinte teljesen átrajzolják, és „napjainkban a tér mérték nélkülivé válik."[51] Történelmi tanulmányainkból, és a filmekből olyan túlromanticizált kép élhet emlékezetünkben, amely szerint a frontokon szolgáló katonák hosszú hónapokon, éveken át leveleztek szeretteikkel, ma azonban „már akár TikTok híresség is válhat az, aki szeretné humorral megfűszerezni a kiszámíthatatlanság övezte háborús körülményeket, sőt még pénzt is kereshet családjának, miközben az ukrán influenszerek is dacolnak az előrenyomuló hadsereg támadásainak kockázatával, hogy dokumentálják az európai szárazföldi háborút."[52] Kíméletlenül közeli képet kaphatunk a közösségi média által a frontvonalról, és a digitális térben is játszódó háborúról, amely ellen többen felszólalnak, tesznek fel ellenposztokat, osztanak meg fekete négyzeteket ezzel demonstrálva az ellenérzetüket, de rendszeresen tesznek közzé olyan fényképeket, és videókat, amelyek a háború brutalitásáról árulkodnak. Sokan ezért is használják a TikTok-háború kifejezést, hiszen miközben a közösségi platformokat működtetők folyamatosan a dezinformáció eltávolításán dolgoznak és visszaszorítják az illegális tartalmak megjelenését, addig huszonévesek dokumentálják az abszurditást. A közösségimédia-platformok felhasználói szinte másodpercenként jutnak új információhoz, amely gyors információáradat hosszú távon a mentális egészséget is veszélyeztetheti.

Az egyének önmagukhoz való viszonyát a digitális térben való megjelenésük lényegében megváltoztatta. Az öndokumentálás, a megosztás, valamint a külső visszajelzés igénye „felcsillantotta a személyiség vágyott formában való megélésének lehetőségét, ami által az egyén érdeklődését önmagára irányította."[53] A közösségimédia-felületek tehát a felhasználók számára olyan új dimenziót nyitottak meg, amelyben egy olyan online profil kialakítására kerülhet sor, ami a leginkább megfelel az egyén önmagáról alkotott képének.[54] A közösségi média mint hadszíntér az információalapú társadalmak korában különösen veszélyes terep. A korábban már említett Arab Tavasz során a napjainkban zajló háborús eseményekhez hasonló állapotokat már tapasztalhattunk az online térben, azonban amint láthatjuk, a közösségi média szerepe azóta jelentősen felerősödött. Az új média hatalma, a kibertér térnyerése hozzájárultak ahhoz, hogy a média adta felhajtással és félelemkeltéssel a közbeszédet hiszterizálják, ami tovább rontja a háborúk miatt amúgy sem felhőtlen közhangulatot.

50 Patró Viktória Lilla: A háború hatása a közösségi médiára. *Nemzeti Közszolgálati Egyetem, Európa Stratégia Kutatóintézet, Európai Polgári Kezdeményezés Figyelő.* 2022. március 01. https://eustrat.uni-nke.hu/hirek/2022/03/01/a-haboru-hatasa-a-kozossegi-mediara

51 Marc Augé: *Nem-helyek. Bevezetés a szürmodernitás antropológiájába.* Budapest, Műcsarnok Nonprofit Kft., 2012. 46–52.

52 Patró (2022) i. m.

53 Kepe i. m. 66.

54 „A közösségi médiában ún. online identitás jön létre, amely az interneten történő személyes megjelenésünk valós és fiktív részeit egyaránt tartalmazza. Ennek része a teljes mértékben kitalált ún. virtuális identitás [...], valamint a digitális identitás, amely egyértelműen a valós személyhez köthető. A digitális identitás azt az adathalmazt jelenti, amely az „én"-t reprezentálja a különböző digitalizált felületeken; ennek egy részét mi magunk hozzuk létre és alakítjuk elképzeléseink szerint, más része viszont akaratunktól függetlenül, mások online jelenlétéhez kapcsolódóan létezik." Uo.

Ahogy látjuk, a közösségi média évről évre egyre jobban beférkőzik a szabad perceinkbe, átszövi a mindennapjainkat, teret kínál, és ha meg tudjuk tartani az egyensúlyt az online és a valódi világ között, akkor összességében egy nagyszerű eszközként aposztrofálhatjuk azt. A piacra egymás után lépnek be az új, feltörekvő platformok, és próbálnak meg versenybe szállni a befutott óriásokkal. A különböző felületek egymással is folyamatosan versenyeznek, hogy a felhasználók az ő felületükön töltsék a legtöbb időt, ezzel dominálva a közösségi hálózatok között. A közösségi média egy olyan eszközt ad az emberek kezébe, amely a hírolvasás, a hirdetések, továbbá a politikai diskurzusok origójává vált rövid időn belül, és amellyel a korábbi tömegkommunikációs médiumokat és csatornákat egy helyen integrálják, ezzel is egyre nagyobb teret engedve a digitális tér mindennapos használatának. A háborúk napjainkban egyszerre a kétes megbízhatóságú információs térben – a hamis információk közlésével vagy éppen manipulációval, az információk elhallgatásával vagy tudatos kiszivárogtatásával – és a frontvonalon zajlanak. Ez már valódi háború a médiában, és média a háborúban.

3.2. Alfa generációs veszélyek a közösségi médiában, és azok szerepe a társadalmi változásokban: a 'digitális bébik' kora

Mielőtt konkrétan a virtuális kihívások, valamint a 2010 után született 'digitális bébik' korában a közösségi média által generált veszélyekre, illetve azok társadalmi változásokban betöltött szerepére rátérnénk, mindenképp indokolt röviden áttekinteni – különösen az önrendelkezéshez kapcsolódóan – a különböző egyezmények által ratifikált, gyermekeket megillető alapvető jogokat.

Az 1948-ban elfogadott Emberi Jogok Egyetemes Nyilatkozata, valamint az 1952-ben megalkotott Polgári és Politikai Jogok Egyezségokmánya mint meghatározó nemzetközi dokumentumok kimondják, hogy a gyermekek joga elválaszthatatlan az emberi jogoktól. Az Egyesült Nemzetek Szervezetének 1989. november 20. napján kelt Gyermekjogi Egyezménye[55] szintén meghatározó alapvető jogokat tartalmazó dokumentum, amelyet Magyarország az 1991. évi LXIV. törvénnyel ratifikált. Ezt több más ENSZ közgyűlési határozat követte, mint például a Riyadi Irányelvek vagy a Tokiói Szabályok, amely egyezmények a fiatalkorúakra vonatkozó igazságszolgáltatási rendszerekről, a szabadságuktól megfosztott fiatalkorúak védelméről, valamint a szabadságelvonással nem járó intézkedésekről is szólnak többek között. Az Európai Unió Alapjogi Chartája pedig külön szól a gyermekek jogairól.

A gyermekek védelméről szóló 1997. évi XXXI. törvény (továbbiakban: Gyermekvédelmi törvény) a gyermeki jogokat, és ezen jogok érvényesítésének garanciáit, a gyermekek védelmét biztosító alap- és szakellátások formáit, a jogosultság feltételeit, az ellátások finanszírozásának elveit és intézményrendszerét, továbbá a gyermekvédelmi gondoskodás, mint hatósági tevékenység fő szabályait és a gyámügyi igazgatás szervezetét foglalja össze. A Gyermekvédelmi törvény 6. § (5) és (6) bekezdése az információs ártalmakról az alábbiak szerint rendelkezik.

55 Az Egyezmény 1. cikke értelmében gyermeknek a 18 éven aluli személyeket tekinti, kivéve, ha az illető az alkalmazandó jogszabályok értelmében nagykorúságát már korábban elérte. A 17. cikk rendelkezik a tömegtájékoztatási eszközök feladatának fontosságáról, foglalkozik a gyermekek fejlődésében betöltött szerepével és feladatával, valamint elvárja nemcsak a káros tartalmakkal szembeni védelmet, hanem a hasznos anyagokhoz és tartalmakhoz való hozzáférés biztosítását. Továbbá szükséges megemlíteni az Egyezmény 29. cikkét, amely a gyermekek oktatásának céljait, valamint az oktatásukkal szemben támasztott elvárásokat sorolja fel.

„A gyermeknek joga van emberi méltósága tiszteletben tartásához, a bántalmazással – fizikai, szexuális vagy lelki erőszakkal –, az elhanyagolással és az információs ártalommal szembeni védelemhez."

„A gyermeknek joga van ahhoz, hogy a médiában fejlettségének megfelelő, ismeretei bővítését segítő, a magyar nyelv és kultúra értékeit őrző műsorokhoz hozzáférjen, továbbá, hogy védelmet élvezzen az olyan káros hatásokkal szemben, mint a gyűlöletkeltés, az erőszak és a pornográfia."

Természetesen egyéb jogszabályok is rendelkeznek a gyermekek jogairól és hangsúlyozzák a gyermekek védelmét, privilegizált helyzetét, mint Magyarország Alaptörvényének XV. cikke, az egészségügyről szóló 1997. évi CLIV. törvény, a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény, a családok támogatásáról szóló 1998. évi LXXXIV. törvény, a munka törvénykönyvéről szóló 2012. évi I. törvény, a nemzeti köznevelésről szóló 2011. évi CXC. törvény vagy a Polgári Törvénykönyv és a Büntető Törvénykönyv, valamint eljárási kódexek.[56] Ezeken túl meg kell említenünk az információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info tv.) szabályait, amit minden Magyarországon folytatott adatkezelésre, valamint az európai országokba irányuló adattovábbításra vonatkozóan alkalmazni kell.

Az alapjogokon túl meg kell említenünk az egyébként gyakran és könnyen sérthető jogokat, mint az internet és a közösségi média használatához kapcsolódó jogok, hiszen a gyermekeket is megilleti a szólásszabadság, a gondolat- és vallásszabadság, a véleményszabadság, de ugyanakkor a gyermekmunkától, a kábítószerektől és emberkereskedelemtől, a szexuális kizsákmányolástól és kínzástól, az embertelen bánásmódtól való védelem, továbbá az erőszakkal szembeni védelem is megilleti őket. Ebből a célból kifolyólag a Gyermekjogi Egyezmény előírja a részes államokban, hogy gondoskodniuk kell a gyermekek számára a szociális, szellemi és erkölcsi jólétük előmozdítását, valamint fizikai és szellemi egészségüket szolgáló tájékoztatásról, valamint az ilyen hasznos anyagok terjesztéséről, amit többek között a különböző hazai és nemzetközi kulturális forrásokból származó tájékoztatás és anyagok előállítása, cseréje és terjesztése érdekében előmozdított nemzetközi együttműködések keretében kell megvalósítaniuk.[57] „A kibertér azért laza, mivel a fiatalok is azok, nyitottak, konvencionálisak."[58] A média a gyermekek oktatásának eszköze kell, hogy legyen, és mint az iskolai oktatásnak, hozzá kell járulnia, hogy a gyermekek ismereteit növelje a lehető legtöbb kérdéssel és témával kapcsolatban. De nem mindegy, hogy hogyan, mivel megérkezett a 'Net Nemzedék'! „A *baby boom* visszhangja még hangosabb, mint az eredeti durranás. Nyolcvannyolcmilliós. A legkisebbek még pelenkában vannak, az öregebbek húsz év körüliek. Ezt a nemzedéket nem csak a létszámában rejlő demográfiai ereje különbözteti meg a korábbiaktól, hanem az is, hogy ez az első, amely a digitális média környezetében nőtt fel. [...]A történelem során most először fordul elő, hogy egy, a társadalom számára központi jelentőségű újítást a gyerekek jobban ismernek, jobban tudnak használni és otthonosabban mozognak az új környezetben, mint a szüleik."[59]

56 Lásd: https://emberijogok.kormany.hu/gyermekek

57 Gyermekjogi Egyezmény 17. cikk *a)–b)* pont.

58 Molnár Attila Károly: A digitális kor kór. *In Medias Res,* 2013/2. 243.

59 Don Tapscott: *Growing Up Digital: How The Net Generation Is Changing Your World.* New York, McGraw Hill, 2009. 2.

Napjainkban olyan világban élünk, amikor a szülők saját maguk tesznek fel a közösségi oldalakra kisgyermekükről képeket, ami több okból sem szerencsés. Egyrészről ez egyáltalán nem veszélytelen, mert a fotókkal, a megadott információkkal mindig vigyázni kell, másrészről a gyermekeket nemcsak közvetlenül, hanem közvetve is ki lehet tenni a közösségi médiában rejlő veszélyeknek. Nyilván egy két-hároméves korú gyermek nem fog tiltakozni a kép feltöltése miatt, és nyilván nem sok szülő gondol bele, hogy mint törvényes képviselő jogosult ugyan a gyermekükről készített fotóval rendelkezni, azonban, ha ténylegesen a gyermek érdekét nézzük, akkor ezek a feltöltött képek igen súlyos kérdéseket is felvethetnek. És ma már az sem elrugaszkodott gondolat, hogy a gyermek 18. életévének betöltése után számonkérje szülein a 18. életévének betöltését megelőzően kialakult, számára sérelmes helyzetet. Így megkezdődött a generációk harca.

A közösségi médiában rejlő, a kiskorúakra leselkedő veszélyek közül két szegmenst, az egyre elterjedtebb virtuális kihívásokat, valamint a – Franciaországban már törvénnyel védett – gyermekkorú influenszerek közösségi médiában betöltött szerepét és az általuk végzett tevékenységet emelem ki a tanulmány további részeiben, mivel a gyermekekről feltöltött képek csak egy szeletét jelentik a közösségi média világában rejtőző lehetséges veszélyeknek.

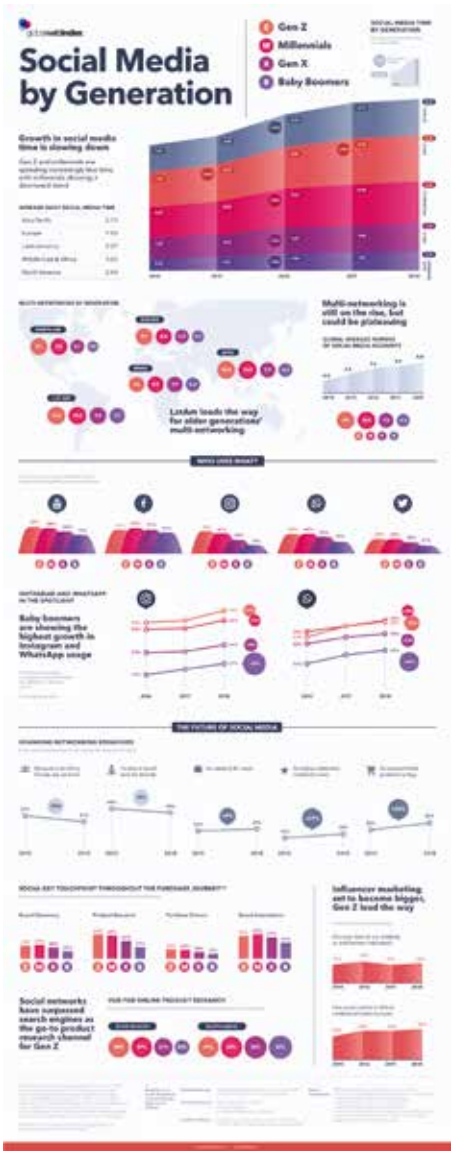
3.2.1. Virtuális kihívások és a FOMO-jelenség

Egy egyszerű keresés vagy egy közösségbe való beavatás során olyan virtuális kihívásokba ütközhetünk, amelyek a felnőttekre nézve is, de a gyermekekre különösen veszélyesek lehetnek. A gyermekek internethasználatával kapcsolatban az elmúlt időszakban számos kutatás készült, amelyek eredménye egyértelműen azt mutatja, hogy a gyermekek egyre fiatalabb koruktól kezdve naponta egyre hosszabb időn keresztül használják az internetet. A virtuális kihívások csalóka jelensége főként a 13–15 éves és annál idősebb kamaszok körében terjedt el, hiszen az egy–egy online kihíváshoz való csatlakozás egyfajta sajátos szocializációt jelent, és a kortársak közötti kapcsolatot is erősítheti. A közösségi beavatás, a kíváncsiság vagy akár a népszerűség kivívása vonzóvá teheti a sokszor félelmet keltő, akár depressziót és poszttraumás stresszt is okozó kihívásokat, amelyek terjedését a közösségi média csak felerősítette az utóbbi időben.[60] A szakirodalom és a pszichológusok a kihívásokban való részvétel okai között a már korábban is említett FOMO-jelenséget emelik ki elsőként, hiszen a kihívások teljesítésével járó társadalmi státusz, a kapcsolatok megerősítése, valamint az idealizált énkép hangsúlyozása az online trendek népszerűségében jelentős szerepet játszanak. A digitális technológiai forradalmak a *részvételi kultúrá*nak nem egyszerűen a következményeként magyarázhatók, mivel azok széles körben való elterjedése azért tud bekövetkezni, mert a tágabb kultúra is támogatja. „[A] kultúra mintegy magába szívja a médiatechnológiákban végbement robbanásszerű fejlődést, reagál arra. A részvételi kultúra és az új médiatechnológia így

60 A Nemzeti Média- és Hírközlési Hatóság közlése szerint az utóbbi években hazánkban is elterjedt, akár halált is okozó kihívások közé tartozik a fahéjkihívás, a vonat-selfie vagy a blackout. Bár a közösségimédia-platformok számos technológiai megoldással küzdenek – ezeknek a fizikai, és lelki problémákat is okozó online jelenségeknek a csökkentésére és a veszélyes kihívások szűrésére és tiltására vonatkozó irányelveket vezettek be –, mégis a mesterséges intelligencia segítségével a tiltási lehetőségek sokszor kikerülhetők. Nemzeti Média- és Hírközlési Hatóság: Mérsékelten, de Magyarországon is terjednek a veszélyes online kihívások. *Nmhh.hu*, 2023. július 21. https://nmhh.hu/cikk/240947/Mersekelten_de_Magyarorszagon_is_terjednek_a_veszelyes_online_kihivasok

kölcsönhatásban állnak egymással, valamint a körülöttük kialakuló kulturális közösségekkel és tevékenységekkel."[61]

6. ábra Közösségi média a generációk tükrében



Forrás: Ashley Viens: Visualizing Social Media Use by Generation[62]

61 Henry Jenkins – Ravi Purushotma – Margaret Weigel – Katie Clinton – Alice J. Robinson: *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century.* Cambridge–London, MIT Press, 2009. https://doi.org /10.7551/mitpress/8435.001.0001

62 Ashley Viens: Visualizing Social Media Use by Generation. *VisualCapitalist.com,* 2019. szeptember 21. https://www.visualcapitalist.com/visualizing-social-media-use-by-generation/

A „digitális bébik" korában az internet, azon belül a közösségi média az élet egyik főszereplőjévé vált. Ez önmagában is sok problémákat okozhat, valamint a számítógép előtt töltött idő vagy a telefon, a tablet nyomkodása az egészségre káros mozgáshiányhoz vezethet, de a rendszeres internetfelhasználás is súlyos pszichés problémát hordozhat magában, mégpedig az úgynevezett kettős morál kialakulását. De mit is jelent ez pontosan? Az online világban a normák megengedőbbek, mint az offline világban, és lehet, hogy az egyébként udvarias és szabálykövető gyermek az interneten másokat megalázó kommenteket tesz, ismerősei személyes adataival visszaél vagy éppen mások becsületébe gázol. Ez a fajta magatartás pedig megszokássá is válhat, minél több időt tölt a gyermek az online térben. „Mindezekről el kell beszélgetni a gyerekekkel. A beszélgetés a gyerek segítségére van abban, hogy „hogyan viselkedjen a közösségi oldalakon és mit várjon el a többi felhasználótól, ők hogyan viszonyuljanak hozzá. Megértse a közösségi média használatának veszélyeit, például, hogy megjelölhetik egy kínos fotón, amit egy partin készítenek róla majd emiatt csúfolhatják. Megértse mennyire kockázatos személyes adatokat megosztani magáról és miért kell átgondolni mindent (szöveget, képet, videót), mielőtt megosztja bármilyen közösségi platformon. Megtanulja, hogyan kezelje a rizikós szituációkat, mit érdemes tenni [...]. Tisztában legyen vele, mit tanácsos lépnie, ha valaki személyes részleteket, információkat, adatokat akar kiszedni belőle, rosszindulatúan viselkedik vele, erőszakos vagy bántalmazó magatartást mutat felé, megalázza nyilvánosan, kényelmetlen érzést vált ki belőle, illetlen megjegyzéseket tesz. Fontos, hogy a gyermek tudja, mi az, ami nem helyes és amit nem kell eltűrni [...]. Foglalkozzon a saját digitális lábnyomával! Ami egyszer felkerül a netre, örökre ott is marad."[63]

3.2.2. Generációk harca – szülő és gyermek találkozása a közösségi médiában

A korábban említett Gyermekjogi Egyezmény kiskorúak védelmére való hivatkozását a legtöbb részes állam jogrendszere magától értetődőnek fogadja el és több állam alkotmányában is külön megjelenik a véleménynyilvánítás szabadságának korlátjaként.[64] A védelem alapvető indoka, hogy a gyermekek életkori sajátosságukból és hiányos élettapasztalatukból kifolyólag védtelenek a külső hatásokkal szemben, nem képesek megfelelően kezelni az őket körülvevő

63 Sáringer Viktória: Így védd ki a gyerekekre és tinédzserekre leselkedő veszélyeket a közösségi médiában. *Közösségi média mindenkinek blog,* 2020. január 25. https://kozossegi-media-mindenkinek.blog.hu/2020/01/25/s_v_a_kozossegi_media_elonyei_es_veszelyei_a_gyerekekre_es_a_tinedzserekre

64 A spanyol alkotmány a véleményszabadság kifejezett korlátjaként nevezi meg a gyermekek és fiatalkorúak védelmét, míg az északi államok közül a finn alkotmány kimondja, hogy a véleménynyilvánítás szabadságát és az információhoz való hozzáférés jogát törvényben lehet megállapítani, a norvég alkotmány pedig lehetővé teszi a véleménynyilvánítás szabadságának előzetes cenzúráját és a megelőző intézkedések alkalmazását. A holland alkotmány a 16 évnél fiatalabb személyek jó erkölcseinek védelme érdekében tartalmaz ilyen rendelkezést, a görög alkotmányban pedig a médiával kapcsolatban jelenik meg a kiskorúak védelmének kérdése. Kóczián Sándor: *Gyermekvédelem a médiajogban.* Budapest, NMHH Médiatanács Médiatudományi Intézete, 2014. 12–13.
Hazánkban a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény rendelkezik a kiskorúak védelmét célzó alapvető szabályokkal. Az Alaptörvény XV. cikkének (5) bekezdése is annyit mond ki, hogy Magyarország külön intézkedésekkel védi a gyermekeket. XVI. cikk (1) bekezdésben pedig kimondja, hogy „Minden gyermeknek joga van a megfelelő testi, szellemi és erkölcsi fejlődéshez szükséges védelemhez és gondoskodáshoz."

valóságot, valamint érdekeiket és jogaikat sem tudják az ahhoz szükséges erővel képviselni és érvényesíteni.[65]

„A kiskorúak védelme ugyanakkor nemcsak az állam kizárólagos feladata, hanem a társadalomé is."[66] Ugyanis „az állam a digitális környezetben [...] már nem képes úgy befolyásolni az elektronikus médiát, mint korábban."[67] Elég csak megnézni a tartalommegosztó oldalakat és láthatjuk, hogy az intimitás fogalma alapjaiban átalakult. Az, hogy önmagunkat, családunkat, mindennapjainkat megmutassuk a nyilvánosságnak, életformává, létezésmóddá változott. Ma már a gyermekek egyharmada születésekor digitális múlttal rendelkezik, és az embert már születése előtt filmre veszik. Mert hány ultrahangfelvételt posztolnak hetente a közösségi felületeken? Hány gyermekről, családról készült fotót osztanak meg a nagyközönséggel a felhasználók? És mi van, ha a magánélet már csak egy elavult, idejétmúlt fogalom, sőt csupán csak illúzió? Így a szülői felelősségvállalásra egyre nagyobb hangsúly helyeződik, hiszen a szülőknek óvniuk kellene gyermekeiket a számukra ártalmas és káros tartalmaktól és hatásoktól, és aktívabban kellene részt venniük a kiskorúak védelmében. A szülői kontroll azonban nem minden esetben jelenik meg.

Kevin Park szerint „a Facebook lett az internet városközpontja."[68] A közösségimédia-felületek számos probléma forrásaként szolgálnak, hiszen rengeteg adatot, információt gyűjtenek össze, ráadásul a gyermekek esetében nem feltétlenül ők rendelkeznek a képmásuk vagy a róluk szóló információk közzétételéről. Ebben a közegben tehát a gyermek különösen nagy veszélynek van kitéve, hiszen önkitárulkozásáról nem dönthet, mégis az online életnek központi szereplőjévé válhat. Ez az internet világában bekövetkezett teljesen új változás pedig már egy új jelenségként is értelmezhető.[69] A társadalmi változások azonban hatnak a jogi változásokra, ahogyan a jog megoldásai is befolyásolják az össztársadalmi viszonyok alakulását. Elmondható továbbá, hogy a jog fejlődését az adott társadalom szabályozási szükségletei, igényei is befolyásolják. Így történt az is, hogy az Európai Unió egyik legbefolyásosabb államában, Franciaországban a kormány igyekszik korlátozni a közösségi média felhasználóira ható, romboló pszichológiai hatásokat és ennek apropójából – az uniós tagállamok közül először – zéró toleranciát hirdetett és átfogó keretet hozott létre az influenszerszektor szabályozására. Az első olyan állam, amely a gyermekkorú influenszereket külön törvénnyel védi,[70] amely szabályozásra az egész világban egyre égetőbb szükség lenne tekintettel arra, hogy évről évre egyre több a 16 év alatti, a közösségi médiában hatalmas összegeket kereső influenszer. A következőkben rövid elemzésen keresztül tekintsük át a tizenhat éven aluli gyermekek képeinek online platformokon történő kereskedelmi felhasználását szabályozó 2020. október 19-i

65 Kóczián i. m. 14.

66 Uo. 16.

67 Uo.

68 Kevin Park: Facebook Used Takedown And It Was Super Effective! Finding A Framework For Protecting User Rights Of Expression On Social Networking Sites. *N. Y. U. Annual Survey of American Law*, vol. 68., no. 4. (2013) 891., 894., 923.

69 Andrew Tutt: The New Speech. *Hastings Consitutional Law Quarterly*, vol. 41., no. 2. (2014) 235–236.

70 2019. december 17-én Bruno Studer, Gilles Le Gende és több munkatársuk törvényjavaslatot terjesztettek a Nemzetgyűlés elé, amely szabályozná a gyermek influenszerek közösségi médiában végzett munkáját. A javaslatot a módosításokkal a Nemzetgyűlés 2020. február 12-én, majd a Szenátus 2020. június 25-én fogadta el. A képviselők 2020. október 6-án véglegesen elfogadták azt, a törvényt pedig 2020. október 19-én ki is hirdették.

törvény,[71] valamint a 2023 januárjában „A gyermekek képmására vonatkozó jogok tiszteletben tartásának garantálása" című törvényjavaslat[72] részleteit.

A francia törvény és -javaslat joghézagot pótol: jogot biztosít a gyermekeknek a szüleik által gyakorolt, közösségimédia-platformokon végzett tevékenységek során. A gyermekkorú influenszerekre – tekintettel arra, hogy ez napjainkban már munkavégzésnek is minősülhet –, akárcsak a gyermekmodellekre, a munka törvénykönyvének szabályai már vonatkoznak. A 2020. október 19-i törvény értelmében azonban elsősorban a szülőknek kell különböző további szabályoknak megfelelniük – és itt elsősorban a kiskorú gyermekek által végzett olyan tevékenységekről beszélünk, amelyek nem esnek a munka törvénykönyvének hatálya alá, vagyis az úgynevezett „internet szürke területei" esetében – és új anyagi kötelezettségük is van, amely szerint a gyermekük bevételének egy részét az úgynevezett *Caisse des Dépôts et Consignations*-ban (Letéti Hivatal) kell elhelyezni, amíg a gyermek el nem éri a nagykorúságát. A törvény célja az olyan jogi keret kialakítása, amely a gyermek érdekeit helyezi előtérbe.

Az 1. cikk egy olyan jogi keretet hoz létre, amely a szórakoztató ágazatban foglalkoztatott kiskorú gyermekekre vonatkozó előzetes engedélyezési rendszert a gyermekinfluenszerekre is kiterjeszti, így azokra a kiskorú gyermekekre is alkalmazni szükséges, akiknek képét egy elérhető médiaszolgáltatáson keresztül sugározzák, valamint azokra a kiskorú gyermekekre, akiknek a végzett tevékenysége munkaviszony részét képezi. Ezzel a törvény garantálja, hogy a kiskorú gyermek foglalkoztatási feltételei összeegyeztethetők legyenek iskoláztatásával, különösen pedig egészségének védelmével.

A 3. cikk előírja, hogy az illetékes hatóságnál be kell jelenteni, ha a 16 év alatti gyermek képmása egy videómegosztó platformon időegység alatt egy meghatározottnál hosszabb ideig vagy gyakrabban jelenik meg, illetve a megjelenés a hatóság által meghatározottnál több bevételt generál, így a kiskorú gyermek munkaideje nem haladhatja meg a törvényben meghatározott küszöböt, a végzett tevékenységből fakadó jövedelmének egy részét pedig nagykorúságának elérésekor meg kell kapnia. Mindezt a törvény annak érdekében teszi, hogy a munka törvénykönyvének hatálya alá nem tartozó kiskorú gyermekek a megfelelő védelemben részesüljenek.

A törvény 2. és 4. cikkének célja a közösségi platformok felelősségteljesebbé tétele, így előírja, hogy minden olyan tizenhat éven aluli kiskorúról készített tartalmat törölni kell a felületekről, amely az előzetes egyéni engedélyezési rendszert figyelmen kívül hagyta. A 4. cikk továbbá arra ösztönzi a közösségi médiaplatformokat, hogy különösen a kiskorú gyermekek tájékoztatásának elősegítése érdekében *chartákat*[73] fogadjanak el, amely charták 'gyermeknyelven' tájékoztatásul szolgálnak az adataik, fényképeik terjesztésének magánéletükre gyakorolt következményeiről, illetve a különféle pszichológiai és jogi kockázatokról.

71 LOI n° 2020–1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne.

72 2023 januárjában Bruno Studer, Éric Poulliat és Aurore Bergé képviselők törvényjavaslatot nyújtottak be a gyermekek hálózatokon elhelyezett képmásairól, amely javaslat végső olvasatra 2024. február 6-án került. „E törvény célja, hogy emlékeztesse a szülőket arra, hogy nem tulajdonosai és nem »üzemeltetői« gyermekeik arcának, hanem inkább védelmezői" – értékelte Bruno Studer a benyújtott törvényjavaslatot. La Montagne: Proposition de loi sur le droit à l'image des enfants sur les réseaux: qu'est-ce qu'elle contient? *La Montagne.* https://www.lamontagne.fr/paris-75000/actualites/proposition-de-loi-sur-le-droit-a-limage-des-enfants-sur-les-reseaux-qu-est-ce-qu-elle-contient_14448227/

73 Ezeknek a chartáknak az elkészítéséért a Superior Audiovisual Council (CSA) a felelős.

A törvény 5. cikke kifejezett jogot biztosít a kiskorúaknak az 1978. január 6-i adatvédelmi törvény értelmében a tartalmak törléséhez vagy elrejtéséhez, ennek megfelelően tehát a gyermekeknek joga van a tartalmak eltávolításához szülői hozzájárulás nélkül is.

A 6. cikk 75.000 eurós bírságot ír elő azoknak a közösségi médiaszolgáltatóknak, akik nem tartják be a törvényben előírt kötelezettségeket.

A fent tárgyalt törvénnyel összhangban a 758. számú törvényjavaslat – amely a gyermekképi jogok tiszteletben tartását célozza – indoklásában az alábbiak olvashatók:

> „Az egyre inkább digitalizálódó társadalomban a gyermekek magánéletének tiszteletben tartása ma már elengedhetetlen biztonságuk, jólétük és fejlődésük szempontjából. [...] a jogalkotási előrelépések azonban nem elegendőek a gyermekek magánéletének teljes körű garantálásához. [...] Éppen ezért ma helyénvaló a gyermekek képmására vonatkozó jogainak kérdésével nyíltan foglalkozni [...].”[74]

A törvényjavaslat indoklása továbbá tartalmazza, hogy egyes becslések szerint egy gyermek átlagosan 1300, a 13. életéve előtt online közzétett fényképen szerepel a saját, a szülei vagy éppen valamelyik hozzátartozójának közösségi felületén. A kiskorú gyermekekről készült és a közösségi platformokon megosztott fényképek közzétételéből fakadó kockázatok leginkább a személyes adatoknak minősülő képek terjesztésének ellenőrzési nehézségében jelentkeznek – valamint érdemes megemlíteni azt is, hogy a gyermekpornográf fórumokon kicserélt fényképek ötven százalékát az először a szülők által a közösségi oldalaikon közzétett fényképek jelentik – hiszen a gyermekek hétköznapi életéről közzétett információk lehetővé tehetik, hogy beazonosítsák tartózkodási helyüket és életmódjukat szexuális ragadozás céljából. De a pedofil kockázaton túlmenően, az interneten közzétett tartalom hosszú távon károsíthatja a gyermeket anélkül, hogy a közösségi médiából való teljes törlés lehetőségével tudna élni. A törvényjavaslat lényege, hogy segítse a szülőket abban, hogy jobban tiszteletben tartsák a gyermekeik képeinek megosztására vonatkozó jogokat és tisztában legyenek az ezen a területen fennálló kötelezettségeikkel.

A két röviden bemutatott törvény és törvényjavaslat külön témában való kifejtése véleményem szerint rendkívül fontos lenne, hiszen az azokban előírtak egy önálló kutatás tárgyát képezik. Azonban összességében elmondható, hogy az egyre sokszínűbbé váló és az államok által egyre kevésbé kontrollálható média világában, már egyre inkább a tudatos médiafogyasztás szorgalmazása révén teremthető meg az emberek védelme.

„A »médiatudatosság« olyan készségeket, ismereteket és értelmezési képességeket jelent, amelyek alapján a fogyasztók hatékonyan és biztonságosan tudják használni a médiát. A médiatudatossággal rendelkező emberek tájékozottan tudnak választani, […] és jobban meg tudják védeni magukat és családjukat a káros vagy sértő anyagoktól.”[75]

A kiskorúak védelmének érdekében pedig nem lehet elégszer hangsúlyozni, hogy az új médiumok megfelelő használata mind a gyermekek, mind a szülők részéről elengedhetetlen követelmény kell, hogy legyen. Mert a szülők sokszor nem eléggé felkészültek ahhoz, hogy a digitális világban meg tudják óvni gyermeküket a lehetséges ártalmaktól, márpedig a kiskorúak

74 Proposition de loi n°758 visant à garantir le respect du droit à l’image des enfants. https://www.assemblee-nationale.fr/dyn/16/textes/l16b0758_proposition-loi#D_Article_1er

75 Audiovizuális médiaszolgáltatásokról szóló 2010/13/EU irányelv, (47) preambulumbekezdés.

védelmét célzó szabályok csak úgy érvényesülhetnek hatékonyan, ha a szülő kellő ismerettel rendelkezik, tudatában van a gyermeket érő hatásoknak, tisztában van a szabályozási eszközökkel és nem utolsó sorban tudatosan felügyeli gyermeke médiafogyasztását.

4. Összegzés

„Az emberek eddig még sosem jutottak ennyi információhoz, mint most, de ennek ellenére nem mondható el, hogy tájékozottabbak lennének. A forráskritika hiánya és a kiélezett verseny oda vezet, hogy nem az számít, igaz-e egy történet, hanem hogy érdekes-e." (Tari Annamária, pszichológus)[76]

Problémafelvetésemben a tanulmány elején azt a kérdést tettem fel, hogy milyen lehetőségek rejlenek a közösségi médiában, és azokat a társadalmi változásokban hogyan és miképpen lehet előremozdítani. Áldás, vagy átok a társadalmi változásokban a közösségi média léte? A bemutatottak alapján az látható, hogy a kérdés nem válaszolható meg egyértelműen, aminek az az oka, hogy a közösségi média – ahogy maga az internet is – elsősorban eszköz. Eszköz arra, hogy a véleménynyilvánítás lehetőségével olyan kultúra legyen kialakítható, ami politikai és állampolgári szabadságjogokat igényel. Eszköz továbbá arra, hogy a hírek mellett a nézeteket is kevésbé lehessen korlátozni. És eszköz nem utolsó sorban arra is, hogy az önkifejezés elsődleges csatornájaként biztosítsa az emberek számára a társadalmi kölcsönhatások új alakzatait, illetve a tér és idő korlátjainak leküzdését. A fő kérdés megválaszolásában a lényeg tehát az, hogy a felhasználók milyen tevékenység(ek)re használják a közösségi média adta lehetőségeket. Tudásgyűjtés, bizalomépítés, kapcsolatmenedzsment, vagy identitásmenedzsment? Esetleg önreprezentáció vagy valamely szórakozási kategória kihasználása? Ami biztos, hogy a felhasználók részéről a rendszer mozgásban tartása aktív közreműködést és tartós elköteleződést kíván, akár egyedi tevékenységről beszélünk, akár nem.

A közösségi platformok valóban lehetővé teszik a hatalmi eloszlás és ellenőrzés megvalósítását, a hatalom pedig a legdrasztikusabb lépéshez folyamodva akár el is lehetetlenítheti a felhasználók kapcsolattartását azzal, hogy kiiktatja az internet- és mobiltelefon-szolgáltatást, ahogyan erre a tanulmány ide vonatkozó fejezetében is utaltunk. Mert valóban, a huszonegyedik század legmeghatározóbb kommunikációs eszközei a közösségi oldalak. Azonban ahogyan említettem, a társadalmi változások hatnak a jogi változásokra, a jog megoldásai pedig mindig befolyásolják az össztársadalmi viszonyok alakulását. A digitális média kibontakozásával a hétköznapi felhasználók szerepvállalása és aktivitása tovább fokozódik, és egy valódi *részvétel* irányába mozdul el, hiszen a közösségi platformok segítségével az átlagember már nemcsak mint közönség lehet jelen a médiában, hanem ebben a közegben már egyszerűbben, könnyebben, és sokkalta nagyobb mértékben tud bekapcsolódni a tartalomelőállítás folyamatába is. Vagyis „a közösségi média többé már nem egy, a kiválasztott réteg számára hozzáférhető *niche*, amelyet figyelmen kívül lehetne hagyni."[77]

76 Tari Annamária: *Z generáció*. Budapest, Tercium, 2023.

77 Prasanto Kumar Roy: India's era of digital activism. A growing number of people voice their opinion online shifting the dynamics between people and power. *Al Jazeera Online*, 2024. január 06. https://www.aljazeera.com/opinions/2014/1/6/indias-era-of-digital-activism

A becsülethez és jóhírnévhez való jog megsértése a közösségi platformokon

Vitkovics Bálint

1. Bevezető gondolatok

A mindennapjainkat alapjaiban változtatja meg a jelenleg is zajló negyedik ipari forradalom, az egyre fokozódó technológiai fejlesztések hatására. Ez az igen dinamikus és rapid digitális fejlődés többek között azzal is jár, hogy életünk egy jelentős részét már a virtuális térben, online módon éljük. Ennek az új világnak a megállás nélkül formálódó együttélési szabályai több helyütt is eltérnek a hagyományos offline világ rendjétől, amelyek merőben eltérő magatartási szabályokat eredményeznek.

Konrad Lorenz értekezésében – amelyben a civilizált emberiség nyolc halálos bűnét taglalta – már figyelmeztette az olvasókat a folyamatos gazdasági versenyfutás és technológiai fejlődés kapcsán várható, szociális értelemben vett negatív hatásokra, úgymint az ember elmagányosodására, illetve a megszokott értékei, tradíciói devalválódására.[1] Mindezek arra sarkallnak minket, hogy tüzetesebben vegyük górcső alá az online platformok jelenlegi helyzetét, és vonjuk le az ezzel kapcsolatos jogi következtetéseinket: mely esetkörök azonosak vagy hasonlóak a valós és a virtuális világban, mely esetkörök térnek el jelentősen az online és offline térben, illetőleg ezek milyen jogi válaszokat igényelnek?

Jelen tanulmányunkban a vizsgálódásunk fókuszában azok a jogesetek állnak, amelyek tárgya a közösségi platformok felületén elkövetett becsület- és jóhírnévsértő magatartások. Ezzel összefüggésben azt a kérdéskört járjuk körül, hogy a közösségi platformokon milyen mértékben érvényesülnek ezek a személyiségi jogok: melyek a tipikus jogsértő magatartások, mely platformokon történik a legtöbb jogsérelem, valamint a magyar bíróság ítélkezési tevékenysége során mennyire helyez hangsúlyt az online térben történő személyiségi jogi sérelem jelenségére.

Utóbbi vizsgálódási kör esetében tanulmányunkban különös figyelmet fordítunk arra, hogy a közösségi platformon elkövetett személyiségi jogi jogsértés esetében, az ítélkezési gyakorlatban a sérelemdíj megítélése során mennyiben veszi figyelembe a joggyakorlat a virtuális világ sajátos jellemzőit, amelyek következtében az egyes személyiségi jogi konfliktusok térben és időben nem zártak, emiatt olyan személyi körhöz is el tudnak jutni a sérelmezett közlések[2] – különösen a mesterségesintelligencia-alapú algoritmusok működése miatt –, akik egyébként nem feltétlenül szereztek volna tudomást a jogsértésről, és ez adott esetben súlyosabb kihatással lehet az érintett személy társadalmi megítélésére. Ezzel összefüggésben arra is választ keresünk, hogy az ítélkezési gyakorlatunk tesz-e különbséget az online vagy offline térben megvalósuló jogsértések esetén.

1 Konrad Lorenz: *A civilizált emberiség nyolc halálos bűne*. Budapest, Helikon Kiadó, 2022. 24–36.

2 A későbbiekben látni fogjuk, hogy a jogsértő magatartások jellemzően valamilyen bejegyzést takarnak, amelyeket az érintett fél kifogásol.

Tanulmányunkban a jelenlegi magyar joggyakorlat bemutatását tűztük ki célul. Ennek biztosítása érdekében két megszorítással is éltünk. Egyrészről a releváns és gazdag szakirodalmi munkák elemzését, másrészről a nemzetközi joggyakorlat széles körű ismertetését mellőztük, mivel azok részletes bemutatása szétfeszítené a tanulmányunk terjedelmi kereteit.

A választott témánk feldolgozásában a hangsúly a nyilvánosan elérhető bírósági határozatok feldolgozásán volt azzal, hogy azon döntéseket ismertetjük érdemben, amelyek vonatkozásában a jogvita a hatályos Ptk. 2:45. §-án alapult, illetve a közösségi platformon történő jogsértés körülményeit érdemben mérlegelte döntése meghozatala során a bíróság.[3]

2. Online platformok – közösségi platformok

A különböző online felületek egyre inkább alakítják a kommunikációs szokásokat. Erre reflektálva jegyezte meg az Alkotmánybíróság, hogy az internetre olyan 'kommunikációs csatornaként' érdemes tekinteni, amely az emberek közötti kommunikáció változatos formáinak ad teret.[4] Az új kommunikációs szokások alakulásában a közösségi platformoknak is szerepük van, emiatt indokoltnak tartjuk egyrészről a platform fogalmának tisztázását, másrészt néhány közösségiplatform-használati adat ismertetését.

2.1. A platform fogalma

Ződi Zsolt a platformok megjelenésére mint az internettel együtt járó információs válság következményére tekint, amelynek célja a válság megfelelő irányítása és lehetőség szerint ennek a válságnak a kezelése. A válság okozójaként a korábban nem látott adatgazdagságot, az online világban egyre szaporodó interakciót említhetjük. Álláspontja szerint a platformok elsődleges feladata ennek a megtapasztalt újfajta bőségnek a koordinálása, kezelése algoritmikus működés útján.[5] Nem véletlen, hogy a hatékony működés biztosítása érdekében egyre nagyobb szerep jut a mesterséges intelligenciának (MI) az adatok feldolgozása, azok rendszerezése és elemzése során. A minél optimálisabb felhasználói élmény garantálása érdekében az MI bizonyos magatartási mintákat, illetve az éppen aktuális trendeket veszi figyelembe, ezáltal képesek az egyes platformok személyre szabott és célzott szolgáltatást nyújtani.[6]

3 Kutatásunk során az egyes határozatokat a Bírósági Határozatok Gyűjteményéből töltöttük le azzal, hogy a korlátozott precedensrendszerre is tekintettel azon jogvitákat dolgoztuk fel, amelyek tárgyában a Kúria döntött. Figyelemmel arra, hogy több vizsgált jogesetben a különböző bírósági szinteken eltérő döntések születtek, tanulmányunkban nem kizárólag a Kúria értékelési szempontrendszere jelenik meg, hanem az alsóbb szintű bíróságok értékelései is.

4 165/2011. (XII. 20.) AB határozat, Indokolás IV/1.4. pontja.

5 Ződi Zsolt: A platform mint elméleti konstrukció és mint narratív keret. A platformfogalom kialakulásának történetei. In.: Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika Egyetemi Kiadó, 2022. 18–19.

6 Ld. Domokos Márton: A mesterséges intelligencia szerepe az internetes platformokon – Szabályozási kihívások. In: Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika Egyetemi Kiadó, 2022. 403.; Ződi Zsolt: Algoritmikus koordináció a platformuniverzumban. A platform mint új koordinációs mechanizmus és ennek jogi következményei. In: Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest, Ludovika Egyetemi Kiadó, 2021. 500–501.

Az MI alkalmazása az előbb említett előnyök ellenére azonban számos aggályt is felvet – például az adatvédelem vonatkozásában.

A szakirodalom emellett felhívja még a figyelmet a platformok tömegjellegére, mivel egy sikeres online platformnak a tömegekhez kell szólnia, és fenn is kell tartania a tömegek érdeklődését.[7]

Jogi szempontból 2015-től kezdődően tekinthető egyre fajsúlyosabbnak a platform mint jelenség, amely különböző kodifikációs megoldásokhoz vezetett.[8] E körben az egyik nagy visszhangot kiváltó vita a platformüzemeltetők felelőssége körül bontakozott ki, a felületükön biztosított interakciók vonatkozásában.[9] E kérdés megválaszolása jogilag komplex, mivel a magánjogi megközelítés mellett figyelemmel kell lenni az olyan komoly közjogi megalapozottsággal bíró kérdésekre is, mint a véleménynyilvánítás szabadságának érvényesülése. Ezt az alapjogi relevanciát csak erősíti az utóbbi időben kirajzolódó azon tendencia, miszerint az emberek egy része a közös ügyeiket érintő véleményének egyre inkább a különböző közösségi platformokon ad hangot.[10] Az e körben felmerült kérdések kapcsán egyre fokozódott az igény a hatékony szabályozás iránt. Ennek egyik ismert esete volt a hatékony moderálás kereteinek kidolgozása körében történt diszkurzus.[11] A felelősségi kérdés további komplexitását adja az online szolgáltatások határokon átnyúló jellege is, amely szintén növeli a normaalkotás iránti igényt.[12]

A platform jogi definíciójának megadása terén egészen a közelmúltig kihívással álltunk szemben, mivel nem volt egységes fogalom – ez részben magyarázható volt a platformok sokszínűségével.[13] E téren azonban jelentős változást hozott a digitális szolgáltatásokról szóló DSA rendelet,[14] ami többek között egy komplex fogalomrendszert hozott létre. A rendelet bevezette a közvetítő szolgáltatás fogalmát, amely három különféle szolgáltatást foglal magában: az egyszerű továbbítást, a gyorsítótárazást, valamint a tárhelyszolgáltatást.[15] Témánk szempontjából a tárhelyszolgáltatás bír relevanciával, amelyet a rendelet olyan szolgáltatásként ír le, „amely a szolgáltatás igénybe vevője által küldött és a szolgáltatás igénybe vevőjének kérésére tárolt információ tárolásából áll".[16] A tárhelyszolgáltatás amiatt fontos, mivel a rendelet

7 Kiss György: A digitális platformok általi foglalkoztatás társadalmi, gazdasági hatásai és a jog válasza. In: Török–Ződi (szerk.) (2022) i. m. 92.

8 Ződi Zsolt (2022) i. m. 31.

9 Ld. Menyhárd Attila: A platformok polgári jogi felelőssége. In: Török–Ződi (szerk.) (2022) i. m. 130–132.; Ződi Zsolt: *Platformok, robotok és a jog. Új szabályozási kihívások az információs társadalomban.* Budapest, Gondolat Kiadó, 2018. 108–113.

10 Mezei Kitti – Szentgáli-Tóth Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In: Török–Ződi (szerk.) (2022) i. m. 327–329.; Koltay András: *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása*. Budapest, Wolters Kluwer Hungary, 2019. 190–193.

11 Ld. Török Bernát: A szólásszabadság a közösségi platformokon és a Digital Service Act. In: Török–Ződi (szerk.) (2022) i. m. 195–201.; Szikora Tamás: A platformszabályozás egy új iránya Donald Trump Facebookról való kitiltásának példáján keresztül. In: Török–Ződi (szerk.) (2022) i. m. 209–211.

12 Ld. a joghatósági kihívások tárgyában Gombos Katalin: A Digital Service Act és a Digital Markets Act várható kihívásai a jogalkalmazásban. *In Medias Res,* 2023/2. 109–113.

13 Ld. Belényi Pál: Digitális és technológiai piacok közgazdasági kérdései. In: Tóth András (szerk.): *Technológia jog – Új globális technológiák jogi kihívásai.* Budapest, KRE ÁJK, 2016. 11.; Ződi Zsolt (2018) i. m. 102–103.; Koltay András (2019) i. m. 189.

14 Az Európai Parlament és a Tanács (EU) 2022/2065. számú rendelete a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (a továbbiakban: DSA rendelet).

15 DSA rendelet 3. cikk *g)* pont.

16 DSA rendelet 3. cikk *g)* pont iii. alpont.

meghatározza az online platform fogalmát is, amelynek részét képezi a tárhelyszolgáltatás fogalma. A rendelet szerint ugyanis az online platform „olyan tárhelyszolgáltatás, 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 funkcionalitása, amely 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."[17]

A közösségi platformra az online platform egyik sajátos altípusaként tekintünk. Ezt a rendelet is megerősíti, amikor a preambulumbekezdéseinél a közösségi hálózatot az online platform altípusaként említi.[18] Tanulmányunkban közösségi platform alatt az olyan MI-alapú algoritmusos működésen nyugvó online közvetítő felületet értjük, amelynek célja a személyek közötti kapcsolattartás elősegítése, valamint különböző szolgáltatások nyújtása. E munkadefinícióra tekintettel a Magyarországon is nagy népszerűségnek örvendő közösségi média főbb reprezentánsait is vizsgálódásunk fókuszába emeltük.[19]

2.2. Közösségiplatform-használati szokások

A magyar adatok elemzése alapján arra a megállapításra jutunk, hogy hazánk esetében az internetezők többségét leginkább a különböző híroldalak érdeklik, mégis idejük legnagyobb részét különböző közösségi oldalakon töltik el. Ez mintegy napi negyvenkilenc percet jelent.[20] Az egyes közösségi platformokra lebontva azt látjuk, hogy a magyar felhasználók körében a Facebook a legnépszerűbb, naponta átlag másfélmillió, havonta legalább egyszer több mint ötmillió ember látogatja. A második helyen a YouTube található, amelyet naponta közel egymillió, havonta legalább egyszer közel négy és félmillió ember látogat meg. Az Instagram napi látogatottsága a maga kétszázezer megtekintésével jelentősen elmarad az első kettőtől, azonban a havi szintű látogatottsága meghaladja a kétmilliót. Hasonlóan nagy különbség látható a napi és havi adatokban a negyedik legnépszerűbb közösségi platform, a TikTok esetében, amelyet naponta százezren, havonta legalább egyszer több mint másfélmillióan keresnek fel. Az X (korábban Twitter) kilencvenezer napi látogatottsággal, valamint egymillió-háromszázezres havi látogatottsággal rendelkezik.[21] Egy korábbi felmérés azt mutatta ki, hogy a magyar társadalom közel fele naponta veszi igénybe a Facebook-ot, míg az emberek több mint kétharmada legalább hetente használja. Ezekhez a számokhoz képest az Instagram jelentős lemaradásban van, mivel az internetezők csupán alig egyharmada használja.[22] Demográfiai szempontból az internethasználat összefüggést mutat az iskolai végzettséggel és a

17 DSA rendelet 3. cikk *i)* pont.

18 DSA rendelet (13) preambulumbekezdés.

19 A munkadefiníció alapján a közösségi platformok közé soroljuk különösen az alábbiakat: Facebook, Instagram, YouTube, X (a korábbi Twitter), TikTok, Reddit, Snapchat stb.

20 Nemzeti Média- és Hírközlési Hatóság: Az online médiatér közönsége. 2023. augusztus. *nmhh.hu,* szeptember 12. 6. https://nmhh.hu/cikk/241830/Az_online_mediater_kozonsege_2023_augusztus (a felmérésre a továbbiakban NMHH-felmérésként hivatkozunk).

21 Uo. 19.

22 Republikon Intézet: *Médiafogyasztás Magyarországon. Televíziós csatornák, hírportálok, közösségi média*. 2021. június. 28. 5–6. http://republikon.hu/media/98833/republikon-mediafogyasztas-21-06-28.pdf (a felmérésre a továbbiakban Republikon-felmérésként hivatkozunk).

település méretével: minél magasabb valakinek a végzettsége, illetve minél nagyobb településen lakik valaki, annál nagyobb a valószínűsége annak, hogy valamilyen mértékben használja az internetet.[23]

A fenti adatok ismeretében megállapítható, hogy a magyar lakosság előszeretettel használja a különböző közösségi platformokat, ennélfogva az online tér ezen szegmense jelentős befolyással van mind a magán-, mind a társadalmi életünk alakulására.

3. A becsülethez és jóhírnévhez való jog polgári jogi megközelítése

A becsülethez és jóhírnévhez való jog a Ptk. 2:45. §-ban rögzített nevesített személyiségi jog. A magánjogi kódexünkben szereplő személyiségi jogi generálklauzula egyértelműen kijelenti,[24] hogy valamennyi személyiségi jog forrásaként az emberi méltóságot kell tekinteni, azaz komoly alapjogi kapcsolat mutatható ki a konkrét személyiségi jogok esetében.[25] E téren érdemes kiemelnünk, hogy a magyar magánjogi gondolkodástól ez a típusú absztrakt személyiségi jogi védelmi szemlélet egyáltalán nem idegen[26] – ezt már Szladits Károly is megemlítette.[27]

A Ptk. személyiségi jogi generálklauzulája összhangban áll az Alkotmánybíróság gyakorlatával is, amely szerint egyes személyiségi jogok az emberi méltóságból mint általános személyiségi jogból származnak.[28] Az emberi méltóság tartalmát azonban nehéz pontosan meghatározni annak generális jellege miatt.[29] A becsülethez és jóhírnévhez való jog normatartalmát a már említett Ptk. 2:45. §-a tartalmazza. Eszerint a becsület megsértését azok a kifejezésmódjukban indokolatlanul bántó véleménynyilvánítások eredményezik, amelyek alkalmasak más személy társadalmi megítélésének hátrányos befolyásolására.[30] A jogsértéshez e körben egy kvalifikáltan bántó véleménynyilvánításra van szükség, amely a társadalmi megítélés negatív változását eredményezi, azaz két feltételnek kell egyszerre megfelelni. A bírói gyakorlatra hárul annak eldöntése, hogy egy megnyilvánulás mikor tekinthető kifejezésmódjában indokolatlanul bántónak.

A kommentárirodalomban találunk a becsület vonatkozásában olyan fogalomalkotási kísérletet, amely szerint a becsület nem más, mint a „személy társadalmi megítélése." [31] Ez a

23 Republikon-felmérés 10.

24 Ptk. 2:42. § (3) bekezdés.

25 A jóhírnévhez való jog erős alapjogi vonatkozását mutatja, hogy az Alaptörvény VI. cikk (1) bekezdésében külön is említésre került annak tiszteletben tartása. Ezt a jelentős szerepet tovább fokozza, hogy a Ptk. 2:42. § (1) bekezdésben fellelhető személyiségi jogi generálklauzula szövegében is szerepel. A becsülethez való jog ilyen kitüntetett helyet nem foglal el; sem az Alaptörvényben, sem az említett generálklauzulában nem történik rá hivatkozás.

26 Ld. Görög Márta: Gondolatok a személyiség magánjogi védelme körében. In: Menyhárd Attila – Gárdos-Orosz Fruzsina: *Személy és személyiség a jogban*. Budapest, Wolters Kluwer, 2016. 99–104.

27 Szladits Károly: *A magyar magánjog vázlata. I. rész* (negyedik, átdolgozott kiadás). Pécs, Ponte Press, 1999. 360.

28 36/1994. (VI. 24.) AB határozat Indokolás II/1.2. pontja; 7/2014. (III. 7.) AB határozat Indokolás [43] bekezdése.

29 Ld. Koltay András: Az emberi méltóság védelmének újabb gyakorlata a médiaszabályozásban. *Iustum Aequum Salutare*, 2023/4. 137–148., illetve Koltay András (2019) i. m. 21–41.

30 Ptk. 2:45. § (1) bekezdés.

31 Wellmann György (szerk.): *Polgári Jog. Bevezető és Záró rendelkezések, Az ember mint jogalany, Öröklési jog. A Ptk. magyarázata I/VI.* Budapest, HVG-ORAC, 2021. 196.

definíció azonban túlzóan leegyszerűsített egyes szakirodalmi álláspontok szerint, mivel nem reflektál a becsület valamennyi aspektusára.[32]

A jóhírnevet különösen a valótlan tény állítása, híresztelése, valamint a valós tény hamis színben történő feltüntetése sérti.[33] Az elhatárolás alapja tehát az, hogy míg becsületsértés esetén véleménynyilvánítás történik, addig a jóhírnévsérelem esetén tényállítás. Szintén különbségként említendő, hogy a Ptk. a jóhírnévsértés esetén az érintett személyét sértő[34] tényállításon kívül nem támaszt további feltételt, mint például egy konkrét és hátrányos eredmény bekövetkezését – bár a jóhírnévsérelem tényállása implicite magában foglalja a társadalmi megítélés védelmét is. Ezzel ellentétben a becsületsértéshez explicite szükséges a társadalmi megítélés hátrányos változása is. Ezzel összefüggésben a kommentárirodalom szerint a jóhírnévsérelem többféle negatív következménnyel is járhat.[35] A kimutatható hátrányok az alkalmazni kért szankciók szempontjából is jelentőséggel bírnak, mivel ahogy azt később ismertetjük, a sérelemdíjban marasztaláshoz nem elegendő önmagában a jogsértés ténye, ahhoz szükséges még egy nem vagyoni sérelem megléte, mivel ez a jogintézmény részben ezt a sérelmet hivatott kompenzálni.

3.1. Alapjogok harca: véleménynyilvánítás kontra emberi méltóság

A korábban említett erős alapjogi háttér leginkább a véleménynyilvánítás szabadsága és az emberi méltóság összeütközése révén érhető tetten, ahogy azt a Kúria is megállapította.[36] Jelen alfejezetben e körben kívánunk néhány jelzésértékű megállapítást tenni a vizsgált jogesetek minél teljesebb megértése érdekében.

A töretlen alkotmánybírósági gyakorlatra is figyelemmel a bíróságnak fel kell ismernie az alapjogi vonatkozást, fel kell tárnia a releváns alapjog tartalmát, valamint azt érvényre is kell juttatnia.[37] Ez praktikusan azzal a következménnyel jár, hogy a vizsgált bírósági határozatok többször alapítják megállapításaikat az irányadó alkotmánybírósági határozatokra. Ezek a határozatok ebből a szempontból egy szilárd belső magot alkotnak, és e köré építi fel a bíróság saját gyakorlatát.

Az emberi méltósághoz hasonlóan önállóan került szabályozásra az Alaptörvény IX. cikkében a véleménynyilvánítás szabadsága, amely az előbbihez hasonlóan szintén anyajogi jelleget mutat.[38] Az Alkotmánybíróság kiemelten védi a véleménynyilvánítás szabadságának

32 Ld. Koltay András: A becsület, a jóhírnév és az emberi méltóság fogalmi elhatárolása a magyar magánjogban. In: Darák Péter – Koltay András (szerk.): *Ad astra per aspera. Ünnepi kötet Solt Pál 80. születésnapja alkalmából*. Budapest, Pázmány Press, 2017. 435–458.

33 Ptk. 2:45. § (2) bekezdés.

34 A bírói gyakorlat alapján azonban a sérelmet nem a sértett fél szubjektív megítélése vagy érzékenysége alapján ítéli meg, hanem egy objektív, külső mérce alapján, amely a társadalmi közmegítélést, közízlést, illetve felfogást veszi alapul.; lásd például Pfv.IV.21.238/2020/8.

35 Wellmann i. m. 196.

36 Kúria Polgári Kollégiuma Joggyakorlat-elemző csoport 2021.El.II.JGY.P.2. számú összefoglaló véleményének kivonata (a továbbiakban: Kúria Joggyakorlat-elemző csoport) [13] bekezdés.

37 3/2015. (II. 2.) AB határozat Indokolás [18] bekezdése; 3145/2018. (V. 7.) AB határozat Indokolás [66]–[68] bekezdései; 3111/2022. (III. 23.) AB határozat Indokolás [24]–[25] bekezdései.

38 Árva Zsuzsanna: *Nagykommentár Magyarország Alaptörvényéhez*. Budapest, Wolters Kluwer, 2022. Jogtárformátum. https://uj.jogtar.hu/#doc/db/428/id/A20Y2225.KK/ts/20230101/

érvényesülését. Megközelítése szerint ez az alapjog ugyanis lényeges alapja a demokratikus társadalomnak, a sokszínű társadalmi és politikai viták lefolytatásának, illetőleg az egyéni autonómia kiteljesedésének.[39] Ez a kitüntetett szerep azonban nem jelenti azt, hogy a véleménynyilvánítás ne lenne korlátozható alapjog.[40] Ezzel összefüggésben érdemes hivatkozni arra a bírói gyakorlatra, miszerint a valótlan tény állítása, valamint híresztelése a véleménynyilvánítás szabadságának korlátját képezi.[41]Az emberi méltóság korlátozhatósága kapcsán érdemes megemlíteni továbbá, hogy az Alkotmánybíróság szerint „az emberi méltóság védelméhez való jog csak az emberi státusz jogi meghatározójaként korlátozhatatlan, míg más általános személyiségi jog és a belőle származó személyiségi jogok korlátozhatók."[42] Eszerint az emberi méltóságnak van tehát egy belső magja, amely korlátozhatatlan, ez az emberi mivolthoz tapad, míg vannak olyan személyiségi jogok – mint például becsülethez vagy jóhírnévhez fűződő jogok –, amelyek korlátozhatók.

Az Alkotmánybíróság több ízben is foglalkozott már magával a jóhírnévhez való joggal, azonban azt meg kell jegyeznünk a testület megállapítására hivatkozva, hogy e gyakorlat erősen hiányos.[43] A főbb megállapításokat az alábbiak szerint foglalhatjuk össze: a jóhírnév megsértésének megállapításához szükséges az érintett személy jóhírnevének sérelme: a valós tények állítása vagy híresztelése emiatt nem is eredményezheti a jogsértés megállapítását.[44] Megemlíthető továbbá, hogy a gyakorlat a jogsértés megállapításának feltételéül nem a sérelem bekövetkezését várja el, hanem magának a sértő közlésnek a meglétét.[45] Alapjogi megközelítés alapján a jóhírnév védelmének célja annak biztosítása, hogy az egyes személyekről valós tényekből történő következtetések alapján alakuljon ki a társadalmi kép. Ez azonban nem zárja ki annak lehetőségét, hogy az e tényekből leszűrt következtetés eredményeként kialakult kép téves legyen.[46] Mindezekre tekintettel az Alkotmánybíróság egyik határozatában akként értelmezte a jóhírnevet, hogy az „az egyén életéről alkotott kép."[47]

A becsülethez való jog alkotmánybírósági gyakorlata szerint a törvényi védelem nem általánosságban tiltja a sértő kifejezéseket, hanem azok minősített esete fennállásakor állapítható meg a jogsérelem. Ellenkező esetben ugyanis a véleménynyilvánítás szabadsága aránytalan korlátozást szenvedne el.[48] Az Alkotmánybíróság a véleménynyilvánítás szabadsága korlátjaként tekint e körben az olyan közlésre, amely az emberi méltóság korlátozhatatlan magját

39 36/1994. (VI. 24.) AB határozat Indokolás II/2. bekezdése; 7/2014. (III. 7.) AB határozat Indoklás [39]–[45] bekezdései; 13/2014. (IV. 18.) AB határozat Indokolás [23] bekezdése; 3145/2018. (V. 7.) AB határozat [27] bekezdése.

40 Lásd 7/2014. (III. 7.) AB határozat Indokolás [42] bekezdése.; illetve Koltay András: A véleményszabadság alkotmányos védelme az Alaptörvény első évtizedében. *Acta Humana,* 2021/2. 88. http://doi.org/10.32566/ah.2021.2.3.

41 Lásd Pfv.IV.20.955/2017/9.

42 7/2014. (III. 7.) AB határozat Indokolás [43] bekezdése; 7/2021. (II. 19.) AB határozat Indokolás [26] bekezdése.

43 3516/2021. (XII. 13.) AB határozat Indokolás [55] bekezdése.

44 3165/2021. (IV. 30.) AB határozat Indokolás [43] bekezdése; 3516/2021. (XII. 13.) AB határozat Indokolás [62] bekezdése.

45 3165/2021. (IV. 30.) AB határozat Indokolás [43] bekezdése; 3516/2021. (XII. 13.) AB határozat Indokolás [62] bekezdése.

46 3165/2021. (IV. 30.) AB határozat Indokolás [44] bekezdése; 3516/2021. (XII. 13.) AB határozat Indokolás [63] bekezdése.

47 3516/2021. (XII. 13.) AB határozat Indokolás [55] bekezdése.

48 7/2021. (II. 19.) AB határozat Indokolás [31] bekezdése.

sérti, így arra, amely az emberi státuszt nyilvánvalóan és súlyosan becsmérli.[49] Az Alkotmánybíróság szerint a bírói gyakorlat ezekben az esetekben a '*gyalázkodás*' kifejezést szokta alkalmazni.[50] Az emberi méltóságból fakadó becsülethez való jog e szerint a 'gyalázkodó' kifejezések vonatkozásában mindenféleképpen védelmet élvez a véleménynyilvánítás szabadságával szemben.

Speciális esetkört ölel fel a közéleti szereplők becsülethez és jóhírnévhez való jogának érvényesülése, figyelemmel a Ptk. 2:44. § (1) bekezdésből levezethető fokozott tűrési kötelezettségre, valamint az ennek nyomán kialakított alkotmánybírósági korlátozhatósági tesztre is.[51]

3.2. A kommentek jogi státusza

A tanulmány témája szempontjából érdemes külön is foglalkozni a kommentek[52] jogi státuszával. E körben indokolt hivatkozni az Alkotmánybíróság azon álláspontjára, miszerint különbséget kell tenni a közösségi oldalak, véleményoldalak, valamint az internetes oldalak üzemeltetői által szerkesztett tartalomszolgáltatások között.[53] Az előbbi csoportba sorolható többek között a Facebook is. E közösségi, illetve véleményoldalak jellemzője, hogy rendeltetésük nem a tájékoztatás, hanem az egyéni gondolatok kifejtése, illetve azok megosztása. További jellemzőjük egy bizonyos fokú spontaneitás megléte. Erre tekintettel ezeken a felületeken közzétett bejegyzések védett magánközlések, amelyek nyilvánossága korlátozott, mivel csak a korlátozó által meghatározott körhöz tudnak eljutni, például Facebook esetén a felhasználó ismerőseihez. A közéleti szereplők, intézmények esete azonban ettől eltérő.[54] A korlátozott hozzáférés esetében álláspontunk szerint annyi pontosítás szükséges, hogy az egyes közösségi platformok működési elvei lehetővé teszik, hogy egy személy bejegyzése tágabb körhöz is elérjen.[55] A kommentért való felelősség kapcsán érdemes megemlíteni, hogy az Alkotmánybíróság határozatában arra az álláspontra helyezkedett, hogy a moderálás nem mentesíti az online felület fenntartóját, mivel a felelősség a jogsértő közlés tényén alapszik, nem pedig annak moderált vagy nem moderált voltától függ.[56] Ez logikailag azt is jelenti, hogy a jogsértés esetében a tényleges jogsértő mellett felmerülhet a fenntartó felelősségének megállapítása is. Ez különösen azokban az esetekben lehet jelentős, amikor a tényleges jogsértő kilétének azonosítása nem lehetséges.

A fentiekkel összefüggésben érdemes megemlíteni a bíróság azon döntését, miszerint a zárt Facebook-csoportban közzétett álláspont jogilag kommentnek minősül, függetlenül attól,

49 13/2014. (IV. 18.) AB határozat Indokolás [40] bekezdése.

50 3329/2017. (XII. 8.) AB határozat Indokolás [35] bekezdése; lásd továbbá Pfv.IV.20.970/2018/7.

51 Ld. részletesebben Vitkovics Bálint: A becsület és a jó hírnév megsértése a közéleti szereplők esetében. In: *Mailáth György Tudományos Pályázat 2022. Díjazott dolgozatok.* Budapest, Országos Bírósági Hivatal, 2023. 35–72.

52 Már az ilyen típusú írásos közlések elnevezése is sokszínűséget mutat: komment, hozzászólás, bejegyzés. A tanulmányunkban ezeket az elnevetéseket szinonimaként használjuk.

53 19/2014. (V. 30.) AB határozat Indokolás [61] bekezdés, illetve korábbról 165/2011. (XII. 20.) AB határozat Indokolás IV/1.4. pontja.

54 19/2014. (V. 30.) AB határozat Indokolás [61] bekezdése.

55 Gondoljunk csak arra az esetre, amikor a Facebook ismerősünk egy másik ismerőse bejegyzéséhez szól hozzá, és az megjelenik a mi hírfolyamunkban, annak ellenére, hogy az eredeti bejegyzést közzé tett személy nem a mi ismerősünk.

56 19/2014. (V. 30.) AB határozat Indokolás [64]–[65] bekezdései.

hogy azt valaki saját nevét közvetlenül felvállalva, vagy pedig valamilyen álnéven teszi közzé.[57] A bejegyzés közzétételével kapcsolatos felelősség kapcsán a bírói gyakorlat szerint a felek felelősséggel tartoznak a saját Facebook-oldalukon közzétett tartalmak alá érkező bejegyzések taralmáért is, mivel az adott profil üzemeltetőjének lehetősége van annak beállítására, hogy a kérdéses oldal a nyilvánosság mely köre számára lehet hozzáférhető, illetve azon mások milyen tartalmat tehetnek közzé. A bejegyzések engedélyezésével tehát azzal is számolnia kell a Facebook-oldal üzemeltetőjének, hogy azon jogsértő tartalmak is megjelenhetnek.[58]

A bejegyzések tekintetében érdekes kérdést vetnek fel azok az esetek, amikor az egyes sérelmezett állításokat nem írott formában teszik közzé, hanem videó formájában. Az utóbbi években több olyan platformot említhetünk, amelyek teret biztosítanak véleményvideók közzétételére – gondoljunk csak a Facebookra, a YouTube-ra, az Instagramra vagy éppen a TikTokra. Erre tekintettel a bíróságnak érdemben kellett foglalkoznia az ilyen típusú videók jogi helyzetével. Egy ilyen jogesetben mondta ki a bíróság, hogy egy, a Facebookon közzétett sérelmezett videó nem minősül az adott körülményekre tekintettel sajtótájékoztatónak, hanem az egy képi megjelenéssel társított jegyzet, ekként pedig véleménynyilvánításként értékelhető.[59]

A bejegyzések vonatkozásában említésre méltó azon esetkör, amikor egy vásárló akár erőteljes megfogalmazású véleményének ad hangot egy vásárolt termék vagy szolgáltatás vonatkozásában. A bírói gyakorlat alapján ez esetben a vásárló mint egy szerződéses jogviszony egyik alanya, azaz mint szerződő fél formál véleményt a konkrét szerződéses folyamatról akként, hogy ezt a véleményét a nyilvánosság számára is hozzáférhetővé teszi. E véleményt is megilleti a véleménynyilvánítás szabadsága azzal, hogy figyelembe kell venni a másik fél jóhírnévhez való jogát.[60] E körben állapította meg a bíróság, hogy a „sunyi, megbízhatatlan bolt" bejegyzés kifejezésmódjában kétségtelenül erőteljes, azonban jóhírnévsértést nem alapoz meg, figyelemmel a társadalmi közmegítélésre.[61]

4. A becsülethez és jóhírnévhez való jog megsértése a közösségi platformokon

Tanulmányunk jelen fejezetében ismertetjük, hogy milyen általános következtetéseket lehet levonni az érintett jogesetek személyi köréről, illetve az általuk kért szankciókról. Választ keresünk továbbá arra is, hogy melyek a leginkább érintett közösségi platformok, illetve a bírói gyakorlat milyen jelentőséget tulajdonít az itt elkövetetett becsület- és jóhírnévsértésnek.

4.1. Általánosságban a vizsgált jogesetekről

A tanulmányunkban összesen 35 bírósági határozatot dolgoztunk fel a fent megjelölt vizsgálati szempontok figyelembevételével. Az e szempontoknak megfelelő döntések a 2016–2023 közötti

57 Pfv.IV.20.102/2023/8.
58 BH2016.330., Pfv.IV.20.796/2020/5.
59 Pfv.IV.20.521/2022/4.
60 Jogi személy esetében kizárólag a jóhírnév sérelméről beszélhetünk, mivel a becsületsértés fogalmilag kizárt. Ld. továbbá a jogi személyek személyiségi jogai vonatkozásában: Pfv.IV.21.177/2022/7.; Pfv.IV.21.198/2018/3.
61 Pfv.IV.20.945/2019/3.

időszakot ölelik fel. A vizsgált bírósági határozatok közül összesen 30 olyan jogesetet találtunk, ahol a személyiségi jogi szempontból sérelmezett bejegyzést valamilyen Facebook-profilon vagy -csoportban tették közzé. A második helyet a YouTube videómegosztó platform foglalja el a maga 3 bírósági döntésével. Ez a szám statisztikai szempontból azt jelenti, hogy a vizsgálattal érintett időszakban a népszerű videómegosztó portálon megvalósított tevékenységek nagyjából tizedannyi jogvitát generáltak Facebookhoz képzest. A fennmaradó 2 ügy olyan fórumokon tett bejegyzéseket takar, amelyek pontos behatárolása az anonimizálás miatt nem volt lehetséges. Mindazonáltal érdemes megjegyezni, hogy nem találkozunk olyan jól ismert közösségi platformokkal, mint az Instagram, az X (korábban Twitter), a TikTok, a Snapchat, Viber vagy éppenséggel a Reddit.

Ez egyrészt magyarázható a korábban ismertetett internetfogyasztási szokásokkal: mivel a témánk szempontjából releváns platformok közül átlagosan a Facebook felületén töltjük a legtöbb időt, érthető, hogy a legtöbb becsület- és jóhírnévsértéssel kapcsolatos jogvita is innen kerül ki. Beszédes azonban, hogy a közbeszédben szintén nagy gyakorisággal előforduló közösségi platformok esetén – mint például az Instagram vagy a TikTok –, nem találunk fellelhető jogesetet. Ez valószínűsíthetően nem azt jelenti, hogy kizárólag a Facebookon, illetve a YouTube-on fordulnak elő sérelmezett közlések. Minden bizonnyal a többi közösségi platform esetében is találkozhatunk olyan tartalommal, amely alkalmas lehet a becsület vagy jóhírnév, illetőleg más személyiségi jog sérelmének megállapítására, azonban az internetfogyasztási trendek alapján ezeknek a platformoknak az aktivitása nem éri el azt a volument, mint a Facebook vagy YouTube esetében. Másfelől feltehetően demográfiai szempontból is magyarázható: gondoljunk itt csak arra, hogy az Instagram vagy éppenséggel a TikTok felhasználói köre fiatalabb a Facebook átlag használóinál.[62] Ez a generációs különbség eltérő platformhasználati jellemzőkkel jár, ami többek között kihatással lehet az egyes sérelmezett tartalmak jogi következményeinek levonására .[63]

A fentieket látszik alátámasztani az a tény is, amely szerint a feldolgozott 35 jogesetből 25, azaz a vizsgált ügyek közel háromnegyede közéleti szereplőkhöz vagy közügyi érintettséggel rendelkező vitához kötődött. Ezen belül is a valamilyen helyi vagy országos politikai természetű vitához kapcsolódó ügyek száma 21 volt. Ez az erős közéleti jelleg alapvetően határozta meg a vizsgált jogesetek megítélését, hiszen a bíróságnak ezáltal az esetek túlnyomó részében fokozottan kellett figyelembe vennie az Alkotmánybíróság gyakorlatát a véleménynyilvánítási szabadság és közéleti viták viszonya vonatkozásában. Érdemes megemlíteni a teljesség kedvéért, hogy a közéleti hátterű jogviták után azonos számokat produkáltak a szolgáltatásokkal és az egyéb magánjellegű viszonyokkal kapcsolatos ügyek. Az előbbi esetkör valamilyen termék vásárlását követően tett elégedetlen vásárlói bejegyzéseket takar. A 35 vizsgált jogesetből ez az esetkör összesen 5 ügyet ölelt fel. Az utóbbi esetkörben úgyszintén 5 ügyet találtunk. Ezek az ügyek valamilyen családi, illetve egyéb magánviszonyokat érintő, sérelmezett kijelentéseket öleltek fel.

A kereseti kérelmekben kért szankciók sokszínűek, azonban jellemzően a jogsértés megállapítását, a jogsértés abbahagyását, a jogsértéstől való eltiltást, elégtétel adását, valamint

62 Republikon-felmérés 14–16.

63 Az ebben a bekezdésben jelzett generációs különbség pontos feltárása célzott jogszociológiai kutatást igényel, amely vizsgálódási körébe vonhatná, hogy az új generáció miként gondol a személyiségi jogai bírósági úton történő érvényesítésére.

sérelemdíj megítélését kérelmezik. Az elégtétel adásánál többször szerepelt olyan kérelem, amelynek értelmében a jogsértő félnek saját Facebook-oldalán vagy a jogsértéssel érintett Facebook-A csoportban kellett bejegyzést közzétennie.[64]

A sérelemdíjként megítélni kért összegek is heterogének. Az esetek többségében ötszázezer forintban határozták meg a felek a sérelemdíj mértékét, ezt szorosan követi az egymillió forint, illetve a háromszázezer forint. Összességében azonban a kettőszázezer forinttól a kétmillió-négyszázezer forintig több összeg is előfordult, sőt volt példa arra is, hogy a sérelemdíj mértékét tízezer euróban[65] kérték megállapítani. A bíróság átlagosan kettőszázhatvankétezer-háromszáznyolc forintot ítélt meg sérelemdíjként. A leggyakoribb összeg háromszázezer forint volt. A legkisebb megítélt összeg tízezer, míg a legmagasabb egymillió forint volt. A megítélt sérelemdíjak vonatkozásában azonban érdemes azt is megemlíteni, hogy a vizsgált ügyek kétharmadában nem került sor sérelemdíj megállapítására – jellemzően a kereset elutasítása miatt –, azonban volt arra is példa, hogy a jogsértett fél nem kért sérelemdíjat,[66] illetve olyan üggyel is találkoztunk, ahol a bíróság a jogsértés csekély súlyára tekintettel nem tartotta indokoltnak a sérelemdíjban történő marasztalást.[67]

Általánosságban megállapíthatjuk, hogy a közösségi platformok felületén elkövetett becsület- és jóhírnévsértések tipikusan a Facebookon történnek, jellemzően valamilyen közéleti vita keretében tett bejegyzést érintenek. Az érintett felek mindegyike vagy legalább egyike az esetek többségében politikus közéleti szereplő. A kereseti kérelmek többségében a jogsértés megállapítására, a jogsértés abbahagyására, az attól való eltiltásra vonatkozik, illetve rendszerint ötszázezer forint sérelemdíj megfizetését foglalják magukban. Az ügyek jelentős részében a kereset elutasításra kerül, azonban amikor megállapítható a jogsértés, a bíróság jellemzően kétszázhatvanezer forint körüli összeget állapít meg sérelemdíjként.

4.2. A bíróság döntésének főbb szempontjai

Miként azt korábban említettük, a vizsgált jogesetek komoly alapjogi megalapozottsággal rendelkeznek. E körben érdemes megemlíteni továbbá még a sajtóhelyreigazítási perekhez kapcsolódó PK 12., 13. és 14. számú állásfoglalásokat, mivel azok több esetben megjelentek hivatkozási alapként az egyes bírósági határozatokban.

A közösségi platformon történő jogsértés megítélése az elégtételadás, valamint a sérelemdíj megítélése körében bírt jelentőséggel a jogviták eldöntése során. Előbbi esetében jellemző kereseti kérelemként jelent meg a sajnálkozást kifejező elégtétel adása oly módon, hogy a jogsértő a közösségi platformon meghatározott ideig, illetve meghatározott tartalommal tegyen közzé bejegyzést.[68] Az utóbbi vonatkozásában pedig a sérelmet szenvedett fél a személyét ért jogsértésre alapítva kérte a jogsértő kötelezését sérelemdíj megfizetésére.

64 Ld. például Pfv.IV.20.399/2020/23.; Pfv.IV.20.101/2016/10.
65 Pfv.IV.21.177/2022/7.
66 Pfv.IV.21.238/2020/8.
67 Pfv.IV.20.945/2019/3.
68 Ld. például Pfv.IV.21.112/2022/4.; Pfv.IV.21.113/2021/5.; Pfv.IV.20.399/2020/23.; Pfv.IV.21.238/2020/8.; Pfv.21.487/2021/5.; Pfv.IV.22.614/2017/8.; Pfv.IV.20.101/2016/10.

A Ptk. irányadó rendelkezése alapján a sérelemdíj mértékét a bíróság egy összegben határozza meg az eset körülményeire figyelemmel.[69] E körülmények vizsgálatának lehetséges szempontjait a Ptk. példálózó jelleggel meghatározta: jogsértés súlya, ismétlődő jellege, felróhatóság mértéke, illetve a jogsértésnek a sértettre és környezetére gyakorolt hatása.[70]

A sérelemdíj megítélése kapcsán fontos felhívni a figyelmet azon bírói gyakorlatra, miszerint önmagában a személyiségi jogi jogsértés ténye nem eredményezi automatikusan a sérelemdíjban történő marasztalást, mivel a sérelemdíj egyik funkciója a nem vagyoni sérelmek kompenzációja, azaz ennek hiányában nem lehet sérelemdíjat követelni. A Ptk. 2:52. § (2) bekezdése e körben pusztán a sértett felet mentesíti a hátrány bizonyításának eljárásjogi kötelezettsége alól. A sérelemdíj mértékét az eset összes körülménye, a nem vagyoni sérelem, illetve a Ptk. 2:52. § (3) bekezdése szerinti szempontok alapján határozzák meg azzal, hogy akár a ténylegesen fennálló nem vagyoni sérelem esetén is lehetőség van mellőzni a sérelemdíjban történő marasztalást, ha az nem szükséges az okozott hátrány kompenzálásához.[71]

A sérelemdíj említett funkciójára tekintettel célszerű megemlíteni, hogy e jogintézmény kettős funkcióval rendelkezik: egyrészről a már említett kompenzációs szerep mellett egyfajta magánjogi büntetésként is lehet rá tekinteni, amelynek célja a hasonló jogsértések megelőzése.[72] Erre is tekintettel valószínűleg nem véletlen, hogy a Ptk. 2:52. § (3) bekezdésében olyan orientáló jellegű szempontrendszer került meghatározásra, amely szóhasználatában inkább illeszkedik a büntetőjog terrénumához, semmint a magánjogéhoz.[73] A sérelemdíj büntető jellegére tekintettel érthető a jogszabályi szövegezés 'büntetőjogias' megközelítése. A közösségi platformok bírósági megítélését leginkább a sérelemdíj vonatkozásában tett mérlegelés útján lehet megismerni, a Ptk.-ban meghatározott szempontrendszeren keresztül.

4.2.1. A közösségi platform nyilvánossága

A közösségi platformokkal elérhető nyilvánosságot a bíróság rendszerint a sérelemdíj megítélése körébe vonja, mint szempontot. E körben került megállapításra, hogy egy zárt csoportban közölt, sérelmezett bejegyzés a csoport tagjai személyi összetételére is figyelemmel inkább volt országos szintűnek tekinthető, valamint az értékelés körébe vonta a bíróság azt is, hogy a sérelmezett bejegyzés a zárt csoporton kívül is eljutott más személyekhez is.[74] A nyilvánosság esetében a bíróság tehát vizsgálódása körébe vonja a bejegyzéssel potenciálisan elérhető személyek körének relatív nagyságát. Ezzel összefüggésben ismerünk olyan döntést, ahol a sérelemdíj mértékének meghatározása körében figyelemmel volt a bíróság többek között arra is, hogy a sérelmezetten megosztott felhívás a jogsértő Facebook-oldalán korlátozott nyilvánossághoz jutott csak el, erre is figyelemmel szállította le a jogerős ítélet a megítélt sérelemdíj összegét tízezer forintra.[75] Ezen jogesetre is figyelemmel joggal merül fel a kérdés: mekkora követőbázissal kell rendelkeznie egy jogsértőnek ahhoz, hogy a nyilvá-

69 Ptk. 2:52. § (3) bekezdés.
70 Ptk. 2:52. § (3) bekezdés.
71 Pfv.IV.20.089/2023/7.; Pfv.IV.20.954/2022/4.; Pfv.IV.20.464/2018/8.; Pfv.IV.21.764/2015/4.
72 Pfv.IV.20.101/2016/10.; Debreceni Ítélőtábla 1.Pf.20.249/2021/6/III.
73 Ld. Vékás Lajos (szerk.): *A Polgári Törvénykönyv magyarázatokkal*. Budapest, CompLex ,2013. 72–74.
74 Pfv.IV.20.067/2022/4.
75 Pfv.IV.20.101/2016./10.

nosság relatív nagyságát figyelembe vegye a bíróság? Erre tekintettel érdemes megemlíteni azt a bírósági döntést, amelynek során a sértett fél arra hivatkozott, hogy az őt ért sérelem az ő Facebook-oldalán került közzétételre, amely többtízezres látogatottságú volt, és azt jellemzően a sértettel szimpatizáló személyek látogatták. Érdekes módon a bíróság pont erre a tényre alapozva állapította meg a csekély mértékű jogsérelmet, mivel a sérelmezett kijelentés kapcsán a sértetthez alapvetően együttérző, őt támogató bejegyzések érkeztek, míg a jogsértő irányába ellenszenvet tükröző bejegyzések lettek közzétéve.[76] Egy másik esetben a Facebookon százhuszonhétezer követővel rendelkező személy esetében a bíróság szintén nem tartotta ezt a nyilvánosságot kellően nagynak, illetve párhuzamba állította a Facebookon tett bejegyzést egy sajtótájékoztató nyilvánosságával. Az ügyben a jogsértés esetében a bíróság figyelembe vette azt is, hogy a jogsértő tartalom csak hét órán keresztül volt elérhető, valamint a bejegyzést egy sajtószerv sem vette át.[77] Ez természetesen nem azt jelenti, hogy a Facebook vagy más közösségi platform nem képvisel olyan nyilvánosságot, amelyet figyelembe lehetne venni. Inkább egyfajta relatív vagy korlátozott nyilvánosságról lehet beszélni a bírói gyakorlat alapján, amely a sérelemdíj mértékének meghatározásánál vehető figyelembe.[78] Erre példa azon bírósági határozat, amely a sérelemdíj meghatározása során mérlegelése körébe vonta a közösségi platformon való megjelenést, mivel az egyes oldalak látogatottsága miatt szélesebb körhöz tud eljutni a sérelmezett közlés, ennélfogva a sérelemdíj mértékét növelheti a közösségi platformon való közzététel.[79] A nyilvánosság helyének fontosságára hívja fel a figyelmet az döntés is, amelynek értelmében a Facebookon közzétett jogsértő tartalom esetében tekintettel kellett lenni arra, hogy jogsértő közlések széles körben váltak ismertté a nyilvánosság előtt.[80]

A Facebookon közzétett, erőteljes indulatszavak alkalmazása vonatkozásában a bíróság megállapíthatónak tartotta a személyiségi jogi jogsérelmet, és a sérelemdíj megítélése során a mérlegelés körében a bíróság hangsúlyt fektetett arra, hogy a sérelmezett szavak használata a Facebook által biztosított nyilvánosságon keresztül valósult meg, azaz a bíróság a közösségi platformon való bejegyzést olyannak ítélte, amely megalapozhatja a sérelemdíj megítélését a sértett fél részére.[81] Ezt támasztja alá azon bírósági döntés is, amely során egy ékszervásárlás kapcsán egy blogon, illetve a Facebookon közzétett, negatív tartalmú, tagekkel ellátott bejegyzés tárgyában a bíróság megállapíthatónak tartotta a jóhírnévsérelmet, és a sérelemdíj megállapításánál figyelemmel volt a Facebookon tett bejegyzés nyilvánosságára azzal, hogy mivel a bejegyzésnek nem volt széles körben kimutatható hatása, emiatt az nem adott alapot jelentős mértékű sérelemdíj megítéléséhez. A bíróság álláspontja szerint ugyanis nem tipikus, hogy ékszervásárlás előtt a sértetti vállalkozás értékeléseit a vásárlók tüzetesebben ellenőrzik, így a sértő megjegyzések üzleti hírnévre gyakorolt hatása korlátozott – figyelemmel a sértő fél Facebook-elérésére is.[82]

A nyilvánosság jogi jelentőségének jó példájaként szolgál azon jogeset is, amelyben egy családon belül elmérgesedett viszony keretében a sértett fél vonatkozásában durva vádakat

76 Pfv.IV.20.725/2019/5.

77 Fővárosi Ítélőtábla 8.pf.20.297/2022/6., valamint Pfv.IV.21.112/2022/4.

78 Ld. például Szegedi Ítélőtábla Pf.II.20.152/2019/4.; az ítélőtábla másodfokú ítéletét a Kúria Pfv.IV.21.348/2019/8. döntésével hatályon kívül helyezte, azonban az ítélőtáblai határozat jó példaként szolgál a közösségi platform korlátozott nyilvánosságának megítélése szempontjából.

79 Szegedi Ítélőtábla Pf.II.20.044/2021/7., valamint Pfv.IV.21.113/2021/5.

80 Győri Ítélőtábla Pf.IV.20.017/2020/8., illetve Pfv.IV.20.796/2020/5.

81 Pfv.IV.20.970/2018/7.

82 Fővárosi Ítélőtábla 17.Pf.20.313/2019/4-I., valamint Pfv.IV.21.439/2019/5.

közöltek. Az egyik sértő fél ezzel összefüggésben magánlevelet írt egy államtitkárnak, amely levél utóbb egy tisztázatlan hátterű Facebook-oldalon közzétételre került. A bíróság ezzel összefüggésben állapította meg, hogy egy magánlevél tartalma önmagában nem szolgáltathat alapot a jóhírnév megsértéséhez, ahhoz ugyanis a nyilvánosság számára való közlés szükséges.[83] A bíróságnak e megközelítése annyiban figyelemre méltó, hogy a Ptk. 2:45. § (2) bekezdéséből nem következik egyértelműen valamilyen szűkebb vagy tágabb társadalmi tudomásszerzés, mivel a jogszabályi szöveg alapján a jóhírnévsértés különösen a más személyére vonatkozó és e személyt sértő valótlan tények állításával, híresztelésével, illetve a valós tény hamis színben való feltüntetésével valósulhat meg. Ebből következően egy harmadik személy részére írt magánlevélben szereplő jóhírnévsértő tényállítás alapvetően alkalmas lehet a jogsértéshez. Álláspontunk szerint még megválaszolásra vár az a kérdés, hogy a bírói gyakorlat által is megkövetelt nem vagyoni sérelem realizálódása milyen mértékű nyilvánosság meglétét teszi szükségessé az ilyen típusú jogvitákban, azaz egy harmadik személynek címzett, valakiről valótlan tényállításokat tartalmazó magánlevél *ab ovo* alkalmatlan-e a jóhírnévsérelemhez, vagy fennállhatnak olyan körülmények, amelyek mérlegelése alapján lehetséges a sérelemdíjban történő marasztalás. A becsületsértés esetében annyiban eltérő a helyzet, hogy ott olyan kijelentésre van szükség, amely alkalmas az érintett személy társadalmi megítélésének hátrányos befolyásolására. Bár önmagában ez az elvárás sem jelenti álláspontunk szerint azt, hogy ne valósulhatna meg egy harmadik fél számára írt magánlevéllel a becsületsértés.

A nyilvánosság jelentőségét legalább két aspektusból lehet vizsgálni a bírói gyakorlat alapján. Egyrészről az érintett személy közösségi oldalának látogatottsága bír nagyobb súllyal, másfelől pedig az is értékelésre kerül, hogy ezek a platformok jellemzően interaktívak, azaz nemcsak elolvasni vagy megtekinteni lehet valaki oldalán az egyes bejegyzéseket, videókat, hanem ahhoz kapcsolódóan mások is bejegyzéseket tehetnek közzé, amelyek ezáltal virálissá is válhatnak, ennélfogva pedig akár nagy visszhangot is kaphatnak.[84] A bírói gyakorlat alapján az eset összes körülménye vizsgálatának nemcsak arra kell kiterjednie, hogy potenciálisan mekkora nyilvánossághoz juthatott el a sérelmezett bejegyzés, hanem azt is meg kell vizsgálni, hogy a bejegyzés az olvasók számára milyen valódi jelentést hordozhatott.[85]

4.2.2. A bejegyzésekért való felelősség egyes elemei

A közösségi platformokon való bejegyzések rendkívül heterogének: saját véleményünket teszszük közzé, hozzászólunk mások véleményéhez, esetleg megosztunk más által közölt híreket. Bármilyen körülmény alapján tettük is közzé bejegyzésünket, azért felelősséggel tartozunk. Ez a mások által közölt hírek, vélemények megosztása esetén is komoly jelentőséggel bír. Erre példa az a jogeset, amelyben az alperes a saját Facebook-oldalán osztott meg egy felhívást, amely egy település ingatlangazdálkodására vonatkozott. E körben a bíróság kiemelte, hogy a Facebook-profil üzemeltetője vonatkozásában is megállapíthatóak személyiségi jogi szankciók a Ptk. 2:51–53. §-ai alapján, figyelemmel arra, hogy a közzétett felhívás valótlan tényeken alapult, így a jóhírnévsérelem megállapítható, mivel annak egyik lehetséges módja a valótlan

83 Fővárosi Ítélőtábla 1.Pf.20.841/2015/3/II., valamint Pfv.IV.21.044/2016/3.
84 Ld. ezzel kapcsolatban Pfv.IV.21.487/2021/5.; Pfv.IV.21.828/2018/6.
85 Pfv.IV.20.070/2021/4.

tények híresztelése. A sérelemdíj körében felmerülő felelősségi kérdések körében azonban a bíróság figyelembe vette, hogy a közzétett felhívás tartalmának ellenőrzésére az érintett félnek csekély súly tulajdonítható, valamint a híreszteléssel, azaz a felhívás megosztásával kiváltott sérelem is csak kisebb részben volt felróható a számára, így összességében a jogsértés is csak csekély súlyúnak minősült. Értékelésre került a gyakoriság körében az, hogy kizárólag egyszeri megosztásról volt szó.[86]

A felelősséggel összefüggésben vonta a bíróság értékelése körébe a sérelmezett közlést tett fél esetében annak képzettségét, valamint tisztségét. E körben hangsúlyozták, hogy az alperes jogi relevanciájú kijelentést tett, mindezt úgy, hogy jogász végzettséggel rendelkezett, azaz a témában professzionális jártassággal bírt, valamint országgyűlési képviselői tisztségéből eredő szervezeti háttere lehetővé tette volna számára, hogy az általa tett kijelentés valóságtartalmát tüzetesebb vizsgálat alá vonja, és ennek alapján tegye meg közlését. Mindezekre tekintettel a bíróság szerint megállapítható volt, hogy az alperes nem tanúsította a tőle elvárható gondosságot.[87]

A közlésért való felelősség külön említésre is méltó esete volt, amikor a bíróságnak abban az ügyben kellett határozatot hoznia, amely során egy személy a saját Facebook-oldalán közzétett egy katonatörténetet, amelyet azután egy sajtószerv átvett. E körben a bíróság a sajtószerv objektív felelősségét abban látta, hogy a Facebookon közzétett, korlátozott nyilvánosságú bejegyzést átvette, ezzel szélesebb nyilvánosság számára tette annak tartalmát hozzáférhetővé. A sérelemdíj mértékének megállapítása során a bíróság csekély mértékű jogsérelmet vélt megállapíthatónak, mivel a sértett félnek lehetősége volt az azonnali reagálásra, amellyel élt is, valamint a bíróság álláspontja szerint a társadalom helyén tudja kezelni a katonatörténetek valóságtartalmát.[88]

A fokozott gondosság körében érdemes továbbá megemlíteni azon döntést is, amelynek alapjául szolgáló ügyben a jogsértő fél tájékoztatás céljából egy videót osztott meg a YouTube-csatornáján, amelyben valótlan tényállítást tett. E körben a bíróság úgy értékelte, hogy a jogsértő félnek lehetősége volt a vitatott videóközlemény szerkesztésére, megvágására, illetve arra is lehetősége lett volna, hogy teret adjon a sértett fél számára a reagálásra. Ezek elmaradása miatt a felelősséget megállapíthatónak tartotta a bíróság.[89]

A felelősség körében érdemes megemlíteni a jogsértés gyakoriságának kérdését is. Erre szolgál példaként azon jogeset, amelyben éppen az ismétlődő jellegre is tekintettel állapítottak meg sérelemdíjat egy jogvita során, amelyben egy civil érdekvédelmi szervezet tagjai között elmérgesedett nézeteltérés odáig eszkalálódott, hogy a jogsértő felek saját Facebook-profiljukon, illetve különböző Facebook-csoportokban tettek közzé olyan bejegyzéseket, amelyek alkalmasak voltak a sértett becsületének és jóhírnevének sérelmére.[90]

4.2.3. Következtetések

A fentiek alapján azt a következtetést vonhatjuk le, hogy az offline és online térben elkövetett jogsértések megítélésében éles distinkció nem állt fenn a vizsgált időszakban. Ez részben

86 Pfv.IV.20.101/2016/10.
87 Fővárosi Ítélőtábla 2.Pf.20.903/2018/8-II., valamint Pfv.IV.20.683/2022/5.
88 Pfv.IV.20.903/2016/7.
89 Pfv.IV.21.167/2019/4.
90 Pfv.IV.20.399/2020/23.

