
STUDIA IURIS

JOGTUDOMÁNYI TANULMÁNYOK / JOURNAL OF LEGAL STUDIES

2025. II. ÉVFOLYAM 3. SZÁM



Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.

A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.

A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.

A folyóirat online verziója szabadon letölthető (open access).

ALAPÍTÓ TAGOK

BODZÁSI BALÁZS, JAKAB ÉVA, TÓTH J. ZOLTÁN, TRÓCSÁNYI LÁSZLÓ

FŐSZERKESZTŐ

JAKAB ÉVA ÉS BODZÁSI BALÁZS

OLVASÓSZERKESZTŐ

GIOVANNINI MÁTÉ

SZERKESZTŐBIZOTTSÁG TAGJAI

BOÓC ÁDÁM (KRE), FINKENAUER, THOMAS (TÜBINGEN), GAGLIARDI, LORENZO (MILANO),
JAKAB ANDRÁS DSc (SALZBURG), SZABÓ MARCEL (PPKE), MARTENS, SEBASTIAN (PASSAU),
THÜR, GERHARD (AKADÉMIKUS, BÉCS), PAPP TEKLA (NKE), TÓTH J. ZOLTÁN (KRE),
VERESS EMŐD DSc (KOLOZSVÁR)

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola

Székhely: 1042 Budapest, Viola utca 2-4

Felelős Kiadó: TÓTH J. ZOLTÁN

A tipográfia és a nyomdai előkészítés: CSERNÁK KRISZTINA (L'Harmattan) munkája

Nyomdai kivitelezés: Prime Rate Zrt., felelős vezető: TOMCSÁNYI PÉTER

Honlap: <https://ajk.kre.hu/index.php/jdi-kezdolap.html>

E-mail: doktori.ajk@kre.hu

ISSN 3057-9058 (Print)

ISSN 3057-9392 (Online)

URL: KRE ÁJK - Studia Iuris

<https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html>

A CYBERBULLYING JOGI MEGKÖZELÍTÉSE: HATÁR- VONALAK ÉS ÁTFEDÉSEK A MODERN JOGRENDSZERBEN

THE LEGAL APPROACH TO CYBERBULLYING: BOUNDARIES AND OVERLAPS IN THE MODERN LEGAL SYSTEM

PERGER ÁDÁM¹

ABSTRACT ■ The study examines cyberbullying as a form of deviance occurring in the digital communication space, focusing on its criminal law and fundamental rights implications. The phenomenon raises increasingly complex legal and ethical issues due to the transformation of social interactions and the growing dominance of online platforms. Challenges in legal enforcement stem from non-linear, often anonymous and cross-border communication structures, jurisdictional anomalies, and frequent collisions between fundamental rights—particularly freedom of expression and data protection. The aim of the research is to identify current regulatory gaps and assess the responsiveness of both international norms and domestic legislation to the phenomenon of cyberbullying, with special attention to the heightened vulnerability of children and minors. The study analyzes relevant jurisprudence, evaluates European and international regulatory models in a comparative context, and proposes regulatory and enforcement directions that take into account the unique characteristics of the online environment and the delicate balance between the affected fundamental rights. Special attention is given to the role of preventive and educational solutions, as well as to the analysis of the responsibilities that technological service providers and platforms may bear in curbing online harassment. Thus, the study seeks not only to critically examine existing legal frameworks but also to formulate a coherent legal policy and rights-based response to effectively address emerging social harms in the digital age. The aim of the research is to identify regulatory gaps and assess the responsiveness of international norms and domestic legislation, with particular attention to the heightened vulnerability of children.