érthető, hiszen miként azt korábban említettük, a bíróságnak fel kell ismernie az előtte lévő jogvita alapjogi relevanciáját, és e körben figyelembe kell vennie az alkotmánybírósági gyakorlatot, amely ennélfogva részben megjelenik a bírósági döntéseiben. Az Alkotmánybíróság a vizsgált időszakban azonban nem helyezett akkora hangsúlyt az online platformon történt jogsértésre, ami természetesen nem jelenti azt, hogy ne foglalkozott volna érdemben a technológiai változások nyomán tetten érhető kommunikációs közeg változásaival – erre jó példa a kommentek jogi helyzetével foglalkozó alkotmánybírósági határozat –, azonban az kétségtelen, hogy alapjogi szempontból a jóhírnév-, illetve becsületsértési ügyekben az online térben történő elkövetést nem állították élesen szembe a hagyományos, offline térben elkövetett jogsértésekkel, emiatt érthető módon az ítéletek alapjogi relevanciájú részeinél sem tudott ez a különbségtétel szignifikáns módon megjelenni.

A bírói gyakorlat is alapvetően a már kijegecesedett mérlegelési szempontokat alkalmazta az online jogsértések vonatkozásában. Az online és offline térben elkövetett jogsértések erős szembeállítását, valamilyen szisztéma szerinti klasszifikációját azonban nem tartotta indokoltnak, ennélfogva nem is alakulhatott ki olyan ítélkezési gyakorlat, amely eltérő módon kezelte volna a különböző színtereken elkövetett jogsértéseket. Sokkal inkább azt láthatjuk a bírósági döntések áttanulmányozását követően, hogy a bíróság az online térben történő elkövetésre egyfajta specifikumként tekint, amely leginkább a jogsértés körülményeinek vizsgálata körében bír relevanciával.

Nem tartjuk indokoltnak az offline és online jogsértések szigorú szembeállítását és azok vonatkozásában eltérő jogi rezsimek kidolgozását, hiszen a jelenlegi szabályozási környezet is megadja a lehetőséget az elkövetés körülményeinek megfelelő mérlegelésére, azaz a bíróság számára megfelelő mozgásteret biztosít a hatályos normaszöveg.[91] Álláspontunk szerint azonban az online térben elkövetett jogsértés egyik fontos jellemzője, hogy az sem térben, sem időben nem tekinthető lezártnak, és a közösségi platformok MI-alapú algoritmikus működése olyan személyekhez is el tudja juttatni a jogsértő vagy annak vélt bejegyzéseket, akik a hagyományos kommunikációs körülmények között nem is szereznének erről tudomást. E jelentékeny specifikum miatt indokolt lehetne egy egységes és koncepciózus bírói gyakorlat kialakítása az online térben történő elkövetésre. Ennek jelei már tetten érhetők a fent említett relatív vagy korlátozott nyilvánosság megítélése tekintetében formálódó gyakorlat révén, amely keretében vizsgálat tárgyát képezi a sérelmezett bejegyzés potenciális elérhetőségi köre, valamint annak hatása, ugyanakkor vannak még nyitott kérdések, mint például a realizált nem vagyoni sérelem és a nyilvánosság közötti kapcsolat.

5. Összegző gondolatok

A tanulmányunkban említett adatok alapján megállapítható, hogy mindennapjainkra egyre nagyobb hatással vannak a különböző közösségi platformok, amelyeket előszeretettel használunk informálódásra, véleményünk megosztására, valamint vásárlásra is. E platformok gyakori használatára is figyelemmel nem meglepő, hogy a bírói gyakorlatnak is több ízben kellett olyan jogvitában döntenie, ahol a jogsértés valamelyik közkedvelt platformon történt.

91 E körben hivatkozunk kifejezetten a Ptk. 2:52. § (3) bekezdésében foglaltakra.

E körben talán meglepetésként az szolgálhat, hogy e jogsértések leginkább a Facebookra, valamint a YouTube-ra korlátozódnak, más, szintén népszerű közösségi platformok még nem jelentek meg. Ezt részben mindenféleképpen magyarázhatjuk a Facebook rendkívüli mértékű elterjedtségével, azonban említésre érdemesek az Instagram és újabban a TikTok által elért havi látogatottság számadatai. Ennek ellenére a tanulmány megírása során nem találtunk olyan, a Bírósági Határozatok Gyűjteményében szereplő anonimizált bírósági döntést, ahol e platformok valamelyikén történt volna jogsértés. Álláspontunk szerint ebből azonban nem lehet olyan következtetést levonni, hogy e platformok mentesek lennének a személyiségi jogi jogsértésektől, sokkal inkább egy demográfiai megközelítésű válasz tűnik valószínűnek: az ezeket a platformokat leginkább használók körében feltételezhetően eltérő érdekérvényesítés tapasztalható.

A hazai joggyakorlat a közösségi platformokon történő jogsértés során figyelembe veszi a platform által biztosított relatív nyilvánosságot. E körben nincs egy konkrét ismerősi, követői szám meghatározva, amelynek elérése esetén egy sérelmezett bejegyzés vonatkozásában megállapítható lenne, hogy a bejegyzés jelentős személyi körhöz ért el. Sokkal inkább arról van szó, hogy a bírói gyakorlat mérlegelése során figyelemmel van a bejegyzéssel érintett profil vagy csoport ismertségére, látogatottságára, valamint annak személyi összetételére. A gyakorlat a közösségi platform nyilvánosságára inkább egyfajta potenciális lehetőségként tekint, melynek során a sérelmezett bejegyzés a társadalom minél nagyobb szeletéhez képes eljutni. Ez egyben azt is jelenti, hogy önmagában egy nagy követői bázissal rendelkező Facebook-profilon közzétett bejegyzés esetében a jelentős mértékű jogsértés ténye nem lesz automatikusan megállapítható, mivel az eset összes körülményét is figyelembe kell venni: ki tette azt közzé, milyen a kontextusa, arra milyen reakciók érkeztek, eljutott-e másokhoz, mennyi ideig volt elérhető.

Álláspontunk szerint a felelősség mérlegelése tárgyában a bírói gyakorlat egyik legfontosabb eleme annak vizsgálata, hogy a jogsértő szakmai kompetenciája, jártassága, illetve esetleges szervezeti háttere mennyiben teszi lehetővé számára az általa állított vagy közölt tények valóságalapjának ellenőrzését. E vizsgálat eredménye a sérelemdíj mértékének meghatározásában jut kifejezésre.

Összegzésként megállapíthatjuk egyfelől, hogy a bírói gyakorlat az online térben elkövetett személyiségi jogi jogsértések vonatkozásában alapvetően az offline térben elkövetett jogsértésekhez hasonlóan jár el azzal, hogy az online tér sajátosságait, azaz a relatív vagy korlátozott nyilvánosságot veszi figyelembe döntése meghozatalakor. Másfelől azonban érdemben nem foglalkozik azzal a kérdéssel, hogy az online tér sajátosságai miatt eltérő megítélés alá kell-e vonni az online térben elkövetett jogsértéseket, vagy nem szükséges az offline és online tér között éles határvonalat húzni a személyiségi jogi jogsértések vonatkozásában.

A közösség elleni uszítás jogalkalmazási gyakorlata

Botos Mihály Bálint

1. Bevezetés

A gyűlölet-bűncselekmények kategóriája a kriminológiában ismert és használt klasszifikáció, a büntető anyagi jog ilyen meghatározást nem ismer. Kriminológiai értelemben számos büntetőjogi tényállás e kategóriába sorolható, továbbá a Btk.-ban találhatók olyan tényállások is, amelyek kifejezetten a gyűlölet valamilyen formában történő kifejtését rendelik büntetni.[1] E kategóriába sorolható a közösség elleni uszítás tényállása is, amelyet sokszor a gyűlöletbeszéd büntető anyagi jogi megfelelőjeként azonosítanak.

A választott téma aktualitását szemléleti, hogy 2021-ben az Európai Bizottság kezdeményezte, hogy az uniós bűncselekményi területek listája a gyűlöletbeszéddel és a gyűlölet-bűncselekménnyel bővüljön.[2] Ennek ellenére 2010 után e téma büntetőjogi szakirodalmi feldolgozottsága elenyésző, ugyanis az ezt követő időszakban nem születtek átfogó, alkotmányos büntetőjogi fókuszú elemzések a véleményszabadságnak kollektív jogi tárgyra figyelemmel történő korlátozása tárgyában.[3]

Jelen tanulmány a közösség elleni uszítás jogalkalmazási gyakorlatát vizsgálja. Ennek érdekében a Fővárosi Főügyészségen 50, közösség elleni uszítás miatt indult eljárás ügyiratát elemeztem 2013–2023 között. Adatvédelmi okokból az ügyeket saját, egyedi megjelöléssel jelöltem.[4]

A határozatok elemzése előtt azonban szükséges az Alaptörvény negyedik módosítása előtti joghelyzetet röviden bemutatni (alkotmánybírósági és rendes bírósági gyakorlat szerint), hiszen az a jelenlegi gyakorlat megértéséhez elengedhetetlen. Nem célom a vonatkozó alkotmánybírósági határozatok részletes elemzése, csupán a döntések lényegi megállapításait

1 Ez utóbbi bűncselekményeket viszont éppen a kriminológiai szakirodalom nem tekinti gyűlölet-bűncselekménynek. Szomora Zsolt: Dogmatikai és alkotmányjogi megjegyzések a gyűlölet-bűncselekmények büntetőjogi szabályozásához. *Belügyi Szemle,* 2013/2. 36–39.

2 A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak. Inkluzívabb és védelmezőbb Európa: az uniós bűncselekmények listájának kibővítése a gyűlöletbeszéddel és a gyűlölet-bűncselekményekkel. COM(2021) 777 final. Az ügyben még nem történt előrelépés, jelenleg az Európai Parlament jelentéstervezetet készített, amelyben politikai felhívást intézett a Tanácshoz a szükséges határozat elfogadása céljából.

3 Az alábbi monográfiák emelhetők ki az Alaptörvény negyedik módosítása előtt: Koltay András: *A gyűlöletbeszéd korlátozása Magyarországon. Alkotmányos és jogalkalmazói megközelítések, európai kitekintéssel.* Budapest, CompLex, 2013; Bárándy Gergely: *A gyűlöletbeszéd Magyarországon*. Budapest, Scolar, 2009; Hornyák Szabolcs: *A köznyugalom elleni bűncselekmények* [Doktori értekezés]. Pécsi Tudományegyetem, 2009. https://rb.gy/ocg3so

4 Az egyedi jelölés a következő módon történik. A Ku. a közösség elleni uszításra utal; ezt követi az évszám, hogy melyik évben indult az ügy; egy adott évben indult ügyeket pedig 1-től felfelé sorszámoztam. (pl.: Ku.2023/1.) Sok esetben a feljelentést elutasító határozat ellen panasz érkezett, így, ha az adott ügyben panaszt elbíráló határozat is született, akkor az utóbbi határozatot P-vel jelölöm (pl.: KuP.2023/1.). Egy esetben történt, hogy a bíróság az eljárást megszüntette, amely ellen az ügyészség fellebbezést jelentett be. A másodfokú határozatot római számmal jelöltem az alábbi módon (Ku.2014/3-II.).

vizsgálom, amelyek a jelenlegi gyakorlatban is visszatükröződnek. A közösség elleni uszítást elemző tanulmányok[5] központi vizsgálati tárgya az igen vitatott *clear and present danger* mércéje, amelyre való utalás már a véleménynyilvánítási szabadsággal és uszítással (akkor izgatás) foglalkozó, mára alaphatározatnak számító 30/1992. (V. 26.) AB határozatban (a továbbiakban: Abh1.) is megjelenik.[6] Ebből kifolyólag szükséges röviden a mérce jelentéstartamát feltárni és vizsgálni, hogy valóban e mérce kerül-e alkalmazásra a hazai joggyakorlatban.

2. A clear and present danger jelentéstartalma

A *clear and present danger*-elv amerikai megjelenése, majd általános elfogadása sem volt zökkenőmentes, hiszen az elv kezdetben különvéleményekben jelentkezett. Az első megfogalmazása a Schenk v. United States ügyben történt, amelyben Holmes bíró a kérdést abban látta, hogy „a használt szavak vajon olyan körülmények közepette kerültek-e nyilvánosságra, és olyan jellegűek-e, hogy jelentős károk [...] nyilvánvaló és közvetlen veszélyét idézik elő."[7] A Whitney-ügyben – szintén különvéleményben – megerősítésre került ez az álláspont, ugyanis tovább pontosították a mércét, amely alapján a „véleménynyilvánítás által előidézett veszély okozta kárnak komolynak kell lennie, a veszélynek pedig azonnalinak és egyértelműnek."[8]

Ahogy Molnár Péter is bemutatja, ezt követően sem került alkalmazásra a teszt az amerikai jogalkalmazási gyakorlatban. A Dennis-ügyben az Amerikai Kommunista Párt vezetőit ítélték el a kormány erőszakos megdöntését támogató konspiráció vádjával, amelyben egyáltalán nem vizsgálták a következményeket, hogy a vád tárgyává tett megnyilvánulás előidézte-e az erőszak azonnali veszélyét.[9] Koltay András az elv tényleges megszilárdulását és a mai napig érvényben lévő megfogalmazását a Brandenburg-ügyhöz köti, azonban már – ahogy bemutatja – a Yates v. United States ügyben is található a *clear and present danger* elvét átalakító megfogalmazás: „a korlátozáshoz eszerint az kell, hogy a közlő kifejezetten felhívjon valamely jogsértő cselekmény végrehajtására, függetlenül az ezáltal keletkező veszély mértékétől."[10] Látható, hogy itt a veszély nyilvánvaló és közvetlen volta nem része a tesztnek („független a keletkező veszély mértéktől").

A Brandenburg-ügyben *criminal syndicalism* (erőszakos célú szervezkedés, illetve annak támogatása) miatt ítélték el a Ku-Klux-Klan egyik vezetőjét, mivel egy felvételen keresztégetés közben a zsidóságra és feketékre is sértő megjegyzéseket tett. A teszt alapján „azok a közlések, amelyek erőszakra vagy más jogsértésekre hívnak fel, csak akkor korlátozhatóak, ha

5 A teljesség igénye nélkül: Koltay András: A 'clear and present danger' elv fordulatos története az Egyesült Államokban és Magyarországon. *Magyar Jog,* 2009/7. 415–423.; Sajó András: A rasszista nézetek büntetésének alkotmányosságáról. In: Gellér Balázs (szerk.): *Györgyi Kálmán ünnepi kötet*. Budapest, KJK-Kerszöv, 2004. 479–509.; Vaskuti András: A közösség elleni izgatás bírói gyakorlata. In: Ligeti Katalin (szerk.): *Wiener A. Imre 70. születésnapjára.* Budapest, Közgazdasági és Jogi Kiadó, 2005. 185–205.; Zentai Ágnes: Véleményszabadságtól a Molotov-koktélokig avagy a 'clear and present danger' és az önrendelkezési jog szomorú története. *Rendészeti Szemle*, 2010/2. 42–63.

6 30/1992. (V. 26.) AB határozat, ABH 1992, 167. 179.

7 Koltay (2009) i. m. 415.

8 Molnár Péter: Uszítás vagy gyalázkodás? *Fundamentum,* 2001/4. 119.

9 Uo. 120.

10 Koltay (2009) i. m. 417.

kifejezetten az azonnali erőszakra vagy jogsértésre való rábírásra irányulnak, arra kifejezetten felhívnak, és annak bekövetkezte valószínűsíthető."[11]

Az eredeti megfogalmazásában a *clear and present danger* elve a Brandenburg-ügy alapján teljesen átalakult. Egyetértve Molnár álláspontjával, új mérce került megfogalmazásra a nyilvánvaló és közvetlen veszélyt előíró teszt helyett.[12] Az új mérce már nemcsak egy valóságosan bekövetkező veszélyes cselekedetet követel meg, hanem erre közvetlenül vonatkozó kifejezett felhívást (rábírást). Ebből következik, hogy a felhívás típusú nyilatkozat közvetlen oka az ez alapján bekövetkező veszélynek. Ilyen követelmény az eredeti tesztből nem volt kiolvasható.

Az amerikai jogfejlődésben a mérce 1969-re jelentősen átalakult, leszűkült, azonban hatóköre a mai napig bizonytalan, ugyanis a Legfelső Bíróság igen változatos ügyekben alkalmazta.[13] A mérce értékelésére és a magyar jogrendszerben történő implementálásnak, illetve azzal összeegyeztethetőségének kérdésére, a magyar alkotmánybírósági gyakorlat áttekintését követően kerül sor (3. pont).

3. Az alkotmánybírósági és rendes bírósági gyakorlat vázlatos áttekintése az Alaptörvény negyedik módosítása előtt

Az Alkotmánybíróság a közösség elleni uszítás tényállásának alkotmányos megítélésével érdemben négy alkalommal foglalkozott.[14] Az Abh1.-ben a testület nemcsak a véleményszabadság mint kommunikációs alapjog lényegi tartalmát foglalta össze, hanem a nemzetközi kötelezettségek[15] áttekintése után, az uszítás elkövetési magatartását is – történeti kontextusban – elemezte.

Az (1) bekezdést[16] alkotmányosnak tekintette, a gyalázkodási fordulatot[17] alkotmányellenesnek. A taláros testület legfontosabb megállapításai a következők:

a) a véleményszabadság a kommunikációs alapjogok anyajoga, ezért igen kevés joggal szemben kell engednie. A közlés tartalmától függetlenül védelemben részesül, tehát a vélemények állam általi, tartalmi alapon való korlátozása alkotmányosan nem

11 A bíróság egyébként megváltoztatta a döntést és megsemmisítette a döntés alapjául szolgáló normát is. Koltay (2009) i. m. 417.

12 Molnár i. m. 121.

13 Koltay (2009) i. m. 417–418.

14 30/1992. (V. 26.) AB határozat, ABH 1992, 167.; 12/1999. (V. 21.) AB határozat, ABH 1999, 106.; 18/2004. (V. 25.) AB határozat, ABH 2004, 303.; 95/2008. (VII. 3.) AB határozat, ABH 2008, 782.

15 Az Alkotmánybíróság utalt az Emberi Jogok Európai Egyezményére, illetve az EJEE alapján kialakult gyakorlatra. Tanulmányomban nem foglalkozok az Emberi Jogok Európai Bíróságának gyakorlatával. Ennek indoka, hogy a strasbourgi bíróság gyakorlata nem kiforrott, ugyanis a konkrét mérce meghatározása a részes államok feladata. Fontos megemlíteni, hogy az EJEB gyakorlatában – szemben a magyar alkotmánybírósági gyakorlattal – léteznek eleve olyan szólások, amelyek kívül esnek az EJEE 10. cikkének védelmi hatókörén, ezért sok esetben a panasz befogadását megtagadja az Egyezmény 17. cikkére hivatkozással (joggal való visszaélés tilalma). Ehhez lásd: Norwood v. United Kingdom, no. 23131/03., admissibility decision, 2004. november 16-i döntés.

16 „(1) Aki a nagy nyilvánosság előtt

a) a magyar nemzet vagy valamely nemzetiség,

b) valamely nép, felekezet vagy faj, továbbá a lakosság egyes csoportjai ellen gyűlöletre uszít [...]."

17 „(2) Aki nagy nyilvánosság előtt a magyar nemzetet, valamely nemzetiséget, népet, felekezetet vagy fajt sértő vagy lealacsonyító kifejezést használ, vagy más ilyen cselekményt követ el [...]."

megengedett, ezért a véleményszabadságnak kizárólag külső korlátai lehetnek. Ezen megállapításához állította fel a következő követelményt:

„A vélemény szabadságával szemben mérlegelendő korlátozó törvénynek nagyobb a súlya, ha közvetlenül másik alanyi alapjog érvényesítésére és védelmére szolgál, kisebb, ha ilyen jogokat csakis mögöttesen, valamely »intézmény« közvetítésével véd, s legkisebb, ha csupán valamely elvont érték önmagában a tárgya (pl. a köznyugalom).”[18]

b) Az elkövetési magatartással összefüggésben a határozat az alábbiakat tartalmazza:

„[O]lyan magatartások értendők ide, »amelyek alkalmasak arra, hogy az emberek nagyobb tömegében a szenvedélyeket oly magas fokra lobbantsák, amelyből gyűlölet keletkezvén, a társadalmi rend és béke megzavarására vezethet«. A társadalmi rend és béke – a Btk. szóhasználatával élve a köznyugalom – ilyen megzavarása mögött ott van nagyszámú egyéni jog megsértésének a veszélye is: a csoport ellen felszított indulat fenyegeti a csoporthoz tartozók becsületét, méltóságát (szélsőséges esetben életét is), megfélemlítéssel korlátozza őket más jogaik gyakorlásában is [...]. Az (1) bekezdésben szankcionált magatartás olyan veszélyt hordoz egyéni jogokra is, amelyek a közvetlen tárgyként szereplő köznyugalomnak olyan súlyt adnak, hogy [...] a véleményszabadság korlátozása szükségesnek és arányosnak tekinthető. Noha a mérlegelés gyakorlati eredménye hasonló, ebben a gondolatmenetben nem csupán a köznyugalom megzavarásának intenzitásáról van szó, amely egy bizonyos mérték fölött (»*clear and present danger*«) igazolja a szabad véleménynyilvánításhoz való jog korlátozását. Itt az a döntő, hogy mi került veszélybe: az uszítás az alkotmányos értékrendben szintén igen magasan álló alanyi jogokat veszélyeztet.”[19]

A határozat indokolásának ezen része az, amely a gyakorlatban – és a jogtudományban is – értelmezési nehézségeket vet fel. Az Abh1. *clear and present danger*-mércéjére utaló indokolása mind a későbbi alkotmánybírósági határozatokban, mind a közzétett eseti döntésekben visszaköszön.

Az 1999-es AB határozat indokolásának egyetlen egy része utal valamilyen veszély kialakulására:

„a már száz éve követett bírói gyakorlat szerint is csakis az uszítás foglalja magában azt a »bizonyos mérték« fölötti veszélyt, amely a véleménynyilvánításhoz való jog korlátozását megengedhetővé teszi.”[20]

A 2004-es alkotmánybírósági határozatig a bírói gyakorlat tolta feljebb az uszítás büntetendőségének alsó határát. Ennek indokát Szomora Zsolt abban látta, hogy a bíróságok észlelték a megváltozott jogszabályi környezetet: az izgatás uszításra változott, azonban az Alkotmánybíróság e két fogalmat azonosnak tekintette.[21]

18 30/1992. (V. 26.) AB határozat, ABH 1992, 167, 178.

19 Uo. 178–179.

20 12/1999. (V. 21.) AB határozat, ABH 1999, 106, 110.

21 Szomora Zsolt: *Alkotmány és anyagi büntetőjog. A büntetőjog-alkalmazás alkotmányosságának egyes kérdései*. Szeged, Iurisperitus, 2015. 40.

Ezt jól szemléleti a BH1997. 165. számon közzétett eseti döntés: „az uszítás nem egyszerűen gyűlölet, hanem olyan gyűlölet felkeltésére irányul, amely aktív tevékenységbe megy át. Aki »gyűlöletre uszít«, az másokat aktív, tevékeny gyűlöletre ingerel." Azonban érdemes a határozat ezen, indokolást megelőző szövegrészére utalni, amelyben a Legfelsőbb Bíróság kifejtette, hogy

> „[e] bűncselekmény tehát veszélyeztető cselekmény. Ez azt jelenti, hogy valamilyen valóságos sérelem mint eredmény már nem tartozik a törvényi tényálláshoz. Nincs jelentősége annak sem, hogy az uszításra a jelenlévők hogyan reagálnak. A lényeg az, hogy az elkövető gyűlöletre uszított vagy sem."

A BH1998. 521. *ratio decidendi*je kizárólag az elkövető tudattartalmára vonatkozó megállapítást tartalmaz, hiszen „a cselekmény megvalósulásához elegendő, hogy az elkövető tudatában legyen annak: a nagyobb nyilvánosság előtt tett kijelentései a gyűlölet keltésére objektíve alkalmasak." A *ratio decidendi* értelmezése alapján a Legfelsőbb Bíróság a tényállást (még) absztrakt veszélyeztető tényállásként kezelte.[22]

Végül a Fővárosi Ítélőtáblának a Hegedűs-ügyben hozott döntése volt az, amely a közösség elleni uszítás tényállását alkalmazhatatlanná tette, ugyanis a büntetendőséghez hármas követelményt támasztott:

> „nem a véleménynyilvánítási szabadságával él, hanem gyűlöletre uszít az, aki erőszakos cselekedetre, ilyen magatartás vagy tevékenység kifejtésére hív fel akkor, ha a veszély nem csupán feltételezett, hanem a veszélyeztetett jogok konkrétak, és az erőszakos cselekedet közvetlenül fenyeget."[23]

Tehát a gyakorlat az erőszakra és a gyűlöletre uszítást egy fogalomként kezelte, holott az akkori tényállás kizárólag a gyűlöletre uszítást tartalmazta, továbbá az elkövetési magatartásból felhívás lett.[24] Valójában ez a megfogalmazás nem is az eredeti *clear and present danger*-, hanem a Brandenburg-teszt.

A probléma az, hogy a 18/2004. (V. 25.) AB határozat a táblabíróság téves értelmezését fogadta el „élő jogként", aminek következménye az lett, hogy a jogalkalmazási gyakorlat végérvényesen eredmény-bűncselekményt kreált egy absztrakt veszélyeztető tényállásból.[25] A határozat ezen kívül a *clear and present danger* mércéjére is utal:

> „[a] szabad véleménynyilvánítás jogának korlátozására a »gyűlöletre uszítás« esetében az egyéni alapjoggyakorlás sérelme, illetve annak közvetlen veszélye miatt kerül sor. Végül fontos, hogy a köznyugalomban okozott veszély ne csupán feltételezés legyen, és a legalább hipotetikus visszacsatolás [...] elengedhetetlen. A köznyugalom megzavarásának intenzi-

22 Hasonló indokolást tartalmaz az EBH1999. 5. szám alatt közzétett legfelsőbb bírósági döntés is.

23 Az ítélet megjelent BH2005. 46. szám alatt.

24 A 2016-os Btk. módosítása választotta el a két fogalmat, amikor bekerült a tényállásba az erőszakra uszítás. Ennek jelentőségével az 5. pontban foglalkozom.

25 Szomora (2015) i. m. 40.

tása ugyanis »egy bizonyos mérték fölött (*clear and present danger*) igazolja a szabad véleménynyilvánításhoz való jog korlátozását.«"[26]

A közösség elleni uszítás alkotmányos megítélésével foglalkozó utolsó, 2008-as alkotmánybírósági határozat, bár explicit módon nem említi meg a *clear and present danger* mércéjét, mégis olyan indokolást használ, amely nem hagy kétséget afelől, hogy a gyakorlat a bűncselekmény dogmatikai karakterét megváltoztatta:

„[a]bban az esetben pedig, ha a rasszista beszéd az elhangzás körülményei folytán erőszakcselekmény veszélyével, egyéni jogok sérelmével fenyeget, és a jogsérelem a személyek pontosan meg nem határozható, nagyobb csoportját érinti, az elkövető [...] közösség elleni izgatás miatt felelősségre vonható."[27]

Az alkotmánybírósági és rendes bírósági határozatok indokolásának bemutatását azért tartottam szükségesnek, mert ahány indokolás, annyi fajta eltérő értelemzés olvasható ki a *clear and present danger* mércéjére vonatkozóan. Ebből következik, hogy a jogirodalomban is egymással szemben álló álláspontok találhatók a határozatokból kiolvasható 'valamilyen' veszély értelmezésére.[28]

Magam részéről messzemenőkig egyetértek Zentai Ágnes megállapításával, hogy az Abh1.-ben (és a későbbi határozatokban is) a *clear and present danger* mércéje a határozat teljes értelmezési mátrixában értelmezhetetlen, az arra történő utalás a koherenciát megbontja.[29] Ehhez az alábbiakat szükséges rögzíteni:

a) A teszt (*clear and present danger; Brandenburg*) eltérő jogrendszerben, eltérő történelmi és kulturális kontextusban fogalmazódott meg az Amerikai Egyesült Államokban. Alapvető különbség, hogy az Alkotmánybíróság elvi éllel mondta ki, hogy a véleménynyilvánítás szabadsága minden közlésre kiterjed, a tartalom szerinti korlátozás alkotmányosan nem megengedett.[30] Ezzel szemben az amerikai jogrendszer a közlések egy bizonyos csoportját eleve kizárja a szólásszabadság védelmi hatóköréből.[31] Ezt a distinkciót azért szükséges kiemelni, ugyanis, ha az Alkotmánybíróság ténylegesen e mérce magyar jogrendszerbe történő beemelése mellett döntött volna, akkor az azon véleményszabadságot korlátozó tényállásoknál is alkalmazandó lett volna, amelyek a köznyugalmat védik (pl. önkényuralmi jelkép használata, nemzeti jelkép megsértése, holokauszttagadás). Azonban a taláros testület ilyen mércét ezekben a határozatokban nem alkalmazott.

b) Az előző ponttal összefügg, hogy nem hagyható figyelmen kívül, hogy a bevezetett mércéket eltérő dogmatikai karakterű és védelmi célú bűncselekményekhez állították fel. A Brandenburg-ügyben a vád tárgya ún. *criminal syndicalism* (erőszakos célú

26 18/2004. (V. 25.) AB határozat, ABH 2004, 303, 309.

27 95/2008. (VII. 3.) AB határozat, ABH 2008. 782, 792.

28 Koltay három csoportba osztja a határozatokat értelmező álláspontok képviselőit: Az első csoportba azok tartoznak, akik nyilvánvaló és közvetlen veszélyt, a másodikba azok, akik valamilyen (reális, valós, tényleges) veszélyhelyzetet követelnek meg, a harmadikba pedig azok, akik mindenféle veszélyhelyzet-követelményt elutasítanak, mert nem tartozik a tényálláshoz (tradicionalista büntetőjogi álláspont). Koltay András: A rémhírterjesztés büntethetőségének alkotmányosságáról. *In Medias Res*, 2020/2. 326–327.

29 Zentai i. m. 48.

30 Megjegyzem, létezik az alkotmánybírósági gyakorlatban tartalomorientált korlátozás is (jelképhatározatok): 13/2000. (V. 12.) AB határozat, ABH 2000, 61.; 14/2000. (V. 12.) AB határozat, ABH 2000, 83.

31 Ilyen pl. a megfélemlítő közlés. Sajó i. m. 495. Erre hívja fel a figyelmet Lévay Miklós is a 2008-as határozathoz fűzött párhuzamos indokolásában is. 95/2008. (VII. 3.) AB határozat, ABH 2008, 782, 804.

szervezkedés, illetve annak támogatása) volt, amely bűncselekmény az adott történelmi kontextusban volt értelmezhető, ugyanis ez egy olyan jogi fogalom, amelynek lényege az erőszakot a társadalmi változás eszközeként alkalmazó tanok és tevékenységek tiltása, és amely a szindikalista és más forradalmi munkásmozgalmak növekedésének köszönhette eredetét az Egyesült Államokban a 20. század első két évtizedében.[32]

c) Szintén a dogmatikai karakterrel függ össze, hogy a mérce, sőt bármilyen nem absztrakt veszély megkövetelése a törvényi tényállásból nem olvasható ki. A tényállástanban az eredmény (annak sértő vagy veszélyeztető változata) egyértelműen körülírt, objektív tényállási elem. Amennyiben ilyen fordulatot nem tartalmaz a tényállás, a bűncselekmény immateriális. Egyetértve Zentai álláspontjával, amennyiben a testület az Abh1.-ben tényleg a nyilvánvaló és közvetlen veszély tesztjét alkalmazta volna és állította volna fel irányadó mércének, akkor az (1) bekezdést is megsemmisítette volna.[33]

Látható, hogy az Alaptörvény negyedik módosítása előtt a tényállás dogmatikai karaktere jelentősen átalakult, amiben nemcsak a taláros testület a hibás (az adott szövegkörnyezetben értelmezhetetlen utalás a *clear and present danger* mércéjére), hanem a jogirodalom is, hiszen túl nagy jelentőséget tulajdonított – a szövegkörnyezetből kiragadva – a mérce esetleges értelmezésének. Innentől már csak 'egy lépés' volt, hogy a bírói jogalkalmazás eredmény-bűncselekményt kreáljon az absztrakt veszélyeztető tényállásból, amelyet az Alkotmánybíróság 2004-ben élő jogként 'szentesített'. A hibás gyakorlat oda vezetett, hogy 2005–2008 után gyakorlatilag nem történt felelősségre vonás, a közösség elleni uszítás miatt indult eljárásokat megszüntették, még extrém gyűlöletbeszéd esetén is.[34]

4. A közösség elleni uszítás jelenlegi gyakorlata

Az előbbiekben kifejtetteket azért tartottam szükségesnek bemutatni, mivel vizsgálandó kérdés, hogy az Alaptörvény negyedik módosítása után mennyiben veszi figyelembe a jogalkalmazói gyakorlat a régi, módosítás előtti alkotmánybírósági határozatokat. Szomora Zsolt már 2013-ban hangsúlyozta, hogy a tarthatatlan gyakorlat megváltoztatása első lépésként az ügyészség feladatköre: vádat kell emelni minden olyan gyűlöletkeltő megnyilvánulás miatt, amit korábban nem tekintettek bűncselekménynek.[35] Beszédes adat az általam végzett joggyakorlat-elemzésből, amely előrevetítheti a tanulmány joggyakorlat tarthatatlanságára vonatkozó megállapítását: az 50 ügyből 2 esetben került sor vádemelésre. Ezek közül egy esetben került sor a büntetőjogi felelősség megállapítására.

32 Woodrow C. Whitten: Criminal Syndicalism and the Law in California: 1919-1927. *Transactions of the American Philosophical Society*, vol. 59, no. 2. (1969) 3.

33 Zentai i. m. 47.

34 A nyomozó hatóságok az eljárást még abban az extrém esetben is megszüntették, amikor az inkriminált megnyilvánulás a következő volt: „Az SZDSZ és a zsidópárt holdudvarának minden tagjának felajánlunk egy-egy bőröndöt a meneküléshez. Cserébe elfogadunk aranyat (nem baj, ha fog formájú) ezüstöt (a tőlünk ellopott családi érdekelne a leginkább) valamint emberi bőrt lámpaernyő készítéséhez. Hitelre nem adunk semmit, mert tudjuk, hogy nem kapnánk vissza. Amennyiben két bőröndöt vásárol, úgy ajándékba egy Zyklon B-t tartalmazó gázpalackot adunk. Jó utat Izraelbe, soha ne halljunk egymásról!" Zentai i. m. 62.

35 Szomora (2013) i. m. 49–50.

4.1. Védett csoportok

A Btk. 332. §-a által felsorolt védett közösségek nem képeznek zárt listát, a jogalkotó *exemplifikatív* felsorolást alkalmaz. Ide tartozik a magyar nemzet, valamely nemzeti, etnikai, faji, vallási csoport, illetve annak tagja vagy a lakosság egyes csoportjai, illetve azok tagjai. A védett csoportok joggyakorlati vizsgálatánál nem foglalkozom a közösségek méltóságának, illetve ezzel összefüggésben az Alaptörvény IX. cikk (5) bekezdésének kérdéskörével, mivel ennek – álláspontom szerint – a lehetséges mércénél van jelentősége (5. pont).

A védett csoportok nem elkövetési tárgyként szerepelnek a tényállásban, a jogalkotó által megjelölt csoportok „absztrakt tárgyak".[36] Hogy mit jelent a közösség, arra vonatkozóan a jogirodalomban sem találunk egységes definíciót. Bárándy szerint a közösség „olyan személyösszesség, amelynek tagjai egymással összetartozónak, kívülállóktól különbözőnek érzik magukat."[37] Ebben a fogalomban főképp a szubjektív elem a domináns, tehát a közösség fogalmának lényegi alkotóeleme a szubjektív összetartozás és különbözőség érzésének tudata. Bárándy hangsúlyozza, hogy egy adott közösséghez tartozás nem minden esetben egyéni döntés kérdése (nemzet, etnikai hovatartozás), szemben pl. a vallási közösséghez tartozással.[38] Azonban az már mindenkinek az egyéni döntése, hogy szabadon kiléphet az adott csoportból, esetleg a nemi identitását is megváltoztathatja. Koltay András fogalommeghatározás helyett általános ismérveket állított fel csoportalkotó tényezőknek. Ezek: összetartozás-érzés; más csoportoktól való észrevehető elkülönülés; rendelkeznek belső, csak tagjaikra vonatkozó szabályokkal; és a csoportalkotó tényezők a külvilág számára jól felismerhetők.[39]

Álláspontom szerint ezek mérlegelési szempontként érvényesülhetnek egy közösségi jelleg megállapításánál, azonban nem minden egyes elemnek kell ténylegesen fennállnia, hiszen akkor a védelem hatókörét jelentősen szűkítenénk (értelemszerűen egy nemi identitás alapján létrejövő közösségnek nincs belső, csak a tagjaira vonatkozó szabályzata). Valamint szükséges megemlíteni, hogy a közösség elleni uszítás nem (kizárólag) a kisebbségeket védő tényállás, ugyanis már a diszpozíció első helyen utal a magyar nemzetre. Ebből következik, hogy általános definíciót nem lehet és nem is kell megadni ahhoz, hogy egy szerveződést közösségnek minősítsünk, az minden esetben a jogalkalmazó egyedi mérlegelésén múlik, hogy az adott közösség a közösség elleni uszítás védendő csoportjának tekinthető-e. Fontos mérlegelési szempont azonban az, hogy az adott csoport, szerveződés céljait és tevékenységét tekintve alkotmányos keretek között jött létre, illetve működik, ugyanis jogtárgyharmonikus értelmezéssel[40] arra a megállapításra kell jutnunk, hogy az e követelménybe ütköző csoportok eleve kívül esnek a bűncselekmény védelmi hatókörén.

Kérdésként merült fel, hogy ezek a szempontok a jelenlegi gyakorlatban visszatükröződnek-e, valamint, hogy melyek az adott védett csoportok, amelyeknek a gyakorlatban relevanciájuk van. Az mindenképp rögzíthető, hogy a nyomozóhatóságok sok esetben a védett

36 Mezőlaki Erik: XXXII. Fejezet. A köznyugalom elleni bűncselekmények. In: Karsai Krisztina (szerk.): *Nagykommentár a Büntető Törvénykönyvhöz*. Budapest, Wolters Kluwer Hungary, 2022. 789.

37 Bárándy i. m. 28.

38 Uo.

39 Koltay András: A közösségek méltóságának védelme. *Iustum Aequum Salutare* 2005/1. 162.

40 A jogtárgyharmonikus értelmezés alapján egy adott büntetőjogi rendelkezést úgy kell értelmezni, hogy az lehetőleg alkalmas eszköz legyen a szabályozással elérni kívánt törvényi cél elérésére. A jogtárgyharmonikus értelmezéshez lásd: Szomora (2015) i. m. 29–35.

csoportok vizsgálatát (a közösségi jelleg mérlegelését) mellőzik. Az általam vizsgált ügyekben egy esetben sem mondták ki, hogy nem volt védett csoporti minőség, még akkor sem, ha a feljelentésekben foglalt megnyilvánulások konkrétan beazonosítható (egy) személyre vonatkoztak. Ezt az alábbi ügyekkel szemléltetem.

A feljelentő szerint az elkövető nyíltan kívánta a miniszterelnök halálát, ugyanis egy közösségi portálon az alábbi bejegyzést írta:

> „A szomszédomat viszik. Többet nem látom élve. Pedig nem arra az oldalra szavazott szerintem, amire én. A poloskát is wc-papírba csomagolva dobtam ki nyáron az ablakon, de ahogy az Ozban a gonosz boszorkány halálát várták, úgy várom [a miniszterelnökét] is, és pezsgőt fogok bontani, ha megdöglik. Mert emberek élete szárad a lelkén. Az olaszok már régen [a miniszterelnökre] gyújtották volna a karmelita menzát..."[41]

A nyomozóhatóság nem a hiányzó védett csoporti minőségre hivatkozva, hanem az elkövetési magatartás megvalósulásának hiánya miatt utasította fel a feljelentést.

Ehhez hasonló eset volt, amikor a cikk írója azt sérelmezte, hogy Magyarország miniszterelnöke – amennyiben megkapja a Kormány a koronavírus-veszélyhelyzetére tekintettel a felhatalmazást – korlátlan hatalmat kapna a veszélyhelyzet idejére. Szerinte

> „A helyzetet súlyosbítja, hogy a vészhelyzet végének elrendeléséről is egyszemélyben [a miniszterelnök] döntene. Ezzel olyan helyzet állna elő, mint a harmincas évek náci Németországában, amikor is totális diktátorrá választották Adolf Hitlert."

Felsorolta a törvénytervezet nyugtalanságra okot adó részeit, így azt, hogy a miniszterelnöknek hatalmában állna betiltani az időközi választásokat és az országos népszavazásokat. Ez alapján aggasztónak nevezte, hogy az ellenzéknek nincs lehetősége tiltakozásra, így egyetlen esélyként azt látja, ha mindenkinek eljuttatják a hírt, hogy „milyen veszélyeket rejt magában az, amire [a miniszterelnök] készül."[42] A feljelentést elutasító határozatban a nyomozóhatóság „belemagyarázta" a védett csoporti minőséget, ugyanis utalt arra, hogy a cikk írója a célzott társadalmi csoport tagjai részére sértő megnyilvánulást nem tett, holott pedig a közlés kizárólag egy személyre vonatkozott, nem pedig a kormánypártra.

Ugyancsak kizárólag a közösség elleni uszítás elkövetési magatartását vizsgálta és elemezte a nyomozóhatóság abban az ügyben, amikor ismeretlen tettes olyan képet készített, amelyen egy magyarországi parlamenti ülésen a miniszterelnök látható egy halántékot ért lövéssel, melynek következtében a vére is folyik. Az így elkészített fényképhez azt a megjegyzést írták, hogy „Lát valaki ezzel valami problémát, én nem."[43] Itt sem található a feljelentett megnyilvánulásban olyan utalás, amely valamely védett csoportra vonatkozott volna.

Azt, hogy a nyomozóhatóságok sok esetben mennyire figyelmen kívül hagyják a védett csoporti minőséget, jól példázza az alábbi (extrém) eset.

A feljelentő egy interneten megjelenő cikket sérelmezett, amelyben a [a párt neve] elnöke szó szerint hazaárulónak nevezte a '48-as forradalmárokat, mert szembe mertek fordulni a

41 Ku.2020/2.
42 Ku.2020/7.
43 Ku.2018/1. Hasonló eset volt egy kizárólag miniszterre vonatkozó közlés esetén is. Ku.2015/2.

Habsburgokkal. Sérelmezte továbbá, hogy „még koccintást is rendeznek minden évben október 6-án, a nemzeti gyásznapon az aradi tizenhármak kivégzésének évfordulóján! Az aradi vértanúk felségáruló, esküszegő, lázadó és fegyveres, az uralkodójuk ellen felkelt tisztek" voltak, akik csak azt a büntetést kapták, amelyet egyértelműen megérdemeltek."[44]

Ebben az ügyben is kizárólag a tényállás elkövetési magatartását vizsgálta a nyomozóhatóság. Az kérdéses, hogy mit tekinthetett itt védendő csoportnak. A politikai párt elnöke mondta a sérelmezett megnyilvánulásokat, az aradi vértanúk értelemszerűen nem tartoznak a védendő csoport kategóriájába, így kizárólag a magyar nemzet (?) fordulatát lehet(ne) felhozni. Bár a közösség elleni uszítás elkövetési magatartásának joggyakorlati bemutatására és értékelésére a következő pontban (4.2.) kerül sor, egészen érthetetlen az elutasítás indokolása, tekintettel a feljelentésben foglalt megnyilvánulásra:

> „A gyűlöletre uszítás fogalmának kiterjesztése az erőszak érzelmi előkészítését még nem jelentő magatartásokra az alkotmányos értelmezés sérelmével járna. A feljelentett cselekmény önmagában nem volt alkalmas arra, hogy az előbbiekben írt hatást kiváltsa, ezért nem jelentette a közösség elleni uszítás elkövetési magatartásának kifejtését."

Az, hogy milyen hatás kiváltásáról beszélt a nyomozóhatóság, nehezen megfejthető.

Három esetben találtam – valamiféle – indokolást, mérlegelést, utalást a védett csoporti minőség megállapítására.

Az első esetben a nyomozóhatóság igen érdekes védett személyösszességet állapított meg. A feljelentést egy közösségi portálon megjelent bejegyzés miatt tették. A bejegyzés tartalma az alábbi volt:

> „[m]a lesz másodfokú ítélet a roma népünk rasszista gyilkosainak az ügyében. Az unortodox keleti barbár horda a halálbüntetést kezdje ezekkel a kopasz, bőrfejű aljas tetvekkel. Majd folytathatjuk a pedofil papokkal, a hazaáruló idegen országnak kémkedő [párt neve] politikusokkal ezek utána a több milliárdot sikkasztó brókerekkel és akkor máris rájönnének, hogy mennyi Koppány keleti hordabélit kellene kardélre hányni, mit ahogyan azt István királyunk tette."[45]

A feljelentést elutasító nyomozóhatóság védett csoportra történő utalást tett:

> „A szövegből kiderül, hogy nem a nemzet tagjainak kivégzését sürgetik és nem akarják a lakosság csoportjainak – papok, brókerek, politikusok – ok nélküli kardélre hányását, hanem megnevezett hír kapcsán felmerült halálbüntetés-téma allegóriájaként az író mintegy tovább fűzi gondolatát, miszerint az életfogytig tartó szabadságvesztésre ítélt elkövetők esetén túlmenően bűnösként megjelölt pedofil papok, sikkasztó brókerek és hazaáruló politikusok esetében is ezt látja megoldásnak. Tehát a szövegben nem a papok, brókerek és politikusok csoportjainak megöléséről, kiirtásáról van szó, hanem a csoport – közvélemény szerint súlyosnak ítélt bűncselekmények elkövetésével – bűnösnek ítélt tagjainak – általuk jogállami keretek között visszaállítani kívánt büntetésnemmel történő megbüntetéséről."

44 Ku.2016/4.
45 Ku.2015/8.

A nyomozóhatóság az okfejtés után az elkövetési magatartást vizsgálta és arra történő hivatkozással utasította el feljelentést. Ebből következik, hogy implicit elfogadta védett csoportnak a sérelmezett megnyilvánulásból kivehető csoportokat, pontosabban a megjelölt csoportok (papok, brókerek, politikusok) bűnösként elítélt tagjaiból képződő személyösszességet.

A következő ügyben a feljelentő szerint a cikk szerzője azzal, hogy az ellenzéket „ellenségnek" és nem ellenzéknek nevezi, illetve azzal a kifejezéssel, hogy „bármilyen eszköz megengedett a védekezéshez" a gyűlöletre uszítás elkövetési magatartását valósítja meg.[46] A feljelentést elutasító határozatban a nyomozóhatóság elsőként a védett csoporti minőséget vizsgálta:

> „a »magyar ellenzék« és a nevesített pártok is valamilyen ismérv szerint elkülönülő személyösszesség, így ezen fogalmak beleesnek a lakosság egyes csoportjai kategóriába."

A harmadik eset azért is kiemelkedő, mert eljutott a vádemelésig, azonban a bíróság bűncselekmény hiányában megszüntette az eljárást, amit a másodfokú bíróság helybenhagyott. A vád tárgyává tett megnyilvánulásból („Sóherhimnusz" című dal, elemzéshez lásd: 4.2.4.), csak a védett csoportra történő utalást emelem ki:

> „Parlamentben persze mulatnak a népek, nagy verda, nagy ház, millás fizetések! Ébredj, magyar, rázd le a láncot, tolvaj kutyák lopják országod! Elég volt ebből, lángoljon minden, bibliai pusztulás lesz, kegyelem nincsen! Mit kezdjek én, mikor sóher az ország, az emberek itt kurva rabszolgák. Minden nap meló, a fizetés meg apró, szopjon le [...] meg minden tapló! Bársonykézből etetik a népet, közben milliókat keres mindegyik féreg."[47]

Az első fokon eljáró bíróság indokolásában előadta, hogy

> „a cselekménynek eszerint a lakosság egyes csoportjai ellen kell irányulnia, amelyek közül a Btk. nevesíti a nemi identitást, a szexuális irányultságot és a fogyatékosságot. Ezen ismérvek azonban nem jelentenek kizárólagosságot, a lakosság egyes csoportjainak körében a rögzült jogalkalmazói gyakorlat szerint gyakorlatilag bármilyen ismérv szerint elkülönülő személyösszesség tartozhat, és a fenti szöveggel érintett csoport – a bársonyszékben és a parlamentben ülő politikusok csoportja megfelel ennek a követelménynek."

A másodfokú bíróság hozzátette, hogy álláspontja szerint „az érintett csoport nem csupán a bársonyszékkel jelzett kormányzó politikusok, hanem a parlamentben ülőként megjelölt képviselők összessége is."[48]

A bármilyen ismérv szerint elkülönülő személyösszesség kategóriájába a nevesített védett csoportokon felül gyakorlatilag mindenféle közösség (magyar nemzet, vallási közösség stb.) beletartozhat. E tág meghatározást szemlélteti, hogy a gyakorlat még egy megemlékezésen részt vevő személyösszességet is védett csoportnak tekintett.[49] Itt a védett csoport jellegadó

46 Ku.2019/3.
47 Ku.2014/3.
48 Ku.2014/3-II.
49 Ku.2021/3.

körülménye, hogy a személyek (megemlékezés céljából) térben és időben egy helyen vannak, bárki, aki odamegy és részt vesz a megemlékezésen, védelem alá kerül.

Álláspontom szerint annak van döntő jelentősége, hogy az elhangzott szólás közvetlen utalást tartalmazzon egyértelműen beazonosítható személyösszességre. A közvetett utalást tartalmazó, valamint kizárólag egyetlen egy beazonosítható személyre tett megnyilvánulás nem elegendő.

Az általam elemzett ügyekben a következő védett csoportok kerültek megállapításra: politikai párt, beleértve a teljes ellenzéket (5 ügyben);[50] képviselők (1 ügyben);[51] homoszexuálisok (4 ügyben);[52] ukrán nemzetiség (1 ügyben);[53] zsidó vallásúak (7 ügyben);[54] autisták (1 ügyben);[55] gyűlésen részt vevő személyek (1 ügyben);[56] megemlékezésen részt vevő személyek (2 ügyben);[57] szurkolók (1 ügyben);[58] tüntető civil aktivisták, demonstrálók (2 ügyben);[59] férfi nem (1 ügyben);[60] magyar nemzet (1 ügyben);[61] határon túli magyarok (2 ügyben)[62] fekete bőrűek (3 ügyben);[63] keresztények (2 ügyben);[64] muszlim vallásúak (2 ügyben);[65] az iszlám valláson kívüli vallási közösségek (1 ügyben);[66] roma származásúak (1 ügyben);[67] bevándorlók (3 ügyben);[68] menekültek (2 ügyben).[69]

4.2. Az elkövetési magatartás és az ezzel összefüggő (absztrakt?) veszély

Az elemzett határozatokat négy csoportba osztottam. Közös a határozatokban, hogy a bűncselekményt nem absztrakt veszélyeztető, hanem konkrét veszélyeztető tényállásként kezelik.

4.2.1. A nyilvánvaló és közvetlen veszélyből levezetett felhívás mint elkövetési magatartás

Az első csoportba azokat a blanketta- (feljelentést elutasító) határozatokat soroltam, amelyek az Abh1. *ratio decidendi*jét a nyilvánvaló és közvetlen veszélyben határozták meg, és ebből vezették le a joggyakorlat által kimunkált eltérő tesztet:

50 Ku.2023/1.; Ku.2020/7.; Ku.2019/2.; Ku.2019/3.; Ku.2015/9.
51 Ku.2014/3.
52 Ku.2023/2.; Ku.2022/1.; Ku.2020/9.; Ku.2014/1.
53 Ku.2022/2.
54 Ku.2022/3.; Ku.2021/1.; Ku.2020/5.; Ku.2017/3.; Ku.2017/5.; Ku.2015/5.; Ku.2014/2.
55 Ku.2022/4.
56 Ku.2021/2.
57 Ku.2021/3.; Ku.2020/4.
58 Ku.2015/1.
59 Ku.2017/2.; Ku.2017/4.
60 Ku.2017/1.
61 Ku.2018/2.
62 Ku.2018/3.; Ku.2018/4.
63 Ku.2020/8.; Ku.2020/11.; Ku.2019/1.
64 Ku.2020/1.; Ku.2020/3.
65 Ku.2020/10.; Ku.2016/2.
66 Ku.2015/4.
67 Ku.2020/6.
68 Ku.2015/3.; Ku.2016/3.; Ku.2006/1.
69 Ku.2015/7.; Ku.2015/6.

> „Az alkotmánybíróság a közösség elleni uszítás tekintetében megállapította, hogy figyelemmel kell lenni a nyilvánvaló és közvetlen veszély követelményére, és csak e mérték fölött igazolható alkotmányosan a szabad véleménynyilvánításhoz való jog korlátozása."[70]

Ezt követően a nyilvánvaló és közvetlen veszélyre hivatkozással taglalják, hogy a joggyakorlat ennek megfelelően dolgozta ki az elkövetési magatartásra vonatkozó, hármas követelményt felállító mércét: erőszakos cselekedetre felhívás, veszélyeztett jogok konkrétsága és az erőszakos cselekedet közvetlenül fenyeget.[71] Az Abh1. itt álcázóhálóként került hivatkozásra, vagyis a nyomozóhatóság úgy tett, mintha e határozatból vezette volna le a döntését, de érvelése tartalmilag ellentmond annak.[72] Ezekben az ügyekben a feljelentésekben tartalmazott megnyilvánulásokat egy esetben sem minősítették felhívásként.

Ide tartozik az előző pontban bemutatott, kizárólag a miniszterelnökre vonatkozó közlés, amelyben azt sérelmezték, hogy veszélyhelyzet idejére korlátlan hatalmat kapna.

Nem valósított meg felhívást az a személy sem, hanem csak a véleményét közölte, aki a közösségi portálon egy erdélyi magyarok választójogáról szóló bejegyzéshez az alábbi kommentet fűzte: „ezeket az undorító férgeket tudnám géppityuval szaporítani."[73]

Ugyancsak a felhívást vizsgálta a nyomozóhatóság abban az ügyben, amelyben az elkövető egy internetes portálon a „Flashmobot szerveznének a deviánsok [...] háza elé" című cikk alá egy homoszexuálisokra vonatkozó hozzászólást fűzött: „Mocskos buzi köcsögöket le kell vadászni a gecibe! Kiirtani mindet!"[74] A feljelentés elutasításának az indoka,

> „hogy a felhasználó személyes véleménye és annak megfogalmazása nem alkalmas a különböző társadalmi csoportok közötti békés egymás mellett élésének megzavarására. Továbbá a nevezett által írtak nem értelmezhetők felhívásként. Felhív, aki mást bűncselekmény elkövetésére rábírni törekszik. A felhasználó csak véleményét közölte és a puszta véleménynyilvánítás nem azonosítható a bűncselekmény elkövetésére való rábírni törekvés."

Szintén nem felhívás, hogy „ki kell mondanunk, hogy fehér, keresztény gyermekeket akarunk országainkba, és nem afrikaiakat, muszlimokat vagy cigányokat;"[75] a *Mein Kampf* kiadása és terjesztése; [76]„az összes rohadt muszlimot bebaszni a szemétégetőbe!!!";[77] valamint egy publicistának az Országgyűlés Igazságügyi bizottságának nyilvános ülésén megjelenő, transzparensekkel békésen tüntető civil aktivistákkal kapcsolatos közlése:

70 Ku.2017/2.
71 Ku.2017/4.
72 Szomora (2015) i. m. 70.
73 Ku.2018/4.
74 Ku.2020/9.
75 Ku.2016/2.
76 Ku.2017/5. A nyomozóhatóság vizsgálta a holokauszttagadás tényállását is (Btk. 333. §), ami azért nem valósult meg, mivel Adolf Hitler művének kiadása, terjesztése a 333. §-ban foglalt magatartások körét nem fedi le, a mű kiadása és terjesztése nem jelenti a holokauszt tagadását, kétségbe vonását, illetve jelentéktelen színben való feltüntetését, vagy nem igazolja ebbéli törekvését. Ezen magatartások megállapításához közvetlen és ráutalóbb, konkrétabb magatartás kifejtése szükséges, mint a hivatkozott mű kiadása vagy terjesztése.
77 Ku.2020/10.

> „ha még egyszer ezek vagy ilyenek megjelennek a parlament épületében, és ott megzavarják a munkát, akkor úgy kell őket kivágni, mint a macskát szarni. Ha a taknyukon és a vérükön kell őket kirángatni, akkor a taknyukon és a vérükön. Ha kell, akkor szanaszét kell verni a pofájukat. Ez ugyanis Magyarország parlamentje, nem pedig a nyilvános vécé, ahova ezek valók."[78]

Végezetül ide soroltam azt az egészen extrém esetet, amelyben a zsidó vallású szurkolók ellen az alábbi bejegyzést tették:

> „Na lassan indulhat a vonat..., Felszállás a megszokott józsefvárosi pályaudvaron..., A végállomás pedig megint Auschwitz.... Indiánszökdelésben menjetek és közben dúdolgassátok halkan..., Miénk az a f.... A dal szerzőjét és megrendelőjét a vagon aljára tegyétek!SSSS"[79]

A nyomozóhatóság a feljelentés elutasításának indokát abban látta, hogy az az uszítás szintjét el nem érő megvetéskinyilvánítás, gyalázkodó közlés, amely nem jár az erőszakcselekmény nyilvánvaló és közvetlen veszélyével, nem büntethető. Álláspontja szerint a bejegyzésben foglalt közlés elfogadhatatlan, mélyen elítélendő, gyalázkodó jellegű, amelyből azonban nem vonható le olyan következtetés, hogy a zsidó vallási csoporttal szembeni tevékenységre, erőszakra történő konkrét felhívásra, gyűlölet keltésére lenne alkalmas, várhatóan ahhoz vezetne.

4.2.2. A hármas követelmény vizsgálata

Ebbe a csoportba azokat a határozatokat soroltam, amelyek sok esetben utaltak az Abh1.-re (szintén álcázóhálóként), azonban nem a határozat *clear and present danger*t taglaló indokolására, hanem az elkövetési magatartást elemző részére.[80] Azért is tekintem álcázóhálónak, ugyanis az Abh1. indokolása ezen részének helyes értelmezéséből kitűnik, hogy a testület a tényállást (még) absztrakt veszélyeztető tényállásként kezelte. A nyomozóhatóságok pedig erre való hivatkozással indokolták, hogy ezzel a döntés nyomán a jogalkalmazói gyakorlat a hármas követelményt orientálja.

Nem teljesült a konjunktív követelményrendszer abban az ügyben, amelyben egy újságíró egy spanyol személynek a zsidó származásúakkal kapcsolatos álláspontját mutatta be az alábbi módon:

„a zsidók hivatásszerűen tetszelegnek üldözöttként történelmük kezdete óta, holott valójában vérszomjas üldözők, amikor csak tehetik; ez a spanyol leányzó égő szavakkal üzent hadat a szervezett zsidóságnak, napjaink egyetlen tényleges világhatalmának, hogy méltó legyen a zsidók kiüldözésével elévülhetetlen történelmi érdemeket szerző legendás névrokona, Kasztíliai Izabella emlékéhez."[81]

78 Ku.2017/2.

79 Ku.2015/1.

80 „A törvény eme kifejezés alatt »izgat« nem valamely kedvezőtlen és sértő véleménynek nyilvánítása, hanem olyan lázongó kifakadások értendők, amelyek alkalmasak arra, hogy az emberek nagyobb tömegében a szenvedélyeket oly magas fokra lobbantsák, amelyből gyűlölet keletkezvén, a társadalmi rend és béke megzavarására vezethet." 30/1992. (V. 26.) AB határozat, ABH 1992, 167, 177.

81 Ku.2021/1.

Szintén erre való hivatkozással utasították el a feljelentést, amelyben a „Felvonulás a cigánybűnözés ellen a Deák téren" című hírlevél tartalmát sérelmezték:

„Kedves Bajtársunk! Téged is hívunk [...] órára az Országos Roma Önkormányzat székháza elé, ahonnan együtt vonulunk a Deák térre, ahol megemlékezünk [a] pénteki lincselés áldozatairól. Rendszerszintű változásra van szükség, hogy ne fordulhassanak elő ilyen szörnyű tragédiák. Várunk téged is, mondju[n]k együtt nemet a cigánybűnözésre! Szibériába a gyilkosokkal!"[82]

Ugyancsak a Fővárosi Ítélőtáblának hármas követelményrendszerét vizsgálták akkor, amikor a „Mi tetszik a migránson?" című, közösségi portálon közzétett bejegyzéshez a következő hozzászólás érkezett: „SCANIA féknyom; én még hátramenetet is kapcsolnék! Biztos, ami biztos!"[83] A nyomozóhatóság álláspontja szerint

"csak olyan feszültséget gerjesztő magatartás tekinthető tényállásszerűnek, amely aktív, erőszakos cselekedetre, illetve ilyen magatartás vagy tevékenység kifejtésére hív fel, továbbá, ha a veszély nem csupán feltételezett, hanem a cselekedet magában hordozza az erőszakos sérelem konkrét és reális lehetőségét."

A konjunktív feltételeket jól szemlélteti a következő, bevándorlók ellen elhangzott gyűlöletbeszéd: „a sok papírok nélküli ingyenélőt kivinni a Duna partra sortűz és a többit a folyam megoldja!"[84] A nyomozóhatóság hosszas indokolásba nem bocsátkozott és implicite az inkriminált megnyilvánulást felhívásként értékelte, ugyanis arra hivatkozva utasította el a feljelentést, hogy „fent nevezett hozzászólás esetén azonban a veszély csupán feltételezett, a veszélyeztetett jogok nem konkrétak, és az erőszakos cselekedet közvetlenül nem fenyeget, így nem meríti ki a tényállást." Tehát a felhívást követő feltételrendszer nem teljesült.

Szintén nem felhívás egy videómegosztón közzétett videón elhangzott magyarellenes beszéd, amelyben olyan, a magyar nemzetet szidalmazó, becsmérlő kifejezések hangoztak el, mint például: „én kívánom az összes magyarnak, hogy nektek is lőjék le a családotok", „A ti családotokat kéne lelőni tetves geci magyarok! Titeket kéne lelőni...".[85]

Az elemzett határozatokból kitűnik, hogy a jogalkalmazási gyakorlat a közösség elleni uszítás tényállását dogmatikailag nem tudja értelmezni, és a határozatok indokolásában egymásnak ellentmondó érvelések figyelhetők meg. Erre jó példa az a határozat, amelyben a feljelentő azt sérelmezte, hogy egy párt által szervezett rendezvényen egy „Az igazság szabaddá tesz" feliratú molinót látott, amely véleménye szerint a Holokauszt emlékét sérti és alkalmas a közösség elleni uszításra. A nyomozóhatóság a feljelentést – helyesen – elutasította, azonban az indokolásban diszkrepancia figyelhető meg:

„a bűncselekmény megállapíthatósága szempontjából mind a gyűlölet kialakulása, mind a gerjesztett gyűlölet aktivizálódása irreleváns, megvalósulásához sem feltételezett, sem közvetlen veszély bekövetkezésére nincs szükség. Büntetőjogi eszközökkel kizárólag a védett csoport iránt érzett gyűlöletből fakadó kijelentés szankcionálható, amely az elhangzás, közzététel körülményei folytán az erőszak közvetlen jelen lévő, világos veszélyével és egyéni jogok sérelmével fenyeget. A rendezvényen használt »Az igazság szabaddá tesz« feliratú molinó nem

82 Ku.2020/6.
83 Ku.2016/3.
84 Ku.2015/3.
85 Ku.2018/2.

minősül a gyűlölet kialakítására alkalmas olyan kijelentésnek vagy konkrét tevékenységre felhívásnak, amely erőszak érzelmi előkészítésére alkalmas lenne."[86]

Az indokolás nem hagy kétséget afelől, hogy a gyakorlat nemcsak konkrét veszélyeztető tényállásként kezeli az egyébként absztrakt veszélyeztető tényállást, hanem a hármas konjunktív követelményrendszernek köszönhetően *sui generis* előkészületi bűncselekményt kreált a közösség elleni uszításból („a védett csoport iránt érzett gyűlöletből fakadó kijelentés szankcionálható, amely az elhangzás, közzététel körülményei folytán az erőszak közvetlen jelen lévő, világos veszélyével és egyéni jogok sérelmével fenyeget").[87] Ugyanezen indokolással utasították el azt a feljelentést, amelyben egy interneten megjelenő cikkben egy publicista a bevándorlókra olyan kijelentéseket tett, mint „a puszta létezésetek egyre és egyre elviselhetetlenebb és irritálóbb"; „Itt elég volt belőletek. Kitelt becsület, rohadékok! Ne várjátok meg, hogy ezt másképpen is elmagyarázza nektek valaki;"[88] valamint azt, amelyben a kormány által kihelyezett plakátok tartalmát sérelmezték: „Ha Magyarországra jössz, nem veheted el a magyarok munkáját!" és „Ha Magyarországra jössz, tiszteletben kell tartanod a magyarok kultúráját!"[89] Utóbbi indokolásban hatásvizsgálat is megjelenik, ugyanis a nyomozóhatóság álláspontja szerint a plakátkampány hatására nem alakult ki olyan veszélyhelyzet, amely a sérelem bekövetkezésének reális veszélyét jelentené. Az absztrakt veszélyeztető bűncselekményekre jellemző objektíve alkalmasságot *in concreto*, a külvilágban megjelenő hatások alapján vizsgálták: „semmilyen adat nem merült fel arra vonatkozóan, hogy a kihelyezett plakátok, illetve kiküldött kérdőív bármiféle indulatot szított volna a bevándorlók ellen azok körében, akik tartalmát megismerték."

4.2.3. Konkrét, reális veszélyhelyzet, de a felhívás mint elkövetési magatartás megkövetelése nélkül

A harmadik csoportba azokat a határozatokat soroltam, amelyeknek indokolásában valamilyen (konkrét, reális) veszélyre utalás jelenik meg (sokszor a veszélyeztetett jogok konkrétságával együtt), azonban a nyomozóhatóság a felhívás követelményére nem hivatkozik, azt nem vizsgálja. Ide soroltam két, eltérő védett csoport ellen irányuló hasonló közlés miatt érkezett feljelentést. Az egyik ügyben a „MEGÖLNI AZ ÖSSZES BUZIT?"[90], a másikban pedig „KIFELÉ AZ UKRÁN SZEMÉTTEL"[91] volt az inkriminált megnyilvánulás, amelyeket nyilvános területeken, jól látható helyeken helyeztek el. A nyomozóhatóságok elutasították a feljelentéseket, azonban mindkét határozatban közös, hogy felhívás nélküli veszélyhelyzetet követeltek meg. A homoszexuálisok ellen irányuló megnyilvánulást azért nem tekintették bűncselekménynek, mivel „a cselekmény tényállásszerűségéhez nem elegendő az absztrakt veszély kialakulása, kell, hogy a veszélyeztetett jogok konkrétak legyenek, és az erőszakos

86 Ku.2015/5. Arra a határozatban nem találtam információt, hogy a feljelentő szerint „Az igazság szabaddá tesz" felirat miért sérthette a Holokauszt emlékét.

87 Ez értelemszerűen elhatárolási problémákat okoz a közösség tagja elleni erőszak – egyébként generálisan büntetendő – előkészületétől. Ehhez lásd: Szomora (2013) i. m. 42.

88 Ku.2015/7.

89 Ku.2015/6.

90 Ku.2022/1.

91 Ku.2022/2.

cselekedet közvetlenül fenyegessen." Ez pedig – a nyomozóhatóság álláspontja szerint – eleve kizárt, tekintettel arra, hogy a közlés végén kérdőjel van, amelyből az következik, hogy konkrét veszélyhelyzet – e szólás hatására – nem alakulhat ki. Érdekes lett volna az az eset, ha a mondat végi kérdőjel nem lett volna ott, ugyanis a Pesti Központi Kerületi Bíróság egy „HALÁL A ROMÁKRA" hasonló feliratot közösség elleni uszításnak értékelt.[92]

Az ukrán nemzetiségekre tett megnyilvánulás tényállásszerűségét azért nem látták megállapíthatónak, mivel tekintettel kell lenni arra, hogy

> „a kialakult veszélyhelyzet konkrétsága a sérelem bekövetkeztének reális lehetőségét jelenti, így olyan helyzet fennállását, amikor a folyamat a sérelem bekövetkezése irányába ható továbbfejlődésének lehetőségével számolni kell. A trolimegállóban elhelyezett felirat nem alkalmas arra, hogy az emberek nagyobb tömegében a szenvedélyeket olyan mértékben feltüzelje, hogy a keletkező gyűlölet a társadalmi rend és béke megzavarását eredményezné vagy a támadott társadalmi csoport elleni erőszakos jellegű tevékenységben manifesztálódjon."

Ugyanezen indokolás található két, fekete bőrűekre tett cikk miatt érkezett feljelentést elutasító határozatban. Az egyik feljelentés szerint egy internetes oldalon megjelent „ÉLŐ-ben nézhető Philadelphia nálunk: N"""'k fosztogatnak, törnek zúznak az antifák" bejegyzés a következőket tartalmazza:

> „Az [internetes portál] szerkesztősége talált egy ÉLŐ videót, ezen lehet követni Philadelphia utcáit. Mi is élőben közvetítjük, harc, lángoló autók, a mocskos n"""'r banánzabáló f"""'e s"""'k fosztogatásait és a terrorista antifák harcait. Az ÉLŐ közvetítés tehát valós idejű, és addig közvetítjük mi is, ha kell egész nap, ameddig a tudósító az utcán tartózkodik."[93]

A másik feljelentés szintén egy internetes portálon megjelent bejegyzést sérelmezett:

> „Ez lenne a jövő? Ki...tt n...k mocskos bakancsát kell csókolgatni és önfeledten mosolyogni hozz[á]? Örülni? Mert másképp kinyírnak vagy összevernek? Akkor inkább irány Szibéria! Istenem... hát mivé lett ez a világ..."[94]

A nyomozóhatóság mindkét esetben utalt a konkrét sérelem reális lehetőségére, majd a cikkben és a bejegyzésben foglaltakat értékítéletnek (véleménynek) minősítette, amelyeknek álláspontja szerint nincsenek olyan elemei, amelyek a szenvedélyeket akár erőszakos formában felkeltenék.[95]

A következő ügyben arra hivatkozással utasította el a nyomozóhatóság a feljelentést, hogy „a bejegyzés szövege alapján a lakosság egyes csoportjainak konkrét jogai nem kerültek veszélybe, és nem fenyegetett erőszakos cselekedettel. A szöveg nem gerjeszt ellenséges

92 Pesti Központi Kerületi Bíróság Fk.10.202/2015. számú ítélete. Kúria joggyakorlat-elemző csoportjának 2014/El.II.JGY.1/2. véleménye az egyes alapjogokat sértő bűncselekmény ítélkezési gyakorlatának elemzéséről. (Alapjogi példatár, 22. eset).

93 Ku.2020/8.

94 Ku.2022/11.

95 Ugyanezzel az indokolással utasították el azt a feljelentést, amely „a fehér keresztények rémisztő képződmények" közlést sérelmezte. Ku.2020/1.

indulatokat, és ilyen célzat nem is olvasható ki belőle."[96] A feljelentő szerint az autistákkal szemben hangzott el egy internetes fórumon gyűlöletbeszéd:

> „nem értem a problémádat, ha problémás és kényelmetlen, netán beteg a kedves rokon, rangon aluli kapcsolatot akar kiépíteni, akkor csak ki kell lövetni és kész. Ment ez a harmadik birodalomban is. Gond letudva. Mégis mit gondoltál, milyen megoldást tud ajánlani a csoport tagsága? Az autizmussal lehet élni. Lehet önálló életvitelt folytatni. A vagyonelemeket be lehet úgy biztosítani, hogy ne tudják tőle elcsalni és így tovább. Ha nagyon instabillá válik, akkor vannak nagyon jó terápiák, gyakorlatok, amivel a mentális és egyéb képességei szintén tarthatók és fejleszthetők. Attól, hogy ő másképp működik, mint elvárnád, még vannak jogai."

A szöveg teljes kontextusát vizsgálva egyet lehet érteni a feljelentés elutasításával, ugyanis összességében a védett csoport alapvető jogait hangsúlyozza. Az indokolásban a konkrét jogok veszélybe kerülése és erőszakos cselekedet közvetlen fenyegetése mellett a célzat is megjelenik, ami azért problémás, mert a bűncselekmény nem célzatos (ebben a gyakorlat egységesnek mondható).

4.2.4. A két vádemelés

Külön csoportba soroltam azt a két ügyet, amelyekben vádemelés történt. Az első esetben büntetőjogi felelősség megállapításra is sor került.[97]

A vádirati tényállás szerint [a párt neve] és egyéb társadalmi szervezetek „Rendet Borsod Megyében" címmel az illetékes hatóságnál bejelentett gyűlést kívántak tartani 2020 februárjában [a település neve]-n a megyei kormányhivatal előtt, majd azt követően [a település neve]-n a polgármesteri hivatalnál. Az esemény kapcsán, nagy nyilvánosság előtt egy közösségi oldalon [a vádlott neve] tettek közzé videó felvételt. A felvételen szereplő személy a közleményben a többek között kijelenti, hogy a felvonulás „el lesz marasztalva", „meg fog dőlni", amit azzal indokol, hogy annak ellenzői összefogtak, ezért a gyűlés szervezői megijedtek. A gyűlés megakadályozására vonatkozó üzenetét azzal a fenyegetéssel nyomatékosította, hogy „ha mégis odamennek, onnan ki nem jönnek", majd hozzátette, „a cigányok harcban akarnak meghalni, nem elnyomottként". Egyben hadba hívta „az összes borsodit, hogy haljanak meg a gyerekeikért a mocskos senkiházi undorító rossz eszmével gondolkodó emberek ellen", továbbá fenyegetőzött, hogy „ha baj van, ki kell szaggatni a szívüket a kutyáknak", és olyan felszólítást tesz közzé, miszerint „tiporjuk el őket, álljunk fel ellenük kőkeményen és harcoljunk" (a továbbiakban: 1. tényállási pont).

A [párt neve] elnökének, egyben a rendezvény vezérszónokának azt üzente, hogy „egy az egyben felállok veled, és az agyadat be fogom ütni, a koponyádat. Addig fogom beütni, míg a másik oldalon ki nem folyik a füleden – baszd meg – az agyad" (a továbbiakban: 2. tényállási pont).

96 Ku.2022/4.
97 Ku.2021/2.

Mindezek alapján az ügyészség közösség elleni uszítás (1. tényállási pont), valamint zaklatás [Btk. 222. §. (2) bekezdés *a)* pont] (2. tényállási pont) miatt emelt vádat. A bíróság a vádlott büntetőjogi felelősségét mindkét bűncselekményben megállapította és 10 hónap szabadságvesztést szabott ki, amelyet 2 évre próbaidőre felfüggesztett. Tekintettel arra, hogy büntetővégzés meghozatalával zárult az ügy,[98] részletes indokolás nem található, kizárólag a vádirati tényállásból lehet következtetni arra, hogy miért emeltek vádat e cselekménnyel szemben.

Az ügyészség az 1. tényállási pontban megfogalmazott közlést erőszakra, gyűlöletre felhívásként (mindkét fordulatot tartalmazta a vádirat) értékelte. Ehhez szükséges megjegyezni, hogy amennyiben a „ha baj van, ki kell szaggatni a szívüket a kutyáknak", valamint a „tiporjuk el őket, álljunk fel ellenük kőkeményen és harcoljunk" megnyilvánulást az ügyészség felhívásnak tekintette, akkor a korábban bemutatott pl. „az összes rohadt muszlimot bebaszni a szemétégetőbe!!!"; „Ha kell, akkor szanaszét kell verni a pofájukat"; „A dal szerzőjét és megrendelőjét a vagon aljára tegyétek!" közléseket is felhívásként kellett volna minősíteni.

A gyakorlat további feltételként tűzi a veszélyeztetett jogok konkrétságát és azt, hogy az erőszakos cselekedet közvetlenül fenyegessen. E követelmények teljesülésére abból tudok következtetni, hogy az 1. tényállási pontban foglalt közlésben a vádlott térben és időben konkrétan behatárolható helyszínt jelölt meg, amellyel beazonosíthatóvá vált az ezen részt vevő személyek köre (ezzel összefüggésben a veszélyeztetett jogok), ami a védett csoporti minőséget is megalapozta. Valamint nem hagyható figyelmen kívül a 2. tényállási pontban feltüntetett, kétségkívül zaklatásnak minősülő közlés, amely szintén egyértelműen beazonosítható, a rendezvény fő szervezőjére vonatkozó fenyegetést tartalmazott. Álláspontom szerint ez alapozta meg, hogy a vádhatóság a másik két feltételt is megvalósultnak látta. Megjegyzem, végül a gyűlés atrocitásmentesen zajlott le.

A második ügyben a videómegosztó portálra feltöltött „Sóherhimnusz" című szerzemény miatt emelt vádat az ügyészség. A vádiratban a dal teljes szövegét feltüntették, azonban a vádhatóság kiemelte azokat a részeket, amelyek álláspontja szerint kimerítették a közösség elleni uszítás tényállását:

> „Ébredj, magyar, rázd le a láncot, tolvaj kutyák lopják országod! Elég volt ebből, lángoljon minden, bibliai pusztulás lesz, kegyelem nincsen! (refrén)
> Egyre több indokkal szolgáltak ahhoz, hogy sortűz elé basszunk a falhoz! Azt a sok szarházit, aki ezt tette, egységben az erő, öcsém, minden rendben! Ez az ország a miénk, a magyaroké baszdki, minden büdös köcsögöt haza fogunk baszni!"

A bíróság bűncselekmény hiánya miatt megszüntette az eljárást.[99] Az elsőfokú bíróság elsőként a védett csoporti minőséget vizsgálta (lásd 4.1.), majd a nagy nyilvánosság előtti elkövetést, amely tekintettel arra, hogy a szerzeményt egy videómegosztón osztották meg, megvalósult. Ezt követően az alkotmánybírósági, majd a rendes bírói gyakorlatot tekintette át.

98 A büntetővégzés meghozatalára irányuló eljárást a Be. külön eljárásként szabályozza, amelynek célja az eljárás egyszerűsítése, gyorsítása, hiszen ebben az esetben az eljáró bíróság kizárólag az iratok alapján dönt, bizonyítást nem folytat le. A büntetővégzés ellen fellebbezésnek nincs helye, azonban a kézbesítéstől számított 8 napon belül kérhető a tárgyalás megtartása. Vö. Be. C. fejezet.

99 Ku.2014/4.

Az alkotmánybírósági gyakorlat bemutatásánál kizárólag az Abh1.-ben foglalt megállapításokra hivatkozott. Itt utalt arra, hogy

> „a hivatkozott tényállást egyrészről a nyilvánvaló és közvetlen veszély – *clear and present danger* – formulájának, illetve a támadott értékek egyediségének követelményének szempontjából vizsgálta, amely szerint csak bizonyos mérték fölött, tehát a nyilvánvaló és közvetlen veszély esetén igazolható alkotmányosan a szabad véleménynyilvánításhoz való jog korlátozása, másrészről pedig a véleménynyilvánítás szabadsága egyebekben is csak nagyon szűk körben szorítható korlátok közé."

Ezt követően a 3. pontban bemutatott, közzétett eseti döntésekre hivatkozott. A gyakorlat áttekintését követően megállapította, hogy

> „[m]indezek alapján a gyűlöletre uszítás akként értelmezhető, mint az erőszak érzelmi előkészítése, gyakorlatilag olyan gyűlölet felkeltésére irányul, ami aktív tevékenységbe megy át, és magában hordozza az erőszakos jellegű konkrét sérelem bekövetkezésének reális lehetőségét."

A vád tárgyává tett megnyilvánulás vizsgálatánál utalt a bíróság arra, hogy kizárólag a vádiratban kiemelt szövegrészeket vizsgálja, ugyanis a szerzemény többi része még áttételesen sem tartalmaz aktív cselekvésre buzdító mondatot, azok csak vélemény formájában közzétett ténymegállapítások. Utalt arra is, hogy nem lehet figyelmen kívül hagyni a szerzemény műfaji (rap) sajátosságait, ugyanis a szöveget azzal összhangban kell értelmezni, hiszen

> „az mindenképpen figyelembe veendő, hogy egyes általánosan elfogadott, sőt magasan jegyzett költők vers[e]i is tartalmaznak ehhez hasonló metaforikus sorokat, elegendő hivatkozni e helyütt Ady Endre *Nekünk Mohács kell* vagy József Attila *Favágó* című műveire, amelyek nyilvánvalóan nem vonnának maguk után ma sem büntetőeljárást, holott szövegszerű értelmezésük folytán akár ki is meríthetnék több Büntető Törvénykönyvbe ütköző tényállást."

Erre való tekintettel vizsgálta elsőként a refrént, amely álláspontja szerint felszólítást nem tartalmaz, az csupán metaforikus jelentésű. A refrénen kívüli, kiemelt szövegrésznél a bíróság a hármas követelményi rendszerre utalt, azonban a döntés *ratio decidendi*je – álláspontom szerint – ettől eltérő:

> „nyilvánvalóan különbséget kell ugyanis tenni aközött, hogy egy bizonyos tartalom a világhálón elérhető és szabadon meghallgatható bárki számára úgy, hogy a tartalomfogyasztás saját döntés kérdése, illetőleg aközött, hogy a dal nagyobb nyilvánosság előtt, inkább egyfajta szónoki beszéd, vagy felhívás hangzik el akként, hogy az általa felszított gyűlölet nyilvánvalóan szélsőséges aktivitásba fordulhat. A bíróság megítélése szerint jelen esetben ilyenről szó sem lehet. A vádlott, vagyis a szerző és megosztó gondolatai ugyan értékelhetőek sértőnek, azok meghökkentőek és alkalmasak aggodalom keltésére, de figyelemmel a szerzemény műfajára és megjelenési formájára is semmi esetre sem alkalmasak arra, hogy magában hordozza erőszakos jellegű konkrét sérelem bekövetkezésének reális lehetőségét.

> Nyilvánvaló és közvetlen veszélyt nem jelent a szerzemény tehát, így a véleménynyilvánításhoz való jog büntetőjogi eszközökkel történő korlátozása semmiképpen nem igazolható."

A bíróság tehát a nyilvánvaló és közvetlen veszély tesztjét alkalmazta és konkrét veszélyeztető tényállásként kezelte a közösség elleni uszítást, holott még az indokolásában is megjelenik, hogy a vádlott gondolatai nem alkalmasak aggodalom keltésére. Amennyiben a bíróság az absztrakt veszélyeztető jelleget elfogadta volna, amely a bűncselekmény dogmatikai karakteréből következik, úgy lehet, hogy eltérő döntés született volna.

A *ratio decidendi*ből az is következhet, hogy egy videómegosztóra feltöltött szerzemény vagy egy internetes fórumon közzétett bejegyzés, amely egy védett csoport ellen irányuló 'gyűlöletbeszédet' tartalmaz, sosem lenne büntethető, mivel az interneten bárki számára hozzáférhető megnyilvánulások fogyasztása saját döntés kérdése, amely eleve kizárja a nyilvánvaló és közvetlen vagy bármilyen reális, konkrét veszély megállapíthatóságát.

Az ügyészség a hármas követelményrendszerre tekintettel fellebbezést nyújtott be, azonban a másodfokon eljáró bíróság az elsőfokú végzést helybenhagyta.[100] A másodfokú határozat is ugyanarra az álláspontra helyezkedett, mint az elsőfokú bíróság. Egyrészt a műfaj sajátosságaira hivatkozva állapította meg, hogy

„a műfaj híveiben [...] a dalban használt, a műfajhoz képest nem kirívó kifejezések nem gerjesztenek olyan indulatokat, melyek okán erőszakos jellegű konkrét sérelem bekövetkezésének reális lehetőségével számolni kellene, míg az ilyen művészethez nem vonzódó személyre nyilván semmilyen hatással nem lehet."

Végül a másodfokú bírósági döntés is az elsőfokú döntés – vitatható – *ratio decidendi*jét erősíti meg:

> „A videómegosztón közzétett, konkrét személyt, csoportot meg nem szólító, a műfajba illő kifejezéseket használó dal esetében a közzétevőnek nem kell azzal számolnia, hogy az ellenséges indulatok kitörhetnek."

5. A jelenlegi gyakorlat értékelése és út egy lehetséges új mérce felé

A fentebb bemutatott esetek alátámasztják a sokszor ismételt kijelentést: a jelenlegi gyakorlat tarthatatlan. Ehhez az alábbiak megjegyzése szükséges:

a) A jogalkalmazói gyakorlat sok esetben álcázóhálóként tekint az Abh1.-ben foglaltakra, ugyanis vagy a *clear and present danger* mércéjét kiragadva próbálják igazolni a jelenlegi gyakorlat által felállított eltérő követelményrendszert, vagy pedig az alaphatározat elkövetési magatartást – történeti kontextusban – elemző részével. Ez azért vitatható, mert az Abh1. helyes értelmezése alapján a bűncselekmény absztrakt veszélyeztető tényállás.
b) A gyakorlat továbbra is konkrét veszélyeztető tényállásként kezeli a bűncselekményt, amely dogmatikailag tarthatatlan. A hármas követelmény felállításával és érvényesítésével a bűncselekményt a gyakorlat tulajdonképpen *sui generis* előkészületi cselekményként

100 Ku.2014/4-II.

értelmezi, amely lehetetlenné teszi a közösség tagja elleni erőszak előkészületétől történő elhatárolást. Továbbá a nyomozóhatóságok sok esetben értékítéletnek (véleménynek) minősítették a közlést, ami eleve kizárja a felhívás megvalósulását, mint például „Mocskos buzi köcsögöket le kell vadászni a gecibe! Kiirtani mindet!" Holott álláspontom szerint értékítélet is lehet objektíve a köznyugalom megzavarására alkalmas, mint az előbb hivatkozott esetben.

c) A fentebb bemutatott ügyek majdnem mindegyikében a feljelentett közlés internetes fórumon vagy videómegosztón jelent meg. Az elemzésből az a kép rajzolódik ki, hogy egy ilyen megnyilvánulás eleve nem egyeztethető össze a gyakorlat által felállított konkrét, reális (nyilvánvaló és közvetlen) veszéllyel, ennek megállapíthatósága az esetek túlnyomó részében eleve kizárt. Ehhez az lenne szükséges, hogy a gyakorlat által megkövetelt felhívás konkrétan beazonosítható csoportot szólítson meg, egyértelműen beazonosítható védett csoporttal szemben, továbbá az „elkövetés helyének" térben és időben lehatároltnak kellene lennie. Ezt támasztja alá az az ügy, amely végül büntetőjogi felelősség megállapításával végződött.

d) A védett csoport alatt tulajdonképpen bármilyen ismérv alapján létrejövő személyösszesség érthető, amely akár spontán, egyszeri alkalmat is jelenthet, mint például egy megemlékezésen összegyűlt tömeg esetén.

e) Bár a közösség elleni uszítás elkövetési magatartása az erőszakra uszítással bővült,[101] amellyel egyértelművé vált, hogy a gyűlöletre uszítás és az erőszakra uszítás nem azonos fogalmak, a 2016-ot követő jogalkalmazási gyakorlat továbbra sem tesz különbséget e két alakzat között, ugyanis erre történő utalás, vizsgálat egy határozatban sem volt. Azzal, hogy a jogalkalmazói gyakorlat a Btk.-módosításról nem vesz tudomást, és a már hatályon kívül helyezett Btk.-szöveg és az arra vonatkozó, szintén hatályon kívül helyezett alkotmánybírósági gyakorlat alapján indokol, egyértelmű törvénysértést valósít meg.

Mindezek azért is sajnálatra méltók, mert nemcsak az elkövetési magatartása bővült a bűncselekménynek, hanem 2013. április 1. hatállyal az Alaptörvény véleményszabadságot deklaráló rendelkezése is kiegészült és bekerült *explicit* korlátként a közösségek méltósága.[102] A közösségek méltóságának jogtárgyként történő elfogadhatóságával egy korábbi írásomban már foglalkoztam.[103] A konkrét mérce felállításánál azonban sokkal inkább annak van jelentősége, hogy az Alaptörvény IX. cikk (5) bekezdését ténylegesen büntetőjogi korlátként fogjuk fel, úgy, mint a rágalmazás és becsületsértés tényállásainál az emberi méltóságot korlátként felállító (4) bekezdést. Ennek alkotmányos alapjait a taláros testület a nemzetiszocialista és kommunista rendszer bűneinek nyilvános tagadása tényállás (Btk. 333. §) alkotmányos megítélését vizsgáló határozatában[104] fektette le, amikor a határozatban hivatkozik az Alaptörvény IX. cikk (4) és (5) bekezdésére mint a korlátozás elfogadhatóságának indokára, ami

101 2016. évi CIII. törvény 55. § (3). Hatályos: 2016. 10. 28-tól.

102 Alaptörvény IX. cikk (5): „A véleménynyilvánítás szabadságának a gyakorlása nem irányulhat a magyar nemzet, a nemzeti, etnikai, faji vagy vallási közösségek méltóságának a megsértésére. Az ilyen közösséghez tartozó személyek – törvényben meghatározottak szerint – jogosultak a közösséget sértő véleménynyilvánítás ellen, emberi méltóságuk megsértése miatt igényeiket bíróság előtt érvényesíteni."

103 Botos Mihály Bálint: A közösség elleni uszítás jogi tárgyáról. *Iustum Aequum Salutare,* 2022/4. 27–41.

104 16/2013. (VI. 20.) AB határozat, ABH 2013, 688–706.

„nem hagy kétséget afelől, hogy a nevesített korlátozási okok a büntetőjogi szankcionálás alkotmányos alapját is jelenthetik."[105]

Az Alkotmánybíróság 2021-ben értelmezte elsőként a kollektív méltóságot deklaráló rendelkezést, amelyben, bár elmulasztotta az (5) bekezdés alkotmányos tartalmát kibontani, egy lehetséges mérce elvi alapjait fektette le, ugyanis analógia útján a (4) bekezdés alapján kialakított gyakorlatát tekintette kiindulópontnak. Ha ezt elfogadjuk, akkor a rágalmazás és becsületsértés alkotmányos megítélésével foglalkozó alaphatározatban felállított alkotmányos követelményeket is – analógia útján – vizsgálat alá vonhatjuk. E szerint a jogalkalmazónak elsőként azt kell vizsgálnia, hogy a szólás közéleti vitában kifejtett álláspontot tükröz-e, ezt követően, hogy az inkriminált kifejezés tényállítás vagy értékítélet-e, végül, hogy a szólás az érintett személy emberi méltóságának korlátozhatatlan aspektusát sértette-e.[106] Álláspontom szerint a közéleti vitához tartozás vizsgálata is szerepet játszhat a közösség elleni uszításnál, amely vizsgálat – a véleményszabadság kitüntetett helyéből kifolyólag – indokolt lehet (pl. politikai, jogalkotási vitákban, helyi közügyek kapcsán). A tényállítás/értékítélet elhatárolásának nincs akkora jelentősége, mint az egyéni méltóságot védő rágalmazás/becsületsértés esetén, ahol a konkrét mérce kiválasztásánál játszik döntő szerepet.

Sokkal inkább a teszt utolsó vizsgálati pontját lehet analógia útján felhasználni, függetlenül attól, hogy elfogadnánk-e a közösség méltóságának létezését. Ehhez azonban elsőként el kell fogadni, hogy a gyűlöletre és az erőszakra uszítás nem azonos fogalmak. A gyűlöletre uszítás elkövetési magatartásánál a mércét a következőként határozhatjuk meg. Az Alkotmánybíróság a gyűlöletet az egyik legszélsőségesebb, negatív, nagyfokú ellenséges indulatként határozta meg, azonban a gyakorlat hozzátette, hogy az uszítás nem egyszerűen gyűlölet, hanem olyan gyűlölet felkeltésére irányul, amely aktív tevékenységbe megy át. Ennek helyes értelmezése az lenne, hogy a gyűlöletre uszítás olyan negatív, nagyfokú ellenséges indulat, amely objektíve alkalmas a köznyugalom megzavarására. Az objektíve alkalmassághoz a korlátozhatatlan aspektus követelményét – analógia útján – felhasználva juthatunk. Az egyéni méltóságnál ez azt jelenti, hogy az embert emberként kezeljük (pl. ne állatként állítsuk be, vagy tárgyiasítsuk). Álláspontom szerint a közösség elleni uszításnál az a döntő, hogy az adott védett csoport lényegi meghatározójára vonatkozik-e a gyűlölködő megnyilvánulás. Amennyiben a csoport létezésének megszűnésére, kiirtására, jogtól való megfosztására vagy alsóbbrendűségére vonatkozik a közlés, úgy mindenféle felhívás, nyilvánvaló és közvetlen vagy reális/konkrét veszély nélkül a gyűlöletre uszítás megállapítható, hiszen ez adja az adott csoport lényegi aspektusát. Az erőszakos cselekedet konkrét veszélyére pedig az erőszakra uszítás fordulat továbbra is alkalmazható.

Meglátásom szerint a helyes az lenne, ha a jogalkalmazás bevonná az Alaptörvény IX. (5) bekezdést az értelmezésbe, ugyanis ez elindíthatna egy olyan folyamatot, amelynek végén az Alkotmánybíróság újra alkotmányos revízió alá vonhatná a közösség elleni uszítás tényállását, amire – figyelemmel a jelenlegi jogalkalmazásra – nagy szükség van.

105 Szomora (2015) i. m. 41.

106 13/2014. (IV. 18.) AB határozat, ABH 2014, 588.

Botok a közösségi médiában

Kovács Andrea

1. Bevezetés

A közösségi médiát ma már nemcsak emberi felhasználók milliói használják, hanem részben vagy egészen automatizált fiókok is. Legtöbbször negatív kontextusban kerülnek a média – és a szabályozó testületek – figyelmének középpontjába. Ilyen kontextus például a 2016-os amerikai elnökválasztási kampányban való részvételük, vagy a Covid19-járvány idején terjesztett hamis információk. A politikai kampányokban vagy a dezinformáció terjesztésében játszott szerepükre reagálva több szabályozási reakció is született, amelyek leginkább ezekre a jelenségekre reagálnak. Azonban a botok jó célokat is szolgálhatnak. Dezinformáció helyett terjeszthetnek közérdekű információkat, amelyek akár életet menthetnek.

Jelen tanulmány célja áttekinteni, hogy védi-e a szólásszabadság a botfiókok tevékenységét, továbbá röviden bemutatni a botokat érintő kaliforniai szabályozást és annak viszonylatában a hatályba nem lépett föderális szabályozást is. Ezt követően a Dezinformáció visszaszorítását célzó uniós gyakorlati kódex, a Digitális Szolgáltatásokról szóló uniós rendelet botokat említő szakaszait veszi sorra, kiegészítve a három szolgáltató – a Meta (Facebook és Instagram), az X/Twitter és a TikTok – által 2023 januárjában és 2023 júliusában benyújtott riportokkal, valamint rövid leírást ad ezen szolgáltatók botokat érintő szabályzatairól. Végezetül pedig kísérletet tesz a szabályok szintetizálására, aminek középpontjába a politikai botok tevékenységét helyezi. A tanulmány nem tér ki a kifejezetten üzleti felhasználók számára ajánlott automatizáció lehetőségére, ahogy a reklámokhoz kapcsolódó automatizált eszközök használatára sem.