KEYWORDS: online, cyber, bully, terrorism, data, defense

ABSZTRAKT ■ A tanulmány a cyberbullying, mint a digitális kommunikációs térben megvalósuló deviancia büntetőjogi és alapjogvédelmi összefüggéseit vizsgálja. A jelenség a társadalmi interakciók átalakulásával, valamint az online platformok térnyerésével egyre összetettebb jogi és etikai problémákat vet fel. A jogalkalmazás nehézségeit a nemlineáris,

¹ PhD hallgató, Debreceni Egyetem, Marton Géza Állam- és Jogtudományi Doktori Iskola.

gyakran anonim és határokon átnyúló kommunikációs struktúrák, a joghatósági anomáliák, valamint az alapvető jogok – különösen a szólásszabadság és az adatvédelem – közötti gyakori kollíziók generálják. A kutatás célja, hogy feltárja a jelenlegi szabályozási hiátusokat, és értékelje a nemzetközi normák, valamint a hazai jogalkotás válaszképességét a cyberbullying jelenségére, különös tekintettel a gyermekek és fiatalkorúak fokozott sérülékenysége. A tanulmány elemzi a releváns joggyakorlatot, összehasonlító kontextusban értékeli az európai és nemzetközi szabályozási modelleket, valamint javaslatot tesz olyan szabályozási és jogalkalmazási irányokra, amelyek figyelembe veszik az online környezet sajátosságait és az érintett alapjogok közötti érzékeny egyensúlyt. A vizsgálat külön figyelmet fordít a preventív és edukációs megoldások szerepére is, valamint annak elemzésére, hogy a technológiai szolgáltatók és platformok milyen felelősséget viselhetnek az online zaklatás visszaszorításában. A kutatás célja, hogy feltárja a szabályozási hiátusokat és értékelje a nemzetközi normák, valamint a hazai jogalkotás válaszképességét, különös tekintettel a gyermekek fokozott sérülékenysége.

KULCSSZAVAK: online, cyber, zaklatás, terrorizmus, adat, védelem

1. BEVEZETÉS

A digitalizáció előretörésével párhuzamosan az emberi kapcsolatok jelentős része áttevődött a virtuális térbe. Az online jelenlét mára nem csupán kommunikációs csatorna, hanem társadalmi tér, közéleti fórum, munkahelyi környezet és oktatási platform is egyben. Ezzel együtt azonban megjelentek azok a jelenségek is, amelyek korábban főként a fizikai világban voltak jelen, ám a digitális tér sajátosságai – mint a láthatatlanság, az anonimitás, a gyors terjedés és a permanencia – új dimenziókat adtak nekik. Ilyen jelenség a ‘cyberbullying’, azaz az internetes zaklatás, amely sajátos módon ötvözi az információs társadalom előnyeit és visszasságait. A cyberbullying – jóllehet gyakran társadalmi és pszichológiai kategóriaként tárgyalt fogalom – a jog szempontjából is egyre nehezebben megkerülhető kérdés. *„A tudományos életben elfogadott nemzetközi definíció szerint a cyberbullying olyan online deviancia, amelynek lényege, hogy szándékosan és hosszabb ideig fejt ki valaki zaklató magatartást, mindezt pedig az internet felhasználásával teszi. A jelenség két, hatalmi pozícióját tekintve eltérő csoport vagy személy között zajlik, ahol általában a gyengébb vagy gyengébbnek tűnő fél az áldozat.”*² A cyberbullying jelensége egyre égetőbb társadalmi problémát jelent, különösen a fiatalkorúak körében. Az érintettek gyakran kiskorú vagy serdülőkorú személyek, akik életkori

² MONORI ZSUZSANNA ÉVA: Zaklatás-e a cyberbullying? *In Medias Res*, 2016 (2), 246.

sajátosságaiknál fogva fokozottan kiszolgáltatottak az őket érő pszichológiai nyomásnak, különösen akkor, ha az online térben történik, ahol a határok elmosódnak, a tartalmak kontrollja pedig gyakran lehetetlen. Az elkövetők sok esetben szintén fiatakorúak, ami tovább bonyolítja a jogi megítélést. Egyrészt, mivel életkoruk miatt korlátozott büntetőjogi felelősséggel bírnak, másrészt pedig azért, mert az általuk alkalmazott magatartásformák nem feltétlenül illeszkednek a hagyományos büntetőjogi kategóriákba. Ezzel együtt az ilyen cselekmények következményei súlyosak lehetnek: az áldozatok nemcsak pillanatnyi lelki terhelést élnek meg, hanem hosszú távú mentális, pszichoszociális és közösségi következményekkel is számolniuk kell.