2. Védi-e a szólásszabadság a botfiókok tevékenységét?

Ahhoz, hogy a botfiókok tevékenységét megfelelően értékelni tudjuk, meg kell vizsgálnunk annak a véleménynyilvánítás szabadságához fűződő aspektusait. A kérdés annyiban nem újkeletű, hogy a robotjogok a technológia fejlődésével átléptek a *science fiction* világából a realitás talajára. A mesterséges intelligencia elképesztő mértékű fejlesztése pedig nyomást helyez a jogalkotókra, hogy megoldást találjanak az ebből adódó jogi problémákra. Ugyanakkor a közösségimédia-botok esetében nemcsak mesterséges intelligencia vezérelheti a fiókot, hanem lényegesen egyszerűbb programkódok is.

A kérdés tehát komplex vizsgálatot igényel, amelyhez Tim Wu 2013-ban felállított tesztjének elemeit használom fel. Fontos kiemelni, hogy a teszt alapvetően az Amerikai Legfelső Bíróság joggyakorlata alapján született, és abban segít eligazodni, hogy egy adott – jelen esetben hipotetikus[1] – ügy esetében releváns-e az Első Alkotmánykiegészítés alkalmazása.[2]

1 Wu tanulmánya alapvetően azt vizsgálja, hogy az algoritmusok kimenetét – különös tekintettel a keresőmotorok kimenetére – védi-e az Első Alkotmánykiegészítés. Tim Wu: Machine Speech. *University of Pennsylvania Law Review,* vol. 161., no. 6. (2013).

2 Uo. 1500.

Bár a teszt az Egyesült Államok Legfelső Bíróságának esetjoga alapján készült, az egyes elemei az európai – és ezáltal a magyar – jog számára is relevánsak lehetnek. Emellett nem hagyhatjuk figyelmen kívül azt a tényt, hogy a vizsgált platformok közül a Meta és a Twitter is amerikai székhelyű, így működésükben az Egyesült Államok jogrendszere meghatározó, azaz egy-egy jogszabály vagy döntés közvetlenül kihathat a magyar felhasználókra is.

A teszt négy tényezőt vesz figyelembe: 1) személyiség (*personhood*), 2) beszéd (*speech*), 3) kormányzati motiváció a szabályozásra, 4) korlátozás a szólásszabadságra vonatkozik-e (*abridgement*).[3]

2.1. Személyiség

Az Emberi Jogok Egyetemes Nyilatkozatának 19. cikke tartalmazza a véleménynyilvánítás szabadságát az alábbi megfogalmazással: „Minden *személynek* joga van a vélemény és a kifejezés szabadságához […]". Bár az egyes emberi jogi egyezmények már *mindenkinek*[4] vagy *minden egyénnek*[5] ismerik el a véleménynyilvánításhoz való jogát, jelen tanulmány a személyiség vizsgálatát helyezi előtérbe és úgy tekinti, hogy a személyiség megléte esetén a közösségimédia-botok is a *mindenki* és *minden egyén* fogalma alá értendők. Magyarország Alaptörvénye IX. cikk (1) bekezdése is a *mindenki* kifejezést tartalmazza.

Mind az Egyesült Államokban, mind Európában elfogadott, hogy nemcsak természetes személyek rendelkeznek szólásszabadsággal, hanem jogi személyek is.[6] Wu a szólásszabadságot ahhoz köti, hogy ezek a személyek képesek a koncepcionális gondolkodásra, és ki is tudják fejezni a mérlegelésük eredményeként kialakult véleményüket.[7] Bár a teszt megalkotásakor, 2013-ban még igaz lehetett, hogy erre a gépek nem képesek,[8] egy évtizeddel később már rendelkezésre áll olyan technológia, amely a koncepcionális gondolkodás látszatát kelti.[9] Éppen ezért Wu nyomán két irányban érdemes vizsgálatot folytatni: magának a botnak van-e személyisége és ezáltal szólásszabadsága, vagy egyszerűen csak a botot használó/programozó emberek szólásszabadságáról van-e szó? A botok esetében a személyiség kérdését leginkább a mesterséges intelligencia kapcsán vizsgálja a szakirodalom. A kérdésben két álláspont látszik kirajzolódni: egyfelől a mesterséges intelligencia rendelkezhet önálló (korlátolt) jogi személyiséggel és ezáltal lehet közvetlen jogok és kötelezettségek alanya, lehet szólásszabadsága;[10]

3 Uo.

4 Emberi Jogok Európai Egyezménye 10. cikk Emberi Jogok Amerikai Egyezménye 13. cikk.

5 Emberek és Népek Jogainak Afrikai Chartája 9. cikk.

6 Wu i. m. 1503.; Matthew Hines: I smell a Bot: California's S.B. 1001, Free Speech, and the Future of Bot Regulation. *Houston Law Review,* vol. 57., no. 2. (2019) 417.

7 Ezzel kapcsolatban lásd: Autronic AG v. Switzerland, no. 12726/87 1990. május 22-i ítélet, 47. bek.

8 Wu i. m. 1503.

9 A köznyelvben használt mesterséges intelligencia leginkább a statisztikai alapú intelligenciát jelenti, ugyanakkor létezik egy másik típusú, koncepcionális mesterséges intelligencia is. Ződi Zsolt: A robottanácsadók jogi problémái: hogyan szabályozzuk a robotokat? *Állam- és Jogtudomány*, 2020/4. 123.

10 Bert-Jaap Koops – Mireille Hildebrandt – David-Olivier Jaquet-Chiffelle: Bridging the Accountability Gap: Rights for New Entities in the Information Society? *Minnesota Journal of Law, Science & Technology,* vol. 11., no. 2. (2010) 555–559.

másfelől a mesterséges intelligencia 'csupán' jogtárgy, és a használója/programozója jogainak érvényesülését és kötelezettségeinek teljesítését[11] hivatott elősegíteni.[12]

A mesterséges intelligencia személyként való meghatározásának egyik leggyakrabban említett feltétele az önálló, alkotójától független döntéshozatali képesség, mérlegelési képesség, a kifejezés megválasztásának képessége, illetve a már említett koncepcionális gondolkodásra való képesség.[13] Skálán szemléltetve ez a pont akkor következik be, amikor a mesterséges intelligencia eléri az autonómiának azon fokát, ahol már nem pusztán automatizmusról, hanem olyan szándékos cselekvésről beszélhetünk, amely az öntudaton alapszik.[14] A szakirodalom ismer ugyanakkor olyan álláspontot is, amely elegendőnek tartja az olyan társadalmilag komplex funkcionalitást, amely már az emberi autonómia területét érinti.[15]

Ugyanakkor a szólásszabadság szempontjából érdemes megjegyezni, hogy e szabadságnak az egyik központi eleme a politikai beszéd. Fel kell tenni a kérdést, hogy még ha el is ismerjük a mesterséges intelligencia szólásszabadságát, vajon mennyiben van értelme politikai kérdésben nyilatkoznia, ha nem rendelkezik választójoggal,[16] a politikai témák közül pedig több *per definitionem* nem is érintheti? Például értelmezhető-e a mesterséges intelligencia szólásszabadsága az abortuszkérdésben?

Bár a botok fontos szerepet játszhatnak az információk megalkotásában, formába öntésében és terjesztésében, ezeket a jelen tanulmány mégsem közvetlenül a bot jogának tekinti.[17] Ennek egyik oka, hogy a feldolgozott amerikai szakirodalom a hallgatóság jogaira koncentrál, a szólásszabadság kérdéskörét ebből az aspektusból közelíti meg. Ez a megközelítés a magyar jogtól sem áll távol.[18] Másrészt a szólásszabadság egyik központi elemének tekinthető az önkifejezés és az egyéni autonómia,[19] amelyek megléte a botok esetében erősen kétséges, ugyanakkor fontos szerepük lehet az információk terjesztésében.[20]

11 Federico Gustavo Pizzetti: Embryos, Organoids and Robots: „legal subjects"? *BioLaw Journal,* 2021/1. 348–349.; Hines i. m. 408.

12 Jelen tanulmánynak nem tárgya a mesterséges intelligencia jogi személyként való elismerésének vizsgálata, így arról mindössze a közösségimédia-botok politikai megnyilvánulásának szempontjából tesz csak említést. A mesterséges intelligencia személyiségéről érték, felelősség és kereskedelem kontextusában bővebben lásd: Visa A. J. Kurki: *The Theory of Legal Personhood.* Oxford, Oxford University Press, 2019. 175–190.

13 Wu i. m. 1503. Toni Massaro – Helen Norton: Siri-ously? Free speech rights and artificial intelligence. *Northwestern University Law Review,* vol. 110., no. 5. (2016) 1183.

14 Koops–Hildebrandt–Jaquet-Chiffelle i. m. 553.; Tóth András – Klein Tamás: Technológia és Robotjog. In: Tóth András (szerk.) *Az infokommunikációs és technológia jog alapjai*. NKE, Online kiadás, 2018. 39.

15 Yurii Vadymovych Sheliazhenko: Artificial Personal Autonomy and Concept of Robot Rights. *European Journal of Law and Political Sciences,* 2017/1. 19.

16 A mesterséges intelligencia állampolgárságával és választójogával kapcsolatban ld. pl.: Clark Summers: Can „Samantha" Vote? – On the question of Singularity, Citizenship and the Franchise. Newport (2016. november 3–5.): *Humanities and Technology Association Conference.* Online: https://www.academia.edu/29673069

17 vö. Sheliazhenko i. m. 20., amelyben a nyolcadik jognak tekinti a kommunikáció jogát.

18 Koltay a hallgatóságra tekintettel találja indokolhatónak a jogi személyek, sajtóorgánumok és pártok esetében is a szólásszabadság megadását, mert az individualista alapon még akkor is nehezen alátámasztható, ha ezek mögött a szervezetek mögött végső soron emberek vannak. Koltay András: *A szólásszabadság alapvonalai – magyar, angol, amerikai és európai összehasonlításban.* Budapest, Századvég, 2009. 145.

19 Az individualista igazolásokról összefoglalóan lásd: Koltay i. m. 38–43.

20 A magyar Alkotmánybíróság gyakorlatában a nyilvános társadalmi kommunikációban való részvételben látja a szólásszabadság hatályát. Török Bernát: *A szólásszabadság magyar doktrínája az amerikai jogirodalom tükrében* [Doktori disszertáció]. Szegedi Tudományegyetem ÁJK, 2018. 40–42. https://doktori.bibl.u-szeged.hu/id/eprint/9719/1/disszertáció_TB.pdf

A botok és lehetséges jogaik kiértékelésekor számításba vehető a bot intelligenciája is.[21] A mesterséges intelligencia a közösségi média botok egy igen szűk rétegét jelenti, és még ebben az esetben is kérdéses, hogy rendelkezhet-e maga a mesterséges intelligencia szólásszabadsággal. Összefoglalóan jelen tanulmány úgy tekinti, hogy a közösségimédia-botok esetében maga a bot nem rendelkezik szólásszabadsággal, azaz szükséges vizsgálni, hogy a botok megfelelő közvetítői-e a botot használó/programozó ember(csoport) szólásszabadságának. Hosszabb távon azonban elkerülhetetlennek tűnik, hogy a mesterséges intelligencia és a mesterséges intelligencia által vezérelt közösségimédia-botok akár saját jogon, akár a hallgatóság jogán a szólásszabadság alanyai vagy kötelezettjei legyenek.[22]

Mivel a bothasználó/programozó természetes vagy jogi személy, vagy ezeknek egy csoportja,[23] ezért szólásszabadsága nem vitatható. Tekinthető úgy, hogy a bot által közzétett vagy megosztott tartalom közvetlenül a programozó munkájának eredménye, így ő a beszélő.[24] Természetesen előfordulhat, hogy a botot nem maga az üzenet közvetítője programozza, a bot maga képes lehet bármilyen üzenet közvetítésére, ez a képesség pedig meg is vásárolható. Ebben az esetben élesen elválik egymástól a bot programozójának személye és a bot használója, így a vásárló tölti be a beszélő szerepét.[25]

További kérdésként azonban felvethető, hogy akár a bot programozójának, akár használójának a személye eltávolodhat-e annyira a botfióktól, hogy az már ne az ő véleményét tükrözze, azaz válhat-e a bot tevékenysége annyira mechanikussá, hogy az egy szólásszabadsággal biztosan rendelkező entitásnak sem betudható.[26] A válasz ez esetben is igen, bár ezen álláspont vitatott. Benjamin a linkgyűjtés és sportújságírás automatizálásának folyamatát lépésről lépésre elemezve nem talál olyan fázist, amelynek során a programozó szólásszabadsága elveszhetne. A szerző által elsőként vizsgált példa az 'Isten halott' kifejezésre adott eredmények gyűjteménye egy online falon, amelynek lehet üzenetértéke, de maga az üzenet ismeretlen. A második példában egy újságíró automatizálja a meccsösszefoglalók megírásának minden lépését. A közösségimédia-botok működésére mindkét példa alkalmazható, azonban mégsem tökéletesen. Az első esetben egy online tábláról van szó, amelyet az egyedi link ismeretében tevőleges magatartással (linkre kattintás) meg kell látogatni, ellentétben a közösségimédia-botok által megosztott vagy közzétett tartalmakkal. Ezekhez a felhasználó külön erőfeszítés nélkül, pusztán a bejelentkezéssel akartalanul hozzáférhet a platform algoritmusaitól függően. A sportújságíró esetében pedig maga az újságíró végzi az automatizálást, amelynek során maga adja meg az adatforrásokat és közvetlenül ő állítja össze azokat a panelkifejezéseket és információkat, amelyekből a későbbiekben összeáll a cikk, így közvetlen ráhatása van annak

21 Összefoglalóan lásd: James B. Garvey: Let's Get Real: Weak Artificial Intelligence Has Free Speech Rights. *Fordham Law Review,* vol. 91., no. 3. (2022) 970–974.; Samuel C. Woolley: Computational Propaganda and Political Bots: An Overview. In: Shawn Powers – Markos Kounalakis (szerk): *Can Public Diplomacy Survive The Internet? Bots, Echo Chambers, and Disinformation.* United States Advisory Commission on Public Diplomacy, 2017. 13–18. https://www.state.gov/wp-content/uploads/2019/05/2017-ACPD-Internet.pdf

22 Massaro–Norton i. m. 1192., Garvey i. m. 991., Koops–Hildebrandt–Jaquet-Chiffelle i. m. 555–559.

23 A mesterséges intelligencia által programozott bot is végső soron visszavezethető egy emberi programozóra vagy azok csoportjára.

24 Hines i. m. 420.

25 Uo.

26 Koops–Hildebrandt–Jaquet-Chiffelle i. m. 508., Wu i. m. 1504.

tartalmára.[27] Ezáltal feltételezhető, hogy az algoritmusok kimenetét teljes mértékben kontrollálja, szabadon módosíthatja még a publikálás előtt. A példa akkor állná meg a helyét, ha az újságíró nem egy, hanem számtalan cikket írna így egységnyi idő alatt, amelyek tartalma számára ismeretlen lenne, és azokat számtalan néven (vagy név nélkül), nagy mennyiségben tenné közzé oly módon, hogy azt az olvasó akkor is látná, ha nem szeretné, azaz nem lenne egyetlen médium (újság vagy weboldal) direkt felkereséséhez kötve.

Ha a személyiség meglétének eldöntésekor kiindulópontnak tekintjük az önálló döntéshozatalra, mérlegelésre való képességet, akkor belátható, hogy ez a döntéshozatal és mérlegelés nem történik meg minden alkalommal az ember részéről, amikor az általa használt bot megnyomja a „tetszik" gombot, hozzászólást generálva, mert akkor a bot használata elveszítené az értelmét.[28]

Ha úgy tekintjük, hogy léteznek olyan botok, amelyek önmagukban nem alanyai a szólásszabadságnak és tevékenységük annyira eltávolodott a bot használójától, hogy az már nem neki betudható,[29] a személyiség kérdésének vizsgálata továbbra is szükséges marad a hallgatóság oldaláról, mivel a szólásszabadságban megjelenik az információhoz jutás joga is.[30] Ebben a hallgatóságot is szükséges két csoportra bontani: emberi hallgatóságra, amely egyértelműen rendelkezik a véleménynyilvánítás szabadságával, és bot-hallgatóságra. Bár a valóságban kicsi az esélye, de a közösségi média botok hatalmas száma miatt előfordulhat, hogy egy-egy üzenet bár nagyszámú fiókhoz eljut, ezen fiókok közül kevés mögött áll valós felhasználó, így az üzenet hallgatósága hamis. A 'hamis hallgatóság' kifejezés alatt értendők a mind a manuálisan irányított bábfiókok, mind pedig a botok.[31] Tagadhatatlan azonban, hogy a botok által generált vagy megosztott beszéd értékkel bírhat a hallgatóság számára,[32] de veszélyeket is rejthet magában. Ezek a veszélyek indokolják a botok szabályozását, mert ebben az esetben a hallgatóság jogai védelmének kell előtérbe kerülniük.[33]

Az Amerikai Legfelső Bíróság a védelem feltételeit a Spence-ügyben[34] állapította meg. A Spence-teszt szerint akkor merülhet fel az Első Alkotmánykiegészítés alkalmazása, ha a beszélő szándékában áll olyan üzenet küldése, amelynek lehet olyan hallgatósága, aki ezt az üzenetet megérti akkor is, ha az nem egyértelmű. Jelen alfejezetben tárgyaltak alapján feltehető a kérdés, hogy védendő-e az üzenet, ha annak sem a küldője, sem a fogadója nem rendelkezik szólásszabadsággal, azaz mindkettő bot? Mivel ennek valószínűsége igen alacsony,

27 Stuart Minor Benjamin: Algorithms and Speech. *University of Pennsylvania Law Review,* vol. 161., no. 6. (2013) 1458–1472.

28 Ismert az a jelenség, hogy az emberi felhasználók is megosztanak bejegyzéseket vagy megnyomják a 'tetszik' gombot anélkül, hogy a bejegyzés tartalmát valóban megismerték volna. Maksym Gabielkov – Arthi Ramachandran – Augustin Chaintreau – Arnaud Legout: Social Clicks: What and Who Gets Read on Twitter? *ACM SIGMETRICS / IFIP Performance 2016*, vol. 44., no. 1. (2016) 179–192. A különbség a kettő közt, hogy már maga a megismerés nélküli megosztás is egy mérlegelést igénylő döntés az emberi felhasználó részéről.

29 Telefontársaságok esetén látunk erre példát, hogy a telefontársaság kapcsolata a beszéddel túl távoli és túl mechanikus, a tartalom ismerete és a választás is hiányzik ahhoz, hogy kiadónak tekintse őket a jog. Wu i. m. 1521.

30 Benjamin i. m. 1477–1478.; Emberi Jogok Európai Egyezménye 10. cikk 1. bekezdés; Emberek és Népek Jogainak Afrikai Chartája 9. cikk 1. bekezdés; Emberi Jogok Amerikai Egyezménye 13. cikk.

31 Aaron Delwiche: Computational Propaganda and the Rise of the Fake Audience. In: Paul Baines – Nicholas O'Shaughnessy – Nancy Snow (szerk.): *The SAGE Handbook of Propaganda.* London, SAGE, 2020. 107. https://doi.org/10.4135/9781526477170

32 Massaro–Norton i. m. 1174., 1178., 1190–1191.

33 Uo. 1191–1192.

34 Wu i. m. 1510., Benjamin i. m. 1463.

a közzétett vagy megosztott tartalom szinte bizonyosan el fog jutni legalább egy emberhez, így a kérdés pusztán elméleti, kifejtése pedig túlmutat jelen tanulmány keretein.

2.2. Beszéd (speech)

Általánosan elfogadott, hogy nem minden kommunikáció tartozik a védelemre érdemes beszéd körébe.[35] Ilyen kommunikáció példájaként említi Wu az autó riasztójának hangját.[36] A közösségi média tekintetében a kommunikáció a platformszolgáltató által előre meghatározott keretek között lehetséges, így a kommunikáció egyes formái, mint az autóriasztó szirénázása, nem fordulhatnak elő, illetve olyan formában fordulhatnak elő, hogy valaki azokat hangfájlként feltölti és közzéteszi. A hangfájlként való közlésnek azonban már lehet üzenetértéke, így minősülhet védett beszédnek.

A botok által végzett tipikus tevékenységek jellemzően: a „tetszik" gomb használata, tartalom közzététele, megosztása, megjegyzések hozzáfűzése egyes bejegyzésekhez.[37] Ezek a tevékenységek mind – emberi felhasználó esetében legalábbis biztosan – véleménynyilvánításnak minősülnek, vagyis amennyiben az így közvetített üzenet nem ütközik tilalomfába (pl.: nem gyermekpornográfia vagy gyűlöletbeszéd[38]), úgy azt a jog védi.[39]

A botok szerepét gyakran az álhírek terjesztésével összefüggésben vizsgálják a kutatók. Egyértelmű, hogy jogi szempontból a beszéd – pusztán hamis volta miatt – nem kerül ki az alkotmányos védelem köréből, ugyanakkor más mércével mérendő a kereskedelemben előforduló hamis beszéd és a politikai álhírek. Míg az előbbi nem élvez védelmet, addig az utóbbi esetben a szankcionálhatóság egy szűk körre korlátozódik.[40]

2.3. Kormányzati motiváció a szabályozásra

A kormányzati motiváció vizsgálatakor a kérdés az, hogy a szabályozás célkeresztjében a beszéd mondanivalója van-e vagy esetleg egyéb körülmény: hely, idő vagy a kifejezés módja,[41] esetleg egészen

35 Wu i. m. 1506. Végiggondolásra érdemes, hogy akár maga a programkód is lehet védett beszéd. Hines i. m. 420.

36 Wu i. m. 1497. Ez nem azt jelenti, hogy nem fordulhat elő, hogy mégis védelemre érdemes kommunikáció legyen. Uo. 1524.

37 Tevékenységüktől függően néhány szerző nevesíti és csoportosítja ezeket a botokat (pl.: like-botok). Összefoglalóan ld.: Kovács Andrea: A közösségi média botok lehetséges csoportosítási szempontjai mint a jövőbeli szabályozás alapja. *Themis,* 2023/2. https://doi.org/10.55052/themis.2023.2.36

38 További példákat a tiltott beszédre ld.: Wu i. m. 1509–1510.; Jan Oster: *European and International Media Law*. Cambridge, Cambridge University Press, 2016. 223–241.

39 A 'tetszik' gomb használatáról mint a véleménynyilvánítás egy jog által védett (vagy szankcionálható) formájáról ld.: Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Medas Res,* 2019/1. 2–4., továbbá a 'tetszik'gomb használatáról, a megosztásról és a megjegyzésekről/bejegyzésekről lásd: Papp János Tamás: A hamis hírek alkotmányos helyzete és szerepe a demokratikus nyilvánosság befolyásolásában. *In Medias Res,* 2020/1. 141–144.

40 Papp i. m. 150–157. Philip N. Howard – Samuel C. Woolley – Ryan Calo: Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics,* vol. 15., no. 2. (2018) 88.

41 Wu i. m. 1514–1515.

más, például gazdasági érdek.[42] Wu példaként a gyújtogatást hozza: bár az ellenségünk házának felgyújtása kifejezi nemtetszésünket a személy iránt, mégsem a nemtetszés kifejezése tiltott. Egy zászló elégetése azonban már rendelkezhet üzenetértékkel, ennek a cselekménynek a tiltása vitatható.[43]

Az online térben a beszéden kívüli cselekmények köre eléggé korlátozott (ilyen cselekmény lehet például egy túlterheléses támadás, adatlopás), a jelen tanulmányban vizsgált szabályozások esetében a botokon keresztül folytatott vagy botok által közvetített kommunikáció kerül célkeresztbe, ezért nem kérdés, hogy a motiváció a véleménynyilvánítás szabályozására vonatkozik. Ugyanakkor jelen alfejezet keretében érdemes megvizsgálni, hogy konkrétabban mi motiválhatja a jogalkotót a botok szabályozására.

A közösségimédia-botok politikai tevékenysége bár korábban is jelen volt,[44] igazán fókuszba mégis a 2016-os amerikai elnökválasztást követően került.[45] Azóta számos tanulmány született arról, hogy az egyes választások során milyen bot-tevékenység figyelhető meg, hogyan használják a politikai ellenfelek (vagy harmadik személyek) a botokat a választások befolyásolására.[46] Amennyiben a közösségimédia-bot tevékenysége beszédnek minősül, úgy tevékenységének korlátozása csak jogos érdekből lehetséges. Ilyen jogos érdek lehet többek között: a mások jogainak biztosítása, a demokratikus társadalom erkölcse, a közrend és közegészség védelme.[47]

A legkézenfekvőbb jogos érdek ebben az esetben a közrend mint a demokratikus berendezkedés védelme, azaz a botok tevékenységének szabályozásával a választópolgárok megfelelő és hasznos információkhoz juthatnak.[48] Felmerülhet még a mások jogainak biztosítása is, mint a hallgatóság információhoz jutásának joga, valamint a politikai ellenfelek lejáratásával kapcsolatban a jóhírnév védelme.[49] A közelmúltban a közegészségügy védelme is relevánssá vált. A Covid19-járvány során a közösségi médiában rengeteg információ jelent meg, a bejegyzések körülbelül 10%-át közösségimédia-botok tették közzé.[50]

Részben ezen három jogos érdekhez kapcsolódóan merül fel a hamis hírek terjesztésének kérdése is. Erre a hatásra reagálva születtek meg olyan jogi instrumentumok, mint Szingapúrban a hamis hír törvény, amelynek alkalmazása során súlyosbító körülményként kell értékelni, ha a

42 Benjamin i. m. 1478.

43 Wu i. m. 1515–1516. Hasonló eset Magyarországon is előfordult: egy izraeli zászló elégetésével kívántak tiltakozni egy Tilos Rádióban elhangzott kijelentés ellen. Ez esetben végül a zászlóégetők garázdaság vádjával álltak bíróság elég. Index: Botrányos ítélethirdetés a zászlóégetők perén. *Index.hu,* 2004. június 17. https://index.hu/bulvar/mgiorgio1193/

44 Ld. pl.: Samuel C. Woolley: Automating power: Social bot interference in global politics. *First Monday,* vol. 21., no. 4. (2016).

45 Ld. pl.: Riccardo Cantini – Fabrizio Marozzo – Domenico Talia – Paolo Trunfio: Analyzing Political Polarization on Social Media by Deleting Bot Spamming. *Big Data and Cognitive Computing,* vol 6., no. 1. (2022), Howard–Woolley–Calo i. m.

46 Ld. például: Woolley 2016 i. m.

47 Emberi Jogok Európai Egyezménye 10. cikk 2. bekezdés, Emberi Jogok Egyetemes Nyilatkozata 29. cikk 2. bekezdés, Emberi Jogok Amerikai Nyilatkozata 13. cikk 2. bekezdés, Emberek és Népek Jogainak Afrikai Chartája 27. cikk 2. bekezdés, Oster i. m. 68–111.

48 Hines i. m. 430–431.

49 Howard–oolley–Calo i. m. 83.

50 Wen Shi – Diyi Liu – Jing Yang – Jing Zhang – Sanmei Wen – Jing Su: Social Bots' Sentiment Engagement in Health Emergencies: A Topic-Based Analysis of the COVID-19 Pandemic Discussions on Twitter. *International Journal of Environmental Research and Public Health,* vol. 17., no. 22. (2020) 8711.

hamis hírek terjesztése automatizált fiókok segítségével történik,[51] vagy az Európai Unióban (a továbbiakban: EU) a dezinformáció visszaszorítását célzó magatartási kódex,[52] és a német *Medienstaatsvertrag* (a továbbiakban: MStV). Az MStV a német tartományközi médiaegyezményt takarja, amely 2020-ban lépett hatályba az AVMS rendelet[53] nyomán. Az MStV alapján, amennyiben a szolgáltatók tartalmat vagy üzenetet számítógépes programmal automatikusan hoznak létre vagy küldenek, akkor a felhasználó(ka)t értesíteni kell a fiók automatizált voltáról.[54] A 18. § (3) bekezdése szerinti címkézésről pedig a közvetítő médiaszolgáltató köteles gondoskodni.[55] Az MStV a DSA-nál szigorúbb előírást tartalmaz, amely nem csak a chatbotokra alkalmazandó.

2.4. A korlátozás elsősorban a szólásszabadságot érinti-e (abridgement)

A teszt utolsó pontja arra vonatkozik, hogy a szabályozás valóban a beszédet érinti-e. Wu példaként a szerzői jogi szabályokat hozza, amelyek esetében a Legfelső Bíróság nem vizsgálja a szólásszabadság kérdését.[56] Politikai kérdések tekintetében a válasz egyértelműen pozitív, azonban marketing- és értékesítési tevékenység esetében már szóba jöhetnek egyéb jogterületek, mint például a versenyjog vagy a fogyasztóvédelem, tekintettel arra, hogy ezek általánosan alkalmazandó jogszabályok.[57]

3. Mit mondanak a jogi normák?

3.1. Szabályozási kísérletek az Egyesült Államokban

Az Egyesült Államokban több tervezet született a botok tevékenységének szabályozására,[58] ezek közül a valóban hatályba lépett kaliforniai szabályozással és a hatályba nem lépett

51 Papp i. m. 159.

52 Gergely Gosztonyi: *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices.* Cham, Springer, 2023. 57.

53 2018/1808/EU irányelv az 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 HL L 303, 2018. 11. 18. 69–92. o.

54 Medienstaatsvertrag 18. § (3) bekezdés; Az MStV nem alkalmazandó, amennyiben a felhasználók átlagos száma 6 hónapon belül nem haladja meg az egymilliót, ha árukra vagy szolgáltatásokra specializálódott és azokról aggregált, válogatott tartalmat tesz közzé vagy ezeket prezentálja, illetve ha kizárólag üzleti vagy családi célú. MStv 91. §.

55 MStV 93. § (4) bekezdés; Algorithm Watch: Germany's new media treaty demands that platforms explain algorithms and stop discriminating. Can it deliver? *AlgorithmWatch*, 2020. március 09. https://algorithmwatch.org/en/new-media-treaty-germany/

56 Európában ez sokkal kevésbé volt kategorikus, lehetőséget adott a szólásszabadsági szempontok vizsgálata is. Ennek változását vizionálták az új szerzői jogi irányelv 13. cikkeként elhíresült, végül 17. cikként elfogadott rendelkezések ellenzői. Ld. pl.: *Article 13 – Monitoring and Filtering of Internet Content is Unacceptable* [Nyílt levél]. https://www.eff.org/files/2017/10/16/openletteroncopyrightdirective_final.pdf

57 Benjamin i. m. 1482.

58 Kasey Stricklin – Megan K. McBride: *Social Media Bots: Laws, Regulations and Platform Policies* [Report]. Washington. CNA, 2020. https://www.cna.org/reports/2020/10/DIM-2020-U-028193-Final.pdf

föderális tervezettel foglalkozik a tanulmány. Ezek egyike az azóta már hatályos *Bot Disclosure Law*ként elhíresült Senate Bill No. 1001. (a továbbiakban: S. B. 1001)[59] Kaliforniában, amely a kereskedelmi kódexet egészíti ki, a másik az úgynevezett *Bot Disclosure and Accountability Act of 2019*,[60] amely végül nem került elfogadásra. Ez utóbbinak két szövegváltozata létezik: a Szenátusban 2019 júliusában bemutatott, Demokrata Párt által támogatott[61] (a továbbiakban: BDAA) és a Képviselőházban 2019 szeptemberében bemutatott, Republikánus Párt által támogatott[62] változat. A két változat közötti legszembetűnőbb különbség, hogy a Republikánus Párt által támogatott változatból kikerült a botok használatának tiltása a politikai hirdetésekhez.

Az S. B. 1001 mindössze annyit ír elő, hogy amennyiben a bot üzleti tevékenységre (áruk vagy szolgáltatások eladására vagy vételére) buzdítja a felhasználót, vagy a bot tevékenysége a választások kimenetelének befolyásolására irányul, úgy a kaliforniai felhasználók előtt fel kell fedni, hogy bottal állnak kapcsolatban[63] (a továbbiakban: transzparenciakövetelmény). Definíció szerint a bot olyan automatizált fiók (*automated online account*), amelynek egyetlen tevékenysége sem, vagy lényegében egyetlen tevékenysége sem embernek betudható.[64] A transzparenciakövetelmény azonban csak azokra az online platformokra vonatkozik, amelyek látogatóinak száma az Egyesült Államokban meghaladja tizenkét egymást követő hónap többségében a tízmillió főt.[65] Bár az S. B. 1001 nem nevesíti a közösségimédia-platformokat, egy weboldal chatbotjára nehezen értelmezhető az automatizált fiók kifejezés. A törvény hiányosságaként róható fel, hogy a transzparenciakövetelményt kizárólag a bothasználó kötelezettségévé teszi, a platformok felelősségét kifejezetten kizárja.[66]

A BDAA esetében a Kongresszus előírná a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission) számára, hogy kötelezze a közösségimédia-platformokat, hogy a bothasználóknak tegyék kötelezővé az automatikus fiókok jelölését.[67] Továbbá előírná az FTC-nek, hogy kötelezze a közösségimédia-platformokat, hogy tegyenek észszerű intézkedéseket az automatizált fiókok azonosítására és – amennyiben a bothasználó azt nem teszi meg – címkézésére vagy eltávolítására.[68] A BDAA emellett kiegészítette volna a választási törvényt is azzal, hogy választásokkor a jelöltek és pártok nem használhatnak botokat és nem támogathatják azok használatát semmilyen üzenet felerősítésére, megosztására vagy más módon történő közvetítésére, valamint nem kérhetnek, nem fogadhatnak el, nem vásárolhatnak vagy adhatnak el botokat semmilyen célra.[69]

A politikai bizottságok, vállalatok és szakszervezetek esetében a tiltott kampánytevékenységek listáját kiegészítették volna azzal, hogy nem használhatnak botokat és nem támogat-

59 California Business and Professional Code § 17941 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001

60 Az első tervezete 2018-ban látott napvilágot: S. 3127 Bot Disclosure and Accountability Act of 2018. https://www.congress.gov/bill/115th-congress/senate-bill/3127/text

61 S. 2125 Bot Disclosure and Accountability Act of 2019. https://www.congress.gov/bill/116th-congress/senate-bill/2125/text

62 H.R. 4536 Bot Disclosure and Accountability Act of 2019. https://www.congress.gov/bill/116th-congress/house-bill/4536/text

63 S. B. 1001 § 17941 (a) bekezdés.

64 S. B. 1001 § 17940 (a) bekezdés.

65 S. B. 1001 § 17940 (c) bekezdés.

66 S. B. 1001 § 17942 (c) bekezdés; Hines i. m. 434.

67 BDAA Sec. 4. (c) bekezdés (1) pont.

68 BDAA Sec. 4. (c) bekezdés (3)–(5) pont.

69 BDAA Sec. 5. (a) bekezdés (1) pont.

hatják azok használatát olyan üzenetek felerősítésére, megosztására vagy más módon történő közvetítésére, amelyek kifejezetten egy jelölt megválasztása mellett vagy ellen kampányolnak, illetve amelyek politikai kommunikációnak minősülnek a választási törvény szerint.[70] Továbbá számukra is tiltott lenne botok kérése, elfogadása, vásárlása vagy eladása az előző pontban felsorolt célokra.[71]

3.2. A botok szabályozása az Európai Unióban – a dezinformáció visszaszorítását célzó kódex vonatkozó rendelkezései és a DSA[72]

Az EU-ban 2018-ban az Európai Parlamentben az Európai Bizottság arra a kérdésre, hogy tervez-e az S. B. 1001-hez és a BDAA-hoz hasonló szabályozást,[73] azt a választ adta, hogy aktuálisan nincs ilyen terv. Ugyanakkor a válaszban hivatkoztak a 2018-as dezinformáció visszaszorítását célzó magatartási kódexre,[74] amely az I. pont v. alpontban megfogalmazza, hogy a közösségimédia-platformoknak egyértelmű jelölési rendszereket és szabályokat kell kialakítaniuk, hogy a botfiókok tevékenysége egyértelműen megkülönböztethető legyen az ember által kezelt fiókokétól, ehhez pedig stratégiát tesznek közzé, amelyet az EU-n belül végre is hajtanak.[75] A kódexet 2022-ben megerősítették , amelyben megállapították, hogy az aláírók további kötelezettségvállalásai szükségesek a félretájékoztatás és a dezinformáció jelenségének csökkentésére.[76] A szöveg szerint e jelenségen értendő az üzenet botok általi felerősítése is.[77] A megerősített kódex alapján a platformok kötelesek közzétenni, milyen szabályzataik léteznek a dezinformáció jelenségének korlátozására, és ezek alapján milyen intézkedéseket tettek.[78] Az első riportokat 2023 januárjára vonatkozóan 2023 februárjában tették közzé az aláírók. Bár maguk a riportok nem kifejezetten az automatizált fiókokra koncentrálnak, nem tesznek különbséget ember által üzemeltetett és teljesen automatizált fiókok között, erősen valószínűsíthető, hogy csak a Facebook esetében a 2022 Q3-ban hamisság miatt eltávolított 1.5 milliárd(!) fiók[79] jelentős hányada bot lehetett. Csökkenő tendenciát

70 BDAA Sec. 5. (a) bekezdés (2) pont (A) alpont.

71 BDAA Sec. 5. (a) bekezdés (2) pont (B) alpont.

72 Jelen szakasz a 2022-ben megjelent rövid tanulmányom 218–219. oldalainak átdolgozott, aktualizált és kiegészített változata. Kovács Andrea: Botok, automatizált fiókok a közösségi médiában. *Jogi tanulmányok*, (2022) 209–223. https://doi.org/10.56966/2022.14.Kovacs

73 Marietje Schaake: Bot disclosure laws in the EU. Parlamentary question E-004306/2018. 2018. augusztus 22. https://www.europarl.europa.eu/doceo/document/E-8-2018-004306_EN.html

74 European Commission: Answer given by Ms Gabriel on behalf of the European Commission. E-004306/2018 (ASW) 2018. november 14. https://www.europarl.europa.eu/doceo/document/E-8-2018-004306-ASW_EN.html; European Commission: A dezinformáció visszaszorítását célzó uniós gyakorlati kódex. 2018. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

75 A dezinformáció visszaszorítását célzó uniós gyakorlati kódex 2018. II. C. fejezet 5. pont.

76 A kódexben foglaltak csak az aláírók számára tartalmaznak kötelezettségeket, és aláírása pedig nem kötelező, a leginkább érintett platformok, mint a Facebook, az Instagram, a X/Twitter és a TikTok üzemeltetői is az aláírók között szerepeltek.

77 European Commission: The Strengthened Code of Practice on Disinformation. 2022. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

78 The Strengthened Code of Practice on Disinformation Measure 14.2.

79 Code of Practice on Disinformation – Meta Baseline Report 2023 January. https://disinfocode.eu/signatory-report/meta/ (a továbbiakban: Meta Baseline Report).

mutat a Meta 2023 júliusi riportja, amely alapján 2023 első félévében nagyságrendileg 1 milliárd fiókkal szemben jártak el gyanús tevékenységük miatt.[80] Az Instagram esetében ilyen adat nem áll rendelkezésünkre.[81]

A TikTok esetében országos bontásban is rendelkezésünkre állnak az adatok, amelyek alapján a 2023 januári riport szerint 9.196 magyar érintettségű fiókkal szemben jártak el, míg a teljes EU-ban ez 864.926 db fiók volt.[82] 2023 júliusában már 5.885.958 hamis fiókot távolítottak el a platformról, amelyből 15.821 db volt magyar érintettségű.[83] Az X/Twitter esetében hasonló számokkal nem rendelkezünk, 2023 januári riportjuk adatokban szegényes,[84] míg 2023 júliusából már nem rendelkezünk riporttal, mivel a platform úgy döntött, nem kívánja a Kódex hatályát a továbbiakban magára kötelezőnek elismerni.[85] Ahogyan Thierry Breton belső piacért felelős biztos is felhívta rá a figyelmet, hatályba lép(ett) az EU új szabályozása, „amely hasonló kötelezettségeket ró a szolgáltatóra." [86]

A digitális szolgáltatásokra vonatkozó rendelet (*Digital Services Act*, a továbbiakban: DSA)[87] foglalkozik a botok kezelésével, amely rendelkezések kevéssé változtak a rendelet korábbi szövegtervezetéhez képest.[88] A DSA a mesterséges intelligenciára vonatkozó rendelettel összhangban előírja, hogy a közösségimédia-szolgáltatónak explicit módon jelezni kell a felhasználónak, ha chatboton keresztül kommunikál, emellett természetesen biztosítania kell a szükséges emberi erőforrást is,[89] amennyiben emberi beavatkozásra (kommunikációra) van szükség. Az aktív felhasználók fogalmához fűzött indoklásban szerepel, hogy amennyiben a szolgáltató le tudja vonni az automatizált felhasználók – többek között a botok – számát további személyes adat feldolgozása nélkül az aktív felhasználók számából, akkor ezt megteheti,[90] azaz csökkentheti a felhasználók számát, amely alapján akár más szolgáltatói kategóriába eshet. Erre azonban csak akkor van lehetőség, ha az személyes adatok további kezelése vagy további nyomon követés nélkül is lehetséges.

Az online óriásplatformok és a nagyon népszerű keresőprogramok esetében kiemelt kockázatként nevezi meg a DSA a dezinformációs kampányokat, különösen a közegészségügy, a kiskorúak

80 Code of Practice on Disinformation – Report of Meta for the period 01 January 2023 to 30 June 2023. https://disinfocode.eu/signatory-report/meta-july-2023-report/ (a továbbiakban: Meta 2023 júliusi riport). A kézirat lezárásakor a 2024 januári riport még nem elérhető.

81 Az Instagram esetében a riportból hiányzik – míg Facebooknál megtalálható – a hamis fiókokra vonatkozó szabályok megnevezése is. Ld.: Uo. 44.

82 Code of Practice on Disinformation – Report of TikTok for the period 16 June – 16 December 2022. 2023. https://disinfocode.eu/signatory-report/tiktok/ (a továbbiakban: TikTok Baseline Report).

83 Code of Practice on Disinformation – Report of TikTok for the period 1 January 2023 – 30 June 2023. 2023. https://disinfocode.eu/signatory-report/tiktok-july-2023-final-version/ (a továbbiakban: TikTok 2023 júliusi riport).

84 Code of Practice on Disinformation – Report of Twitter for the period H2 2022. 2023. https://disinfocode.eu/signatory-report/5273-2/ (a továbbiakban: X/Twitter Baseline Report); Az X/Twitter jelentésével Vera Jourová sem volt teljes mértékben elégedett. European Commission: Daily News 09/02/2023. https://ec.europa.eu/commission/presscorner/detail/en/mex_23_723

85 Thierry Breton X/Twitter bejegyzése: https://twitter.com/ThierryBreton/status/1662194595755704321

86 Uo.

87 2022/2065/EU rendelet a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról, HL L 277, 2022. 10. 27. 1–102. o. A DSA-val kapcsolatban összefoglalóan ld.: Ondrej Moravec – Ivan Smiesko – Ewa Galewska – Gergely Gosztonyi – Sirio Zolea – Pascal Schneiders: Digital Services Act Proposal (Social Media Regulation). *Studia Politica Slovaca*, XIV, 2021/2–3. https://doi.org/10.31577/SPS.2021-3.5

88 Lásd: Kovács (2022) i. m. 218–219.

89 DSA (43) preambulumbekezdés.

90 DSA (77) preambulumbekezdés.

védelme, a mentális jólét és a nemi alapú erőszak esetében,[91] valamint a jogellenes beszéd terjesztését, tiltott termékek vagy szolgáltatások kereskedelmét,[92] az emberi jogi jogsérelmeket, ideértve a szólásszabadságot, tömegtájékoztatás szabadságát és sokszínűségét,[93] illetve a demokratikus folyamatokra és közbiztonságra gyakorolt hatásokat.[94] Ezen témakörök kapcsán a szolgáltatóknak kockázatelemzést kell végezniük, és felül kell vizsgálniuk a szolgáltatásaikat, hogy azok összehangolt és manipulált használata, valamint szabályzataik rendszerszintű megsértése milyen összefüggésben áll az említett kockázati csoportokkal.[95] A DSA érintett szakasza kifejezetten említi a szolgáltatás nem autentikus használatát, nevesítve a hamis és automatizált fiókokat.[96] A szolgáltatóknak kellő gondosság mellett csökkenteniük kell ezen kockázatokat, azonban mérlegelniük kell az intézkedések alapjogokra – például a szólásszabadságra – gyakorolt negatív hatását.[97]

Mindemellett a rendelet előírja, hogy az Európai Bizottság támogassa az egyes közérdekű problémák megoldása kapcsán különböző kódexek elfogadását, amelyekhez a szolgáltatók önkéntesen csatlakozhatnak.[98] Kifejezetten ilyen közérdekű cél a botok általi hamis információk terjesztésének visszaszorítása,[99] amely cél érdekében már a DSA előtt megszületett a már tárgyalt magatartási kódex. Ugyanakkor ki kell emelni, hogy pusztán a kódexek aláírása nem jelenti automatikusan a DSA-nak való megfelelőséget.[100]

A célok megvalósításához a DSA eszközöket, lehetséges szankciókat is javasol a közösségimédia-szolgáltatóknak: nem autentikus használat esetén – ide értendők a botfiókok is - indoklás nélkül(!) csökkenthetik a láthatóságot az érintett tartalom hátrasorolásával, hozzáférhetőség korlátozásával vagy a felhasználó egyes közösségekből való, értesítés nélküli kizárásával, sőt demonetizálással is.[101]

A DSA érdekessége, hogy a fenti példák mind kizárólag az indokolásból származnak, a „bot" szó nem található meg a rendelkező rész szövegében,[102] azaz az európai jogalkotók azonosítják a botok lehetséges szerepeit és hatásait a közösségimédia-platformokon, azonban a szabályozás nem konkrétan a botokra, hanem az általuk generált torzító, káros hatásokra koncentrál.

91 DSA (83) preambulumbekezdés, 34. cikk (1) bek. *d)* pont. Az óriásplatformokkal és az általuk okozható sérelmekkel kapcsolatban ld. pl.: Sally Broughton Micova: *What is the harm in size? Very large online platforms in the Digital Services Act* [Issue paper]. Centre on Regulation in Europe, 2021. https://cerre.eu/wp-content/uploads/2021/10/211019_CERRE_IP_What-is-the-harm-in-size_FINAL2.pdf

92 DSA (80) preambulumbekezdés.

93 DSA (81) preambulumbekezdés, 14. cikk (4), 34. cikk (1) bek. *b)* pont.

94 DSA (82) preambulumbekezdés, 34. cikk (1) bek. *c)* pont. A rendszerszintű kockázatok kapcsán ld.: David Sullivan – Jason Pielemeier: Unpacking „Systemic Risk" Under the EU's Digital Service Act. *Techpolicy.press,* 2023. július 19. https://www.techpolicy.press/unpacking-systemic-risk-under-the-eus-digital-service-act/

95 DSA (84) preambulumbekezdés; 34. cikk (2) bek.

96 Uo. A preambulum (84) bekezdése és a 34. cikk (2) bekezdése szintén eltérést mutat. Míg előbbi nevesíti az automatizált fiókok használatát mint inautentikus használatot, utóbbi azt nem részletezi, hogy mi minősül inautentikus használatnak, ugyanakkor kiegészül az automatizált támadás kifejezéssel.

97 DSA (86) preambulumbekezdés; 14. cikk (4) bek.

98 DSA (103) preambulumbekezdés; 45. cikk.

99 DSA (104) preambulumbekezdés.

100 Uo. A magatartási kódexek kapcsán ld.: Rachel Griffin – Carl Vander Maelen: Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges. Rotterdam, (2023. június 9.): *Law, AI & Regulation Conference*.https://dx.doi.org/10.2139/ssrn.4463874

101 DSA (55) preambulumbekezdés, 17. cikk (2). A preambulumhoz képest eltérés, hogy az indoklási kötelezettség alól mentesül a szolgáltató, ha az információ megtévesztő, nagy mennyiségű, kereskedelmi tartalom.

102 A preambulum szerepéről a normaszöveg értelmezése kapcsán ld. pl.: Koós Gábor: A preambulum szerepe az Európai Uniós jogi normák értelmezésében. *Acta ELTE*, 2013/50. 187–205.

3.3. Mesterséges intelligencia a platformokon – a dezinformáció visszaszorítását célzó kódex, a DSA és a mesterségesintelligencia-rendelet

A botok témakörében külön kiemelendők a manipulált tartalmak – leginkább valamilyen mesterséges intelligencia által generált tartalom és annak kezelése. A DSA 35. cikk (1) bekezdés *k)* pontja a kockázatcsökkentés körében tárgyalja, hogy az online óriásplatformoknak és nagyon népszerű keresőprogramoknak egyértelműen láthatóvá és megkülönböztethetővé kell tenniük a manipulált vagy generált kép-, hang- és videóanyagokat a nem manipulált tartalmaktól, illetve az ilyen jelöléshez szükséges eszközöket biztosítaniuk kell a felhasználóik számára.

Hasonló kötelezettséget ír elő a dezinformáció visszaszorítását célzó kódex is. A 15. számú vállalásban azok az aláírók, amelyek mesterséges intelligenciát fejlesztenek vagy működtetnek és amelyek szolgáltatásain keresztül mesterséges intelligencia által generált vagy manipulált tartalom terjed, fellépnek ez ellen a mesterségesintelligencia-rendelettel összhangban. Mind a Meta, mind pedig a TikTok riportjában megemlítik, hogy a vállalás teljesítésével kapcsolatban csatlakoztak a Partnership on AI's Responsible Practices for Synthetic Media keretrendszerhez,[103] illetve mindkét vállalat említést tesz egyéb munkacsoportokban való részvételről is.[104] A 15.1-es vállalás tekintetében mindkét vállalat megemlíti saját manipulált médiára vonatkozó szabályzatát.[105] A Meta esetében ezen szabályzat alapján nem megengedett az olyan módosítás, amely megtéveszti az átlagos felhasználót, aki elhiszi, hogy a videón szereplő személy azt mondta, amit a videóban lát, holott ez nem igaz és a videót mesterséges intelligencia vagy gépi tanulás segítségével készítették. Kiemelendő, hogy a szabályzat kizárja a hatásköréből a szatírákat, paródiákat, illetve olyan videókat, amelyekben szavakat hagytak ki vagy a sorrendjüket módosították.[106]

A TikTok szintetikus médiára vonatkozó szabályzata alapján a realisztikusnak tűnő tartalmakat jelölni kell, amelyhez a szolgáltató tippeket is ad; a kísérő szövegben vagy vízjelen megadott kulcsszavak használatával teljesítheti a felhasználó ezt a kötelezettségét. Emellett azonban kifejezetten tiltott valós magánszemélyekkel kapcsolatos módosított tartalmak megjelenítése, közszereplők politikai vagy kereskedelmi célú megjelenítése módosított tartalmakban, illetve az oly módon szerkesztett anyagok közzététele, amely alkalmas más felhasználók megtévesztésére.[107]

Az X/Twitter is rendelkezik hasonló szabályzattal, amely megtévesztő médiatartalomnak tekinti azokat a tartalmakat, amelyeket szignifikáns és megtévesztő módon módosítottak, manipuláltak vagy alkottak meg, de ide tartoznak azok is, amelyeket megtévesztő módon vagy hamis kontextusban osztanak meg, illetve amelyek feltehetően a felhasználók széles körét zavarják össze a közügyeket érintően, esetleg hatással lehetnek a közbiztonságra vagy

103 Meta júliusi riport 53.; TikTok júliusi riport 72. Érdekesség, hogy egyik vállalat Baseline Reportja sem említi kifejezetten a mesterséges intelligenciát, a fókusz még a manipulált médián van. A hangsúly a júliusi jelentésekben kerül csak a mesterséges intelligenciára, amely feltehetően a ChatGPT népszerűvé válásának köszönhető.
104 Meta júliusi riport 53.; TikTok júliusi riport 72.
105 Uo.
106 Meta: Manipulated Media. https://transparency.meta.com/fa-ir/policies/community-standards/manipulated-media
107 TikTok: Integrity and Authenticity, Synthetic and Manipulated Media. https://www.tiktok.com/community-guidelines/en/integrity-authenticity/#3

komoly sérelmeket okozhatnak.[108] Természetesen kivételt képeznek a mémek, a szatírák és a rajzolt médiatartalmak is, illetve megengedett a kommentár, az értékelés, a vélemény kifejezése és a reakció is. A szabályzat sehol nem nevesíti külön a mesterséges intelligenciával előállított tartalmakat, ahogyan a januári jelentésük szövege sem.

Meg kell említeni a mesterséges intelligenciára vonatkozó rendelettervezetet is.[109] A mesterségesintelligencia-rendszerek esetében az emberekkel történő interakció, illetve tartalom létrehozása különleges kockázatot jelent, így amennyiben már létező személyekre, helyekre vagy eseményekre a megtévesztésig hasonlító audiovizuális tartalmat állítanak elő vagy manipulálnak, a tartalmakat címkézni kell.[110] Bár e kötelezettség nem érinti közvetlenül a közösségimédia-szolgáltatást, említésre méltó, hogy például a Meta is fejleszt saját mesterséges intelligenciát.[111] A rendelet indokai és céljai között azonban kiemelik, hogy csevegőrobotok és deepfake-ek használata esetén csak minimális átláthatóság javasolt.[112]

4. Közösségi irányelvek és egyéb platformspecifikus szabályok[113]

4.1. Automatizált fiókok, botok szabályozása az X/Twitter, a Meta platformok és a TikTok közösségi irányelveiben

Az automatizált fiókok létét az online óriásplatformok közül az X/Twitter, a Meta és a TikTok is tudomásul veszi, a botok a platformok mindennapi működésük részei, igyekeznek az automatizált felhasználókra szabályokat alkotni és alkalmazni. Mindhárom platform esetében találunk akár az automatizált fiókokra, akár a botokra mint a hamis fiókok egy alcsoportjára alkalmazandó közösségi irányelveket. Általánosságban elmondható, hogy a botok szabályozását leginkább a hamis voltuk, illetve a – sokszor tiltott – tevékenységük alapján próbálják szabályozni a szolgáltatók.[114] E szabályzatok kiváló összefoglalását nyújtja Kasey Stricklin és Megan K. McBride. A botokra vonatkozó szabályok jelentős részét a nem autentikus tevékenységre vonatkozó szabályzatok teszik ki, amelybe beleértendők a spamre és a mesterséges felerősítésre vonatkozó tilalmak. Az alkalmazandó szabályok kisebb részét a hamis fiókokra és az automatizációra vonatkozó általános szabályok teszik ki, ez utóbbihoz tartoznak a fejlesztőknek szánt iránymutatások.

108 Twitter: Synthetic and manipulated media policy. 2023. április. https://help.twitter.com/en/rules-and-policies/manipulated-media

109 Az Európai Parlament és Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló javaslata COM(2021) 206 final 2021/0106(COD) https://eur-lex.europa.eu/legal-content/HU/TXT/?uri= CELEX:52021PC0206 (a továbbiakban: MI rendelet).

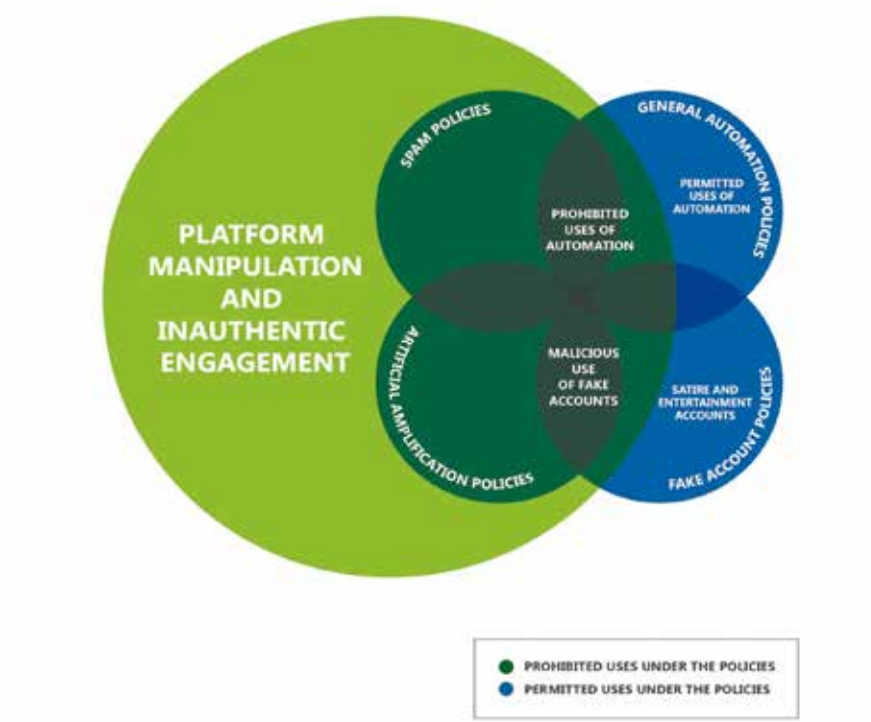
110 MI rendelet (70) preambulumbekezdés.

111 Llama. https://ai.meta.com/llama/

112 MI rendelet Indokolás 1.1. pont. Erről részletesen ld.: Gosztonyi Gergely – Lendvai Gergely Ferenc: Deepfake: A Multifaceted Dilemma in Ethics and Law. *Journal of Information Ethics,* vol. 32., no. 2. (2023) 109–121. https://doi.org/10.2307/JIE.32.2.109

113 Jelen fejezet a 2022-ben megjelent rövid tanulmányom 214–218. oldalainak aktualizált, átdolgozott és kiegészített változata. Kovács (2022) i. m. 214–218.

114 Stricklin–McBride i. m. 14.



1. ábra A közösségimédia-botok szabályozása szempontjából releváns közösségi irányelvek
Forrás: Delwiche (2020) [115]

A mesterséges felerősítés lehet passzív is, a követés gomb megnyomását követően a botfiókok hozzájárulnak egy személy vagy oldal népszerűbbnek mutatásához,[116] de hozzájárulnak a hamis hallgatóság jelenségéhez is.[117] Tevékenységük aktívan kiterjedhet például meggyőzésre, hamis konszenzus kialakítására, megosztó témák trenddé tételére vagy marginalizálására, de akár választások idején jelöltek népszerűsítésére vagy démonizálására is.[118] A következő szakaszokban röviden ismertetem a három platform releváns szabályait.

4.2. Automatizált fiókok az X/Twitteren

Az X/Twitter külön szabályrendszer szerint engedélyezi az automatizált fiókok használatát. A platformon számos ismert bot működik, amelyeknek kifejezetten pozitív példái a természeti katasztrófákat – elsősorban földrengéseket – jelző botok.[119] Az ilyen fiókokat a szolgáltató címkézni szeretné,

115 Stricklin–McBride i. m. 16.
116 A botok csoportosításáról – akár tevékenységük szerint lásd: Kovács (2023) i. m. A TikTok 2023 júliusi jelentésében találunk hamis like-ok és hamis követők törlésére vonatkozó adatokat (52., 57.). Magyarország esetében a szolgáltató szerint 2023 első félévében 337.974 hamis like-ot töröltek, és 6.371.084 hamis like-ot akadályoztak meg, hamis követőkből 140.336-at töröltek, a szolgáltató pedig 17.953.492 hamis követést akadályozott meg.
117 Delwiche i. m. 105–108.
118 Uo. 109.
119 X/Twitter: About automated account labels. https://help.twitter.com/en/using-twitter/automated-account-labels (a továbbiakban: X/Twitter FAQ).

összhangban a rá vonatkozó jogszabályokkal, ezáltal is egyértelművé téve a felhasználók számára a fiókok bot voltát. [120] Ezt jelenleg a fióknál megjelenő robot ikon és az "automated by' kifejezés jelöli. A rendszer jelenleg nem kötelező, az egyértelműen botfiókokat nem minden esetben jelölik meg.[121]

A X/Twitter kizárólag a szolgáltató által biztosított API-kon[122] keresztül engedélyezi az automatizálást, más formában nem.[123] Engedélyezett bármilyen automatizálás, amennyiben hasznos információt közvetít a felhasználók felé, automatikusan válaszol a felhasználók megkeresésére vagy közvetlen üzeneteire, vagy általánosságban olyan új megoldás, amely segíti az embereket (az X/Twitter egyéb szabályainak betartása mellett).[124] A szabályzat szerint tilos bármilyen X/Twitter szabályzat megsértése, az API nem megfelelő használata vagy az API korlátozásainak megkerülése, az X/Twitter API-tól eltérő automatizálása (ami akár végleges tiltást is vonhat maga után), illetve a spammelés, valamint a felhasználók zaklatása kéretlen üzenetekkel.[125]

Kifejezetten tiltott minden olyan tevékenység, amely spammelésnek minősül, ezek közül kiemelten:

– valamely népszerű témáról (*trending topic)* történő automatikus bejegyzéskészítés és bejegyzésközzététel, ha annak célja a népszerű témák befolyásolása vagy manipulálása, vagy
– duplikált vagy lényegében hasonló bejegyzések közzététele egy vagy több, ugyanazon felhasználó által üzemeltetett fiók segítségével.[126]

Tilos a fiókok duplikálása vagy lényegében azonos fiókok létrehozása, azonban a hasonló fiókok automatizálása megengedett.[127] A fenti szabályok alapján nehezen értelmezhető, hogy mit jelent tulajdonképpen a duplikálás vagy lényegében azonos célú fiók létrehozása. Fontos kiemelni, hogy amennyiben a duplikálás a *retweet* gomb használatával vagy saját tartalommal kombinálva történik, úgy az X/Twitter nem lép fel, hiszen a fenti feltételek mellett a duplikálás nem spammelő, hiteles tevékenységnek tekinthető módon történik.[128] Az automatikus *retweet*elés célja szórakoztatás, informálás vagy újdonság lehet.[129] Továbbá tilos a tömeges regisztráció, a regisztráció esetében pedig tilos az automatizáció, azaz nem hozhatók létre automatikusan új fiókok.[130] Az X/Twitter azonban lehetőséget ad több fiók üzemeltetésére, a fiókok számát pedig tízben maximalizálja.[131]

120 James Clayton: Twitter to label 'good' bot accounts. *BBC.com,* 2021. szeptember 10. https://www.bbc.com/news/technology-58510594

121 Például az LA Quake Bot (https://twitter.com/earthquakesLA) esetében megjelenik az említett ikon és szöveg, de az Earthquake Bot (https://twitter.com/earthquakeBot) esetében nem. Mindkét fiókot ugyanaz a felhasználó üzemelteti.

122 A Twitter különböző API-kat kínál a felhasználóknak többek között automatizálásra, adatgyűjtésre és akadémiai kutatásokra ingyenesen, azonban ez regisztrációhoz között. X/Twitter: Getting Started. About the Twitter API. https://developer.twitter.com/en/docs/twitter-api/getting-started/about-twitter-api#item0

123 X/Twitter: Automation rules. 2017. november 03. https://help.twitter.com/en/rules-and-policies/twitter-automation (a továbbiakban: Automation rules).

124 Uo.

125 Uo. X/Twitter Baseline Report 20.

126 Uo. X/Twitter Baseline Report 20.

127 Uo.

128 X/Twitter: Copypasta and duplicate content policy. 2022. május. https://help.twitter.com/en/rules-and-policies/copypasta-duplicate-content

129 Automation rules.

130 X/Twitter Baseline Report 19.

131 X/Twitter: Platform manipulation and spam policy. 2023. március. https://help.twitter.com/en/ rules-and-policies/platform-manipulation

Az X/Twitter kifejezetten spammelésre vonatkozó szabályzata is több esetet tartalmaz, amely szintén kiemeli az automatizált duplikációt mint tiltott tevékenységet több, ugyanazon személy (legyen az természetes vagy jogi személy) által üzemeltetett fiók között.[132] A platformon tilos továbbá az automatizált lájkolás, az X/Twitter fiókok nagy mennyiségű, agresszív vagy nem megválogatott követése vagy kikövetése – ideértve az olyan applikációkat, amelyek felhasználói követések növelését célozzák –, illetve tilos a felhasználók listához vagy *tweet*ek gyűjteményeihez hozzáadása nagy mennyiségben vagy válogatás nélkül.[133]

4.3. A Meta és az automatizáció

A Meta esetében szó szerinti említést a botokról a fejlesztői irányelvekben tesz a szolgáltató,[134] azonban minden szabályzat és irányelv alkalmazandó rájuk, amely a facebookos applikációkra vonatkozik, ugyanis a szolgáltató az applikáció fogalma alá sorolja a botokat.[135] Ennek oka, hogy az irányelvek megalkotásakor a szolgáltató elsősorban a csevegőbotokat tartotta szem előtt. [136] Ezeket az Appokat egyébként a Meta ellenőrzi.[137]

A Meta nevesítetten az alábbi kötelezettségeket rója a fejlesztőkre, illetve az alábbi tilalomfákat állítja fel:

- bot leírásának és kategóriájának folyamatos frissítése;[138]
- kapcsolatba lépés más fiókkal a másik fiók kifejezett hozzájárulása esetén, opt-out lehetőség biztosítása és a kapcsolat blokkolásának elfogadása;[139]
- emberi operátor hozzáférésének biztosítása az üzenetekhez (az Instagram esetében); [140]
- spammelés tiltása;[141]
- botok nagyon gyakori, manuális vagy automatikus létrehozásának tilalma.[142]

132 Uo.

133 Automation rules, X/Twitter Baseline Report 20.

134 Meta: Developer Policies. 2022. május 19. https://developers.facebook.com/devpolicy (a továbbiakban: Meta Developer Policies). Ez a helyzet 2016 óta nem változott, ld.: Nathalie Marechal: When Bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites. *International Journal of Communication,* vol. 10., (2016) 5026–5027.

135 Meta: Meta Platform Terms. 2023. április 25. 12. pont a) alpont. https://developers.facebook.com/terms

136 Marechal i. m. 5026.

137 Meta: Meta App Review. https://developers.facebook.com/docs/app-review/ (a továbbiakban: Meta App Review).

138 Meta Developer Policies 1. pont 5.

139 Uo. 8. pont 3/b. alpont.

140 Uo. 8. pont 9/b.

141 Spammelés alatt értendő a Facebook Közösségi Irányelvei alapján „[t]artalom közzététele, megosztása, arra való reagálás, valamint fiókok, csoportok, oldalak, események vagy más objektumok létrehozása manuálisan vagy automatikusan, rendkívül nagy gyakorisággal." Meta: Spam. https://transparency.fb.com/hu-hu/policies/community-standards/spam/. Az Instagram Közösségi Irányelvei nem határozták meg a spammelést, magyar fordításban mindössze kéretlen tartalom küldése szerepel. Instagram: Közösségi Irányelvek. 2022. https://www.facebook.com/help/instagram/477434105621119/?cms_id=477434105621119&maybe_redirect_pol=true A Facebook esetében bizonyos mutatók meghaladása esetén plusz feltételeket szabhat a platform, azonban ezekhez a feltételekhez a Developer Policy nem tartalmaz linket. Meta Developer Policies 5. pont 2.

142 Uo.

A CNA ábrájának megfelelően a botokra vonatkoznak a nem autentikus használatra vonatkozó tiltások is. A Meta 2023 júliusi riportjában az alábbi szabályzatokat nevezte meg e témakörben:

– nem autentikus használatra vonatkozó szabályok;
– koordinált nem autientikus használatra vonatkozó szabályok.[143]

Nem autentikus használatnak minősül többek között több Facebook-fiók használata, a többi felhasználó megtévesztése a fiók kezelőjének személyazonosságáról, a fiók vagy tartalom népszerűségéről, illetve a tartalom forrásáról vagy származásáról.[144] Koordinált nem autentikus használatnak minősül, ha több fiók és Facebook-oldal együttműködik más felhasználók megtévesztésében és ennek központi eleme a fiókok hamis volta.[145] A Meta az Instagram esetében nem nevesíti a hamis fiókokat a jelentésében, bár a szabályzatok mindkét platform esetében megegyeznek.[146]

4.4. Automatizáció a TikTok közösségi irányelveiben

A TikTok integritásra és hitelességre vonatkozó szabályzata tiltja azokat a tranzakciókat, amelyeknek tárgya az egyes tartalomelemek esetén az interakciók számának mesterséges növelése. Szankcióként pedig megemlíti az így keletkezett hamis like-ok és hamis követők törlését.[147] Ugyanezen szabályzat egy másik pontja tér ki a spammelés, más megszemélyesítésének és más felhasználók félrevezetésének tiltására.[148]

Spamfiókoknak tekinti a TikTok azokat a fiókokat, amelyeket együttesen üzemeltetnek, nem engedélyezett automatizáció segítségével üzemeltetnek vagy nagy mennyiségű üzleti üzenet küldése a céljuk. Ugyanezen kategóriába esnek azok a fiókok, amelyek hálózatban működnek, hasonló entitásokat személyesítenek meg és hasonló tartalmakat is tesznek közzé annak érdekében, hogy más fiókokhoz, tartalmakhoz vagy webhelyekhez vezessék a felhasználókat.[149]

Megszemélyesítés alatt pedig nemcsak valós személyek megszemélyesítése értendő, hanem nem létező személyeké is, ha a cél mások megtévesztése.[150] Paródiafiókok és rajongói fiókok természetesen működtethetők, d azzal a megkötéssel, hogy ennek szerepelnie kell a fiók megnevezésében.[151] Ugyanakkor megemlítendő, hogy a TikTok kifejezetten engedélyezi több fiók használatát, hogy több csatornát tudjon biztosítani a kreativitás kifejezésre.[152]

143 Meta Baseline report 44.
144 Meta: Inauthentic Behavior. https://transparency.fb.com/en-gb/policies/community-standards/inauthentic-behavior/
145 Uo.
146 Meta Baseline Report 44.
147 TikTok: Integrity and Authenticity. 2023. március. https://www.tiktok.com/community-guidelines /en/integrity-authenticity/#4
148 Uo.
149 Uo.
150 Uo.
151 Uo.
152 Uo.

5. Az ideális szabályozás kialakításának lehetőségei

A közösségi média nehezen kezelhető országos szinten, mivel többségében globális nagyvállalatokról van szó, ezért az állami szabályozást érdemes az ismertetett EU-s szabályokkal, azok közösségi irányelveivel összhangban kezelni. Korábbi tanulmányaimban[153] bemutattam, hogy a közösségimédia-botok csoportosítására többféle megoldás is született, azonban közülük igen kevésre reagáltak a jogalkotók és a platformok. Míg az Egyesült Államokban felmerült kifejezetten a politikai célra használt botok tiltása, addig az EU a dezinformáció terjesztésének megakadályozása kapcsán említi a botokat a DSA-ban, illetve a dezinformáció visszaszorítását célzó magatartási kódexben. A platformok esetében a Facebook szabályzatai igencsak szűkszavúan nyilatkoznak a botokról: az iránymutatások applikációközpontúak és leginkább az üzleti felhasználók által használt chatbotokra alkalmazhatóak. Esetükben a botokra az összes szabály általánosságban alkalmazandó, és kifejezetten a spammelés tiltásakor említik meg őket külön. Ezzel szemben az X/Twitter kifejezett szabályokkal rendelkezik arra vonatkozóan, hogyan engedélyezi az automatizációt és mire nem használhatók a botok, ez alatt értve elsősorban a spammelést.

Kiemelhető, hogy mind a jogszabályok, mind a közösségimédia-szolgáltatók szabályzatai sporadikus, egyes botkategóriákra és a szabályozási motivációknál említett jelenségek közül csak egy-egy jelenségre reagálnak. A felhasználók számára azonban szükség van egy átfogó, univerzális és tartalomfüggetlen szabályozásra,[154] amely segíti a döntéshozatalt, hogy az adott fiók automatizálható-e és ha igen, milyen tevékenység és hogyan végezhető vele. A szakirodalomban ismert ezzel ellentétes álláspont is, mely szerint a botok állami szabályozásának csak egyes botkategóriákra szabad vonatkoznia, és azokra is csak bizonyos kontextusban. Ezen álláspont szerint a szabályoknak csak a káros hatások enyhítésére kell szorítkoznia, mivel a beszédet szabályozó hatályos jogszabályok elegendőek, így csak frissíteni szükséges őket.[155]

A szabályozásnak több szinten kell megvalósulnia, azaz az alkalmazandó szabályokat és azok végrehajtását nem érdemes kizárólag az államokra vagy kizárólag a szolgáltatókra bízni. A tartalomszabályozás kapcsán Gorwa a szabályozás három fő szereplőjének az államokat, a civil szervezeteket és a vállalatokat nevezte meg.[156] A közösségimédia-botok esetében is ez a három szereplőtípus vehet részt a szabályozásban és a végrehajtásban. Ezek közül a tanulmány kifejezetten az állami szereplők és a platformok által megfogalmazott szabályokra szorítkozik, jelen fejezet pedig csak arra tesz javaslatot, hogy ezen szereplők között hogyan oszthatók meg a botok szabályozásának egyes aspektusai.

Ződi Zsolt a mesterséges intelligencia szabályozásának kapcsán megállapítja, hogy a szabályozásnak egyszerre kell vonatkoznia az államra, a vállalatra és a magánszemélyre is.[157] Álláspontom szerint mindezért a közösségimédia-botok kapcsán ugyanennek a három szereplőnek a szabályozása szükséges. Meg kell határozni, hogy mi az állam joga vagy kötelezett-

153 Kovács (2022) i. m.; Kovács (2023) i. m.

154 Marechal i. m. 5023.

155 Madeline Lamo – Ryan Calo: Regulating Bot Speech. *UCLA Law Review*, vol. 66., no. 4. (2019) 1026–1027.

156 Robert Gorwa: The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review,* vol. 8., no. 2. (2019). https://policyreview.info/articles/analysis/platform-governance-triangle-conceptualising-informal-regulation-online-content

157 Ződi i. m. 123.

sége, például használhat-e egyáltalán automatizált fiókokat és ha igen, akkor milyen célra,[158] illetve milyen közösségi irányelvek megalkotására és betartására kötelezheti a szolgáltatókat, és ezek végrehajtását hogyan ellenőrzi és szankcionálja. Azt állítom, hogy a válasz pozitív, az állam használhat botokat kifejezetten tájékoztatási céllal, akár rövid szöveges üzenetek formájában,[159] de csak azok számára, akik ehhez kifejezetten hozzájárulnak. Ennek oka, hogy a magyar internetezők – mint azt az összefoglalás későbbi részében ismertetem – jelentős mértékben a közösségi médiából tájékozódnak. Azt a célt, amit korábban az SMS-ek szolgáltak, ma már közösségimédia-üzenetekkel is el lehet érni, sőt nagyobb volumenben és hosszabb üzenetek is eljuttathatók a felhasználókhoz.[160]

A vizsgált szabályozásokban közös pont a transzparencia, azaz mindegyik valamilyen módon előírja a bot használója számára, hogy fedje fel annak bot voltát. Bár a szólásszabadság anonim módon is gyakorolható,[161] a transzparencia hagyományosan elfogadott a politikában, például a politikai hirdetések esetében előírás annak közzététele, hogy az adott hirdetést ki finanszírozta.[162] Ez a fajta transzparencia lehet korlátozó, ugyanis ha egy botnak tűnő fiók esetében szükség van annak bizonyítására, hogy nem botról van szó, akkor a legkézenfekvőbb módon az úgy lehetséges, hogy azonosítjuk a mögötte álló személyt.[163] A transzparencia-előírás ugyanakkor a közösségimédia-botok által terjesztett üzenetek automatikus korlátozásához vezethet.[164] A tapasztalat továbbá azt mutatja, hogy ha az emberi felhasználó tudatában van annak, hogy bottal lép kapcsolatba, akkor megváltozik a hozzáállása, illetve az is, hogy mennyire gondolja hitelesnek a fiók által közvetített tartalmat.[165] Mivel bár a botok szolgálhatnak szórakoztatási célokat és szerepet játszhatnak pozitív üzenetek láthatóvá tételében és terjesztésében is, nem lenne szerencsés, ha ez utóbbi üzenetek hitelességüket vesztenék pusztán annak folytán, hogy egy botfiók osztotta meg őket. Bár erre vonatkozó kutatás – tudomásom szerint – még nem született, nem gondolom, hogy például a földrengést jelző botok vagy szórakoztatóbotok esetében befolyásoló tényező lenne, ha a fiók mellett megjelenne a 'bot' kifejezés vagy a bot voltát jelző valamilyen szimbólum. Politikai üzenetek

158 Például a Meta nem autentikus használatra vonatkozó szabályai között kifejezetten szerepel, hogy tilos a részvétel külföldről vagy kormányok koordinált, nem autentikus tevékenységében.

159 A híres-hírhedt 2013. március 15-i SMS-ek mintájára hasonló tömeges üzenetküldés lehetséges a közösségi médiában is, amennyiben ehhez a felhasználó hozzájárul. Szűcs Gyula – Haász János – Tóth Balázs: Emberemlékezet óta nem volt ilyen bénázás. *Index.hu,* 2013. március 16. https://index.hu/belfold/2013/03/16/katasztrofa_minden_fronton/

160 Hasonló példa lehet, hogy a Covid19 elleni oltás regisztrációjakor megadott e-mail címre – amennyiben a regisztráló kérte – tájékoztatást is kapott a vakcinákkal és beadatásukkal kapcsolatban: https://www.nnk.gov.hu/ index.php/koronavirus-tajekoztato/912-elindult-a-regisztracio-a-vedooltasra. A kiküldött e-mailek tartalmával kapcsolatos problémákról ld. pl.: Bolcsó Dániel: A kormány olyasmire használja az oltási regisztrációkor megadott emailcímeket, amiről megígérte, hogy nem fogja. *Telex.hu,* 2022. január 11. https://telex.hu/koronavirus/ 2022/01/11/vakcinainfo-oltas-regisztracio-email-cim-adatkezeles-tajekoztato-level-jarvany-propaganda

161 Ld. például: Delfi AS v. Estonia no. 64569/09., 2015. június 15-i ítélet, 147. bek.

162 Hines i. m. 427–428., 431.

163 Hines i. m 429–430., John Frank Weaver: Everything is not 'Terminator': We need the California bot bill, but we need it to be better. *The Journal of Robotics, Artificial Intelligence & Law*, vol. 1., no. 6. (2018) 432–434. . https://search.informit.org/doi/10.3316/agispt.20200604031266

164 Lamo–Calo i. m. 1024–1025.

165 Candice Lanius – Ryan Weber – William I. MacKenzie Jr.: Use of bot and content flags to limit the spread of misinformation among social networks: a behavior and attitude survey. *Social Networking Analysis and Mining,* vol. 11., no. 32. (2021) 10–12.

és hírek esetében pedig kifejezetten pozitívnak tartom, ha a felhasználó kritikusan szemléli az adott üzenetet. Hasonló célt hivatott szolgálni a tényellenőrzés és a hírek mellett megjelenő hasonló hírek is: a 'bot' jelzés csak egy újabb eszközt jelent.

Továbbá a botokat – legyen az akár mesterséges intelligencia – kódok és nem jogszabályok vezérlik, így szükséges a jogszabályokat lefordítani kódra.[166] Ezt a fajta fordítást az engedélyezett tartalmak egy körének esetében már a szolgáltatók végzik, például az applikációk esetében,[167] amelyekért végső soron felelősséggel is tartoznak. Jómagam hasonló szabályozást tartok elképzelhetően a botok esetében is.

A transzparenciakövetelmény és az automatizáció ellenőrzése véleményem szerint a platform által biztosított API-kon keresztül megvalósítható. Amennyiben egy platform úgy dönt, hogy felületén megengedett az automatizált fiókok használata, akkor kötelező módon biztosítson ehhez megfelelő API-kat. Ezáltal egyrészt a platform maga automatikusan címkézheti a botfiókokat,[168] hiszen tisztában van azzal, mely fiókok használják az API-kat, másrészt akár beépített módon korlátozható a tevékenységük, például hogy hány üzenetet küldhetnek ki egységnyi idő alatt vagy hány oldal követőbázisához csatlakozhatnak.[169] Ráadásul az API-k biztosításának előírásával együtt a szolgáltatók számára is előírható gondossági kötelezettség, hogy gondoskodjanak megfelelő technikai korlátok felállításáról és ezek monitorozásáról, megszegésük esetén pedig a fiók megfelelő szankcionálásáról, például az API használatától való ideiglenes vagy végleges eltiltástól.

Politikai botok esetében nem értek egyet azzal, hogy a használatukat tiltani kellene. Ennek oka, hogy az emberi figyelmet tekinthetjük korlátos jószágnak, amely a közösségi média tartalmak esetében megoszlik a szórakoztató tartalmak és a (politikai) hírek között.[170] A magyar internetezők 75%-a használja hírfogyasztásra a közösségi médiát, de a megkérdezettek 55%-a csak azokat a híreket olvassa el, amelyek bekerülnek a hírfolyamukba. A megkérdezettek 53,7%-át pedig érdeklik az ellentétes álláspontok is, de csak akkor, ha azok szintén bekerülnek a hírfolyamba, és megkeresésük nem igényel erőfeszítést.[171] A figyelem korlátossága és a hírfogyasztási szokások miatt megengedhetőnek tartom a botok használatát politika tartalmak közvetítésére.

Persze a politikai botok használata sem lépheti át a szolgáltatók által felállított korlátokat. Amennyiben a szolgáltató tiltja az automatizációt, úgy a politikai botok használata is tiltott. Amennyiben engedélyezi az automatizációt, úgy nem tilthatja meg a politikai célú használatot. A spammelésre vonatkozó tiltást azonban a politikai botok sem kerülhetik meg. Ebben az esetben azt, hogy milyen kvantitatív mutatók esetén minősül a tartalom megosztása vagy

166 Lawrence Lessig: *Code: Version 2.0.* New York, Basic Books, 2006. 1–8.; Ződi i. m. 126–127.

167 Meta App Review, TikTok: Developer Guidelines. https://developers.tiktok.com/doc/ our-guidelines-developer-guidelines?enter_method=left_navigation

168 Ld. pl: X/Twitter FAQ.

169 Meta: Rate limits. https://developers.facebook.com/docs/graph-api/overview/rate-limiting/; X/Twitter: Rate limits. https://developer.twitter.com/en/docs/twitter-api/rate-limits; TikTok: Frequently Asked Questions. https:// developers.tiktok.com/doc/research-api-faq?enter_method=left_navigation

170 Andrew M. Guess – Benjamin A. Lyons: Misinformation, Disinformation, and Online Propaganda. In: Nathaniel Persily – Joshua A. Tocker: *Social Media and Democracy: The State of the Field, Prospects for Reform.* Cambridge, Cambridge University Press, 2020. 17., 21. https://doi.org/10.1017/9781108890960

171 Rab Árpád – Török Bernát: Bizalom, tudatosság, veszélyérzet az interneten. *Információs Társadalom*, 2020/3. 4. https://www.ludovika.hu/wp-content/uploads/2020/06/EJKK-ITKI_Bizalom-tudatossag-veszelyerzet-az-interneten.pdf

közzététele spammelésnek, a szolgáltatókra bíznám, mivel ők rendelkeznek azokkal az eszközökkel, amelyekkel ezt monitorozni tudják. A politikai botok esetében – a tartalom kényes volta miatt – a monitorozott mutatók közzététele szükséges, azaz melyek azok a mérőszámok, illetve az ezek alapján számított értékek, amelyek átlépésénél a szolgáltató beavatkozhat. Hasonló szabályozás nem idegen a magyar jogban, hiszen hasonló előírásokat találunk például a médiaszolgáltatók tekintetében a választási törvényben.[172] Ugyanakkor ezt az analógiát fenntartásokkal kell kezelni, mert a törvény a kampányidőszakra korlátozza a politikai hirdetéseket és kiköti, hogy ezért cserébe a szolgáltató nem fogadhat el ellentételezést. A közösségimédia-platformok esetében politikai tartalmú bejegyzésekkel találkozhat a felhasználó kampányidőszakon kívül is, továbbá arról is meglehetősen nehéz információt szerezni, hogy ha magáért a bejegyzés közzétételéért nem is, de a botok használatáért fizetett-e az üzenetet közvetíteni kívánó személy vagy szervezet. A platformok számára meglehetősen nehéz feladat az üzenetek kiegyenlített közvetítése, azonban ők rendelkeznek a megfelelő technikai eszközökkel az üzenetek monitorozására, illetve a nagy mennyiségű automatizált közzététel vagy üzenetküldés esetében pedig a korrigálásra.

172 A választási eljárásról szóló 2013. évi XXXVI. törvény 147–148. §.

II. Adatvédelem és digitális technológiák

Adatvédelem az online platformokon

Bálint János

1. Bevezetés

A digitális korban az online platformok váltak az információáramlás, a kereskedelem és a társadalmi kapcsolatok központjaivá, mely tevékenységek keretében jelentős mennyiségű személyes adatot gyűjtenek és kezelnek. Megkérdőjelezhetetlen, hogy az online platformok számos előnyt nyújtanak a felhasználóik részére. Egyrészt a közbeszéd számottevő része manapság a közösségimédia-platformokon zajlik, az országok többségében pedig elképzelhetetlen egy választási kampány lebonyolítása, a kormányzati döntések bejelentése, mozgalmak szervezése vagy éppen a közszolgáltatások nyújtása az online tér segítsége nélkül.[1] Az online kampányok elterjedését nagyban elősegíti a különféle választói csoportok motivációi által kialakított célzott politikai hirdetések elterjedése is.[2] Másrészt az online platformok algoritmikus irányítás és a rendelkezésre álló felhasználói adatok segítségével képesek a fogyasztói igényeknek megfelelően elosztani a szűkös erőforrásokat, miközben a folyamatos innovációnak és az éles digitális versenynek köszönhetően képesek úttörő termékeket és szolgáltatásokat piacra hozni.

Ezzel szemben egyesek szerint a Facebook egyenesen a cenzúra valaha ismert legnagyobb rendszerét működteti, hiszen több emberi kommunikációt szabályoz, mint bármelyik állam a történelem során, és mindezt az államoknál sokkal hatékonyabban is teszi.[3] Továbbá a személyre szabott tartalomkínálat hatására félő, hogy a felhasználók egyre jobban elszigetelődnek egymástól, valamint az eltérő nézőpontoktól, ezáltal növelve a társadalmi polarizációt és aláásva a demokratikus párbeszéd kialakulásának lehetőségét.[4] Ugyanakkor a megtévesztő és félrevezető adatalapú kereskedelmi gyakorlatok és sötét mintázatok jogszerűtlenül befolyásolhatják a kibertérben tranzakciós döntések millióit.[5] A digitális ökoszisztémák kialakulása következtében a domináns platformok által támasztott kereskedelmi korlátok ma már még jelentősebbek lehetnek, mint a nemzetállamok által támasztott kereskedelmi korlátok.[6]

Az online platformok valós társadalmi jelentőségének felismeréséhez szükség volt a Cambridge Analytica-botrányra, a Brexit- és Trump-kampányra, valamint a menekültválság idején

1 Susan Benesch: But Facebook's Not a Country, How to Interpret Human Rights Law for Social Media Companies. *Yale Journal on Regulation Online Bulletin*, vol. 38. (2020) 87.

2 Mráz Attila: Platformszabályozás és kampányszabályozás a demokráciában. In: Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora*. Budapest, NKE Ludovika Egyetemi Kiadó, 2022. 342.

3 Benesch i. m. 86.

4 Gálik Mihály: A hálózati hírmédia sajátosságai, különös tekintettel a visszhangkamra- és a szűrőbuborék-jelenségre. *In Medias Res*, 2019/2. 340.

5 Nicholas McSpedden-Brown: Consumer Policy: A Complement to Competition Policy in Tackling Dominant Online Businesses. *Competition Policy in Eastern Europe and Central Asia*, *OECD–GVH Newsletter,* no. 16. (2021) 12. https://caa.gov.al/wp-content/uploads/2023/05/oecd-gvh-newsletter16-mar2021-en.pdf

6 Firniksz Judit: Rangsorolás – Új szabályozási igény a platformok és az információs túlterheltség korában. In: Valentiny Pál et al. (szerk.): *Verseny és szabályozás 2021*. Budapest, KRTK Közgazdaságtudományi Intézet, 2021. 173.

elszabadult gyűlöletbeszédre.[7] Az orosz–ukrán háború és a Covid19 során terjedő dezinformációs kampányok még időszerűbbé tették a szabályozási beavatkozást.[8] Az uniós és tagállami jog, valamint gyakorlat jelenleg is igyekszik megtalálni az egyensúlyt az online platformok egyre csak növekvő térnyerése és adatéhsége, az innováció szükségessége, valamint az egyének magánéletének és személyes adatainak védelme között. E körben alapvető jogszabály a mára majd öt és fél éve a tagállamokban egységesen alkalmazandó általános adatvédelmi rendelet.[9] Az online platformok nyújtotta különféle szolgáltatásokhoz kapcsolódó adatkezelések céljait és eszközeit az azokat üzemeltető technológiai óriások határozzák meg, ezáltal a GDPR fogalomrendszerében adatkezelőnek minősülnek.[10] A GDPR számos, az online platformok működése körében kulcsfontosságúnak tekinthető kérdést szabályoz, a vonatkozó előírásoknak való megfelelés pedig az adatkezelők felelőssége.

Először, a felhasználó által adott hozzájárulás önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű jellege számos esetben kérdőjeleződik meg a szolgáltatások *take it or leave it* jellemzői, valamint a különböző forrásokból gyűjtött adatok összekapcsolásának kötelező volta kapcsán.[11] Másodszor, az érintetti joggyakorláshoz elengedhetetlen információk sok esetben hiányosak, pontatlanok, homályosan megfogalmazottak vagy több különböző dokumentum összeolvasása esetén ismerhetik meg azokat a felhasználók, mely gyakorlat által sérülhetnek az érintett tájékoztatására irányadó rendelkezések, valamint az átláthatóság elve.[12] Harmadszor, az adattakarékosság elve és a beépített és alapértelmezett adatvédelem követelménye alapjaiban mond ellent az online platformok alapvető működési modelljének, a felhasználókról való minél szélesebb körű adatgyűjtés gyakorlatának.

A GDPR alkalmazandóvá válása óta a tíz legnagyobb mértékű bírságot online platformot üzemeltető technológiai céggel szemben szabták ki.[13] Egy friss riport alapján pedig a bírságok harmada a gyermekek személyes adatainak kezelése kapcsán azonosított hiányosságok miatt született.[14] A konkrét bírságok alapjául szolgáló jogsértések pedig a fentebb említett három fő csomópont köré csoportosíthatók. Jelen tanulmány témája e csomópontok részletes

7 Polyák Gábor et al.: Versenyjogi előzmények és piacszabályozási eszközök a digitális piacokról szóló európai rendelet tervezetében. In: Valentiny (szerk.) i. m. 150.

8 Lendvai Gergely Ferenc: Media in War: An Overview of the European Restrictions on Russian Media. *European Papers*, vol. 8., no. 3. (2023); Lina Warnke – Anna-Lena Maier – Dirk Ulrich Gilbert: Social media platforms' responses to COVID-19-related mis- and disinformation: the insufficiency of self-governance. *Journal of Management and Governance*, vol. 28. https://doi.org/10.1007/s10997-023-09694-5

9 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, HL L 119, 2016. 05. 04. (a továbbiakban: GDPR), 1–88.

10 Christian Kurtz et al.: Accountability of platform providers for unlawful personal data processing in their ecosystems – A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR. *Journal of Responsible Technology*, vol. 9. (2022) 8. https://doi.org/10.1016/j.jrt.2021.100018

11 Beatriz Kira – Vikram Sinha – Sharmadha Srinivasan: Regulating digital ecosystems: bridging the gap between competition policy and data protection. *Industrial and Corporate Change*, vol. 30., no. 5. (2021) 1353–1354.

12 Milou Jansen: *User-Privacy and Personal Data on Online Platforms* [Academic paper]. Universität Salzburg, 2017. február 25. 6. https://www.academia.edu/32116881/User_Privacy_and_Personal_Data_on_Online_ Platforms

13 CMS, GDPR Enforcement Tracker. https://www.enforcementtracker.com

14 Surfshark: ⅓ of social media's GDPR fines linked to children. *Surfshark.com,* 2023. november 7. https://surfshark.com/ research/chart/social-media-gdpr-fines#

bemutatása az elmúlt évek uniós adatvédelmi hatósági és bírósági gyakorlatán keresztül. Szintén hangsúlyos szerepet kapnak jelen tanulmány keretében az adatvédelmi hatóságok által közzétett, jogi kötőerővel nem bíró iránymutatások. A proaktív jogalkalmazói fellépés ugyanis egyrészt segít az elhúzódó hatósági eljárások elkerülésében, másrészt a GDPR általánosságban megfogalmazott követelményeit konkretizáló gyakorlatias javaslatok nagyban elősegítik az adatkezelők adatvédelmi megfelelését.

Jelen bevezetést követően a 2. pont röviden ismerteti az online platformok közös jellemzőit, az elterjedésük fő mozgatórugóit. A 3. pont összefoglalja az online platformok által nyújtott szolgáltatásokhoz kapcsolódó adatkezelések esetén alkalmazható jogalapok közül az érintett hozzájárulásának követelményeit, valamint a gyakorlatban felmerülő legelterjedtebb jogsértéseket. Ezt követően, a 4. pont jó gyakorlatokat mutat be az érintettek GDPR által lefektetett jogai gyakorlásának előfeltételeként nyújtott átlátható tájékoztatás körében, majd ismerteti a technológiai óriások gyakorlatának vonatkozó hiányosságait. A 5. pont a beépített és alapértelmezett adatvédelem, mint a GDPR előírásainak teljesítéséhez és az érintett jogainak védelméhez szükséges garanciák folytonos figyelembevételét járja körül az adatkezelő által teljesítendő konkrét kötelezettség, valamint a kapcsolódó adatvédelmi hatósági döntések elemzése által. A 6. pont kitekintésként azonosítja a jelen, valamint a közeljövő nyitott kérdéseit az online platformok adatvédelmi megfelelése terén. Végezetül a 7. pont összefoglalja a tanulmány legfontosabb megállapításait.

2. Az online platformok sajátosságai

A platform alapvetően egy felforgató, más néven romboló technológia (*disruptive technology*), hiszen „a hatályos jogi kereteket feszegeti" és „a korábbi technológiai szinthez igazodó szabályozási eszközök elégtelenné, vagy éppen túlszabályozóvá válhatnak."[15] A platform azonban nem egyszerűen egy új üzleti modell, egy új társadalmi technológia vagy egy új infrastrukturális alakzat. A platform az információs társadalom alapvető szervezeti formája, egy 'általános kontrollmechanizmus'.[16] A platformok nem belépnek a piacokra vagy bővítik azokat, hanem felváltják őket.[17] A digitális környezetben az információhoz való hozzáférés, sokszorosítás és terjesztés minimális határköltségei versenyelőnyhöz juttatják a platformokat a már létező struktúrákkal szemben, és lehetővé teszik számukra, hogy egy minimális, algoritmusalapú infrastruktúra által ellenőrizzék és irányítsák szolgáltatásaik nyújtását több millió ember részére.[18]

Az online platformok ún. kétoldalú piacokon működnek, melyek „két, egymástól jól elkülönülő csoporttal jellemezhető[k], amely csoportok találkozásánál az igénynek megfelelő

15 Klein Tamás: A közösségi (média)platformok társadalmi integrációs és dezintegrációs hatásai. *Glossa Iuridica*, 2020/1–2. 71.

16 Ződi Zsolt: Algoritmikus koordináció a platformuniverzumban. A platform mint új koordinációs mechanizmus és ennek jogi következményei. In: Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai*. Budapest, NKE Ludovika Egyetemi Kiadó, 2021. 492.