A depresszió, az iskolai teljesítmény csökkenése, a társas kapcsolatok romlása, sőt, szélsőséges esetekben az önsértés vagy az öngyilkosságig vezető pszichológiai krízis sem kizárt. Ebben a kontextusban a jogrendszer egy olyan kihívással néz szembe, amely egyszerre teszi próbára a jogi normák hatékonyságát, a szabályozás koherenciáját és a jogérvényesítés gyakorlati lehetőségeit. A hagyományos jogi gondolkodás, amely meghatározott, tipizált tényállásokban rögzíti a bűncselekményeket, nehezen tud lépést tartani egy olyan valósággal, amely dinamikusan változik, és ahol az elkövetési magatartások formái napról napra új megjelenési módokat öltenek. A digitális tér sajátosságai – mint a gyorsaság, a nyilvánosság, az anonimitás és a platformok közötti átjárhatóság – alapvetően írják át azokat a kereteket, amelyekre a klasszikus büntetőjog épült. Ennek következtében az online zaklatás gyakran csak részlegesen, nehézkesen vagy utólagosan illeszthető be a hatályos jogi keretek közé, különösen akkor, ha az elkövetés nem valósít meg egyértelműen kimerített bűncselekményi tényállást.

A jelen tanulmány célja, hogy átfogó képet nyújtson arról, miként viszonyul a magyar jogrendszer a cyberbullying mint új típusú, határokat nem ismerő társadalmi jelenség kezeléséhez. A kutatás fókuszában az áll, hogy hol húzódnak a hatályos szabályozás keretei, mely jogterületek érintettek, és milyen átfedések, esetleges ellentmondások tapasztalhatók közöttük. A vizsgálat különösen fontosnak tartja annak feltárását, hogy a büntetőjog milyen válaszokat képes nyújtani e problémára, milyen lehetőségeket biztosít a polgári jog a személyiségi jogi védelem terén, hogyan kapcsolódik mindehhez az adatvédelmi szabályozás a digitális személyes adatokkal való visszaélés kapcsán, valamint milyen szerepe van a gyermekvédelmi rendszernek az áldozatok támogatásában és a prevencióban.

2. A CYBERBULLYING FOGALMA ÉS FORMÁI

A ‘bullying’ kifejezés az angol nyelvterületen Thomas Hughes 1856-ban megjelent *Tom Brown’s School Days* című regényének hatására terjedt el, és vált a zaklatás egyik formájának megnevezésére.³ A ‘cyberbullying’ kifejezés az angol nyelvű szakirodalomból származik, és a digitális eszközökkel történő zaklatást, bántalmazást jelöli. Noha a fogalom jelentése a különböző kutatók és jogalkotók értelmezésében eltérő lehet, alapvetően olyan ismétlődő, szándékos magatartást értünk alatta, amely az áldozat megalázását, fenyegetését vagy pszichológiai nyomás alá helyezését célozza, és mindez az online térben, elsősorban közösségi médián, üzenetküldő alkalmazásokon vagy más elektronikus kommunikációs csatornákon keresztül történik. Ebből kiindulva a cyberbullying olyan ismétlődő, ellenséges viselkedésformát jelent, amely során iskoláskorú fiatalok – kihasználva vélt vagy valós erőfölényüket – digitális eszközök és az internet segítségével próbálják megfélemlíteni, megalázni, zaklatni, kiközösíteni vagy neveltség tárgyává tenni gyengébbnek tűnő kortársaikat.⁴