17 Julie E. Cohen: Law for the Platform Economy. *U. C. Davis Law Review*, vol. 51. (2017).

18 Giovanni Sartor: The secondary liability of online intermediaries. In: Pier Luigi Parcu – Elda Brogi (szerk.): *Research Handbook on EU Media Law and Policy*. Cheltenham, Edward Elgar, 2021. 142.

szolgáltatás nyújtása révén egy közvetítő áll."[19] Ezzel szemben létezik olyan nézet is, mely szerint a platform valódi célja nem a közvetített tranzakciók utáni jutalék beszedése, hanem a tranzakciók közben kinyert adattömeg monetarizálása. Vagyis a két- vagy többoldalú piaci jelleg előtérbe helyezése csak leplezi a valódi működést.[20]

A platformok közös jellemzője, hogy minden kommunikációt adattá alakítanak, algoritmikusan vezérelnek, áruvá változtatnak, végső soron pedig pénzzé teszik, hasznosítják. Ezenkívül a platformok egy meghatározott területen jelentős súllyal bírnak, és arra törekednek, hogy minél nagyobb számú felhasználót érjenek el.[21] E kettő tulajdonság egy szinte öngerjesztő folyamatot eredményez, ahol „minél többen használják az adott platformot", „annál nagyobb adatmennyiség generálódik", és „minél nagyobb mennyiségű adat generálódik", annál többen csatlakoznak a platformhoz, az egyre inkább személyre szabott szolgáltatás miatt.[22]

További jellemzőjük a zéró áras üzleti modell, vagyis a felhasználók pénzbeli ellenszolgáltatás helyett, a személyes adataikkal és a figyelmükkel fizetnek a szolgáltatásért.[23] A fogyasztók lényegesen nagyobb valószínűséggel választanak egy ingyenes terméket, mint egy hasonló, nem ingyenes terméket, még akkor is, ha az ingyenes termék rosszabb minőségű.[24] Szintén ide kapcsolódik az adatvédelmi paradoxon (*privacy paradox*), mely alapján annak ellenére, hogy a felhasználók tisztában vannak az ezzel járó adatvédelmi kockázatokkal, továbbra is apránként feladják a magánéletüket, mivel túl gyakran és túl olcsón adják ki az adataikat.[25]

A platformok versenyjogi vonatkozású sajátossága, hogy a felhasználók bizonyos számának elérése (ún. kritikus tömeg) esetén könnyen monopolhelyzet alakulhat ki. A hálózati hatás következtében ugyanis a felhasználók azon platformokhoz csatlakoznak, ahol már alapból minél több felhasználó van jelen, a kilépés költségei pedig ezáltal egyre súlyosabbak lesznek. A platform a méretgazdaságosság következtében végezetül kiszorítja a piacról a többi versenytársat.[26] Az ún. *tipping point* elérése után a verseny már nem a piacon, hanem a piacért folyik. Mindezek következtében a felhasználóknak nincsen többé reális lehetősége, hogy szolgáltatást váltsanak. Az extrém megtérülési ráta és a külső hálózati hatások miatt az inkumbens vállalkozás rendkívüli piaci fölényre tesz szert.

Mindezt kiegészíti a domináns platformtól eltérő szolgáltatások igénybevételének (*multihoming*) megnehezítése és a különböző forrásokból gyűjtött és összekapcsolt adatok által előidézett, a 'győztes mindent visz' jelenség. A platformokon belül a keresőmotorok kifeje-

19 Szabó Endre Győző: A kétoldalú piacok elmélete és a személyes adatok védelme – a Google-ítélet elemzése versenyjogi és adatvédelmi szempontok szerint. *In Medias Res*, 2017/1. 173.

20 Ződi Zsolt: A platform mint elméleti konstrukció és mint narratív keret – A platformfogalom kialakulásának történetei. In: Török–Ződi (szerk.) (2022) i. m. 27–28.

21 Ződi Zsolt: *Platformok, robotok és a jog*. Budapest, Gondolat, 2018. 102–103.

22 Pók László Gábor: Védeni vagy megosztani? – A személyes adatok szerepe az internetes platformok szabályozásában. In: Török–Ződi (szerk.) (2022) i. m. 381.

23 Tóth András: Fogyasztóvédelmi, adatvédelmi, médiajogi és versenyjogi eszközök együttes alkalmazása az online figyelempiacok kudarcainak kiküszöbölésére. *Infokommunikáció és Jog*, 2021/77. 8.

24 Pásztélyi Emese – Bordács Bálint: Competition concerns in zero price markets. *Versenytükör*, 2020/2. 27.

25 Giancarlo F. Frosio: Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility. *Oxford International Journal of Law and Information Technology*, vol. 26., no. 1. (2018) 10. https://doi.org/10.1093/ijlit/eax021

26 Ződi (2018) i. m. 109.

zetten olyan szolgáltatások, „amelyek működésével kapcsolatban a felhasználó nagyon kevés információval rendelkezik, ezért a kockázatok csökkentése érdekében hajlamos a már bevált szolgáltatást igénybe venni."[27] Ez a jelenség az ún. 'automatikus beidegződés', miszerint „a felhasználó számára ismeretlen típusú oldalakat a Google segítségével keres meg".[28] Napjainkban „az online platformokon való jelenlét nem kényelem vagy szabad döntés, hanem társadalmi elvárások kérdése."[29]

3. Hozzájárulás

A GDPR által lefektetett elvek között első helyen szerepel a jogszerűség,[30] mely alapján az adatkezelők kötelesek az adatkezelést megelőzően meghatározott, konkrét adatkezelési céljaikhoz hozzárendelni a GDPR által lefektetett jogalapok egyikét. Az adatkezelési célok között megkülönböztetett szerepet tölt be az érintett hozzájárulása,[31] hiszen azt az érintett bármikor ugyanolyan egyszerű módon visszavonhatja, amilyen egyszerű módon az eredeti hozzájárulását megadta,[32] ezáltal számottevő hatást gyakorolhat az őt érintő adatkezelés időtartamára és kiterjedtségére. Az érintett hozzájárulása egyébiránt „az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez."[33] A hozzájárulás annyiban érvényes, amennyiben a fogalmi elemek közül valamennyi maradéktalanul teljesül.

3.1. Iránymutatások

3.1.1. A hozzájárulás önkéntes jellege

A hozzájárulás önkéntességének előfeltétele, hogy az érintett valós és szabad választási lehetőséggel rendelkezzen, vagyis lehetősége legyen anélkül megtagadni vagy visszavonnia hozzájárulását, hogy abból kára származna.[34] Például nem önkéntes az adatkezeléshez való hozzájárulás, amennyiben azt olyan szerződés teljesítésének vagy szolgáltatás nyújtásának feltételéül szabták, mely szerződés teljesítéséhez vagy szolgáltatás nyújtásához nem szükséges az adott személyes adatok kezelése.[35] Vagyis a hozzájárulásra való felkérés „nem gátolhatja szükségte-

27 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. 109.
28 Polyák Gábor – Pataki Gábor: Google Shopping: a 2017-es versenyjogi „gigabírság" elemzése, avagy milyen tanulságokkal szolgált a keresőmotorra kiszabott rekordbüntetés. In: Polyák (szerk.) (2020) i. m. 276.
29 Pünkösty András: Egy új digitalis etika megalapozásának egyes szempontjai – big data, algoritmusos döntéshozatal és a személy az adatalapú társadalomban. In: Török–Ződi (szerk.) (2021) i. m. 60.
30 GDPR 5. cikk (1) bekezdés *a)* pont.
31 GDPR 6. cikk (1) bekezdés *a)* pont.
32 GDPR 7. cikk (3) bekezdés.
33 GDPR 4. cikk 11. pont.
34 GDPR (42) preambulumbekezdés.
35 GDPR 7. cikk (4) bekezdés.

lenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kérik",[36] például azáltal, hogy az a szerződéses feltételek nem megtárgyalható részébe van foglalva.[37]

Nem tekinthető önkéntesnek a hozzájárulás, amennyiben az érintett számára nincsen lehetőség külön-külön hozzájárulni a különböző személyes adatkezelési műveletekhez.[38] Az esetben is sérül a hozzájárulás önkéntes volta, amennyiben az egyetlen egyszerű kattintással megadható, azonban a visszavonása hosszas erőfeszítéseket és egy komplex többlépcsős folyamat teljesítését igényli az érintett részéről.[39] Szintén GDPR-ellenes az érintett folyamatos, rendszeres jellegű felkérése a hozzájárulásának megadására, amennyiben azt korábban már visszautasította, mivel az ilyen módon előbb-utóbb beszerzett hozzájárulás sem az érintett szabad akaratán alapult.[40]

Online szolgáltatások esetén a hozzájárulás önkéntességének körében alapvető kérdés, hogy az érintett felhasználó a további célokra vonatkozó hozzájárulás megtagadása esetén is hozzáfér-e az adatkezelő egyenértékű (alap)szolgáltatásához. Például amennyiben a személyre szabott hirdetési szolgáltatások elutasítása esetén a felhasználó nem tudja használni az adott online platformot, valószínűleg nem tekinthető önkéntesnek az esetlegesen megadott hozzájárulása. Tekintettel az online piacokon jellemző kiterjedt piaci részesedéssel rendelkező vállalatokra, valamint a tényleges alternatívák hiányára, az Európai Adatvédelmi Testület (angolul: European Data Protection Board, a továbbiakban: EDPB) úgy foglalt állást, hogy az 'egyenértékű szolgáltatás' feltétele csak az adott adatkezelő vonatkozásában vizsgálandó. Vagyis a jelen bekezdésben részletezett módon beszerzett hozzájárulás akkor sem tekinthető érvényesnek, amennyiben a megtagadása vagy visszavonása esetén az érintett felhasználó igénybe tudná venni egy versenytársa egyenértékű szolgáltatását.[41]

Szintén aggodalomra adhat okot, amennyiben a megfogalmazás vagy egyéb kapcsolódó vizuális elemek egy bizonyos választási lehetőség felé terelik a felhasználót, befolyásolva ezáltal döntésében. A túlzóan negatív vagy pozitív hangvételű, esetleg felszólító vagy fenyegetőző jellegű hozzájárulásra felkérések arra késztethetik az érintett felhasználókat – és különösen a gyermekeket, valamint a sérülékeny csoportokhoz tartozó egyéneket –, hogy több adatot osszanak meg magukról, mint amennyi feltétlenül szükséges lenne.[42] Hasonló eredménnyel járhat a hozzájárulás megadását jelentő lehetőség vizuális – például színbeli – kiemelése, valamint a megtagadás elrejtése, például halványabb szín, kisebb betűtípus alkalmazásával.[43]

3.1.2. A hozzájárulás konkrét és megfelelő tájékoztatáson alapuló jellege

Az érintett hozzájárulása annyiban érvényes, amennyiben azt az egyes adatkezelési célok tekintetében egymástól függetlenül is megadhatja, vagyis a választási lehetősége nem kor-

36 GDPR (32) preambulumbekezdés.

37 EDPB: 5/2020 Iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról, 2020. május 4. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_hu.pdf [a továbbiakban: EDPB (2020a)] 8.

38 GDPR (43) preambulumbekezdés.

39 EDPB: Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 2023 február 14. 21. https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_ deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

40 Uo. 17.

41 EDPB (2020a) i. m. 13.

42 EDPB (2023) i. m. 19–20.

43 Uo. 22.

látozódik az összes adatkezelési cél egységként történő elfogadására vagy elutasítására.[44] A megfelelő tájékoztatás kötelezettsége azt jelenti, hogy az adatkezelő köteles legalább az adatkezelő személyének kilétét és a személyes adatok kezelésének a célját az érintett rendelkezésére bocsátani a hozzájárulásának begyűjtését megelőzően.[45] Az EDPB iránymutatása alapján ezeken túlmenően az adatkezelő köteles az érintett tudomására hozni az adatkezeléssel érintett adattípusokat, a hozzájárulás visszavonásának lehetőségére való utalást, az automatizált döntéshozatalra vonatkozó tájékoztatást, valamint az esetleges harmadik országba vagy nemzetközi szervezetek részére történő adattovábbítás megfelelőségi határozat és megfelelő garanciák hiányából fakadó lehetséges kockázatait.[46] Az egyesült királyságbeli adatvédelmi hatóság (angolul: Information Commissioner's Office, a továbbiakban: ICO) ezzel szemben az adatkezelő személyének kilétén és a személyes adatok kezelésének célján túl, csak az adatkezelési műveletekre és a hozzájárulás visszavonásának lehetőségére való utalást várja el.[47]

3.1.3. A hozzájárulás egyértelmű jellege

Az érintett hozzájárulását megteheti írásban, szóban vagy elektronikus úton is, például a megfelelő négyzet bejelölésével, gomb megnyomásával vagy kattintással. Minden esetben elvárt azonban az érintett aktív közreműködése, vagyis a hallgatás, passzivitás, továbbgörgetés, az előre bejelölt négyzet nem minősülnek érvényes hozzájárulásnak.[48] Ez utóbbit ítéletében az Európai Unió Bírósága (a továbbiakban: EUB) is megerősítette.[49] Az olyan kreatív adatkezelői megoldások is ellentétesek az egyértelmű hozzájárulás követelményével, mint az *opt-out*-négyzetek. Ilyen esetben az érintett aktív eljárása – a négyzet bepipálása – szükséges a hozzájárulás megtagadásához.[50] A magyar adatvédelmi hatóság (Nemzeti Adatvédelmi és Információszabadság Hatóság, a továbbiakban: NAIH) pedig olyan megoldással is találkozott már hatósági ellenőrzés során, hogy az előre ki nem pipált négyzetet a rendszer automatikusan kipipálja a regisztráció elküldésekor.[51] A hozzájárulásnak el kell továbbá különülnie a szerződés vagy általános szerződési feltételek elfogadásától.[52]

3.1.4. Gyermekek hozzájárulása

Elterjedt tévhit, hogy a gyermekek személyes adatainak kezelése kizárólag érvényes hozzá-

44 GDPR (32) preambulumbekezdés.
45 GDPR (42) preambulumbekezdés.
46 EDPB (2020a) i. m. 17–18.
47 ICO: Lawful basis for processing, Consent, 2022. október 17. https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent-1-0.pdf [a továbbiakban: ICO (2022a)] 25.
48 GDPR (32) preambulumbekezdés.
49 C-673/17. sz. ügy Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. kontra Planet49 GmbH [ECLI:EU:C:2019:801].
50 ICO (2022a) i. m. 36.
51 NAIH: Tájékoztató a webáruházakra vonatkozó adatvédelmi követelményekről, 2017. február 17. 11. https://naih.hu/files/2017-02-17-webaruhaz-tajekoztato-NAIH-2017-1060-V.pdf
52 EDPB (2020a) i. m. 21.

járulásuk – esetleg a törvényes képviselőjük hozzájárulása – esetén jogszerű. Ezzel szemben a GDPR 6. cikk (1) bekezdésében található hat lehetőség bármelyike érvényes jogalap lehet ilyen jellegű adatkezelés esetén, azonban bizonyos esetekben – így a hozzájárulás körében is – további feltételeknek is meg kell felelniük az adatkezelőknek, amennyiben kiskorúak is igénybe veszik online szolgáltatásaikat.[53]

A közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezeléséhez a gyermekkorú érintettek – a korábbiakban ismertetett feltételek maradéktalan teljesülése esetén – 16 éves koruktól érvényes hozzájárulást adhatnak. A tagállamok lefelé eltérhetnek a 16 éves alsó határtól, és 13 évnél nem alacsonyabb életkort is megállapíthatnak nemzeti jogszabályukban.[54] Magyarországon az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény nem él az eltérés lehetőségével, azonban az Egyesült Királyságban például a 13 éves kor az irányadó.[55]

Az elvárt minimuméletkort el nem érő gyermekek esetén a szülői felügyeletet gyakorló személy adhat érvényes hozzájárulást az adott adatkezelés tekintetében.[56] E körben az adatkezelő felelőssége és kötelessége, hogy ésszerű erőfeszítéseket tegyen annak ellenőrzése érdekében, hogy az elvárt minimuméletkort el nem érő gyermekek esetében a szülői felügyeleti jogot gyakorló adta a hozzájárulást.[57] Kiemelendő, hogy a közvetlenül gyermekek részére nyújtott megelőzési és tanácsadási szolgáltatások gyermekek általi igénybevételéhez nincsen szükség a szülői általi hozzájárulásra, még akkor sem, amennyiben az érintett nem éri el a tagállamonként eltérően meghatározott minimális életkort.[58]

Szintén hangsúlyozandó, hogy jelen előírások nem érintik a hozzájárulástól eltérő jogalapon alapuló adatkezelések jogszerűségét, így kifejezetten a gyermek által kötött szerződések érvényességére, alakiságára vagy hatályosságára vonatkozó nemzeti jogszabályokat.[59] Az adatkezelő e körben is köteles biztosítani, hogy megfelel a gyermekek szerződéskötési képességére vonatkozó nemzeti jogszabályoknak.[60]

A GDPR 8. cikkének hatókörébe nem kizárólag a 'kifejezetten' gyermekeknek kínált online szolgáltatások esnek. Fordítva megközelítve a kérdést, csak azon szolgáltatások esnek kívül ezen cikk hatályán, melyeket kizárólag legalább 18 éves felhasználók részére nyújt az adatkezelő, és minden kapcsolódó tájékoztatás és reklám is ezt támasztja alá.[61] Vagyis 'közvetlenül gyermekeknek kínált' a szolgáltatás, amennyiben bármely felhasználó számára élet-

53 DPC: Fundamentals for a Child-Oriented Approach to Data Processing, 2021. december. https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf [a továbbiakban: DPC (2021a)] 22.

54 GDPR 8. cikk (1) bekezdés.

55 Data Protection Act 2018, 9. szakasz (a) pont.

56 GDPR 8. cikk (1) bekezdés.

57 GDPR 8. cikk (2) bekezdés.

58 GDPR (38) preambulumbekezdés.

59 GDPR 8. cikk (3) bekezdés.

60 EDPB: 2/2019 iránymutatás a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének *b)* pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében, 2019. október 8. 6. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_ consul tation_hu.pdf

61 EDPB (2020a) i. m. 31.

korra tekintet nélkül elérhető, vagy ha a minimális korhatáron alapuló korlátozások lehetővé teszik, hogy 18 év alatti gyermekek is igénybe vegyék azt.[62]

Bár a GDPR nem írja elő kifejezetten az adatkezelők számára az életkorellenőrzési mechanizmusok alkalmazását, a gyakorlatban ez sok esetben a GDPR 8. cikk szerinti hozzájárulás érvényessége szempontjából alapvető követelmény.[63] Az EDPB iránymutatása alapján egyes alacsony kockázatot jelentő szolgáltatások esetén elegendő lehet az életkor önbevalláson alapuló ellenőrzése, például a születési év vagy dátum megadása vagy egy egyszerű, az adott felhasználó nagykorúságára irányuló eldöntendő kérdés által.[64] Jó gyakorlat lehet technikai intézkedések alkalmazása, megakadályozva például azt, hogy egy 18 éven aluli életkort megadó gyermek rögtön újból kitölthesse az életkorára irányuló kérdést. A megfelelő adatvédelmi garanciák alkalmazása mellett szintén jó gyakorlat lehet a mesterséges intelligencián alapuló megoldások alkalmazása, melyek a szolgáltatás használata során tanúsított interakciói alapján képesek kiszűrni a kiskorú felhasználókat.[65] A legszigorúbb ellenőrzési módszereket az olyan szolgáltatások nyújtói kötelesek alkalmazni, amely szolgáltatások nyújtása illegális kiskorúak részére; erre jó példa a szerencsejáték vagy a felnőtt tartalmú weboldalak.[66]

Alacsony kockázattal járó adatkezelések esetében észszerű erőfeszítésnek minősülhet a szülői felügyeleti joggal rendelkező elektronikus elérhetőségének megszerzése, majd a hozzájárulás ilyen módon történő ellenőrzése. Az EDPB az adattakarékosság elvét is szem előtt tartva magasabb kockázatú szolgáltatások igénybevétele esetén harmadik fél általi ellenőrző szolgáltatások igénybevételét javasolja.[67] Ez utóbbi esetben szintén indokolt lehet a személyazonosító igazolványok bekérése vagy egy visszatérítendő pénzbeli szolgáltatás teljesítése átutalással vagy bankkártyás fizetéssel.[68]

3.2. Releváns hatósági gyakorlat

A francia adatvédelmi hatóság (franciául: Commission Nationale de l'Informatique et des Libertés, a továbbiakban: CNIL) 50 millió eurós (kb. 19,1 milliárd forint) bírságot szabott ki a Google LLC vállalattal szemben a hozzájárulás érvényességének hiánya, valamint az érintett tájékoztatására vonatkozó rendelkezések megsértése miatt.[69] A határozatot később helyben hagyta a francia legfelsőbb közigazgatási bíróság, az Államtanács (franciául: Conseil d'État) is.[70] A hatósághoz beérkezett panaszok azt sérelmezték, hogy az Android

62 ICO: Applications, Children and the GDPR, 2018. május 25. 24. https://ico.org.uk/media/for-organisations/ guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf.
63 DPC (2021a) i. m. 44.
64 EDPB (2020a) i. m. 32.
65 ICO: Age appropriate design: a code of practice for online services, 2022. október 17. https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code -guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.[a továbbiakban: ICO (2022b)]. 34.
66 DPC (2021a) i. m. 47.
67 EDPB (2020a) i. m. 32–33.
68 DPC (2021a) i. m. 42.
69 CNIL: Délibération SAN-2019-001. 2019. január 21. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT0000 38032552/.
70 Conseil d'État, 430810. 2020. június 19. https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042040546.

operációs rendszerrel rendelkező mobiltelefonok felhasználóinak el kellett fogadniuk a Google-szolgáltatások nyújtására irányadó felhasználási feltételeket és adatkezelési tájékoztatót, az elfogadás hiányában ugyanis nem használhatták a készüléküket. A CNIL érvelése alapjaként kiemelte, hogy bár a felhasználóknak lehetőségük volt a Google-fiók igénybevétele nélkül beállítaniuk a készüléküket, a felhasználói út Google általi kialakítása révén a felhasználók részére egyszerűbb volt ezen nyilatkozatok elfogadása, mint elutasítása.

A CNIL vizsgálata eredményeként megállapította, hogy a felhasználók hozzájárulása nem volt kellőképpen konkrét és egyértelmű. Egyrészt nem különült el a felhasználási feltételek elfogadásának, valamint a hozzájáruláson alapuló adatkezelések tekintetében a hozzájárulás megadásának az aktusa, mivel minderre egyetlen *checkbox* állt a felhasználó rendelkezésére. Másrészt a *checkbox* előre be volt pipálva, vagyis a felhasználó figyelmetlensége, passzívsága esetén is megadottnak tekintette a Google a hozzájárulást, annak megtagadása azonban aktív részvételt igényelt a felhasználótól. Harmadrészt a Google nem nyújtott lehetőséget az érintettek számára, hogy a különböző adatkezelési célok tekintetében külön hozzájárulást adjanak, kizárólag mindegyik adatkezelési célhoz való hozzájárulásra vagy azok elutasítására volt lehetőségük.[71]

Az ír adatvédelmi hatóság (angolul: Data Protection Commission, a továbbiakban: DPC) 405 millió eurós (kb. 155 milliárd forint) bírságot szabott ki az Instagram online platformot üzemeltető Meta Platforms Ireland Limited vállalattal szemben az Instagram üzleti fiók funkcióját használó gyermekek e-mail címeinek és/vagy telefonszámainak nyilvánosságra hozatala, valamint a gyermekek személyes Instagram-fiókjainak alapértelmezés szerinti nyilvánossága kapcsán. A végleges döntés szövege nem érhető el publikusan, így az alábbi esetelemzés az EDPB GDPR 65. cikke szerinti kötelező erejű döntésén keresztül mutatja be a DPC és az EDPB releváns megállapításait.[72]

A 2016-os bevezetéstől kezdve 2019 szeptemberéig az 'üzleti fiókra' (*business account*) váltó felhasználóknak – beleértve a gyermek felhasználókat is – kötelező volt e-mail címüket és/vagy telefonszámukat nyilvánosan feltüntetniük a felhasználó profilján. Pontosabban, az üzleti fiókváltási folyamat befejezéséhez a felhasználónak vagy egy e-mail címet vagy egy telefonszámot kellett megadnia. A privát Instagram-fiókkal rendelkező felhasználóknak pedig a fiókváltási folyamat részeként nyilvános fiókra kellett váltaniuk. Az Instagram üzleti fiókjaival összefüggésben nyilvánosságra hozott e-mail címek és/vagy telefonszámok nem titkosított módon és egyszerű szövegként láthatóak voltak bárki részére.[73]

Az üzleti fiókok esetében nyilvánosan elérhetővé tett elérhetőségekhez kapcsolódó adatkezelés jogalapjaként az Instagram a GDPR 6. cikk (1) bekezdés *b)* és *f)* pontjait jelölte meg, melyeket a DPC döntéstervezetében el is fogadott,[74] az EDPB azonban eltért ettől a minősítéstől a kötelező erejű döntésében. Egyrészt az elérhetőségek nyilvánosságra hozatala nem volt szükséges a felhasználókkal kötött felhasználási feltételek teljesítéséhez, mivel az csak általános utalásokat tartalmazott az üzleti fiókok létrehozásának lehetőségére vonatkozóan.[75] Másrészt kevesebb személyes adat kezelését lehetővé tévő opció is elérhető volt a

71 CNIL (2019) i. m.

72 EDPB: Binding Decision 2/2022. 2022. július 28. https://edpb.europa.eu/system/files/2022-09/edpb_binding decision_20222_ie_sa_instagramchildusers_en.pdf.

73 Uo. 10.

74 Uo. 11–12.

75 Uo. 30–31.

közvetlen üzenetküldés révén, vagyis az adatkezelő jogos érdekeinek érvényesítéséhez sem volt szükséges az adatkezelés.[76] Összességében az EDPB megállapította, hogy az Instagram nem rendelkezett az adatkezeléshez fűződő érvényes jogalappal, vagyis szükséges lett volna a gyermek felhasználók érvényes hozzájárulásának beszerzése.

Az ICO 12,7 millió fontos (kb. 5,66 milliárd forint) bírságot szabott ki a TikTok Information Technologies UK Limited és TikTok Inc. vállalatokkal szemben a gyermekkorú felhasználók személyes adatainak kezelése, valamint a kapcsolódó tájékoztatás hiányossága miatt.[77] A TikTok felhasználási feltételei alapján 13 évesnél idősebb felhasználók regisztrálhattak a platformra. Ehhez kapcsolódóan a regisztrációs folyamat során a leendő felhasználóknak meg kellett adniuk a születési dátumukat, azonban más módon nem erősítették meg, hogy valós adatot szolgáltattak-e.[78] A TikTok érvelésében kiemelte, hogy a regisztrációt követően is alkalmazott intézkedéseket a 13 évesnél fiatalabb felhasználók azonosítására és a profiljuk törlésére. Egyrészt összeállított egy listát olyan szavakról és szóösszetételekről, melyeket túlnyomórészt 13 év alatti felhasználók használtak a profilleírásukban, valamint a közzétett tartalmaikban. Másrészt azonban csak akkor minősítettek a felhasználói feltételekkel ellentétesnek egy adott fiókot, amennyiben a profil leírásában kifejezetten szerepelt, hogy a felhasználó 13 évesnél fiatalabb, és legalább 4 videója alapján arra a következtetésre jutott a TikTok moderátori csapata, hogy kinézete alapján az adott felhasználó valószínűleg nem éri el a megkövetelt életkort.[79]

Mindezek ellenére a hatóság becslése alapján az eljárás alapját képező időszak alatt 1,1 és 1,4 millió közötti 13 évesnél fiatalabb felhasználó használhatta a platformot, mely ezen egyesült királyságbeli korosztály 11–14%-át teszi ki.[80] A hatóság rendelkezésére bocsátott több belső dokumentum is tartalmazott a TikTok munkavállalóinak aggályairól szóló nyilatkozatokat a platformot használó 13 év alatti gyermekekkel kapcsolatos megközelítéssel kapcsolatban. Egyrészt a „kiskorúaknak címzett *livestream*-kommentek gyakran szexualizáltak és helytelenek", másrészt pedig a „kiskorúak száma vonzóvá teszi a TikTok-ot a [szexuális] ragadozók számára".[81] A TikTok továbbá nem tett erőfeszítéseket arra vonatkozóan sem, hogy a 13 évesnél fiatalabb felhasználók esetében ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte. Ennek megfelelően az ICO megállapította, hogy a TikTok elmulasztotta megfelelően korlátozni a platformjához való hozzáférést a 13 év alatti felhasználók számára, ami azt jelentette, hogy szülői hozzájárulás nélkül túl fiatal gyermekek is használhatták a platformot.

A DPC 210 millió eurós (kb. 80,5 milliárd forint) bírságot szabott ki a Facebook platformot üzemeltető Meta Platforms Ireland Limited vállalattal szemben, mivel érvényes jogalap nélkül kezelte a felhasználók személyes adatait a személyre szabott hirdetések megjelenítéséhez kapcsolódóan, valamint a vonatkozó átláthatósági kötelezettségeit sem teljesítette.[82]

76 Uo. 35.
77 ICO: TikTok Penalty Notice, 2023. április 4. https://ico.org.uk/media/4025182/tiktok-mpn.pdf.
78 Uo. 13.
79 Uo. 34–36.
80 Uo. 28.
81 Uo. 37–38.
82 DPC: IN-18-5-5, 2022. december 31. https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20DECISION%20%28ADOPTED%29%2031-12-22%20-%20IN-18-5-5%20%28Redacted%29.pdf [a továbbiakban: DPC (2022a)].

A DPC ezzel egyidőben és nagyrészt hasonló érvek mentén 180 millió eurós (kb. 70 milliárd forint) bírságot szabott ki az Instagram platform,[83] valamint 5,5 millió eurós (kb. 2,1 milliárd forint) forintos bírságot a WhatsApp alkalmazás vonatkozásában.[84] A vizsgált ténybeli háttér, jogi kérdések és hatósági érvelés hasonlósága folytán az alábbiakban kizárólag a Facebook szolgáltatás kapcsán hozott határozat kerül részletesen bemutatásra.

A GDPR alkalmazandóvá válásával a személyre szabott reklámok megjelenítéséhez kapcsolódó adatkezelés kapcsán, a Facebook az érintett hozzájárulásáról áttért a szerződés teljesítéséhez szükséges jogalapra. A korábban regisztrált felhasználóknak ehhez kapcsolódóan el kellett fogadniuk a módosított felhasználási feltételeket. Amennyiben ezt nem tették meg, a Facebook-fiókjukat törölték.[85] A felhasználási feltételek első sora szerint a Facebook egy személyre szabott szolgáltatás, mely reklámokat is tartalmaz.[86] Ennek ellenére, egyrészt a szerződés a személyre szabott reklámtevékenységet nem a Facebook szerződéses kötelezettségeként határozta meg, valamint nem is írt elő szankciót a hibás vagy nemteljesítés esetére. Másrészt a DPC kiemelte, hogy elérhetőek kevesebb személyes adatkezeléssel járó reklámozási lehetőségek, mint például a földrajzi elhelyezkedésen, használt nyelven vagy a tartalmon alapuló kontextuális hirdetések, melyekhez nem szükséges az érintettekről való profilalkotás.

Mivel a Facebook-használat és a Facebook felhasználási feltételek elfogadásának fő célja a felhasználók számára a másokkal való kommunikáció, nem pedig a személyre szabott reklámok fogadása, az ezen tevékenységhez kapcsolódó adatkezelés nem szükséges a szerződés teljesítéséhez.[87] A vonatkozó kötelező erejű döntésében az EDPB kiemeli, hogy egy ellenkező döntés kiüresítené a GDPR 6. cikk (1) bekezdés *b)* pontját, és elméletileg jogszerűvé tenné a személyes adatoknak az érintettel kötött szerződés teljesítésével kapcsolatos *bárminemű* gyűjtését és felhasználását.[88]

Az EDPB máshol annak a veszélyét is hangsúlyozza, hogy az adatkezelők minden egyes adatkezelési célt és műveletet az általános szerződési feltételeikbe foglalva az adattakarékosság elvének figyelmen kívül hagyásával maximalizálhatják az adatgyűjtésük és -kezelésük hatókörét.[89] Vagyis a GDPR 6. cikk (1) bekezdés *b)* pontjának alkalmazhatóságához nem elegendő a releváns adatkezelés szerződésben történő megemlítése.[90] Az adott adatkezelés 'szerződés teljesítéséhez szükséges' volta fokozott vizsgálatot igényel több különálló szolgáltatás vagy egy szolgáltatás egymáshoz nem kapcsolódó részeinek egyetlen szerződésbe foglalása esetén. Ez ugyanis 'kell vagy nem kell' (*take it or leave it*) választás elé állíthatja azon érintetteket, akik csak egyik szolgáltatást vagy a szolgáltatás egyik részét kívánják igénybe venni.[91]

Az EDPB érvelése alapján az online szolgáltatások jellemzőinek konkrét figyelembevételével a tartalmak személyre szabása adott esetben szükséges lehet az érintett felhasználókkal

83 DPC: IN-18-5-7, 2022. december 31. https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20Decision%20%28ADOPTED%29%20-%20IN-18-5-7%20-%2031-12-22%20%28Redacted%29.pdf [a továbbiakban: DPC (2022b)].

84 DPC: IN-18-5-6, 2023. január 12. https://www.dataprotection.ie/sites/default/files/uploads/2023-04/WhatsApp%20FINAL%20DECISION%20%28adoption%20version%29%20Redacted.pdf [a továbbiakban: DPC (2023b)].

85 DPC (2022a) i. m. 3.

86 Uo. 34.

87 Uo. 44–46.

88 Uo. 48.

89 EDPB (2019) i. m. 7.

90 Uo. 10.

91 Uo. 12.

fennálló szerződés teljesítéséhez. Ezzel szemben a személyre szabott hirdetésekhez kapcsolódó adatkezelés főszabály szerint nem alapítható a GDPR 6. cikk (1) bekezdés *b)* pontjában található jogalapra, még akkor sem, amennyiben az online viselkedésen alapuló hirdetések közvetve finanszírozzák az adott szolgáltatás nyújtását.[92] Ezt támasztja alá az a tény is, hogy az érintetteknek korlátlan joguk van a személyes adataik közvetlen üzletszerzés céljából történő kezelését megtiltani.[93] Ezzel megegyező következtetésre jutott az EUB is a Facebook által nyújtott személyre szabott hirdetések kapcsán.[94]

4. Az érintett tájékoztatása

Szintén elvi szinten deklarálja a GDPR, hogy az adatkezelők kötelesek a személyes adatok kezelését az érintettek számára átlátható módon végezni,[95] beleértve a személyes adatok gyűjtésének, felhasználásának, az azokhoz való hozzáférésnek, valamint az egyéb módon történő és tervezett kezelésének mértékét.[96] Elvi szinten elvárás, hogy az adatkezelő által biztosított átláthatóság segítségével az érintett meghatározhassa „az adatkezelés hatókörét és következményeit, valamint hogy a későbbiek folyamán ne okozzon meglepetést az érintettnek a személyes adatai felhasználásának módja."[97] A 29. cikk szerinti adatvédelmi munkacsoport (angolul: Article 29 Working Party, a továbbiakban: WP29) álláspontja szerint az 'összetett, technikai vagy váratlan' adatkezelések esetében a GDPR 13–14. pontjaiban meghatározott információkon túl az adatkezelés lehetséges kockázatait, következményeit és hatásait is az érintettek tudomására kell hozni.[98] Az adatkezelők konkrét kötelezettsége, hogy az érintettre vonatkozó személyes adatok kezeléséhez, valamint az érintettet megillető jogokhoz kapcsolódóan kötelezően nyújtandó tájékoztatás tömör, átlátható, érthető és könnyen hozzáférhető formájú, világos és közérthetően megfogalmazott legyen.[99] Hasonlóan a hozzájárulás érvényességéhez szükséges feltételekhez, jelen felsorolás is kumulatív jellegű, vagyis bármelyik fogalmi elem hiánya a GDPR sérelmét eredményezi.

4.1. Iránymutatások

4.1.1. Tömör és átlátható

Online környezetben a különböző adatkezelési műveletek változatossága és kiterjedt volta miatt alapvető fontosságú, hogy az információtúlterhelés helyett az érintettek hatékony módon juthas-

92 EDPB (2019) i. m. 16–17.
93 GDPR 21. cikk (1)–(3) bekezdés.
94 C-252/21. sz. ügy Meta Platforms és társai (Conditions générales d'utilisation d'un réseau social) [ECLI:EU:C:2023:537] 97–104. pont.
95 GDPR 5. cikk (1) bekezdés a) pont.
96 GDPR (39) preambulumbekezdés.
97 WP29: Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról, WP260 rev.01, 2018. április 11. 8. https://ec.europa.eu/newsroom/article29/items/622227
98 Uo. 8.
99 GDPR 12. cikk (1) bekezdés.

sanak érdemi információkhoz a személyes adataik kezelése kapcsán. A túlzott mértékű információ egyidejű elérhetővé tétele ugyanis kontraproduktív lehet, amennyiben elriasztja az érintetteket a személyes adataik kezelésére vonatkozó részletek megismerésétől. Ilyen esetben a megadott hozzájárulás érvényessége is megkérdőjeleződhet a megfelelő tájékozottság hiánya miatt.[100]

Az adatvédelmi tájékoztatást – a hozzájáruláshoz hasonlóan – el kell különíteni az egyéb szerződéses rendelkezésektől vagy általános szerződési feltételektől.[101] A NAIH ajánlása alapján adott esetben jó gyakorlatnak minősülhet egy kérdezz-felelek felépítésű adatkezelési tájékoztató vagy ahhoz kapcsolódó kiegészítés, mely „a leggyakrabban felmerült kérdésekről ad rövid, tömör és lényegre törő tájékoztatást."[102] Az átláthatóságot elősegítendő, javasolt tartalomjegyzéket is beilleszteni az adatkezelési tájékoztató elejére, valamint az esetleges módosítások esetén javasolt a korábbi verziókat is elérhetővé tenni, esetlegesen közérthető összefoglalót készíteni a változásokról.[103] Szintén jó gyakorlat a tájékoztatást táblázatos formában közzétenni, mely által az érintett egy sorban érheti el az adott adatkezelési célhoz kapcsolódó jogalapot, a kezelt személyes adatok körét, valamint az adatmegőrzés időtartamát.[104] Az egyre több hatóság által javasolt táblázatos forma elterjedésével az érintetteknek nyújtott adatvédelmi tájékoztatás egyre inkább a GDPR 30. cikke szerinti, az adatkezelők által vezetett belső adatvédelmi nyilvántartásra hasonlít formailag is.[105]

4.1.2. Érthető

Szintén alapvető követelmény, hogy az adatkezelő rendelkezzen bizonyos ismeretekkel az adatkezeléssel érintett személyek köréről, és a konkrét tájékoztatás szövegezésénél figyelembe vegye a célcsoport képességeit annak megértésére.[106] Például, amennyiben az adott online szolgáltatást – a határokon átnyúló jellege miatt – eltérő anyanyelvű érintettek is igénybe veszik, kötelező az adatkezelési tájékoztató lefordítása.[107] Továbbá, gyengénlátó vagy idős célcsoport esetében legyen technikai lehetőség a tájékoztatás betűméretének nagyítására, vak személyek esetében pedig a tájékoztató felolvastatására.[108]

4.1.3. Könnyen hozzáférhető

Annyiban valósul meg az átlátható tájékoztatás követelménye, amennyiben az adatkezelő proaktívan elősegíti az érintett információkhoz való hozzáférését, vagyis az érintetteknek nem

100 EDPB (2023) i. m. 16.
101 WP29 (2018) i. m. 7.
102 NAIH: Ajánlás az előzetes tájékoztatás adatvédelmi követelményeiről, 2015. október 9. 5. https://naih.hu/file / tajekoztato-ajanlas-v-2015-10-09.pdf
103 EDPB (2023) i. m. 25–26.
104 NAIH (2015) i. m. 5.
105 Alex Jameson: Instagram, Facebook and WhatsApp at the EDPB. *Privacy and Data Protection*, vol. 23., no. 4. (2023) 3.
106 WP29 (2018) i. m. 7.
107 ICO: Individual rights, The right to be informed, 2022. december 17. 40. https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed-1-0.pdf [a továbbiakban: ICO (2022c)].
108 NAIH (2015) i. m. 18.

kell további erőfeszítéseket tenniük azok felkutatása végett. Jó gyakorlat e körben, amennyiben az adatkezelési tájékoztatóra, vagy annak közvetett elérésére mutató link az adatkezelő által üzemeltetett honlap minden egyes oldalán elérhető.[109] Vagyis, „a tájékoztatás soha ne legyen »két koppintásnál távolabb«".[110] Szintén jó gyakorlat, amennyiben a regisztráció elküldésekor, a hozzájárulás megadásakor vagy a rendelés véglegesítésekor a *checkbox* kísérőszövegében elhelyezett link által az érintett egyből eljuthat az adatkezelési tájékoztatóhoz.[111]

A komplex adatkezelési műveleteket magában foglaló adatkezelések esetében jó gyakorlat lehet a többszintű adatkezelési tájékoztató alkalmazása. Az első szinten megjelenített információ ilyen esetben az adatkezelés céljára, az adatkezelő személyére, az érintett jogainak leírására, a második szinten található információk elérésére, valamint az 'összetett, technikai vagy váratlan' adatkezelések kockázataira, következményeire és hatásaira korlátozódhat; a második szint pedig a GDPR 13–14. cikkeiben meghatározott további vagy az összes információt tartalmazhatja egy helyen. Alapvető fontosságú e körben, hogy az egyes szintek nem tartalmazhatnak egymásnak ellentmondó információkat, a tájékoztatást következetes és egységes módon kell megadni.[112] Bár nem határozható meg pontosan, maximum hány szintből állhat az érintetteknek nyújtott tájékoztatás, e megközelítés sem hátráltathatja az érintettek jogainak gyakorlását azáltal, hogy az elszórtan fellelhető információkat az érintettnek kellene erőfeszítéseket téve összeollóznia.[113]

A WP29 e körben különbséget tesz '*push*' és '*pull*' értesítések között. '*Push*' értesítésnek minősülnek a '*just-in-time*' felugró ablakok, adatvédelmi értesítések, melyek a konkrét adatkezelési művelet megkezdését megelőzően tartalmaznak releváns adatvédelmi információkat. '*Pull*' értesítésre példa az 'adatvédelmi irányítópult', melynek segítségével az érintett tematikusan, adatkezelési célokhoz kapcsolódóan tájékozódhat, adhatja meg, valamint vonhatja vissza a hozzájárulását, tiltakozhat a személyes adatai további kezelése ellen.[114] Jó gyakorlat az egységes tájékoztató vonatkozó részeiben az adatvédelmi irányítópult megfelelő részeire mutató linkek elhelyezése.[115]

Az új információs technológiák megjelenésével és elterjedésével a könnyen hozzáférhető tájékoztatás fogalma is átalakul. Az ICO például IoT-eszközök (angolul: *Internet of Things*, azaz az internet segítségével egymással kommunikálni képes okoseszközök) esetében a hang-, fény-, rezgés- vagy haptikus jelzés alkalmazását javasolja meghatározott valós idejű adatgyűjtések esetén.[116]

4.1.4. Világos és közérthető

A tájékoztatás – hasonlóan a hozzájárulás beszerzéséhez – megadható írásban, szóban vagy elektronikus úton is.[117] Jó gyakorlat, amennyiben a személyes adatok gyűjtésének módjával

109 WP29 (2018) i. m. 8.
110 Uo. 9.
111 NAIH (2017) i. m. 14.
112 WP29 (2018) i. m. 11–12.
113 EDPB (2023) i. m. 30.
114 WP29 (2018) i. m. 22–23.
115 ICO (2022c) i. m. 50.
116 Uo. 57–58.
117 GDPR 12. cikk (1) bekezdés.

megegyező módon válik az érintettek részére elérhetővé a vonatkozó tájékoztatás.[118] Az írásos vagy adott esetben elektronikus úton biztosított információkat a lehető legegyszerűbben szükséges biztosítani, az összetett mondatok és komplex nyelvi szerkezetek, valamint a túlságosan jogi vagy technikai nyelvezet lehetőség szerinti mellőzésével. Szintén kerülendő a kétértelmű kifejezések, a feltételes mód és a szenvedő szerkezetek használata, melyek teret engedhetnek az érintettek eltérő értelmezésének. A WP29 kiemeli a szöveg megfelelő strukturálásának, valamint az eredetileg más nyelvről lefordított verziók nyelvtani és értelmi megfelelőségének a fontosságát is.[119] Ezzel szemben kerülendő ugyanazon információ több helyen, adott esetben több megfogalmazásban történő feltüntetése, mivel az hátráltathatja az érintettek általi megértését.[120] A NAIH pedig a példák minél szélesebb körű alkalmazását javasolja a közérthetőség biztosítása végett.[121]

4.1.5. Gyermekeknek szóló tájékoztatás

A gyermekeknek címzett információk esetében különös hangsúllyal bírnak az átlátható tájékoztatás egyes elemei.[122] A gyermekek különleges védelme – mint a GDPR egyik hangsúlyos eleme – megköveteli a gyermekeket érintő adatkezelés vonatkozásában az információ és kommunikáció olyan világos és közérthető nyelven való megfogalmazását, amelyet a gyermek könnyen megért.[123] E körben figyelemmel kell lenni többek között az alkalmazott szókincsre, hangnemre és stílusra.[124] A DPC kiemeli, hogy nem szükséges egy második, kifejezetten gyermekeknek szóló adatkezelési tájékoztató elkészítése, hiszen a gyermekek számára érthető információ a legtöbb esetben a többi felhasználói csoport vonatkozásában is teljesíti az átlátható tájékoztatás elvárását.[125] Amennyiben ugyanazon tájékoztatóból több verzió elérhető, jó gyakorlat közvetlenül a komplexebb vagy egyszerűbb változatra mutató link elhelyezése, hogy a gyermekek könnyedén válthassanak az érettségüknek és megértési képességüknek legjobban megfelelő szövegre.[126]

A konkrét szolgáltatás jellemzőitől függően például videómegosztóplatform-szolgáltatás esetén, valamint a szolgáltatás használatához igénybe vett eszköz figyelembevételével – például okostelefon, televízió, laptop vagy egyéb okoseszköz tekintetében – figyelemmel kell lenni a tájékoztatás elérhetőségének módjára is. Jó gyakorlat lehet a szöveges tájékoztató helyett vagy mellett egyéb vizuális megjelenítési módok alkalmazása is, például videók, képek, ikonok vagy rajzok által.[127] Az eredendően és elkerülhetetlenül komplex információkat tartalmazó tájékoztatás vagy a gyermekekre nézve kockázatosabb eredményeket jelentő válasz-

118 ICO (2022c) i. m. 45.
119 WP29 (2018) i. m. 9–11.
120 EDPB (2023) i. m. 28.
121 NAIH (2015) i. m. 4.
122 GDPR 12. cikk (1) bekezdés.
123 GDPR (58) preambulumbekezdés.
124 WP29 (2018) i. m. 11.
125 DPC (2021a) i. m. 27–28.
126 ICO (2022b) i. m. 40.
127 DPC (2021a) i. m. 29.

tási lehetőségek előtt ajánlott arra vonatkozó figyelmeztetés elhelyezése, hogy bizonytalanság esetén az érintett forduljon felnőtthöz.[128]

4.2. Releváns hatósági gyakorlat

A holland adatvédelmi hatóság (hollandul: Autoriteit Persoonsgegevens, a továbbiakban: AP) 750 ezer eurós (kb. 287 millió forint) bírságot szabott ki a TikTok Inc. vállalattal szemben, mivel az nem teljesítette a felhasználók, és kifejezetten a gyermekkorú érintettek tájékoztatásához kapcsolódó kötelezettségét.[129] Egy 2019 végén végzett indikatív felmérés szerint kb. 830.000 18 év alatti holland gyermek használta a TikTokot ez időben.[130] 2020 augusztusában pedig a holland felhasználók 28%-a, azaz kb. 1.260.000 felhasználó volt gyermekkorú.[131] Vagyis az adott jogsértés esetén kiszabott szankció kevesebb mint 1 eurónak felelt meg minden érintett kiskorú esetében.[132]

A regisztrációs folyamat során a leendő felhasználókat egy holland nyelvű szöveg tájékoztatta arról, hogy a regisztrációval elfogadják a TikTok felhasználási feltételeit és adatkezelési tájékoztatóját.[133] Azonban az adatkezelési tájékoztató mind a regisztrációs folyamat, mind az alkalmazás használata során kizárólag angol nyelven volt elérhető.[134] A TikTok a hatósági eljárás során előadta, hogy számos további intézkedést is eszközölt a felhasználók megfelelő tájékoztatása céljából. Egyrészt a felhasználók részletes adatvédelmi beállítások közül választhattak, az alkalmazás használata során adatvédelmi felugró ablakok tájékoztatták az érintetteket az őket érintő adatkezelés részleteiről, valamint a Súgóközpont (Help Centre) és a Biztonsági Központ (Safety Centre) is számos releváns információt tartalmazott. Másrészt a TikTok 2020 júliusában közzétette adatkezelési tájékoztatójának holland nyelvű összefoglalóját. Továbbá, a TikTok szerint a holland gyermekek angoltudása világszinten is kiemelkedő, így nem volt szükséges a részletes tájékoztató holland nyelvű közzététele.[135]

Az AP először is leszögezte, hogy irreleváns a holland gyermekek angoltudásának általános minősége, és a GDPR 12. cikke szerinti átlátható tájékoztatási kötelezettség körében alapvető, hogy amennyiben az adatkezelő egy bizonyos nyelvet használó felhasználók részére nyújt szolgáltatást, az adatkezelési tájékoztatóját is lefordítsa azon nyelvre. Bár az egyéb módon nyújtott információk és alkalmazott intézkedések hozzájárultak a nagyobb mértékű átláthatósághoz, nem helyettesítették az adatkezelési tájékoztató lefordításának követelményét, mivel a megkövetelt tájékoztatásnak csak részeit tartalmazták, valamint a Súgóközpont és a Biztonsági Központ esetében az érintettnek kellett erőfeszítéseket tennie az információk

128 Uo. 31.
129 AP: TikTok-döntés, 2021. április 9. https://autoriteitpersoonsgegevens.nl/uploads/imported/boete_tiktok.pdf.
130 Uo. 14.
131 Uo. 16.
132 Charles Tan – Katie Ta: *GDPR Case Study: Dutch DPA Fines TikTok Over Privacy Policy* [Project paper]. Brown University Computer Science Courses, Course CSI 2390Privacy-Conscious Computer Systems, 2021. 1–3. https://cs.brown. edu/courses/csci2390/2021/assign/gdpr/ctan-kta1-tiktok.pdf
133 AP (2021) i. m. 12.
134 Uo. 13.
135 Uo. 20.

felkutatása kapcsán.[136] A hatósági eljárás hatására a TikTok egyébként elkészítette az adatkezelési tájékoztatójának holland fordítását, valamint egy külön dokumentumot is, amely nyelvileg és tartalmilag is jobban megfelel a hollandul beszélő gyermekkorú felhasználók számára.[137]

A DPC 345 millió eurós (kb. 131 milliárd forint) bírságot szabott ki a TikTok közösségimédia-platformot üzemeltető TikTok Technology Limited vállalattal szemben a tisztességes eljárás, az átláthatóság és az alapértelmezett adatvédelem elvének többszöri megsértése miatt, kifejezetten a gyermekek adatait érintő adatkezelési tevékenységekkel összefüggésben.[138] Az alábbiakban a DPC érvelésének az érintettek tájékoztatása, valamint a gyermekek adatainak kezelése kapcsán született legfontosabb megállapításait mutatom be.

A TikTok mobilalkalmazásként és webes verzióban is elérhető. A mobilalkalmazáshoz regisztráció szükséges, de a webes változatot – korlátozott funkcionalitással – a nem regisztrált felhasználók is elérhetik, valamint megtekinthetik a felhasználó profiloldalának bizonyos tartalmait és a TikTok 'Neked' (*For You*) főoldalát. A TikTok általános szerződéses feltételei szerint 13 év alatti felhasználók nem használhatják a platformot.[139] A DPC érvelése ennek megfelelően a 13–18 év közötti felhasználók személyes adatainak kezelésére helyezi a hangsúlyt, de emellett kitér a TikTok életkorellenőrzési intézkedéseinek vizsgálatára is. A TikTok számos esetben és módon tájékoztatta a felhasználókat az adatkezelés részleteiről, ideértve a *just-in-time* értesítéseket, felugró ablakokat, az adatkezelési tájékoztatót és a gyermekek részére készült összefoglalót az adatkezelési tájékoztatóról.[140]

A DPC mindezek ellenére megállapította, hogy mindezen források nem tájékoztatják kellőképpen a felhasználókat arról, hogy nyilvános fiókjaikat a TikTok weboldalán keresztül korlátlan számú személy láthatja, beleértve a nem regisztrált felhasználókat is.[141] A DPC kifejezetten sérelmezte, hogy a 'nyilvános' (*public*), a 'mindenki' (*everyone*) és a 'bárki' (*anyone*) kifejezések félreérthető módon szerepeltek a dokumentumokban, mivel egyaránt vonatkozhattak regisztrált és nem regisztrált felhasználókra.[142] Mivel a TikTok elmulasztotta ezen megkülönböztetést – noha azt könnyen megtehette volna –, a DPC szerint a TikTok nem adott megfelelő tájékoztatást a gyermek felhasználóknak a személyes adataik címzettjeinek kategóriáiról.[143]

A CNIL fentebb hivatkozott határozata alapján a Google-fiók igénybevételét megelőzően, a felhasználók számára linkek segítségével elérhetők voltak a vonatkozó felhasználási feltételek és az adatkezelési tájékoztató, a regisztrációt vagy belépést követően pedig számos egyéb forrás útján is elérhetők voltak részükre az adatkezeléssel kapcsolatos információk. Például, a regisztrációt követően egy emlékeztető e-mail üzenetet kaptak az adatvédelmi beállításaik felülvizsgálata kapcsán, a Google-szolgáltatások igénybevétele során pedig számos felugró

136 Uo. 21.
137 Uo. 22.
138 DPC: IN-21-9-1. 2023. szeptember 1. https://edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf [a továbbiakban: DPC (2023a)].
139 Uo. 3–4.
140 Uo. 69.
141 Uo. 74., 80.
142 Uo. 78., 80.
143 Vö. GDPR 13. cikk (1) bekezdés *e)* pont.

ablak tájékoztatta a felhasználókat az adatvédelmi relevanciájú információkról.[144] A CNIL leszögezte, hogy az információk különböző dokumentumokban való elhelyezése a kötelezően nyújtandó tájékoztatás széttöredezettségéhez vezetett, a felhasználóknak pedig nagy mennyiségű információt kellett gondosan áttanulmányozni ahhoz, hogy megérthessék az őket érintő adatkezelés részleteit. Továbbá, egyes adatkezelési műveletek esetében 5–6 kattintás is szükséges lehetett az összes releváns részlet megismeréséhez.[145] Összességében a Google mint adatkezelő nem segítette elő a felhasználókat megillető jogok gyakorlásához kapcsolódó, kötelezően a rendelkezésükre bocsátandó információk megismerését. Bár tudtukra hozta az információk elérhetőségének a helyét, az alkalmazott kialakítás az érintettektől túlzottan aktív és kezdeményező szerepet várt el.

A fentebb hivatkozott kötelező erejű döntés alapjául szolgáló tényállás szerint az Instagram esetében az üzleti felhasználók e-mail-címének és/vagy telefonszámának kötelező jellegű nyilvánosságra hozatala kapcsán a fiókváltási folyamat során felugró ablak formájában nyújtott tájékoztatás nem is utalt ezen személyes adatok publikusan elérhető voltára. Az EDPB véleménye szerint ezáltal nem volt elvárható, hogy egy gyermek előre lássa az őt érintő adatkezelés részleteit és esetleges következményeit, kifejezetten azt például, hogy elérhetőségi adatainak nem kívánt nyilvános közzététele által bármilyen személy – beleértve azokat is, akikkel nem állt kapcsolatban vagy nem volt kapcsolata – közvetlenül kapcsolatba lépjen vele.[146]

A DPC 225 millió eurós (kb. 86 milliárd forintos) bírságot szabott ki a WhatsApp Ireland Ltd. vállalattal szemben a GDPR átláthatósági rendelkezéseinek megsértése miatt, a WhatsApp szolgáltatás felhasználói és az adatkezeléssel érintett egyéb személyek vonatkozásában.[147] A WhatsApp Ireland Ltd. az EUB előtt megtámadta az EDPB vonatkozó, kötelező erejű döntését,[148] azonban a Törvényszék elutasította a keresetet.[149] A WhatsApp Ireland Ltd. fellebbezése nyomán az eljárás jelenleg is folyamatban van az EUB előtt.[150]

A WhatsApp mobiltelefonos üzenetküldő alkalmazás használata során a felhasználóknak lehetőségük van arra, hogy hozzáférést adjanak a WhatsApp részére a készülékükön elmentett kontakt információikhoz. Ezáltal a WhatsApp nem felhasználó érintettek személyes adatait is kezelheti, igaz, az alkalmazott technikai megoldás miatt nem több, mint néhány másodpercig.[151] A felhasználók részére nyújtott kapcsolódó tájékoztatás kapcsán a DPC több esetben is megállapította, hogy azt csak töredékesen ismerhették meg az érintettek a felhasználási feltételeken, az adatkezelési tájékoztatón, valamint számos egyéb összefoglalón és körkörösen egymásra mutató linken keresztül. Ugyanazt az információt adott esetben több, egymásra mutató forrás is tartalmazhatta, kisebb-nagyobb szövegszerű eltérésekkel. A tájékoztatás hasonló módon való megfogalmazása miatt a felhasználóknak kellett erőfeszítéseket tenniük az információk több forrásból való felkutatása során, valamint adott esetben a

144 CNIL (2019) i. m.
145 Uo.
146 EDPB (2022) i. m. 39.
147 DPC: IN-18-12-2, 2021. augusztus 20. https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf [a továbbiakban: DPC (2021b)].
148 EDPB: 1/2021. sz. kötelező erejű döntés, 2021. július 28. https://edpb.europa.eu/system/files/2022-03/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_hu.pdf
149 T-709/21. sz. ügy WhatsApp Ireland kontra Európai Adatvédelmi Testület [ECLI:EU:T:2022:783].
150 C-97/23. P. sz. ügy WhatsApp Ireland kontra Európai Adatvédelmi Testület [ECLI:EU:C:2023:608].
151 DPC (2021b) i. m. 18–19.

hasonló nyelvezet, és egymással tartalmi átfedésben lévő szövegváltozatok miatt figyelmen kívül hagyhattak releváns részleteket. A DPC értékelése alapján pedig mindez az adatkezelő részéről egy átgondolt megközelítés hiányából fakadt, nem a felhasználók rendelkezésére bocsátandó információk bonyolult jellegéből.[152] Összességében „inkább a szerencse, mintsem a logika kérdése volt, hogy a felhasználó hozzáfért-e az információkhoz vagy sem."[153]

Az ICO fentebb hivatkozott döntése[154] alapján a TikTok adatkezelési tájékoztatója és egyéb átláthatósági intézkedései által sem kaptak a gyermek felhasználók elegendő, valamint életkoruknak és képességeiknek megfelelő információt ahhoz, hogy tájékozott döntést hozhassanak arról, hogy részt vesznek-e a platformon és amennyiben igen, hogyan.

Egyrészt a használt nyelvezet sok esetben nem volt világos és közérthető, valamint különösen nehezen érthető volt a gyermek felhasználók számára. Például a 'jogos érdekekre' való utalással kapcsolatban az adatkezelési tájékoztató a 'kapcsolódó metaadatokra' hivatkozott anélkül, hogy a metaadatot definiálta, vagy legalábbis körülírta volna. A dokumentum alapján az adatkezelő az érintettek személyes adatait adatelemzésre és a platform tesztelésére is felhasználta a „stabilitás és a biztonság biztosítása érdekében". A tájékoztatás azonban e körben sem szolgált magyarázattal a konkrétan felhasznált adatok kategóriáinak és a felhasználás konkrét módjainak vonatkozásában.[155] Továbbá a hatóság megítélése szerint zavaró volt a tájékoztató egy másik részére való hivatkozás, amely lényegében ugyanazt az információt tartalmazta.[156]

Másrészt az adatkezelési tájékoztató nem tartalmazott világos és közérthető információ arról, hogy mennyi ideig őrzik meg az adatokat. Az időtartam meghatározásához használt kritériumok sem tették lehetővé a felhasználó számára, hogy megértse, mennyi ideig tárolják a személyes adatait. Az alkalmazott nyelvezet túl tág és általános volt, és nem volt kellően részletes ahhoz, hogy az érintettek megértsék például, hogy a TikTok „érintett információkkal kapcsolatos szerződéses kötelezettségei és jogai" hogyan befolyásolják az adatmegőrzési időszakokat, vagy egyáltalán, hogy melyek ezek a szerződéses kötelezettségek és jogok. Az egyes kritériumok jelentése és jelentősége nem volt világosan meghatározva, valamint a dokumentum gyakorlati példákat sem tartalmazott arra vonatkozóan, hogy ezen kritériumok hogyan hatnának az adatmegőrzési időkre.[157]

A fentebb hivatkozott, a Facebook, az Instagram és a WhatsApp adatvédelmi gyakorlatát vizsgáló DPC eljárások alapján a személyre szabott hirdetésekhez kapcsolódó, adatkezelésre vonatkozó információk különböző dokumentumokban voltak elérhetőek a felhasználók számára.[158] Az adatkezelési célokat és az alkalmazott jogalapokat pedig csak általánosságban határozták meg. A DPC értékelése alapján ugyanazon, akár eltérően megfogalmazott információ több dokumentumban való megjelenése önmagában még nem GDPR-ellenes. Azonban, amennyiben az adott adatkezelési célokhoz és jogalapokhoz kapcsolódóan a tájékoztatás nem tartalmazza a vonatkozó adatkezelési műveleteket és az érintett személyes adatok kö-

152 Uo. 98–99., 104., 122., 135., 154–155.
153 Uo. 164.
154 ICO (2023) i. m.
155 Uo. 54–55.
156 Uo. 56.
157 Uo. 55–56.
158 DPC (2022a) i. m. 72.

rét, az adatkezelő nem teljesíti a GDPR 13. cikkében előírt tájékoztatási kötelezettségét.[159] Az adatkezeléssel érintett személyes adatok körének nyílt végű felsorolással történő megjelenítése szintén nem elégíti ki a szükséges információk átlátható módon történő rendelkezésre bocsátásának követelményét.[160]

5. Beépített és alapértelmezett adatvédelem

A GDPR elvi szinten deklarálja, hogy az adatkezelők kizárólag az adatkezelés céljához képest szükséges személyes adatokat kezelhetnek.[161] Az adatkezelők kapcsolódó konkrét kötelezettsége egyrészt, hogy az adattakarékosság hatékony megvalósítása céljából megfelelő technikai és szervezési intézkedéseket hajtsanak végre az adatkezelésük teljes időtartama alatt, mintegy 'beépítve' a szükséges garanciákat az adatkezelés folyamatába.[162]

Másrészt, az adatkezelő köteles megfelelő intézkedéseket hozni a célból, hogy a kezelt személyes adatok mennyisége, az adatkezelés mértéke, az adatmegőrzési idő és az adatokhoz való hozzáférhetőség is alapértelmezett módon, az adatkezelési célok eléréséhez képest szükséges mértékre korlátozódjon.[163] Minden esetben az adatkezelő felelőssége, hogy az adatkezelésének alapértelmezett beállításait és lehetőségeit ezen elvárásoknak megfelelve válassza meg, valamint felelősséget vállaljon azok végrehajtásáért.[164]

5.1. Iránymutatások

Annak meghatározásakor, hogy összességében mennyi személyes adat szükséges az adott adatkezelési cél eléréséhez, figyelemmel kell lenni az adatok típusaira, kategóriáira, valamint részletességükre.Vagyis, amennyiben „a személyes adatok bizonyos kategóriái szükségtelenek, vagy ha részletes adatokra azért nincs szükség, mert kevésbé részletes adatok is elegendőek, a felesleges személyes adatok nem gyűjthetők."[165] Az adatkezelő az érintettek számára felajánlott választási lehetőségek közül alapértelmezetten köteles a legkevesebb adatkezeléssel járó opciót bejelölni, mivel a felhasználók nagyobb eséllyel fogadják el ezen alapértelmezett beállításokat, mint változtatnak rajtuk.[166]

A hozzáférhetőség körében alapvető követelmény, hogy az érintettek személyes adatai – hozzájárulások nélkül – ne válhassanak előre meghatározatlan számú személy számára elérhetővé.[167] Ez ugyanis az eredetileg tervezettnél szélesebb körben történő hozzáférhetőséget eredményezhet, mely számos kockázatot jelent az érintettekre – és kifejezetten a gyermekek-

159 Uo. 73.
160 Uo. 74.
161 GDPR 5. cikk (1) bekezdés *c)* pont.
162 GDPR 25. cikk (1) bekezdés.
163 GDPR 25. cikk (2) bekezdés.
164 EDPB: 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2020. október 20. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_ dataprotection_by_design_ and_by_default_v2.0_hu.pdf 12 [a továbbiakban: EDPB (2020b)].
165 Uo. 13.
166 EDPB (2023) i. m. 22–23.
167 GDPR 25. cikk (2) bekezdés.

re, valamint egyéb kiszolgáltatott csoportokra – nézve. Jó gyakorlat, amennyiben az adatkezelő kizárólag az érintettek érvényes hozzájárulása esetén teszi személyes adataikat nyilvánosan elérhetővé.[168]

Gyermek érintettek esetén indokolt lehet a *privacy friendly nudge*-ok, vagyis a kevesebb adatkezeléssel járó lehetőségek választását hangsúlyozó dizájnelemek alkalmazása. Szintén jó gyakorlat a felnőttek bevonásának ösztönzése, elősegítése minél több esetben. Az adatvédelmi irányítópulthoz hasonló szülői irányítópult esetén például a szülői felügyeleti joggal rendelkező felhasználó megtekintheti, nyomon követheti, valamint adott esetben módosíthatja is a gyermekének adatvédelmi beállításait. E körben alapvető elvárás, hogy a gyermek felhasználó megfelelő információkkal rendelkezzen az őt érintő információkról, döntésekről.[169]

5.2. Releváns hatósági gyakorlat

A gyermekkorú felhasználók TikTok regisztrációjuk során választhattak, hogy privát vagy nyilvános fiókot szeretnének létrehozni. A felugró ablak a 'Privát fiókra váltok' (*Go private*) és az 'Átugrom' (*Skip*) lehetőségeket ajánlotta fel. A felugró ablak arra vonatkozóan is tartalmazott tájékoztatást, hogy privát fiók esetén csak a felhasználó által engedélyezett követők láthatják a felhasználó által megosztott tartalmakat, míg nyilvános fiók esetén azokat bárki megtekintheti. A felhasználók egyébiránt később bármikor szabadon módosíthatták ezen beállítást.[170]

A nyilvános fiókot választó felhasználó minden videójának közzététele előtt, egy további felugró ablakban kapott tájékoztatást a videó nyilvános voltáról, valamint a 'Most közzéteszem' (*Post now*) és a 'Mégsem' (*Cancel*) opciók közül választhatott.[171] A DPC szerint az 'Átugrom' és a 'Most közzéteszem' gomboknak a képernyő jobb oldalán való elhelyezése a legtöbb felhasználót arra késztette, hogy ezeket az opciókat válasszák, mivel megszokták, hogy e helyre kattintva folytathatják.[172] Szintén kiemelte a DPC, hogy míg az alapértelmezettnek beállított lehetőség ('Most közzéteszem') fekete, addig az alternatív opció ('Mégsem') világosszürke betűszínnel jelent meg.[173]

A DPC álláspontja szerint a felugró ablakokban foglalt lehetőségek megfogalmazása azt sugallta, hogy a nyilvános profil létrehozása és nyilvános videók közzététele az alapértelmezett beállítás. Ez számos további következménnyel is járt a gyermek felhasználók magánéletének védelmére. Például bármely regisztrált felhasználó hozzászólhatott a közzétett tartalmaikhoz, valamint a '*Duet*' és '*Stitch*' ('Duett' és 'Kollázs') funkciók alapértelmezett engedélyezése által bármely felhasználó további videókat fűzhetett a gyermekek által közzétett tartalmakhoz.[174] Ezen alapértelmezett beállítások a DPC szerint növelték a rosszhiszemű szereplők által esetlegesen elkövethető visszaélések veszélyét.

168 EDPB (2020b) i. m. 14.
169 DPC (2021a) i. m. 65.
170 DPC (2023a) i. m. 28.
171 Uo. 29.
172 Uo. 88.
173 Uo. 28.
174 Uo. 37.

Mindez a felhasználók személyes adatainak a szándékuknál nagyobb mértékű kezeléséhez vezetett, a platform kialakítása tudat alatt olyan döntésekre ösztönözte a gyermekeket, melyek hátrányosak voltak a magánéletük védelme szempontjából. Továbbá a TikTok a gyermekekre hárította a felelősséget, hogy rendelkezzenek elegendő technikai tudással ezen beállítások megváltoztatásához. A DPC e körben a TikTok arra vonatkozó érvelését sem fogadta el, hogy a platform célja – lévén egy globális tartalommegosztó közösség – és a kapcsolódó kontextus kellően tájékoztatta volna a gyermekeket az adatkezelés mértékéről.

A 'Családi párosítás' (*Family pairing*) funkció szülői felügyeletre adott lehetőséget a gyermek felhasználó fiókja felett egy másik felhasználónak, így például lehetővé tette az elérhető tartalom szűkítését, a keresés és a közvetlen üzenetek letiltását, a fiók priváttá tételét és a megjegyzések korlátozását. A fiókok párosítása a nem gyermek felhasználó számára generált QR-kód segítségével valósult meg. Ezt a kódot a gyermek felhasználónak kellett beolvasnia, valamint megerősítenie, hogy kívánja-e a fiókok összekapcsolását. A DPC összességében úgy vélte, hogy e folyamat ellenére nem történt meg a két felhasználó közötti kapcsolat megfelelő ellenőrzése.[175]

Szintén kifogásolta a DPC, hogy a szülői felügyeletet gyakorló felhasználó akkor is engedélyezhette a közvetlen üzenetek küldését a 16 év feletti gyermek fiókja számára, ha a gyermek maga kikapcsolta ezt a funkciót. Tekintettel arra, hogy a konkrét szülői felügyelet gyakorlására való jogosultság ellenőrzése sem volt megfelelő, a DPC szerint ez a lehetőség további veszélyeket rejtett a gyermekekre nézve, hiszen akár az akaratuk ellenére is lehetővé tette rosszhiszemű felhasználók részére a velük történő kapcsolatfelvételt.[176] Ez a megállapítás is azt támasztja alá, hogy a DPC szerint a gyermekekre nézve fokozott kockázatot jelent az esetlegesen akaratuk ellenére történő közvetlen kapcsolatfelvétel lehetősége, akár a hozzászólási funkció, akár közvetlen üzenetküldés útján.

A TikTok életkorellenőrzési intézkedéseket vezetett be annak megakadályozására, hogy 13 év alatti gyermekek hozzáférjenek a platformhoz. Egyrészt a leendő felhasználók kötelesek voltak a regisztráció során megadni életkorukat, a 13 éves korhatár alatt pedig nem volt lehetőség a regisztráció véglegesítésére vagy újból egy idősebb életkor megadására. Másrészt utólagos intézkedéseket is alkalmazott a TikTok a 13 év alatti gyermekkorú felhasználók fiókjainak azonosítására és eltávolítására.[177] Összességében a DPC nem állapított meg jogsértést ezen életkorellenőrzési intézkedések kapcsán.

A TikTok életkornak megfelelő kialakításról szóló adatvédelmi hatásvizsgálata nem azonosította a 13 év alatti gyermekeknek a platformhoz való hozzáférésével járó konkrét kockázatokat, amit a DPC úgy értékelt, hogy a TikTok nem hozott megfelelő intézkedéseket az adatvédelmi megfelelés biztosítására és bizonyítására.[178] Ez fontos indikátora annak a szabályozói elvárásnak, hogy a minimális felhasználói küszöbértékkel rendelkező digitális szolgáltatásoknak figyelembe kell venniük a szolgáltatás engedélyezett alsó korhatár alatti felhasználóira vonatkozó kockázatokat, többek között az adatvédelmi hatásvizsgálatuk révén.

A DPC megerősíti ezen túl, hogy az olyan hivatalos okmányok, mint a személyigazolvány vagy az útlevél (*hard identifiers*) megkövetelése aránytalan intézkedés volna. A DPC álláspontja

175 Uo. 30.
176 Uo. 41–42.
177 Uo. 45.
178 Uo. 48–49.

szerint, mivel a gyermekek sok esetben nem rendelkeznek hivatalos okmányokkal vagy nem férnek hozzá azokhoz, ez kizárná vagy korlátozná azon gyermekkorú felhasználókat, akik egyébként használhatnák a platformot.[179]

A fentebb hivatkozott ügy tényállása alapján az Instagram alapértelmezett beállítása lehetővé tette, hogy az Instagram-fiók közösségi médiatartalmát bármely Instagram-felhasználó, valamint olyan személyek is megtekinthessék az Instagram webböngésző változata segítségével, akik nem regisztráltak Instagram felhasználóként. Ezzel szemben, ha egy felhasználói fiókot privátnak állítottak be, a felhasználó által közzétett tartalmakhoz csak a fiók tulajdonosa által személyesen jóváhagyott felhasználók férhettek hozzá. Ahhoz, hogy egy felhasználói fiókot privátté lehessen állítani, a fiók tulajdonosának az Instagram-felhasználóként való regisztrációt követően meg kellett változtatnia az alapértelmezett beállításokat.[180]

A DPC döntésében megállapította, hogy az alapértelmezetten nyilvános fiókbeállítás nem volt szükséges és arányos az Instagram által megállapított adatkezelési célok eléréséhez, mivel egyrészt a kiskorú felhasználóknak korlátozott lehetőségük volt megváltoztatni ezen beállítást, másrészt pedig az ezáltal közzétett személyes adatokhoz globálisan bárki hozzáférhetett. Mivel az adatkezelő nem hajtott végre megfelelő technikai és szervezési intézkedéseket annak érdekében, hogy kizárólag az adatkezelés céljából szükséges személyes adatokat gyűjtsön, megsértette az adattakarékosság, valamint a beépített és alapértelmezett adatvédelem elvét.[181]

6. Kitekintés

A kritikák szerint a jelenlegi szabályozás összességében pont azon szereplőket részesítette előnyben, melyek adatvezérelt tevékenységeit leginkább korlátozni célozta. A szinte kimeríthetetlen erőforrásokkal rendelkező technológiai óriások ugyanis jobban pozícionáltak, hogy megfeleljenek a szigorúbb adatvédelmi szabályozásnak, mint a versenytársaik. Ezáltal a korábban is monopoljellegű adathalmazokkal rendelkező vállalatok könnyedén kiszoríthatják a kisebb piaci szereplőket.[182] Például a várakozásokkal ellentétben a GDPR alkalmazandóvá válását követően a Google képes volt megszilárdítani piaci fölényét az online keresők hirdetések piacán, ezáltal *de facto* adatvédelmi szabályozóvá válva.[183]

A piaci koncentráció hatására adatvédelmi szempontból megkérdőjeleződik az érintettek hozzájárulásának önkéntessége, fogyasztóvédelmi szempontból pedig a tájékozott ügyleti döntés teljesülése. A különböző jogterületek közötti határvonalak elmosódását jól szemlélteti, hogy a Facebookot érintő német versenyhatósági ügy kapcsán az EUB kimondta, hogy a tagállami versenyhatóságok az erőfölénnyel visszaélés tényállásának megállapítása során – szorosan együttműködve a releváns adatvédelmi hatósággal – érté-

179 Uo. 50.

180 EDPB (2022) i. m. 43.

181 Uo. 44.

182 Sara Quach et al.: Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, vol. 50. (2022) 1318.

183 Damien Geradin – Theano Karanikioti – Dimitrios Katsifis: GDPR Myopia: how a well-intended regulation ended up favouring large online platforms – the case of ad tech. *European Competition Journal*, vol. 17., no. 1. (2021) 51., 88. https://doi.org/10.1007/s11747-022-00845-y

kelhetik a vállalkozás adatvédelmi megfelelését.[184] Ennek megfelelően számos szerző érvel az említett jogterületek közötti szorosabb együttműködés mellett.[185]

A konvergencia jogalkotási terméke a digitális piacokról szóló jogszabály.[186] A DMA az alapvető platformszolgáltatásokat nyújtó, valamint jelentős és tartós piaci hatásuk miatt kapuőrré minősített vállalkozásokra vonatkozóan tartalmaz speciális, adatvédelmi jellegű előírásokat is. Az európai bizottsági minősítés alapján kapuőrnek minősül többek között a ByteDance a TikTok, a Meta a Facebook, az Instagram, a WhatsApp és a Messenger, valamint az Alphabet a YouTube és a Google Search az online platformok vonatkozásában.[187] A kapuőrök például nem kapcsolhatják össze a felhasználók különböző forrásokból származó személyes adatait, valamint nem használhatják azokat egyéb szolgáltatásaik céljára a felhasználók érvényes hozzájárulása nélkül.[188] Összességében, míg a GDPR általános előírásainak való elvárt megfelelés érdekében tett konkrét, technikai és szervezési intézkedések mértéke az adatkezelés által jelentett kockázatok, és nem az adatkezelők méretének függvénye, addig a DMA kifejezetten a legkockázatosabb kapuőröket célozza.[189] Szintén cél a személyes adatok és a magánszféra alapjogi védelmén, valamint az érintettek transzparens tájékoztatásán túl az adatalapú gazdaság fellendítése, az európai digitális piacok versenyképességének növelése, valamint a kapuőrök konkrét adatkezelési műveleteinek korlátok közé szorítása.[190]

A fentebb részletesen is bemutatott, a Facebook, az Instagram és a WhatsApp platformok vonatkozásában lefolytatott DPC eljárásokat[191] követően a Meta a jogos érdek jogalapra tért át a személyre szabott hirdetések vonatkozásában. A korábban is említett, szerződéses jogalap alkalmazhatóságát kizáró EUB döntés azonban a jogos érdek mint jogalap alkalmazhatóságát is erősen megkérdőjelezte.[192]A norvég adatvédelmi hatóság (norvégül: Datatilsynet) ezt követően a GDPR 66. cikk (1) bekezdése alapján sürgősségi eljárás keretében ideiglenes intézkedést fogadott el, melyben három hónapos időtartamra megtiltotta, hogy a Meta a jogos érdekére hivatkozva jelenítsen meg személyre szabott reklámokat a norvég felhasználóknak, valamint végleges intézkedések elfogadására hívta fel az EDPB-t.[193] Az EDPB a GDPR 66. cikk (2) bekezdése alapján a Datatilsynet kérelmének megfelelő döntést hozott, melyben

184 C-252/21. sz. ügy i. m. 62–63. pont.

185 Inge Graef: *Data as Essential Facility. Competition and Innovation on Online Platforms* [doktori értekezés]. KU Leuven CITIP, 2016. június 29. 307. https://lirias.kuleuven.be/1711644&lang=en.; Tóth András: Médiaszabályozási indikációk az online figyelempiacok kudarcainak kiküszöböléséhez. *In Medias Res*, 2021/2. 294.; Bálint János: The Digital Markets Act: The Future of Competition Law in the Digital Market. *Versenytükör*, 2023/VIII. 13–14.

186 Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról, HL L 265, 2022. 10. 12., 1–66. o. (a továbbiakban: DMA).

187 Európai Bizottság: A digitális piacokról szóló jogszabály: a Bizottság döntése hat kapuőri minősítésről. 2023. szeptember 6. https://ec.europa.eu/commission/presscorner/detail/hu/ip_23_4328

188 DMA 5. cikk (2) bekezdés *b–c)* pont.

189 Tuulia Karjalainen: The battle of power: Enforcing data protection law against companies holding data power. *Computer Law & Security Review*, vol. 47. (2022) 9. https://doi.org/10.1016/j.clsr.2022.105742

190 Tóth András et al.: A GDPR és a Digital Markets Act viszonyának tisztázása. *In Medias Res*, 2023/2. 45.

191 DPC (2022a) i. m., DPC (2022b) i. m., DPC (2022c) i. m.

192 C-252/21. sz. ügy i. m. 105–124. pont.

193 Datatilsynet: Urgent and Provisional Measures – Meta, 21/03530-16, 2023. július 14. https://www.datatilsynet .no/contentassets/36ad4a92100943439df9a8a3a7015c19/urgent-and-provisional-measures--meta_redacted.pdf

kötelezte a DPC-t mint a Meta fő felügyeleti hatóságát, hogy minden uniós felhasználó tekintetében tiltsa meg az adatkezelő részére a jogos érdek jogalap alkalmazását a személyre szabott reklámokhoz kapcsolódó adatkezelése tekintetében.[194]

2023 novemberétől az Európai Unió területén élő felhasználói számára a Facebook és az Instagram szolgáltatások tekintetében a Meta lehetővé tette, hogy a személyre szabott hirdetések megjelenítéséhez való hozzájárulás helyett havidíjat fizetve kikapcsolhassák a reklámokat a platformok használata közben.[195] Az adatvédelmi aktivistákból álló, *noyb* (*none of your business*) elnevezésű osztrák csoport rögtön panasszal is élt az osztrák adatvédelmi hatóságnál. Véleményük szerint nem tekinthető önkéntesnek és ezáltal érvényesnek az olyan hozzájárulás, amely megtagadása esetén a felhasználó köteles havidíjat fizetni, máskülönben nem tudná igénybe venni az adott szolgáltatást.[196] Ezen túlmenően, az egyetlen kattintással megadható hozzájárulás visszavonásának kizárólagos módja, hogy a felhasználó számtalan oldalon és felugró ablakon átnavigálva havidíjas előfizetésre váltson.[197]

A '*pay-or-okay*' vagy '*pay-or-consent*' megoldás jogszerűsége általánosságban sem teljesen tisztázott kérdés,[198] azonban az EDPB vonatkozó véleménye nagy online platformok esetében szolgál némi iránymutatással.[199] Az EDPB szerint a nagy online platformok nem felelnek meg az érvényes hozzájárulás követelményeinek, amennyiben a felhasználókat csak a személyes adatok viselkedésalapú reklámcélú kezeléséhez való hozzájárulás és a díjfizetés közötti bináris választás elé állítják. A szolgáltatás viselkedésalapú hirdetést tartalmazó változatának kidolgozásakor a nagy online platformoknak meg kell fontolniuk, hogy az érintettek számára olyan „egyenértékű alternatívát" kínáljanak, amely nem jár díjfizetéssel. Ha az adatkezelők úgy döntenek, hogy díjat számítanak fel az „egyenértékű alternatívához" való hozzáférésért, az adatkezelőknek meg kell fontolniuk egy másik, viselkedésalapú reklám nélküli, ingyenes alternatíva felajánlását is, pl. olyan reklámformával, amely kevesebb (vagy semmilyen) személyes adat kezelésével jár.[200]

Az olasz adatvédelmi hatóság (olaszul: Garante per la Protezione dei Dati Personali, a továbbiakban: Garante) 2023. március 30-án átmenetileg az olasz felhasználókat érintő adatkezelései korlátozására kötelezte a ChatGPT szolgáltatást nyújtó OpenAI LLC. vállalatot. A Garante sérelmezte, hogy a ChatGPT szolgáltatás weboldalán egyáltalán nem volt elérhető adatkezelési tájékoztató, az OpenAI nem rendelkezett érvényes jogalappal az algoritmusok fejlesztéséhez és tanításához kapcsolódó adatkezelés esetében, valamint a felhasználási felté-

194 EDPB: Urgent Binding Decision 01/2023, 2023. október 27. https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf

195 Meta: Facebook and Instagram to Offer Subscription for No Ads in Europe. 2023. október 30. https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

196 noyb: noyb files GDPR complaint against Meta over "Pay or Okay". 2023. november 28. https://noyb.eu/en/ noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

197 Noyb: Meta ignores the users' right to easily withdraw consent. 2024. január 11. https://noyb.eu/en/meta-ignores -users-right-easily-withdraw-consent

198 Christophe Carugati: The 'pay-or-consent' challenge for platform regulators. *Bruegel*, 2023. november 6. https://www.bruegel.org/sites/default/files/2023-11/the-'pay-or-consent'-challenge-for-platform-regulators-9508_3.pdf

199 EDPB: Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024 április 17. https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

200 Uo. 20–21., 27–29.

telekben foglalt korlátozással szemben az adatkezelő nem alkalmazott megfelelő technikai és szervezési intézkedéseket a 13 évnél fiatalabb felhasználók kiszűrése érdekében.[201]

Az OpenAI vonatkozó vállalásainak fényében a Garante április 11-i döntésével feloldotta a korlátozást. Az OpenAI vállalta, hogy adatkezelési tájékoztatót készít, és azt a ChatGPT szolgáltatás weboldalán, valamint a felhasználók regisztrációs folyamata során is elérhetővé teszi. Az adatkezelő vállalta továbbá, hogy a szerződés teljesítéséhez szükséges jogalapról – a konkrét adatkezelési műveletek és a GDPR vonatkozó előírásainak figyelembevételével – áttér a hozzájárulás vagy jogos érdek jogalapra. Előbbi esetben a hozzájárulás visszavonását, utóbbi esetben pedig az adatkezelés ellen való tiltakozás lehetőségét könnyen elérhető módon biztosítja a felhasználói számára. Ezen túl az OpenAI vállalta, hogy megfelelő életkor-ellenőrző megoldásokat vezet be annak elérése érdekében, hogy 13 évesnél fiatalabb gyermekek ne használhassák a szolgáltatását.[202] Úgy tűnik, az adatkezelő vállalásai nem oszlatták el teljes mértékben a hatóság aggodalmait, ugyanis 2024. január 29-én a Garante bejelentette, hogy eljárást indít a ChatGPT szolgáltatás kapcsán, mivel a vonatkozó adatkezelés sérti a GDPR előírásait.[203] Nem sokkal később pedig a NAIH is eljárást indított hasonló tárgykörben.[204]

7. Összefoglalás

A GDPR összességében pozitív fejleményként értékelendő az online tér felhasználói személyes adatainak, valamint magánéletének védelme terén. A fentebbi példákból azonban az is jól látszik, hogy a jelen tanulmányban azonosított, az online platformok működésének alapvetéseit érintő adatvédelmi szabályok gyakorlati alkalmazása a GDPR alkalmazandóvá válását követően öt évvel is fontos szerepet játszik az uniós állampolgárok személyes adatainak és magánszférájának védelme terén. Az érintettek hozzájárulásának érvényessége, az átlátható tájékoztatás követelményei, a beépített és alapértelmezett adatvédelem, valamint a mindezeken átívelő gyermekvédelmi szempontok teljeskörű érvényre juttatása ugyanis sok esetben ellentétes a technológiai óriások üzleti és pénzügyi érdekeivel. A folyamatos technológiai fejlődésnek és innovációnak köszönhetően elérhetővé váló és robbanásszerűen elterjedő újszerű megoldások – mint például a generatív mesterségesintelligencia-megoldások – új köntösben vetik fel a régi problémákat. A felmerülő kihívások kezeléséhez pedig elengedhetetlen a GDPR vonatkozó előírásainak gyakorlati alkalmazásának vizsgálata; ehhez kívánt jelen tanulmány is hozzájárulni.

201 Garante: 9870832, 2023. március 30. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832

202 Garante: 9874702, 2023. április 11. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/ docweb/9874702

203 Garante: ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla normativa privacy, 2024. január 29. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020

204 Portfolio: A magyar adatvédelmi hatóság vizsgálja a ChatGPT-t, kiderült, mikorra várható döntés, 2024. április 8. https://www.portfolio.hu/uzlet/20240408/a-magyar-adatvedelmi-hatosag-vizsgalja-a-chatgpt-t-kiderult-mikor ra-varhato-dontes-678663

Adatbiztonság és a magánszféra védelme mint közjó

Datafikáció és a digitális lábnyom

Mozsonyi Norbert

Napjaink egyik legdrámaibb folyamata az információs robbanás és az ennek nyomán végbemenő drámai társadalmi átalakulás.[1] A digitális lábnyomokból rekonstruálhatóak eddig rejtett szerkezetek és összefüggések, továbbá módosul a megismerés eszköztára, módszertana és eredményei is.[2] A technológia lényege a minél sokoldalúbb, minél több, eltérő kategóriájú, időzítésű adat komplex, napi szinten fejlődő, új és újabb megoldásokkal, műveletekkel történő hasznosítása. Ettől még nem lesz a '*privacy* halott', ahogyan ezt sokan gondolják[3] – egyszerűen csak arról van szó, hogy a személyes adatok védelme helyett, talán inkább a személyes adatok kezelésének szabályain lesz a hangsúly. Ahhoz, hogy használhassuk és kihasználhassuk a mobileszközök, a mesterségesintelligencia-alapú Big Data-technológia,[4] valamint a hibrid felhőszolgáltatás komplex rendszer[5] előnyeit, az adatok megosztását elő kell segítenünk, és olyan szabályozásra van szükségünk, amely ezt úgy teszi lehetővé, hogy közben az adat bizalmas jellege megmarad az adatkezelőnél. Eszerint le kell számolni azzal a szabályozási előfeltevéssel, hogy magánszemély képes kontrollálni a személyes adatainak az áramlását. A megfigyelés társadalmában élőknek – vagyis mindannyiunknak – meg kell birkóznunk azzal a gondolattal, hogy adataink, viselkedésünk nyomai értékké váltak, amelyet lehet, hogy éppen most dolgoz fel, elemez valaki valahol. Az adataink kezelése tekintetében cél az adatbiztonság megvalósítása, tehát hogy digitális lábnyomaink, személyes adataink ne kerüljenek illetéktelen kezekbe, ne okozzanak az érintett tekintetében joghátrányt. Álláspontunk szerint az első és talán legfontosabb adatvédelmi aggály a jogpolitikai célok és a technológia működési elvének összeütközéséből ered.

---

1 Kenneth Cukier – Viktor Mayer-Schönberger: *Big Data – Forradalmi módszer, amely megváltoztatja munkánkat, gondolkodásunkat és egész életünket.* Budapest, HVG Könyvek, 2014. Eredetiben: Cukier–Mayer-Schönberger: *Big Data: A revolution that will transform how we live, work, and think.* Boston – New York, Houghton Mifflin Harcourt, 2013.

2 Csepeli György – Dessewffy Tibor: Big Data. A technological change that will fulfil sociology. *Review of Sociology*, 2015/3.

3 Kate Crawford – Jason Schultz: Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review,* vol. 55., no. 93. (2014) 94.; Omer Tene – Jules Polonetsky: Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online,* vol. 63. (2012). https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/

4 Dessewffy és Láng a Big Datát, a „digitális adatok robbanásszerű mennyiségi növekedése miatt előálló minőségileg is új társadalmi gyakorlatok és megismerési módok együttese"-ként határozza meg. A szerzők szerint az új ismeretelméleti paradigma nemcsak a 21. században keletkező megnövekedett adatmennyiség következtében alakult ki, a keletkezésnek meghatározó eleme volt a digitális rögzítések általános elterjedése is. Dessewffy Tibor – Láng László : Big Data és a társadalomtudományok véletlen találkozása a műtőasztalon. *Replika* 2015/3–4.

5 Az IoT-eszközök, a Big Data-adatfeldolgozás, valamint az adattovábbítási és adattárolási struktúra is feltételezi a mesterséges intelligenciát, ami fordítva is igaz, hisz a mesterséges intelligencia sem képes működni robusztus mennyiségű adat, valamint megfelelő adattovábbítás, tárolási, illetve számítási kapacitás nélkül, amelyek különösen bonyolult informatikai technológiai rendszert alkotnak.

1. Bevezető

Napjainkban válik igazán nyilvánvalóvá, hogy az információs társadalomban szinte már mindennek azonnal digitális nyoma marad, amelyeket mesterségesintelligencia-alapú Big Data-technológia[6] alkalmazásával dolgoznak fel, továbbá eddig megfigyelhetetlen viszonyokat, hálózatokat tesznek láthatóvá és kutathatóvá. Életünk egyre több területe bontható le jól strukturált adathalmazokra, amelyeket az egyre növekvő digitális eszközök és hálózatok képesek sokféleképpen kezelni és különböző célok mentén feldolgozni.[7] A digitális információk mennyisége szignifikáns módon, robbanásszerűen növekszik, és bár ezen információk jellemzően már nem a szándékosan átadott személyes adatok körébe tartoznak, ennek ellenére a Big Data-technológia[8] által azzá, sőt különleges adatokká válnak, így a személyes adatkezelés hatálya alá kerülnek. Nem tudjuk elkerülni, hogy digitális lábnyomunk maradjon, és azt sem tudjuk elkerülni, hogy ezeket folyamatosan különböző struktúrákban feldolgozzák,[9] hisz ez a szolgáltatás alapja, ez képezi annak motorját. A többmilliárd IoT-eszközből származó robusztus mennyiségű adat elemzése a hagyományos relációs adatbázisokkal nem jól kezelhető. A nagy adathalmaz jelenséget az alapozza meg, hogy az információs társadalomban szinte már mindennek azonnal valós időben digitális nyoma marad, vagyis így mérhetetlen adatmennyiség jön létre nap mint nap. De nem a méret a lényeg, hanem a korlátlan növekedési képesség és az adatelemzés, valamint az, hogy a statisztikával ellentétben e rendszer nem az egyént kérdezi, hanem a viselkedését monitorozza, és nem befolyásolja a rendszert, hogy mi miért történik, csak gyűjti az adatokat.

2. Alapjogi szemlélet

Az emberi jogok mint alapjogok az egyes államok alkotmányos rendjének és a nemzetközi közösségnek is a legalapvetőbb értékei közé tartoznak csakúgy, mint a jogállami demokrácia

6 A Big Data forradalom tétje szerintük az, hogy a Big Data-elemzés mindenfajta emberi tevékenységet és döntést befolyásol a társkereséstől a vásárlásig, az egészségügytől az oktatásig, a jogérvényesítéstől a terrorizmus elleni küzdelmen át a demokratikus választásokig. Neil M. Richards – Jonathan H. King: Big Data ethics. *Wake Forest Law Review*, vol. 49. (2014).

7 A Cambridge-i Egyetem Pszichometria Központjában például kidolgoztak egy rendkívül hatékony és gyors módszert, amellyel egy ember vagy egy embercsoport jellemzői a különböző adatokból nagy pontossággal kielemezhetők. Michal Kosinski – David Stillwell – Thore Graepel: Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences (PNAS),* vol. 110., no. 15. (2013) https://doi.org/10.1073/pnas.1218772110

8 A Big Data elnevezés azt a hatalmas információmennyiséget és feldolgozást jelenti, amelyet a cégek és az egyéni felhasználók és a hálózatba kötött digitális eszközök hoznak létre, és számítógépek elemeznek. Ennek eredményeként digitális lábnyomaink személyes adatokká, sőt különleges adatokká válnak, amelyeket rendszerszinten számítási felhőben tárolnak és dolgoznak fel.

9 A Big Data a generált adathalmazokat összekapcsolja, s ezáltal olyan következtetések és predikciók előtt nyitja meg a kaput, amelyekkel akár beleláthatunk az emberek legbelsőbb gondolataiba is. A prediktív adatelemzés során a profilokat felállítva rendkívül pontos előrejelzések tehetők az érintett jövőbeli döntéseivel kapcsolatban, vagyis az egyén digitális lábnyoma már előre konstruált, és tudják, hogy bele fog lépni, mert tudják előre, mit fog csinálni. Ződi Zsolt: Privacy és a Big Data. *Fundamentum,* 2017/1–2. 19. https://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf.

alapértékei. Az alkotmányjog olyan vertikális hatályú[10] normák rendszere, amelyek a közhatalom gyakorlója és az állampolgár közti viszonyt szabályozzák. Az európai jogfejlődés ezt a vegytiszta képletet az utóbbi évtizedekben már meghaladta, és – elismerve, hogy életünkre és jogaink érvényesülésére korántsem csak az államhatalom lehet meghatározó befolyással – egyes alapjogok tekintetében túllépett a jog vertikális hatályának körén. Az alapjogok horizontális hatályán ehhez képest azt értjük, amikor a polgár az alkotmányos jogainak a védelmét nem az állammal, hanem másik magánféllel szemben igényelheti.[11] Nem lehet kétségünk afelől sem, hogy a nagy gazdasági befolyással rendelkező nagyvállalatok, sőt kisebb vállalkozások és magánszemélyek is gyakorolhatják oly módon jogaikat, hogy azok nem felelnek meg feltétlenül a nemzetközi emberi jogi sztenderdeknek. Mára jelentősen megváltoztak a hatalmi viszonyok, melyek során minden természetes és jogi személy is potenciális jogsértő lehet, így nem látom alapját annak, hogy emberi jogaink védelmét kizárólag az állammal szemben kell, illetve lehet érvényesíteni.[12] A kiválóság és a bizalom megközelítésére építő Fehér könyv is az Európai Unió alapértékei, köztük az alapvető jogok védelmét emeli a mesterséges intelligencia fejlesztésének, használatának és szabályozásának központi követelményévé. A mesterséges intelligencia fejlesztése és használata tehát nem lehet önmagában való cél, hanem kizárólag az egyetemes emberi értékek, alapjogok érvényesülését és kiteljesítését szolgáló technológiai eszközként kell tekinteni rá és ebben a szellemben szükséges szabályozni.

3. Kapuőrök monopol helyzete

A kapuőrök[13] mint minősített adatkezelők[14] által kezelt személyes adatok tekintetében az adatkezelő-központú szabályozás felől nagymértékben el kellene tolódni az adatkezelési szerződésen alapuló szabályozás felé. Ezek a közvetítő szolgáltatók[15] szolgáltatási tevékenységük során tartalmak tömegét rangsorolják (például keresőmotorok, közösségi platformok találati listájának rangsorolása) vagy moderálják. Ehhez a szűrési, rangsorolási tevékenységhez

10 A modern alkotmányok abból a célból jöttek létre, hogy világosan meghatározott keretek közé tereljék az államhatalom működését, így biztosítva mindenekelőtt az alapjogok gyakorlásának lehetőségét. Ebből a rendeltetéséből adódóan az alkotmány szabályai az államot és annak szerveit kötelezik: megmondják, hogyan kell eljárniuk, meddig terjed a közhatalmuk, és mit kell tenniük az emberi jogok megfelelő garantálása érdekében.

11 A magánjog közjogiasodása címen igazolt jelenséget mutatja be Gárdos-Orosz Fruzsina: *Az emberi jogok alkalmazásának lehetőségei a rendes bíróságokon, különös tekintettel a magánjogi vitákra* [Doktori értekezés kézirata]. Győr, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2010. 42–51.

12 Andrew Z. Drzemczewski: *European Human Rights Convention in Domestic Law. A Comparative Study*. Oxford, Clarendon Press Publication, 1983. 8. fejezet. 373–377. https://www.corteidh.or.cr/tablas/a11660.pdf

13 A digitális gazdaság sajátosságai miatt néhány meghatározó 'kapuőrplatform' kikezdhetetlen pozíciókra tett szert, amellyel képes kontrollálni a digitális gazdasági ökoszisztémák fejlődési irányait, egyúttal a verseny előnyös hatásai is korlátozottá váltak. A platformfogalom minősített adatkezelői szintre történő formálódásában fontos mérföldkő a digitális piacokról szóló (DMA), valamint a digitális szolgáltatásokról szóló (DSA) rendelettervezet.

14 Óriásplatformokra differenciált követelményrendszert telepít a DSA rendelet. Berrak Genç-Gelgeç: Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies? *Croatian Yearbook of European Law & Policy*, Zagreb, vol. 18. (2022). https://doi.org/10.3935/cyelp.18.2022.485

15 Vö.: Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Eker. irányelv) 4. szakasz: A közvetítő szolgáltatók felelőssége.

nagy mennyiségű meta-[16] és személyes adatot[17] kezelnek. A tartalmak személyre szabásához elengedhetetlen szűrési, rangsorolási, moderálási tevékenységük során pedig egyre nagyobb mértékben használnak mesterséges intelligencián[18] alapuló komplex technológiákat.[19] A mai minősített adatkezelés mesterségesintelligencia-alapú Big Data-technológia[20], valamint vezeték nélküli kommunikációs infrastruktúra[21] és hibrid felhőszolgáltatás együttesének[22] felhasználásával valósul meg. A digitalizáció a fentiekben leírt folyamatok által – az adat kiemelkedő jelentősége mellett – a mindennapi életünk szerves részét képező új felületeit hozza létre a társadalmi, gazdasági működésnek, valamint a kommunikációnak, melyeket más szerzők jelentős digitális jelenléttel rendelkező online platformoknak[23] is neveznek. Ezek a platformok döntően nagy adathalmazokkal és algoritmikus döntésekkel dolgoznak.[24] Piaci

16 A mesterségesintelligencia-alapú rendszerek egyik sajátos fajtájának tekinthetők a már létező, metaadatokat rendszerező keresők (ilyen a jogforrások és esetjog keresésére egyaránt alkalmas Eur-Lex, vagy az esetjog áttekintésére a Bíróság ítélkezési gyakorlatának keresőmotorja). Ezen adatkezelés során keletkező széles információk más adathalmazokkal, adatbázisokkal való elemzése, értékelése esetén szintén személyes adatokká képezhetők. (European Case Law Identifier – Az európai esetjogi azonosító (ECLI) keresésére szolgáló program.)

17 A személyes adatok kapcsán sokáig az adatok védelmét biztosító szabályozáson volt a hangsúly. A platformok infrastruktúrájába épített automatizált rendszerek (algoritmusok) segítségével a platformok üzemeltetői könnyebben tudják értelmezni a felhasználói magatartási mintákat, valamint a platformhasználati trendeket, és ennek alapján nem csak személyre szabott tartalmakat nyújthatnak, de egyéb, a felhasználókat jelentős mértékben érintő döntéseket is hozhatnak.

18 A mesterséges intelligencia fogalmát sokan, sokféle értelemben használják. Az Európai Bizottság által adott definíció szerint: „A mesterséges intelligencia olyan rendszereket takar, amelyek intelligens magatartást tanúsítanak a környezetük analizálása és a meghatározott célok elérése érdekében – bizonyos mértékű autonómiával – tett lépéseik révén." European Commission, Independent High-Level Expert Group on Artificial Intelligence: A Definition of AI: Main Capabilities and Scientific Disciplines. (2019. április 8.) https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines. Lásd még a definitív megközelítésekre: Jan De Bruyne – Cedric Vanleenhove (szerk.): *Artificial Intelligence and the Law.* Cambridge, Intersentia, 2021; Thomas Wischmeyer – Timo Rademacher: *Regulating Artificial Intelligence.* Cham, Springer, 2020.

19 Az IoT-eszközök, a Big Data-adatfeldolgozás, valamint az adattovábbítási és adattárolási struktúra is feltételezi a mesterséges intelligenciát, ami fordítva is igaz, hisz a mesterséges intelligencia sem képes működni robusztus mennyiségű adat, valamint megfelelő adattovábbítás, tárolási, illetve számítási kapacitás nélkül, ami különösen bonyolult informatikai technológiai rendszert alkot.

20 A Big Data a generált adathalmazokat összekapcsolja, s ezáltal olyan következtetések és predikciók előtt nyitja meg a kaput, amelyekkel akár beleláthatunk az emberek legbelsőbb gondolataiba is. A prediktív adatelemzés során a profilokat felállítva rendkívül pontos előrejelzések tehetők az érintett jövőbeli döntéseivel kapcsolatban, vagyis az egyén digitális lábnyoma már előre konstruált, és tudják, hogy bele fog lépni, mert tudják előre, mit fog csinálni. Ződi (2017) i. m. 19. http://fundamentum.hu/sites/default/files/fundamentum-17-1-2-02.pdf.

21 A többmilliárd IoT-eszközből származó, robusztus mennyiségű adat elemzése a hagyományos relációs adatbázisokkal nem jól kezelhető. Nem a méret a lényeg, hanem a korlátlan növekedési képesség és az adatelemzés, valamint, hogy a statisztikával ellentétben nem az egyént kérdezi, hanem a viselkedésüket monitorozza, és nem befolyásolja a rendszert, hogy mi miért történik, csak gyűjti az adatokat.

22 Az igazi fejlődést meglátásom szerint elsősorban nem az egyes technikák és technológiák erőforrást nem kímélő innovációja jelenti, hanem az, hogy ezek a technikák és technológiák megannyi területen kapcsolódnak kapcsolódnak, s együtt, egymást kiegészítve képeznek komplex technológiai rendszereket. Kollár Csaba: A mesterséges intelligencia, mint komplex rendszer információbiztonsági kihívásai. In: Rajnai Zoltán (szerk.): *Kiberbiztonság – Cybersecurity 2.* Budapest, Biztonságtudományi Doktori Iskola, 2019. 66–67. https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf.

23 A platformok hatalmával kapcsolatban: Margrethe Vestager: New technology as a disruptive global force. Paris (2019. január. 21.): *Youth and Leaders Summit*.

24 Vö. Margrethe Vestager: Algorithm and competition. Berlin (2017. március 16.): *Bundeskartellamt 18th Conference on Competition*.

erejüknél fogva és a digitális ökoszisztéma felett gyakorolt kontrollálási képességük, valamint a felhalmozott adatvagyonuk révén monopol vagy oligopol helyzetben vannak.[25] Az általuk létrehozott, fejlesztett digitális szolgáltatást nyújtó platformok a betöltött szerepüknél fogva[26] nagyon nehezen ellenőrizhetők, elszámoltathatók. Az ilyetén mértékű piaci erejük kialakulásának egyik oka, hogy a fúziókontrollt a versenyhivatalok 'alulérvényesítették' a technológiai szektorban.[27] A 2008 és 2018 közötti években a Google, az Apple, az Amazon, a Facebook (Meta) és a Microsoft együttesen több mint 400 felvásárlást hajtottak végre, de egyik sem került tiltásra.[28] Ez a technológiai szektorban gyakori jelenség azt jelenti, hogy a nagy technológiai vállalkozások még azelőtt megvásárolják az innovatív, új – de piaci részesedéssel, vagy jelentős piaci erővel nem rendelkező – vállalkozásokat, mielőtt azok jelentős tényezővé tudnának válni.[29] Ezzel az adott ötlet vagy ígéretes üzleti megoldás még azelőtt 'beleolvad' a felvásárló vállalkozásba, mielőtt az valódi versenynyomást tudna kifejteni, és csupán a nagy technológiai vállalkozás portfóliója bővül tovább.[30] Az óriásplatformok működése egyszerre vet fel versenyjogi, adatvédelmi, fogyasztóvédelmi és a magánszférához kapcsolódó kérdéseket, így adódik egy további kérdés, hogy vajon a jogalkalmazás képes lesz-e adekvát választ adni az ezen területek keresztmetszetében meghúzódó tevékenységek értékelésére,[31] vagy fennmarad a platformok számára kedvező helyzet, hogy az egyszerre több jogág megközelítését szükségszerűen átfedő, összetett tevékenységük értékelése hatásköri okokból csupán csak szűkebb narratívának kell megfeleljen.[32]

25 A szerzői jog és iparjogvédelem alá tartozó oltalmi tárgyak védelmének közös célja, hogy olyan szellemi produktumokat részesítsenek mértékük szerint különböző, de minden esetben kizárólagos, monopoljellegű, abszolút szerkezetű védelemben, amelyek vagyoni vagy egyéb jelentőséggel bírnak a jogosultjuk, és szélesebb értelemben a társadalom számára.

26 A szellemi alkotások oltalmi formáinak célja, hogy a szellemi alkotások létrehozói számára abszolút jellegű jogokat biztosítanak, amelyeknek tartalma elsősorban az, hogy a jogosult maga hasznosíthatja kizárólagosan alkotását, vagy engedélyezheti annak hasznosítását, vagy az oltalmi jogot – esetleg az abból származó hasznosítási jogot – átruházhatja bizonyos kivételekkel, és ezek fejében őt ellenszolgáltatás illeti meg.

27 Mike Walker: Competition Policy and Digital Platforms: Six Uncontroversial Propositions. *European Competition Journal*, vol. 16., no. 1. (2020) 1–10. https://doi.org/10.1080/17441056.2020.1730063

28 Uo. 5.

29 Pünkösty András: Merre tart az európai szintű platformszabályozás? – Áttekintés a platformok szabályozásának versenyjogi ösztönzőiről, valamint a fúziókontroll lehetséges fejlesztéséről. In: Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika Egyetemi Kiadó, 2023. 176–192. https://webshop.ludovika.hu/termek/konyvek/tarsadalomtudomany/az-internetes-platformok-kora/

30 Az FTC a technológiai óriás ellen – időben később – indított keresetében kifogásolta, hogy a Facebook versenyző magatartás helyett felvásárolta azokat a cégeket, amelyek veszélyt jelenthettek volna a piaci pozícióira. Az eredeti keresetet lásd Federal Trade Commission v. Facebook, INC. Case No.: 1:20-cv-03590. (2022. 01. 13.).

31 *Intersection of Competition, Consumer Protection, and Privacy.* International Competition Network, 2022. március 15. www.internationalcompetitionnetwork.org/news-events/intersection-sept2021/

32 Lásd a Bundeskartellamt Facebook-döntésének (B6-22/16, 2019. február 6.) a bírósági felülvizsgálata során kibontakozott jogértelmezési vitát, illetve az ahhoz kapcsolódóan 2021. március 24-én kezdeményezett előzetes döntéshozatali eljárást. ECLI:DE:OLGD:2021:0324.KART2.19V.00. (2022. 06. 26.).

4. Algoritmizált döntési folyamat mint új technológia

Az exponenciális korban minden felgyorsul,[33] és a digitalizáció egyre újabb és újabb jelenségekkel egészíti ki a világunkat, amelyekhez folyamatosan alkalmazkodnunk kell [34]. A datafikációval[35] az emberi emlékezet gyakorlatilag korlátlanul kiterjeszthető, a digitális adatokba kódolt jelentés kontextustól függően újra és újra értelmezhető, mert minden folyamat és tény, amelyhez digitális eszköz kapcsolódik, immár tetszés szerinti ideig és nagy részletességgel megfigyelhető, megmérhető és következtetések alapjául felhasználható. A digitális szolgáltatás igénybevétele során keletkező adatok csupán digitális lábnyomok, melyeknek „önmagukban nincsen jelentésük, a jelentést a feldolgozó alkotja."[36] Mára az adatkezelés nem a születési adataink, anyja neve, lakcím és személyiigazolvány-számunk kezelését jelenti, hanem napi több terabájt digitális lábnyom[37] feldolgozását. A teljesség igénye nélkül: algoritmus szűri ki a spameket az e-mailek közül,[38] segíti az online vásárlásokat,[39], állít összse szerződéseket,[40] minősít hitelkérelmeket,[41] állít föl orvosi diagnózisokat,[42] vezet autót,[43] őrzi a határt,[44] választ az állásra jelentkezők közül,[45] és akár a szabadságelvonásról döntő büntetőbírót is támogathatja a döntésében.[46] Az érintett szektorok és társadalmi hatások listája tehát igen széles: infokommunikáció, pénzügyek, HR-döntések, egészségügy, biztosítások, bűnüldözés, jogalkalmazás, és még sorolhatnánk az élet szinte minden területéről. Nem

33 Azzem Azhar: *The Exponential Age: How Accelerating Technology is Transforming Business, Politics and Society*. Diversion Books, USA, 2021.

34 Ennek az alkalmazkodásnak pedig az új jelenségek jogrendszeri adaptációja is része kell, hogy legyen, annak érdekében, hogy az irányítás lehetőségét velük kapcsolatban megőrizhessük.

35 A datafikáció vagy adatosodás széles körben elterjedt szóhasználat az elektronikus adatbázisok és a Big Data kapcsán, lényegében a környezetünkből származó digitális adatok felhalmozódására, a fizikai környezet digitális leképződésére utal, azaz egyre több digitális formában rögzített és tárolt adat áll rendelkezésünkre a világunkról. Lásd erről bővebben: Parti Tamás: A jog fölméréséről és az intézményi adatkutatásról. *Jogtudományi Közlöny*, 2021/11–12. 493–506.

36 Németh Renáta: A számok tényleg magukért beszélnek? *Replika,* 2015/3–4. 203–209.

37 A Big Data 6 V-vel leírható jellemzői közül ez a 'Variety': az összes online és offline tevékenység növeli az ember digitális lábnyomát (pl. online aktivitás monitorozása, CCTV, GPS, IoT [*Internet of Things*], banki tranzakciók stb.).

38 Thiago S. Guzella – Walmir M. Caminhas: A review of machine learning approaches to Spain filtering. *Expert Systems with Applications,* vol. 36., no. 7. (2009) 10206.

39 Cade Metz: Now anyone can tap the AI behind Amazon's recommendations. *Wired*, 2022. november 12. https://www.wired.com/2015/04/now-anyone-can-tap-ai-behind-amazons-recommendations

40 Lauren Henry Scholz: Algorithmic contracts. *Stanford Technology Law Review,* vol. 20., no. 2. (2017).

41 Danielle Keats Citron – Frank Pasquale: The Scored society. Due process for automated predictions. *Washington Law Review,* vol. 89., no. 1. (2014); Mikella Hurley – Julius Adebayo: Credit scoring in the era of Big Data. *The Yale Journal of Law and Technology,* vol. 18., no. 1. (2016).

42 William Nicholson Price II: Black-box medicine. *Harvard Journal of Law and Technology*, vol. 28., no. 2. (2015) 432–434.

43 Alexis C. Madrigal: The trick that makes Google's self-driving cars work. *The Atlantic*, 2014. május 15. https://www.theatlantic.com/technology/archive/2014/05/all-the-world-a-track-the-trick-that-makes-googles-self-driving-cars-work/370871/

44 Jose Sanchez del Rio – Daniela Moctezuma – Cristina Conde – Isaac Martin de Diego – Enrique Cabello: Automated border control e-gates and facial recognition systems. *Computers & Security*, vol. 62. (2016) 49.

45 Marianne Bertrand – Sendhil Mullainathan: Are Emily and Greg more employable than Lakisha and Jamal? A field experiment on labor market discrimination. *American Economic Review,* vol. 94., no. 4. (2004).

46 State v. Loomis, 881 N.W.2d 749 (Wis. 2016); Megan T. Stevenson – Christopher Slobogin: Algorithmic Risk Assessments and the Double-Edged Sword of Youth. *Washington University Law Review*, vol. 96. (2018) 681.

lehet elégszer hangsúlyozni, hogy a digitális lábnyomaink[47] mint metaadatok a feldolgozást követően válnak személyes adatokká, sőt sok esetben különleges[48] adatokká. A legfontosabb probléma, hogy az irodalom sokszor nem fordít kellő hangsúlyt az adat és az adatforrás elhatárolására. Zavart jelent a digitális adatok megértésében, hogy nem mindig világosak az 'adat', a 'jelentés' és az 'információ' összefüggései, amit tovább bonyolít a digitális adatoknak egy-egy sajátos tulajdonság oldaláról, például a forrásuk felől való kizárólagos megközelítése, mint az a személyes adatok esetében is történik. Amikor a jog adatról beszél, ritkán tisztázza, hogy magáról a digitális adatról van-e szó, vagy valami olyasmiről, ami ennek a digitális adatnak a forrásául szolgál. Digitális adat technológiai úton jön létre,[49] míg a személyes adat forrása az ember,[50] aki az adatot digitalizálja. Az adatok forrás szerinti megközelítése az adatvédelem egyik fontos kiindulópontja, ahogyan azt a már létező személyes adatok védelmét szolgáló normák is bizonyítják, ezek fókuszában a személyiségi jogok védelme áll, vagyis egyértelműen nem az adatot, hanem annak a forrását, az élő természetes személyt védik. Az adatokat a forrásaik oldaláról megközelítve fontos tehát különbséget tenni egyrészt a személyes adatok, másrészt az anonimizált adatok[51] és a nem személyes meta-[52] és egyéb digitális

47 Tudatos emberi tevékenység nyomán jöttek létre, de nem megfigyelésből és nem kutatói szándékból születtek. A digitális lábnyomokból rekonstruálhatók eddig rejtett szerkezetek és összefüggések. Dessewffy–Láng i. m. 158.

48 A Big Data technológiai környezetben az adatállományok egymásra vetítésével az adatokból különleges adatot, szenzitív adatot képes építeni, melyet az adatvédelmi rendelkezések többletvédelemmel láttak el, ami abban az időben nagyon is hatásosnak bizonyult [35 Avtv. 3. § (2) bek.; EK irányelv 8. cikk; Infotv. 5. § (2) bek.; GDPR 9. cikk (1)–(2) bek.]. Mező István: *Személyes adatok védelme az Európai Unió jogában és Magyarországon.* [Doktori értekezés]. Miskolc, Miskolci Egyetem Deák Ferenc Állam-és Jogtudományi Doktori Iskola, 2007. 132–134. http://midra.uni-miskolc.hu/ document/5522/1411.pdf.

49 Eszközök, rendszerek, platformok használata során megvalósuló szenzorokkal érzékelhető inger, jel, elektromágneses impulzus, amely bináris kóddá alakítva bitekké, vagyis adatokká válik. Tehát a digitális adat alapegysége a bit.

50 A természetes személyek digitalizációval összefüggő alapjogain, az emberi méltósághoz, emberi szabadsághoz, magántitokhoz, információs önrendelkezéshez való jogain és ezekhez kapcsolódó egyéb jogain nyugvó érintettség alapozza meg, amelyeken a GDPR és az arra épülő adatvédelmi normarendszer és a hozzájuk kapcsolódó titokvédelmi normák is alapulnak. Ezek a szabályok eredményezik azt, hogy az ilyen érzékeny forrásoktól származó adatbemeneteknek a titokjogosult, illetve adatvédelemre jogosult engedélye/hozzájárulása nélküli adattá konvertálása esetén a jogosult felléphet az adatot előállító ellen, és a digitális adatok esetében kérheti akár azok törlését is.

51 Fontos, hogy a DMA szövege értelmében a személyes adatnak minősülő keresési, kattintási és megtekintési adatokat anonimizálni kell. A DMA az *'anonymised'* szót használja, és bár nem definiálja a fogalmat, vélhetően ez az adatvédelmi rezsim 'anonim információk' fordulatának feleltethető meg. Továbbá a DMA tartalmazza a nem személyes adat fogalmát is, amely megfelel az adatvédelmi jogban ismert anonimizált adat fogalmának. Olyan adatokról van szó, amelyek nem köthetők meghatározott természetes személyhez, ennélfogva nem terjed ki rájuk a személyes adatok védelme. Azonban ez a jelen technológiai fejlettség mellett már nem felel meg feltétlenül a valóságnak. Az adatok anonimizálása nem feltétlenül magától értetődő, rutinszerűen végrehajtott műveletet jelent, hiszen számolni kell a nagy és összetett adatbázisok úgy nevezett deanonimizálásának, azaz a visszafejtésének, más szóval az eredeti állapot helyreállításának kockázatával.

52 Metaadat, információ az adatról. Releváns digitális nyomok többféle módon kinyerhetők az adathalmazból, például kulcsszavas kereséssel, dokumentumlekéréssel, metaadat-attribútumegyeztetéssel, hashfüggvény alapú kereséssel, vagy szabványos formátumú üzenetek keresésével. A dokumentumokat elérhetővé tevő rendszerekben, archívumokban a megtalálás, visszakeresés biztosítására szolgáló, a dokumentum feldolgozása során hozzárendelt, másodrendű információ. A legtöbb esetben a metainformációt metaadatnak lehet minősíteni, amennyiben megadják a metainformáció típusát. A metaadat a dokumentumok formai, tartalmi, strukturális jellemzőit, valamint használati kapcsolatait leíró, tipizált, másodrendű információ. Két fő típusa a forgalmi és a leíró metaadat, melyek közül az első gyűjtése, elemzése alkalmas eszköz ízlés- és véleménycsoportok beazonosítására, és ezáltal felhasználói profilok kialakítására. A leíró metaadat pedig a dokumentumok formai, tartalmi és strukturális jellemzőit biztosító, tipizált, másodrendű információ.

adatok között. Az általános adatvédelmi rendelet fogalomrendszerében személyes adat minden olyan adat, amely közvetlenül vagy közvetve azonosítani képes egy élő személyt.[53] E megközelítés értelmében a nem személyes adatok és az anonimizált adatok olyan adatok, amelyekből személyes információ nem származtatható. A megkülönböztetés gyakran meglehetősen nehéz, mivel a különféle adatkontextusok, eltérő korrelációk elemzése során egy-egy adathalmaz elemzése úgy is rámutathat egy konkrét élő személyre, hogy az elemzett adatok között e személy egyetlen személyes adata sem szerepel.[54] A mesterségesintelligencia-alapú Big Data-technológia[55] jellemzője, hogy nem személyes adatok elemzése eredményeként még akár szenzitív információk kinyerésére is képes. Már lassan egy évtizede közismert tény, hogy a Big Data-elemzésekre támaszkodva a magánszemély és az adat között felszámolt összefüggés helyreállítható,[56] például az eddig nem védett metaadatok használatával.[57] A digitális piacokról szóló rendelet[58] 2. cikkében határozza meg, a személyes adat, profilalkotás és hozzájárulás fogalmakat, melyeket az általános adatvédelmi rendelet meghatározására visszautalva használ. A személyes adat így a DMA rendelkezéseiben is az adatvédelmi rezsim 4. cikk 1. pontjában meghatározott személyes adat,[59] míg viszont az adatok lehetnek „aktusok, tények vagy információk bármilyen digitális megjelenítései, vagy az ilyen aktusok, tények és információk összeállításai, ideértve a hang-, kép- vagy audiovizuális felvétel formájában történő megjelenítést is", tehát tágabb kört von az adat fogalma alá. Míg az adatvédelmi rendelet a természetes személyek magánszféráját hivatott védeni, addig a fenti rendelet a belső piac megfelelő működéséhez szükséges szabályokat rögzíti, és e tekintetben nem elsődleges szempont, hogy az adat összefüggésbe hozható-e természetes személlyel vagy sem.[60]

53 A norma személyes adatot említ, holott a fentiek alapján itt valójában személyre vonatkozó információról van szó, mint ahogy azt az alkotmánybíróság is kifejtette a 15/1991(IV.13.) AB határozatban.

54 Csányi Gergely Márk – Vági Renátó – Nagy Dániel – Vadász Pál – Orosz Tamás: Challenges and Open Problems of Legal Document Anonymization. *Symmetry,* vol. 13., no. 8. (2021) 1490. https://doi.org/10.3390/sym13081490

55 A felhalmozott adatvagyon piacralépési korlátot jelenthet abban az esetben, ha az új belépő nem képes az adatokat olyan mértékben gyűjteni, vagy az adatokhoz olyan hozzáférést vásárolni, mint az inkumbens vállalkozás. Jellemző, hogy a már a piacon lévő nagy online szolgáltatásoknak hólabdaszerűen fokozódik az előnye, hiszen minél több adat áll rendelkezésükre, annál jobb szolgáltatást tudnak nyújtani, egyúttal annál több felhasználó fogja használni az adott szolgáltatást, többet tud fordítani a fejlesztésre és mindezzel fordítottan arányosan egyre kisebb az elvi valószínűsége, hogy egy versenytárs valaha fölzárkózzon az adott piacon. Hólabdaszerűen napról napra fokozódik az előnye, továbbá ennek eredményeként bővül a szolgáltatás specifikuma, javul a minősége, kifinomultabb lesz a megjelenése, illetve az egyedisége, egyénre szabott mivoltak okán egyre jobb szolgáltatást nyújtva egyre többet tud a fejlesztésre fordítani, erőforráselőnybe kerül, és mindezzel fordítottan arányosan egyre kisebb az elvi valószínűsége, hogy egyes versenytársak valaha fölzárkózzanak az adott piacon.

56 Paul Ohm: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review,* vol. 57. (2010) 1718.

57 The White House: *Big Data: Seizing Opportunities, Preserving Values.* Interim Progress Report, February 2015. https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

58 Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály, Digital Markets Act, DMA).

59 Személyes adat: azonosított vagy azonosítható természetes személyre – mint érintettre – vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

60 A DMA nemcsak a személyes, hanem a nem személyes adat fogalmát is meghatározza a 2. cikk (26) bekezdésében.

A Big Data-alapú adatgyűjtő és -elemző technikák[61] szemléltetésével szeretnék rámutatni arra, hogy az egyén kezébe adott jogvédelmi eszköz, az információs önrendelkezési jog mint alapjog ilyen magas szintű technológiai fejlettség mellett már nem feltétlenül adekvát. Az adatkészletek nem adatfelvételi céllal keletkeznek, hanem valamilyen más céllal de leginkább cél nélkül, egyszerűen naplózva bizonyos digitális aktivitásokat. Adatok tárolása rendszerint már az adatgyűjtési stációban is valamilyen távoli szerveren történt, hogy a szükséges műveleteket[62] el lehessen rajtuk végezni. A technológiai alkalmazás elterjedésének ebben a fázisában a hangsúly a gyakorlati előnyökön van: azon, hogy a sok szempont mérlegelését igénylő döntések a tömeges adathalmazt elemző algoritmus segítségével minden eddiginél több információ figyelembevételét követően hozhatók meg. A Big Data korában az az előfeltevés uralkodik, hogy ez a technológia biztosítja tömeges adatnak az emberi képességeinket jócskán meghaladó gyorsaságú értékelését.[63] A digitális lábnyomok[64] összegyűjtésére, összekapcsolására, értékesítésére és elemzésére hivatott iparág rohamosan fejlődik, továbbá százmilliók napi rutinja ismerhető meg a műholdak, WiFi- és mobilhálózatok által követett mozgásával, kommunikációs szokásaival, társas kapcsolataival, online kereséseivel.[65] Nem lehet belőle kimaradni,[66] nincs választási lehetőségünk. Mára már illúzió a személyes adatok

61 A különféle döntéseket támogató, tömeges adathalmazok elemzését és értékelését végző algoritmizált eljárások törvényszerűen jelentek meg az utóbbi évtizedben, amelyet a Big Data korának is neveznek. A jelenlegi definíció úgy hangzik, hogy az érintett természetes személyre vonatkozó bármely információ – vagyis nem minden adat személyes adat, annak az érintettre természetes személyre kell vonatkoznia. A nem természetes személyre vonatkozó vagy már álnevesített adatbázisok, összekapcsolva más, nyilvános adatbázisokkal igen könnyen visszanevesíthetők a Big Data-korszakban, így már minden adat személyes, sőt legtöbbször szenzitív adat (European Convention on Human Rights).

62 Az adatkezelési művelet nagy mennyiségű, általában nem strukturált és gyakran folyamatosan keletkező adat tárolását és feldolgozását jelenti elosztott rendszerarchitektúra segítségével, illetve az elemzési eszközök szoros integrálását a rendszerbe, ami jelentősen növeli a feldolgozási folyamat hatékonyságát. A tisztított adatok általában a felhő alapú számítástechnika által kínált szolgáltatások révén nemcsak a megfelelő adatbázisokban és adattárházakban tárolódnak, hanem a feldolgozás, az elemzés, az adatvizualizáció, a döntés-előkészítés, illetve -támogatás, valamint a szabályozás úgyszintén a felhőben történik meg.

63 Ezt szokták a Big Data-ra jellemző 6 V-ből a '*Volume*'-ként emlegetni, miszerint az addig felhasználhatatlan adatok is hirtelen felhasználhatókká válhatnak, ha minél több adat áll rendelkezésre, mert így a korreláció esélye nő. A mennyiség – nem a minőség – határozza meg, hogy a begyűjtött adatok információvá válhatnak-e, vagy sem.

64 Digitális lábnyom az, amit valahol hagyunk egy digitális rendszerben, és vagy kitörölhetetlenül ott marad, ahol nyomot hagyott, vagy másolatok készülhetnek róla. A különböző adatok és tartalmak azonosítanak, minősítenek, kiemelnek, látható idővonalra helyezik el az élet eseményeit, és megjósolhatóvá tesznek egyes viselkedésformákat. Egy-egy felhasználóhoz tartozik egy olyan adatkészlet, amely azonosítja, identifikálja, illetve elhelyezi más, szintén azonosítható adatkészletek hálózatában. A metaadat pedig adat az adatról, így a metaadatok maguk is adatok.

65 Ságvári Bence: Társadalomtudomány a Big Data korában. *Statisztikai szemle*, 2017/5. https://doi.org/10.20311/stat2017.05.hu0491 492

66 Nincs mindenki benne a hálózatban, de akit kizártak a hálózatból, annak is meghatározó a hálózathoz való viszonya – így emelkedik ki az információs fejlődés hatására az úgynevezett negyedik világ. Manuel Castells: *The End of the Millennium, The Information Age: Economy, Society and Culture. Volume III.* Oxford, Wiley-Blackwell, 2010. Magyar nyelven: Manuel Castells: *Az évezred vége*. (Berényi Gábor – Rohonyi András ford.) Budapest, Gondolat–Infonia, 2007.

kezelésének következetes nyomon követése egy kapuőr, mint online platform szolgáltató,[67] vagy más néven egy minősített adatkezelő[68] esetében.

Telefonjaink cellainformációi másodpercre pontosan megmondják, hogy merre járunk, lépésszámláló és fitness alkalmazásaink szokásos útvonalainkat is az elemző elé tárják. Minden kapcsolat, cselekvés, érdeklődés, tevékenység, amely „a hálózat kontextusában születik, történik"[69] nyomot hagy a rendszerben, megmarad, visszakereshetővé és elemezhetővé, kutathatóvá[70] válik a jelenben, vagy a távoli jövőben bármikor. Ezek a rendszerek mindenkori működési elvük szerint a lehető legnagyobb adathalmazhoz történő hozzáférést igénylik, ennek megfelelően az adatok gyűjtésekor sem szívesen vannak tekintettel az olyan korlátozásokra, mint a célhoz kötöttség, adattakarékosság vagy korlátozott tárolhatóság.[71] Ez abból az egyszerű törvényszerűségből ered, hogy az adatgyűjtés pillanatában nem szükséges – és nem is lehetséges – teljes körűen tisztában lenni a lehetséges felhasználási/hasznosulási lehetőségekkel, ugyanis ezeket a mesterséges intelligencia-rendszer maga fogja kimunkálni ismeretlen összefüggések megtalálásával és új következtetések levonásával. Ez adatvédelmi szempontból alapelvi szinten okoz problémákat az átláthatóság hiánya miatt, de az érintetti jogok tiszteletben tartása és jogérvényesítés elősegítése is komoly akadályokba ütközhet. Maguk a digitális adatok a gazdasági, és ezzel együtt a jogi forgalomban jelenleg is úgy funkcionálnak, hogy a velük végzett számítási, értékelési műveletek a pozitív jog számára csaknem láthatatlanok.[72] Az adatkezelők a technológiai védelem mellett a büntetőjog és a szerződésen kívüli felelősségi jog csatornáin, a *sui generis* adatbázisjogon keresztül, továbbá az üzleti titok védelmének szigorításával és büntetőjogi szankciók alkalmazásával quasi „ tulajdonosi" védelmet biztosítanak a hatalmukban lévő adatok vonatkozásában.[73]

67 A platform mai jelentésének kialakulásában Gillespie konkrét fordulópontot jelöl meg, mégpedig azt a pillanatot, amikor a Google felvásárolta 2006-ban a YouTube-ot. Gillespie szerint ezek a nagyvállalatok nemcsak a politikai befolyásolás, lobbizás, a szabályozói környezet finom alakítgatása révén igyekeznek saját maguk számára előnyös környezetet teremteni, hanem 'diszkurzív munkával' is, és ennek a diszkurzív munkának, tudatos keretezésnek volt a része az is, hogy a Google a YouTube-ot következetesen elkezdte 'platformnak' hívni, amikor a felvásárlás utáni marketingkommunikációban fokozatosan lecserélte a 'weboldal', 'szolgáltatás', 'fórum', 'közösség' kifejezéseket egységesen a 'platform' szóra.

68 Az online óriásplatformok kiemelt kockázatot jelentenek a jogellenes tartalmak terjesztése és a társadalmi károkozás tekintetében. Külön szabályok vonatkoznak azokra a platformokra, amelyek legalább a 10%-át elérik az Európában élő 450 millió fogyasztónak. 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, Digital Services Act, DSA). https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022R2065

69 Szűcs Zoltán – Yoo Jinil: Big Data az információs társadalom új paradigmája. *Információs Társadalom*, 2016/1. 9. http://real.mtak.hu/43454/1/it_2016_01_1_szuts_yoo.pdf

70 Dessewffy–Láng i. m. 157–160.

71 Mayer-Schönberger–Cukier (2013) i. m. 26.

72 A digitális világ tekintetében egyetlen számonkérés működik, miszerint a jogalkalmazó megkéri, hogy írják le és tegyék nyilvánossá a szabályzataikat. És mi – a hatóság – ezt képesek vagyunk ellenőrizni, hogy megfelel-e a hatályos előírásoknak.

73 Parti Tamás: *A digitális adatok tulajdoni adaptációja, a digitális javak vagyonjogi kölcsönhatásainak tükrében.* [Doktori értekezés.] Budapest, Károli Gáspár Református Egyetem Állam és Jogtudományi Doktori Iskola, 2023. 77–79. https://ajk.kre.hu/images/doc2023/di/PHD_ertekezes_Parti_Tamas.pdf

5. Összefoglaló

Álláspontom szerint az adataink kezelése tekintetében az egyre növekvő több terrabájt mennyiségű adatok átláthatatlan módon történő, felfoghatatlan mértékű kezelésén van a hangsúly,[74] így az adatbiztonság megvalósítása kell, hogy a cél legyen és nem az önrendelkezési joggyakorlás. A Big Data keretében értelmezhetetlenné válhatnak[75] az adatvédelem egyes alapvető elvei és fogalmai, mint például a személyes adat fogalma, a célhoz kötöttség követelménye, vagy a tájékoztatáson alapuló, önkéntes hozzájárulás, illetve a transzparencia megvalósítása is nehézségekbe ütközik,[76] sőt az óriásplatformok digitális működésük tekintetében nehezen elszámoltathatók, ellenőrizhetők.[77] Az elmúlt évtizedben a rendelkezésünkre álló robusztus és folyamatosan „termelődő" adatmennyiség, a számítási kapacitások exponenciális növekedése, a gyakorlatban is kipróbálható és belátható időn belül jelentős eredményt produkáló algoritmusok, valamint a különböző technológiák egyre szélesebb körű – konvergens – kapcsolódása immerzív virtuális világot hozott létre életünk szinte minden területén, melynek felépítését, működését kizárólag annak tulajdonosa képes átlátni és megérteni.

Az általános adatvédelmi rendelet egyik fontos célja az adatkezelők kötelezettségeinek és felelősségeinek erősítése volt, és legalább részben ezen keresztül a hasonló platformszolgáltatásokkal kapcsolatban felmerülő, harmadik országba irányuló jogszerűtlen adattovábbítások elleni fellépés.[78] A DSA és a DMA a jellemzően Európán kívülről nyújtott platform- és digitális szolgáltatásokkal érintett piacot kívánja szabályozni, és e tekintetben a jogsértések felmerülésének helye, az adatvédelmi követelmények megsértéséhez hasonlóan – legalábbis a legnagyobb kapuőröket és a digitális szolgáltatást nyújtókat figyelembe véve –, szintén a transzatlanti tengely. Ha a digitális gazdaság legfontosabb alapanyaga az adat, akkor megállapítható, hogy az európai adatok közel kilencven százalékát az Egyesült Államokban

74 A Big Data, vagyis a nagy mennyiségben rendelkezésre álló adatok alkalmazhatóságát jól szemlélteti a Pop Tarts nevű édesség vásárlása és a hurrikánok közötti összefüggés klasszikus példája. Az amerikai Walmart áruházlánc óránként több mint két terabájt adatot gyűjt. Charles Duhigg: *Power of habit: why we do what we do in life and business*. New York, Random House, 2014.

75 A rendszer inputjaként az adatok nagyon széles körűek lehetnek: származhatnak nyilvánosan elérhető szenzorokból, IoT-eszközökből, közösségi médiából, különböző ügyletekből, mesterséges intelligenciától, lehetnek geolokációs adatok, logfájlok, egészségügyi adatok, vagyis összességében a rendszerről és a környezetéről, valamint a rendszer és alrendszerei, illetve az egyes rendszerek közötti kölcsönhatásokból, kommunikációból, állapotjelentésekből származó adatok, valamint az adatok elemzésével, feldolgozásával, az elemzési és feldolgozási folyamatban alkalmazott módszerek és eljárások hatékonyságáról szóló adatok is.

76 Fülöp Réka: Személyes adatok védelme az internetet különös tekintettel azok vagyonjogi helyzetére. In: Péterfalvi Attila: *Szemelvények az információs jogok felügyeletének elmúlt 25 évéből*. Budapest, Nemzeti Adatvédelmi és Információszabadság Hatóság, 2020. 140.

77 A német versenyhatóság Facebook-döntése megállapította, hogy a Facebook visszaél az erőfölényes helyzetével akkor, amikor üzletfeleit (felhasználókat) lényegében korlátlan adatgyűjtést engedélyező és adatvédelmi szempontból is jogellenes feltételek elfogadására kényszeríti. Bundeskartellamt, B6-22/16. Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing. 2019. 02. 15. 526–527. pont.

78 Kis Kelemen Bence – Hohmann Balázs: A Schrems-ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. *Infokommunikáció és Jog*, 2016/2–3. https://bit.ly/3N6vEtV, 64–66.; Cedric Ryngaert – Mistale Taylor: The GDPR as Global Data Protection Regulation? *American Journal of International Law* vol. 114. (2020) 5–9. https://doi.org/10.1017/aju.2019.80

kezelik, és azokhoz az amerikai kormányzati szerveknek hozzáférésük lehet.[79] Az amerikai technológiai óriások az ingyenesség[80] látszatát keltő, úgynevezett zéróáras, valamint az egyre szélesebb körű hálózatban működő termékek és szolgáltatások fejlesztését kínáló fenntartható üzleti modellje az Egyesült Államokba szívja az európai adatvagyont,[81] amiről – a látszólagos tájékoztatáson felül – semmilyen információval nem rendelkezünk, továbbá sem átlátni, sem pedig számonkérni nem vagyunk képesek. A Big Data keretében értelmezhetetlenné válhatnak[82] az adatvédelem egyes alapvető elvei és fogalmai, mint például a személyes adat fogalma, a célhoz kötöttség követelménye vagy a tájékoztatáson alapuló, önkéntes hozzájárulás. A gyakorlatban a transzparencia nehézségekbe ütközik,[83] sőt az óriásplatformok digitális működésük tekintetében nehezen elszámoltathatók, ellenőrizhetők.[84]

Álláspontunk szerint az egyén kezébe adott jogvédelmi eszköz, az információs önrendelkezési jog mint alapjog ilyen magas szintű technológiai fejlettség mellett már nem feltétlenül adekvát. Az adataink kezelése tekintetében cél, hogy digitális lábnyomaink, személyes adataink ne kerüljenek illetéktelen kezekbe, ne okozzanak az érintett tekintetében joghátrányt, tehát a cél az adatbiztonság megvalósítása. A technológiavezérelt döntéshozatal dacol az érdemi kivizsgálással és elszámoltathatósággal, holott e kettő alapfeltétele volna a tisztességes eljárásnak.[85] A technológiai óriásplatformok tekintetében az adatvédelem mára már nem az önrendelkezési jog gyakorlása, hanem inkább a jogi és technológiai, valamint szervezéstechnikai alapú adatbiztonsági kérdés, melynek okán a személyes adatok védelme helyett talán inkább a személyes adatok kezelésének szabályain lesz a hangsúly a jövőben. Ez a koncepció túlmutat az országhatárokon, és keretet kínál a nemzetek közötti együttműködés előmozdítására a technológiai fejlődés által támasztott kihívások kezelésének érdekében.

79 Samuel Stolton: LEAK: Commission in Bid for EU Data Sovereignty with Digital Decade Targets. *Euractive*, 2021. március 8. https://bit.ly/46InNtT; Sean Fleming: What is Digital Sovereignty and Why is Europe So Interested in it? *World Economic Forum,* 2021. március 15. https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty

80 Az online figyelemkereskedők szolgáltatásai ingyenesen indultak és többek között ennek is jelentős mértékben köszönhetően gyűjtöttek hatalmas felhasználói tömeget. Csak miután dominánssá váltak, akkor emelték meg a reklámok arányát, melynek során jelenleg a felhasználók már kétszeresen fizetnek az úgynevezett ingyenes szolgáltatásokért: az adataikkal és a figyelmükkel. Az ingyenesség gyakorlata, vagyis az adattal fizetés a pénzzel fizetés alternatívája lesz, ami az EU adatvédelmi biztosa szerint ellentétes az adatvédelem szellemiségével, mert a személyes adatok védelme alapvető jog, ezért a személyes adatok nem tekinthetők árunak.

81 Az EUB 2020 júliusában hozott ítélete meg is erősíti ezt az aggodalmat. Ebben az ítéletében az EUB megállapította, hogy az EU és az Egyesült Államok közötti adatvédelmi pajzs keretrendszere már nem megfelelő mechanizmus az EU adatvédelmi követelményeinek való megfeleléshez a személyes adatoknak az Európai Unióból az Egyesült Államokba való továbbítása vonatkozásában. C-311/18 sz. ügy Adatvédelmi biztos kontra Facebook Ireland és Schrems [ECLI:EU:C:2020:559] 180–184.

82 A Big Data működésének lényege és egyben a legnagyobb előnye is, hogy célzás nélkül képes robusztus mennyiségű adatot gyűjteni; ráadásul egyszerre mindent, mindenhonnan, és bármilyen formában.

83 Fülöp i. m. 140.

84 A német versenyhatóság Facebook-döntése megállapította, hogy a Facebook visszaél az erőfölényes helyzetével akkor, amikor üzletfeleit (felhasználókat) lényegében korlátlan adatgyűjtést engedélyező és adatvédelmi szempontból is jogellenes feltételek elfogadására kényszeríti. Bundeskartellamt, B6-22/16. sz. Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing. 2019. 02. 15. 526–527. pont.

85 Ari Ezra Waldman: Power, process, and automated decision-making symposium. Rise of the machines. Artificial intelligence, robotics, and the reprogramming of law. *Fordham Law Review*, vol. 88., no. 2. (2019) 613–632.

Meta kontra Bundeskartellamt

A platformszabályozás kapcsolata az adatvédelemmel

Kálmán Kinga

2023. július 4-én az Európai Unió Bírósága (a továbbiakban: EUB, vagy Bíróság) ítéletet hozott a Meta kontra Bundeskartellamt ügyben (a továbbiakban: Meta-döntés, vagy döntés).[1] A határozat fontos követelményeket támaszt az EU általános adatvédelmi rendeletének (a továbbiakban: GDPR)[2] értelmezésével, valamint a versenyhatóságok és az adatvédelmi felügyeleti hatóságok közötti lojális együttműködéssel kapcsolatban, különösen a fogyasztók személyes adatainak a közösségimédia-platformok által közvetlen üzletszerzés céljából történő személyre szabott felhasználása tekintetében. A döntésben a Bíróság a digitális szolgáltatásokról (*Digital Services Act,* a továbbiakban: DSA)[3] és a digitális piacokról szóló *(Digital Markets Act*, a továbbiakban: DMA)[4] uniós rendeleteket még nem alkalmazhatta, mindazonáltal nem hagyta figyelmen kívül, hogy a döntést megelőző eljárás során teljesen megváltozott a platformokat övező szabályozási környezet. Ebből kifolyólag a Bíróság következtetéseit az adatvédelem uniós keretének értelmezésén keresztül éri el.

A tanulmány célja kettős: egyrészről a Meta-döntés analitikus jogesetelemzésén keresztül megvizsgálja, mennyiben illeszkedik az EUB értékelése és a GDPR a DSA és a DMA vonatkozó keretrendszerébe. E vizsgálat során a DSA-hoz fűződő viszony nagyobb hangsúllyal kerül kifejtésre. Másrészt a szerző górcső alá veszi, hogyan és mennyiben formálják a döntésben kifejtett mércék főként az adatvédelmi joggyakorlatot a platformok működésén túl, akár általánosabb jelleggel is. Míg az első cél tekintetében az elemzés a döntés, a vonatkozó jogszabályi rendelkezések és szakirodalom szintetizálásán alapul, utóbbi esetében mindez kiegészül a releváns esetjog sarokköveinek elemzésével is. A kitűzött célokhoz illeszkednek a tanulmány hipotézisei is, melyek szerint (i) a döntés alkalmazhatóságuk hiányában is a DSA és a DMA rendelkezéseinek megfelelő megállapításokat tesz, mindezzel azonban (ii) a platformok különleges helyzetén túlmutató, általánosan érvényes mércéket állít fel, miközben az értékelés szempontjait a platformok sajátosságai vezérlik.

A tanulmány szerkezetét tekintve négy logikai egységre oszlik: (1.) a Meta-döntés elemzését követően (2.) bemutatja a döntés (és ezáltal a GDPR) kapcsolatát a DSA-val és a DMA-val, majd (3.) kitér a versenyhatóságok adatvédelmi jogsértés vizsgálatára kiterjedő hatáskörére. Végül, de nem utolsó sorban (4.) az értékelésből levonható következtetésekkel, valamint a jövőre nézve tehető latolgatással zárul. Fontos kiemelni, hogy a tanulmány a döntést és a mögötte húzódó keretrendszert túlnyomó részben adatvédelmi szempontból

1 C-252/21. sz. ügy Facebook Inc. és társai kontra Bundeskartellamt [ECLI:EU:C:2023:537].

2 (EU) 2016/679 rendelet 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, HL L 119, 2016. 5. 4., 1–88. o.

3 (EU) 2022/2065 rendelet a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról, HL L 277, 2022. 10. 27., 1–102. o.

4 (EU) 2022/1925 rendelet a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról, HL L 265, 2022. 10. 12., 1–66. o.

közelíti, kizárólag érintve az azzal kapcsolatban álló versenyjogi aspektusokat. Konklúzióként előrevetítem, hogy míg a döntésben felsorolt szempontok értékelése alkalmas lehet a platformokra vonatkozó jogi kötelezettségek kimunkálására, általános alkalmazhatósága ugyanakkor kérdéseket vet fel.

1. A Meta-döntés elemzése

1.1. Az ügy tényállása

A német szövetségi versenyhatóság (Bundeskartellamt) 2016-ban eljárást indított[5] a Meta Platforms, a Meta Platforms Ireland és a Facebook Deutschland ellen, amelyben arra a következtetésre jutott, hogy a Facebook használata során keletkezett, valamint a Facebookon túli adatok [egyéb Meta platformokon (pl. Instagram vagy Whatsapp) regisztrált fiókokban kezelt személyes adatok és a Facebookkal programinterfészeken keresztül összekapcsolt harmadik weboldalak és alkalmazások megtekintésére vonatkozó adatok (utóbbi két kategória a továbbiakban: off-Facebook-adatok)] ÁSZF-re alapított összekapcsolt kezelésével a Meta visszaél erőfölényes helyzetével és megtiltotta ezen gyakorlat folytatását.

A Bundeskartellamt értékelése szerint a Facebook ÁSZF-jének adatkezelési rendelkezései – mint az említett erőfölény megnyilvánulásai – visszaélésszerűek, mivel az off-Facebook-adatok ÁSZF-ben előírt kezelése a GDPR-ba ütközik többek között azért, mert nem rendelkezik a Facebook érvényes jogalappal az összekapcsolt adatkezelésekre. Az ügy az Oberlandesgericht Düsseldorfon (Düsseldorfi Regionális Felsőbíróság, Németország) keresztül előzetes döntéshozatali eljárás keretében a Bíróság elé került.

1.2. A döntés érvelése

Athanasios Rantos főtanácsnoki indítványához[6] (a továbbiakban: főtanácsnoki indítvány) hasonlóan a Bíróság négy csoportba tagolta az előzetes döntéshozatalra utalt kérdéseket:

f) a versenyhatóságok személyes adatok kezelésére vonatkozó szabályok megsértésének megállapítására és szankcionálására vonatkozó hatásköre, valamint az általános adatvédelmi rendelet értelmében vett fő hatósággal való együttműködési kötelezettségek (első és hetedik előzetes döntéshozatalra terjesztett kérdés);
g) a különleges személyes adatok kezelésének speciális feltételei és azok értelmezése (második kérdés);
h) az off-Facebook személyes adatok kezelésének jogszerűsége egyes, a Facebook ÁSZF szerinti esetekben (harmadik, negyedik és ötödik kérdés), és

5 Ld.: Bundeskartellamt: *Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules.* Sajtóközlemény, 2016. március 2.https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html.

6 C-252/21. sz. ügy Athanasios Rantos főtanácsnok indítványa: Facebook Inc. és társai kontra Bundeskartellamt [ECLI:EU:C:2022:704.].

i) az erőfölényben lévő adatkezelő vállalkozásnak a személyes adatok kezelésére vonatkozóan adott hozzájárulás érvényessége (hatodik kérdés).

1.2.1. Versenyhatóságok hatásköre adatvédelmi tárgykörben

A Bíróság értékelése során kiindulópontként van jelen az a megegyezés, miszerint a személyes adatokhoz való hozzáférés és ezen adatok kezelésének lehetősége ma már a digitális gazdaságban működő vállalkozások közötti verseny jelentős tényezőjét képezi, így annak figyelmen kívül hagyása a versenyhatóságok részéről sértené a versenyjog Unión belüli tényleges érvényesülését.[7]

Noha sem a GDPR, sem más uniós jogi aktus nem ír elő e tekintetben különös szabályokat, ez nem változtat azon, hogy a GDPR mint uniós jogszabály alkalmazása során valamennyi érintett nemzeti hatóságot köti az EUSZ 4. cikk (3) bekezdésében rögzített lojális együttműködés elve.[8] Ezenkívül nincs olyan jogszabály, amely megtiltaná a nemzeti versenyhatóságoknak, hogy feladataik ellátása keretében megállapítsák, hogy sérti a GDPR-t az erőfölényben lévő vállalkozás által végzett olyan adatkezelés, amely ezen erőfölénnyel való visszaélésnek minősülhet,[9] így elvégezheti ezen vizsgálatot anélkül, hogy elvonná az adatvédelmi hatóságok hatáskörét.[10]

Ilyen esetekben ugyanakkor a lojális együttműködés követelményére tekintettel a nemzeti versenyhatóságnak és az adatvédelmi hatóságnak együtt kell működnie a GDPR egységes alkalmazásának biztosítása érdekében.[11] Ezen együttműködés legfontosabb sarokköve, hogy mindkét hatóság köteles tiszteletben tartani egymás jogköreit és hatásköreit,[12] a versenyhatóságnak ellenőriznie kell, hogy e magatartás vagy hasonló magatartás már tárgyát képezte-e az illetékes adatvédelmi hatóság vagy akár a Bíróság határozatának, és amennyiben igen, attól nem térhet el, mindazonáltal *szabadon vonhatja le belőle* a versenyjog szempontjából releváns következtetéseket.[13]

Emellett a versenyhatóság köteles egyeztetést kezdeményezni az adatvédelmi hatóságokkal, és kérnie az együttműködést az adatvédelmi kérdésekben, vagy abban, hogy informálódjon és eldöntse, meg kell-e várnia, hogy a saját értékelésének megkezdése előtt azok határozatot hozzanak.[14]

7 Meta-döntés 51. pont.
8 Uo. 53. pont.
9 Uo. 46. pont.
10 Uo. 48–49. pont.
11 Uo. 52. pont.
12 Uo. 54. pont.
13 Uo. 56. pont.
14 Uo. 63. pont.

1.2.2. Különleges személyes adatok kezelése

A második kérdés kapcsán a Bíróság először is úgy foglal állást, hogy a GDPR 9. cikkének (1) bekezdését[15] úgy kell értelmezni, hogy abban az esetben, ha az online közösségi hálózat felhasználója azon keresztül weboldalakat vagy alkalmazásokat nyit meg, és adott esetben feliratkozás vagy online megrendelések során ott adatokat ad meg, az integrált interfészek, cookie-k vagy hasonló adatrögzítési technológiák segítségével gyűjtött személyes adatok között tilos személyes adatok különleges kategóriáit gyűjteni.[16]

Emellett, a GDPR 9. cikke alóli kivételként a 'nyilvánosságra hozatal'[17] kizárólag az érintett által kifejezetten nyilvánosságra hozott adatokra vonatkozhat,[18] és jelen esetben az érintett legfeljebb arra számíthat, hogy a weblap vagy alkalmazás kezelője férhet hozzá az ezen tevékenység során keletkező adatokhoz és azokat semmiképp sem osztja meg a nyilvánossággal.[19]

Ezek alapján az érintett nem hozza kifejezetten nyilvánosságra az e megnyitásra vonatkozó, az ezen online közösségi hálózat üzemeltetője által cookie-k vagy hasonló adatrögzítési technológiák révén gyűjtött adatokat. Amennyiben az érintett felhasználók ténylegesen rendelkeznek választási lehetőséggel, amikor weboldalakon vagy alkalmazásokban adatokat visznek be, vagy olyan kiválasztási gombokra kattintanak, mint például a 'Tetszik', vagy a 'Megosztás', csak a szándékos egyéni beállítás alapján egyértelműen kifejezett döntés esetén tekinthetők úgy, mint akik kifejezetten nyilvánosságra hozzák különleges személyes adataikat.[20]

1.2.3. Egyes adatkezelési jogalapok jogszerűsége

A tartalmak személyre szabása, valamint a szolgáltatás biztosítása céljából végzett, szerződés teljesítése jogalapra helyezett adatkezelés körében a Bíróság megerősíti, hogy egyrészről a Meta szolgáltatásokat személyre szabás nélkül, másrészről összekapcsolás nélkül külön-külön is igénybe lehet venni, ezért egyik adatkezelés sem *objektíve elengedhetetlen* a szerződés teljesítéséhez.[21] A Bíróság objektíve elengedhetetlennek akkor ítéli az adatkezelést, ha a szerződés fő tárgya nem lenne elérhető a szóban forgó adatkezelés nélkül, tehát nem állnak rendelkezésre más, gyakorlatban megvalósítható és kevésbé beavatkozó jellegű megoldások.[22]

A Bíróság a jogos érdek igazolása körében hangsúlyozza egyrészt annak vizsgálatát, hogy az adatkezeléshez fűződő jogos érdek észszerűen nem érhető-e el ugyanolyan hatékonyan más, kevésbé alapjog-korlátozó eszközökkel, másrészt az adattakarékosság érvényesülését, miszerint a személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell

15 GDPR 9. cikk (1) bekezdés: A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.

16 Meta-döntés 73. pont.

17 GDPR 9. cikk (2) bekezdés e) pont: Az (1) bekezdés nem alkalmazandó abban az esetben, ha az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott.

18 Meta-döntés 72. pont.

19 Uo. 78. pont.

20 Uo. 81–82. pont.

21 Uo. 102–104. pont.

22 Uo. 98–99. pont.

lenniük, és a szükségesre kell korlátozódniuk.[23] Emellett fontos az érintett észszerű elvárásait mérlegelni az alapján, hogy milyen mértékű, hatású és terjedelmű adatkezelésre számíthat.

Értékelése alapján a Facebookhoz hasonló online közösségi hálózat felhasználói nem számíthatnak még az ingyenesség ellenére sem arra, hogy hozzájárulás nélkül – az összekapcsolások által – ilyen széleskörűen, potenciálisan korlátlan mennyiségben dolgozzák fel és kapcsolják össze személyes adataikat. Ezen adatkezelés nyomonkövetésszintű hatással bírhat a felhasználóra, a folyamatos megfigyelés érzésének keltésével.[24]

Az illetékes bűnüldöző és büntetés-végrehajtási szerveknek a bűncselekmények megelőzése, felderítése és üldözése érdekében történő tájékoztatásával kapcsolatos cél esetében a Bíróság megállapítja, hogy a Meta-hoz hasonló magánjogi gazdasági szereplő nem hivatkozhat ilyen, a gazdasági és kereskedelmi működésétől idegen jogos érdekre, kivéve akkor, ha az objektív módon szükséges az őt terhelő jogi kötelezettség teljesítéséhez.[25]

Az érintett, vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges adatkezelés körében a Bíróság utal a GDPR (46) preambulumbekezdésére, amely példaként erre az adatkezelésre a járványok és azok terjedésének nyomon követését, valamint a humanitárius vészhelyzeteket hozza. Ebből kiindulva az olyan adatkezelő, amelynek tevékenysége alapvetően gazdasági és kereskedelmi természetű, nem hivatkozhat a felhasználói vagy más személyek életéhez fűződő alapvető érdek védelmére annak érdekében, hogy abszolút, ugyanakkor absztrakt és megelőző jelleggel igazolja az off-Facebook-adatok kezelésének jogszerűségét.[26]

A GDPR 6. cikk (1) bekezdés *e)* pontjának[27] alkalmazása tekintetében a Bíróság a kérdést előterjesztő bíróság feladatává teszi annak vizsgálatát, hogy a Metát közérdekből végzett feladat végrehajtásával vagy közhatalmi jogosítvány gyakorlásával bízták-e meg, különösen közérdekű kutatás, valamint a biztonság, integritás és a védelem elősegítése érdekében. Ugyanakkor a Bíróság előrebocsátja, hogy a Meta tevékenységének típusára és alapvetően gazdasági és kereskedelmi jellegére tekintettel kevéssé tűnik valószínűnek, hogy közérdekű feladattal vagy közhatalmi jogosítvánnyal bízzák meg.[28]

1.2.4. A hozzájárulás mint adatkezelési jogalap jogszerűsége

A hozzájárulás önkéntessége körében a Bíróság arra a következtetésre jutott, hogy az a körülmény, hogy a Meta erőfölényben van az online közösségi hálózatok piacán, önmagában nem zárja ki, hogy a felhasználók érvényesen hozzájárulhassanak a személyes adataik kezeléséhez. Mindazonáltal fontos tényezőnek minősül annak meghatározása szempontjából, hogy a hozzájárulást ténylegesen érvényesen, és önkéntesen adták-e meg, amit az adatkezelőnek kell bizonyítania.[29]

23 Uo. 109. és 121. pont.
24 Uo. 116–118. pont.
25 Uo. 124. pont.
26 Uo. 135–137. pont.
27 GDPR 6. cikk (1) bek. *e)* pont: A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.
28 Meta-döntés 133. pont.
29 Uo. 154. pont.

Emellett kimondta, hogy a felhasználóknak jogosultnak kell lenniük arra, hogy a szerződéskötési folyamat keretében egyedileg megtagadják a szerződés teljesítéséhez nem szükséges konkrét adatkezelési műveletekhez való hozzájárulásukat, anélkül, hogy kötelesek lennének teljes egészében lemondani a szolgáltatásról. Ebben az esetben a felhasználónak – adott esetben megfelelő díjazás ellenében – olyan egyenértékű alternatívát kell felajánlani, amelyhez nem kapcsolódnak ilyen adatkezelési műveletek. Emellett biztosítani szükséges, hogy a felhasználó a Facebook- és az off-Facebook-adatok kezeléséhez külön hozzájárulást adhasson.[30]

2. A Meta-döntés és a GDPR kapcsolata a DSA-val és a DMA-val

Az elmúlt évek során a Bíróság számos alkalommal vizsgálta és értékelte a platformok működésének konformitását az Európai Unió (a továbbiakban: EU) jogi keretrendszerével. Ezen jogfejlesztő tevékenysége nyomán a Bíróság többek között kidolgozta a GDPR 17. cikke szerinti 'elfeledtetéshez való jog' alkalmazhatóságát a Google keresési találataira,[31] valamint pontosította a (szerzői) jogsértést megvalósító tartalmak közvetítéséért felmerülő platform-felelősség határait.[32] Emellett versenyjogi szempontból értékelte többek között az olyan platformspecifikus kereskedelmi magatartásokat, mint például az Android operációs rendszer versenykorlátozó összekapcsolása a Google Play Áruházzal,[33] vagy a Google keresőben a Google-féle árösszehasonlító szolgáltatás eredményeinek előre sorolásával megvalósuló erőfölénnyel való visszaélés.[34]

A 'platformokra szabott' esetjog gazdagsága legtöbb esetben az EU jogi keretrendszerének válságjeleit indikálta, amely arra vezethető vissza, hogy a jogalkotás képtelen volt hatásosan kezelni a platformok elterjedésével megjelenő újszerű, az akkor hatályos keretek között nehezen, vagy egyáltalán nem elhelyezhető kérdéseket.[35] A jogalkotói válaszlépések lassan követték az EUB munkáját: 2022-ben elfogadták az EU két átfogó 'platformjogszabályaként' a DSA-t és a DMA-t. A rendeletek előkészítése és elfogadása hozzávetőlegesen azonos időszakban folyt végig, mint a Meta döntés és az alapjául szolgáló nemzeti eljárások menete. Az időbeli egyezőségből kiindulva is jól látható, hogy a döntésben visszaköszönnek a DSA és a DMA rendelkezései és a mögöttük húzódó szabályozási irányok, amelyekről részletesen a következő két alfejezetben írok.

30 Uo. 150–151. pont.

31 Ld.: C-131/12. sz. ügy Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja Gonzalez [ECLI:EU:C:2014:317]; C-136/17. sz. ügy GC és társai kontra Commission nationale de l'informatique et des libertés (CNIL) [ECLI:EU:C:2019:773]; C-507/17. sz. ügy Google LLCkontra Commission nationale de l'informatique et des libertés (CNIL) [ECLI:EU:C:2019:772]; és C-460/20. sz. ügy TU és RE kontra Google LLC [ECLI:EU:C:2022:962].

32 Ld.: a teljesség igénye nélkül: C-70/10. sz. ügy Scarlet Extended SA [ECLI:EU:C:2011:771]; C-360/10. sz. ügy SABAM [EU:C:2012:85]; C-18/18. sz. ügy Glawischnig-Piesczek [ECLI:EU:C:2019:821]; és C-682/18. és C-683/18. sz egyesített ügyek Frank Peterson kontra Google LLC és társai, valamint Elsevier Inc. kontra Cyando AG [ECLI:EU:C:2021:503].

33 T-604/18. sz. ügy Google LLC és Alphabet, Inc. kontra Európai Bizottság [ECLI:EU:T:2022:541].

34 T-612/17. sz. ügy Google LLC, korábban Google Inc. és Alphabet Inc. kontra Európai Bizottság [ECLI:EU:T:2021:763].

35 A platformok megjelenése és elterjedése által okozott ' válságról' ld. bővebben: Ződi Zsolt: *Platformjog.* Budapest, Ludovika, 2023. 4–5. fejezet.

2.1. A Meta-döntés és a GDPR kapcsolata a DSA-val

A Meta döntés a hirdetésekre vonatkozó megállapításai körében kapcsolódik a DSA-hoz. A DSA alapján a reklámok célzásához szükséges beszerezni az érintett hozzájárulását,[36] amely a GDPR 22. cikke szerinti profilalkotás[37] három lehetséges jogalapját (uniós vagy tagállami jogszabály felhatalmazása; szerződés teljesítése; az érintett hozzájárulása)[38] szűkíti le online platformok adatkezelése esetén. Ebből következően a reklám célzásához nem lehetséges a GDPR adatkezelési jogalapjai közül a szerződés teljesítésére vagy a jogos érdekre való hivatkozás. Ez a hozzájáruláson alapuló *opt-in* modell összhangban áll a GDPR szerinti adattakarékosság, valamint a *privacy by design and default* alapelvi követelményeivel is.[39]

Emellett a GDPR szerinti hozzáférési és tiltakozási jog gyakorlását is segítheti a DSA 26. cikk (1) bekezdésének *d)* pontja, amely előírja az online platformot üzemeltető azon szolgáltatóknak, akik online interfészükön hirdetéseket jelenítenek meg, hogy biztosítsák a hirdetésekre vonatkozó információk (pl. hirdető személye, hirdetés finanszírozása, célzásra használt paraméterek) elérhetőségét.[40] A hirdetésekről szóló információk DSA alapján történő kötelező közzététele ezáltal a GDPR-ban foglalt általános,[41] valamint a profilalkotáshoz kötődő speciális[42] tájékoztatási kötelezettség kiegészítéseként is értelmezhető.

Míg a GDPR az érintett kifejezett hozzájárulásához köti a profilalkotáson alapuló hirdetések megjelenítését,[43] addig a DSA tiltja az online platformokon, amennyiben az személyes adatok különleges kategóriáinak, vagy kiskorúak adatainak[44] felhasználásán alapul.[45] Bár a DSA tilalma a különleges személyes adatok felhasználásával történő, profilalkotáson alapuló hirdetések 'megjelenítésére' vonatkozik – nem pedig magára a profilalkotási tevékenységre –,

36 DSA (68) preambulumbekezdés.

37 A GDPR 22. cikke azon profilalkotásokra terjed ki, amelyek az érintettre nézve joghatással járnak, vagy hasonlóképpen jelentős mértékben érintik.

38 GDPR 22. cikk (1)–(2) bekezdés.

39 E körben ld. bővebben: European Data Protection Supervisor Opinion 1/2021 on the Proposal for Digital Services Act. 2021. február 10. 16–17. https://www.edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

40 Tóth András: A Digital Services Act és az EU fogyasztóvédelmi joga. *KözigazgatásTudomány*, 2023/2. 32.

41 GDPR 13–14. cikk.

42 GDPR 22. cikk (3) bekezdés.

43 GDPR 9. cikk (1) bek. *a)* pont; 22. cikk szerinti profilalkotás esetén: GDPR 22. cikk (4) bekezdés.

44 A DSA 28. cikk (3) bekezdése alapján kiskorúak profilalkotáson alapuló célzás tilalmának teljesítése nem kötelezi az online platformot üzemeltető szolgáltatókat arra, hogy további személyes adatokat kezeljenek annak értékelésére, hogy a szolgáltatás igénybe vevője kiskorú-e. Az ehhez kapcsolódó életkorellenőrzés hatékony és jogszerű megvalósítására azonban nem érhető el általános útmutatás, amely már a GDPR 8. cikkének alkalmazása során is gondot okoz. Erre a kérdésre a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) is csupán meglehetősen absztrakt szintű állásponttal szolgál azáltal, hogy az adatkezelő feladatává teszi a kérdést. Ld: NAIH-4317-2/2021.

45 DSA 26. cikk (3) bekezdés. Itt szükséges megjegyezni, hogy a DSA a hirdetések megjelenítésének tilalmát mondja ki a különleges személyes adatokon alapuló profilozás esetén, míg a döntés az ilyen profilozás adatvédelmi jogszerűségével foglalkozik. Mindazonáltal figyelembe véve, hogy a platformok tevékenysége során a profilozás döntő többségében online hirdetések megjelenítése céljából történik, a DSA és a döntés vonatkozó részei összekapcsolódnak. A DSA és a GDPR főbb kapcsolódási pontjairól ld. bővebben: Gabriela Zanfir-Fortuna – Vasileios Rovilos: Eu's Digital Services Act Just Became Applicable: Outlining Ten Key Areas of Interplay With the GDPR. *Future of Privacy Forum*, 2023. augusztus 31. https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/.

azt a GDPR-ban a személyes adatok profilalkotás céljából történő adatkezelésre vonatkozó kötelezettségekkel együtt kell értelmezni.[46] Ez azt jelenti, hogy a kifejezett hozzájárulás nem ad zöld utat a profilozásnak az online platformokon, amennyiben azok különleges adatkategóriák vagy a kiskorúak adatainak feldolgozására építenek. Ezek alól a rendelkezések alól a jogszabály értelmezése alapján nincsenek kivételek.[47] A Meta-döntés e körben járul hozzá a DSA értelmezéséhez és alkalmazásához, amikor kimondja, hogy a Facebook különleges személyes adatokat kezel azáltal, hogy az érintett az összekapcsolt hálózatban bármely Meta terméken keresztül, potenciálisan különleges személyes adatokat gyűjtő weboldalak megnyitása és kezelése során ott különleges személyes adatokat ad meg.[48]

2.2. A Meta-döntés és a GDPR kapcsolata a DMA-val

A DMA alapján a kapuőrök (mint amilyen a Meta is) kizárólag a végfelhasználó hozzájárulása alapján

a) kezelhetnek harmadik személy szolgáltatásának használata során gyűjtött személyes adatokat online hirdetésküldés céljából;
b) kapcsolhatnak össze különböző szolgáltatásaikból, vagy harmadik személy szolgáltatásaiból gyűjtött személyes adatokat;
c) használhatják fel az alapvető platformszolgáltatásaik használatából származó személyes adatokat más szolgáltatások céljaira, és
d) léptethetik be az érintettet a kapuőr más szolgáltatásaiba személyes adatok összekapcsolása céljából.[49]

Ezen rendelkezés a Meta-döntés vonatkozó megállapításait[50] mintegy tárgytalanná teszi, mivel azok a kapuőrök esetében teljesen megegyeznek a DMA tényállásával; nem véletlenül, hiszen a DMA egyébként is kazuisztikus jellegű szabályozásával összhangban annak 5. cikkét a Meta-döntés tényállása 'ihlette'.[51]

A hozzájárulás kötelezővé tételével a DMA (és ezzel összhangban a Meta-döntés is) a GDPR-ban szereplő hat jogalap közül a legtörékenyebbet engedi csak meg a kapuőröknek. Ha a végfelhasználó hozzá is járul az ilyen típusú adatkezelésekhez, azt bármikor visszavonhatja a GDPR 7. cikk (3) bekezdése alapján, aminek lehetőségét az adatkezelő köteles is biztosítani. Emiatt a hozzájárulásra támaszkodás nem nyújt hatékony jogalapot az adatkezelők szempontjából, viszont jelentősen megnöveli az érintettek alkupozícióját.[52]

46 Uo.

47 Florina Pop – Jannigje Bezemer – Laura Grant: The Digital Services Act: creating accountability for online platforms and protecting users' rights? *EIPA Blog*, 2022. szeptember 6. https://www.eipa.eu/blog/the-digital-services-act-creating-accountability-for-online-platforms-and-protecting-users-rights/

48 Meta-döntés 73. pont.

49 DMA 5. cikk (2) bekezdés.

50 Ld. a harmadik, negyedik és ötödik kérdésekre vonatkozó megállapításokat.

51 Peter J. van de Waerdt: Meta v Bundeskartellamt: Something Old, Something New. *European Papers*, vol. 8., no. 3. (2023) 1078. https://doi.org/10.15166/2499-8249/703

52 Rideg Gergely – Tóth András – Szabó Endre Győző – Németh Szabolcs – Rudics Regina: A GDPR és a Digital Markets Act viszonyának tisztázása. *In Medias Res*, 2023/2. 50–51. https://doi.org/10.59851/imr.12.2.3

A DMA szerint a kapuőröknek lehetővé kell tenni, hogy a végfelhasználók szabadon dönthessenek az adatkezelési és a beléptetési gyakorlatok elfogadásáról, mégpedig olyan módon, hogy kisebb mértékű személyre szabással járó, de egyenértékű alternatívát kell kínálni anélkül, hogy az alapvető platformszolgáltatásnak vagy egyes funkcióinak az igénybevételét a végfelhasználó hozzájárulásától tennék függővé. A kisebb mértékű személyre szabással járó alternatíva nem lehet eltérő vagy rosszabb minőségű a hozzájáruló végfelhasználóknak nyújtott szolgáltatáshoz képest, kivéve, ha a minőség romlása közvetlenül abból adódik, hogy a kapuőr nem kezelheti az ilyen személyes adatokat vagy nem tudja beléptetni a végfelhasználókat egy szolgáltatásba.[53] Ezen megfontolás összhangban áll a Meta-döntés rövid, de annál nagyobb súlyú megállapításával, miszerint a platform adott esetben megfelelő díjazás ellenében olyan egyenértékű alternatívát is felajánlhat, amelyhez nem kapcsolódnak profilalkotáson alapuló, célzott hirdetésküldés célú adatkezelési műveletek. [54]

A DMA és a Meta-döntés is hozzájárul ahhoz a sokat és hevesen vitatott diskurzushoz,[55] hogy a felhasználó személyes adatai megadásával azzal egyenértékű cselekményt végez-e, mintha pénzbeli ellenértéket nyújtana a használatáért.[56] A Meta nemrég bevezette szolgáltatásának hirdetésmentes, előfizetésen alapuló verzióját,[57] amelyet adatvédelmi szervezetek azon érvelés mellett kifogásolnak adatvédelmi hatóságok előtt, hogy a személyes adatok védelméhez való alapjog nem tehető pénz kérdésévé.[58] A kifogások nyomán induló eljárások bizonyosan további adalékokat adnak majd ehhez a diskurzushoz, amelynek során könnyen elképzelhető, hogy a Bíróság is tovább cizellálja a döntésben egy mondatban felvetett álláspontját.[59]

Az EDPB is foglalkozott a kérdéskörrel, hogy az érintett hozzájárulása valós és önkéntes-e, arra jogszerűen alapítható-e az ilyen adatkezelés, ha annak megtagadása esetén a szolgáltatásért díjat köteles fizetni az adatkezelő részére. Véleményében (a továbbiakban: EDPB-vélemény) kifejti, hogy a „nagy online platformok" kötelesek olyan alternatívát kínálni, amely külön díjfizetési kötelezettség nélkül kínál olyan szolgáltatást, amely kevesebb személyesadat-kezeléssel jár, ezáltal tulajdonképpen megsemmisítve a '*Pay-or-Okay*' modellek lehetőségét.[60]

53 DMA (36)–(37) preambulumbekezdés.

54 Meta-döntés 150. pont.

55 A teljesség igénye nélkül elegendő a Facebookkal szemben indított versenyhatósági eljárásokra gondolni, amelyeknek központi kérdése az volt, hogy a Facebook hirdetheti-e ingyenesként a szolgáltatását, miközben a felhasználók személyes adatainak hirdetési célú gyűjtéséből és monetizálásából tartja azt fenn. A magyar viszonylatban a Facebook ingyenességre utaló kereskedelmi kommunikációját megtévesztőnek tartotta a Gazdasági Versenyhivatal, és 1,2 milliárd forint bírságot szabott ki (Vj-85/2016/189), a Kúria viszont a GVH döntésével ellentétesen foglalt állást azáltal, hogy kimondta: pénzbeli ellenérték fizetése vagy más érdemi, a fogyasztót ért hátrány hiányában ingyenesnek mondható a szolgáltatás (Kfv.II.37.243/2021/11.).

56 Hannah Ruschemeier: Competition law as a powerful tool for effective enforcement of the GDPR. *VerfassungsBlog*, 2023. július 7. https://verfassungsblog.de/competition-law-as-a-powerful-tool-for-effective-enforcement-of-the-gdpr/

57 Meta: Facebook and Instagram to Offer Subscription for No Ads in Europe. 2023. október 30. https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

58 Ld.: noyb files GDPR complaint against Meta over „Pay or Okay". *Noyb.eu*, 2023. november 28. https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

59 A *'Pay-or-Okay'* modell értékelésének lehetséges hatásairól ld. bővebben: Giulia Torchio: Meta's 'Pay or Okay': Is this the final challenge for EU GDPR? *European Policy Centre*, 2023. december 4. https://epc.eu/en/Publications/Metas-Pay-or-Okay-Is-this-the-final-challenge-for-EU-GDPR-5672dc

60 EDPB: Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024. április 17. https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

Ezzel összhangban nem kellett sokat várni a következő fejleményre: 2024 júliusában az Európai Bizottság eljárást indított a Metával szemben, mivel álláspontja szerint a '*Pay-or-Okay*' modell a DMA 5. cikk (2) bekezdésébe ütközhet.[61]

3. Versenyhatóságok hatásköri kérdései

Végül, de nem utolsó sorban érdemes kitérni arra a szakmai diskurzusra, amit a versenyhatóságok adatvédelmi megfelelésvizsgálatában megállapított hatáskörével, valamint a hatóságok közötti együttműködéssel kapcsolatosan a Meta-döntés elindított.

A Bíróság szerint a személyes adatokhoz való hozzáférés a digitális gazdaságban a verseny jelentős paraméterévé vált. Ezért ha a versenyhatóságok kizárnák a GDPR szabályait az erőfölénnyel való visszaéléssel kapcsolatos ügyekben figyelembe veendő jogi keretből, azzal figyelmen kívül hagynák e gazdasági fejlődés valóságát, és mindez alkalmas lenne arra, hogy aláássa a versenyjog hatékonyságát az EU-n belül.[62]

A Bíróság már korábban is elismerte,[63] hogy egy másik jogterület megsértése is tényező lehet a versenyjog megsértésének megállapításában. Az adatvédelmi fogalmaknak a versenyjog megsértésének megállapítása céljából történő értelmezése kapcsán a Bíróság azt is megállapítja, hogy a versenyhatóság szabadon levonhatja a saját következtetéseit a versenyjog alkalmazása szempontjából, még akkor is, ha a magatartással kapcsolatban már hozott releváns határozatot adatvédelmi hatóság vagy a Bíróság.[64]

Fontos ugyanakkor hangsúlyozni a versenyjog és a GDPR közötti kapcsolat körében, hogy a GDPR megsértése nem minősül automatikusan visszaélésnek, különösen nem a valódi versenyjogi érdekek és megfontolások mérlegelése nélkül.[65] Úgy tűnik, hogy a döntés a versenyhatóságok számára mozgásteret hagy arra, hogy a GDPR-tól eltérő beavatkozási küszöbértékeket állapítsanak meg az adatvédelmi szabályok értelmezésekor, a versenyjogi jogsértés megállapítása céljából. A Meta-döntésben a GDPR-ról mint a versenyjogi értékelés egyik tényezőjéről lehetett szó, a Bíróság azonban nem vizsgálta, hogy a GDPR hogyan használható fel a versenyjog megsértésének megállapítására.

A Bíróság értelmezése alapján az adatvédelmi hatóság elvben megtartja az értelmezési elsőbbségét, míg a versenyhatóság egyoldalúan dönthet arról, hogy egy – az adatvédelmi hatóság értelmezése szerint – a GDPR-t (nem) sértő magatartás milyen jelentőséggel bír a visszaélések értékelése során.[66] Ez például lehetővé teszi, hogy a versenyhatóság a személyes adatok

61 Európai Bizottság: Commission sends preliminary findings to Meta over its „Pay or Consent" model for breach of the Digital Markets Act [Sajtóközlemény.] 2024. július 1. https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3582

62 Meta-döntés 51. pont.

63 Ld.: C-457/10 P. sz. ügy AstraZeneca AB és AstraZeneca plc. kontra Európai Bizottság [ECLI:EU:C:2012:770]; C-32/11. sz. ügy Allianz Hungária Biztosító Zrt. és társai kontra Gazdasági Versenyhivatal [ECL:EU:C:2013:160].

64 Meta-döntés 56. pont.

65 Peter Georg Picht – Cédric Akeret: Back to Stage One? – AG Rantos' Opinion in the Meta (Facebook) Case. *Papers.ssrn.com,* 2023. április 11. http://dx.doi.org/10.2139/ssrn.4414591.

66 Peter Georg Picht: CJEU on Facebook: Gdpr Processing Justifications and Application Competence. *Papers.ssrn.com,* 2023. július 26. https://dx.doi.org/10.2139/ssrn.4521320

tisztességtelen kezeléséből álló erőfölénnyel való visszaélést állapít meg, noha az adatvédelmi hatóság ugyanezen magatartás miatt nem állapítaná meg a GDPR megsértését.[67]

Ezen példa nyomán ellentétes álláspontok olvashatók a különböző értékelések jogegységhez, jogbiztonsághoz fűződő viszonyában. A pozitív megközelítés onnan indul, hogy az uniós versenyjognak a magánélethez és az adatvédelemhez kapcsolódó kérdésekben való alkalmazását az Európai Unióról szóló szerződés (a továbbiakban: EUSZ) 7. cikke keretében kell elemezni, amely az EU intézményi koherenciáját hivatott biztosítani. Az EUSZ 7. cikkének alapvető szempontja annak biztosítása, hogy az EU közös értékeit, köztük a jogállamiságot minden tagállam tiszteletben tartsa. Emellett az uniós intézményeknek tiszteletben kell tartaniuk az EU Alapjogi Chartájában foglalt jogokat (beleértve az adatvédelemhez és a magánélet védelméhez való jogot), és elő kell mozdítaniuk azok alkalmazását. Ez bizonyos értelemben pozitív kötelezettséget ró az EU intézményeire, hogy biztosítsák politikáik következetességét, például azáltal, hogy az adatvédelmi jog hatékonyságának fokozására irányuló erőfeszítések részeként, az uniós versenyjogot bizonyos esetekben az adatvédelmi joggal együtt alkalmazzák.[68]

Másrészről viszont a Meta-döntésben alkalmazott megközelítés potenciálisan eltérő döntésekhez, ebből fakadóan jogbizonytalansághoz, és a megfelelés költségeinek növekedéséhez vezethet, valamint felveti a vállalkozásokra nehezedő teher aránytalan növekedésének kockázatát.[69] Emellett a versenyhatóságok kompetenciájának a lojális együttműködés elvére való alapozásából másik irányból kiolvasható épp ugyanezen elvre hivatkozással a hatáskörök megosztásának, egymás hatáskörei tiszteletben tartásának kötelessége is.

A Bíróság nem írja elő az együttműködés pontos körvonalait, és ezzel arra szólítja fel a verseny- és adatvédelmi hatóságokat, hogy dolgozzanak ki részletesebb kereteket a GDPR egységes alkalmazásának és értelmezésének biztosítása érdekében. Ez most még inkább aktuális a DMA és a DSA hatálybalépésével, hiszen mindkét rendelet olyan gyakorlatokat is szabályoz, amelyek adatkezeléssel járnak, így a GDPR is vonatkozik rájuk. A DMA végrehajtása az Európai Bizottság kezében van, az Európai Adatvédelmi Biztosnak és az Európai Adatvédelmi Testületnek csak tanácsadói szerepet szánnak a DMA magas szintű munkacsoportjában. A szerepek tehát a DMA-ban még erősebben a Meta-döntés irányába mutatnak azzal, hogy az Európai Bizottság ellenőrzi a végrehajtást, beleértve a vonatkozó adatvédelmi koncepciók alkalmazását is.[70] A DSA végrehajtását szolgáló magyar törvény[71] már a DSA szerinti digitális szolgáltatási koordinátor (Magyarországon a Nemzeti Média- és Hírközlési Hatóság) kötelezettségévé teszi az együttműködést a szakhatóságokkal a digitális szolgáltatások piacával kapcsolatos, más jogterületeket is érintő kérdések esetén.

67 Inge Graef: The European Court of Justice in Meta Platforms leaves competition and data protection authorities with an assignment. *European Law Blog,* 2023. július 19. https://www.europeanlawblog.eu/pub/the-european-court-of-justice-in-meta-platforms-leaves-competition-and-data-protection-authorities-with-an-assignment/release/1

68 Fatma Ceren Morbel: Can EU competition law be used for data protection? *Versenytükör,* 2022/2. 45.

69 Csurgai-Horváth Gergely: Az Európai Bíróság bpost-, DB Station-, ENEL- és Meta-ügyekben hozott ítéleteinek a versenyjog és az ágazati szabályozás hagyományos viszonyára gyakorolt hatásai. *Versenytükör,* 2023/2. 47–48.

70 Graef i. m.

71 2023. évi CIV. törvény az internetes közvetítő szolgáltatások egyes szabályairól 6. §.

Mindebből kiindulva kétségtelen, hogy a két terület találkozási pontjai folyamatosan élesednek a digitális szolgáltatások piacán, amely konvergencia jövőbeli alakulása érdemben határozhatja meg nem csupán az uniós, de a nemzeti jogalkalmazás és értelmezés irányvonalait is.

4. Konklúzió

A Meta-döntés utóélete tettenérhető uniós és hazai szinten egyaránt. Az EUB döntése alapul szolgált az EDPB 01/2023. számú sürgősségi eljárásban meghozott kötelező erejű döntéséhez[72] is, amely – miután ismerteti az egyes tagállami felügyeleti hatóságok gyakorlatát[73] – megállapítja, hogy a Meta termékei (szolgáltatásai) által a viselkedésalapú reklámok nyújtásához alapul szolgáló személyes adatok gyűjtésére, kezelésére a Meta által alkalmazott jogalapok (a felhasználóval kötött szerződés teljesítése és az adatkezelő jogos érdeke) egyike sem megfelelő.[74]

A versenyhatóságok hatáskörére vonatkozó EUB-érvelés megjelenik a Gazdasági Versenyhivatal (a továbbiakban: GVH) TikTokkal szemben indított versenyfelügyeleti eljárást lezáró határozatában (a továbbiakban: TikTok-döntés),[75] ahol azonban erőfölényes helyzet helyett fogyasztóvédelmi vizsgálat igazolása céljából használja a Bíróság érvelését. A TikTok adatkezelési gyakorlatainak értékelése körében a GVH kifejti, hogy

„az adatok (tág értelemben vett) kezelésének fogyasztóvédelmi szempontjai meg is haladják a klasszikus, hagyományos (GDPR szerinti) adatvédelem területét, hiszen nem pusztán személyes adatokra, hanem általánosságban, szélesebb értelemben a fogyasztói magatartással generált, profilozást és egyéb piaci felhasználást lehetővé tevő információkra vonatkozik."[76]

Az egyéb szempontú értékelés nélkül is jó példája véleményem szerint a TikTok-döntés annak, hogy a Bíróság érvelése milyen horizontokat tud nyitni az adatvédelem előtt, a különböző jogterületeken felmerülő jogsértések megállapításának eszközeként és útjaként. A GVH a TikTok-döntésben foglalt érvelését megerősítette a Viberrel szemben – szintén fogyasztóvédelmi aggályok miatt – folytatott versenyfelügyeleti eljárását lezáró határozatban is.[77]

Érdemes felhívni a figyelmet arra, hogy a Bíróság (és az EDPB) a Meta-döntésben nem a DSA vagy a DMA, hanem a GDPR értelmezése és alkalmazása útján jutott azon megállapításokra, amelyek tartalmilag megfeleltethetőek sok szempontból a DSA-nak és a DMA-nak (például az adatok összekapcsolásának tilalma körében), vagy illeszkednek a két jogi aktus szabályozási irányába (például a profilalkotáson alapuló célzott hirdetések korlátozása körében). A döntésből is kirajzolódik, hogy a DSA és a DMA azon szakaszai, amelyek szerint hatályuk és alkalmazásuk nem érinti a GDPR-t,[78] a gyakorlatban puszta deklarációvá válhatnak. Ebből kifolyólag a Meta-döntés segítséget nyújthat a három rendelet közötti kapcsolódási

72 EDPB: Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR), 2023. 10. 27. https://www.edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf

73 Uo. 10. bekezdés.

74 Uo. 315–316. bekezdés.

75 Döntés száma: VJ/24-185/2020.

76 Uo. 237. pont.

77 Döntés száma: VJ/6-142/2020.

78 Ld.: DSA 2. cikk (4) bek. *g)* alpont; DMA (37) preambulumbekezdés.

pontok megtalálásában, valamint az összkonform értelmezés és alkalmazás kialakításában. Ezen kapcsolódási pontok, valamint az egymással összhangban álló értelmezés a következő időszak egyik legnagyobb kihívása lehet a digitális szolgáltatások felügyelete során.

A döntés az adatvédelmi kérdések értékelése körében a(z óriás)platformokon túl, általánosabb jellegű iránymutatással is szolgál, amelyek számos kérdést vetnek fel és hagynak nyitva, többek között a hozzájárulás és a szerződés teljesítése jogalapok terén. Felmerül, hogy annak ellenére, hogy a Bíróságnak egy a DSA szerinti online óriásplatform,[79] a DMA szerinti kapuőr[80] szolgáltatását és magatartását kellett értékelnie, a döntésben a hozzájárulás, vagy a szerződés teljesítése jogalap körében tett adatvédelmi jogi megállapítások túlnyúlhatnak a legnagyobb platformok esetkörén és más olyan adatkezelésekre is hatással bírhatnak, amelyekre nézve nem feltétlenül indokolt a Facebook helyzetéhez hasonló korlátozás.

79 A kijelölés körében ld. az Európai Bizottság vonatkozó sajtóközleményét: https://digital-strategy.ec.europa.eu/hu/policies/list-designated-vlops-and-vloses

80 A kijelölés körében ld. az Európai Bizottság vonatkozó sajtóközleményét: https://ec.europa.eu/commission/presscorner/detail/hu/ip_23_4328

III. Versenyjog és szerzői jog

Az alapvető eszközök tana és a DMA

A versenyjog szerepe a szabályozás fényében

Beyer Fülöp – Csillik Kristóf

1. Bevezetés: A digitális gazdaság, hatalom bizonytalansági problémái és a jog doktrinális fejlődése – tényleg meztelen a király?

A technológiai fejlődés és a jog kapcsolata nagyon sokféleképpen ábrázolható. Teljesen triviális a gondolat, hogy a jog csak 'kullog' a technológia mint a kapitalizmus újszerű megnyilvánulási formája mögött, ahogyan az a konkuráló narratíva is, hogy a jog – mint eleve adott tényező – valamennyi, az emberi életet érintő evolúciós folyamatot képes kezelni.[1] A jog és a technológia kapcsolata ennél valójában sokkal bonyolultabb, és bonyolultságában annyi lehetséges problémát rejt, ahány már meglévő és új megközelítésben ábrázoljuk. E téma mély elméleti tartalommal és számos tisztázatlan kérdéssel kecsegtet, valamint számos olyan új megközelítést vet fel, amelyek irányadók lehetnek valamennyi spekulatív vagy empirikus, valamint dogmatikai és elméleti jogi szakirodalmi erőfeszítés tekintetében.[2] A jog vonzáskörzetében ábrázolni a technológia és a társadalom kapcsolatában rejlő kérdéseket pedig a jövő társadalomirányítása tekintetében fontos munka.

A jog és a technológia kapcsolatát e bevezetésben a bizonytalansági probléma körében ábrázoljuk. A bizonytalansági probléma azt az állapotot jelöli, amikor a társadalmi rend alakítója – például az állam és a jogalkotó – képtelen felmérni saját érdekeit és a területen lehetséges okozati összefüggéseket.[3] Ebben az állapotban keres a jogalkotó diszciplináris, azaz professzionális válaszokat, más szavakkal segítséget a döntései meghozatalában. A bizonytalansági probléma így azt a 20. századi tendenciát is jelöli, amelynek keretében a szakmai közeg álláspontja politikailag is releváns értékké válik.[4] Ez a tendencia folytatódik a digitális gazdaság társadalmi tényezővé válásával. A Digital Markets Act[5] jogalkotási folyamatát áthatotta a folyamatos versenyjogi és gazdaságszabályozási szakirodalmi diskurzus. A Bizottság

1 Julie E. Cohen: From Lex Informatica to the Control Revolution, *Berkeley Technology Law Journal,* vol. 36. (2021) 1017. https://doi:10.15779/Z38C53F239.

2 Ilyen megközelítés a jog normativitásának vizsgálata, ehhez kapcsolódóan a technologizálódó társadalomirányítás mély jogelméleti implikációi tekintetében ld.: Lawrence Lessig: *Code: And Other Laws of Cyberspace, Version 2.0*. New York, Basic Books, 2006.

3 Peter M. Haas: Introduction: Epistemic Communities and International Policy Coordination, *International Organization,* vol. 46., no. 1. (1992) 1–35. https://doi:10.1017/S0020818300001442

4 Harvey Brooks: Scientific Concepts and Cultural Change. *Daedalus, Science and Culture Winter 1965*, vol. 94., no. 1. (1965) 66–83. http://www.jstor.org/stable/20026896

5 Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022.szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról.

intézményi szerepfelfogása is értékelhető a bizonytalansági probléma körében, mint az uniós politikai folyamatokban a professzionalizmust megtestesítő végrehajtó szerv.

A jog mint szaktudomány maga is egy lehetséges professzionális keret, amely képes informálni a bizonytalansági problémával szembesülő jogalkotót. A dogmatikus gondolkodás ridegsége és rezilienciája képes egy kényelmes egyszerűsítésként redukálni vagy absztrahálni a bizonytalansági probléma összetett kérdéseit azáltal, hogy a közpolitika-alkotás személyi apparátusa nagy részének hazai pályát ad: „ezt már szabályozza (x) jogág."[6] A jog szerepe a közpolitika-alkotásban, a bizonytalansági probléma okán professzionalizálódó társadalmi irányítás kontextusában ugyanaz, mint egy természettudományos módszeré. Egyszerűsít, kontextualizál, és mint paradigma behatárolja[7] a közpolitika tartalmát.

A bizonytalansági probléma szabályozással való kezelésének tehát egy központi eleme a közpolitikai döntéseket informáló szaktudományi, azaz diszciplináris tudás.[8] Ebben az értelemben igazán releváns a tanulmány tekintetében az elmélet, mert e diszciplináris tudás mindig egy paradigma függvénye. A politika- vagy értékmentes professzionális kormányzás, amely közpolitikai döntéseit kizárólag a tudományos módszer adta eredményekkel hozza, kecsegtető gondolat, de még a technológia vagy a tudományosság által legmélyebben átitatott, legkomplexebb területeken sem igaz. A tudományos módszerek és a tudományos tudás mögött valamennyi esetben egy értékválasztásokat vállaló paradigmatikus nézetrendszer áll, amely a technokratizálódó társadalmi irányítás folyamatában, a bizonytalansági probléma körében a közpolitikai döntésekben is megnyilvánul. Ebben a tekintetben a bizonytalansági probléma körében segítségül hívott professzionalizmus sem teljesen értéksemleges.

E folyamat elképzelhető egy, a közpolitikai döntéshozást informáló értéklánccént is. A tanulmány szempontjából releváns hasonló értéklánc pedig a közgazdaságtan–versenyjog–szabályozás interdiszciplináris együttműködésben ragadható meg. A versenyjogi analízis keretében a fogyasztói jólét és a hatékonyság céljaihoz hű jogalkalmazás elengedhetetlen kelléke a körültekintő és objektív elméleti közgazdaságtani piaci vizsgálat,[9] amely egy empirikus és a tudományos módszeren alapuló, a jogbiztonságot garantáló konzisztens folyamat. A versenyjog paradigmatikus ebben az értelemben: a fogyasztói jólét céljának megvalósításában a tudományos módszeren alapuló közgazdaságtani eszközök elkerülhetetlenek.[10] A versenyjog ilyen

6 Mátyás Bódig: Legal Doctrinal Scholarship and Interdisciplinary Engagement. *Erasmus Law Review*, 2015/2. https://doi.org/10.5553/ELR.000035.