Az elkövető és az áldozat közötti kapcsolat nem feltétlenül személyes jellegű, a támadások gyakran anonim módon történnek, így az elkövető kiléte sok esetben rejtve marad. Az online környezet sajátossága, hogy a tartalmak gyorsan terjednek, a nyilvánosság széles köre számára elérhetővé válnak, és sok esetben hosszú időn keresztül fennmaradnak. E tényezők jelentősen súlyosbítják a cyberbullying következményeit a hagyományos zaklatással összehasonlítva. A jelenség meghatározása a hazai jogi és társadalomtudományi szakirodalomban is sokféleképpen történik. A kutatók szerint az elektronikus zaklatás legveszélyesebb sajátossága az, hogy a megalázó tartalom azonnal és gyakorlatilag korlátlanul terjeszthető. Ennek következtében nemcsak szélesebb nyilvánosságot ér el, hanem az áldozat újra meg újra, akár hosszú időn keresztül kénytelen szembesülni vele.⁵ Egyes szerzők a cyberbullyingot az online zaklatás szinonimájaként kezelik, míg mások megkülönböztetik azt az egyéb, hasonló digitális bántalmazási formáktól, például a gyűlöletbeszédtől, a becsületsértéstől vagy az adatvédelemmel kapcsolatos visszaélésektől. A jelen tanulmány az átfogóbb megközelítést követi, és a cyberbullying fogalma alá sorolja mindazokat a digitális térben megvalósuló szándékos, ismétlődő cselekményeket, amelyek más személy lejáratására,

³ DEÁK DOROTTYA: A cyberbullying problémája Magyarországon. *A NIT ifjúsági szakmai folyóirata*, 2022 (2), file:///C:/Users/felhaszn%C3%A1l%C3%B3/Downloads/NIT_Y.Z.+Folyoirat_2022-2.lapszam-25-35.pdf.

⁴ DOMONKOS KATALIN: Cyberbullying: Zaklatás elektronikus eszközök használatával. *Alkalmazott pszichológia*, 2014 (1), 59.

⁵ DOMONKOS 2014, 60.

megalázására, kiközösítésére vagy fenyegetésére irányulnak, és ezáltal pszichológiai, érzelmi vagy társadalmi kárt okoznak az érintett számára.

A cyberbullying legjellemzőbb formái közé tartozik a személy lejáratása vagy rágalmazása, amely gyakran valótlan információk terjesztésével, manipulált képek vagy videók közzétételével történik. Az online zaklatás különböző formákban nyilvánulhat meg, például sértő, gyűlöletkeltő üzenetek küldésében, pletykák terjesztésében az interneten, személyes adatok engedély nélküli nyilvánosságra hozatalában, megalázó képek és videók megosztásában, valamint a „szexting” – azaz szexuális tartalmú üzenetek és képek – terjesztésében.⁶ Az ismételt, fenyegető vagy megalázó üzenetek küldése szintén gyakori jelenség, amely különösen akkor súlyosbodik, ha az elkövető több platformon keresztül is kapcsolatba lép az áldozattal. Nem ritka az sem, hogy a sértettet szándékosan kizárják online közösségekből, ami a társadalmi elszigetelődés formáját ölti.

Egy másik elterjedt módszer a személyazonosság jogosulatlan használata: hamis profilok létrehozásával, más nevében történő posztolással az elkövetők az áldozat hitelrontását célozzák meg. Egyes esetekben a zaklatás szexuális töltetű is lehet, például amikor szexuális tartalmú képek visszaélésével – úgynevezett ‘revenge porn’ vagy szexting esetén – igyekeznek nyomást gyakorolni az érintettre. Idesorolható továbbá az úgynevezett ‘doxing’ is, amikor az áldozat személyes adatait (például lakcímét, telefonszámát vagy iskoláját) szándékosan nyilvánosságra hozzák annak érdekében, hogy mások is támadják vagy zaklassák. A szakirodalom általában úgy értelmezi a doxing fogalmát, mint személyes, privát, azonosításra alkalmas és érzékeny információk – például név, lakcím vagy tartózkodási hely – „online közzétételét”. A doxing során ezen adatok nyilvánosságra hozatala „hozzájárulás nélkül” és jellemzően „rosszindulatú szándékkal” történik, azzal a céllal, hogy az áldozatot megalázzák, zaklassák, megfélemlítsék, megbüntessék, zsarolják, vagy hogy bizonyos cselekedeteket, illetve eszméket elítéljenek. Összességében a doxing az „online zaklatás” egyik formájának tekinthető, amely súlyos károkat okozhat. A doxingot állami és nem állami szereplők egyaránt alkalmazhatják.