7 A kuhni paradigma-elmélet egy fontos olvasata, hogy a paradigma a természeti világban való vizsgálódás episztemológiai alapját fekteti le a kutatóközeget jellemző módszertani szokásokkal. E szokások ugyanazok a tényezők, amelyek lehetővé teszik a tudományos paradigmák közötti inkommenzurábilitás és a tudományos forradalmak kuhni elméletét. Sungjoon Cho a paradigma szót arra az episztemikus közösségekben megosztott közös tudásra használja, amelynek fontos jellemzője egy kognitív korlátozó minőség. E szerint egy paradigma kiindulópont, meghatározza a lehetséges 'jó' válaszok körét. A két paradigmaelmélet összehasonlításában ez a kognitív limitáló jelleg a fontos, amely nem kizárólag a jó válaszok körét, hanem azt a folyamatot is korlátozza, amelynek folyamán eljuthatunk a jó válaszokhoz. Sungjoon Cho: The Evolving Geography of American Antitrust Mind. *Virginia Law and Business Review,* vol. 18. (2023) 14–15. https://ssrn.com/abstract=4246088; James Ladyman: *Understanding philosophy of science*. London and New York, Routledge, 2002. 98–100; Thomas S. Kuhn – Ian Hacking: *The structure of scientific revolutions* [Fourth edition],.Chicago, The University of Chicago Press, 2012.

8 Haas i. m. 15.

9 Tóth Tihamér: *Uniós és Magyar Versenyjog*. Wolters Kluwer Hungary, 2020. 122–128.; Haas i. m. 25.

10 Oles Andriychuk: EU Digital Competition Law: The Socio-Legal Foundations. *Cambridge Yearbook of European Legal Studies*, vol. 25., (2023). https://doi.org/10.1017/cel.2023.12 [a továbbiakban: Andriychuk (2023a)].

természete legitimáló hatással bír, hiszen a tudományos módszer látszólag nem kontingens és objektív, azaz nem önkényes emberi döntések függvénye. A versenyjog ilyen természete a versenyjogi dogmatika tartalmát is meghatározza. Ez a jog szerepéről írtak függvényében ahhoz vezet, hogy a versenyjog, mint a kapitalizmus dinamizmusát (érdemi verseny, piaci struktúra) elsődlegesen szabályozó jogi korpusz, mindazon közpolitikai megfontolások tetszetős episztemológiai kerete is, amelyek e területet érintik.[11]

Nincsen ez másként a platformpiacok szabályozása körében sem.[12] Az is egy, a neoklasszikus, liberális versenyjog által motivált gondolat, hogy a DMA által való szabályozás indokolatlan, a piac és a verseny (vagy a verseny hiánya) önmagában hordozza a prosperitást. A versenyjog mai formája ugyanis a közgazdaságtan, az árelméleti analízis eszközei útján a tudományos módszerrel, valamint a hibaköltségi keretrendszer narratív modelljével igazoltja saját legitimitását.[13] A jogág tudományos szolipszizmusa[14] e tekintetben egy ígéret a politikamentes, tudományos alapú állami beavatkozásra a gazdasági koncentráció és a piaci folyamatok szabályozása ügyében, és az internetes tömegközvetítés jelentette gazdasági kihívások tekintetében is.

Azonban felmerül a kérdés, hogy a versenyjog alapjait képező olyan igazolóelvek, mint a fogyasztói jólét vagy a hatékonyság valóban azok a sorvezetők-e, amelyek a kapitalizmus egy radikálisan új formáját hivatottak meghatározni. Ebben a kérdésben vajon tényleg perdöntő jelentőségű-e az, hogy a versenyjogot igazoló elméleti tudás a tudományos módszeren alapszik, úgy, hogy az ezt lefektető episztemikus közösség, a chicagói iskola értékelkötelezettségének is tekinthető piaci fundamentalizmus nyíltan egy politikai értékvállalás?[15] Ahogyan a közpolitika-alkotásba behatol a versenyjogi hagyomány, valójában tényleg egy csak a professzionalizmus objektív értékeit megjelenítő tudás termékenyíti meg a közös gondolkodást a jó szabályozásról? Amennyiben a kérdésekre a válasz 'nem', úgy a király meztelen, és az önbizalom, amit a versenyjog eszköze a bizonytalansági problémát is képező digitális piacok szabályozásának kérdésében ad, tévedésekhez vezet.

Tanulmányunkban a DMA és a digitális piacok bizonytalansági problémájának kontextusában kíséreljük meg elhelyezni a versenyjog nélkülözhetetlen eszközökről szóló doktrináját.

11 A hírközlési piacszabályozást a konzisztens piaci kudarcok felszámolása feladatában a versenyjogi eszközök alkalmatlansága igazolja, a Bizottság által felállított teszt is ezt tükrözi. COM(2003) 497 A Bizottsági ajánlása a releváns termék- és szolgáltatási piacokról az elektronikus kommunikációs szektorban, amelyek előzetes szabályozásnak lehetnek kitéve az Európai Parlament és a Tanács 2002/21/EK irányelve alapján. HL L 114, 2003. 05. 08., 45–49. o. (9) preambulumbekezdés.

12 Az internetes tömegközvetítést a versenyjog keretében való vizsgálatához ld.: Herbert Hovenkamp: Gatekeeper Competition Policy. *Michigan Technology Law Review*, vol. 30., no. 1. (2023). http://dx.doi.org/10.2139 /ssrn.4347768; Manuel Wörsdörfer: The Digital Markets Act and E.U. Competition Policy: A Critical Ordoliberal Evaluation. *Phylosophy of Management,* vol. 22., no. 1. (2022). http://dx.doi.org/10.2139/ssrn.4187064

13 Jacques Crémer – Robert Welker – Heike Schweitzer: Competition Policy for The Digital Era. *Competition Policy International*. (2019) 50.; Julie E. Cohen: *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York, Oxford University Press, 2019. 184.

14 Andriychuk (2023a) i. m. 6.; Oles Andriychuk: Do DMA Obligations for Gatekeepers Create Entitlements for Business Users? *Journal of Antitrust Enforcement,* vol. 11., no. 1., (2023) 123–132. https://doi.org/10.1093/jaenfo/jnac034 [a továbbiakban: Andriychuk (2023b)].

15 Lina M. Khan: Amazon's Antitrust Paradox. *The Yale Law Journal,* vol. 126., no. 3., (2017) 564–907.; Cho i. m. 20.; Tim Wu: *The Curse of Bigness: Antitrust in the New Gilded Age*. New York, Columbia Global Reports, 2018.

A nélkülözhetetlen eszközök tana egy speciális versenyjogi eszköz, amely a belső piaci integráció történeti kontextusában egy közpolitikai célkitűzés módjára alakult.[16] Emiatt jól mintázza a versenyjog és a speciális gazdasági szabályozók közötti kapcsolatot, segítségével jól oldható az a fogalmi feszültség, ami a tömeges közvetítés szabályozásának ügyében a versenyjogi gondolat és a piacszabályozás között fennáll. Tanulmányunkban azt kíséreljük meg bemutatni, hogy valójában a király nem meztelen, de nem azért, mert a versenyjog érákon átívelő tanulsága szükségszerűen igaz, hanem azért, mert a jogfejlődésében megjelenő tudás értékes, és van szerepe egy új intézményes rend kialakításában.

2. A tömeges közvetítés üzleti modellje, a digitális gazdaság sajátosságai

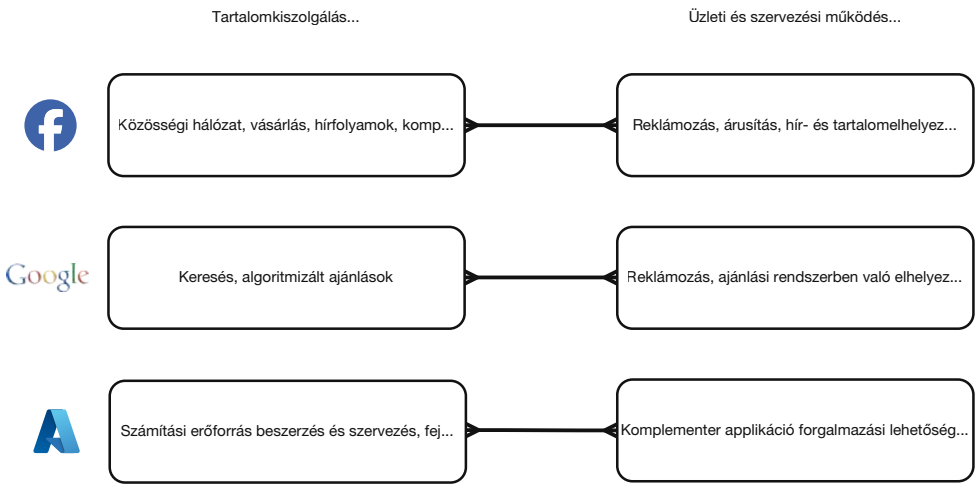
2.1. A tömeges közvetítés kontextusa – exponencialitás, hálózati hatások és ökoszisztémák

A 21. században az elektronikus hírközlési technológiák konvergenciájával és az internethozzáférés magas fokú elterjedésével, az internet rétegén kialakult a platformizált tömegközvetítés többoldalú piacokon is működő üzleti modellje. Az üzleti modell értékpropozíciója az interneten levő decentralizált érték szervezése (aggregálása), centralizálása és végződtetése, valamint ügyletek bonyolítása a piac egyik oldalán (tartalomkiszolgálás), míg az értékteremtés lehetőségeinek segítése, reklámelhelyezés és ügyletek bonyolítása a piac másik oldalán (üzleti és szervezési működés).[17] Bár a tömegközvetítés modellje nem teljesen általános a digitális platformok terén, azonban a többoldalú piacok illusztrálásának feladatában segítőkész narratíva.

16 Marco Vargiu: Revitalisation of the Essential Facilities Doctrine in EU competition law. The complementarity with the new Digital Markets Act. *Journal of Law, Market & Innovation.* vol. 2., no. 1. (2023). https://doi.org/10.13135/2785-7867/7442; Sébastien J. Evrard: Essential Facilities in the European Union: Bronner and Beyond. *Columbia Journal of European Law,* vol. 10., no. 3. (2004).

17 Geoffrey Parker – Marshall van Alstyne – Georgios Petropoulos: Digital Platforms and Antitrust [Working paper]. *Bruegel.org,* 2020. november 3. https://www.bruegel.org/working-paper/digital-platforms-and-antitrust; Juan Montero – Matthias Finger: Regulating Digital Platforms as the New Network Industries. *Competition and Regulation in Network Industries,* vol. 22., no. 2. (2021). https://doi.org/10.1177/17835917211028787

1. ábra A kétoldalú piacok architektúrája



Saját szerkesztés

A tömeges közvetítési szolgáltatás gyakran egy szolgáltatási ökoszisztéma részeként működik. A Google Search szolgáltatása például kapcsolódik a Chrome böngészőalkalmazással, de az Android operációs rendszerrel is, valamint a közkedvelt Gmail levelezőalkalmazással is. A Facebook Messenger kapcsolódik a klasszikus Facebook-felülettel, és mindkét vállalkozás komplementer szolgáltatásai együttműködnek a vállalkozások reklámozási megoldásaival (Google Ads, Meta for Business). Az ökoszisztémák átjárható szoftveres és hardveres technológiákból álló sajátos közegek, amelyek célja a végfelhasználók valamennyi fogyasztói számítástechnikai igényének kielégítése, és legfontosabb eszközük a szolgáltatások és hardverelemek komplementaritásából eredő választékgazdaságosság.

A tömeges közvetítési modell e felsorolt többoldalú piacokon hálózati hatásokra támaszkodik.[18] E hatások azt a folyamatot jelölik, amelynek részeként a piacokat működtető hálózat értéke a résztvevő végpontok sokasodásával exponenciálisan nő. A digitális gazdaságban ismert továbbá a közvetett hálózati hatások jelensége is. Közvetett hálózati hatásokról beszélhetünk, amennyiben a többoldalú piac egyik oldalán résztvevő szereplők, valamint a másik oldal szereplői bármelyik oldal növekményéből kölcsönösen és egymásra tekintettel részesülnek. A közvetett hálózati hatások a platform- vagy szoftver- és hardverelemek integráltan működő, komplementer funkcionalitásokon alapuló rendszerében működnek hatékonyan (a továbbiakban: ökoszisztéma), hiszen a heterogén felhasználói köröket a sokoldalúsága függvényében tudják bevonni.[19]

18 Crémer–Welker–Schweitzer i. m. 15.; Parker–Petropoulos i. m. 3.; Ioannis Lianos: Value Extraction and Institutions in Digital Capitalism: Towards a Law and Political Economy Synthesis for Competition Law. *European Law Open,* vol. 1., no. 4. (2022) https://doi.org/10.1017/elo.2023.2; Montero–Finger i. m. 3–5.

19 Montero–Finger i. m. 3.; Christopher T. Marsden – Ian Brown: App Stores, Antitrust and Their Links to Net Neutrality: A Review of the European Policy and Academic Debate Leading to the EU Digital Markets Act. *Internet Policy Review,* vol. 12., no. 1. (2023). https://doi.org/10.14763/2023.1.1676

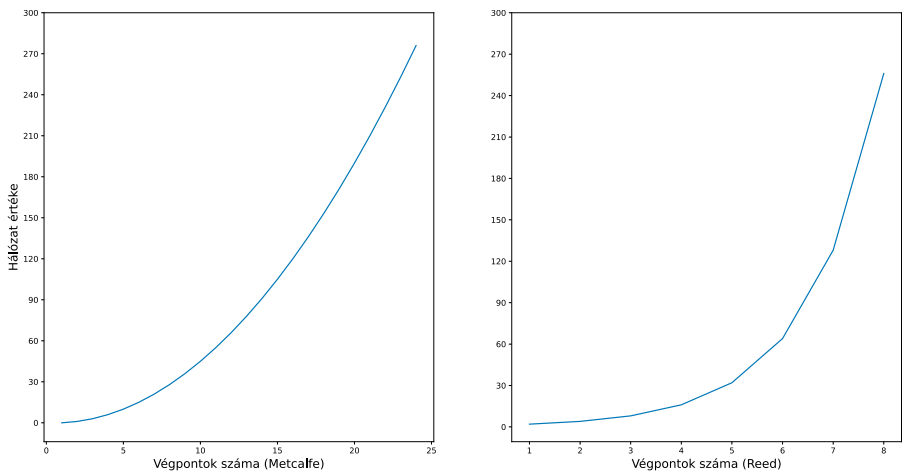
A hálózati hatásokat tovább lehet specifikálni aszerint, hogy a piac mely oldalán, milyen intenzitással fejtik ki értéknövelő hatásukat. Bár a hálózati hatásokból fakadó externáliák hálózatok értékét növelő mértékével kapcsolatban a szakirodalom megosztott. A Metcalfe-féle szabály értelmében a hálózati externália minden hozzáadott végponttal elért értéknövekménye arányos a hozzáadott végpont által lehetővé tett kapcsolatok számával. Metcalfe teóriája a kiterjedt hálózatokra kevéssé igaz, hiszen azokban nem mindegyik hálózati végpont csatlakozik mindegyik másikhoz. Metcalfe szabálya – amelyben *n* a kapcsolatok számát jelöli – így a lehetséges összeköttetések számával hozza összefüggésbe a hálózat növekedését:[20]

$$V_{Metcalfe}(n) \sim n^2 \sim n(n-1)/2$$

Reed szabálya Metcalfe-éval szemben a hálózatok azon képességére világít rá, hogy azon a hálózati végpontok csoportokba szerveződnek. Reed a hálózati externália mértékét a hálózaton egy addicionális hálózati végpont bekapcsolásával formálható csoportok számával hozza összefüggésbe. Reed szerint minden új hálózati végpont megduplázza a hálózat értékét:[21]

$$V_{Reed}(n) \sim 2^n$$

2. ábra Metcalfe és Reed szabálya



Saját szerkesztés

A hálózati externália mértékének megbecsülése több módszertanban is elképzelhető, azonban a módszertanokban az közös, hogy a hálózat egyre kiterjedtebbé válásával a hálózat értéke folyamatosan és exponenciálisan nő.[22] A hálózati hatások gyakorlata a tömeges közve-

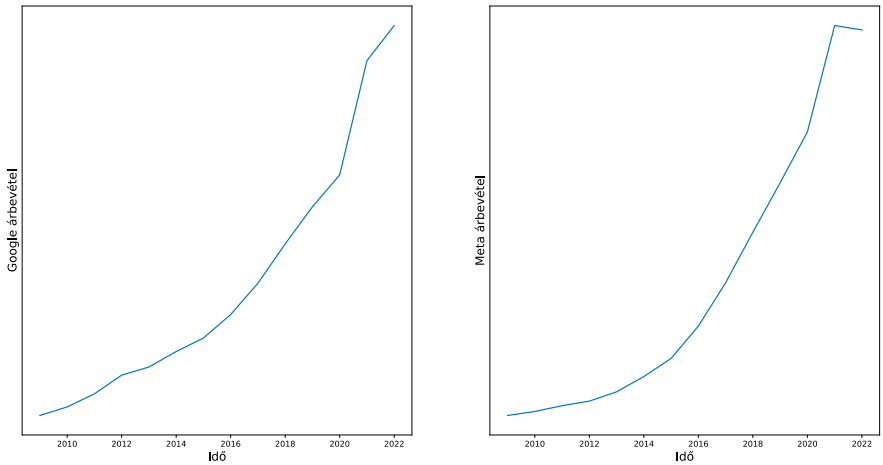
20 Harald Øverby – Jan Arild Audestad: *Introduction to Digital Economics: Foundations, Business Models and Case Studies*. Cham, Springer International Publishing, 2021. https://doi.org./10.1007/978-3-030-78237-5

21 Uo. 141.

22 A negatív hálózati hatások is exponenciálisan növekvő fogyasztói váltást idéznek elő, és így a versenynek nem akadálya a hálózati hatások által képzett belépési korlátrendszer. Gary Winslett: *Populists' Overreach on Antitrust and Big Tech* [Working paper]. 2022. november 9. https://dx.doi.org/10.2139/ssrn.4273123

títés piacának történeti kontextusa is, hiszen a techóriások növekedését az exponencialitás, és ezáltal a hálózati hatások gazdasági jelentősége jellemzi.

3. ábra A Meta és az Alphabet cégek árbevételei az idő függvényében



Saját szerkesztés

A hálózati hatások végső soron képesek megmagyarázni a szakirodalomból is ismert 'piacért folytatott verseny' jelenségét is. Amikor a hálózatok kiterjedtsége, tehát a végpontok száma egy bizonyos mértéket (kritikus tömeg) elér, a hálózati hatások okán és a megnövekedett váltási költségek felmerülésével az inkumbenssel szembeni frontális verseny elméleti kategóriává, tehát gyakorlatilag lehetetlenné válik.[23] A hálózati hatások és a növekedés exponenciális jellege tetten érhetőek az inkumbensek árbevételi mutatóiban is.[24]

A digitális gazdaság egy sajátossága, hogy az internetes tömegközvetítés óriásplatformjai és e platformokat is tömörítő digitális ökoszisztémák infrastrukturális tényezőként jelentkeznek a gazdasági folyamatokban.[25] Ilyen szerepük a piacok struktúrájából, piaci erejük mértékéből és a tömegközvetítés üzleti modelljének minőségéből fakad. A tömeges közvetítés a decentralizált érték aggregált közvetítése a végfelhasználók felé, ami skálázása folytán exponenciálisan válik egyre jövedelmezőbbé a közvetítést bonyolító számára. Ebből adódóan ezen üzleti modellt követő vállalkozások érdeke, hogy egyedüli alternatívaként szolgáltassanak elérési kapukat a végfelhasználók felé, azáltal, hogy megkettőzhetetlen és megkerülhetetlen infrastrukturális

23 Crémer–Welker–Schweitzer i. m. 55.; Pierre Larouche – Alexandre De Streel: The European Digital Markets Act: A Revolution Grounded on Traditions. *Journal of European Competition Law & Practice,* vol. 12., no. 7. (2021) 542–560. https://doi.org/10.1093/jeclap/lpab066; Montero–Finger i. m. 5.

24 A Szerzők tudomásul veszik, hogy az ábrák módszertani szempontból nem kifogásolhatatlan pontosságúak, azonban felhívják az olvasó figyelmét arra, hogy a bemutatott ábrák csak a hálózati hatások matematikai elmélete és a valóság közötti primitív összefüggés szemléltetésére készültek. Ez az összefüggés a hálózatos tömegközvetítés üzleti modell alapja.

25 Christoph Busch: *Regulation of Digital Platforms as Infrastructures for Services of General Interest* [WISO Diskurs 2021/9.]. Bonn, Friedrich Ebert Stiftung, 2021; Cohen (2021) i. m. 5.

elemekké válnak az érintett többoldalú piacokon, például az online reklámozás piacán. Minden vállalkozás érdeke, hogy monopolhelyzetbe kerüljön, azonban nem minden üzleti modell lényege ilyen mérvű koncentráció és függőség[26] kiépítése. Ez az infrastrukturális szerep az a kontextus, amelyben gyakorlatilag létrejött korunk internete, 'a kapuőrök internete', valamint amelyben megszületett a felismerés és aggodalom, hogy a Big Tech rendszerszintű monopolhelyzete társadalmi probléma.[27]

A tömeges közvetítést végző szolgáltatások kapcsán érdemes szót ejteni néhány, a tanulmány tekintetében fontos jellegzetességről. Fontos írnunk az adatfelhalmozásról és az adat ellenőrzésének lehetőségéről, az ökoszisztémák többé-kevésbé integrált hozzáférési kapukból álló vertikális struktúrájáról és ehhez kapcsolódóan az ökoszisztémák közötti átjárhatóság hiányáról.

2.2. Az adatok szerepe

Nehéz túlbecsülni az adatakkumuláció szerepét a tömeges közvetítés modelljében. A folyamatos adatgyűjtés eredményeiben rejlő értéket a tömeges közvetítő szolgáltatók a szolgáltatási palettájukba és a saját gazdasági döntéshozatali eljárásukba több ponton integrálják. Az adat jelentette érték beépítésének legadekvátabb módjai a profilozási technológiákon keresztüli célzott reklámozás és az adatanalitikai eredményeket is hasznosító (általában *downstream* piacra szánt) termékfejlesztés.[28] E két gazdasági működés szempontjából kritikus a kellő mennyiségű adat felhalmozása. Ennek tekintetében a tömeges közvetítők adatgyűjtésének mértéke gyakorta merül fel a szabályozást motiváló (lebontandó) belépési korlátként egyes piacok tekintetében. Ennek szabályozási eszköze egyrészt az adatok 'silózása', azaz szétválasztásának előírása az ökoszisztéma egyes részeit képező szolgáltatások között, másrészt az adatvagyon megosztásának kötelezettsége a piacra belépők számára.[29]

Az adatok jelenléte a tömeges közvetítő ökoszisztémájában, a többoldalú piacok működése tekintetében is fontos tényező. Az üzleti oldalon jelenlévő vállalkozások adatanalitikai információinak értéke egyenesen arányos az ökoszisztémán bonyolított ügyletek számával. Értelemszerűen ezen érték nem vihető át ökoszisztémákon keresztül. Az adat ebben a kontextusban az üzleti felhasználók oldalán jelentkező váltási költségként jelenik meg, ami annál nagyobb, minél jobban megalapozott az adott üzleti felhasználó jelenléte az adott ökoszisztémában.[30]

26 Fontos, hogy a tömegközvetítés infrastrukturális szerepe nem kizárólag a vállalkozások piaci erejéből adódik. Antonio Davola – Gianclaudio Malgieri: Data, Power and Competition Law: The (Im)Possible Mission of the DMA? In: Frank Fagan – James Langenfeld (szerk.): *The Economics and Regulation of Digital Markets* [Research in Law and Economics, vol. 31.]. Leeds, Emerald Publishing, 2023. https://doi.org/10.1108/S0193-589520240000031003

27 Andriychuk (2023a) i. m. 15.; Cohen (2019) i. m. 1033.

28 Az Amazon által a *downstream* piacra fejlesztett és saját online áruházában kínált termékeinek fejlesztéséhez felhasznált adatok tekintetében ld.: Khan i. m.

29 DMA 5. cikk (2) bekezdés, 6. cikk (2) bekezdés, 6. cikk (10) bekezdés; Jean Tirole: Competition and the Industrial Challenge for the Digital Age. *Annual Review of Economics,* vol. 15., no. 1. (2023). https://doi.org/10.1146/annurev-economics-090622-024222

30 Marshall W. Van Alstyne – Georgios Petropoulos – Geoffrey Parker – Bertin Martens: „In Situ" Data Rights. *Communications of the ACM*, vol. 64., no. 12. (2021). https://doi.org/10.1145/3491270

2.3. Ökoszisztémák és hozzáférési kapuk

A tömeges közvetítés üzleti modellje általában egy digitális ökoszisztéma részeként működik. Az ökoszisztéma teszi lehetővé, hogy kialakuljon egy, a részvételen és nem a tulajdoni hányadon alapuló közös értékteremtési tér, ahol a felhasználók által teremtett értékből más felhasználók, és végül az ökoszisztémát működtető fél is részesedik.[31] Az ökoszisztéma vonzó a felhasználó számára, hiszen az értékteremtés és a már megteremtett értékből való részesülés lehetőségét egy átjárható, egymást kiegészítő szolgáltatásokból álló technológiai közegben teszi lehetővé. Az Apple ökoszisztémája például *flagship* hardvereszközein keresztül kínál egy teljesen integrált szoftveres környezetet, amely saját elosztási csatornáin keresztül 'szívesen lát' harmadik felektől származó szoftvereket.

Az ökoszisztéma elemeit hozzáférési kapuk integrálják egy *walled garden* típusú mikrokozmoszba, amely kizárólag saját keretein belül átjárható.[32] Az ökoszisztémák jól szervezett, komplementáris szolgáltatásokon alapuló közvetett hálózati hatásain keresztül tekintélyes választékgazdaságosságot jelentenek (*economies of scope*).[33] A hozzáférési kapuk működési elve az, hogy az ökoszisztémán belüli, de akár az ökoszisztémán kívül keletkezett értéket is kizárólag az ökoszisztémába integráltan tegyék elérhetővé. A piacvezető alkalmazásáruházak (Play Store [Alphabet], AppStore [Apple]) klasszikusan ilyen funkciót látnak el. Az Android vagy iOS operációs rendszerrel ellátott okoseszköz használata során a végfelhasználó a harmadik személytől származó szoftvert (ökoszisztémán kívül keletkezett érték) az ökoszisztémába integráltan, az alkalmazásáruházon keresztül képes elérni. A hozzáférési kapu létezésével az ökoszisztémán kívüli érték technológiailag és gazdaságilag is függő helyzetben van az értéket aggregáló és szervező, a hozzáférési kaput ellenőrző ökoszisztémától.[34]

A számfüggetlen személyközi hírközlési szolgáltatások (Facebook Messenger [Meta], WhatsApp [Meta]) terén bár nem kizárólag egy szereplő szolgálja ki az egész piacot, de a piaci koncentráció mértéke magas.[35] Mivel e szolgáltatások a piac azonos oldalán közvetlen hálózati hatásokkal működnek (annál kedvezőbb helyzetben van a végfelhasználó, minél többen használják a szolgáltatást), az átjárhatóság határainak szigorú megvonásával az ökoszisztéma részeként az üzenetküldő szolgáltatást működtető lekorlátozza és kisajátítja az adott üzenetküldő szolgáltatáshoz kötődő, közigényt kielégítő hálózat pozitív hálózati hatásait.[36] E szolgáltatások közötti teljes átjárhatóság a piac (a személyközi, gyors és az élőszóra hasonlító üzenetküldéshez kapcsolódó közigény termékének piaca) egészére terjesztené ki a kedvező hálózati hatásokat, azonban jóllehet, az üzenetküldő szolgáltatást magában foglaló ökoszisztémát (Meta – Facebook) egy hozzáférési kaputól fosztaná meg, hiszen már nem lenne elengedhetetlen az ökoszisztémában való részvétel ahhoz, hogy adott szolgáltatás (Meta – Messenger) végfelhasználóit elérjük.

31 Lianos i. m. 859.; Tirole i. m. 576.

32 Montero–Finger i. m. 11.

33 Busch i. m. 10.

34 Frédéric Marty: Ecosystems As Quasi-Essential Facilities: Should We Impose Platform Neutrality? *Journal of Law, Market & Innovation,* vol. 1., no. 3. (2022). https://www.ojs.unito.it/index.php/JLMI/article/view/7170.

35 BEREC Report on interoperability of Number-Independent Interpersonal Communication Services (NI-ICS). BoR (23) 92. BEREC, 2023. 12. https://shorturl.at/JQpfE

36 Vincent Heimburg – Manuel Wiesche: Digital Platform Regulation: Opportunities for Information Systems Research. *Internet Research,* vol. 33., no. 7. (2023). https://doi.org/10.1108/INTR-05-2022-0321

A tömegközvetítő ökoszisztémák (Lényegében a GAFAM[37] betűszóval jelölt cégek) ellenőrző és szervező szerepük okán maguk is hozzáférési kaput jelentenek a piacon termelhető és megragadható értékhez. Innen ered a DMA szemléletes szóhasználata saját hatálya tekintetében, amely szerint 'kapuőröket' szabályoz. A tömegközvetítés üzleti modelljének sarkos eleme a *fontos kapu* kiépítése, hiszen adott ökoszisztéma használatának növekedése a hasznosítható adatok növekedésével és sok esetben a már említett választékgazdaságosság hatékonyabbá válásával jár. Minél fontosabb egy kapu, annál többen fogják azt igénybe venni. A tömegközvetítés üzleti modellje akkor működik a legjobban, ha adott szolgáltatás a digitális gazdaságot szervező, megkerülelhetetlen és megkettőzhetetlen infrastruktúrává válik.[38]

A talán legadekvátabb példa a hozzáférési kapukon keresztül épített, vertikálisan szorosan integrált választékgazdaságosságra az Apple rendszere. Ez az ökoszisztéma a digitális értéklánc valamennyi rétegén összekapcsolt termékeket kínál, a hardverektől és a hardveres kiegészítőktől az operációs rendszereken át a végfelhasználói szoftverekig. A tömeges közvetítés üzleti modellje az Apple ökoszisztémájában az AppStore képében jelenik meg. Az AppStore szolgáltatása az interneten létező érték (az Apple végpontjain futtatható szoftveralkalmazások) aggregálása, minőségbiztosítása és kiszolgálása. Az ökoszisztéma *flagship* hardvertermékeibe beágyazott operációs rendszert a felhasználó a hardver használatával automatikusan igénybe veszi, az operációs rendszerhez tartozó licenciaszerződés alanyává válik. Az operációs rendszerrel (iOS, iPadOS) az AppStore kapcsolt szolgáltatás, és egyelőre az egyetlen, a licenciaszerződésnek megfelelő szoftveres megoldás bármilyen harmadik féltől származó szoftver alkalmazás beszerzésére.[39] Más szavakkal, az iOS-t és iPadOS-t használó végfelhasználó kizárólag az AppStore-t használhatja alkalmazások letöltésére. Ilyen értelemben az AppStore egy hozzáférési kapu, az Apple okoseszközök e kapun keresztül használhatók teljességükben. Ugyanezen eszközökön kizárólag a gyártónak fenntartott hely az alkalmazásokban intézett fizetések digitális bonyolítása is, hiszen az AppStore-ban való megjelenés feltétele az Apple fizetési interfészének beágyazása a saját fejlesztésbe, amennyiben az applikáció alkalmazáson belüli fizetési lehetőséget biztosít.[40] Ahogyan az AppStore maga, az Apple alkalmazáson belüli fizetési interfészei is monetizációs lehetőségeket tömörítenek. Az AppStore keresési funkcionalitásaiba például nagyszerűen integrálható rangsorolási és reklámozási megoldás, az interfészek alkalmazásába pedig egy egyszerű szolgáltatási díj.[41]

Az árukapcsoláshoz közel álló módszer több releváns történeti példában elégítette ki a versenyjogi tényállás mögött fekvő kárelméletet, mégpedig azt, hogy az egyébként versenykörülmények között megtermett érték árukapcsoláson keresztüli átvitele (*leverage*) másodlagos piacokra e piacokon torzítja a versenyt.[42] Az árukapcsolás területén kívül az ökoszisztémák implikációja a piaci verseny tekintetében az, hogy mint termékek és szolgáltatások sorát tömörítő entitások, esetükben az egymáshoz kapcsolódás okán nem határozhatóak meg termékpiacok. Az ökoszisztémák közötti verseny mint az inkumbensek között folyó verseny szintén rossz elméleti keret,

37 Google, Amazon, Facebook, Apple, Microsoft.

38 Vargiu i. m. 119.

39 Apple Developer Program License Agreement 6. rész

40 Apple Developer Program License Agreement 7.2. rész.

41 Apple Developer Program License Agreement Schedule 3., 3.5. rész.

42 T-201/04 Microsoft Corporation kontra Európai Közösségek Bizottsága [ECLI:EU:T:2007:289] 1010. pont; T-612/17 Google LLC, Google Inc. és Alphabet, Inc. kontra Európai Bizottság [ECLI:EU:T:2021:763] 300–617. pont; a leverage taktikák és a választékgazdaságosság elválasztásának fontosságáról lásd: Hovenkamp i. m. 22.

hiszen ezen ökoszisztémák nyitottsága eltérő. Az említett Apple talán a legzártabban integrált értékláncból álló ökoszisztéma, míg az Alphabet a hardvergyártás piacán nincs számottevően jelen, a hozzáférési kapuként szolgáló operációs rendszerében (Android) rejlő értékét az OEM-ekkel[43] kötött licensziaszerződések útján mélyíti el saját ökoszisztémájában.

Az internetes tömegközvetítés üzleti modelljét követő vállalkozások és az ökoszisztémákat működtető inkumbensek általában valamennyi üzleti és közhatalmi relációban a legtöbb információval rendelkező félnek számítanak. Az adatok felhalmozásából származó előnyön kívül, csak az inkumbenseknek van hozzáférése az ökoszisztémákat működtető komplementer szolgáltatások működésének modalitásaihoz, így például az algoritmizált kereső- és ajánlórendszerek részleteihez. Ugyanez a helyzet az adatakkumuláció mértékéhez kapcsolódó tudással, ami értelemszerűen elérhetetlen bárkinek, aki nem kezeli egészében és összekapcsoltan az ökoszisztémában felhalmozott adatokat. Ez az információs aszimmetria több implikációt rejt magában. Egyrészt, ahogyan az adatakkumulációról szóló részben említettük, a piac lényegi működtetéséből származó tudás erőteljes *downstream* versenyelőny az üzleti felhasználókkal, azaz a platform üzlettársaival szemben a termékfejlesztés tekintetében. Az információs aszimmetria másik szempontból a rendszerek működésével kapcsolatos transzparencia hiányát is jelenti. A transzparencia hiánya fontos szempont a szabályozás tekintetében, hiszen amíg a szabályozó nem ismeri a rendszer működésének összefüggéseit, addig a lehetséges szabályozás tartalma sem teljes. A transzparencia hiánya addicionális lobbitaktikaként is alkalmazható a szabályozási csapdák kialakításának (*regulatory capture*) tekintetében.

2.4. Gazdaságszabályozás és versenyjog

A kapitalista, demokratikus, liberális jogállamok gazdasági rendszere magántulajdonban lévő gazdasági társaságok szabadpiaci versengésén alapul. A piaci verseny legfontosabb gazdasági funkciója az allokációs és a dinamikus hatékonyság biztosítása. A versenyjog a versenypolitika végrehajtására szolgáló eszközrendszer, a versenypolitika célkitűzését pedig a jogalkotó vagy a jogalkalmazó versenyelméletről vallott felfogása határozza meg. A versenyelmélet feladata megtalálni a versenyjog helyét és szerepét az allokációs és a dinamikus hatékonyság, illetve a gazdasági jólét és a holisztikus jólétfogalom koordináta-rendszerében.

A versenyelméletről vallott felfogás determinálja a gazdaságszabályozás és a versenyszabályozás delimitációs pontját, azaz azon szektorális és strukturális jellemzőket is, amelyek alapján meghatározható, hogy a *versenypolitika célját milyen eszközrendszer szolgálja a leghatékonyabban*. Azon területeken, amelyeken a jogalkotó vagy jogalkalmazó által vallott versenyelméleti felfogás szerint a versenyszabályozás elégséges, a hatékony (tehát az allokációs és a dinamikus hatékonyságot garantáló) versenyt versenyjogi eszközökkel biztosítják a versenyhatóságok. A digitális gazdaság legnagyobb és legbefolyásosabb vállalkozásai tekintetében azonban a jogalkotó a gazdaságszabályozás eszközéhez fordult. A kapuőrök szabályozási rezsimje e tekintetben *ex-ante* szabályokkal törekszik megteremteni egyfajta speciális gazdasági rendet.

E szerkezeti egységben a digitális gazdaság különlegességének bemutatásával érzékeltettük, hogy mi indokolja a versenyjog empirikus hagyományától való eltérést. A gazdaságsza-

43 Original Equipment Manufacturer. A betűszó azokat a vállalkozásokat jelöli, amelyek a fenti esetben az Android operációs rendszert használó hardverelemeket (okostelefon) előállítják.

bályozás kevéssé paradigmatikus, a specializált élethelyzeteket specializált rezsimekkel kezelni képes állami beavatkozási eszköze, legitimitása is ebben rejlik: a digitális gazdaság és a platformizáció a hagyományos, paradigmatikus jogi gondolkodás szemüvegében olyannyira szokatlan és obskúrus,[44] hogy egy nem szukcesszív jogi innovációnak adhat teret.

3. A kapuőrök szabályozási rezsimje

3.1. A Digital Markets Act

A Digital Markets Act az Európai Unió másodlagos jogi aktusa, amely a platformszolgáltatók gazdasági szabályozását egy teljesen a konkrét szabályozási alanyokra szabott, speciális rezsimben valósítja meg. E rezsim egy különleges, a DMA által felállított kijelölési-megfelelési eljárás keretében működik, és lényegében azt jelenti, hogy a jogalkalmazó által kijelölt kapuőrök egy kazuisztikus kötelezettség együttes alanyává válnak. A DMA általános szabályozói szemlélete az, hogy azokat a vállalkozásokat, amelyek szolgáltatásai kapuként szolgálnak más szereplőknek nagy számú végfelhasználó elérésében, ezen kapuk nyitására és más speciális magatartásokra kötelezze a speciális kötelezettség együttes[45] betartatásával.

A DMA fogalomhasználatában azok a vállalkozások minősülnek kapuőrnek, amelyek valamilyen, a DMA hatálya alá tartozó alapvető platformszolgáltatást[46] nyújtanak (videómegosztó-platformok, személyközi számfüggetlen kommunikációs szolgáltatások, online piacterek, közösségi média site-ok, felhőalapú számítástechnikai szolgáltatások stb.), és

- jelentékeny hatást gyakorolnak a belső piacra (legalább 7.5 milliárd euró árbevétel a megelőző három pénzügyi évben);
- alapvető platformszolgáltatásuk kapuként szolgál üzleti felhasználóik számára a végfelhasználók elérésében (a megelőző pénzügyi évben legalább 45 millió aktív végfelhasználóval és 10.000 üzleti felhasználóval rendelkeznek); és
- megszilárdult és tartós piaci pozíciót élveznek működésük során.

A kapuőrfogalomnak kvantitatív szempontból megfelelő vállalkozásoknak a Bizottság felé be kell jelenteni, hogy kapuőröknek minősülhetnek.[47] A vállalkozások jelzése után a Bizottság kijelöli a kapuőröket, és a kijelöléssel rájuk nézve a DMA 5–7. cikkeiben foglalt 18 speciális magatartási előírás kötelezővé válik. Ilyen magatartási előírás például az önpreferálás tiltása. A DMA tiltja, hogy egy alapvető platformszolgáltatásnak minősülő online keresőmotort vagy online piacteret üzemeltető kapuőrvállalkozás előnyben részesítse saját vertikumához tartozó szolgáltatásait vagy termékeit.[48]

44 Julie E. Cohen: Law for the Platform Economy. *UC Davis Law Review*, vol. 51., no. 1. (2017). https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-1_Cohen.pdf

45 DMA 5–7. cikk

46 DMA 2. cikk 2. pont

47 DMA 3. cikk (3) bekezdés.

48 Luís Cabral – Justus Haucap – Geoffrey Parker – Georgios Petropoulos – Tommaso Valletti – Marshall Van Alstyne: *The EU Digital Markets Act: A Report from a Panel of Economic Experts.* Luxemburg, Publications Office of the European Union, 2021. https://data.europa.eu/doi/10.2760/139337

A szabályozás középpontjában álló 'kapuőrfogalom' kvalitatív természetű, azonban a kvalitatív feltételek teljesülését vélelmezni kell, amennyiben a DMA által támasztott kvantitatív mutatókat (árbevétel, felhasználók száma) megvalósítja az adott vállalkozás.[49] A kvantitatív feltételek vonatkozhatnak a kapuőrvállalkozásra (árbevétel) vagy a vállalkozás által nyújtott alapvető platformszolgáltatásra (felhasználók száma), azaz azokra a szolgáltatásokra, amelyek tekintetében kijelölésre kerül a kapuőr, és amelyek tekintetében a kapuőr valamilyen hozzáférési kaput ural.

A DMA kijelölési hatásmechanizmusa és a kijelölési folyamatban vétett hibák korrekciós mechanizmusai – mint például a piaci vizsgálat kezdeményezése vagy a kijelölési eljárásban eredetileg megjelölt alapvető platformszolgáltatások körének adjusztálása – mind a Bizottság diszkrécióján alapszanak.[50] A DMA első kijelölési határozatai között van példa arra, hogy a Bizottság egyes alapvető platformszolgáltatásokat a kvantitatív megfelelés ellenére, a vállalkozás érvelésével egyetértve végül nem vont a DMA hatálya alá. A kvantitatív feltételek mint vélelmet alapító, rugalmas bemeneti feltételek, kiegészülve a diszkrecionális kvalitatív feltételekkel olyan szempontból is jó megközelítésnek bizonyulnak, hogy a piaci erő és a kapuőrökre vonatkozó ellenőrző, infrastrukturális szerep nem teljesen egyenlő.[51] Bár tiszta fogalmi demarkációt nehéz lenne vonni a két fogalom között, az biztos, hogy a piaci jelenlét operacionalizálására vonatkozó sztenderdek a kapuőri minőséget nem hivatottak mérni, hiszen a kapuőrök infrastrukturális jellemzőit és ellenőrzési képességeit nem építik be a vizsgálati módszertanukba. Az alapvető platformszolgáltatások meghatározásának kérdésében szembetűnő a Bizottság tág mozgástere. A DMA alkalmazása során az adott alapvető platformszolgáltatás pontos meghatározásának feladatában a Bizottság nem riad vissza e tág mozgástér alkalmazásától.[52] Az alapvető platformszolgáltatások meghatározása a DMA alkalmazásában az egyik legfontosabb mozzanat, hiszen az alapvető platformszolgáltatások vonják meg a DMA kötelezettségegyüttesének tárgyi hatályát az adott kapuőr tekintetében.

A DMA alapján a Bizottságnak lehetősége van olyan alapvető platformszolgáltatások alapján kapuőrnek minősíteni vállalkozásokat, amelyek kizárólag kvalitatív szempontból minősülnek ilyennek.[53] A kvalitatív alapú kijelölés, azaz a kvantitatív feltételekből eredő törvényi vélelem által nem támogatott Bizottsági döntés a már említett piaci vizsgálati eljárás[54] függvénye. A Bizottság kijelölési eljárása és a kijelölés részeként az alapvető platformszolgáltatások meghatározása saját döntési kompetenciájának függvénye, nincs szerv, amely a Bizottság helyett eldönthetné, hogy mely vállalkozás kerüljön kijelölésre. A kijelölő határozatok ellen azonban természetesen van lehetőség jogorvoslatra.[55]

A DMA erős versenyjogi éllel rendelkező, speciális gazdaságszabályozási eszköz. A versenyjogi hagyomány relevanciája első sorban a piaci jelenlétet is vizsgáló kapuőrfogalom tartalmá-

49 DMA 3. cikk (2) bekezdés.

50 Anne C. Witt: The Digital Markets Act: Regulating the Wild West. *Common Market Law Review,* vol. 60., no. 3. (2023) http://dx.doi.org/10.2139/ssrn.4395089; Andriychuk (2023b) i. m. 21–22.; Alba Ribera Martínez: The Requisite Legal Standard of the Digital Markets Act's Designation Process. *Journal of Competition Law & Economics,* nhae011 (2024). http://dx.doi.org/10.1093/joclec/nhae011

51 Busch i. m. 4.

52 Ribera Martínez i. m. 12.

53 DMA 3. cikk (8) bekezdés.

54 DMA 17. cikk.

55 EUMSz. 263. cikk.

ban érhető tetten, amely a testreszabás jegyében speciális, a kapuőrök az általuk uralt piacok ellenőrzési lehetőségeire (és hatalmi pozíciójukra) reflektáló szempontokkal egészül ki.

A tekintetben, hogy saját céljaként a platformgazdaság szempontjából releváns piacok 'megtámadhatóságát'[56] segíti elő, a DMA megjelenít liberalizációs, piacnyitó célokat is. A DMA létrehozását – a jogharmonizáció[57] mellett – az indokolja, hogy részben a versenyjoggal átfedő célokat szolgál, és ilyen minőségében a DMA a kijelölési határozatok és a speciális kötelezettségek által megvont körben a versenyjoghoz képest előnyben részesített beavatkozási eszköz. Azonban mi annak az oka, hogy a szabályozó a digitális piacok megtámadhatóságának liberalizációs kérdésében a versenyjog általános eszközétől elfordult és a szabályozás útját választja?

3.2. Az időbeli dimenzió kérdése[58]

Az *ex-post* alapú versenyjogi beavatkozás alaptétele az, hogy mindent szabad, amíg nem rendelkezünk arról szóló határozattal, hogy az, amit nem szabadott volna, a versenyt érdemben korlátozta, vagy kizárta. Természetesen ezt árnyalja a versenyjogi jogalkalmazásból eredő elrettentés, azonban még egy precedens által lefedett ügyben sem köteles egyetlen vállalkozás sem arra, hogy (a fúziókontroll tárgykörét kivéve) gazdasági működését a versenyhatósággal folyamatosan auditáltassa. Erre a hatályos versenyjogi rezsim alatt lehetősége sincs. Sok esetben adott piaci magatartás jogszerűségének megítélése évtizedes jogi, közgazdaságtani munka eredménye. A digitális gazdaság világában végbemenő gazdasági folyamatok hatékony állami ellenőrzésében a versenyjog e szerint azért nem megfelelő eszköz, mert e folyamatok (például a piacért folytatott verseny) által esetlegesen okozott versenykár a versenyjog beavatkozási pontjában már visszafordíthatatlan.[59] A DMA célja e tekintetben a tiltott magatartások pontos meghatározásával és az anyagi jogba ágyazott, a Bizottságot kötő bizonyítási sztenderdek alacsonyabban való megvonásával az időszerű közhatalmi beavatkozás lehetőségének megteremtése.[60]

3.3. Tartalmi korlátok – transzparencia és a versenyjogi analízis nehézségei

A versenyelméletről vallott felfogás nyomán kialakított gazdaság- és versenyszabályozási környezetben érvényesülő versenypolitika eszközeként megjelenő versenyjogi normák alkalmazásának közös tartalmi tesztje a 'teljesítmény' sérelme. Amennyiben a magatartás nyomán a 'teljesítmény' romlik, úgy a magatartás jogellenes.

A felhalmozódó közgazdaságtani és jogalkalmazói tapasztalat egyes magatartásokkal kapcsolatban azok várható 'teljesítményre' gyakorolt hatása nyomán a joggyakorlat strukturált jogi teszteket alakított ki, amely jogi tesztek tehát valójában azok a proxyk, amelyen keresztül a vizsgált magatartás piaci hatásait feltárni szándékozik a jogalkalmazó. A strukturált jogi teszt (amely tehát a magatartások formai jegyeit jeleníti meg) 'teljesítményre' gyakorolt káros

56 DMA (6), (7), (13) preambulumbekezdés.

57 A DMA saját szövege [(8) preambulumbekezdés] szerint a szabályozás jogalapja a jogharmonizációs célú EUMSz. 114. cikk.

58 DMA (28) preambulumbekezdés.

59 Crémer–Welker–Schweitzer i. m. 52.

60 Wörsdörfer i. m. 3.; Larouche – De Streel (2021) i. m. 556.

hatását magyarázó elméleti kategória a 'kárelmélet' (*theory of harm*). Noha minden versenyjogi visszaélés különbözik, egyes magatartástípusok káros hatásaival kapcsolatban magasabb absztrakciós szinten is megállapítható, hogy azok a versenyre *jellemzően* káros hatást gyakorolnak (azaz: rontják a 'teljesítményt'), a kárelmélet pedig a magatartás és a teljesítményromlás közötti közgazdaságtani összefüggésekre kínál magyarázatot.

A kárelmélethez való tartalmi ragaszkodás – tehát az az alapvetés, hogy a kárelmélet igazolása nélkül a közhatalmi beavatkozás jogtalan –, a digitális gazdaság szabályozása során a gazdasági folyamatok átláthatatlanságából eredő bizonyítási nehézségek, valamint a digitális gazdaság sajátosságai okaiból eredően egy olyan helyzetet generált, amelyet a második típusú (be nem avatkozási) versenyjogi kikényszerítési *hibák* jellemeznek.[61] A kapuőrök extremitásokba hajló piaci jelenlétének fényében a versenyjog korlátai leginkább az EUMSZ. 102. cikkének kikényszerítésének és bizonyos speciális okokból a fúziókontroll fényében relevánsak.

A versenyjogi bizonyítás a kárelmélet és a vizsgált magatartás hatásai tekintetében tartalmilag kötött az anyagi jog szerint. A tényállás tisztázása a jogalkalmazó feladata, és a versenyjogi jogalkalmazás történetét tekintve a közösségi és uniós versenyjogi ügyek időtartama fényében ez egy nehéz és bonyolult folyamat, hiszen a részleteiben tisztázott tényállás a helytálló jogi következtetés levonásának záloga. Azonban a túl magasan meghatározott bizonyítási sztenderd gátolhatja a hatékony jogalkalmazást. A digitális gazdaságot uraló ökoszisztémák ellen folyó ügyekben például egy végtelenül bonyolult rendszer belső összefüggéseiben rejlik valamilyen versenyjogilag releváns tény, és a rendszer üzemeltetőjének legkevésbé sem érdeke, hogy e tény bizonyítottan tudottá váljon.[62] Hovatovább, a gépi tanuláson alapuló algoritmikus rendszerek vizsgálata során a tényanyag teljes és hiteles felderítése el is lehetetlenülhet, hiszen ezek esetében a releváns tények (a rendszer döntései) okait jelentő adatkorpusz napról napra változik, illetve egyes algoritmizált döntési folyamatok kevéssé visszafejthetőek. Természetesen a mindenkori közhatalom versenyjogi apparátusának elégtelensége a tényállás teljeskörű feltárásának feladatában önmagában nem indokolhatja egy speciális, és szigorú kötelezettségeket támasztó szabályozás létrejöttét, azonban a DMA által szabályozott szektorban az információs aszimmetria, ami a platformok, a nyilvánosság és a közhatalom tengelyén fennáll, pozitív, speciális magatartási szabályok hiányában elfedhet olyan magatartásokat, amelyek egyébként is tiltottak, de felderítésük és a kárelmélet igazolásához szükséges mértékű bizonyításuk nagyjából lehetetlen.

A kárelmélet igazolásához (azaz a versenyjogi kihágást állító nyitott törvényi tényállások alkalmazásához) a versenyjog strukturált jogi tesztjei felépítése során közgazdaságtani szempontból leginkább az árak segítségével operacionalizálja a vizsgált magatartások hatásait. Ezt a bevezetőben a versenyjog tudományos szolipszizmusának neveztük. E minőségnek azonban a DMA komplementerszerepe tekintetében is van relevanciája. A digitális gazdaság sajátosságai fényében a versenyjog számára megnehezül mind a releváns termékpiac, mind a verseny érdemi korlátozása tényeinek megállapítása. Ennek egyik oka az, hogy számos releváns szolgáltatás pénzben ki nem fejezhető áron vehető igénybe. A releváns piac meghatározásában

61 Khan i. m.; Cohen i. m. (2017) 188.

62 A tartalomszabályozás (*content moderation*) és a keresőmotorok, valamint más algoritmizált szortírozási platformműködések modalitásai fontos téma. Erről ld.: Cohen (2019) i. m. 52., 140. Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról (P2B rendelet, HL L 186, 2019. 07. 11., 57–79. o.) indokolásában is többször előfordul, hogy az átláthatóság hiánya a *downstream* piacokon káros kereskedelmi gyakorlatokhoz vezethet; P2B rendelet (8) preambulumbekezdés, 5. cikk (1) bekezdés, 9. cikk.

kulcsszerepet játszó keresleti helyettesíthetőség például kevéssé mérhető akkor, ha a szolgáltatások ingyenesek.[63] A termékpiacok meghatározásának további nehézsége, hogy kevés olyan digitális szolgáltatás létezik a számunkra releváns piacokon, amely önmagában valósítaná meg értékpropozícióját. Vegyük például az Outlook rendszerét. Az Outlook és a Gmail számfüggetlen személyközi hírközlési szolgáltatásai közös piacának megállapításában gondot jelent, hogy mindkét szolgáltatás egy nagyobb ökoszisztéma része. Az Outlookra kifejtett versenykényszer a Google részéről tehát nem kizárólag abból ered, hogy a Gmail minősége esetlegesen jobb, hanem több eltérő okból, például olyanokból, hogy az Outlook jellemzően a Microsoft Teams-szel kapcsolt funkciókat szolgál ki, és közösen alkotják egy-egy *business* szolgáltatási csomag részeit. Ezek a szolgáltatások könnyen lehet, hogy valójában nem alternatívái egymásnak, az általuk kiszolgált *igények* tekintetében. Az ökoszisztémák versenye ebből a szempontból a közös termékpiac meghatározását gyakorlatilag kizárja.

3.4. Elméleti korlátok – a versenyjog szerepe

A DMA specialitása indokolható egy elvontabb síkon is. Ahogyan említettük, a DMA mint a digitális piacok megtámadhatóságát előteremtő szabályozás rendelkezik liberalizációs célokkal is. Az uniós gazdasági szabályozás egy történeti jellemzője, hogy a piac szabályozásának ügyében a piacot építi is, de nem kizárólag a versenyjog eszközével. Az ordoliberális doktrína szerint a releváns piacokon az állam szerepe egy olyan kontextus *létrehozása*, (piaci konstruktivizmus) amelyben megvalósulhat a szabad verseny. Ez a belső piac tekintetében nem a teljes elfordulást jelenti a természetes gazdasági valóságtól, amely a *laissez-faire* gazdaságpolitika nívója, hanem bizonyos szintű pozitív integrációs (re-regulációs) gazdaságszabályozási célt.[64]

A piaci konstruktivizmus a versenyjog szerepét is befolyásolja. A versenyjog ordoliberális szemléletben azon magatartások szankcionálására eszköz, amelyek formális[65] és tartalmi[66]

63 Például vegyük a sokat használt SSNIP-tesztet, ami egy hipotetikus monopolista iteratív áremeléseinek hatását vizsgálja. A teszt úgy működik, hogy egy hipotetikus monopóliumot egy hipotetikus piacon veszünk alapul, és azt vizsgáljuk, hogy e monopólium 5%-os áremelése nyereséges lehet-e ezen a piacon. Ha a nem, az éppen vizsgált termékkereslet rugalmasságának köszönhető, tehát a hipotetikus piac nem definiálja a meghatározandó piacot, nagyobb árukosarat kell bevonni. Ezt a nagyobb kosarat azután bevonjuk a hipotetikus piacmeghatározásba és a kereslet rugalmasságát ismét a fent leírt módon teszteljük. Ezt a lépéssorozatot egészen addig ismételjük, amíg a monopolista nem tud kis lépésekben árat emelni és megtartani a keresletet. Amikor a hipotetikus monopólium kicsi, de jelentékeny módon tud árat emelni anélkül, hogy a fogyasztók alternatív termékeket keresnének, meghatároztuk a releváns piacot. A Bizottság közleménye a közösségi versenyjog alkalmazásában az érintett piac meghatározásáról, HL C 372, 1997. 12. 09., 5–13.; a Bizottság döntése a IV/M. 190 Nestlé/Perrier-ügyben, HL L 356, 1992. 12. 05., 1–31. o.

64 Ngoc Nha Tinh Tran: *EU Competition Law under Ordoliberalism – A Case Study of Excessive Pricing in Pharmaceutical Sector* [Szakdolgozat]. Malmö, Malmö Universiteit, Kultur och Samhälle, 2020. https://www.diva-portal.org/smash/get/diva2:1483789/FULLTEXT01.pdf

65 A formális hozzáállás veszélyeiről a vertikális megkötések versenykorlátozó minőségének megítélése kérdésében ld.: Hans Zenger – Mike Walker: Theories Of Harm In European Competition Law: A Progress Report. In: Jacques Bourgeois – Denis Waelbroeck (szerk.): *Ten Years of Effects-Based Approach in EU Competition Law.* Brüsszel, Bruylant, 2012. 21.

66 Az EUMSZ. 101. cikke szempontjából jogellenes magatartások meghatározásához a 101. cikk (3) bekezdése alapján tartalmi szempontokat is szükséges vizsgálni. Oles Andriychuk: *The Normative Foundations of European Competition Law.* Cheltenham–Northampton, Edward Elgar Publishing, 2017. 272. https://doi.org/10.4337/9781786436078

szempontból is eltérnek a tökéletes verseny jellemzőitől. Elméleti szempontból tehát a versenyjog azokon a piacokon hatékony eszköz, amelyek sajátosságaikból adódóan nem törekszenek monopóliumok kialakulása felé; azokon a piacokon, ahol legalább hipotetikusan adott az érdemeken alapuló verseny sztenderdje. A liberalizációs célok, a piacnyitás pedig azokban a szituációkban játszik szerepet, amikor ez hiányzik. Ezt a viszonyt nagyon jól szemlélteti a hírközlési liberalizáció folyamata, amelynek az elején kevéssé volt opció tisztán a versenyjog eszközével garantálni a piac hatékony működését, leginkább azért, mert az inkumbensek jelenlétében és a verseny hiányában a verseny önszabályozói és elosztói szerepe is hiányzott. A hírközlési piac szabályozásában ismerünk egy, a versenyjogi gondolatiságra támaszkodó, a speciális jelentős piaci erőt megállapító háromelemű tesztet, amely strukturális és nem átmeneti belépési korlátokkal terhelt olyan piacokon reagál pozitívan, ahol állandósult piaci kudarcok okán a versenyjogot kiegészítő szabályozási eszközökre van szükség.[67] E teszt annak a példája, amikor a versenyjogon kívüli eszközöket igazolunk a versenyjogban is használatos fogalmakkal, hasonló gondolatisággal. A DMA ebben a kontextusban pedig az a speciális eszköz, amely a természetes monopólium felé törekvő digitális piacokon megteremtheti a megtámadhatóság állapotát: egy szabadpiacot, ahol a kapuőrökkel való frontális és komplementer[68] verseny nem pusztán elméleti lehetőség, hanem gyakorlati realitás. Ez az az állapot, amelyben már újból elégséges lehet a szabályozás körén kívül visszatérni a versenyjogi eszköztárhoz, mert azok a perzisztens piaci kudarcok, amelyek igazolják a DMA-t, a DMA érvényesülése okán már nem gátolják a verseny kialakulását.

Ebben a narratívában a versenyjog szerepe is tisztábban látszódik. A versenyjog egyik funkciója eszerint az, hogy a DMA által megtámadhatóvá tett, azaz *kialakított* versenyző piacokon, amelyek leginkább a kapuőrök teljes ellenőrzése alól liberalizált *downstream* piacok (ezt értjük komplementer verseny alatt) másrészt pedig a kapuőrök között kialakuló frontális értelemben versenyző piacok tekintetében a hagyományos versenyjogi célokat kikényszeríti. A DMA e tekintetben megszünteti a versenyjogi paradigma idioszinkratikus válságát, amely a tömeges közvetítés sajátos, természetes monopóliumok felé törekvő piacain az elmúlt két évtizedben kialakult. A versenyjog másik, a tanulmány tekintetében fontosabb szerepe pedig az, hogy a kárelmélethez való empirikus ragaszkodása ellenére képes informálni a jó szabályozást a digitális piacokon, hiszen a két állami beavatkozás céljai részben közösek. Ennek a hasonlóságnak a bizonyítéka a fenti háromelemű tesztnek és a komplementer szabályozásnak (DMA) a versenyjoghoz képesti speciális szerepe is. E hasonlóságnak a nélkülözhetetlen eszközök doktrínája pedig a példája, ugyanis e doktrína a DMA több rendelkezése tekintetében és a DMA liberalizációs céljai tekintetében is releváns.

67 Pierre Larouche – Alexandre De Streel: *Interplay between the New Competition Tool and Sector-Specific Regulation in the EU: Expert Study.* Luxemburg, Publications Office of the European Union, 2020. https://data.europa.eu/doi/10.2763/521287

68 A kapuőrök által uralt *downstream* piacokon történő verseny.

4. Az ügyletkötéstől való elzárkózás és a nélkülözhetetlen eszközök doktrínája

4.1. Jogfejlődés és a doktrína lényegi tartalma

Az erőfölénnyel visszaélés (EUMSZ 102. cikk) nyitott törvényi tényállás, ennek megfelelően bármely olyan piaci magatartás, amely visszaélést valósít meg, annak tárgyi hatálya alá eshet.[69] Az ügyletkötéstől elzárkózás lehetséges piaclezáró hatásait elsőként gyógyszeripari alapanyagok kontextusában vizsgálta a Bizottság a Commercial Solvents-ügyben.[70] Az EUB – a Bizottsággal egyetértve – abban látta a verseny sérelmét, hogy az erőfölényes vállalkozás egy nélkülözhetetlen alapanyag szállításának megtagadásával teljesen kizárta a *downstream* piacon zajló versenyt. Az EUB a United Brands-ügyben[71] megerősítette, hogy egy fennálló üzleti kapcsolat versenyellenes hatással járó megszakítása is megvalósíthat visszaélést az EUMSZ 102. cikkének értelmében.

A joggyakorlat felismerte, hogy az ügyletkötéstől elzárkózás szoros összefüggést mutat a szellemi alkotások jogával, hiszen pl. a szabadalom lényege, hogy a szabadalom jogosultja jogszerűen zárhatja ki a hozzáférést keresőket a szabadalom hasznosításából. Az EUB a szellemi alkotások és az ügyletkötéstől való elzárkózás közötti ellentmondást a Magill-ügyben[72] úgy oldotta fel, hogy a hozzáférés megadásának feltételéül szabta egy új termék létrehozását, amelyre valós fogyasztói igény mutatkozik. Hasonló megfontolások vezették a Bíróságot az IMS Health-ügyben hozott ítélet meghozatala során is.[73] A belső piaci integráció az uniós versenyjog evidens célja, ennek megfelelően a párhuzamos exportot ellehetetlenítő ügyletkötéstől elzárkózást is jogellenesnek minősítette a Bíróság a Sot-Lélos-ügyben.[74]

Mindazonáltal a vonatkozó joggyakorlat kapuőr platformok tekintetében legrelevánsabb vonulatát a kritikus infrastruktúrákhoz való hozzáféréssel kapcsolatos ügyek jelentik. Ebben a körben az Oscar Bronner-ügy fektette le a jogalkalmazás alapjait, mely ügyet a liberalizált telekommunikációs piacok hálózata felett rendelkező inkumbens vállalkozások hozzáférési kötelezettségével kapcsolatos gyakorlat követett (ld. pl. a Deutsche Telekom-ügyet). A Bronner-ügy legfontosabb tanulsága, hogyha egy vállalkozás saját használatára hozott létre egy, az általa nyújtott szolgáltatás javítását célzó infrastruktúrát, úgy az ahhoz való hozzáférést csak szigorú feltételek mentén szabad engedélyezni, hiszen ez erodálja az innovációs és kockázatvállalási ösztönzőket. A Slovak Telekom-ügyben a Bíróság cizellálta ezt a megközelítést, amikor is kimondta, hogy amennyiben az erőfölényes helyzetben lévő vállalkozás

69 T-612/17 Google LLC, Google Inc. és Alphabet, Inc. kontra Európai Bizottság [ECLI:EU:T:2021:763] [154].

70 C-6/73. és C-7/73. sz egyesített ügyek Istituto Chemioterapico Italiano S.p.A. és Commercial Solvents Corporation kontra az Európai Közösségek Bizottsága [ECLI:EU:C:1974:18].

71 C-27/76. sz. ügy United Brands Company és United Brands Continentaal BV kontra az Európai Közösségek Bizottsága [ECLI:EU:C:1978:22].

72 C-241/91. P. és C-242/91. P. sz. egyesített ügyek Radio Telefis Eireann (RTE) és Independent Television Publications Ltd (ITP) kontra az Európai Közösségek Bizottsága [ECLI:EU:C:1995:98].

73 C-418/01. sz. ügy IMS Health GmbH & Co. OHG kontra NDC Health GmbH & Co. KG. [ECLI:EU:C:2004:257].

74 C-468/06 és C-478/06. sz. egyesített ügyek Sot. Lélos kai Sia EE és társai kontra GlaxoSmithKline AEVE Farmakeftikon Proïonton, korábban: Glaxowellcome AEVE [ECLI:EU:C:2008:504].

a kérdéses infrastruktúrához bármilyen megfontolásból hozzáférést ad (pl. mert jogszabály kötelezi erre, vagy tisztességtelen feltételek mellett már jelenleg is biztosítja azt), akkor az innovációs ösztönzők már eleve hiányoznak, ezért a hozzáférésnek nem feltétele a kérelmezett eszköz nélkülözhetetlen jellege. További releváns következtetés vonható le a Servizio Elettrico Nazionale-döntés alapján, amely szerint amennyiben a rendelkezésére álló eszközre a vállalkozás nem az érdemeken alapuló verseny során tett szert, úgy az azzal való rendelkezési joga is korlátozott.

A digitális platformpiacok kontextusában a Google-Shopping-ügyben született törvényszéki döntés tartalmaz iránymutatást, amikor is a Bizottság, és a Bizottság nyomán a Törvényszék megállapította, hogy a *leveraging* önálló visszaéléstípus, amely nem azonosítható az ügyletkötéstől elzárkózással. A DMA és az ügyletkötéstől elzárkózás közötti kapcsolatot tehát többek között a joggyakorlatnak az a vonulata alapozza meg, amely egy – az inkumbens vállalkozás által létrehozott – infrastruktúrához (platformhoz) való hozzáférési kötelezettség terjedelmét szabályozza.

Főszabály szerint egy domináns (erőfölényes) vállalkozás sem kötelezhető arra, hogy akarata ellenére üzleti kapcsolatot létesítsen versenytársaival. A tulajdonhoz való jog és a szerződési szabadság olyan alapvető jogosultságok, amelyek korlátozására csak szigorú körülmények között kerülhet sor.

Az ügyletkötéstől való elzárkózást megvalósító magatartás lényege szerint, az erőfölényben lévő vállalkozás a kérdéses '*input*hoz' hozzáférést kérő vállalkozással nem hajlandó szerződést kötni, azaz nem szolgálja őt ki. Ez jellemzően akkor vezet versenyjogi problémákhoz (és ennek megfelelően a jogalkalmazó által alkalmazott strukturált jogi teszt szerint), ha az alábbi feltételek együttesen állnak fenn:

– a vállalkozás erőfölényes helyzetben van;
– a vállalkozás megtagadja az üzletkötést, vagy a meglévő kapcsolatot megszünteti, illetve annak fenntartását irreális feltételhez köti;
– az elzárkózás a piacon folyó versenyre, annak hatékonyságára érezhetően negatív hatással jár.

A piacon folyó versenyre gyakorolt érezhetően negatív hatás jellege határozza meg az adott – károsnak ítélt – magatartás mögött meghúzódó kárelméletet is. Az ügyletkötéstől elzárkózás joggyakorlata lényegében kontextus-specifikusan határozta meg a kárelméletet. Mivel az ügyletkötéstől elzárkózás számtalan kontextusban felmerülhet, ezért absztrakt módon valójában lehetetlen érdemi állítást megfogalmazni annak potenciális versenykárosító hatásairól.
A joggyakorlat ilyen versenykárnak tekinti például az alábbiakat:

– fennálló üzleti kapcsolatok megszakítása a *downstream* piacon már jelen lévő versenytárssal, annak az érintett piacról történő kiszorítása érdekében;[75]
– a kiszolgálás párhuzamos export ellehetetlenítését célzó megtagadása;[76]

75 C-6/73. és C-7/73. sz egyesített ügyek Istituto Chemioterapico Italiano S.p.A. és Commercial Solvents Corporation kontra az Európai Közösségek Bizottsága [ECLI:EU:C:1974:18]; C-27/76. sz. ügy United Brands Company és United Brands Continentaal BV kontra az Európai Közösségek Bizottsága [ECLI:EU:C:1978:22].
76 C-468/06 és C-478/06. sz. egyesített ügyek Sot. Lélos kai Sia EE és társai kontra GlaxoSmithKline AEVE Farmakeftikon Proïonton, korábban: Glaxowellcome AEVE [ECLI:EU:C:2008:504].

– a verseny mesterséges szűkítése a nem az érdemeken alapuló verseny révén megszerzett eszközökhöz való hozzáférés megtagadása révén;[77]
– olyan új termék létrehozásának megakadályozása, amelyre tényleges fogyasztói igény mutatkozik.[78]

Az alábbiakban áttekintjük az ügyletkötéstől elzárkózás doktrínájának történeti fejlődését, különös hangsúlyt fektetve az egyes esetekben megjelenő kárelméletekre.

4.2. A DMA 5. cikk (7) bekezdése az ügyletkötéstől elzárkózás tekintetében – komplementer szolgáltatások

A tömeges közvetítés üzleti modelljében ökoszisztémába integráló hozzáférési kapukat ismerünk, amelyek a DMA tekintetében legtöbbször alapvető platformszolgáltatásnak minősülnek, hiszen ezek kötik össze az üzleti felhasználókat a végfelhasználókkal. A hozzáférési kapuk igénybevételének feltételeit manipulálva a kapuőr erős alkupozíciót élvez, hiszen a hozzáférési kapu igénybevétele a piacon maradás feltétele, azt megkettőzni – az alapvető platformszolgáltatások rétegén kialakítani versenyzői állapotot – a kapuőrök piaci jelenléte, minősége és mértéke tekintetében, figyelembe véve a végfelhasználók váltási költségeit, irreális; és így az adott alapvető platformszolgáltatás egy piaci szűk keresztmetszet.[79] Mindezek fényében ez alkupozíció, és az alapvető platformszolgáltatás tekintetében kialakult függés használható az ökoszisztémába való kötelező integráció eszközeként, azaz az 5. cikk (7) bekezdése tekintetében a komplementer szolgáltatások igénybevételének a hozzáférési kapu igénybevételével való összekapcsolására. Ezt az alkupozíciót célozza gyengíteni a DMA a következő kötelezettség előírásával:

> „Az üzleti felhasználók által a kapuőr alapvető platformszolgáltatásainak igénybevételével nyújtott szolgáltatások esetében a kapuőr nem írhatja elő a végfelhasználók számára, hogy az ő azonosítási szolgáltatását, webböngésző-motorját, pénzforgalmi szolgáltatását vagy pénzforgalmi szolgáltatások nyújtását támogató technikai szolgáltatását – például alkalmazáson belüli vásárlásra szolgáló fizetési rendszerét – használják, illetve nem írhatja elő az üzleti felhasználók számára, hogy az említetteket használják, kínálják, illetve együttműködjenek azokkal."[80]

A DMA idézett cikke a megtámadhatóság fényében arra a kívánalomra reagál, hogy az üzleti felhasználók a kapuőr alapvető platformszolgáltatását úgy is igénybe tudják venni, hogy saját vagy harmadik féltől származó komplementer szolgáltatást használnak. A nélkülözhetetlen eszközök és az ügyletkötéstől való elzárkózás tekintetében az előírás mögött az a megfontolás húzódik, hogy a kapuőrök hozzáférési kapuja nélkül az adott *downstream* piacon az üzleti fel-

77 C-165/19. P. sz. ügy Slovak Telekom, a.s. kontra Európai Bizottság [ECLI:EU:C:2021:239].
78 C-241/91. P. és C-242/91. P. sz. egyesített ügyek Radio Telefis Eireann (RTE) és Independent Television Publications Ltd (ITP) kontra az Európai Közösségek Bizottsága [ECLI:EU:C:1995:98]; C-418/01. sz. ügy IMS Health GmbH & Co. OHG kontra NDC Health GmbH & Co. KG. [ECLI:EU:C:2004:257].
79 Davola–Malgieri i. m. 7.
80 DMA 5. cikk (7) bekezdés.

használó fellépése kizárt (nélkülözhetetlenség), ezt tükrözi az adott szolgáltatás alapvető platformszolgáltatásként való kategorizálása, továbbá az alapvető platformszolgáltatás minősége, amely szerint fontos kapuként szolgál a végfelhasználók elérésében.[81] A nélkülözhetetlen eszköz összekapcsolása az adott komplementer szolgáltatással, a komplementer szolgáltatások piacán torzítja a versenyt az üzleti felhasználó választási szabadságának korlátozásával,[82] hiszen amennyiben a komplementer szolgáltatást nem veszi igénybe az üzleti felhasználó, a kapuőr elzárkózik az ügyletkötéstől. Ez utóbbira reagál az idézett kapuőri kötelezettség, miszerint az alapvető platformszolgáltatásnak a komplementer szolgáltatással való összekapcsolása tiltott.

A DMA 5. cikk (7) bekezdésében impliciten megjelenik az árukapcsolás tényállása is. Az Epic Games, az Alphabet és az Apple ellen folytatott pereiben például az idézett rendeleti tényálláshoz nagyon hasonló, árukapcsolási ügyben született a hozzáférést kérőnek igazat adó ítélet. Ami igazán relevánssá teszi az ügyletkötéstől való elzárkózás tényállását e cikk tekintetében, az az, hogy a DMA itt az alapvető platformszolgáltatáshoz, azaz a nélkülözhetetlen eszközhöz való árukapcsolási feltételektől mentes hozzáférést garantál. E tekintetben a DMA a dominancia, a nélkülözhetetlenség és a hatékonyság beható empirikus vizsgálata nélkül (vagy ezek vélelmezésével), a kapuőrök infrastrukturális erejének[83] gyengítésével egyenlíti ki a komplementer szolgáltatások piacát a megtámadhatóság és a *fair* verseny[84] céljainak érdekében.

4.3. A DMA 6. cikk (4) bekezdése az ügyletkötéstől elzárkózás tekintetében – sideloading előírások

Az Apple *walled garden* típusú ökoszisztémájával szemben leggyakrabban megfogalmazott versenyjogi aggály a *sideloading* tilalmára vonatkozik; nevezetesen arra, hogy az Apple hardwareelemeken futó Apple operációs rendszer csak az Apple alkalmazás áruházából letöltött applikációkat hajlandó futtatni, az ökoszisztéma pedig aktívan, üzleti és technológiai eszközökkel küzd az alternatív forrásból származó szoftverek ellen.[85] Az Apple egyébként éppen jelen tanulmány írása során jelentette be, hogy a DMA-ban előírt kötelezettségek teljesítése céljából felszámolja a *sideloading* tilalmát szolgáló intézkedéseket.[86]

Ahogyan a digitális gazdaság jellemzőiről szóló részben írtuk, a vertikálisan integrált digitális ökoszisztémák létrehozása mögött meghúzódó gazdasági racionalitás, a végfelhasználókhoz való hozzáférés feletti kontroll kiaknázásának lehetősége.[87] Az ökoszisztéma működtetője

81 DMA 3. cikk (1) bekezdés b) pont.

82 DMA (43) preambulumbekezdés.

83 Busch i. m. 11.

84 Ariel Ezrachi: EU Competition Law Goals and the Digital Economy. *Oxford Legal Studies Research Paper,* 17/2018., 1–27. https://doi.org/10.2139/ssrn.3191766

85 Friso Bostoen – Daniel Mândrescu: Assessing Abuse of Dominance in the Platform Economy: A Case Study of App Stores. *European Competition Journal,* vol. 16., no. 2–3. (2020). https://doi.org/10.1080/17441056.2020.1805698

86 Ld. az Apple bejelentését: Apple: Apple announces changes to iOS, Safari, and the App Store in the European Union [Sajtóközlemény]. *Apple.com,* 2024. január 25. https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union

87 Thomas Höppner – Philipp Westerhoff – Jan Weber: Taking a Bite at the Apple: Ensuring a Level-Playing-Field for Competition on App Stores. *SSRN Electronic Journal*, 2019. május 13. https://dx.doi.org/10.2139/ssrn.3394773

egyrészt szorosan ellenőrizheti a felhasználóinak szánt tartalmat, másrészt a tőle független fejlesztők és a felhasználók közötti tranzakciók után jutalékot számíthat fel, harmadrészt az infrastruktúra feletti teljes hatalom lehetővé teszi a saját, *downstream* piacokon versengő szolgáltatásainak diszkriminatív kiemelését.[88]

A DMA 6. cikk (4) bekezdése a *walled garden* típusú ökoszisztémák fentiekből fakadó versenyelőnyét igyekszik kompenzálni, amikor is előírja, hogy:

> „[a] kapuőrnek meg kell engednie és technikailag lehetővé kell tennie az olyan, harmadik fél szoftveralkalmazásai vagy szoftveralkalmazás-áruházai telepítését és tényleges használatát, amelyek a kapuőr operációs rendszerét használják vagy azzal együttműködnek, és biztosítania kell, hogy e szoftveralkalmazásokhoz vagy szoftveralkalmazás-áruházakhoz a kapuőr érintett alapvető platformszolgáltatásaitól eltérő eszközökkel is hozzá lehessen férni."

A DMA által választott szabályozási megoldás gyakorlatilag egy szektorális hatályú, *ex-ante,* jogellenes magatartás hiányában is megkövetelt ügyletkötési kötelezettség.[89] Az ügyletkötéstől elzárkózás eseti *ex-post* jogorvoslatának szektorális kiterjesztése mögött meghúzódó jogalkotói megfontolás minden bizonnyal az, hogy a vertikálisan integrált digitális ökoszisztémákban a *sideloading* tilalma a piacszerkezetből fakadó olyan természetes következmény, amely az alkalmazásáruházak és az applikációik piaci szintjén jelentkező strukturális okokkal magyarázható. A fentiekkel összhangban pedig a versenyszabályozás és a gazdaságszabályozás egyik delimitációs pontját éppen a strukturális okokra visszavezethető piaci kudarcok jelentik. További következtetés vonható le ennek megfelelően arra nézve, hogy a jogalkotó piaci kudarcként azonosítja a vertikálisan integrált digitális ökoszisztémák sajátos működési mechanizmusát, nevezetesen a platform feletti totális kontroll és alternatívátlanság jelenségét.[90]

Az ügyletkötéstől elzárkózással kapcsolatos több évtizedes versenyjogi joggyakorlatból származó tudás tehát a DMA 6. cikk (4) bekezdésében is megjelenik, azzal, hogy a fent elemzett bekezdés is egyértelműen rámutat arra a sajátos helyzetre, hogy jelen esetben a szektorális szabályozás és a versenyjog célja megegyezik, eszközeik pedig lényegileg nem különböznek (hiszen pl. az általuk adresszált jelenségre adott megoldásuk is hasonló: interoperabilitási/ügyletkötési kötelezettség előírása).

5. Konklúzió – a versenyjog helye a kapuőrök szabályozási rezsimében

Felmerül a kérdés, hogy lehet-e helye a versenyjog alkalmazásának egy speciális követelményeket előíró, versenyserkentő célzatú szektorális szabályozási rezsim keretei között is, avagy a DMA *lex specialis*-ként (figyelemmel annak az EUMSZ 102. cikkével nagy mértékben rokon szabályozási tárgykörére) valójában alkalmazhatatlanná teszi a versenyjogi szabályokat. A Bíróság a Deutsche Telekom-ügyben megállapította, hogy

88 Bostoen–Mândrescu i. m.

89 Firniksz Judit: *Pillanatkép a digitális piacok szabályozásáról – A DMA a vállalati compliance tükrében.* Budapest, Wolters Kulwer Hungary, 2023. 182.

90 Pablo Colomo: *The New EU Competition Law*. Oxford, Hart Publisher, 2023. 135.

> „[a]lkalmazandó az [EUMSZ 101. cikk] és az [EUMSZ 102.] cikk, ha kitűnik, hogy a nemzeti szabályozás nyitva hagyja a lehetőséget, hogy a vállalkozások autonóm magatartása a verseny megakadályozására, korlátozására vagy torzítására vezethessen."[91]

Amennyiben analógiaként alkalmazzuk a DMA-ra a nemzeti szabályozási rezsimmel kapcsolatban megállapítottakat, akkor levonhatjuk azt a következtetést, hogy a versenyjog csak abban a szűk körben nem alkalmazható, amelyen belül a szektorális szabályozási rezsim konkrétan előírja a vállalkozások számára a követendő magatartást. Mindazonáltal figyelemmel arra, hogy a DMA 6. cikk (4) bekezdése szigorúbb feltételeket támaszt, mint az EUMSZ 102. cikk alapján megkövetelhető magatartás (hiszen a kapuőrnek nincs mérlegelési jogköre abban a tekintetben, hogy kíván-e interoperabilitást biztosítani *downstream* versenytársai számára, és csak kivételes esetekben tagadhatja meg azt, szemben a versenyjog eseti megítélésű megközelítésével), így ezen bekezdés tekintetében a legvalószínűbbnek az tűnik, hogy noha a versenyjogi előírások továbbra is kötelezik a kapuőröket,[92] fogalmilag nem jöhet létre olyan helyzet, hogy a kapuőr magatartása nem ütközik a DMA 6. cikk (4) bekezdésébe, sérti azonban az EUMSZ 102. cikkét.

A DMA a kapuőrök szabályozási rezsimjét a nélkülözhetetlen eszközök és az ügyletkötéstől elzárkózás hagyománya tekintetében, versenyjogi szempontból releváns tények vélelmezésével valósítja meg. A legfontosabb ilyen általános vélelem az alapvető platformszolgáltatás; a kapuőr fogalmi kettősben jelenik meg, hiszen az alapvető platformszolgáltatásként való kijelölés implikálja, hogy a kapuőr egy megkerülhetetlen üzleti partner, az alapvető platformszolgáltatása pedig egy megkettőzhetetlen infrastruktúra. A fent említett rendelkezések tekintetében azonban e vélelmek tárgya versenyjogi szempontból leginkább az, hogy a tömeges közvetítés üzleti modelljének exkluzív stratégiái, a tömeges közvetítést végző infrastrukturális szerepű vállalkozásoktól függő *downstream* piacokon torzítják a versenyt, és ezáltal károsak. A hasonlóság az ügyletkötéstől való elzárkózás és a DMA között magyarázható a versenyjogi vélelmekkel, amelyek a DMA-t mint az EUMSZ 102. cikkének szabályozási formában való megvalósítását lehetővé teszik.

Visszatérve a tanulmány bevezető gondolataihoz, fontos leszögezni, hogy ez az a fajta hasonlóság, amely tekintetében nem meztelen a király. A DMA legtöbb rendelkezése a versenyjogi joggyakorlatban elért tudást vezeti be egy, a versenyjogtól alapvetően különböző, *ex-ante*, *compliance* alapú szabályozási rezsimbe. Ahogy említettük, e rezsim megvalósításának feladatában a Bizottság tág diszkréciónak örvend, hatásköreinek terjedelme egyes kérdésekben, például az alapvető platformszolgáltatások konkrét meghatározásának eljárási kívánalmainak kérdésében, nem tisztázott. A Bizottság tág mozgásterében tátongó űr jogi tartalommal való megtöltése e diszkréció okán nagy felületű jogértelmezési kihívás. Ebben a kihívásban pedig a hasonlóság okán feltétlenül szükség lesz a versenyjogi hagyomány használatára.

91 A C-280/08. P. sz. ügy. Deutsche Telekom AG kontra Európai Bizottság [ECLI:EU:C:2010:603] 80. pont.
92 DMA (11) preambulumbekezdés.

Az algoritmusok szerepe a közösségimédia-platformokon alkalmazott sötét megoldások tekintetében

Az interfész mögötti manipulatív technikák kora[1]*

Huszár Daniella

1. Bevezetés

A közösségimédia-platformok 2024-re vitathatatlan népszerűségnek örvendenek, amit mi sem mutathat jobban, mint hogy közel 5 milliárd felhasználó használja ezen platformok valamelyikét, ami a világ népességének több mint 60%-át teszi ki. Statisztikai adatok alapján e platformok közül a Meta Platforms Inc. Facebook platformja rendelkezik a legtöbb, mintegy 3,05 milliárd felhasználóval. Egy átlag felhasználó naponta hozzávetőlegesen 2,5 órát tölt a virtuális valóság kínálta szolgáltatások, valamint élmények világában.[2] E számadatokat látva nem meglepő, hogy a közösségimédia-platformok mindennapi életünk szerves részévé váltak, átalakítva a kommunikációnkat, az információszerzési folyamatainkat, mi több, még a döntéshozatalunkat is, legyen szó akár egy célzott hirdetésről, influenszermarketingről, vagy az algoritmusalapú tartalomszűrésről és -generálásról. A digitális fejlődés eredményeként a korábban kizárólag offline térben elérhető tevékenységek és szolgáltatások szinte kivétel nélkül hozzáférhetővé váltak a digitális szférában is, sőt, adott esetben sokkal nagyobb választékot nyújtanak. A lehetőségek terjedésével egyre több olyan módszer és eszköz jelent meg, amelyek célja a felhasználói döntések manipulálása, szándékos irányítása, gyakran a felhasználók saját érdekeivel ellentétes, nem kívánt eredmények előidézése.[3] Ezekre a módszerekre főként 'sötét megoldásokként', vagy angolul '*dark pattern*'-ként utalnak, amelyek a korábbi, a felhasználók minél szélesebb körének elérését és bevonását célzó marketingstratégiákkal ellentétben mára sokkal kifinomultabb és hatékonyabb technikákat jelölnek, amelyek képesek nemcsak megszólítani a felhasználókat, de még a kívánt eredmény felé is terelni őket.[4] Tekintettel arra, hogy a sötét megoldások elterjedése továbbra is komoly etikai aggályokat vet fel, természetük és hatásuk megértése kiemelkedően fontos témává vált napjainkban.

A digitális fejlődéssel és a közösségimédia-platformok népszerűségével a mesterséges intelligencia- (MI-) alapú technológiák használata is fokozottan nőtt, ami megfigyelhe-

1 *A tanulmány a Kulturális és Innovációs Minisztérium ÚNKP-23-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

2 Rohit Shewale: Social Media Users 2024 (Global Data & Statistics). *DemandSage.com,* 2024. március 4. https://demandssage.com/social-media-users/index.html

3 Európai Bizottság: *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation – Final report.* Luxemburg, Publications Office of the European Union, 2022. https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1

4 Ryan Calo: Digital Market Manipulation. *George Washington Law Review*, vol. 82., no. 4. (2014). http://dx.doi.org/10.2139/ssrn.2309703.

tő mind a platformok kialakításában, mind a sötét megoldások alkalmazásában. Az MI használatával a platformok könnyen testre szabhatják a felhasználói élményeket és interfészeket, valamint manipulálhatják a felhasználói viselkedést is, mindezt azonban gyakran a felhasználók autonómiájának és magánéletének rovására. A sötét megoldások, különösen az algoritmusalapú technikák rendszerint az emberi pszichológiára vonatkozó ismereteket használják fel a felhasználói igényekre szabott tervezéssel kombinálva, növelve ezzel a felhasználói elkötelezettséget és a szolgáltatás ismételt igénybevételét.[5] E technikáknak ennek megfelelően gyakori működési elvük arra az emberi hajlamra építeni, miszerint a felhasználók gyakran hagyatkoznak feltételezéseikre, így nem feltétlenül olvasnak el minden egyes szót egy oldalon, félreértve ezzel akár az oldal tényleges célját, vagy éppen könnyen adják hozzájárulásukat olyan, általuk nem ismert adatkezelési műveletekhez, amelyek a megszokott zöld színnel jelölt ikonnal vagy kapcsolóval vannak társítva.[6] Figyelembe véve, hogy a közösségimédia-platformok által nyújtott szolgáltatások többnyire ingyenesen vehetők igénybe, bevételeik nagy részét hirdetésekből nyerik, amihez nélkülözhetetlen a felhasználói adatok gyűjtése, elemzése és felhasználása.[7] Ebből kifolyólag nem véletlen, hogy a közösségimédia-platformok arra törekednek, hogy minél inkább optimalizálják interfészeiket és növeljék a felhasználói elkötelezettséget annak érdekében, hogy a felhasználók minél több információt osszanak meg magukról, a lehető legtöbb bevételt generálva ezzel.[8] E célok elérése végett pedig a platformok közismerten olyan módszereket használnak, mint a sötét megoldások.[9]

Felhasználóik figyelmének növekvő pénzbeli értéke miatt[10] a technológiai vállalatok olyan függőséget okozó eszközökkel árasztották el interfészeiket,[11] amelyek kifinomult tervezési technikákra támaszkodnak a figyelem minél hosszabb ideig történő megtartása érdekében.[12] A felhasználók pedig könnyen ezen digitális élmények rabjaivá válnak, éppúgy, ahogyan a digitális világban zajló társadalmi interakciók függői lesznek.[13] Tekintettel ezen

5 Thomas Mildner – Gian-Luca Savino: Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook. In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21).* New York, Association for Computing Machinery, 2021 [a továbbiakban: Mildner–Savino 2021a]. https://doi.org/10.1145/3411763.3451659

6 Eetu Eskelinen: *Dark Design Patterns What Are the Next Steps Towards More Ethically Designed Digital Products and Services?* [Szakdolgozat.] Tampere, Tampere University of Applied Sciences, 2021. https://www.theseus.fi/handle/10024/476195

7 Thomas Mildner – Gian-Luca Savino: How Social Are Social Media: The Dark Patterns in Facebook's Interface [Konferenciaelőadás kézirata]. Yokohama (2021. május 8.): *Workshop 28: What can CHI Do About Dark Patterns?* on *2021 CHI Conference on Human Factors in Computing Systems*. https://arxiv.org/abs/2103.10725 [a továbbiakban: Mildner–Savino 2021b].

8 Mildner–Savino (2021b) i. m. 2., Lisette De Vries – Sonja Gensler – Peter S. H. Leeflang: Popularity of Brand Posts on Brand Fan Pages: An Investigation of the Effects of Social Media Marketing. *Journal of Interactive Marketing,* vol. 26., no. 2. (2012).

9 Eskelinen i. m. 15.

10 Thomas H. Davenport – John C. Beck: *The attention economy. Understanding the New Currency of Business Ubiquity.* Brighton, Harvard Business Review Press, 2002. 28.

11 Adam Alter: *Irresistible: The rise of addictive technology and the business of keeping us hooked.* New York, Penguin Press, 2017. 223.

12 Colin M. Gray – Yubo Kou – Bryan Battles – Joseph Hoggatt – Austin L. Toombs: The dark (patterns) side of UX design. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing* Systems (CHI '18). New York, Association for Computing Machinery, 2018. 7. https://doi.org/10.1145/3173574.3174108

13 Larry Dossey: FOMO, digital dementia, and our dangerous experiment. *Explore*, vol. 10., no. 2. (2014) 71.

tervezési technikák, illetve sötét megoldások elterjedtségére és problematikus jellegére, az átláthatóság és szabályozás legfőbb akadályait azon sötét megoldások alkalmazása jelenti, amelyek még nem szabályozottak egyértelműen, így egy szürke zónában helyezkednek el,[14] mint az akadályozási technikák (pl. 'csótánymotel'/'nehezített lemondás'), a kényszerített cselekvések (pl. 'kényszerített regisztráció') vagy az érzelmekre ható üzenetek (pl. 'megszégyenítés'). További kihívást jelentenek ugyanakkor azon manipulatív gyakorlatok is, amelyek kihasználják a felhasználók egyéni sebezhetőségét (pl. a felhasználó olyan üzeneteket, illetve hirdetéseket kap, amelyek a felhasználóról gyűjtött adatok alapján vannak személyre szabva), de éppen úgy okozhat nehézséget sokszor a klasszikus sötét megoldások azonosítása is.[15]

Az új addiktív technikák alkalmazása során sérülhet a felhasználó magánélethez való joga, amely magában foglalja az egyén döntési autonómiáját [16] – így annak eldöntését is, hogy ki és milyen mértékben férhet hozzá a felhasználó személyes adataihoz –, valamint jelentős hatással lehet mindemellett a véleménynyilvánítás és az információk, eszmék megismerésének és közlésének szabadságára is.[17] Mindezeket figyelembe véve, nem meglepő, hogy a sötét megoldások káros hatásai világszerte felkeltették a szabályozó szervek figyelmét, amelynek köszönhetően megtették az első lépéseket a felhasználók magánéletének és autonómiájának védelme felé, így többek között a kaliforniai fogyasztó védelmi törvény (California Consumer Privacy Act – CCPA), a coloradói adatvédelmi törvény (Colorado Privacy Act – CPA) vagy az Európai Unió digitális jogszabály-csomagjában található digitális szolgáltatásokról szóló jogszabály (Digital Service Act – DSA), illetve az adatrendelet (Data Act) elfogadásával.[18] E tanulmány az Európai Unió szabályozási rezsimére fókuszál elsődlegesen, amelynek részletesebb elemzését a 3. szakasz tartalmazza.

Következésképpen a fentiek alapján vitathatatlan, hogy a jogi elemzés kulcsfontosságú annak felmérésében, hogy ezek a gyakorlatok, valamint tervezési technikák összeegyeztethetők-e a hatályos törvényekkel, szabályozásokkal és etikai normákkal. Jelen kutatásom tézise, hogy a közösségimédia-platformok szolgáltatói, illetve a technológiai vállalatok által alkalmazott tervezési technikák és sötét megoldások nem összeegyeztethetőek a jelenlegi jogszabályi keretekkel, illetve etikai elvekkel. E tanulmány célja ennek megfelelően, hogy jogi szempontból vizsgálja a közösségimédia-platformokon alkalmazott sötét megoldásokat, valamint az MI alkalmazásának hatását, feltárva a felhasználók jogaira, a szabályozási megfelelésre és az általános etikai környezetre gyakorolt lehetséges következményeket. A vizsgálat során olyan releváns területeket elemzek, mint az adatvédelem, a fogyasztóvédelem és a plat-

14 Martin Brenncke: Regulating Dark Patterns. *Notre Dame Journal of International & Comparative Law*, vol. 14., no. 1. (2024).

15 European Commission: *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation – Final report.* Luxemburg, Publications Office of the European Union, 2022 április. https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1 27.

16 Marjolein Lanzing: "Strongly recommended" revisiting decisional privacy to judge hypernudging in self-tracking technologies. *Philosophy & Technology*, vol. 32., no. 3. (2019). https://doi.org/10.1007/s13347-018-0316-4

17 Az Emberi Jogok Európai Egyezménye 10. cikke szerinti véleménynyilvánítás szabadsága részeként védelemben részesülő jogok.

18 Thomas Mildner – Merle Freye – Gian-Luca Savino – Philip R. Doyle – Benjamin R. Cowan – Rainer Malaka: Defending Against the Dark Arts: Recognising Dark Patterns in Social Media. In: *Proceedings of the 2023 ACM Designing Interactive Systems Conference (DIS '23).* New York, Association for Computing Machinery, 2023. https://doi.org/10.1145/3563657.3595964

formszabályozás. A kutatás egy központi eleme a szabályozás feltárása mellett az alkalmazott gyakorlatok vizsgálata, és azok hatásának feltárása, átfogó képet nyújtva arról, hogy a sötét megoldások alkalmazása milyen mértékben sértheti a felhasználói jogokat, használhatja ki sebezhetőségüket, és sértheti potenciálisan a meglévő jogi szabályozási kereteket.

2. Sötét megoldások megjelenése és a taxonómia megalkotására törekvő kísérletek

A pszichológia tudományában már az 1990-es évek elején megjelentek az egyes viselkedési mintákat a viselkedésfüggőség formáinak minősítő nézetek.[19] Kutatók kimutatták, hogy számos viselkedés addiktívvá válhat, ha az eredmény kellően jutalmazó ahhoz, hogy sóvárgást váltson ki az egyénből.[20] Hamar világossá vált a technológia fejlődésével és a digitális kommunikációs technikák terjedésével, hogy egyes ember–gép interakciók is képesek különösen jutalmazónak minősülni, így adott esetben akár függőséget kiváltani.[21] Az újabb és

újabb technológiai vívmányok megjelenésével a függőségek típusainak is új fajtái törtek utat maguknak. Ezek a technikák többnyire a szokáshurok háromlépcsős folyamata köré épülnek, kezdve egy viselkedés végrehajtására késztetéssel (pl. értesítés érkezése arról, hogy egy ismerősünk reagált egy bejegyzésünkre), ezt követve egy cselekvés végrehajtásával (kijelző ellenőrzése, applikáció megnyitása), majd végül a cselekvésért járó jutalmazással (a társadalmi elfogadás által keltett kiteljesedés érzése).[22] Ennek a ciklusnak a többszöri megismétlése aztán ahhoz vezet, hogy a felhasználóban szokássá válik a szóban forgó termék vagy szolgáltatás használata.[23] A pszichológiában ezt *operáns kondicionálásnak* nevezik, amely esetében az egyének azt tanulják meg, hogy az általuk adott válasz minden esetben egy egyedi következménnyel jár.[24] Mivel azonban ezek a jutalmak és gyakoriságuk a felhasználók számára sokszor átláthatatlanok, szükségét érzik, hogy a biztonság kedvéért folyamatosan ellenőrizzék a készülékük vagy az alkalmazásokat, a jutalom reményében bízva. Az ehhez hasonló technikák, valamint sötét megoldások alkalmazása során a vállalkozásoknak lehetőségük van arra, hogy a felhasználókat a platformjukhoz láncolják a jutalmak (pl. reakciók, kommentek, jelvények) révén, még akkor is, ha ez azzal a következménnyel jár, hogy függőséget vált ki a felhasználókban.[25] A legtöbb interaktív digitális élmény, amelyet mindennap használunk, jellegét tekintve szokásformáló,[26] és olyan társa-

19 Isaac Marks: Behavioural (non-chemical) addictions. *British Journal of Addiction*, vol. 85., no. 11. (1990). https://doi.org/10.1111/j.1360-0443.1990.tb01618.x

20 Alter i. m. 223.

21 Mark Griffiths: A 'components' model of addiction within a biopsychosocial framework. *Journal of Substance Use,* vol. 10., no. 4. (2005). https://doi.org/10.1080/14659890500114359

22 Riccardo Chianella: Addictive digital experiences: the influence of artificial intelligence and more-than-human design. In: *Conference: 14th International Conference of the European Academy of Design, Safe Harbours for Design Research*. Blucher Design Proceedings, Blucher Publishing House, 2021. https://doi.org/10.1080/14659890500114359

23 Nir Eyal: *Hooked: How to build habit-forming products.* New York, Portfolio–Penguin, 2014. 56.

24 Stefano Calicchio: *A tudományos pszichológia története A pszichológia születésétől a neuropszichológiáig és a legaktuálisabb alkalmazási területekig*. Stefano Calicchio, 2021. 87.

25 Eskelinen i. m. 20–21.

26 Eyal i. m. 60.

dalmi dinamikán alapuló stratégiákat támogatnak, amelyek miatt a felhasználók kényszert éreznek arra, hogy aktívan részt vegyenek bennük, a kimaradás miatti szorongó érzést (FOMO – *fear of missing out*) elkerülve.[27] E manipulatív technikák, sötét megoldások, módszerek és eszközök széles skálája, valamint gyors terjedése révén nem meglepő, hogy idővel felkeltette az emberek figyelmét.

A sötét megoldások vizsgálatára fókuszáló kutatások kezdeti szakaszában párhuzamosan volt megfigyelhető az akadémiai, valamint a szakpolitikai aktivitás. A korai kutatások ugyanakkor egymástól elzártan igyekeztek megoldást találni e jelenségek megértésére és szabályozására, kezdve a manipulatív gyakorlatok eseti elemzéseivel, eljutva egészen a nevesített sötét megoldások rendszerbe foglalásáig, különböző taxonómiák mentén. Maga a sötét megoldások fogalma Harry Brignull UX-designertől származik,[28] aki úgy definiálta a sötét megoldásokat, mint „olyan megtévesztő felhasználói felületek, trükkök, amelyek arra késztetik a felhasználót, hogy akkor is vásároljon meg egy terméket vagy iratkozzon fel valamilyen szolgáltatásra, ha ez nem állt éppen kifejezett szándékában." Ez az első definíció erősen leíró jellegű volt, amely nem egy szisztematikus rendszerezésen alapult, csupán a weboldalakon azonosított megoldások példálózásán. Brignull rendszerében először összesen tizenkét manipulatív technikát azonosított[29] köztük a 'sürgetést' (*urge*), vagyis a vásárló gyors döntéshozatali helyzetbe kényszerítését, vagy a 'csalás és átverést' (*bait and switch*), azaz látszólag kedvező árú termékek reklámozását azzal a szándékkal, hogy vásárláskor gyengébb vagy drágább árukkal helyettesítsék őket.[30]

A sötét megoldások kezdeti definíciójának megjelenését követően Gregory Conti és Edward Sobiesk vállalkozott egy újabb taxonómia kidolgozására. Az egyéves adatgyűjtésük eredményeként végül tizenegy rosszindulatú gyakorlatot azonosítottak. Az ő megközelítésükben a sötét megoldás „olyan felhasználói felület, amely szándékosan sérti meg a bevett felhasználóbarát tervezési gyakorlatot, amelynek eredményeképpen a kellemes felhasználói élménnyel ellentétben manipulálja és kihasználja a felhasználót." Az azonosított sötét megoldások egy része egybevágott a korábbi, Brignull által meghatározott gyakorlati példákkal, ugyanakkor olyan új kategóriákat vezettek be, amelyek alkalmasabbnak bizonyultak a különböző technikák csoportosítására.[31] Az első próbálkozásokat követően több megközelítés terjedt el a sötét megoldások azonosítását illetően, mind a korábbi taxonómiákra építve, mind pedig új kategóriákat bevezetve, újabb és újabb aspektusuk szerint vizsgálva e gyakorlatokat.[32] Christoph Bösch és munkatársai elemzésének fókuszában már a felhasználói adatvédelem állt, így a sötét megoldások tanulmányozása során a GDPR 25. cikke szerinti beépített és

27 Andrew K. Przybylski – Kou Murayama – Cody R. Dehaan – Valerie Gladwell: Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, vol. 29., no. 4. (2013).

28 Harry Brignull – Mark Leiser – Cristiana Santos – Kosha Doshi: Deceptive Patterns – User Interfaces Designed to Trick You. *Deceptive.design*. https://www.deceptive.design/

29 Uo.

30 Arunesh Mathur – Jonathan Mayer – Mihir Kshirsagar: "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods". In: *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* New York, Association for Computing Machinery, 2021. https://doi.org/10.1145/3411764.3445610

31 Gregory Conti – Edward Sobiesk: "Malicious interface design: Exploiting the User". In: *Proceedings of the 19th international conference on World wide web (WWW '10).* New York, Association for Computing Machinery, 2010.

32 Gray et. al. (2018) i. m. 7.

alapértelmezett adatvédelem koncepciójához szorosan kapcsolódó 8 féle tervezési technikát gyűjtöttek össze, amelyek olyan rendszereket foglaltak magukban, amelyek az adatgyűjtés és a felhasználók személyes preferenciáinak testre szabására vonatkozó cselekvési lehetőségek korlátozását célozzák, így például a 'rossz alapértelmezett beállításokat' (*bad defaults*), ahol az alapértelmezett beállítások úgy vannak kiválasztva, hogy megkönnyítsék vagy ösztönözzék a személyes adatok megosztását.[33]

Végül, az eddigi legkimerítőbb feltérképezést 2021-ben Arunesh Mathur és munkatársai végezték, akik kísérletet tettek a kutatásukig megjelent, valamennyi sötét megoldásokkal kapcsolatos szakirodalom rendszerezésére, amely során automatizált technikák segítségével mintegy 1818 sötét megoldást azonosítottak, amelyek 7 tágabb kategórián belül 15 típust képviseltek a manipulatív technikák mögöttes befolyását és potenciális negatív hatását hangsúlyozva.[34] A sötét megoldások kognitív torzításai vonatkozásában Mathur és munkatársai tovább elemezték e technikákat,[35] amelynek eredményeképpen 5 közös jellemzőt ismertek fel a sötét megoldásokban, vagyis az aszimmetriát; korlátozást; bújtatást; megtévesztést; és végül az információ elrejtését. Egy későbbi munkájuk során már ezeket a jellemzőket vették alapul a korábbi taxonómia áttekintésére, kiterjesztve a vizsgálatot egy hatodik jellemzővel, az úgynevezett eltérő bánásmóddal.[36] Ugyanakkor ez a csoportosítás sem tért még ki azon sötét megoldások körére, amelyek mögöttes célja a felhasználók további elkötelezettségének növelése lett volna egy adott platform irányába, annak ellenére, hogy az ilyen manipulatív technikák alkalmazása meglehetősen sikeres, mivel a felhasználó viselkedését és cselekedeteit organikusnak érzi, ami alapján úgy tűnhet, mintha a szabad akarata szerint cselekedne.[37]

33 Christoph Bösch – Benjamin Erb – Frank Kargl – Henning Kopp – Stefan Pfattheicher: Tales from the Dark Side: Privacy Dark Strategies and Privacy DarkPatterns. (2016. július) *Proceedings on Privacy Enhancing Technologies*, 2016/4. https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf

34 Arunesh Mathur – Gunes Acar – Michael J. Friedman – Elena Lucherini – Jonathan Mayer – Marshini Chetty – Arvind Narayanan: Dark Patterns at Scale. In: *Proceedings of the ACM on Human-Computer Interaction,* vol. 3, no. CSCW. https://doi.org/10.1145/3359183

35 Uo. 1–32.

36 Mildner et al. (2021) i. m. 3.

37 Pekka Kallioniemi: Facebook's Dark Pattern Design, Public Relations and Internal Work Culture. *Journal of Digital Media & Interaction,* vol. 5., no. 12. (2022).

1. táblázat
Összegzés a korábban említett négy nagyobb, sötét megoldások gyakorlatára vonatkozó taxonómiáról

Brignull 2010[38]	**Conti – Sobiesk 2010**[39]	**Bösch et al. 2016**[40]	**Mathur et al. 2019**[41]
• becsapós kérdések (*trick questions*) • kosárba csempészés *(sneak into basket)* • csótánymotel/ nehéz lemondás *(roach motel)* • ösztönzés egyre több személyes adat megadására *(privacy zuckering)* • megszégyenítés (*confirmshaming)* • álcázott hirdetés (*disguised ads)* • árösszehasonlítás megakadályozása *(price comparison prevention)* • elirányítás *(misdirection*) • rejtett költségek *(hidden costs)* • csalás és átverés *(bait and switch)* • kényszerű folytonosság *(forced continuity)* • barátok behívása (*friend spam*)	• kényszerítés (*coercion*) • zavarás (*distraction*) • többletcselekvés (*forced work*) • manipulált navigáció (*manipulating navigation*) • funkcionalitás korlátozása (*restricting functionality)* • trükk (*trick*) • zavarás • (*confusion*) • hibák kihasználása (*exploiting errors*) • megszakítás (*interruption*) • homályosítás (*obfuscation*) • sokkolás (*shock*)	• ösztönzés egyre több személyes adat megadására *(privacy zuckering)* • rejtett jogi kikötések (*hidden legalese stipulations)* • árnyékprofilok *(shadow user profiles)* • rossz alapértelmezések *(bad defaults)* • halhatatlan fiók *(immortal accounts)* • információfejés *(information milking)* • kényszerített regisztráció *(forced registration)* • címjegyzéklékelés *(address book leeching)*	• visszaszámláló *(countdown timers)* • időbeni korlátozást jelző üzenetek *(limited-time messages)* • magas keresletet sejtető üzenetek *(high-demand messages)* • aktivitást jelző értesítések *(activity notifications)* • megszégyenítés (*confirmshaming)* • ismeretlen eredetű ajánlások *(testimonials of uncertain origins)* • nehéz lemondás (*hard to cancel*) • vizuális zavarás *(visual interference)* • alacsony készletet jelző üzenetek (*low-stock messages)* • rejtett feliratkozás *(hidden subscriptions)* • vásárlásra késztetés *(pressured selling)* • kényszerített feliratkozás *(forced enrolment)*

Saját szerkesztés

A legújabb kutatások viszont különbséget tesznek már a manipulatív felhasználói felületek első és második generációja között. Az első generációs sötét megoldásokat alkalmazó felületek a fent említett taxonómiákban azonosított manipulatív technikákon alapulnak, amelyek közvetlenül a felhasználókat célozzák meg, így ezáltal viszonylag könnyen fel is ismerhetők. A második generációs sötét megoldások azonban már nagyobb kihívást jelentenek, ugyanis bár az első generációs gyakorlatokon alapulnak, azoknál sokkal fejlettebbek. Ezek a technikák gyakran teljes egészében rejtve tudnak maradni a felhasználók elől azáltal, hogy az egyes platformok rendszerarchitektúrájába építik be őket, így csupán a weboldal fejlesztőinek és üzemeltetőinek válnak észrevehetővé.[42] A második generációs sötét megoldások jellemzően

38 Brignull i. m. Deceptive patterns.
39 Conti et al. i. m. 271–280.
40 Bösch et al. i. m. 237–254.
41 Mathur et al. i. m. 12.
42 Agnieszka Kitkowska – Johan Högberg – Erik Wästlund: Barriers to a well-functioning digital market: Exploring dark patterns and how to overcome them. In: *Proceedings of the 55th Hawaii International Conference on System Sciences, Human-centricity in a Sustainable Digital Economy.* Manoa, University of Hawai'i at Manoa, 2022. https://scholarspace.manoa.hawaii.edu/items/24a63982-4927-488a-b5c3-c9dfca54fb39

a böngészési előzmények és az online viselkedés kiterjedt nyomon követése révén gyűjtött felhasználói adatokon alapulnak, kifejezetten az egyéni sebezhetőségek vagy preferenciák kihasználására építve. E megoldások mögött sok esetben algoritmusalapú rendszerek állnak, amelyek kifinomult módon, gyakran kifejezett beleegyezés vagy tájékoztatás nélkül irányítják a felhasználókat bizonyos viselkedésmódok vagy eredmények felé.[43]

A fenti fogalommeghatározások, illetve kategorizálások alapján jól látható, hogy a sötét megoldások azonosításának empirikus kutatás eredményének kell lennie. [44] A rendszerezések során ugyanis világossá vált, hogy a sötét megoldások különböző eseteinek azonosításához elengedhetetlen egy adott technika egyedi megjelenésének felismerése, valamint a különböző technikák mögötti közös jellemzők feltárása, lehetővé téve ezzel a fogalmak megfelelő elvonatkoztatását az adott kontextusától.[45] Az eltérő taxonómiák és vizsgálatok alapján az is jól látható, hogy egy megfelelő szabályozási rezsim kialakításának elsődleges kiindulási feltétele egy egységes fogalomrendszer kidolgozása kell, hogy legyen, amely egyszerre képes alapot nyújtani a már azonosított fajták összefogására, ám kellő absztraktsággal is rendelkezik ahhoz, hogy a sötét megoldások folyamatos fejlődésére és újabb és újabb fajtáinak megjelenésére is reagálni tudjon.

3. A sötét megoldások alkalmazásának megítélése az Európai Unió jogrendszerében

Figyelembe véve, hogy magának a sötét megoldásoknak a fogalma és a szabályozási igénye is a jogon kívülről érkezett, sokáig nem is volt azonosítható konkrét szabályozási rendszere a jogon belül. A jelenlegi állapot szerint szabályozási pluralizmus jellemzi a sötét megoldások alkalmazásának megítélését, amelynek köszönhetően a szankcionálásuk is több jogterülethez köthető. Az alkalmazandó szabályok főként az adatvédelem, a fogyasztóvédelem, valamint az újonnan kialakuló platformszabályozás rendelkezéseit jelentik, azonban annak eldöntése, hogy az adott sötét megoldás tekintetében mely szabályok az elsődlegesen alkalmazandók, nagyban függ az eset körülményeitől, és a felhasználókra gyakorolt hatásuktól is.

Jelen tanulmány szabályozási fókusza a közösségi médiában alkalmazott sötét megoldások esetében hangsúlyos Európai Uniós rendeletekre és irányelvekre összpontosít, így különösen a tisztességtelen kereskedelmi gyakorlatokról szóló irányelvre (UCPD),[46] a fogyasztói jogokról szóló irányelvre (CRD),[47] az audiovizuális médiaszolgáltatásokról szóló irányelvre

43 BEUC The European Consumer Organization: *'Dark patterns' and the EU consumer law acquis, Recommendations for better enforcement and reform.* Brüsszel, BEUC, 2022. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf

44 Mildner (2021) et al. i. m. 2.

45 Európai Bizottság (2022) i. m. 27.

46 2005/29/EK irányelv a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról („Irányelv a tisztességtelen kereskedelmi gyakorlatokról"), HL L 149, 2005. 06. 11., 22–39. o. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32005L0029

47 2011/83/EU irányelv a fogyasztók jogairól, a 93/13/EGK tanácsi irányelv és az 1999/44/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 85/577/EGK tanácsi irányelv és a 97/7/EK európai parlamenti és tanácsi irányelv hatályon kívül helyezéséről, HL L 304., 2011. 11. 22., 64–88. o. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32011L0083

(AVMSD),[48] az általános adatvédelmi rendeletre (GDPR),[49] az elektronikus hírközlési adatvédelmi irányelvre (ePrivacy-irányelv),[50] a digitális szolgáltatásokról szóló jogszabályra[51] a digitális piacokról szóló jogszabályra (DMA),[52] az adatrendeletre,[53] valamint a mesterséges intelligenciáról szóló rendeletre (MI-rendelet).[54]

3.1. Adatvédelmi szabályrendszer

A sötét megoldásokat érintő követelmények egy jelentős részét az adatvédelmi rendelkezések töltik meg tartalommal, így bár a GDPR és az ePrivacy-irányelv nem említik kifejezetten a sötét megoldások fogalmát, mégis alapvető jogi keretet nyújtanak alkalmazásuk szabályozása során, különösen, amikor a GDPR szerinti személyes adatok kezelésének, vagy az ePrivacy-irányelv szerinti sütik és marketingkommunikációk alkalmazásának alapja az érintettek, vagyis a felhasználók hozzájárulása. E két jogszabállyal ellentétben a 2024. január 11-én hatályba lépett[55] adatrendelet már kifejezetten említi is a sötét megoldások fogalmát mint a fogyasztók megtévesztésére irányuló manipulatív technikát. A következőkben e jogszabályok ismertetése következik.

3.1.1. Az elektronikus hírközlési adatvédelmi irányelv

Az ePrivacy-irányelv alapvetően a felhasználók magánélethez való jogának és az elektronikus hírközlés bizalmas jellegének védelmére vonatkozó szabályokat állapít meg a GDPR

48 2018/1808/EU irányelv 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, HL L 303, 2018. 11. 28., 69–92. o. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32018L1808&qid=1733473027598

49 2016/679/EU rendelet 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. o. https://eur-lex.europa.eu/legal-content/HU/TXT/ELI/?eliuri=eli%3Areg%3A2016%3A679%3Aoj

50 2002/58/EK irányelv az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), HL L 201., 2002. 7. 31., 37–47. o. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32002L0058

51 2022/2065/EU rendelet a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet), HL L 277., 2022. 10. 27., 1–102. o. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022R2065

52 2022/1925/EU rendelet a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály), HL L 265., 2022. 10. 12., 1–66. o. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri= CELEX%3A32022R1925

53 2023/2854/EU rendelet a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (Adatrendelet), HL L, 2023/2854, 2023. 12. 22., https://eur-lex.europa.eu/legal-content/HU/TXT/?uri= CELEX:32023R2854

54 2024/1689/EU rendelet a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (A mesterséges intelligenciáról szóló rendelet), HL L, 2024/1689, 2024. 7. 12., https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1689

55 Adatrendelet 50. cikk.

rendelkezéseire és fogalmi rendszerére támaszkodva.[56] Az elektronikus hírközlő hálózatok felhasználóinak végberendezései és az ilyen berendezéseken tárolt információk a felhasználók magánszférájának részét képezik, és így a magánélet védelmét élvezik.[57]

Tekintettel arra, hogy a felhasználók eszközein sütiket tároló vagy azokhoz hozzáférő keresőmotor-szolgáltatások az ePrivacy-irányelv 5. cikk (3) bekezdésének kiterjesztett tárgyi hatálya alá tartoznak,[58] a sötét megoldások szabályozása során e bekezdés különös relevanciával bír. A közlések titkossága ugyanis megköveteli, hogy az előfizetők vagy felhasználók egyértelmű és teljeskörű tájékoztatását követő hozzájárulás megadása esetén lehessen csak sütiket, illetve hasonló nyomon követő eszközöket elhelyezni az előfizetői, valamint felhasználói végberendezéseken. Ez alól a követelmény alól az ePrivacy-irányelv csupán két kivételt enged, egyrészt az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás megkönnyítése, másrészt pedig amely az előfizető vagy felhasználó által kifejezetten kért, információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges.[59]

Ahogyan az irányelv említett bekezdéséből is jól kitűnik, a sütik elhelyezése, pontosabban az azokhoz szükséges hozzájárulások megszerzése során figyelhető meg a jogsértő sötét megoldások alkalmazása a gyakorlatban. Az elterjedt megoldások között található például az a technika, amikor megtévesztően tüntetik fel a hozzájárulás megadására, illetve elutasítására szolgáló ikonokat, vagy amikor a hozzájárulás adásának elutasítása csak a sütibanner egy második rétegén érhető el.[60] Ez utóbbi megoldás vezetett a francia adatvédelmi hatóság eljárásában 2021-ben egy 60 millió eurós bírság kiszabásához is a Meta Platforms Inc. Facebook közösségimédia-oldala ellen is, amiért megsértette az ePrivacy-irányelv 5. cikk (3) bekezdés francia jogba átültető rendelkezését. A bírság kiszabása mellett a hatóság továbbá arra is utasította a vállalatot, hogy pontosan olyan egyszerű lehetőséget biztosítson a sütik elutasításához is, mint amilyet az elfogadásukhoz garantál. [61]

Az elektronikus hírközlési adatvédelmi irányelv technológiai fejlődéshez való hozzáigazítása és a GDPR-ral való jobb összehangolása érdekében a Bizottság 2017-ben elfogadta

56 ePrivacy-irányelv 2. cikk *f)* pont, GDPR 94. cikk (1)–(2) bek.

57 Európai Bizottság (2022) i. m. 79., Az Európai Unió Alapjogi Chartája 7. cikk: a magán- és a családi élet tiszteletben tartása.

58 EDPB 5/2019. számú vélemény az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében, 2019. március 12. https://www.naih.hu/files/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_hu.pdf; 1/2008. számú vélemény a keresőmotorokkal kapcsolatos adatvédelmi kérdésekről (WP148), 4.1.3. szakasz, 12. o. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf

59 ePrivacy-irányelv 5. cikk (3) bek.

60 Mark Leiser – Christina Santos: Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface. *European Journal of Law and Technology,* vol. 15., no. 1. (2024) 9. https://ejlt.org/index.php/ejlt/article/download/990/1084/4299

61 Európai Bizottság (2022) i. m. 79., CNIL: Deliberation No. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular «cookies and other tracers») and repealing Deliberation No. 2019-093 of 4 July 2019. 8. https://kutvonen.net/family/cnil-cookies-and-trackers-2020.pdf

az elektronikus hírközlési adatvédelmi rendeletről szóló javaslatot,[62] amelyről azonban még jelenleg is csak tárgyalásokat folytat az Európai Parlamenttel és a Tanáccsal.[63]

3.1.2. Általános adatvédelmi rendelet

A GDPR alapvető szabályokat állapít meg a személyes adatok és a magánélet védelmének biztosítása érdekében[64] azáltal, hogy hatálya kiterjed a személyes adatoknak az EU-ban és az EU-n kívül letelepedett adatkezelők és adatfeldolgozók által végzett minden olyan adatkezelési tevékenységre, amelyek az EU-ban élő érintetteknek szolgáltatásokat vagy árukat kínálnak, vagy az érintettek EU területén belül tanúsított viselkedésének megfigyeléséhez kapcsolódnak.[65]

A sötét megoldások szabályozása tekintetében a GDPR személyes adatok kezelésének elveire,[66] illetve jogszerű alapjaira (főként a hozzájárulásra)[67] vonatkozó rendelkezései[68] bírnak kiemelt jelentőséggel, ám az adatkezelőket érintő tájékoztatási kötelezettségre,[69] az érintetti jogok gyakorlására,[70] valamint a beépített és alapértelmezett adatvédelemre vonatkozó szabályok[71] is hangsúlyosak, ugyanis a GDPR rendelkezései minden olyan kereskedelmi gyakorlatra alkalmazandók, amelyek a személyes adatok kezelésével járnak, így a felhasználók befolyásolására szolgáló sötét megoldásokra is irányadók bizonyos esetekben.

A közösségimédia-platformokon elterjedt sötét megoldások többsége megsérti a GDPR 5. cikke szerinti adatkezelési elvek előírásait. A jogszerűség, a tisztességes eljárás és az átláthatóság követelménye[72] alapján ugyanis a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. A GDPR 12. cikkének (1) bekezdésével együtt az adatkezelésről szóló tájékoztatásnak tömör, átlátható, érthető és könnyen hozzáférhető formában, világos és közérthető nyelven kell történnie. Az ezen elveket sértő leggyakoribb sötét megoldások lehetnek tartalom alapján, de akár még a megjelenési felület alapján is megtévesztők, mint többek között az 'adatvédelmi labirintus' (*privacy maze*), ahol a felhasználónak túl sok oldalon kell végignavigálnia, a túl sok lehetőség, amikor a felhasználónak túl sok lehetséges beállítás közül kell választania, különösen úgy, hogy nem áll

62 Javaslat az Európai Parlament és a Tanács Rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), COM(2017) 10 final, 2017/0003(COD). https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52017PC0010

63 Európai Bizottság (2022) i. m. 80.

64 Az Európai Unió Alapjogi Chartája (Charta) 8. cikk (1) bek. és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikk (1) bek. alapján.

65 GDPR 3. cikk (1)–(2) bek.

66 GDPR 5. cikk.

67 GDPR 4. cikk 11. pont, 7. cikk (1) –(4) bek.

68 GDPR 6. cikk.

69 GDPR 12–14 cikkei.

70 GDPR 15–21. cikkei, de különösen a személyes adatok törléséhez való jog, valamint a tiltakozási jog.

71 GDPR 25. cikk.

72 GDPR 5. cikk (1) bek. *a)* pont.

rendelkezésre elegendő információ; vagy az olyan felhasználói felület kialakítása, amely elrejti az adatvédelemmel kapcsolatos információkat (sötétben hagyják a felhasználót).[73]

A tisztességesség és átláthatóság elve mellett szintén gyakori a célhoz kötöttség elvének megsértése is a sötét megoldások alkalmazása során. A célhoz kötöttség elve alapján a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, amelyek kezelése nem történhet az eredeti célokkal össze nem egyeztethető módon.[74] Ennek megfelelően célhoz kötöttség elvébe ütköznek azok a gyakorlatok, amelyek a szükségesnél több személyes adat megadására kényszerítik a felhasználót azáltal, hogy tömeges és ismétlődő kérésekkel (*continuous prompting*) terhelik a felhasználót a hozzájárulás, vagy az adatok új adatkezelési célhoz történő megadása miatt. Ez különösen megfigyelhető a regisztrációs szakaszban, de a felhasználói fiók életciklusának bármely későbbi szakaszában is.[75]

Ahogy a GDPR 5. cikk (1) bekezdésének *c)* pontja rendelkezik, a személyes adatok kezelésének az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lennie, amellett, hogy a szükségesre kell korlátozódnia. Ez a szabály az adattakarékosság elve, amely gyakran sérül az olyan sötét megoldások alkalmazása során, amelyek azt a célt szolgálják, hogy a felhasználóktól a szükségesnél több információt csaljanak ki, mint például a 'biztonsági zsarolás' esetén, ahol a telefonszámot szükségtelenül kérik a felhasználói fiók biztonsága és hitelesítése céljából, vagy a felhasználói élmény javítására vonatkozó érv alkalmazása.[76]

Ezeket az elveket tovább erősíti a GDPR 25. cikke, amely kimondja, hogy az adatkezelőnek olyan megfelelő technikai és szervezési intézkedéseket kell végrehajtania, amelyek célja az adatvédelmi elvek megvalósítása, valamint a GDPR követelményeinek teljesítése és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelési folyamatokba. E cikk rendelkezései szerint az alapértelmezés kizárólag olyan személyes adatok kezelésére vonatkozhat, amelyek a konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség nem csak a gyűjtött személyes adatok mennyiségére, de a kezelésük mértékére, tárolásuk időtartamára, valamint a hozzáférhetőségükre is egyaránt vonatkozik. Ennek megfelelően a személyes adatok alapértelmezés szerint a felhasználók beavatkozása nélkül nem válhatnak meghatározatlan számú személy számára hozzáférhetővé.[77] Sokáig az 'előre bepipált jelölőnégyzetek' (*pre-ticked checkboxes, preselection*)[78] bizonyultak e cikk, valamint a hozzájárulásra vonatkozó rendelkezések tekintetében a legelterjedtebb gyakorlatnak, azonban az elmúlt években csökkent a számuk a bírósági és hatósági eljárások okán. Ehelyett a sötét megoldás helyett inkább az alapértelmezett hozzájárulási lehetőségek alkalmazásával kínálnak a felhasználóknak például célzott reklámokat. Ezeket a gyakorlatokat 'rossz alapértelmezett

73 Európai Bizottság (2022) i. m. 76.

74 GDPR 5. cikk (1) bek. *b)* pont.

75 Európai Bizottság (2022) i. m.; EDPB: Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 2023. február 14. https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

76 CNIL: Shaping Choices in the Digital World From dark patterns to data protection: the influence of ux/ui design on user empowerment. IP Reports Innovation And Foresight N°06, 2019. https://www.cnil.fr/sites/cnil/files/2023-06/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf; Sorin Berbece: 'Let there be light!' Dark patterns under the lens of the EU legal framework [Szakdolgozat]. Leuven, KU Leuven, 2019. 26.

77 GDPR 25. cikk (1)–(2) bek.

78 GDPR (32) preambulumbekezdés.

beállításoknak' (*bad defaults*) nevezik, mivel a felhasználókat a kívántnál több személyes adat megosztására kényszerítik.[79]

2022-ben az EDPB is felfigyelt a sötét megoldások alkalmazása, valamint elterjedése által jelentett kockázatokra, így iránymutatásokat fogadott el a közösségimédia-platformok felületeinek sötét megoldásaival kapcsolatban.[80] Az iránymutatások gyakorlati ajánlásokat nyújtanak mind a közösségimédia-platformok tervezői, mind a felhasználói számára arra vonatkozóan, hogy miként értékelhetők és kerülhetők el a közösségimédia-felületek sötét megoldásai, amelyek sértik a GDPR követelményeit.[81]

3.1.3. Adatrendelet

Az EU adatrendelete a legfrissebb az adatvédelem területén a maga 2024. január 11-i hatályba lépésével, valamint 2025. szeptember 12-i alkalmazandóságával. Az ePrivacy-irányelvhez hasonlóan az adatrendelet a GDPR rendelkezéseire épít,[82] valamint tovább konkretizálja az adatmegosztásra és az adathordozhatóságra vonatkozó szabályokat. Az adatrendelet alapvetően a termékek vagy kapcsolódó szolgáltatás használatából származó, illetve annak során keletkezett adatok megosztását szabályozza a felhasználók, az adattulajdonosok és harmadik felek között, azonban a rendelet kifejezetten az internetre csatlakoztatott eszközök (*Internet of Things* – IoT) által generált adatokra irányul.[83]

Az adattakarékosság elvével összhangban az adatrendelet alapján harmadik felek csak a felhasználó által kért szolgáltatás nyújtásához szükséges információkhoz férhetnek hozzá. A harmadik fél hozzáférése után az adatokat csak a felhasználóval megállapodott célokra, és az adatbirtokos beavatkozása nélkül kezelheti. Fontos követelmény továbbá, hogy a harmadik fél adatokhoz való hozzáférésének megtagadása vagy megszüntetése ugyanolyan könnyű kell, hogy legyen, mint a hozzáférés engedélyezése volt.[84] A rendelet 4. cikk (4) bekezdése kimondja, hogy a felhasználó választási lehetőségeit, illetve jogainak gyakorlását nem lehet indokolatlanul nehezíteni azáltal, hogy kényszerítik, félrevezetik, manipulálják a felhasználót, aláásva és csorbítva ezzel a felhasználó autonómiát és döntéshozatalt. Ezzel összefüggésben, az adatrendelet az első az EU-s adatvédelmi jogszabályok közül, amely kifejezetten nevesíti a sötét megoldások fogalmát, mint „olyan tervezési technikák, amelyek a fogyasztókat számukra hátrányos következményekkel járó döntések meghozatalára késztetik, vagy arra megtévesztő módon ráveszik."[85] A preambulumbekezdés alapján ezek a manipulatív technikák alkalmasak a felhasználók döntéshozatalának befolyásolására, aminek eredményeképpen olyan nemkívánatos magatartások tanúsítására ösztönzik őket, amelyek az adatközlési

79 OECD: *Dark commercial patterns. OECD Digital Economy Papers, No. 336.* Paris, OECD Publishing, 2022. https://doi.org/10.1787/44f5e846-en; Leiser–Santos i. m. 6.

80 EDPB: Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, 2023. február 14. https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

81 Európai Bizottság (2022) i. m. 75.

82 Adatrendelet 1. cikk (5) bek., illetve ld. (2) cikk szerinti fogalommeghatározások.

83 Adatrendelet 1. cikk.

84 Adatrendelet (38) preamb.

85 Uo. 38.

műveletekkel kapcsolatos döntések meghozatalára hatással vannak, választási szabadságukat és döntési autonómiájukat csorbítva.

Az adatrendelet is hangsúlyozza ugyanakkor, hogy nem minden kereskedelmi gyakorlat minősül automatikusan sötét megoldásnak, azonban ehhez teljesíteni kell a releváns uniós jog szerinti kötelezettségeket.[86] Gyakori sötét megoldás e rendelet vonatkozásában például, amikor harmadik felek olyan választási lehetőségeket tárnak a felhasználók elé, amelyek az adatkezelés céljára vagy a megállapodás szerinti célhoz már nem szükségesek.[87]

4. Fogyasztóvédelmi keretek

A sötét megoldások szabályozási kísérletei a fogyasztóvédelmi jog területén jelentek meg először, mint a kereskedelmi gyakorlatok tiszteségtelen fajtái, amelyek befolyásolják a fogyasztók autonóm üzleti döntéseit. E terület rendelkezései a kereskedelmi gyakorlatok tiszteségtelen megoldásainak szabályozására vonatkozó előírásokkal kívánnak fellépni a sötét megoldások alkalmazásának elterjedése ellen.

4.1. A tisztességtelen kereskedelmi gyakorlatokról szóló irányelv

Az uniós fogyasztóvédelmi jogban a sötét megoldások vizsgálatának kiindulópontja a tisztességtelen kereskedelmi gyakorlatokról szóló irányelv, amely kiemelt jelentőséggel bír a tisztességtelen kereskedelmi gyakorlatok szabályozásában. Bár az UCPD nem említi kifejezetten a sötét megoldások fogalmát, az Európai Bizottság értelmezése alapján széles körű és elvi alapú rendelkezései alkalmasak a sötét megoldást alkalmazó gyakorlatok tisztességtelenségének kiküszöbölésére,[88] már csak az UCPD 2. cikkének *d)* pontjában szereplő kereskedelmi gyakorlat különösen tág megfogalmazásának köszönhetően is. E rendelkezés értelmében kereskedelmi gyakorlatnak minősül ugyanis a kereskedő által kifejtett olyan tevékenység, mulasztás, magatartási forma vagy megjelenítési mód, beleértve a kereskedelmi kommunikációt is (így a reklámot és a marketinget), amely közvetlen kapcsolatban áll valamely terméknek a fogyasztó részére történő eladásösztönzésével, értékesítésével vagy szolgáltatásával.[89] Az irányelv rendelkezései így nemcsak a termékek tekintetében, hanem a szolgáltatások vonatkozásában is jelentőséggel bírnak. Az irányelv széles alkalmazási köre a vállalkozások és a fogyasztók közötti ügyletek egészére kiterjed, legyen az offline vagy akár online. Az UCPD technológiasemleges, így az üzleti vállalkozások és fogyasztók közötti kereskedelmi gyakorlat megvalósításához használt csatornától, médiumtól vagy eszköztől függetlenül alkalmazandó. Ebből kifolyólag az online közvetítőkre is vonatkozik, beleértve a közösségimédia-platformokat is. Az irányelv az olyan gyakorlatokra és termékekre alkalmazandó, mint az algoritmusok, az automatizált döntéshozatal és az MI alkalmazását magába foglaló technológiák.

86 Különösen a 98/6/EK (24) preambulumbekezdés és a 2000/31/EK (25) preambulumbekezdés európai parlamenti és tanácsi irányelvben, valamint a 2005/29/EK és a 2011/83/EU irányelvben megállapított követelményeket.

87 Brenncke i. m. 11.

88 Brenncke i. m. 8.

89 UCPD 2. cikk *d)* pont.

Szabályozás alá esnek ezáltal a kereskedők reklámozás során a fogyasztókkal szemben alkalmazott nyomonkövetési és célzási technológiái, valamint az algoritmikus személyre szabás.[90]

Az olyan közösségimédia-platformok, mint a Facebook, a YouTube, az Instagram és a TikTok lehetővé teszik a felhasználók számára, hogy profiljuk segítségével kommunikáljanak, így információkat és tartalmakat osszanak meg egymással. Ezek a kommunikációk ugyanakkor egyre gyakrabban tartalmaznak olyan kereskedelmi gyakorlatokat, illetve sötét megoldásokat, amelyek az irányelv hatálya alá tartoznak. A sötét megoldások alkalmazása leggyakrabban az UCPD 5–9. cikkeiben foglalt tilalmakba ütköznek. Az UCPD 5. cikkében foglalt általános klauzula a tisztességtelen kereskedelmi gyakorlatokra vonatkozik, amelyek sértik a kereskedő szakmai gondosságát. A tisztességtelen kereskedelmi gyakorlatok közé tartoznak továbbá a megtévesztő kereskedelmi gyakorlatok, ideértve a megtévesztő tevékenységeket,[91] a megtévesztő mulasztásokat,[92] valamint a zaklatás, kényszerítés és nem megengedett befolyásolás alkalmazásával jellemezhető agresszív gyakorlatokat.[93] Ahhoz azonban, hogy egy gyakorlat az UCPD 5–9. cikke értelmében tisztességtelennek minősüljön, a fogyasztót olyan ügyleti döntésre kell késztetnie vagy valószínűsíthetően késztetnie, amelyet egyébként nem hozott volna meg. Az ügyleti döntés meghozatala nemcsak a termék megvásárlására vagy meg nem vásárlására vonatkozó döntést foglalja magában, hanem az ehhez a döntéshez közvetlenül kapcsolódó döntést is. Ilyen megoldások többek között például a közösségimédia-platform vagy harmadik fél kereskedők általi rejtett reklámok (beleértve a megtévesztő influencermarketinget is), a tisztességtelen általános szerződési feltételek; a közösségi médiaszolgáltatások 'ingyenességének' állítása, miközben a hozzáférésért cserébe nagy mennyiségű személyes adatot kezelő hirdetési modellre támaszkodnak.[94]

4.2. A fogyasztói jogokról szóló irányelv

A CRD a fogyasztók és a kereskedők között létrejött valamennyi szerződésre vonatkozik, kivéve a kifejezetten kizárt szerződéseket (pl. a pénzügyi szolgáltatásokat). Az irányelv célja, hogy összehangolja és harmonizálja a nemzeti fogyasztóvédelmi szabályokat a fogyasztóknak a szerződéskötés előtt nyújtandó tájékoztatásáról, valamint a fogyasztók bizonyos feltételek mellett történő elállási jogáról, függetlenül attól, hogy az EU-n belül hol történik a vásárlás.[95] Az olyan sötét megoldások által vezérelt gyakorlatok, mint például a félrevezető felhasználói felület vagy a zavaros web- vagy alkalmazáskialakítás a gyakorlatban a CRD-ben meghatározott követelmények megkerülését jelenthetik.[96] Az ilyen kijátszó gyakorlatok megakadályozása érdekében a bíróságok és a hatóságok a sötét megoldások használatát a CRD céljai megsértésének

90 Commission Notice Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021/C 526/01), 93.

91 UCPD 6. cikk.

92 UCPD 7. cikk.

93 UCPD 8. és 9. cikkei.

94 Commission Notice Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021/C 526/01), 97. o.

95 Európai Bizottság, 2022, i. m. 73.

96 Commission Notice – Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (Text with EEA relevance) 2021/C 525/01 (OJ C, C/525, 29.12.2021, p. 1, CELEX: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021XC1229(04))

tekinthetik, amennyiben azok aláássák a CRD rendelkezéseinek hatékonyságát.[97] A CRD-t az (EU) 2019/2161 irányelv módosította,[98] kiterjesztve annak hatályát azokra a szerződésekre is, amelyekben a kereskedő digitális tartalmat szolgáltat, a fogyasztó pedig személyes adatokat szolgáltat a kereskedőnek. Ezen túlmenően a 16a. cikk (1) bekezdésének *a)* pontja kötelezi az online piactereket arra, hogy általános tájékoztatást nyújtsanak a fogyasztóknak az ajánlatok rangsorolását a fogyasztó keresési lekérdezésének eredményeként meghatározó főbb paraméterekről, valamint e paraméterek relatív fontosságáról más paraméterekkel szemben.[99] Ez az új rendelkezés szorosan tükrözi a DSA rendelet 25. cikkének szövegét.[100]

5. A platformszabályozás térnyerése

A digitális platformok folyamatosan fejlődő környezetében az Európai Unió a tisztességes, átlátható és etikus gyakorlatok biztosítására irányuló szabályozási erőfeszítések élvonalában áll. E törekvés középpontjában a platformok hatékony szabályozásának szükségessége áll, amelyet a platformok által a modern élet különböző aspektusaira gyakorolt mélyreható befolyás tesz szükségessé, a kereskedelemtől a kommunikációig. E szabályozási keret központi elemei az olyan kulcsfontosságú jogalkotási kezdeményezések, mint az audiovizuális médiaszolgáltatásokról szóló irányelv, a digitális szolgáltatásokról szóló törvény, a digitális piacokról szóló törvény és a mesterséges intelligenciáról szóló rendelet. Ezek a jogalkotási eszközök sarokkövekként szolgálnak számos kihívás kezelésében, beleértve a sötét megoldások alkalmazásának problémáját is. E szabályozási keretek vonatkozó rendelkezéseinek vizsgálatával betekintést nyerhetünk abba, hogy az EU mennyire elkötelezett egy olyan digitális környezet előmozdítása mellett, amely a felhasználói jogokat, a fogyasztóvédelmet és a piaci tisztességességet helyezi előtérbe, miközben az innovációt és a versenyt is elősegíti.

5.1. Az audiovizuális médiaszolgáltatásokról szóló irányelv

Az AVMSD eredetileg az audiovizuális médiaszolgáltatásokat, így a hagyományos televíziós adásokat és a lekérhető szolgáltatásokat szabályozta. E szolgáltatások vonatkozásában olyan audiovizuális kereskedelmi közleményekre is kiterjed az irányelv hatálya, amelyek közvetlenül vagy közvetve áruk vagy szolgáltatások népszerűsítését szolgálják a fogyasztók számára (pl. reklám, szponzoráció, vagy termékelhelyezés). Az AVMSD 5. cikke általános tájékoztatási követelményeket állapít meg a szolgáltatók számára, míg a 9. cikk olyan követelményeket határoz meg, amelyeknek minden audiovizuális kereskedelmi közleménynek meg kell felelnie. A 10. és 11. cikk tartalmazza azokat a feltételeket, amelyeket az audiovizuális médiaszolgáltatásokban történő

97 As proposed by BEUC (2022) "Dark patterns" and the EU Consumer Law acquis. Recommendations for better enforcement and reform. Available at: beuc-x-2022-013_dark_patters_paper.pdf

98 2019/2161/EU irányelv a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról, HL L 328, 2019. 12. 18., 7–28. o. https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A32019L2161

99 Európai Bizottság (2022) i. m. 73–74.

100 DSA (67) preambulumbekezdés és CRD (61) preamb ulumbekezdés.

szponzorálásnak és termékelhelyezésnek be kell tartania. Az AVMSD 2018-as felülvizsgálata során a hatályát kiterjesztették a videómegosztó szolgáltatásokra is, mint például a YouTubera, TikTokra, vagy éppen a Facebook videókat megjelenítő oldalára ('*Facebook watch*'). Ennek megfelelően az AVMSD 9. cikk (1) bekezdésében meghatározott követelményeknek ezen platformoknak a saját maguk által közölt kereskedelmi közlemények tekintetében is meg kell felelniük. Az AVMSD ezzel összhangban előírja, hogy a reklámnak és a kereskedelmi közleménynek könnyen felismerhetőnek és a szerkesztői tartalomtól megkülönböztethetőnek kell lennie, míg tiltja a burkolt kereskedelmi közleményeket és a szubliminális technikákat.[101] Ezek a rendelkezések a videómegosztó szolgáltatásokon és a közösségi médiában megjelenő álcázott hirdetések, valamint a célzott reklámok közzététele szempontjából relevánsak.[102]

5.2. A digitális szolgáltatásokról szóló rendelet

A DSA célja a belső piacon jelenlévő közvetítő szolgáltatásokra alkalmazandó szabályok teljes harmonizációja, annak érdekében, hogy a jogellenes tartalmak elleni fellépésével egy biztonságos, kiszámítható, valamint megbízható online környezetet tudjon biztosítani,[103] amely elengedhetetlen az olyan alapvető jogok gyakorlásához, mint a véleménynyilvánítás és a tájékozódás szabadsága, a vállalkozás szabadsága, vagy éppen a megkülönböztetésmentességhez való jog.[104] A rendelet 'online (óriás)platform'-fogalma a Bizottság értékelése alapján kiterjedhet a közösségimédia-platformokra is, mint ahogy azt a Facebook, LinkedIn, Instagram, TikTok, YouTube esetében is látni.

A DSA az Adatrendelet mellett már kifejezetten nevesíti a sötét megoldások fogalmát, ugyanakkor némileg eltérően. A DSA alapján sötét megoldásnak minősülnek az online platformok online interfészein megjelenő olyan gyakorlatok, amelyek „akár szándékosan, akár ténylegesen jelentősen torzítják vagy korlátozzák a szolgáltatás igénybe vevőinek azon képességét, hogy önálló és megalapozott döntéseket hozzanak."[105]A rendelet hangsúlyozza, hogy a sötét megoldások alkalmasak negatív következmények kiváltására azáltal, hogy a felhasználókat nem kívánt magatartások tanúsítására, illetve döntések meghozatalára ösztönözik egy online interfész egészének vagy részének szerkezete, kialakítása vagy funkciói révén. Ezzel összefüggésben a DSA 25. cikke tilalmat állít többek között a visszaélésszerű kialakításokkal szemben, mint a felhasználókat megtévesztő vagy manipuláló, szabad döntésüket befolyásoló olyan vizuális, auditív vagy egyéb elemek alkalmazása az online interfészeken, amelyek a felhasználó figyelmét a szolgáltatónak előnyös döntésre terelik a felhasználó hátrányára.[106] A DSA és az Adatrendelet meghatározásának egyik jelentős különbsége, hogy az autonómia megsértése, amely a DSA-ban szereplő sötét megoldások meghatározására jellemző, nem talál párhuzamot az Adatrendeletben szereplő sötét megoldások meghatározásában, habár mindkét jogszabály preambulumbekezdései kifejezetten védik. [107]

A DSA 25. cikk (3) bekezdése, valamint a (67) preambulumbekezdése felhívja a figyelmet a sötét megoldások néhány fajtájára, így többek között a felhasználói döntéshozatal során az egyes választási

101 AVMSD 9. cikk (1) bek. *a)* és *b)* pont.
102 Európai Bizottság (2022) i. m. 80.
103 DSA (9) preambulumbekezdés, DSA 1. cikk (1) bek.
104 DSA (3) preambulumbekezdés., Európai Unió Alapjogi Chartája 11.cikk, 16. cikk, 21. cikk.
105 DSA (67) preambulumbekezdés.
106 DSA 25. cikk, (67) preambulumbekezdés.
107 Adatrendelet (38) és 4. cikk (4) bek., 6. cikk (2) bek. *a)* pont.

lehetőségek kiemelésére;[108] az olyan felhasználói élményt zavaró felugró ablakok alkalmazására, amelyek ismételt válaszadásra kérik a felhasználót egy már korábban meghozott döntése kapcsán;[109] vagy éppen arra a megoldásra, amely okán a szolgáltatás megszüntetésére/fiók törlésére irányuló eljárás az előfizetés/regisztráció elvégzésénél nehezebben kivitelezhető csak.[110] A DSA jelenlegi rendelkezései alapján a sötét megoldásokra vonatkozó tilalmak értelmezése ugyanakkor nem egyértelmű, ugyanis a rendeletben említett sötét megoldások pontos körülhatárolás, valamint definiálás hiányában szabályozási bizonytalanságnak engedhetnek teret, amely önkényes értelmezéshez és alkalmazáshoz is vezethet. Egy kellően absztrakt, némileg általánosabb megfogalmazás azonban alkalmas lehet arra is, hogy a jövőbe mutatva, az újonnan megjelenő technológiák és a felhasználók viselkedését befolyásoló új, manipulatív megoldások is a rendelet hatálya alá tartozhassanak.[111] A sötét megoldásokat érintő tilalom alkalmazását érintően a Bizottság a DSA 25. cikk (3) bekezdése alapján felhatalmazással rendelkezik értelmezést segítő iránymutatások kiadására, így várhatóan további pontosításra számíthatunk a tilalom vonatkozásában,[112] elkerülve ezzel az önkényes értelmezést.

Ahogy arról korábban már említés esett, az egyes sötét megoldások, illetve manipulatív technikák alkalmazása több jogterület rendelkezéseibe is ütközhet. Éppen ezért az irányadó jogterület meghatározásához, valamint az eljárásra hatáskörrel rendelkező hatóság azonosításához esetről esetre kell vizsgálat alá vetni az egyes megoldásokat és azok hatásait. E nehézség feloldását szolgálja a DSA 25. cikk (2) bekezdése is, amely kimondja, hogy az UCPD, valamint a GDPR hatálya alá tartozó gyakorlatok esetében nem alkalmazandó a DSA tilalma.[113] Ez a kivétel ugyanakkor aggályokat vet fel a rendelkezés hatékonyságát illetően a sötét megoldások elleni küzdelemben, mivel jelenleg szinte valamennyi azonosított sötét megoldás a GDPR és az UCPD hatálya alá tartozik. A DSA azonban szubszidiárius jellegének köszönhetően alkalmas lehet az újonnan megjelenő technológiák szabályozására, amelyek nem tartoznak e két másik jogszabály hatálya alá, mint például a 'végtelen görgetés' (*infinite scrolling*), az 'automatikus lejátszás' (*autoplay*), vagy az 'interfész-interferencia' (*interface interference*).[114]

5.3. A digitális piacokról szóló jogszabály

A DMA célja olyan harmonizált szabályok nyújtása, amelyek hozzájárulnak a belső piac megfelelő működéséhez, biztosítva, hogy a digitális ágazat azon piacai, amelyeken kapuőrök is jelen vannak, az egész Unióban minden vállalkozás számára versengők és tisztességesek legyenek, az üzleti felhasználók és a végfelhasználók javát szolgálva egyaránt.[115] Az Európai Bizottság által bevezetett DMA rendelet célja, hogy megoldást nyújtson egyes kapuőrnek minősülő online platformok szerepére és tisztességtelen gyakorlatára.[116] A DMA mennyiségi paramétereket határoz meg annak megállapításához, hogy egy nagy online platform kapuőrnek

108 DSA 25. cikk 3) bek. *a)* pont.
109 DSA 25. cikk 3) bek. *b)* pont.
110 DSA 25. cikk 3) bek. *c)* pont.
111 Leiser et al. i. m. 21.
112 DSA 25. cikk (3) bek.
113 DSA 25. cikk (2) bek.
114 Leiser et al. i. m. 21.
115 DMA 1. cikk (1) bek.
116 DMA 2. cikk (2) bek., 3. cikk, preambulumbekezdés (16) bek.

minősül-e annak alapján, hogy milyen hatást gyakorol a belső piacra, valamint hogy olyan alapvető platformszolgáltatást nyújt-e, amely nagy felhasználói bázist köt össze számos vállalkozással, illetve, hogy szilárd és tartós piaci pozícióval rendelkezik-e.[117] A kapuőrök ilyen módon történő azonosításával a DMA lehetővé teszi a szabályozók számára, hogy azokra a platformokra összpontosítsanak, amelyek a legnagyobb valószínűséggel alkalmaznak sötét megoldásokat és egyéb tisztességtelen gyakorlatokat.[118] A Bizottság kijelölése alapján jelenleg 6 szolgáltató minősül kapuőrnek, míg 22 alapvető platformszolgáltatást sorolt kapuőri minősítés alá, amelyek között olyan jelentős szolgáltatások találhatóak, mint a TikTok, a Facebook, az Instagram, a LinkedIn, vagy a YouTube.[119]

A DMA kötelezettségeket állapít meg a kapuőrökre vonatkozóan, elsődlegesen a kapuőrök versengő jelleget korlátozó vagy tisztességtelen gyakorlatai vonatkozásában (DMA 5–15. cikk), ugyanakkor sötét megoldásokkal kapcsolatos rendelkezéseket is tartalmaz, hangsúlyozva, hogy a kapuőrök nem tanúsíthatnak olyan magatartást, amely aláássa a rendeletben meghatározott tilalmak és kötelezettségek hatékonyságát.[120] Ide tartozik a nem semleges kialakítás alkalmazása, a felhasználói felület vagy egy része struktúrájának, funkciójának vagy működési módjának a felhasználói autonómia, döntéshozatal vagy választás aláásására vagy csorbítására való felhasználása. A DMA (70) preambulumbekezdése hangsúlyozza továbbá annak fontosságát is, hogy a szabályokat a kapuőrök bármely gyakorlatára alkalmazni kell, függetlenül annak formájától, amennyiben az megfelel a rendeletben meghatározott kötelezettségek valamelyikének tárgyát képező gyakorlat típusának.[121] A rendelkezések azonban nem egyértelműek azzal kapcsolatban, hogy a 'felhasználói felület' kifejezés szigorúan a vállalat felhasználói felületének kialakítására vonatkozik-e, vagy magában foglalja a felhasználói élményt és a használt nyelvet is.

A DMA 13. cikkének (6) bekezdése megtiltja a kapuőröknek, hogy az 5., 6. és 7. cikkeiben meghatározott jogokkal vagy választási lehetőségekkel élő üzleti felhasználók vagy végfelhasználók számára nyújtott alapvető platformszolgáltatások feltételeit vagy minőségét rontsák. Ezek a rendelkezések összhangban vannak a sötét megoldások olyan manipulatív tervezési technikákként való meghatározásával, amelyek a felhasználókat olyan döntésekre kényszerítik vagy ilyen irányban megtévesztik, amelyek számukra negatív következményekkel járnak, ami fontos a felhasználói jogok védelme és a tisztességes verseny biztosítása szempontjából az online piacon.[122]

5.4. A mesterséges intelligenciáról szóló rendelet

A világ első mesterséges intelligenciára vonatkozó átfogó, horizontális jogi keretrendszerét, a mesterséges intelligenciáról szóló rendeletet 2024. július 12-én hirdették ki az EU hivatalos

117 European Commission: Digital Markets Act: Ensuring Fair and Open Digital Markets (European Commission). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

118 DMA 2. cikk (2) bek.

119 Európai Bizottság Magyarországi Képviselete: *A digitális piacokról szóló jogszabály: a Bizottság kijelölt hat „kapuőrt".* Sajtócikk, 2023. szeptember 6. https://hungary.representation.ec.europa.eu/digitalis-piacokrol-szolo-jogszabaly-bizottsag-kijelolt-hat-kapuort-2023-09-06_hu

120 DMA 13. cikk (6) bek.

121 DMA (70) preambulumbekezdés.

122 Leiser et al. i. m. 22–23.

lapjában, és 2024. augusztus 1-én lép hatályba. Az MI-rendelet meghatározásában az MI-rendszer egy „gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet", ami az OECD legutóbbi fogalmát követi. E meghatározás kulcselemei a 'következtet' és az 'autonómia', amelyek egyértelműen megkülönböztetik az MI-rendszereket más szoftverektől. Az MI-rendelet tartalmazza a tiltott MI-gyakorlatok körét, valamint az MI-rendszerek szolgáltatóinak és alkalmazóinak kötelezettségeit. A végleges szöveg fenntartja a korábbi tervezetekben meghatározott kockázatalapú megközelítést, amely az alapvető jogokat veszélyeztető kockázatot mérő skála alapján határozza meg, hogy egy adott MI-rendszer jogszerűen fejleszthető és használható-e, illetve átfogó megfelelési kötelezettségeket állapít meg a magas kockázatú MI-rendszerek számára. [123]

Az MI-rendelet bár nem említi kifejezetten a sötét megoldások fogalmát, rendelkezései elismerik a sötét megoldások által okozott lehetséges károkat. Ennek megfelelően egyértelmű jogi követelményeket határoz meg az MI-rendszerek fejlesztésére és alkalmazására vonatkozóan, beleértve az átláthatóságot, az elszámoltathatóságot és az emberi felügyeletet.[124]Az MI-rendelet 5. cikke tartalmazza a tiltott MI-gyakorlatokat, amely tilalmazott gyakorlatok között olyan technikák is korlátozás alá esnek, amelyek nagyfokú egyezést mutatnak a DSA vagy az Adatrendelet sötétmegoldás-fogalmával. Az MI-rendelet 5. cikk (1) bekezdés *a)* pontja ugyanis tiltja többek között az olyan MI-rendszereket, amelyek szubliminális technikákat alkalmaznak az adott személy tudatán kívül, vagy célzottan manipulatív vagy megtévesztő technikákat alkalmaznak azzal a céllal vagy olyan hatás érdekében, hogy lényegesen torzítsák a magatartását azáltal, hogy jelentősen gyengítik a megalapozott döntéshozatalra való képességet. Mindezek pedig azt eredményezhetik, hogy olyan döntést hozzon az adott személy, amelyet egyébként nem hozott volna meg, és oly módon, amely az említett személynek jelentős károsodást okoz vagy észszerű valószínűséggel okozhat.[125]

E tilalom mellett korlátozás alá esik továbbá az olyan MI-rendszer is, amely egy természetes személynek vagy a személyek egy meghatározott csoportjának az életkor, fogyatékosság, illetve egyedi szociális vagy gazdasági helyzet miatt fennálló valamilyen sebezhetőségét kihasználja azzal a céllal vagy hatással, hogy lényegesen torzítsa az említett személy vagy az említett csoporthoz tartozó valamely személy magatartását oly módon, amely jelentős kárt okoz vagy észszerű valószínűséggel okozhat.[126] A tilalmak megfogalmazása nagyon hasonló az UCPD irányelv rendelkezéseihez a 'személy magatartásának lényeges torzítása' kifejezés használatával, azonban az MI-rendelet szerinti korlátozások hatálya csak az MI-rendszer alkalmazásával végrehajtott gyakorlatot tilalmazza.[127]

Az MI-alapú sötét megoldások összetett és dinamikus gyakorlatokból állnak, amelyek egy weboldal/online szolgáltatás felhasználói felületének vagy felhasználói élményének valós idejű beállításait képesek befolyásolni. Ennek megfelelően az MI-alapú sötét megoldások optima-

123 Uo.
124 Leiser et al. i. m. 4.
125 MI-rendelet 5. cikk (1) bek. *a)* pont.
126 MI-rendelet 5. cikk (1) bek. *b)* pont.
127 Európai Bizottság (2022) i. m. 83.

lizálni[128] is képesek a felhasználó élményt annak érdekében, hogy egy konkrét online viselkedést idézzenek elő. A gépi tanuláson alapuló algoritmusok, valamint a felhasználói adatok segítségével[129] a vállalatok idővel hihetetlen pontossággal hozhatnak létre személyre szabott sötét megoldásokat.[130] Habár jelenleg nincs jelentős bizonyíték az egyéni sebezhetőségeket célzó, személyre szabott megoldások széles körű használatára, az adatgyűjtés, a gépi tanulás és az MI-technikák növekvő konvergenciája megváltoztathatja ezt a helyzetet,[131] ugyanis azáltal, hogy folyamatosan többet tudnak meg a fogyasztók jellemzőiről és az egyes jelzésekre adott reakcióikról, preferenciákról, növekszik a hatékony manipuláció lehetősége is.[132]

6. Szabályozási keretek értékelése

Az áttekintett jogszabályok jól mutatják, hogy az Európai Unió jelenlegi jogi kerete jelentős kihívásokkal néz szembe a közösségimédia-platformok által alkalmazott sötét megoldások megfelelő szabályozása terén. Az egyik fő probléma a digitális technológiák gyors fejlődése, amely gyakran meghaladja a szabályozás frissítésének és végrehajtásának ütemét. Emellett a sötét megoldások összetettsége és sokfélesége is jelentősen megnehezíti, hogy a meglévő jogszabályok átfogóan szabályozzák azokat. Komoly nehézséget okoz továbbá, hogy hiányoznak a sötét megoldásokra vonatkozó konkrét jogi fogalommeghatározások és osztályozások, így a rendelkezések alkalmazása, valamint értelmezés terén is kétségek merülhetnek fel. Továbbá a közösségimédia-platformok puszta mérete és befolyása kihívások elé állítja a szabályozó hatóságokat a nyomon követés és a végrehajtás terén is. A jogi eljárások sokszor lassúak és nehézkesek lehetnek, ami akadályozza a digitális szférában felmerülő problémákra való időben történő reagálást. Emellett a platformok önszabályozására való hagyatkozás elégtelen felügyeletet és elszámoltathatóságot eredményezhet. A nyilvánosság tudatossága és a sötét megoldások megértése gyakran korlátozott, ami akadályozhatja az erősebb szabályozásra irányuló érdekérvényesítő erőfeszítéseket is. Ezen túlmenően a lobbizás és az iparág szerepe befolyásolhatja a jogalkotási eredményeket, ami felhígíthatja a szabályozási intézkedések hatékonyságát.

Az EU különböző típusú korlátozó intézkedéseket alkalmaz a sötét megoldások terén. Mind az adatvédelmi, mind a fogyasztóvédelmi jogszabályok tartalmaznak olyan általánosan megfogalmazott kötelezettségeket, amelyek a sötét megoldásokra is alkalmazandók. Az adatvédelmi jog átfogó elvek (méltányosság, átláthatóság, alapértelmezett és beépített adatvédelem stb.) és a hozzájárulással kapcsolatos jogi követelmények révén jogi védelmet biztosít; a sötét

128 Congressional Research Service: *What Hides in the Shadows: Deceptive Design of Dark Patterns.* 2022. november 4. https://sgp.fas.org/crs/misc/IF12246.pdf,

129 Natalia Helberger – Orla Lynskey – Hans-W. Micklitz – Peter Rott – Marijn Sax – Joanna Strycharz: *EU consumer protection 2.0 Structural asymmetries in digital consumer markets*. Brüsszel, BEUC, 2021. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf 6., vö: Maurits Kaptein – Panos Markopoulos – Boris de Ruyter – Emile Aarts: Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles. *International Journal of Human-Computer Studies,* vol. 77., no. 2. (2015). https://doi.org/10.1016/j.ijhcs.2015.01.004

130 Daniel Susser – Beate Roessler – Helen Nissenbaum: Technology, Autonomy, and Manipulation. *Internet Policy Review,* vol. 8., no. 2. (2019). https://doi.org/10.14763/2019.2.1410

131 OECD: Dark commercial patterns. In: *OECD Digital Economy Papers, No. 336.* Paris, OECD Publishing, 2022. 82.; Stuart Mills: Personalized nudging. *Behavioural Public Policy*, vol. 6., no. 1. (2020) 150–159.

132 Leiser et al. i. m. 26.

megoldásokkal szemben az érintettek egyéni kárát veszik figyelembe. A fogyasztóvédelmi jog, különösen az UCPD tiltja az olyan kereskedelmi gyakorlatok bizonyos típusait, amelyek a fogyasztókat olyan döntés meghozatalára késztetik, amelyet egyébként nem hoztak volna meg. Ezzel szemben a DSA, a DMA és az Adatrendelet sötét megoldásokra vonatkozó konkrét rendelkezéseket tartalmaz, amelyek meghatározzák a sötét megoldás fogalmát, és követelményeket tartalmaznak az interfészek kialakítására vonatkozóan. Ami a sötét megoldások eredményeit és hatásait illeti, úgy tűnik, hogy mind a fogyasztóvédelem, mind az adatvédelem főként az egyéni hatásokra fókuszál. Ezzel szemben a DSA és a DMA a kollektív hatásokat veszi figyelembe,[133] míg az MI-rendelet mind az egyéni, mind a kollektív hatásokra kiterjed.

A fenti áttekintés alapján jól látható, hogy a jelenlegi szabályozási rendszer aktuális formájában nem elegendő a sötét megoldások szabályozására. Optimális helyzetben az Európai Uniónak átfogó szabályozási keretet kellene biztosítania a sötét megoldások és a megtévesztő tervezési gyakorlatok szabályozására, azonban jelenleg a szabályozás hatékonysága nagymértékben függ számos rendelkezés értelmezésétől.[134]

2. táblázat

Az EU sötét megoldások szabályozása kapcsán releváns jogi keretei, valamint azok áttekintése a szabályozás irányát/tárgyát, alkalmazandóság alól kivételét, illetve a sötét megoldás által elért hatás terjedelmét tekintve

EU jsz.	Rendelkezés típusa	Szabályozás iránya/tárgya	Kivétel	Hatás

UCPD	általános klauzulák – kereskedelmi gyakorlat	**Tisztességtelen kereskedelmi gyakorlatok (5–9. cikk)**
		• Megtévesztő kereskedelmi gyakorlat (6. cikk):
		  • hamis információt tartalmaz
		  • bármilyen módon félrevezető – ideértve a megjelenítés valamennyi körülményét
		• Megtévesztő mulasztás (7. cikk):
		  • jelentős információ elhallgatása vagy homályos, érthetetlen, félreérthető, vagy időszerűtlen rendelkezésre bocsátása
		  • a kereskedelmi gyakorlatban alkalmazott kommunikációs eszköz
		• Agresszív kereskedelmi gyakorlat (8–9. cikk):
		  • a kereskedelmi gyakorlat ténybeli összefüggése – figyelembe véve valamennyi jellemzőjét és körülményét
		  • szóhasználat
			Nem kereskedelmi gyakorlat	egyéni

GDPR		**Beépített és alapértelmezett adatvédelem (25. cikk):** • alkalmazások, szolgáltatások és termékek kifejlesztése, tervezése, kiválasztása és felhasználása, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek	nincs személyes adatkezelés	egyéni

133 Leiser et al. i. m. 28.
134 Leiser et al. i. m. 5.

EU jsz.	Rendelkezés típusa	Szabályozás iránya/tárgya	Kivétel	Hatás
Adatrendelet	specifikus szabályok a sötét megoldásokra vonatkozóan	**Sötét megoldások (38. preambulumbekezdés)** • harmadik felek vagy adatbirtokosok a digitális interfészeik tervezésekor nem hagyatkozhatnak 'sötét megoldásokra' (manipulatív tervezési technikák) **Harmadik felek kötelezettségei, akik a felhasználó kérésére adatokat kapnak [6. cikk (2) bek. a) pont]** • választási lehetőség kínálása, többek között egy felhasználói digitális interfész vagy annak egy része révén	nem adatmegosztási és hordoz-hatósági gyakorlatok	kollektív
DSA		**Sötét megoldások (67. preambulumbekezdés)** • az online platformok online interfészei egészének vagy részének szerkezete, kialakítása vagy funkciói révén megjelenő sötét megoldások. • ez magában foglalja többek között, de nem kizárólag a visszaélésszerű kialakítást, vagy olyan alapértelmezett beállítások alkalmazását, amelyek nagyon nehezen módosíthatók **Online interfész tervezése és kialakítása (25. cikk):** • online interfész tervezése, kialakítása és üzemeltetése	A GDPR/UCPD hatálya alá tartozó gyakorlatok	kollektív
DMA		**Kijátszás tilalma [13. cikk (6) bekezdés]:** • nem semleges választási lehetőségek nyújtása a felhasználói interfész egészének vagy egy részének felépítése, kialakítása, funkciója vagy működési módja révén **Megtévesztő, manipulatív interfész (37. preambulumbekezdés):** • A kapuőrök nem tervezhetik, szervezhetik vagy működtethetik az online interfészeiket olyan módon, amely megtéveszti vagy manipulálja a végfelhasználókat, vagy más módon jelentősen befolyásolja vagy korlátozza az önkéntes hozzájárulásuk megadásának lehetőségét	Nem kapu-őrök	kollektív
MI-rendelet		**Tiltott MI-gyakorlatok [5. cikk (1) bek. a)–b) pont]:** • MI-vel működő rendszer forgalomba hozatala, üzembe helyezése vagy használata, amely egy személy tudatán kívül szubliminális technikákat vagy célzottan manipulatív vagy megtévesztő technikákat alkalmaz, oly módon, amely *jelentős károsodást okoz* vagy észszerű *valószínűséggel okozhat* • MI-rendszer forgalomba hozatala, üzembe helyezése vagy használata, amely kihasználja a felhasználó sebezhetőségét, azzal a céllal vagy azzal a hatással, hogy jelentősen torzítsa az adott személy viselkedését oly módon, amely *jelentős kárt okoz* vagy észszerű *valószínűséggel okozhat*	Nem MI-rendszer	egyéni és kollektív

Saját szerkesztés

7. A közösségi médiában alkalmazott sötét megoldások

Jelenleg a felhasználói interfészeket olyan környezeteknek tekintik, amelyek „bizonyos cselekvéseket, gondolatokat, hatásokat, lehetővé tesznek, ösztönöznek, bátorítanak és megakadályoznak, vagy éppen másokat elősegítenek."[135] Ez egyszerre jelentheti a tervezők azon képességét, hogy olyan felületeket alakítsanak ki, amelyek képesek a sötét megoldások által a felhasználói elkötelezettséget növelni, illetve a lehetőséget is olyan funkciók beépítésére, amelyek segítenek a felhasználókat a szolgáltatók érdekei felé irányítani.[136] Egy 2023-as, közösségimédia-platformokat érintő kutatás eredménye azt mutatta, hogy a legnagyobb változatossággal, mintegy 41 különböző típusú sötét megoldás alkalmazásával a Facebook vezetett, ezt követte az Instagram a maga 39 féle sötét megoldásával, majd a Twitter (X), ahol 35 különböző típusú sötét megoldást figyeltek meg, és végül a TikTok, ahol 37 egymástól eltérő típusú technikát azonosítottak.[137]

A közösségimédia-platformokon alkalmazott sötét megoldások leginkább szembetűnő fajtáit az átlagos felhasználó is könnyen észreveszi, mivel e technikákat viszonylag könnyebb azonosítani, valamint alkalmazásuk sem jár többnyire magas kockázattal. Az ilyen sötét megoldások egyik tipikus fajtája az 'interfész-interferencia' (*interface interference*),[138] azaz olyan felhasználói interfészek, amelyek bizonyos elemeket előnyben részesítenek másokkal szemben, és ezzel összezavarják a felhasználókat egy adott választás meghozatalában. Az azonosítás könnyedségében hasonló megítélés alá esik a 'vizuális interferencia' (*visual interference*),[139] vagyis amikor olyan vizuális/grafikai technikákat alkalmaznak, amelyek alkalmasak az interfészen keresztül a felhasználók választásának befolyásolására.[140] Szintén gyakori tervezési technika, és viszonylag könnyen felismerhető az interfészeken az 'akadályozás' (*obstruction*),[141] amely bizonyos cselekvések szükségtelen megnehezítésével jár – sokszor a felhasználók demotiváltságára apellálva –, mint például a 'csótány-motel' (*roach motel*). Az adatvédelem kijátszására törekvő sötét megoldások közül talán a legismertebbek és elterjedtebbek a 'rossz alapértelmezett beállítások' (*bad defaults*),[142] amelyek a felhasználó számára nem kedvező alapértelmezett adatvédelmi beállításokat jelentenek, így például a személyes adataik megosztását, valamint az 'ösztönzést egyre több személyes adat megadására' (*privacy zuckering*),[143] amelynek célja, hogy a szükségesnél és szándékoltnál több információt megszerezzenek a felhasználóról.[144]

135 Maurizio Lazzarato: *Signs and Machines – Capitalism and The Production of Subjectivity*. Cambridge, Semiotext(e), 2014. 30.

136 Kaitlin Woolley – Marissa A. Sharif: *The Psychology of Your Scrolling Addiction.* Boston, Harvard Business School Publishing, 2022. https://hbr.org/2022/01/the-psychology-of-your-scrolling-addiction

137 Thomas Mildner – Gian-Luca Savino – Philip R. Doyle – Benjamin R. Cowan – Rainer Malaka: About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In: *CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. New York, ACM, 2023. Article 192. https://doi.org/10.1145/3544548.3580695

138 Gray et al. (2018) i. m. 7.

139 Mathur et al. i. m. 12.

140 Mildner et al. (2023) i. m. 5.

141 Gray et al. (2018) i. m. 9.

142 Bösch et al. im. 237–254.

143 Brignull i. m., Mildner–Savino (2021b) i. m. 3.

144 Mildner et al. (2023) i. m. 5.

7.1. Algoritmusok alkalmazása a felhasználói interfészek kialakításában

A sötét megoldások széles skáláján azon tervezési technikák minősülnek a legmanipulatívabb fajtáknak, amelyeket a felhasználói felület helyett szándékosan egy online szolgáltatás rendszerarchitektúrájába (*system architecture*), vagyis egy digitális termék vagy alkalmazás szerkezeti tervébe vagy kódszintjére integrálnak.[145] A fejlesztők gépi tanuláson alapuló algoritmusok használatával a felhasználói viselkedés elemzésére, illetve személyre szabott ösztönzők, ajánlások létrehozására képesek, amelyek bizonyos választások felé terelik a felhasználókat. Ezeket az algoritmusokat akár úgy is tervezhetik, hogy a felhasználó jóléte helyett inkább az elkötelezettséget vagy a bevételt optimalizálják, ami olyan rendszerarchitektúrához vezet, amely az üzleti célokat a felhasználói igényekkel szemben előtérbe helyezi.[146]Az algoritmikus tervezéssel foglalkozó tudósok ezeket a 'determinisztikus algoritmusokhoz' sorolják,[147] amelyek remek példája az olyan erősen személyre szabott ajánlás, amely több tényezőt figyelembe véve, beleértve a felhasználói viselkedési adatokat és preferenciákat, a hasonló bemenetekre végezetül ugyanazt a kimenetet képes adni. Hasonlóan problematikusnak bizonyulnak azonban a 'nem-determinisztikus algoritmusokon'[148] alapuló sötét megoldások is, amelyeket talán még a determinisztikus fajtánál is nehezebb felismerni, ellenőrizni, illetve szabályozni.[149] Ezekben az esetekben ugyanis a rendszert szándékosan úgy tervezték meg, hogy ugyanazon bemeneti inputokra különböző kimeneteket adjon, mint például az 'árnyékprofilok' (*shadow user profiles*),[150] vagy olyan adatmegosztási gyakorlatok, amelyek a felhasználók számára nem láthatók, de hatással vannak a magánéletükre vagy a döntéshozatalukra. A 'nem-determinisztikus' megoldások azonosításához általában 'bennfentes' információkra van szükség a platform működéséről, ám az átláthatatlan algoritmusok és gépi tanulási technikák alkalmazása még ezen információk birtokában is komoly veszélyt jelenthetnek a felhasználók autonómiájára, valamint a személyes adatok feletti ellenőrzésre, és az érintetti jogokra.[151] Ezen túlmenően, az algoritmusok használata felerősítheti a manipulatív választási architektúrák

145 Tobias Münch: *System Architecture Design and Platform Development Strategies: An Introduction to Electronic Systems Development in the Age of AI, Agile Development, and Organisational Change* [Első kiadás]. Heidelberg, Springer, 2022. 42.

146 Leiser et al. i. m. 9.

147 GeeksforGeeks: Difference between Deterministic and Non-deterministic Algorithms. *GeeksforGeeks.org,* 2024. május 3. https://www. geeksforgeeks.org/difference-between-deterministic-and-non-deterministic-algorithms/

148 Robert W. Floyd: Nondeterministic Algorithms. *Journal of the ACM*, vol. 14. no. 4. (1967). https://doi.org/10.1145/321420.321422

149 Donald E. Knuth: Estimating the efficiency of backtrack programs. *Mathematics of Computation,* vol. 29., no. 129. (1975). https://shorturl.at/mVbhh

150 Vö. Luis Aguiar – Christian Peukert – Maximilian Schäfer – Hannes Ullrich: Facebook shadow profiles. *SSRN*, (2022). https://shorturl.at/CFZF6; ld. Tipp Moseley – Alex Shye – V. J. Reddi – Dirk Grunwald –Ramesh Peri: Shadow profiling: Hiding instrumentation costs with parallelism. San José (2007. március 11–14.) *International Symposium on Code Generation and Optimization (CGO'07).* https://doi.org/10.1109/CGO.2007.35

151 Sebastião Barros Vale – Gabriela Zanfir-Fortuna: *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities.* Washington, Future of Privacy Forum, 2022. https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf

hatását is, [152] így amikor egy algoritmus olyan tényezők alapján dönti el, hogy mely termékek jelennek meg a felhasználók számára, mint például a népszerűség vagy a nyereségesség, ez megerősítheti a választási architektúrát azáltal, hogy bizonyos lehetőségeket láthatóbbá vagy vonzóbbá tesz. Ez egy olyan önerősítő ciklushoz vezethet, amelyben a rendszerarchitektúra egyre inkább a platform céljaira optimalizálódik, nem pedig a felhasználóéra.

A fogyasztói magatartást, preferenciákat és korábbi interakciókat elemző algoritmusok képesek beágyazódni a közösségimédia-platformok rendszerarchitektúrájába, és a fogyasztók döntéshozatali folyamatát kihasználva manipulálni a nekik bemutatott lehetőségeket. Ez a felhasználás nem csak a felhasználói autonómia vonatkozásában hordozhat magában kockázatokat, de komoly hatása lehet a felhasználók véleményalkotásának és az információk, eszmék megismerésének és közlésének szabadságára is.

Ahogy korábban már említettem, a közösségimédia-platformok gyakran építenek a pszichológiai tapasztalatokra, így a rendszerarchitektúra akár úgy is megtervezhető, hogy az kihasználja a függőséget okozó viselkedést ösztönző pszichológiai elveket és növelje a felhasználói elkötelezettséget.[153] Ilyen technikára épít a sötét megoldások közül például a 'végtelen görgetés' (*infinite scrolling*), vagy az 'automatikus lejátszás' (*autoplay*). A platformok ezekkel a technikákkal a tartalom folyamatos fogyasztását ösztönözhetik azzal, hogy automatikusan új tartalmat töltenek be, amint a felhasználók elérik egy oldal vagy videó végét. Ennek megvalósításához algoritmusok segítségével a felhasználó preferenciái és viselkedése alapján releváns tartalmat keresnek és jelenítenek meg (gyakran egyre több és több javasolt tartalom jelenik meg, minél tovább halad a felhasználó). Gyakori technika még a felhasználók elkötelezettségének növelésére, a változó gyakoriságú 'társadalmi megerősítés' (*social proof*). E pszichológiai ösztönzők létrehozásához olyan algoritmusokat építenek a rendszer felépítésébe, amelyek a felhasználókat szórványosan, vagy olyan elemek bevezetésével jutalmazzák, mint a virtuális valuta, jelvények vagy pontok, amelyeket az alkalmazáson belül lehet megszerezni és beváltani. A jutalmak és a különböző gyakoriságok a felhasználók elkötelezettségének fenntartásához megtévesztő tervezést igényelnek a rendszerarchitektúrában; például a közösségimédia-platformok algoritmusokat használhatnak arra, hogy különböző időközönként értesítéseket és tartalmakat jelenítsenek meg a felhasználók készülékein, így a felhasználók találgathatják, mikor kapják a következő reakciót vagy kommentet.[154] Nem ritka továbbá a 'játékosítás' (*gamification*) sötét megoldás alkalmazása sem, amely során olyan játékszerű elemeket integrálnak a platformba, mint a kihívások, ranglisták és teljesítményrendszerek, növelve a felhasználók elkötelezettségét és motivációját.[155]

152 Karen Yeung: 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society,* vol. 20., no. 1. (2017) 1–19.; Simon Mills – Henrik Skaug Sætra: The autonomous choice architect. *AI & Society*, vol. 39., no. 2. (2024) https://doi.org/10.1007/s00146-022-01486-z; European Parliamentary Research Service Scientific Foresight Unit (STOA): *Understanding algorithmic decision-making: Opportunities and challenges*. Brüsszel, Európai Unió, 2019. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf

153 Maéva Flayelle – Damien Brevers – Daniel L. King – Pierre Maurage – José C. Perales – Joël Billieux: A taxonomy of technology design features that promote potentially addictive online behaviours. *Nature Reviews Psychology,* vol. 2., no. 3. (2023) https://doi.org/10.1038/s44159-023-00153-4

154 Dorcas Adisa: Everything You Need to Know about Social Media Algorithms. *The Sprout Social*, 2023. október 30. https://sproutsocial.com/insights/social-media-algorithms/

155 Leiser et al. i. m. 18–19.

A gyakorlatban egy olyan kifinomult ajánlórendszert, mint amilyen például amilyen a TikTok, a Facebook vagy a YouTube platformján[156] is üzemel, úgy alakítottak ki, hogy az különböző forrásokból legyen képes adatokat gyűjteni a felhasználók viselkedéséről. Ennek megfelelően a platform algoritmusa figyeli a megnézett videó tartalmát, annak feliratát és hangját, az adott napszakot, a felhasználó lokációs, illetve helymeghatározási adatait a videó lejátszásának idején, az újrajátszások számát, sőt még a videó által közvetített érzelmi állapotokat is.[157] A gyűjtött adatok összegzése és elemzése révén képes lesz az algoritmus olyan személyre szabott tartalmakat nyújtani a felhasználó számára, amelyek hosszú ideig képesek lekötni a felhasználó figyelmét.[158]

7.2. A közösségi médiában alkalmazott sötét megoldások csoportosítása

Mint ahogy azt láthatjuk, a sötét megoldások alkalmazásának számtalan formája ismeretes mára a gyakorlatban és a szakirodalomban egyaránt, amelyek különböző szempontokra, illetve hatásokra építve kategorizálják e technikákat. A korábbi forrásokra és tapasztalatokra építve,[159] valamint jelen tanulmány fókuszára tekintettel kísérletet teszek a kifejezetten a közösségimédia-platformokon alkalmazott sötét megoldások csoportosítására a két leggyakrabban elérni kívánt cél mentén, vagyis a felhasználói elkötelezettséget ösztönző technikák, valamint a felhasználók cselekvéseit és döntéseit irányító technikák mentén. Az elkötelezést ösztönző stratégiák célja a felhasználók elkötelezettségének növelése a függőséget okozó funkciók alkalmazásával és a személyre szabott tartalom felhasználásával, a platform hosszan tartó használatának ösztönzése. Ezzel szemben az irányítási megoldások finoman manipulálják a felhasználói viselkedést, igazodva a platform céljaihoz, sokszor a felhasználói autonómia vagy a magánélet rovására, olyan taktikák révén, mint a rejtett beállítások.

7.2.1. Elkötelezést ösztönző sötét megoldások

Az elkötelezést ösztönző technikákat két fő csoportra oszthatjuk; az első az a Mildner és munkatársai által korábban „interaktív horogként" (*interactive hook*) nevesített stratégia, amely olyan tervezési mechanizmusokra épít, amelyek jutalmazó rendszereket alkalmaznak a felhasználók szórakoztatására és figyelmük, valamint idejük lekötésére, hogy ezáltal is több időt töltsenek a platformon. Ide sorolható maga az interfész addiktív kialakítása (*addictive design*), amely olyan jellemzőkkel és elemekkel operál, amelyek a felhasználókat a tartalomhoz kötik. Többek között a korábban ismertetett játékosítás (*gamification*)[160] esete is ide tartozik. Egészen hasonló ehhez a technikához a TikTokon elterjedt virtuális ajándék/pénznem (*virtual gifts / intermediate currency*) is, amely lehetővé teszi a felhasználók számára, hogy virtuális valutát vásároljanak, amelyet aztán digitális árura vagy szolgáltatásra költhetnek. Bár

156 Chianella i. m. 5.
157 Uo. 9.; Mahnoor Sheikh: How the TikTok algorithm works in 2024. *The Sprout Social,* 2024. február 15. https://sproutsocial.com/insights/ tiktok-algorithm/
158 Chianella i. m. 5.
159 Ld. II. fejezet, továbbá vö. Mildner et al. (2023) i. m. 7. 2. táblázat.
160 Mildner et al. (2023) i. m. 14.

e köztes valuták használata nem feltétlenül sötét megoldás, a mechanizmus mögött azonban az a cél áll, hogy a felhasználókat elszakítsa a tényleges valutaértéktől. Ez azt eredményezheti, hogy a felhasználók a virtuális valutát a tényleges valutától eltérően költik el, sokszor jóval könnyelműbben a tényleges pénzüknél.[161] Szintén e kategóriát erősíti a 'végtelen görgetés' (*infinite scrolling*)[162] és a 'húzás a frissítéshez' (*pull to refresh*) technikák is, amelyek mind a négy nagy közösségi média platform – a Facebook, az Instagram, a TikTok, és a Twitter (X) –esetében megfigyelhetők, vagy akár az 'automatikus lejátszás' (*autoplay*), amely szintén megtalálható a Facebook, az Instagram, a TikTok, de még a YouTube gyakorlatában is. A 'húzás a frissítéshez' azt jelenti, hogy a tartalommegjelenítő felületeken lefelé húzva új tartalom töltődik be. Néha a javasolt tartalmak belekeverednek a *feed*be, hogy a felhasználóknak több néznivalót adjanak. Az 'automatikus lejátszás' a tartalom automatikus lejátszását jelenti a felhasználó további műveletei nélkül.[163]

Az interaktív technikák mellett a másik fő csoportot az olyan technikák alkotják, amelyek valamilyen szociális kapcsolatra, közvetítésre építenek. Ezek olyan tervezési mechanizmusok, amelyek arra ösztönzik a felhasználókat, hogy több kapcsolatot hozzanak létre emberekkel (pl. hasonló tulajdonságok alapján), miközben új embereket javasolnak, akikkel kapcsolatba léphetnek, ami arra készteti a felhasználókat, hogy többet osszanak meg a szélesebb nyilvánossággal, mint amennyit szeretnének.[164] Ebbe a kategóriába tartozik többek között a Bösch és munkatársai-féle 'címjegyzéklékelés' (*address book leeching*), amely arra kényszeríti a felhasználót, hogy a szolgáltatás igénybevételéhez megossza kapcsolattartói személyes adatait, vagy a 'közösségi piramis' (*social pyramid*), amely megköveteli a felhasználóktól, hogy más felhasználókat toborozzanak a szolgáltatás használatához. Ezt a módszert gyakran használják a közösségimédia-platformok mellett az online játékokban is. Ebbe a kategóriába sorolható a Brignull-féle 'barátok behívása' (*friend spam*) is, amely kicsit vegyíti az előző két megoldást, ugyanis lényege, hogy egy közösségimédia-platform vagy más online szolgáltatás hozzáférést kér a felhaszhasználó kontakjaihoz, telefonkönyvéhez, annak érdekében, hogy meg tudja találni barátait is az adott szolgáltatás keretében, de a valóságban hozzáférve a felhasználó összes kapcsolatához, képes lesz üzeneteket küldeni nekik.[165] Ide sorolandó azonban még a 'társadalmi megerősítés' (*social proof*) technikája is, amely arra a pszichológiai és társadalmi jelenségre épít, amelynek során az emberek mások cselekedeteit másolják, amikor bizonytalannak érzik magukat, és így próbálják az adott helyzetben a helyes viselkedést tükrözni.[166]

7.2.2. Irányítási stratégiákra építő sötét megoldások

Az irányítási stratégiákra építő sötét megoldások olyan interfésztervezéseket eredményeznek, amelyek a felhasználók döntéshozatalát a platformszolgáltatók céljai felé irányítják. Ezek lényegében a felhasználói viselkedés irányítására vagy szabályozására szolgálnak. E stratégiák

161 Európai Bizottság (2022) i. m. 50–51.
162 Eskelinen i. m. 16.
163 Mildner et al. (2023) i. m. 8.
164 Uo. 8.
165 Gray et al. i. m. (2018) 8.
166 Robert B. Cialdini: *Influence, New and Expanded: The Psychology of Persuasion*. New York, Harper Business, 2021. 127.

körében is több fő csoportot különböztethetünk meg, így a döntési bizonytalanságot kiváltó technikákat, a megnehezített navigációt, illetve az irányított beállításokat.

A döntési bizonytalanságot kihasználó technikák olyan stratégiák, amelyek összezavarják a felhasználókat azáltal, hogy csökkentik a helyzetek értékelésének képességét, és a felhasználó nem tudja, hogy mit várnak el tőle, vagy milyen lehetőségek állnak rendelkezésére.[167] Ehhez a sötét mintához leginkább a 'zavarás' (*confusion*) sötét megoldás hasonlít. Ide sorolandó ugyanakkor a 'homályosítás' (*obfuscation*) és a 'megszégyenítés' (*confirmshaming*) is.

A megnehezített navigációs technikák olyan sötét megoldásokra utalnak, amelyek egymásba ágyazott felületeket foglalnak magukba, könnyű eltévedni bennük, megakadályozva ezáltal a felhasználókat abban, hogy eljussanak a kívánt beállítás kiválasztásához. Ez a technika gyakran azonosítható a közösségimédia-platformok beállításai között, különösen az adatvédelmi, illetve hirdetési beállítások vonatkozásában. A legutóbbi átalakítása során például a Facebook bevezetett egy új funkciót, az 'Adatvédelmi ellenőrzés' nevű funkciót, amely lehetővé teszi a felhasználók számára, hogy egy irányított, lépésről lépésre haladó folyamat során szerkesszék az adatvédelmi beállításokat az előre kiválasztott kategóriákhoz. Az ebben a funkcióban végrehajtott változtatások közvetlenül befolyásolják az adatvédelmi beállításokat, bár hiányos lefedettséggel. Az irányított beállítások funkcióval a Facebook képes megválasztani, hogy a felhasználók milyen beállításokat kezeljenek.[168] Tipikus példája még ennek a technikának az 'elterelés' (*distraction*), vagy a 'csótánymotel' (*roach motel*) gyakorlatok, valamint a 'halhatatlan fiókok' (*immortal accounts*).[169]

Az irányított beállítások olyan, a felhasználó döntési szabadságát korlátozó megoldások, amelyek arra kényszerítik a felhasználókat, hogy szükségtelen lépéseket tegyenek és különböző akadályokat kelljen leküzdeniük, mielőtt elérnék a tényleges céljaikat. Ezek a megoldások többnyire 'rossz alapértelmezett beállítások' (*bad defaults*) vagy olyan 'előre bepipált jelölőnégyzetek' (*pre-ticked checkboxes*) alkalmazását jelentik, amelyek a platformszolgáltatók céljait részesítik előnyben. Ebbe a kategóriába sorolandó még a 'kényszerítés' (*coercion*) is, amely alapján a felhasználóknak először meg kell felelniük bizonyos követelményeknek, mielőtt megtehetnék, amit akarnak.[170]

E fenti csoportosítások alapján jól látható, hogy a közösségimédia-platformok üzemeltetői a sötét megoldások széles skálájával operálnak. A technológia fejlődésével ugyanakkor az is egyre világosabbá válik, hogy amennyiben fel szeretnék venni a lépést a konkurens platformokkal, illetve minél tovább szeretnék a felhasználók figyelmét megragadni, annál inkább vannak rákényszerítve a minél nagyobb fokú perszonalizációra, illetve ennek megfelelően a mesterséges intelligencián alapuló sötét megoldások alkalmazására, még ha ez nem is szolgálja feltétlenül a felhasználói érdekeket.

167 Mildner et al. (2023) i. m. 8.

168 Mildner–Savino (2021a). i. m. 2–3.

169 Brennan Schaffner – Neha A. Lingareddy – Marshini Chetty: Understanding Account Deletion and Relevant Dark Patterns on Social Media. *Proceedings of the ACM on Human-Computer Interaction* vol. 6., no. CSCW2. (2022) 12.

170 Mildner et al. (2023) i. m. 9–10.

3. táblázat

A közösségi média platformokon megjelenő sötét megoldások csoportosítása a Mildner és munkatársai által kidolgozott struktúra alapján, a korábbi taxonómiák figyelembevételével és beépítésével

		Sötét megoldás	Facebook	Instagram	TikTok	X
Elkötelezést ösztönző sötét megoldások	Interaktív technikák	• addiktív kialakítás (*addictive design*)	×	☐	☐	☐
		• játékosítás *(gamification)*	☐	☐	☐	☐
		• automatikus lejátszás *(autoplay)*	☐	☐	☐	☐
		• végtelen görgetés *(infinite scrolling)*	☐	☐	☐	☐
		• virtuális ajándék/pénznem *(virtual gifts / intermediate currency)*	×	×	☐	×
		• húzás a frissítéshez *(pull to refresh)*	☐	☐	☐	☐
	Szociális kapcsolatra, közvetítésre építő technikák	• címjegyzéklékelés *(address book leeching)*	☐	☐	☐	☐
		• társadalmi megerősítés *(social proof)*	☐	☐	☐	☐
		• közösségi piramis *(social pyramid)*	☐	☐	☐	☐
		• barátok behívása *(friend spam)*	☐	☐	☐	☐
Irányítási stratégiákra építő sötét megoldások	Döntési bizonytalanságot kihasználó technikák	• zavarás (*confusion*)	☐	☐	☐	☐
		• megszégyenítés (*confirmshaming)*	☐	☐	☐	☐
		• homályosítás (*obfuscation*)	☐	☐	☐	☐
		• csalás és átverés *(bait and switch)*	☐	×	×	☐
	Megnehezített navigációs technikák	• elterelés (*distraction*)	☐	☐	☐	☐
		• csótánymotel/ nehéz lemondás *(roach motel)*	☐	☐	☐	☐
		• halhatatlan fiókok *(immortal accounts)*	☐	☐	☐	☐
	Irányított beállítási technikák	• rossz alapértelmezett beállítások (*bad defaults*)	☐	☐	☐	☐
		• előre bepipált jelölőnégyzetek *(pre-ticked checkboxes / preselection)*	☐	☐	☐	☐
		• kényszerítés *(coercion)*	☐	☐	☐	☐

Saját szerkesztés

8. Következtetések és gondolatok a szabályozási irányokról

A sötét megoldásokat körülvevő szabályozási környezet jelentős széttagoltságot mutat, ugyanakkor az eltérő szabályozási területek ellenére közös kihívást jelent a sötét megoldások egységes definíciójának, illetve taxonómiájának hiánya, az új sötét megoldások gyors fejlődése, valamint a jogi beavatkozást igénylő sötét megoldások és tervezési technikák azonosításának nehézsége,[171] illetve a jogszerű technikáktól való elválasztása. A szabályozási pluralizmus megnehezíti a jogsértések azonosítását és a megfelelő fellépés lehetőségét, éppen ezért nélkülözhetetlen, hogy a sötét megoldásokkal kapcsolatos szabályozást egyetlen jogszabályi keretben, ideális esetben a platformszabályozás területén belül egységesítsék. A szabályozás ilyen módon történő racionalizálása fokozná a megtévesztő és manipulatív gyakorlatok elleni küzdelem következetességét és hatékonyságát. Ennek a szabályozási környezetnek a kialakításához ugyanakkor elsődleges és nélkülözhetetlen követelmény a sötét megoldások egy általánosan elfogadott definíciójának kidolgozása. Javasolt lehet esetleg az MI-rendelet MI-rendszerekre vonatkozó meghatározásához hasonló fogalommeghatározással operálni, és a sötét megoldásoknak egy olyan definíciót találni, amely egyszerre ragadja meg a sötét megoldások jellemzőit, de kellően rugalmas ahhoz, hogy a technológia fejlődését követve az újabb sötét megoldásokat és technikákat is le tudja fedni.[172]

Az ismertetett gyakorlatok és sötét megoldások mentén jól látható, hogy az MI-rendszerekkel támogatott manipulatív technikák bizonyulnak a felhasználói önállóságot, valamint döntéshozatalt leginkább veszélyeztető és befolyásoló megoldásoknak, hiszen könnyen használhatóak arra, hogy a felhasználókat nem kívánt viselkedésre vegyék rá, vagy számukra előnytelen döntések meghozatalára ösztönözzék őket. Éppen ezért az általános fogalommeghatározást követően érdemesnek tartanám a már eddig azonosított sötét megoldások típusainak, illetve fajtáinak rögzítését is, akár a sötét megoldások felhasználók jogaira jelentett kockázat mértéke alapján történő kategorizálásával, amely megkönnyítené a célzott beavatkozásokat és végrehajtási intézkedéseket. A csoportosítás alapján a könnyen azonosítható technikák kisebb kockázati besorolással rendelkeznének, míg az algoritmusalapú, hangsúlyosan a felhasználó számára célzott tartalmakkal működő sötét megoldások – főleg azok, amelyeket a rendszerstruktúrákba integrálnak bele – a legmagasabb kockázati besorolásba kerülnének. Megfontolásra érdemesnek tartanám továbbá egy megfelelő szankcionálási rendszer kidolgozását is.

Álláspontom szerint a platformok gyakorlatának átláthatóságát növelő további kötelezettségek meghatározása kulcsfontosságú ahhoz, hogy a felhasználók számára követhetőbbé váljon a sötét megoldások használata a közösségimédia-platformokon. Az egyik legfontosabb szempont a megfelelő információk rendelkezésre bocsátása, így megoldás lehet, ha a platformok üzemeltetőit kötelezik arra, hogy a felhasználók számára pontos tájékoztatást nyújtsanak az alkalmazott technikák alapjairól is, vagyis, hogy egy adott tartalmat miért jelenítenek meg a felhasználónak (betekintést engedve az algoritmus által használt források körébe, legyen az akár a korábbi interakcióik, vagy más gyűjtött adatok és elemzések eredménye). Az átláthatóság növelésével talán követhetőbb lenne a felhasználók számára is a hírfolyamuk tartalma, ami segítené a manipuláció

171 Colin M. Gray – Cristiana Santos – Nataliia Bielova – Michael Toth – Damian Clifford: *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective.* In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).* New York, Association for Computing Machinery, 2021. 1–18.

172 Chianella i. m. 11.

lehetőségének csökkentését is. A közösségimédia-platformok üzemeltetőit továbbá kötelezni lehetne arra is, hogy világosan tüntessék fel, ha egy adott tartalom személyre szabott a felhasználó részére, valamint kötelezni őket arra, hogy felhívják a figyelmet az alternatív tartalmak és vélemények elérhetőségére is, így amennyiben nem kívánnak élni ezzel a személyre szabott 'élménynyel', úgy lehetőségük lehessen kikapcsolni ezt a funkciót, és egyéb, objektív szempontok szerint megjelenő tartalmakat fogyasztani (például a felhasználó által követett személyek videóit feltöltési sorrendben). E további kötelezettségek végrehajtásával a platformok olyan helyzetbe hozhatják a felhasználókat, amely lehetővé teszi, hogy a platformon töltött idő során megalapozott döntéseket tudjanak hozni az online interakcióikról. A tartalom megjelenítésével és személyre szabásával kapcsolatos átláthatóság segít a felhasználóknak eligazodni, tisztán látni a sötét megoldások befolyását illetően, végső soron kiegyensúlyozottabb és sokszínűbb online környezetet elősegítve.

Végezetül fontosnak tartom mind a felhasználók, mind a fejlesztők edukációjára irányuló kezdeményezések támogatását is a sötét megoldásokkal kapcsolatos hatások és kockázatok tudatosítása érdekében. Azáltal, hogy a felhasználók felismerik az alkalmazott technikákat, vélhetően nagyobb eséllyel lesznek képesek minimalizálni a manipulatív technikák miatti, számukra előnytelen döntések számát. A fejlesztők részvétele elősegíthetné a technológiák alkalmazásának egészségesebb és felhasználóközpontúbb megvalósítását is, amennyiben a felhasználók szemszögéből is foglalkoznának a kérdéssel, és a felhasználók függőségére építő technikák helyett éppen ellenkezőleg, a függőség kialakulását meggátoló megoldásokat alkalmaznának.[173] Való igaz, hogy jelenleg a platformok érdeke a függőség kialakításában rejlik, azonban a digitalizációnak és a technológia fejlődésének köszönhetően akarva-akaratlanul is áthelyeződik a hangsúly az offline világról az online térre, így hamar szükségtelenné válhat az olyan technikák alkalmazása, amelyek a függőség elemeit implementálják. A több érdekelt fél részvételével zajló párbeszédek és kezdeményezések révén a különböző nézőpontok felhasználhatók a manipulatív taktikák által támasztott, összetett kihívások kezelésére szolgáló holisztikus megoldások kidolgozásához. Az átláthatóság, elszámoltathatóság és a felhasználók mellett a fejlesztők és platformüzemeltetők szerepvállalásának előmozdítása egyaránt szükséges és elengedhetetlen egy olyan digitális környezet kialakításához, amely a sötét megoldások által jelentett újonnan megjelenő kockázatokkal szemben is fenntartja az alapvető jogok és értékek elsőbbségét.

***

A Kulturális és Innovációs Minisztérium ÚNKP-23-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

173 Uo. i. m. 8.

Platformok felelőssége a szerzői jog megsértéséért

A CDSM irányelv és a DSA közötti kölcsönhatás következményei a szellemi tulajdonjogok védelme szempontjából

Kovács György

1. Háttér

Az Egyesült Államok digitális ezredfordulós szerzői jogi törvénye[1] (Digital Millennium Copyright Act, DMCA) volt az egyik első olyan jogszabály, amely behatóan foglalkozott az internetes közvetítők (*intermediaries*), különösképpen az internetszolgáltatók felelősségének kérdésével és mintaként szolgáló rendelkezéseket alkotott ezen a területen, létrehozva az értesítési és eltávolítási eljárás koncepcióját, amely utóbb hatással volt az Európai Unió elektronikus kereskedelemről szóló irányelvére,[2] valamint az Európai Bíróság joggyakorlatára[3] is, és ennek nyomán a tagállami elektronikus kereskedelemről szóló jogszabályokban szintén megjelent.[4]

1 Digital Millenium Copyright Act. Public Law 105–304., 1998. október 28., https://www.congress.gov/105/plaws/publ304/PLAW-105publ304.pdf

2 2000/31/EK irányelv a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv).

3 Az ideiglenes intézkedések alkalmazási körével és céljaival (jelenlegi jogsértés megszüntetése, jövőbeni megelőzése, megakadályozása) foglalkozott az EUB többek között a C-324/09 L'Oreal [ECLI:EU:C:2011:474] és a C-70/10 Scarlet kontra SABAM [ECLI:EU:C:2011:771]; ügyben is. Kifejezetten a jogsértő tartalomhoz történő hozzáférés blokkolására irányuló ideiglenes intézkedésekkel foglalkozott az EUB a C-314/12 UPC Telekabel ügyben [ECLI:EU:C:2014:192], kimondva, hogy nem kell konkrétnak lennie az ideiglenes intézkedésnek, az ideiglenes intézkedés címzettjének kell megtalálnia a hatékony műszaki megoldást. A C-610/15 Ziggo [ECLI:EU:C:2017:456] és a C-682/18 és C-683/18 YouTube-ügyben [ECLI:EU:C:2021:503] pedig már a közvetítő elsődleges felelősségével foglalkozott az EUB, kimondva, hogy a közvetítő elsődleges felelőssége megállapítható, ha aktívan hozzájárul, elősegíti (pl. aktív tartalomrendezés, hozzáférés elősegítése) a jogsértés megtörténtét.

4 Az EUB következetes gyakorlatában közvetítő alatt az olyan gazdasági szereplőt (*economic operator*) értjük, amelynek a szolgáltatásait használják fel harmadik személyek jogsértésre, tehát nemcsak online szolgáltatásokra terjed ki. Ld. C-494/15 Tommy Hilfiger [ECLI:EU:C:2016:528] és C-484/14 McFadden [ECLI:EU:C:2016:689] ügyeket.

A DMCA és az elektronikus kereskedelemről szóló irányelv[5] alapján a közvetítő mindaddig nem felelős az online jogsértő tartalomért, amíg nincs tudomása a jogsértő tartalomról (*actual knowledge*). Amint azonban tudomást szerez a jogsértő tartalomról, haladéktalanul (*act expeditiously*) el kell távolítania (*take down*), hozzáférhetetlenné kell tennie a jogsértő tartalmat. A közvetítő fogalmát az irányelv és a joggyakorlat is úgy határozzák meg, hogy közvetítő minden olyan gazdasági szereplő, amelynek a szolgáltatásait internetes jogsértésre használják fel. A fogalom rendkívül tág, hiszen magában foglalja az internetszolgáltató mellett a tartalomszolgáltatót, az online platformokat, keresőprogramokat, webáruházakat, de akár marketingszolgáltatás nyújtóit is.

Az internetes jogsértésért való felelősség jogi szabályozását alapvetően formálták az Európai Unióban a DSA és a CDSM irányelv[6] szabályai, és így méltán váltottak ki jelentős jogirodalmi visszhangot.[7] Jelen írás ennek a két jogszabálynak a kölcsönhatását, egymáshoz

5 Elektronikus kereskedelemről szóló irányelv 14. cikk. Tárhelyszolgáltatás.
(1) Ha az információs társadalommal összefüggő olyan szolgáltatásról van szó, amely a szolgáltatás igénybe vevője által küldött információ tárolásából áll, a tagállamok biztosítják, hogy a szolgáltatót ne terhelje felelősség a szolgáltatás igénybe vevőjének kérésére tárolt információért, azzal a feltétellel, hogy:
a) a szolgáltatónak nincsen tényleges tudomása jogellenes tevékenységről vagy információról, és – ami a kárigényeket illeti – nincsen tudomása olyan tényekről vagy körülményekről, amelyek nyilvánvalóan jogellenes tevékenységre vagy információra utalnának; vagy
b) a szolgáltató, amint ilyenről tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról vagy az ahhoz való hozzáférés megszüntetéséről.
(2) Az (1) bekezdés nem alkalmazható arra az esetre, ha a szolgáltatás igénybe vevője a szolgáltató irányítása alatt vagy ellenőrzése mellett jár el.
(3) Ez a cikk nem érinti a bíróságok vagy közigazgatási hatóságok arra vonatkozó lehetőségét, hogy a tagállamok jogrendszereivel összhangban a szolgáltatót a jogsértés megszüntetésére vagy megelőzésére kötelezzék, nem érinti továbbá a tagállamoknak azt a lehetőségét sem, hogy eljárásokat alakítsanak ki az információ eltávolításának vagy a hozzáférés megszüntetésének szabályozására.

6 2019/790/EU irányelv a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, HL L 130, 2019. 05. 17., 92–125. o.

7 Eleonora Rosati: The Digital Services Act and Copyright Enforcement: The Case of Article 17 of the DSM Directive. *IRIS*, 2021/1., különszám, https://su.diva-portal.org/smash/get/diva2:1605131/FULLTEXT01.pdf; Eleonora Rosati: The Legal Nature of Article 17 of the Copyright DSM Directive, the (Lack of) Freedom of Member States and Why the German Implementation Proposal Is Not Compatible with EU Law. *Journal of Intellectual Property Law and Practice*, vol. 15., no. 11 (2020), https://doi.org/10.1093/jiplp/jpaa163; Alexander Peukert et al.: European Copyright Society: Comment on Copyright and the Digital Services Act Proposal, European Copyright Society. *International Review of Intellectual Property and Competition Law,* vol. 53. (2022), https://link.springer.com/article/10.1007/s40319-022-01154-1; European Audiovisual Obsetravtory: *The European Audiovisual Observatory publishes new IRIS Special report: Unravelling the Digital Services Act Package* [Sajtóközlemény]. European Audiovisual Obsetravtory, 2021. október 21. https://www.obs.coe.int/en/web/observatoire/press-releases-2021/-/asset_publisher/alYLDl7HvAtD/content/unraveling-the-digital-services-act-package; Grad-Gyenge Anikó: A tartalommegosztó platformszolgáltatók és más közvetítő szolgáltatók szerzői jogsértésekért való felelőssége a Digital Services Act tükrében. *In Medias Res*, 2023/2., 25–44.; Sunimal Mendis: The Magic Bullet That Isn't! The Limited Efficacy of Article 14 DSA in Safeguarding Copyright Exceptions to Quotation and Parody on Social Media Platforms. *Verfassungsblog*, 2023. május 18. https://verfassungsblog.de/no-magic-bullet; Matthias Leistner: European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge? *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal,* vol. 12., no. 2. (2020) https://doi.org/10.1628/zge-2020-0008; Joao Quintais – Sebastian Schwemer: The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright? *European Journal of Risk Regulation*, vol. 13., no. 2. (2022) https://doi.org/10.1017/err.2022.1; Martin Husovec: The DSA as a Creator's Charter? *Journal of Intellectual Property Law and Practice*, vol. 18., no. 2. (2023) 71–73.; Giancarlo Frosio – Sunimal Mendis: Monitoring and Filtering: European Reform of Global Trend? In: Giancarlo Frosio (szerk.): *Oxford Handbook of Online Intermediary Liability.* Oxford, Oxford University Press, 2020. https://doi.org/10.1093/oxfordhb/9780198837138.013.28

való viszonyát vizsgálja, különös tekintettel a közösségi médiumok gyakorlatára várható hatások szempontjából. A fenti vizsgálat előkérdése, hogy felmerülhet-e a két jogszabály együttes alkalmazása, és amennyiben igen, abból milyen következmények adódnak az együttes alkalmazás szempontjából.

2. A DSA és a CDSM irányelv hatályának kérdése

2.1. A személyi hatály kérdése

A CDSM irányelv viszonya a DSA-hoz első áttekintésre a különös viszonya az általánoshoz (*lex specialis – lex generalis*). A CDSM irányelv az internetes szerzői jogsértésekre (*copyright infringments*) vonatkozóan határoz meg új szabályokat, elsősorban az online tartalommegosztó szolgáltatók szempontjából (Online Content Sharing Service Providers, OCSSP). Ehhez képest a DSA a közvetítőkre vonatkozóan tartalmaz szabályozást. A CDSM irányelv alapján az OCSSP[8] egy információs társadalmi szolgáltatást nyújtó szolgáltató, amely szerzői jog által védett (vagy más védelem alatt álló) tartalmat tárol és hozzáférést biztosít ahhoz a nyilvánosság számára, továbbá ezeket a tartalmakat nyereségszerzési céllal össze is rendezi és promotálja. Az irányelv kiveszi az OCSSP köréből a nonprofit online enciklopédiákat, a nonprofit oktatási és tudományos adatbázisokat, a nyílt forráskódú számítógépes programokat fejlesztő, illetve megosztó platformokat, bizonyos elektronikus hírközlési szolgáltatásokat,[9] online piacterek és vállalkozások közötti felhőalapú szolgáltatásokat, továbbá azon felhőalapú szolgáltatásokat, amelyek alapján a felhasználók saját használatukra töltenek fel tartalmakat.

8 CDSM irányelv 2. cikk, 6. pont.

9 Pontosabban a 2018/1972/EU irányelvben meghatározott elektronikus hírközlési szolgáltatásokat, amelyek az irányelv értelmében olyan, általában díjazás ellenében, elektronikus hírközlő hálózatok révén nyújtott szolgáltatások, amelyek az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások segítségével történő tartalomszolgáltatás, illetve az ilyen tartalom felett szerkesztői ellenőrzést biztosító szolgáltatások kivételével magukban foglalják a következő szolgáltatástípusokat: *a)* a 2015/2120/EU rendelet 2. cikkének (2) bekezdésében meghatározott „internet-hozzáférési szolgáltatást"; *b)* a „személyközi hírközlési szolgáltatást"; és *c)* az olyan szolgáltatásokat, amelyek teljes egészükben vagy nagyrészt jelátvitelből állnak, mint például a gépek közötti szolgáltatások biztosítására és műsorterjesztésre használt átviteli szolgáltatások [2018/1972/EU irányelv az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321, 2018. 12. 17., 36–214. o)., 2. cikk, 4. pont]).

A DSA szerinti 'közvetítő szolgáltatás'[10] (*intermediary services*) fogalma[11] az OCSSP fogalmához képest magában foglalja az egyszerű továbbítást (*mere conduit*), a gyorsítótárazást (*caching*), valamint a tárhelyszolgáltatást (*hosting*). Az OCSSP és a közvetítő szolgáltatás fogalma is az információs társadalmi szolgáltatás fogalmára nyúlik vissza, amelyet a 2015/1535/EU irányelv távolról, az igénybevevő egyéni kérelmére nyújtott elektronikus úton nyújtott szolgáltatásként határozott meg.[12] A DSA szerinti közvetítőfogalom három alkategóriája közül az 'egyszerű továbbítás' és a 'gyorsítótárazás' nem tartalmaz a továbbított tartalommal kapcsolatos összerendezési tevékenységet, továbbá a továbbított információk tárolása a gyorsítótárazás esetében is kizárólag automatikus, közbenső és átmeneti tárolás lehet, amelynek kizárólagos célja, hogy a szolgáltatás későbbi igénybevevői részére történő információ továbbítását azok kérésére *hatékonyabbá* tegye. Az információ nem átmeneti jellegű tárolása mint a szolgáltatás fő célja egyedül a tárhelyszolgáltatás esetén merülhet fel, amely egy rendkívül tág kört ölel fel, ebbe a körbe sorolhatóak például a közösségi oldalak, videómegosztó szolgáltatások és webshopok is.

10 A közvetítő szolgáltatások körében érdemes utalni arra is, hogy az EUB gyakorlatában kialakult és korábban bemutatott 'közvetítő' fogalom alapvetően eltér a DSA szerinti 'közvetítő szolgáltatás' fogalmától. Az EUB gyakorlatában a közvetítő fogalmát definiálja, míg a DSA a közvetítő szolgáltatásra tartalmaz definíciót. Míg az EUB gyakorlatában – többek között a McFadden- és a Tommy Hilfiger-ügyben megfogalmazottak szerint – a közvetítő fogalma a DSA fogalmánál lényegesen lazább fogalom, nemcsak online közvetítők által nyújtott szolgáltatásokra vonatkozik, hanem általánosságban a gazdasági szereplőkre (*economic operator*), akiknek a szolgáltatásait jogsértésre használják fel harmadik személyek, addig a DSA a közvetítő által nyújtott szolgáltatást definiálja, online szolgáltatásokra korlátozva a jelentését.

11 'Közvetítő szolgáltatás': az *információs társadalom* alábbi szolgáltatásainak egyike: (i) 'egyszerű továbbítás': olyan szolgáltatás, amely a szolgáltatás igénybe vevője által küldött információnak hírközlő hálózaton keresztül történő továbbításából vagy a hírközlő hálózathoz való hozzáférés biztosításából áll; (ii) 'gyorsítótárazás': 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; (iii) 'tárhelyszolgáltatás': olyan szolgáltatás, amely a szolgáltatás igénybe vevője által küldött és a szolgáltatás igénybe vevőjének kérésére tárolt információ tárolásából áll [DSA, 3. cikk, *g)* pont]. Az 'információs társadalom szolgáltatása' fogalom meghatározása során a DSA visszautal a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításaira vonatkozó irányelv szerinti definícióra: 'az információs társadalom szolgáltatása': a 2015/1535/EU irányelv 1. cikke (1) bekezdésének *b)* pontjában meghatározott 'szolgáltatás', amely alapján 'szolgáltatás': az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, *távolról*, *elektronikus úton* és a szolgáltatást igénybe vevő *egyéni kérelmére* nyújtott szolgáltatás, amelynek során az egyes fogalmi elemeket a következő módon határozza meg az irányelv: (i) 'távolról' azt jelenti, hogy a szolgáltatást a felek egyidejű jelenléte nélkül nyújtják; (ii) 'elektronikus úton' azt jelenti, hogy a szolgáltatás kezdőpontjától való elküldése és célállomásán való fogadása adatok feldolgozására (beleértve a digitális tömörítést is) és tárolására szolgáló elektronikus berendezés útján történik, valamint annak elküldése, továbbítása és vétele teljes egészében vezetéken, rádión, optikai vagy egyéb elektromágneses eszköz útján történik; (iii) 'a szolgáltatást igénybe vevő egyéni kérelmére' azt jelenti, hogy az adatok továbbításával nyújtott szolgáltatás egyéni kérelemre történik. Az irányelv I. melléklete tartalmazza továbbá azoknak a szolgáltatásoknak a listáját, amelyek nem tartoznak e fogalom alá. Az I. melléklet alapján például nem minősül távolról nyújtott szolgáltatásnak a repülőjegyfoglalás utazási ügynökségnél számítógépes hálózat útján, ha az ügyfél fizikai jelenlétében történik, illetve ugyancsak nem minősülnek elektronikus szolgáltatásnak az olyan szolgáltatások, amelyeket nem elektronikus nyilvántartó rendszerek útján nyújtanak, mint például a telefonos orvosi vagy jogi tanácsadás;

12 2015/1535/EU irányelv a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról, HL L 241, 2015. 09. 17., 1–15. o.

A tárhelyszolgáltatások körében bevezet egy új fogalmat az *i)* pont alatt, az 'online platform' fogalmát olyan tárhelyszolgáltatásként, amely a szolgáltatás igénybevevőjének kérésére információkat tárol és nyilvánosan terjeszt, kivéve, ha ez a tevékenység egy másik szolgáltatás kisebb vagy kizárólag kiegészítő eleme, vagy a fő szolgáltatás kisebb funkcionalitása, amely objektív és technikai okokból nem használható az említett másik szolgáltatás nélkül, és az ilyen elem vagy funkcionalitás másik szolgáltatásba való integrációja nem a DSA alkalmazhatóságának elkerülésére szolgál. Ehhez képest a nagyon nagy online platform fogalmát sokkal részletesebben határozza meg a DSA.

A fentiek alapján tehát az online platform fogalma láthatóan lefedi a CDSM irányelv szerinti OCSSP-k körét, ugyanakkor annál jóval tágabb kört ölel fel.

2.2. A tárgyi hatály kérdése

A CDSM irányelv szabályai a szerzői és szomszédos jogokra vonatkoznak, ehhez képest a DSA esetében nem találhatunk ilyen korlátozást, a DSA célja[13] általánosságban a közvetítő szolgáltatások belső piacának megfelelő működése, biztonságos, megbízható és kiszámítható online környezetre vonatkozó harmonizált szabályok meghatározása, amely elősegíti az innovációt és az Európai Alapjogi Kartában rögzített alapjogok védelme is érvényesül. A DSA külön nevesíti a fogyasztóvédelem elvének hatékony védelmét. Ez a céltételezés a DSA megalkotása kapcsán olyan módon is megfogalmazódott, hogy a DSA célja annak biztosítása, hogy ami jogellenes offline környezetben, az legyen jogellenes online környezetben is. A DSA továbbá kiemeli, hogy a felelősségi szabályok alóli mentesülés keretei, a kellő gondossági kötelezettségek meghatározása, valamint a hatóságok közti együttműködés és koordináció is a DSA tárgyi hatálya alá tartozik.[14] A DSA tárgyi hatálya ez alapján álláspontunk szerint kiterjed az internetes szerzői jogi jogsértésekre, ugyanakkor nemcsak a szerzői jogi jogsértéseket fogja át, hanem más szellemi tulajdonnal kapcsolatos, illetve annál tágabb körben elkövetett internetes jogsértésekre (pl. üzleti titoksértés, álhírterjesztés) ugyancsak kiterjed.

2.3. Az együttes alkalmazás kérdése

Az előzőekből következik, hogy miután a DSA közvetítőfogalma magában foglalja a CDSM irányelv OCSSP-fogalmát, valamint a DSA tárgyi hatálya ugyancsak átfogja az internetes szerzői jogsértéseket is, így a két jogszabály együttes alkalmazására kerülne sor az internetes szerzői jogi jogsértések esetében.

A fentiek alapján világosan látszik, hogy a CDSM irányelv és a DSA egymáshoz való relációja nem jellemezhető egyszerűen a *lex specialis* és a *lex generalis* viszonyaként, hiszen a speciális szabályok nem rontják le adott esetben a DSA szabályait, hanem a DSA általánosabb szabályai inkább kiegészítik komplementer módon a CDSM irányelv szabályait és annál tágabb körben érvényesülnek. Ennek a tételnek a további igazolására törekszünk jelen írás további részeiben is.

13 DSA 1. cikk (1) bekezdés.
14 DSA 1. cikk (2) bekezdés.

3. A CDSM irányelv és a DSA felelősségi szabályai

3.1. A felelősség alóli mentesülés kérdése a CDSM irányelv 17. cikke alapján

A CDSM irányelv 17. cikke tartalmazza az OCSSP internetes szerzői jogi jogsértésekért fennálló felelősségének szabályait.[15]

A rendelkezést számos kritika érte[16] annak túlzottan bonyolult, kazuisztikus, adott esetben az irányelv más rendelkezéseinek, valamint az Alapjogi Kartának is ellentmondó[17]

15 A CDSM irányelv 17. cikkelyét érintően már a megalkotásának első két évében is számos jogirodalmi reflexió született. Ld. Leistner i. m.; Axel Metzger et al.: Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law – Comment of the European Copyright Society. *SSRN Electronic Journal*, 2020. április 27. https://papers.ssrn.com/abstract=3589323; Sebastian Felix Schwemer: Article 17 at the Intersection of EU Copyright Law and Platform Regulation. *Nordic Intellectual Property Law Review*, 2020/3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3627446; Thomas Spoerri: On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 10., no. 2. (2019), https://www.jipitec.eu/jipitec/article/view/253; Giancarlo Frosio: Reforming the C-DSM Reform: A UserBased Copyright Theory for Commonplace Creativity. *IIC – International Review of Intellectual Property and Competition Law*, vol. 51., no. 6. (2020) https://doi.org/10.1007/s40319-020-00931-0; Maxime Lambrecht: Free Speech by Design – Algorithmic Protection of Exceptions and Limitations in the Copyright DSM Directive. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 11., no. 1. (2020), https://www.jipitec.eu/jipitec/article/view/272; Gerald Spindler: The Liability System of Art. 17 DSMD and National Implementation – Contravening Prohibition of General Monitoring Duties? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* vol. 10., no. 3. (2020), https://www.jipitec.eu/jipitec/article/view/265; Krzysztof Garstka: Guiding the Blind Bloodhounds: How to Mitigate the Risks Art. 17 of Directive 2019/790 Poses to the Freedom of Expression. In: Paul L. C. Torremans (szerk.): *Intellectual Property Law and Human Rights* [Negyedik kiadás]. Alphen aan den Rijn, Kluwer Law International, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3471791; Jan Bernd Nordemann – Julian Waiblinger: Art. 17 DSM-RL – Spannungsverhältnis Zum Bisherigen Recht? *Gewerblicher Rechtsschutz und Urheberrecht*, vol. 122., no. 6. (2020); Martin Husovec – João Pedro Quintais: How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive. *GRUR International*, 2021/4.; Martin Husovec – João Quintais: Too Small to Matter? On the Copyright Directive's Bias in Favour of Big Right-Holders. In: Tuomas Mylly – Jonathan Griffiths (szerk.): *Global Intellectual Property Protection and New Constitutionalism. Hedging Exclusive Rights*. Oxford, Oxford University Press, 2021.

16 Martin Husovec: (Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement. *SSRN Online Journal,* 2021. szeptember 17. https://papers.ssrn.com/abstract=3784149; Christophe Geiger – Bernd Justin Jütte: Platform Liability Under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match. *GRUR International*, vol. 70., no. 6. (2021), https://doi.org/10.1093/grurint/ikab037; a CDSM 17. cikkével kapcsolatos bizottsági iránymutatás, 2021. 06. 04., COM/2021/288 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0288; Paul Keller: Article 17: (Mis)Understanding the Intent of the Legislator. *Kluwer Copyright Blog*, 2021. január 28. http://copyrightblog.kluweriplaw.com/2021/01/28/article-17-misunderstanding-the-intent-of-the-legislator/; Paul Keller: Article 17 Stakeholder Dialogue: What We Have Learned so Far – Part 1. *Kluwer Copyright Blog*, 2020. január. 13. http://copyrightblog.kluweriplaw.com/2020/01/13/article-17-stakeholder-dialoguewhat-we-have-learned-so-far-part-1/; Paul Keller: Article 17 Stakeholder Dialogue: What We Have Learned so Far – Part 2. *Kluwer Copyright Blog*, 2020. január 14. https://copyrightblog.kluweriplaw.com/2020/01/14/article-17-stakeholder-dialogue-what-we-have-learned-so-far-part-2/

17 C-401/19 sz. ügy Lengyel Köztársaság kontra Európai Parlament és Tanács[ECLI:EU:C:2022:297].

jellege miatt. Az Európai Bíróság ugyanakkor rámutatott, hogy a CDSM irányelv 17. cikke nem sérti az Alapjogi Kartát, tartalmazza az érintett konkuráló alapjogok megfelelő helyes egyensúlyát, amely révén biztosítható a 17. cikk felelősségi szabályainak alapjogi összhangja, és általános monitoringkötelezettséget[18] sem ír elő az OCSSP-k számára. Fontos megjegyezni, hogy a jogirodalomban a magas szintű gondossági kötelezettséget előíró rendelkezéseket értelmezték úgy, hogy azok csak egy általános monitoringtevékenység fenntartása esetén teljesíthetők, azonban az Európai Bíróság világossá tette, hogy ilyen kötelezettséget a CDSM irányelv nem ír elő.[19]

A CDSM irányelv 17. cikk (4) bekezdésének rendelkezése egyfelől tartalmazza a klasszikus értesítési és eltávolítási eljárás (*notice and take down*) rendelkezéseit, másfelől pedig egy gondossági kötelezettséget (*due diligence*) ír elő az OCSSP-k számára, a jogellenes tartalmakkal szembeni folyamatos észszerű intézkedések megtétele és a már eltávolított jogellenes tartalmak újbóli feltöltésének magakadályozása érdekében (*stay down*).

A 17. cikk (4) bekezdés rendelkezésének a kiindulópontja, hogy az OCSSP nyilvánossághoz közvetítést végez azáltal, hogy szerzői jog vagy valamely szomszédos jog által védett műhöz a nyilvánosság számára hozzáférést biztosít, amelyhez szükséges a szerzői jog vagy szomszédos jog jogosultjának az engedélye. Engedély hiányában ugyanakkor felelősséggel tartozik az OCSSP, kivéve, ha bizonyítja, hogy minden tőle telhetőt megtett a szerzői jog jogosultja vagy a licenctulajdonos engedélyének megszerzése érdekében (*due diligence*). A 17. cikk (4) bekezdése ugyancsak előírja, hogy az OCSSP azon művek esetében, amelyeket illetően értesítést kapott a jogosulttól, ott haladéktalanul intézkedett az adott mű(vek) elérhetetlenné tétele érdekében. Ugyancsak fontos tényállási elem, hogy amennyiben az OCSSP értesítést kapott jogellenes tartalomról, abban az esetben haladéktalanul intézkedett a jogellenes tartalom eltávolítása vagy hozzáférhetetlenné tétele érdekében (*notice and take down*). Ehhez tartozó gondossági kötelezettséget tartalmaz a 17. cikk (4) bekezdésének negyedik eleme, amelynek értelmében a már eltávolított jogellenes tartalom esetében az OCSSP köteles kellő gondossággal eljárni, minden tőle telhetőt megtenni annak érdekében, hogy a jogellenes tartalom jövőbeni feltöltését megakadályozza (*stay down*).

18 Már az elektronikus kereskedelemről szóló irányelv 15. cikke is tiltotta a szolgáltatókat terhelő általános monitoring kötelezettség előírását a tagállamok számára: (1) A tagállamok nem állapítanak meg a szolgáltatókat terhelő olyan általános kötelezettséget, amely szerint a 12., 13. és 14. cikk hatálya alá tartozó szolgáltatások nyújtása során az általuk továbbított vagy tárolt információkat nyomon kellene követniük, sem olyan általános kötelezettséget, amely szerint jogellenes tevékenységre utaló tényeket vagy körülményeket kellene kivizsgálniuk. (2) A tagállamok az információs társadalommal összefüggő szolgáltatások nyújtói számára megállapíthatnak olyan kötelezettségeket, amelyek szerint azonnal tájékoztatniuk kell az illetékes közigazgatási hatóságokat a szolgáltatásuk igénybe vevői által folytatott, jogellenesnek vélt tevékenységekről vagy nyújtott információkról, illetve olyan kötelezettségeket, amelyek szerint az illetékes hatóságokkal, azok kérésére, közölniük kell azokat az adatokat, amelyek lehetővé teszik szolgáltatásuk olyan igénybe vevőinek azonosítását, akikkel, illetve amelyekkel adattárolási megállapodásaik vannak.

19 Ezen a ponton érdemes megemlíteni, hogy a CDSM irányelv átültetése semmiképp sem tekinthető problémamentesnek. Ld. bővebben például: Lábody Péter: Hogy is áll az uniós szerzői jogi reform tagállami átültetése? *ITKI blog*, 2021. július 21. https://www.ludovika.hu/blogok/itkiblog%20/2021/07/21/hogy-is-all-az-unios-szerzoi-jogi-reform-tagallami-atultetese/

3.2. Az arányosság alapjogi szintű követelményének érvényesülése a CDSM irányelv 17. cikkében

Az EUB gyakorlatában a szellemi tulajdonjogok érvényesítésének szabályait következetesen a konkuráló alapjogok kontextusában, azokkal egyensúlyban alakították ki[20]. Fontos alapelv, hogy a szellemi tulajdonjogok érvényesítése nemcsak hatékony (*effective*), visszatartó erővel bíró (*dissuasive*), hanem kiegyensúlyozott (*balanced*) is kell, hogy legyen, megtalálva a helyes egyensúlyt a konkuráló alapjogok között, ahol a tulajdonjog a magánszférához való jog, a vállalkozás szabadságához való jog és a véleménynyilvánítás szabadsága kontextusában érvényesül.

Ennek során a véleménynyilvánítás szabadsága csak akkor korlátozható, ha az szükséges és arányos az elérni kívánt cél érdekében, amit az EUB legutóbb a 17. cikkel kapcsolatos eljárásban vizsgált és arra az eredményre jutott, hogy nem aránytalan a korlátozás, adott esetben az Alapjogi Karta 11. cikkének korlátozása igazolt a szerzői jog érvényesítése érdekében.[21] Az EUB egészen pontosan hat fontos garanciát azonosított a 17. cikkben, amelyek az arányosság elvének érvényesülését biztosítják, és amelyek megfelelő átültetése a tagállamok szempontjából kulcsfontosságú, nem megfelelő átültetésük a jövőben kötelezettségszegési eljárások forrása lehet; így különös tekintettel a DSA miatt is megfigyelhető szűkülő mozgástérre leginkább a pontos, a 17. cikkely szövegéhez hű implementáció látszott célravezetőnek.

A 17. cikk (7) bekezdése szerint az arányosság (*proportionality*) alapjogi követelménye magában foglal fontos intézményi garanciákat, amelyek a túlzott szankciókkal[22] (*overenforcement*) szembeni fellépéssel szemben védenek, ennek a követelménynek való megfelelés szempontjából kiemelt jelentőségű rendelkezéseket tartalmaz a (7) bekezdés, amikor előírja, hogy az egyes szerzői jogi kivételek[23] alá eső esetkörök esetén nem alkalmazható a 17. cikk (4) bekezdése

20 C-275/06 Promusicae [ECLI:EU:C:2008:54]; C-557/07 LSG-Gesellschaft [ECLI:EU:C:2009:107]; C-461/10 Bonnier [ECLI:EU:C:2012:219]; C-324/09 L'Oreal kontra eBay [ECLI:EU:C:2011:474]; C-314/12 Telekabel [ECLI:EU:C:2013:781]; C-160/15 GS Media [ECLI:EU:C:2016:221]; C-527/15 Filmspeler [ECLI:EU:C:2017:300]; C-610/15 Stichting Brein kontra Ziggo [ECLI:EU:C:2017:456]; C-682/18, C-683/18 YouTube [ECLI:EU:C:2021:503]; C-18/18 Eva Glawischnig-Piesczek kontra Facebook [ECLI:EU:C:2019:821]; C-567/18 Coty [ECLI:EU:C:2020:267]; C-753/18 Stim and Sami [ECLI:EU:C:2020:26.8].

21 C-401/19 Lengyel Köztársaság kontra Európai Parlament és Tanács [ECLI:EU:C:2022:297] 84. pont.

22 Kris Erickson – Martin Kretschmer: Empirical Approaches to Intermediary Liability. *CREATe Working Paper,* 2019/6., 2019. október 4. https://www.create.ac.uk/blog/2019/10/04/new-working-paper-empirical-approaches-to-intermediary-liability/; Jennifer Urban – Joe Karaganis – Brianna Schofield: Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice. *Journal of the Copyright Society*, 2017.szeptember 28. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126401; Sharon Bar-Ziv – Niva Elkin-Koren: Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown. *Connecticut Law Review*, vol. 50., no. 2. (2018), https://digitalcommons.lib.uconn.edu/cgi/viewcontent.cgi?article=1395&context=law_review; Kris Erickson – Martin Kretschmer: This Video Is Unavailable: Analyzing Copyright Takedown of User-Generated Content on YouTube. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 9., no. 1. (2018), https://www.jipitec.eu/jipitec/article/view/218; Sabine Jacques – Krzysztof Garstka – Morten Hviid – John Street: An Empirical Study of the Use of Automated Anti-Piracy Systems and Their Consequences for Cultural Diversity. *SCRIPTed*, vol. 15., no. 2. (2018); Daphne Keller – Paddy Leerssen: Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation. In: Nathaniel Persily – Joshua A. Tucker: *Social Media and Democracy: The State of the Field and Prospects for Reform*. Cambridge, Cambridge University Press, 2019. https://papers.ssrn.com/abstract=3504930

23 Nevesítve: idézés (*quotation*), kritika (*criticism*), ismertetés (*review*); karikatúra (*caricature*), paródia (*parody*) vagy utánzat (*pastiche*).

szerinti korlátozás, és ezekről a kivételekről a felhasználókat tájékoztatnia kell az OCSSP-nek a 17. cikk (9) bekezdése alapján.[24] A 17. cikk (8) bekezdése az elektronikus kereskedelemről szóló irányelv 15. cikkéhez és a DSA 8. cikkéhez hasonlóan az *általános* nyomonkövetési (*monitoring*) kötelezettség tilalmát tartalmazza, amely alapján külön kérdésként merül fel a jövőre nézve a megengedett mértékű nyomonkövetési kötelezettség határainak a kijelölése.

A nagy platformok, közösségi médiumok, videómegosztó oldalak automatikus tartalomfelismerő rendszerét már több éve jól ismert módon alkalmazzák jogellenes tartalmak kiszűrése céljából. Fontos hangsúlyozni, hogy a 17. cikk (9) bekezdéseiből az is következik, hogy nem hagyatkozhat az OCSSP kizárólag az automatikus, algoritmusvezérelt tartalomfelismerő és tartalommoderáló rendszerekre, hanem lehetővé kell tennie a humán, emberi felülvizsgálat lehetőségét, és a bírói úton történő jogorvoslatot. A szükségesség és arányosság alapjogi követelményéből adódóan, a 17. cikk (7)–(9) bekezdései megelőzik a (4) bekezdés rendelkezéseit, és a (4) bekezdés szerinti kötelezettségeknek a tagállamok úgy kell, hogy eleget tegyenek, hogy közben megfelelnek a (7)–(9) bekezdések, valamint az Alapjogi Karta 17. cikk szabályainak is.

3.3. A DSA felelősségi szabályai

Az OCSSP szabályaihoz képest a DSA 5. cikkében rögzített tárhelyszolgáltatói felelősség szabályozása inkább hasonló az elektronikus kereskedelemről szóló irányelv 14. cikkének a szabályaihoz, ugyanis az értesítési és eltávolítási eljárást az irányelv már lényegében hasonló szövegezéssel tartalmazta. A DSA 5. cikkéhez képest ugyanakkor a CDSM irányelv 17. cikk (4) bekezdése speciális jogszabálynak minősül, emiatt szerzői jogi jogsértések esetén a DSA 5. cikke helyett, a CDSM irányelv 17. cikk (4) bekezdése lesz alkalmazandó.

Felmerül a kérdés, hogy a DSA által meghatározott többi kötelezettség esetében a CDSM irányelv specialitása miatt úgyszintén a CDSM irányelv rendelkezései érvényesülnek, vagy ezekben az esetekben a DSA rendelkezései alkalmazandóak? Figyelemmel a DSA Preambulumának 11. bekezdéseire, valamint a DSA 2. cikk (4) bekezdés *b)* pontjára, azokban az esetekben, ahol a DSA szabályainak megfeleltethető szabályozást nem vagy nem teljeskörűen tartalmazza a CDSM irányelv, ott a DSA szabályai komplementer módon érvényesülnek. Ezeknek a szabályoknak a részletes bemutatása meghaladná jelen írás kereteit, ugyanakkor a teljesség érdekében ezekre a későbbiekben érintő jelleggel kitérünk.

A fentieken túl a CDSM irányelv és a DSA jogforrási különbözőségére is fontos figyelemmel lenni, ugyanis ebből adódik, hogy míg a DSA homogén szabályozást hoz létre a tagállamokban, addig a CDSM irányelv esetében bizonyos mértékig eltérő implementációval szükséges számolnunk a 17. cikk tekintetében is az egyes tagállamokban. A tagállami implementáció során ugyanakkor a tagállamoknak figyelembe kellett venniük, hogy a CDSM irányelv implementációja során nem sérülhettek a DSA rendelkezései. Ilyen rendelkezések többek között a platform-vitarendezési fórum, az alternatív vitarendezési fórum kialakítása és a különböző gondossági, tájékoztatási és jelentéstételi kötelezettségek szabályozása a DSA-ban.

24 Hasonló megközelítéssel az EUB esetjogában már korábban felhasználói jogokként hivatkozott a szerzői jogi kivételekre: C-117/13 Ulmer [ECLI:EU:C:2014:2196], C-469/17 Funke Medien [ECLI:EU:C:2019:623], C-516/17 Spiegel Online [ECLI:EU:C:2019:625].

3.4. A DSA komplementer érvényesülő rendelkezései

Ahogyan korábban kiemeltük, a DSA azon rendelkezéseinek tekintetében, amelyeknél kifejezetten nem tartalmaz párhuzamos szabályozást a CDSM irányelv, ott a DSA szabályai érvényesülnek az OCSSP-k számára is kötelező módon.

Ilyen szabályoknak tekinthetőek különösen a DSA 14–32. cikkei, elsősorban az éves jelentéstételi kötelezettség (15. és 24. cikk), a panaszkezelés, megbízható és visszaélésszerű bejelentések kezelésére vonatkozó szabályok (14., 20–23. cikk), hatóságokkal való együttműködés (9–10. cikk), elektronikus kapcsolattartási pontok (12. cikk), jogellenes tartalom észlelése esetén történő fellépés szabályai (16–17. cikk), kiskorúak védelme (28. cikk), bűncselekmény észlelése esetén történő fellépés szabályai (18. cikk), megtévesztő manipulatív online interfész[25] tilalma (*dark patterns*, 25. cikk), kereskedők nyomonkövetése és fogyasztók tájékoztatása (30–32. cikk), kiskorúak védelme (18. cikk), ajánlórendszerek átláthatósága (27. cikk), hirdetésekkel kapcsolatos rendelkezések (26. cikk), mentességek (19. és 29. cikk), valamint a szankciórendszer (52.–54. cikk) szabályai.

A fentieken túl – ahol a DSA 33. cikkében meghatározott jogszabályi feltételek fennállnak – ugyancsak alkalmazandók természetesen a DSA 34–43. cikk közti, nagyon nagy online platformokra vonatkozó külön szabályok is az OCSSP-k esetében. Itt különösen kiemelést érdemelnek a kockázatértékelésre (34. cikk), kockázatcsökkentésre (35. cikk), valamint a válságreagálási mechanizmusra (36. cikk) vonatkozó szabályok.

4. Következtetések

A CDSM irányelv speciális, szerzői jogra vonatkozó szabályozást tartalmaz a DSA általános, horizontális szabályaihoz képest. A CDSM irányelv 17. cikk (4) bekezdésének szabálya speciális a DSA 5. cikkének tárhelyszolgáltatói felelősségi szabályához képest, ezért szerzői jogi jogsértések esetén a DSA 5. cikkének szabályozása helyett a 17. cikkely szabályai válnak alkalmazandóvá. Ezt a következtetést támasztja alá a DSA (11) preambulumbekezdése és a 2. cikk (4) bekezdés *b)* pontja is.

Fontos különbség adódik a két jogszabály eltérő jogforrási jellegéből is, míg a CDSM irányelv tagállami érvényesülését befolyásolja az eltérő tagállami implementáció, a különböző jogalkotási megoldások révén történt átültetés, addig a DSA – rendeleti jellegéből adódóan – egyformán érvényesül valamennyi tagállamban.

A DSA gondossági kötelezettséget előíró részletes szabályai kiegészítik a CDSM irányelv szabályait, így ezeken a területeken szűkült a tagállamok mozgástere a CDSM irányelv átültetése során.

Az OCSSP-nek minősülő online platformok számára kiemelt jelentősége van annak, hogy szerzői jogi jogsértések esetén egyaránt a CDSM irányelv és a DSA szabályainak is biztosí-

25 Részletesebben: The Norwegian Consumer Council: Deceived By Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. *Forbrukerradet.no,* 2018. június 27. https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf; EDPB: *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them. Version 2.0.* 2023. február 24. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

taniuk kell a megfelelést. Közösségi médiumok, videómegosztó szolgáltatások már hosszabb ideje alkalmaznak tartalomfelismerő algoritmusokat, amelyek automatizált döntéshozatalra képesek a jogsértő tartalom felismerése esetén. Fontos garanciális szabálya a CDSM irányelvnek és a DSA-nak, hogy az online platformoknak biztosítaniuk kell a humán felülvizsgálat lehetőségét az automatizált döntéshez képest.

A konkuráló alapjogok kontextusában az online platformok kiemelt feladata, hogy biztosítsák a véleménynyilvánításhoz való jog, a magánszférához való jog és a vállalkozás szabadságának érvényesülését is. Ennek során a CDSM irányelv és a DSA arányos, kiegyensúlyozott jogérvényesítést előíró garanciális szabályai kiemelt jelentőséghez jutnak, növelik a jogbiztonságot és megerősítik a szellemi tulajdonjogok online érvényesítésének eszköztárát a tagállamokban.

Összefoglalók / Abstracts

#áldás vagy #átok?

– avagy a közösségi média társadalmi hatásainak vizsgálata

Szakálné Szabó Zita

A 21. században a közösségi média teljesítette ki az internetet, és mint egy hatalmas virtuális állam, saját maga határozza meg a követendő normáit, maga értelmezi saját tartalmát, az azzal kapcsolatos döntéseket és azok későbbi esetleges felülvizsgálatát. Tehát mondhatjuk, hogy a részvétel kultúrájában a közösségi média egyértelműen a legmeghatározóbb kommunikációs eszközzé nőtte ki magát. De miként vonhatja be inkább a közügyekbe a társadalmat ez az új médiakörnyezet, mint azt a 'régi' média tette? És milyen lehetőségek rejlenek a közösségi médiában, azokat pedig a társadalmi változásokban hogyan és miképpen lehet előre mozdítani? Végső soron áldás vagy átok a társadalmi változásokban a közösségi média léte, figyelembe véve, hogy a közösségi média platformjainak megjelenése óta azok társadalmi mozgalmakat szervező és kiváltó szerepe folyamatos vita tárgyát képezi, és nemegyszer a történések középpontjába került már? A közösségi oldalak leginkább egy hatalmas virtuális államra hasonlítanak, és fejlődésükben megjelenésük óta sincs egyetlen pillanatra sem megállás. Nagyon nehéz megjósolni, hogy a rohamléptekkel való fejlődés milyen irányba tart, és ugyanakkor jogi szabályozására is általában jellemző, hogy a bekövetkező változásokat pár lépéssel lemaradva követi. A közösségi média a kibertér által biztosított lehetőségeknek köszönhetően a társadalmi folyamatokban nagyon fontos szerepet játszik, gondoljunk csak a vezetők és kormányzatok világszerte alkalmazott digitális platformokon való megnyilvánulásaira, vagy éppen a világon zajló – és a közösségi médiában közvetített – fegyveres konfliktusok frontjairól történő első kézből való tájékoztatásokra.

#blessing or #curse?

A study of the social impact of social media

In the 21st century, social media has filled the Internet, and as a huge virtual state, it sets its own standards to follow, interpreting its own content, making decisions about it and their possible subsequent review. So we can say that in the culture of participation, social media has clearly grown into the most decisive means of communication. But to what extent can this new media environment serve more to engage society in public affairs than the *old* media did? And what is the potential of social media, and how can it be promoted in social changes? In the end, the existence of social media is a blessing or a curse in social change, given that since the emergence of the social media platforms, their role in organizing and triggering social movements has been the subject of constant debate and has often been the focus of events. Social networks mostly resemble a huge virtual state, and their development has not stopped for a single moment since their appearance. It is very difficult to predict the direction in which the development will take, and at the same time its legal regulation is generally

characterized by the fact that it follows changes a few steps behind. Social media plays a very important role in social processes because of the possibilities provided by cyberspace, let's just think of the manifestations of leaders and governments around the world on digital platforms, or first-hand information on the fronts of armed conflicts taking place in the world – and broadcast on social media.

A becsülethez és jóhírnévhez való jog megsértése a közösségi platformokon

Vitkovics Bálint

A digitális technológiai forradalom jelentős hatást gyakorol a mindennapi életünkre; többek között a hagyományos kommunikációs formák is számottevően megváltoztak. Ezzel összefüggésben tanulmányunkban arra a kérdésre kerestük a választ, hogy a hazai bírói gyakorlatban a közösségi platformokon elkövetett személyiségi jogi sérelmek megítélése hogyan alakult a becsülethez és jóhírnévhez fűződő jog vonatkozásában.

E kérdés megválaszolása érdekében egyrészről foglalkoztunk a platform jogi fogalmával, a magyar közösségiplatform-használati szokásokkal, másrészről röviden ismertettük a vonatkozó jogszabályi környezetet, valamint az alkotmánybírósági és bírósági gyakorlatot.

Kutatásunk eredményeként arra a megállapításra jutottunk, hogy az ítélkezési gyakorlatban a vizsgált időszakban nem volt észlelhető éles határvonal az offline, illetve online térben elkövetett jogsértések között, azonban bizonyos sajátosságok kimutathatóak voltak, különös tekintettel a relatív vagy korlátozott nyilvánosság kérdéskörére, és ezek formálódó joggyakorlatban jelentkező hatására.

Violation of the right to honour and reputation on social media platforms

The digital technology transition is having a major impact on our daily lives – including a significant change in traditional forms of communication. In this context, this paper sought to answer the question of how the Hungarian judicial case law has changed in relation to the assessment of personality rights violations, namely the violation of right to integrity and reputation, committed on different social platforms.

In order to answer this question, on the one hand, we dealt with the legal concept of the platform and the Hungarian habits of using social platforms, and on the other hand, we briefly described the relevant legal framework, constitutional court and judicial case law.

As a result of our research, we came to the conclusion that in the Hungarian case law of the period under review there was no sharp dividing line between offline and online infringements, but certain specific features, in particular the question of relative or limited publicity, were identifiable and had an impact on the evolving jurisprudence.

A közösség elleni uszítás jogalkalmazási gyakorlata

Botos Mihály

A közösség elleni uszítás a véleménynyilvánítás szabadságának korlátja. Ennek köszönhetően foglalkozott elsőként a rendszerváltozás után felállított Alkotmánybíróság a tényállás alkotmányos büntetőjogi megítélésével. A 30/1992. (V. 26.) AB határozatban a testület fontos – a mai jogalkalmazásra is kiható – megállapításokat tett a véleményszabadság tartalmára, valamint a közösség elleni uszítás (akkor izgatás) elkövetési magatartásra vonatkozóan. A jogalkalmazási gyakorlat azonban 1992 és 2008 között oda fejlődött, hogy a tényállás gyakorlatilag alkalmazhatatlanná vált, hiszen végérvényesen eredménybűncselekményt kreált egy absztrakt veszélyeztető tényállásból.

A tanulmány a közösség elleni uszítás jelenlegi jogalkalmazási gyakorlatát dolgozza fel, amelyben vizsgálja, hogy a gyakorlat tekintettel volt-e az Alaptörvény negyedik módosítására, valamint a 2016-os Btk. módosítására. Az Alaptörvény negyedik módosítása a véleménynyilvánítás explicit korlátjaként deklarálta a közösségek méltóságát, amely a gyűlöletbeszéd büntetőjogi korlátozás legitimálásának alkotmányos alapját is jelenti. A 2016-os Btk. módosításnak köszönhetően egyértelművé vált, hogy a gyűlöletre uszítás és az erőszakra uszítás nem azonos fogalmak. Ennek alapján vizsgálom, hogy a jogalkalmazási gyakorlat differenciálja-e az elkövetési magatartásokat és miként értelmezi azokat, továbbá, hogy a gyakorlatban a közösség elleni uszítással összefüggésben mely védett csoportok merülnek fel, valamint, hogy a nyomozóhatóságok milyen szempontokat mérlegelnek a védett csoporti minőség megállapításánál. Az elemzett határozatokból kitűnik, hogy a közösség elleni uszítást legtöbbször online platformokon követik el. Ennek alapján vizsgálom, hogy az online térben közzétett inkriminált megnyilvánulások mennyiben hozhatók összhangba a nyilvánvaló és közvetlen veszély mércéjével, valamint e mércét a jogalkalmazó szervek milyen szempontok alapján mérlegelik.

The practice of incitement against a community

Incitement against a community is a restriction on freedom of expression. This is why the Constitutional Court, established after the change of regime, was the first to deal with the constitutional criminal law assessment of this issue. In its Decision No 30/1992 (26 May 1992), the Constitutional Court made important findings – which also affect the application of the law today – on the content of freedom of expression and the incitement against a community (then incitement). However, between 1992 and 2008, the legal practice developed to the point where the regulation of incitement became practically inapplicable, since it definitively created an offence with a result from an abstract threatening offence.

The study reviews the current legal practice of incitement against a community, examining whether this practice has taken the Fourth Amendment of the Fundamental Law and the 2016 amendment of the Criminal Code into account. The Fourth Amendment of the Fundamental Law declared the dignity of communities as an explicit limit to the expression of opinion, which is also the constitutional basis for legitimising the criminalisation of hate speech. The 2016 amendment to the Criminal Code clarified that incitement to hatred and

incitement to violence are not identical concepts. On this basis, I will examine whether and how legal practice differentiates between the offences and how they are interpreted, which protected groups arise in practice in connection with incitement against a community, and what criteria are taken into account by the investigating authorities when determining the protected group status. The decisions analysed show that most incitements against a community are committed on online platforms. As a consequence, I will examine to what extent incriminated expressions posted in the online space can be brought in line with the standard of manifest and imminent danger and what criteria are used by law enforcement authorities to assess this standard.

Botok a közösségi médiában

Kovács Andrea

A közösségi média tereit nemcsak természetes és jogi személy felhasználók töltik be, hanem olyan automatizált fiókok is, amelyek csak kis részben vagy egyáltalán nem igényelnek emberi beavatkozást. Jelenlétük leginkább negatív kontextusban kerül a figyelem középpontjába: a szakirodalom már vizsgálta tevékenységüket választások idején, illetve különböző dezinformációs kampányokban. A tanulmány feszegeti a botokkal kapcsolatban a szólásszabadság egyes kérdéseit Tim Wu Legfelső Bírósági ítéletekhez igazított tesztjével, illetve megvizsgálja a közösségi médiában tevékenykedő botokra adott egyes szabályozói válaszokat az Egyesült Államokból – a kaliforniai kereskedelmi kódexet, illetve a végül el nem fogadott Bot Disclosure and Accountabilty Actet –, az Európai Unióból a dezinformáció visszaszorítását célzó uniós gyakorlati kódexet, valamint a digitális szolgáltatások egységes piacáról szóló rendeletet. Vizsgálat alá kerülnek a Meta, az X/Twitter és a TikTok botokra leginkább vonatkoztatható közösségi irányelvei. Összefoglalásként a tanulmány kiemeli a közös pontokat és felvet néhány szempontot, amelyeket a botok további szabályozásához érdemes lenne figyelembe venni.

Bots on social media

Social Media spaces are not only inhabited by natural and legal persons, but automated accounts as well. These accounts do not or barely require human intervention in their operation. Bots are mentioned mostly in negative context: their operation during elections are questionable and they often take part in disinformation campaigns. This study discusses some questions regarding bots and freedom of speech, using Tim Wu's test, that was created for machine speech and that uses the Supreme Court's case law. Some regulations are examined as well: the Californian Business and Professional Code and the Bot Disclosure Accountability Act from the United States, the voluntary Code of Practice on Disinformation and the Digital Services Act from the European Union. The applicable community guidelines of Meta, X/Twitter and TikTok are examined as well. As summary, this study highlights the common concepts of these regulations and offers some points which should be taken into account when regulating bots.

Adatvédelem az online platformokon

Bálint János

A digitális korszakban az online platformok az információáramlás, a kereskedelem és a társadalmi interakciók középpontjába kerülve jelentős mennyiségű személyes adatot gyűjtenek és kezelnek. Jelen tanulmány a platformok kettős természetét vizsgálja: miközben számos előnnyel járnak, mint például a politikai kampányok és az innovatív termékek elősegítése; a cenzúra, a visszhangkamrák és a tisztességtelen kereskedelmi gyakorlatok kockázatát is magukban hordozzák – mindezt az interakciók és tranzakciók óriási száma alapján történő növekvő személyre szabottságra alapozva. A Cambridge Analytica-botrány, a Brexit- és a Trump-kampányok, valamint a Covid19-világjárvány és az orosz–ukrán háború idején folyó dezinformáció mind a szabályozási beavatkozás szükségességére világítanak rá. Az EU általános adatvédelmi rendelete (GDPR) alapvető jelentőségű a platformok növekedése és az innováció, valamint az egyének magánéletének védelme közötti egyensúly megteremtésében. A kulcsfontosságú területeken azonban továbbra is vannak kihívások, mint például a tájékozott hozzájárulás, az átláthatóság és az adattakarékosság biztosítása.

Jelen tanulmány a technológiai óriások GDPR-megfelelőségét vizsgálja, három területre összpontosítva: a felhasználói hozzájárulás megszerzése, az adatkezelési gyakorlatokról való egyértelmű tájékoztatás, valamint a beépített és alapértelmezett adatvédelmi funkciók megvalósítása. A GDPR rendelkezéseinek legelterjedtebb megsértéseit a Google, a Meta és a TikTok platformok üzemeltetőivel szembeni jogi eljárások és jelentős bírságok szemléltetik, melyet az adatvédelmi hatóságok iránymutatásainak elemzése egészít ki. Az elemzés különös figyelmet fordít a gyermekek adatainak védelmére, példákkal illusztrálva a fiatal felhasználók védelmét elmulasztó platformokkal szemben hozott szabályozási intézkedéseket.

A tanulmány kitér az EU jelenlegi digitális szabályozásának tágabb értelemben vett következményeire is, rámutatva arra, hogy a szigorú adatvédelmi jogszabályok akaratlanul is előnyben részesíthetik a nagy, erőforrásgazdag technológiai vállalatokat, elfojtva a versenyt. Az adatvédelem és a versenyjog konvergenciája, amelyet az európai digitális piacokról szóló jogszabály (DMA) is példáz, ezeket a problémákat kívánja kezelni azáltal, hogy további kötelezettségeket ró a 'kapuőr-platformokra'. A generatív mesterségesintelligencia-technológiák megjelenése tovább bonyolítja a szabályozási környezetet, ami az adatvédelmi elvek folyamatos kiigazítását és érvényesítését teszi szükségessé a felhasználók magánéletének és jogainak hatékony védelme érdekében.

Data protection on online platforms

In the digital era, online platforms have become central to information flow, commerce, and social interactions, collecting and processing significant amounts of personal data. This study explores the dual nature of these platforms: while offering numerous benefits, such as facilitating political campaigns and innovative products, they also pose risks of censorship, echo chambers and unfair commercial practices – all underpinned by increasing personalisation based on the vast number of interactions and transactions. The Cambridge Analytica scandal, the Brexit and Trump campaigns, and disinformation during the COVID-19 pandemic and the Russia-Ukraine war highlight the need for regulatory

intervention. The EU's General Data Protection Regulation (GDPR) is crucial in balancing platform growth, innovation, and individuals' privacy. However, challenges persist in key areas, such as ensuring informed consent, transparency, and data minimisation.

This paper examines the compliance of major technology companies with the GDPR, focusing on three areas: obtaining user consent, providing clear information on data practices, and implementing built-in and default data protection features. Legal procedures and substantial fines against companies like Google, Meta, and TikTok illustrate common violations of the GDPR, which is supplemented by the analysis of guidelines from data protection authorities. Special attention is paid to protecting children's data, with examples of regulatory actions taken against platforms failing to safeguard young users.

The study also discusses the broader implications of current digital regulations in the EU, suggesting that stringent data protection laws may unintentionally favor large, resource-rich tech companies, thereby stifling competition. The convergence of data protection and competition law, exemplified by the European Digital Markets Act (DMA), aims to address these issues by imposing additional obligations on 'gatekeeper' platforms. The emergence of generative AI technologies further complicates the regulatory landscape, necessitating continuous adaptation and enforcement of data protection principles to safeguard users' privacy and rights effectively.

Adatbiztonság és a magánszféra védelme, mint közjó – Datafikáció és a digitális lábnyom

Mozsonyi Norbert

Napjaink egyik legdrámaibb folyamata az információs robbanás és az ennek nyomán végbemenő drámai társadalmi átalakulás. A digitális lábnyomokból rekonstruálhatók eddig rejtett szerkezetek és összefüggések, továbbá módosul a megismerés eszköztára, módszertana és eredményei is. A technológia lényege, minél sokoldalúbb, minél több, eltérő kategóriájú, időzítésű adat komplex, napi szinten fejlődő, új és újabb megoldásokkal, műveletekkel történő hasznosítása. Ettől még nem lesz a '*privacy* halott', ahogyan ezt sokan gondolják; egyszerűen csak arról van szó, hogy a személyes adatok védelme helyett talán inkább a személyes adatok kezelésének szabályain lesz a hangsúly. Ahhoz, hogy használhassuk és kihasználhassuk a mobileszközök, a mesterségesintelligencia-alapú Big Data-technológia, valamint a hibrid felhőszolgáltatás komplex rendszer előnyeit, az adatok megosztását elő kell segítenünk, és olyan szabályozásra van szükségünk, amely ezt úgy teszi lehetővé, hogy közben az adat bizalmas jellege megmarad az adatkezelőnél. Eszerint le kell számolni azzal a szabályozási előfeltevéssel, hogy magánszemély képes kontrollálni a személyes adatainak az áramlását. A megfigyelés társadalmában élőknek, vagyis mindannyiunknak meg kell birkóznunk azzal a gondolattal, hogy adataink, viselkedésünk nyomai értékké váltak, amelyet lehet, hogy éppen most dolgoz fel, elemez valaki, valahol. Az adataink kezelése tekintetében cél, hogy digitális lábnyomaink, személyes adataink ne kerüljenek illetéktelen kezekbe, ne okozzanak az érintett tekintetében joghátrányt, tehát az adatbiztonság megvalósítása. Álláspontunk szerint az első és talán legfontosabb adatvédelmi aggály a jogpolitikai célok és a technológia működési elvének összeütközéséből ered.

Data security and privacy as a public good – Datafication and the digital footprint

One of the most dramatic processes of our time is the information explosion and the dramatic social transformation taking place as a result. Structures and connections that have been hidden until now can be reconstructed from digital footprints, and the toolbox, methodology and results of cognition are also modified. The topicality of the thesis is given by the new interoperability provisions of the recently enacted legislation on contestable and fair markets. Gatekeepers as digital platforms have become a dominant phenomenon in our world, which may be extremely heterogeneous, but almost without exception they can be identified as having a number of interdependent technological, economic and social dimensions of coordination. It is true that the last few decades have seen the recurrence of legal issues relating to the management of data, but these are primarily constitutional approaches in the context of the individual's right to self-determination. Furthermore, it is a fact that enforcement and regulation have not kept pace with the development of extreme market concentration, nor with the achievement of transparency or accountability. The thesis takes a novel approach in several respects. On the one hand, it takes a power approach to the new world of digital sovereignty, that has emerged in the last decade, and on the other hand, it uses the latest findings in systems theory and data science to present a specific approach that, in the current state of technological development, self-determination is no longer necessarily adequate to protect our data. We all have to come to grips with the idea that our data, traces of our behaviour, have become an asset that may be being processed and analysed by someone, somewhere. That does not make 'privacy is dead' as many people think - it is simply, that the focus may be on the rules for handling personal data rather than protecting it.

Meta kontra Bundeskartellamt – A platformszabályozás kapcsolata az adatvédelemmel

Kálmán Kinga

2023. július 4-én az Európai Unió Bírósága ítéletet hozott a Meta kontra Bundeskartellamt ügyben. A határozat fontos követelményeket támaszt az EU általános adatvédelmi rendeletének értelmezésével, valamint a versenyhatóságok és az adatvédelmi felügyeleti hatóságok közötti lojális együttműködéssel kapcsolatban, különösen a fogyasztók személyes adatainak a közösségi média platformok által közvetlen üzletszerzés céljából történő, személyre szabott felhasználása tekintetében. A döntésben a Bíróság a digitális szolgáltatásokról uniós rendeleteket, A DSA-t és a DMA-t még nem alkalmazhatta, mindazonáltal nem hagyta figyelmen kívül, hogy a döntést megelőző eljárás során teljesen megváltozott a platformokat övező szabályozási környezet. Ebből kifolyólag a Bíróság következtetéseit az adatvédelem uniós keretének értelmezésén keresztül éri el.

A tanulmány célja kettős: egyrészről a Meta döntés analitikus jogeset-elemzésén keresztül megvizsgálja, mennyiben illeszkedik az EUB értékelése és a GDPR a DSA és a DMA vonatkozó

keretrendszerébe. E vizsgálat során a DSA-hoz fűződő viszonyra nagyobb hangsúlyt helyez a tanulmány. Másrészt a szerző górcső alá veszi, hogyan és mennyiben formálják a döntésben kifejtett mércék főként az adatvédelmi joggyakorlatot a platformok működésén túl, akár általánosabb jelleggel is. A kitűzött célokhoz illeszkednek a tanulmány hipotézisei is, melyek szerint a döntés alkalmazhatóságuk hiányában is a DSA és a DMA rendelkezéseinek megfelelő megállapításokat tesz, mindezzel azonban a platformok különleges helyzetén túlmutató, általánosan érvényes mércéket állít fel, miközben az értékelés szempontjait a platformok sajátosságai vezérlik.

A tanulmány szerkezetét tekintve négy logikai egységre oszlik: a Meta döntés elemzését követően bemutatja a döntés (és ezáltal a GDPR) kapcsolatát a DSA-val és a DMA-val, majd kitér a versenyhatóságok adatvédelmi jogsértés vizsgálatára kiterjedő hatáskörére. Végül, de nem utolsó sorban az értékelésből levonható következtetésekkel, valamint a jövőre nézvést latolgatással zárul.

Meta v. Bundeskartellamt – The relationship between platform regulation and data protection

On July 4, 2023, the Court of Justice of the European Union (CJEU) issued a judgment in case Meta v. Bundeskartellamt, which sets out important requirements for the interpretation of the EU General Data Protection Regulation (GDPR) and for loyal cooperation between competition authorities and data protection supervisory authorities, in particular with regard to the personalised use of consumers' personal data by social media platforms for direct marketing purposes. In the Decision, the CJEU could not yet apply the EU Digital Services Act (DSA) and Digital Markets Act (DMA), but did not ignore the fact, that the regulatory environment surrounding the platforms had changed completely in the course of the proceedings leading up to the decision. Consequently, the CJEU reaches its conclusions through an interpretation of the EU framework for data protection.

The aim of the paper is twofold: on the one hand, it examines, through case law analysis of the Meta Decision, the extent to which the CJEU's assessment and the GDPR fit into the relevant framework of the DSA and the DMA. In the course of this analysis, the relationship with the DSA will be given greater emphasis. On the other hand, the author will also look at how and to what extent the benchmarks set out in the Decision, in particular shape data protection jurisprudence beyond the operation of the platforms, even more generally. In line with these objectives, the paper hypothesizes that the Decision reaches conclusions in line with the provisions of the DSA and the DMA even in their phase of inapplicability, however it sets generally valid benchmarks that go beyond the specific situation of the platforms, while the criteria of the assessment are guided by the specificities of the platforms.

The paper is structured in four logical units: following the analysis of the Meta Decision, it presents the relationship of the Decision (and thus the GDPR) to the DSA and the DMA, and it then discusses the powers of competition authorities to investigate data protection breaches. Last but not least, it is wrapped up with the conclusions drawn from the assessment and some reflections for the future.

Az alapvető eszközök tana és a DMA – A versenyjog szerepe a szabályozás fényében

Beyer fülöp – Csillik kristóf

A tanulmány a technológiai fejlődés és a jogi keretek kapcsolatát vizsgálja, különös tekintettel a digitális piacok bizonytalanságaira és a jogi doktrínák fejlődésére. A tanulmány kiindulópontja, hogy a jog gyakran lemarad a technológiai fejlődés mögött, ami összetett kérdéseket vet fel, amelyek interdiszciplináris megközelítést igényelnek. Központi eleme a 'bizonytalansági probléma' fogalma, amelynek lényege szerint a döntéshozók nehezen tudják előrejelezni a technológiai változások társadalmi hatásait. A tanulmány a Digital Markets Act (DMA) és a szakmai tudás szerepét vizsgálja a közpolitika formálásában, hangsúlyozva, hogy a jogi doktrínákat – bár látszólag objektívek –, alapvető paradigmatikus megfontolások befolyásolják.

A szerzők a digitális gazdaság tömegközvetítési üzleti modelljét tárgyalják, amelyet hálózati hatások és ökoszisztémák jellemeznek, mint például a Google és a Facebook által létrehozottak. Ezek a platformok a többoldalú piacokon a hálózati externáliák által vezérelt exponenciális növekedést és értékteremtést mutatják be. A tanulmány kiemeli, hogy ezek a dinamikák bonyolítják a szabályozási erőfeszítéseket és kihívást jelentenek a versenyjog hagyományos fogyasztói jóléttel és hatékonysággal kapcsolatos elveinek.

A tanulmány tárgyalja továbbá a versenyjog 'nélkülözhetetlen eszközök' doktrinális megközelítését, amely áthidalhatja a piacszabályozás és a versenypolitika közötti fogalmi szakadékot, különösen a digitális platformok esetében. Az elemzés arra a következtetésre jut, hogy bár a versenyjog történelmi tanulságai értékesek maradnak, alkalmazása a digitális gazdaságra új intézményi realitások megértését igényli.

A közgazdaságtan, a versenyjog és a szabályozás metszéspontjait vizsgálva a tanulmány átfogó képet nyújt a digitális piacok alakításának kihívásairól és lehetőségeiről. A jogi doktrínák folyamatos fejlődését szorgalmazza, hogy azok a digitális gazdaság egyedi jellemzőihez igazodva hatékony szabályozást és tisztességes versenyt biztosítsanak.

The fundamental tools doctrine and the DMA – The role of competition law in the light of regulation

This study explores the relationship between technological advancement and legal frameworks, particularly focusing on the uncertainties of digital markets and the evolution of legal doctrines. It discusses the notion that law often lags behind technological developments, raising complex issues that require interdisciplinary approaches. Central to this discourse is the concept of the 'uncertainty problem', where policymakers struggle to anticipate the implications of technological changes on societal order. The study examines the Digital Markets Act (DMA) and the role of professional knowledge in informing public policy, emphasizing that legal doctrines, while seemingly objective, are influenced by underlying paradigmatic values.

The authors delve into the business model of mass communication in the digital economy, characterized by network effects and ecosystems, such as those created by Google and

Facebook. These platforms illustrate the exponential growth and value creation in multi-sided markets driven by network externalities. The study highlights how these dynamics complicate regulatory efforts and challenge the traditional notions of consumer welfare and efficiency that underpin competition law.

Furthermore, the paper discusses the doctrinal approach to 'essential facilities' in competition law, suggesting that this framework can bridge the conceptual gap between market regulation and competition policy, especially in the context of digital platforms. The analysis concludes that while competition law's historical insights remain valuable, its application to the digital economy requires a nuanced understanding of new institutional realities.

By investigating the intersection of economics, competition law, and regulation, this study provides a comprehensive view of the challenges and opportunities in governing digital markets. It argues for the continued evolution of legal doctrines to accommodate the unique features of the digital economy, ensuring effective regulation and promoting fair competition.

Az algoritmusok szerepe a közösségimédia-platformokon alkalmazott sötét megoldások tekintetében – Az interfész mögötti manipulatív technikák kora

Huszár Daniella

A közösségimédia-platformok mindennapi életünk szerves részévé váltak, átalakítva a kommunikációnkat, az információszerzési folyamatainkat, sőt, még a döntéshozatalunkat is. A digitális fejlődéssel és a közösségimédia-platformok népszerűségével a mesterséges intelligencia- (MI-) alapú technológiák használata is fokozottan nőtt, melynek eredményeként a korábban kizárólag offline térben elérhető tevékenységek és szolgáltatások szinte kivétel nélkül hozzáférhetővé váltak a digitális szférában is, adott esetben még sokkal nagyobb választékkal. Ezzel párhuzamosan egyre több olyan módszer és eszköz jelent meg, amelyek célja a felhasználói döntések manipulálása, szándékos irányítása, gyakran a felhasználók saját érdekeivel ellentétes, nem kívánt eredmények előidézése. Ezekre a módszerekre főként 'sötét megoldásokként', vagy angolul '*dark pattern*'-ként utalnak, amelyek a korábbi, a felhasználók minél szélesebb körének elérését és bevonását célzó marketingstratégiákkal ellentétben mára sokkal kifinomultabb és hatékonyabb technikákat jelölnek.

Az MI-megoldások használatával a platformok könnyen testre szabhatják a felhasználói élményeket és interfészeket, mindezt azonban gyakran a felhasználók autonómiájának és magánéletének rovására teszik. A sötét megoldások, különösen az algoritmusalapú technikák rendszerint az emberi pszichológiára vonatkozó ismereteket használják fel a felhasználói igényekre szabott tervezéssel kombinálva, növelve ezzel a felhasználói elkötelezettséget és a szolgáltatás ismételt igénybevételét. Ebből kifolyólag a felhasználók könnyen ezen digitális élmények rabjaivá válnak éppúgy, ahogyan a digitális világban zajló társadalmi interakciók függői lesznek. Az új addiktív technikák alkalmazása során sérülhet mind a felhasználó magánélethez való joga, amely magában foglalja az egyén döntési autonómiáját, így annak eldöntését is, hogy ki és milyen mértékben férhet hozzá a felhasználó személyes adataihoz, valamint jelentős hatással lehet mindemellett a véleménynyilvánítás és az információk, eszmék megismerésének és közlésének szabadságára is.

Következésképpen a fentiek alapján vitathatatlan, hogy a jogi elemzés kulcsfontosságú annak felmérésében, hogy ezek a gyakorlatok, valamint tervezési technikák összeegyeztethetők-e a hatályos törvényekkel, szabályozásokkal és etikai normákkal, valamint annak feltérképezése, hogy milyen megoldási utak növelhetik a felhasználók jogainak védelmét.

The role of algorithms for dark solutions on social media platforms – The age of manipulative techniques behind the interface

Social media platforms have become an integral part of our daily lives, transforming the way we communicate, gather information and even make decisions. With the digital evolution and the popularity of social media platforms, the use of artificial intelligence(AI)-based technologies has also increased, with the result that activities and services previously available exclusively offline have almost invariably become available in the digital sphere, with a much wider choice of options. At the same time, more and more methods and tools have emerged to manipulate and deliberately guide users' decisions, often leading to undesirable outcomes contrary to their interests. These methods are mainly referred to as 'dark patterns', which, unlike earlier marketing strategies aimed at reaching and engaging a broader range of users, nowadays refer to much more sophisticated and effective techniques.

Using AI solutions, platforms can easily customise user experiences and interfaces, often at the expense of user autonomy and privacy. Dark patterns, especially algorithm-based techniques, may use insights into human psychology combined with tailored design to increase user engagement and repeat usage. Consequently, users may become addicted to these digital experiences, just as they become addicted to social interactions in the digital world. The use of new addictive technologies may infringe both the user's right to privacy, which includes the individual's autonomy of choice, including the right to decide who has access to his or her personal data and to what extent. It may also have a significant impact on freedom of expression and freedom to access and communicate information and ideas.

In conclusion, it is clear from the above that legal analysis is key to assessing whether these practices and design techniques are compatible with existing laws, regulations and ethical standards, and to exploring ways of improving the protection of users' rights.

Platformok felelőssége a szerzői jog megsértéséért – A CDSM irányelv és a DSA közötti kölcsönhatás következményei a szellemi tulajdonjogok védelme szempontjából

Kovács György

A digitális környezet forradalmasította az információ létrehozásának, megosztásának és felhasználásának módját. Ez az átalakulás nemcsak a különböző iparágakat érintette, hanem jelentős kihívásokat jelentett a szellemi tulajdonjogok védelme szempontjából is. Az Európai Unióban két kulcsfontosságú jogszabály, a digitális egységes piacról szóló szerzői jogi irányelv (CDSM irányelv) és a digitális szolgáltatásokról szóló rendelet (DSA) célja, hogy kezelje

ezeket a kihívásokat. Jelen írás a két szabályozási keret közötti összetett kapcsolatot vizsgálja.

A CDSM irányelv és a DSA célja a szerzői jogi és a közvetítői felelősségre vonatkozó szabályoknak a digitális korhoz való hozzáigazítása. Mindkét jogszabály érinti a szellemi tulajdon számos aspektusát, az online platformokat, valamint a különböző online tartalmakat létrehozók és közvetítők jogait, valamint kötelezettségeit. Kölcsönhatásuk megértése alapvető fontosságú. A CDSM irányelv a szerzői jogi védelem online környezetben történő megerősítését célozza, míg a DSA spektruma lényegesen tágabb és további kötelezettségeket ró az online platformokra. A kutatás célja továbbá annak vizsgálata is, hogy a szellemi tulajdonjogok és a véleménynyilvánítás szabadsága, valamint az innováció előmozdításának szükségessége közötti egyensúly mely módon biztosítható a CDSM irányelv és a DSA új szabályainak kölcsönhatásában. A digitális környezet szabályozásának uniós megközelítése hatását tekintve várhatóan messze túlmutat az EU határain, hasonlóképpen, mint ahogyan az a GDPR esetében is érzékelhető. Természetesen az nyitott kérdés marad, hogy a vizsgált új uniós jogszabályok milyen mértékben szolgálnak követendő mintául más régiók és országok számára.

Platform liability for copyright infringement – Implications of the interaction between the CDSM Directive and the DSA for the protection of intellectual property rights

The digital environment has revolutionized the way information is created, shared, and utilized. This transformation has impacted various industries and posed significant challenges for the protection of intellectual property rights. In the European Union, two key pieces of legislation, the Copyright Directive in the Digital Single Market (CDSM Directive) and the Digital Services Act (DSA), aim to address these challenges. This paper examines the complex relationship between these two regulatory frameworks.

The CDSM Directive and the DSA both aim to adapt copyright and intermediary liability rules to the digital age. Both laws affect many aspects of intellectual property, online platforms, and the rights and obligations of those who create and distribute online content. Understanding their interaction is essential. The CDSM Directive aims to strengthen copyright protection in the online environment, while the DSA has a much broader scope and imposes additional obligations on online platforms. The research also aims to explore how to balance intellectual property rights, freedom of expression, and the need to promote innovation within the framework of the new rules of the CDSM Directive and the DSA. The EU's approach to regulating the digital environment is expected to have far-reaching impacts beyond its borders, similar to the effects observed with the GDPR. It remains an open question to what extent these new EU laws will serve as models for other regions and countries.

Szerzőink / Authors

Bálint János az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Doktori Iskola doktorandusza és az Ormai, Papp, Czike és Társai CMS Cameron McKenna Nabarro Olswang LLP Ügyvédi Iroda ügyvédjelöltje. Doktori kutatásának címe *Uniós platformszabályozás: társadalmi kihívások a 21. században*, amely a különböző jogterületek (adatvédelem, média-, fogyasztóvédelmi és versenyjog) konvergenciájára összpontosít az Európai Unió újszerű platformszabályozási jogi kereteinek összefüggésében. Emellett médiajogi előadásokat tart a Károli Gáspár Református Egyetem Állam- és Jogtudományi Karán. 2023-ban a VI. Wolters Kluwer Jogászdíj győztese 'Az év joghallgató tehetsége' kategóriában.

János Bálint is a PhD candidate of the Doctoral School of Law at ELTE Eötvös Loránd University, Budapest, Hungary and trainee lawyer at Ormai, Papp, Czike and Partners CMS Cameron McKenna Nabarro Olswang LLP Law Firm. His PhD research is titled "EU platform regulation: societal challenges in the 21st century", focusing on the convergence of different legal fields (data protection, media, consumer protection and competition law) in the context of the European Union's novel platform regulation legal framework. He also holds media law lectures at the Faculty of Law of the Károli Gáspár University of the Reformed Church in Hungary. Winner of the 6th Wolters Kluwer Lawyer Award 2023 in the category 'Law Student Talent of the Year'.

Beyer Fülöp jogász, 2022-ben végzett az Eötvös Loránd Tudományegyetemen (ELTE) és a Bibó István Szakkollégiumban. Egyetemi évei alatt több közintézménynél dolgozott, többek között a Nemzeti Hírközlési Hatóságnál (NMHH). Jelenleg jogi doktorátust folytat az ELTE-n, és megbízott kutatóként dolgozik az Eötvös József Kutatóközpont Információs Társadalom Kutatóintézetében. Emellett közjogi referensként dolgozik a Fővárosi Önkormányzat Közjogi Ügyek Osztályán. Kutatási területe az internetes közvetítők és a nagy technológiai cégek által vezérelt társadalmi-gazdasági változások. Publikációi az EU „Digital Markets Act" rendeletét és az információs társadalomban infrastrukturális szerepet játszó magánszereplők ellenőrzésére irányuló szabályozási stratégiákat vizsgálják.

Fülöp Beyer is a lawyer who graduated in 2022 from Eötvös Loránd University (ELTE) and Bibó István College for Advanced Studies. During his university years, he worked at several public institutions, including the Hungarian National Regulatory Authority for Telecommunications (NMHH). He is currently pursuing a PhD in law at ELTE and serves as a mandated researcher at the Eötvös József Research Centre, Centre for the Information Society. Additionally, he holds the position of public law officer at the Municipality of Budapest, Department of Public Law Matters. His research interests focus on the socio-economic changes driven by internet intermediaries and big tech companies. His publications explore the EU's Digital Markets Act and the regulatory strategies for controlling private actors that play infrastructural roles in the information society.

Botos Mihály Bálint a Szegedi Tudományegyetem Állam- és Jogtudományi Kar Bűnügyi Tudományok Intézetének doktorandusza. 2021-ben Diploma Príma-díjat, valamint Szegedi Jogi Kari Tudományért emlékérmet kapott. 2022-ben elnyerte az Új Nemzeti Kiválósági ösztöndíjat. Kutatási témája a véleménynyilvánítási szabadság kollektív büntetőjogi korlátai,

amelynek keretében a köznyugalom elleni bűncselekmények fejezetében elhelyezett, és a szólásszabadságot korlátozó tényállásokat alkotmányos büntetőjogi nézőpontból vizsgálja.

Mihály Bálint Botos is a PhD student at the Institute of Criminal Sciences, Faculty of Law and Political Sciences, University of Szeged. In 2021, he was awarded the Diploma Prima Prize and the Memorial Medal for the Science of the Faculty of Law of Szeged. In 2022he was awarded the New National Excellence Scholarship. His research topic is the collective criminal law limits of freedom of expression, in the framework of which he examines the facts that restrict freedom of expression in the chapter of crimes against public order from a constitutional criminal law perspective.

Csillik Kristóf kommunikátor, jogász. Kommunikáció- és médiatudomány alapszakos diplomáját 2017-ben, jogász diplomáját 2022-ben szerezte meg az Eötvös Loránd Tudományegyetemen. Tanulmányi évei alatt a Bibó István Szakkollégium tagja volt. A versenyjogra specializálódott Bassola Ügyvédi Iroda ügyvédjelöltje, az ELTE doktori iskolájának hallgatója. 2021-ben első díjat nyert a Gazdasági Versenyhivatal 'Versenyjog Magyarországon az EU-ban' című esszépályázatán. 2023-ban első díjat nyert a Legfőbb Ügyészség által meghirdetett Kozma Sándor Tudományos Pályázaton. 2023-ban első díjat nyert a Magyar Katonai Jogi és Hadijogi Társaság tudományos pályázatán. Publikációi a polgári perjog, a beruházásvédelmi vitarendezés, az alkotmányjog, a nemzetközi hadijog, az ügyészség alkotmányos helyzete és a versenyjog területeit érintik. Kutatási területe a versenyjogi jogsértéssel okozott károk megtérítése iránt indított perekben alkalmazandó különös bizonyítási szabályok.

Kristóf Csillik is a communicator, a lawyer. He graduated from Eötvös Loránd University in 2017 with a bachelor's degree in communication and media studies and from Eötvös Loránd University in 2022 with a law degree. During his studies, he was a member of the István Bibó Szakkollégium. He is a trainee lawyer at Bassola Law Firm, a law firm specialising in competition law, and is pursuing a PhD at ELTE Doctorate School. In 2021, he won first prize in the essay competition "Competition Law in Hungary in the EU" of the Hungarian Competition Authority. In 2023, he won first prize in the Kozma Sándor Scientific Competition of the Office of the Prosecutor General. In 2023, he won first prize in the Hungarian Military Law Society's science competition. His publications cover the fields of civil litigation, investment protection dispute settlement, constitutional law, international military law, the constitutional status of prosecution and competition law. His research interests focus on the special rules of evidence applicable in actions for compensation for damages caused by competition law infringements.

Huszár Daniella a budapesti Eötvös Loránd Tudományegyetem jogi karán szerzett *cum laude* minősítéssel diplomát 2021-ben, jelenleg a CMS Budapest TMT csoportjának ügyvédjelöltje, ahol adatvédelemmel és technológia joggal foglalkozik. Egyetemi tanulmányai során a közösségimédia-platformok és a mesterséges intelligencia szabályozásával kapcsolatos kérdésekre fókuszált, számos, a véleménynyilvánítás szabadságával és médiajoggal foglalkozó konferencián, valamint versenyen vett részt, mint az ITU Telecom World Conference, az Országos Tudományos Diákköri Konferencia, valamint a Monroe E. Price Media Law Moot Court Competition. 2021-ben a Nemzet Fiatal Tehetségeiért ösztöndíjjal támogatták, hogy

kutatásait folytassa a mesterséges intelligencia szerepével és alapvető jogainkra gyakorolt hatásával kapcsolatban. 2022 őszén megkezdte tanulmányait az ELTE Állam- és Jogtudományi Doktori Iskola PhD képzésén, amelynek keretében mentor oktatóként vett részt a Monroe E. Price Media Law Moot Court Competition egyetemi csapatának felkészítésében. Kutatásai folytatásához a 2023/2024. tanévre az Új Nemzeti Kiválóság Program (ÚNKP) ösztöndíjában, míg a 2024/2025. tanévre az Egyetemi Doktori Kutatói Ösztöndíjban (EKÖP) részesült.

Daniella Huszár graduated cum laude from the Faculty of Law at Eötvös Loránd University, Budapest, in 2021, now she is a lawyer in the TMT team at CMS Budapest, working on data protection and technology law related matters. During her university studies, she focused on the regulation of social media platforms and artificial intelligence, while she participated in numerous conferences and competitions focused on freedom of expression and media law, such as the ITU Telecom World Conference, the National Scientific Students' Associations Conference, and the Monroe E. Price Media Law Moot Court Competition. In 2021, she was supported with the National Young Talent Scholarship to conduct research regarding the role and impact of artificial intelligence on fundamental rights. In 2022, she started her PhD studies at the ELTE Doctoral School of Law and Political Science, where she was involved as a mentor tutor in the preparation of the Monroe E. Price Media Law Moot Court Competition team. To continue her research, she was awarded a scholarship from the New National Excellence Programme ("ÚNKP") for the academic year 2023/2024, and a University Doctoral Research Fellowship for the academic year 2024/2025.

Kálmán Kinga az ELTE Állam- és Jogtudományi Doktori Iskolájának doktorandusz hallgatója, valamint ügyvédjelölt. Ügyvédjelöltként főként adatvédelemmel, IT- és versenyjoggal foglalkozik. Főbb kutatási területe az adatvédelem és az adatgazdaság közötti kapcsolatok, a jelenleg fejlődő szabályozási környezet tükrében kialakuló viszonyrendszer feltérképezése. Több, mint 20 tanulmány (társ)szerzője, munkái elérhetők magyar, angol és lengyel nyelven. Kutatási eredményeit számos hazai, valamint külföldi konferencián ismertette, többek között az American Constitution Society for Law and Policy and Texas A&M University School of Law: Seventh Annual Constitutional Law Scholars Forumon és az International Society of Public Law Seventh Annual Conference eseményen. Korábban a HUN-REN Társadalomtudományi Kutatóközpont Jogtudományi Intézetének kutatási asszisztenseként foglalkozott a mesterséges intelligencia alkotmányjogi vetületeivel, különös tekintettel az MI igazságszolgáltatásban történő alkalmazási lehetőségeire a tisztességes eljárás tükrében.

Kinga Kálmán is a PhD student at ELTE Doctoral School of Law and Political Sciences and a trainee associate. As a trainee associate, her main field of expertise covers data protection, IT and competition law. Her main research interest is the relationship between data protection and the regulation of data economy, mapping the relationship in the light of the currently evolving legal environment. She (co)authors more than 20 papers and her works are available in Hungarian, English and Polish languages. She has presented her research results at numerous conferences both in Hungarian conferences and abroad, including the American Constitution Society for Law and Policy and Texas A&M University School of Law: Seventh Annual Constitutional Law Scholars Forum and the Seventh Annual Conference of the International Society of Public Law. Previously, as a research assistant at the Institute for Legal Studies of the HUN-REN Centre for

Social Sciences, she worked on the constitutional law aspects of artificial intelligence, with special focus on its potential application in the administration of justice in the context of fair trial.

Kovács Andrea az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Doktori Iskolájának doktorandusz hallgatója. 2017–2018-ban az ELTE Price Media Law Moot Court Competition nyolcaddöntős csapatának tagja. Szintén 2018-ban 2. helyezést ért el a Mailáth György Tudományos Pályázat polgári jogi szekciójának joghallgatói tagozatában. Főbb kutatási területei a közösségi média szolgáltatók felelőssége, illetve a közösségimédia-botok tevékenysége, szabályozása.

Andrea Kovács is a PhD student at Eötvös Loránd Tudományegyetem Doctoral School of Law. Member of ELTE's octofinalist team at the 2017/2018 Price Media Law Moot Court Competition. 2nd place at Mailáth György Tudományos Pályázat Civil Law Section, Law Student division. Main research fields: responsibility of social media platforms as service providers, and regulation of social media bots.

Kovács György nemzetközi tranzakciókra szakosodott ügyvéd, és a Pázmány Péter Katolikus Egyetem oktatója, a digitális technológia és adatgazdaság szakjogászképzés szakfelelőse Budapesten. Kutató a Közép-európai Egyetemen, valamint korábban az Európai Bizottság jogi tisztviselője volt. Tagja az Igazságügyi Minisztérium jogi szakvizsga bizottságának, és a Magyar Tudományos Akadémia köztestületének. Rendszeresen publikál és előad nemzetközi konferenciákon. Kutató ösztöndíjasként kutatásokat végzett a Grazi, a Salzburgi, a Saarlandi és a Müncheni Egyetemen az összehasonlító alkotmányjog és az uniós jog területein. Fulbright- ösztöndíjasként amerikai és nemzetközi gazdasági jogot hallgatott a Boston Egyetemen, és doktori kutatást végzett a Harvard Egyetem jogi karán. Európai Uniós jogból szerzett PhD-fokozatot. Szakterületei az uniós alkotmányjog, és uniós jog digitális technológia szabályozása, különösen ezek hatása a szellemi tulajdonjogok védelme szempontjából. A Magyar Fulbright Egyesület elnöke, és a Piarista Diákszövetség alelnöke.

György Kovács is an attorney, specialized in international transactions, and he serves as the head of the graduate program for digital technology and data economy at Pázmány Péter Catholic University in Budapest. He is a research fellow at CEU, and a former policy officer at the European Commission. He is a member of the Bar Exam Committee of the Ministry of Justice, and a member of the Public Body of the Hungarian Academy of Sciences. He is regularly publishing and speaking at international conferences. As a research fellow, he conducted research at the universities of Graz, Saarland, Salzburg and Munich in the areas of comparative constitutional law and EU law. He studied American and International Business Law at the Boston University as a Fulbright Scholar and conducted PhD research at Harvard Law School. He holds a PhD in European Union Law. His research interest include EU constitutional law and the regulation of digital technology under EU law, with a particular focus on their impact on the intellectual property rights enforcement. He is the President of the Hungarian Fulbright Association, and Vice-President of the Hungarian Piarist Alumni Association.

Mozsonyi Norbert harmadéves hallgatói jogviszonyát tölti a Széchenyi István Egyetem Állam és Jogtudományi Doktori Iskola Phd-képzésén, ahol a mesterségesintelligencia-alapú rendszerek

adatvédelmi vonatkozásait kutatja. 2021-ben a Károli Gáspár Református Egyetemen infokommunikációs szakjogászi mesterlevelet szerzett, ezt megelőzően egy évtizeddel korábban pedig a Pázmány Péter Katolikus Jogtudományi Egyetemen diplomázott. Gazdasági informatikus mérnöki és számítástechnikai gépésztechnikus alapvégzettséggel, továbbá közel harmincéves vállalkozásfejlesztési tapasztalattal rendelkezik. A Print Brokers Team Kft.-nél dolgozik mint üzletfejlesztést támogató jogtanácsos és minőségbiztosítási megbízott. A vállalkozásuk a „Minőség -– Innováció 2023" pályázaton innovatív fenntartható üzleti modell kategóriában Nemzeti fődíjas, a nemzetközi mezőnyben pedig finalista lett. Különös érdeklődéssel kutatja az emberi és gépi hálózatok, a szuper- és kvantumszámítógépek fejlesztését, továbbá a digitális technológiák és a mesterségesintelligencia-alapú komplex rendszerek hatását a szereplők együttműködésére.

Norbert Mozsonyi is spending his third year as a student at the Doctoral School of State and Law at Széchenyi István University, during which he is researching the data protection aspects of artificial intelligence-based systems. In 2021, he obtained a master's degree in infocommunications law at the Károli Gáspár Reformed University, and a decade before that, he graduated from the Pázmány Péter Catholic University of Law. He has a bachelor's degree in economic IT engineering and computer engineering mechanical technician and nearly thirty years of business development experience. He is working at Print Brokers Team Kft. as a legal advisor supporting business development and as a quality assurance representative. Their company won the National prize and was an international finalist in the „Quality – Innovation 2023" sustainable business model innovation category. He is particularly interested in researching the development of human and machine networks, super and quantum computers, as well as the impact of digital technologies and complex systems based on artificial intelligence on the cooperation of actors.

Szakálné Szabó Zita jegyző, közigazgatás-szervező, okleveles közgazdász vezetés és szervezés szakon. A Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola PhD hallgatója. Fő kutatási területe a társulási formák szervezete és működése a helyi önkormányzati igazgatásban. Mindezek mellett kiemelten foglalkozik az iskolai tanulmányokat folytatók digitális kommunikációs kompetenciáinak támogatásával.

Zita Szabó Szakálné is a notary, public administration organizer, graduated economist in leadership and organization. She is a PhD student at Széchenyi István University Deák Ferenc Doctoral School of State and Law. Her main research area is the organization and functioning of association forms in the local government. In addition, she focuses on supporting the digital communication competencies of students in school.

Vitkovics Bálint az ELTE Állam- és Jogtudományi Doktori Iskolájának doktoranduszhallgatója. A Mailáth György Tudományos Pályázat keretében díjazott pályaművet nyújtott be a közéleti szereplőkkel kapcsolatos becsület- és jóhírnévsértés joggyakorlata tárgyában. Főbb kutatási területe: személyiségi jog, mesterséges intelligencia, biztosítási jog.

Bálint Vitkovics is a PhD student at ELTE PhD School of Law. He submitted on György Mailáth Scientific Tender an award-winning thesis on the case law of violation of right to integrity and reputation of politically exposed persons. His main research interests are personality rights, artificial intelligence and insurance law.

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 médiaszabályozás 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: *Gyermekvédelem a médiajogban* (2014)
14. Apró István – Paál Vince (szerk.): *A határon túli magyar sajtó Trianontól a XX. század végéig* (2014)
15. Kiss Zoltán – Szivi Gabriella: *A közszolgálati médiaszolgáltatás 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 (szerk.): *Comparative Research on the Approaches of Administrative Judiciaries to Sanctions Issued by Media Regulators in V–4 I.* (2016)
22. Koltay András – Andrej Školkay (szerk.): *Comparative Research on the Approaches of Administrative Judiciaries to Sanctions Issued by Media Regulators in V–4 II.* (2016)
23. Makkai Béla: *Határon túli magyar sajtó – Trianon előtt* (2016)
24. Grad-Gyenge Anikó: *Film és szerzői jog – A megfilmesítési szerződés* (2016)
25. Kőhidi 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 rágalmazás 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 köztehervise lési 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 építészet, 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 csorbításának 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)

Médiatudományi Intézet, Budapest
A kiadásért felel Nyakas Levente
Tördelő: Varga Ákos
Megjelent 16 (B/5) ív terjedelemben, 300 példányban
Médiatudományi Könyvtár: ISSN 2063-5222
Médiatudományi Könyvtár 53.: ISBN 978-615-5302-49-7