A kutatások különbséget tesznek a doxing két típusa között: az egyik az úgynevezett ‘bottom-up’ megfigyelési eszköz, amely lehetővé teszi az állam számára a hatalom megszerzését vagy megerősítését adatalapú tudás és manipuláció révén; a másik a ‘sousveillance’, amely – LI és WHITWORTH szerint – az állam ellenőrzésére szolgál annak érdekében, hogy az egyének visszaszerezzék saját cselekvőképességüket. A doxing megvalósulhat nyílt forrású kereséssel – vagyis

⁶ ANNA COSTANZA BALDRY – ANNA SORRENTINO – DAVID P. FARRINGTON: The Efficacy of the Tabby Improved Prevention and Intervention Program in Reducing Cyberbullying and Cybervictimization among Students. *Int. J. Environ. Res. Public Health*, 2018 (15), 1.

a korábban az áldozat által megosztott érzékeny adatok felkutatásával –, hekeléssel, az online fiókokhoz vagy rendszerekhez való jogosulatlan hozzáféréssel, illetve úgynevezett ‘social engineering’ technikákon keresztül, amely során másokat manipulálnak érzékeny információk megszerzése érdekében, hogy azokat később felhasználhassák ellenük.⁷ Az online térben elkövetett szóbeli provokáció, a ‘trolling’ szintén a cyberbullying határterületét érintheti, különösen akkor, ha a provokáció szisztematikusan ismétlődik, és kifejezett célja az érintett megszégyenítése vagy társadalmi ellehetetlenítése.⁸

A cyberbullying elhatárolása más, részben hasonló magatartásoktól gyakorlati és elméleti szempontból is elengedhetetlen. Noha több ponton átfedést mutathat például a gyűlöletbeszéddel, az utóbbi jellemzően csoportidentitások elleni fellépést takar, míg a cyberbullying gyakran egyéni sérelmet okoz. Hasonlóképpen, míg a klasszikus értelemben vett kiberbűnözés – például hackelés vagy adathalászat – elsősorban gazdasági kárt okoz, addig a cyberbullying következményei elsősorban a személyiségi jogok sérelmében, illetve pszichológiai és társadalmi károkból jelentkeznek. A cyberbullying tehát nem csupán egy újfajta társadalmi probléma, hanem egy olyan komplex jelenség, amely több jogterület határán helyezkedik el, és számos értelmezési és szabályozási dilemmát vet fel, amely nem csak hazai, hanem uniós szinten is komoly kihívást jelent a jogalkotó számára.

3. JOGI KERETEK AZ EURÓPAI UNIÓBAN

Az Európai Unió jogalkotási tevékenysége az utóbbi évtizedben egyre határozottabban reflektál a digitális térben megjelenő új típusú fenyegetésekre, különös tekintettel az internetes zaklatásra, a nők elleni erőszakra és a gyermekekkel szembeni online visszaélésekre. Az uniós jogrendszer célja nem csupán a büntetőjogi válaszok megalkotása, hanem a megelőzés, az áldozatvédelem, valamint az online szolgáltatók felelősségének tisztázása is.

A 2024. május 14-én elfogadott (EU) 2024/1385 irányelv⁹ a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről mérföldkő az európai

⁷ BÀRBARA MOLAS: Doxing: A Literature Review. ICCT Project Report, December 2024, https://icct.nl/sites/default/files/2025-01/Molas_Doxing%20A%20Literature%20Review.pdf.

⁸ KAREN LUMSDEN – HEATHER M. MORGAN: ‘Cyber-Trolling as Symbolic Violence: Deconstructing Gendered Abuse Online’. In: NANCY LOMBARD (ed.): *Routledge Handbook of Gender and Violence*. Chapter 12. London, Routledge, 2018. https://www.researchgate.net/publication/317551298_Cyber_trolling_as_symbolic_violence_deconstructing_gendered_abuse_online.

⁹ Az Európai Parlament és a Tanács (EU) 2024/1385 irányelve (2024. május 14.) a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024L1385>.

büntetőjog és áldozatvédelem fejlődésében. Az irányelv egyértelműen kimondja, hogy a fenyegető, zaklató és megfélemlítő magatartás – akár az online térben, akár azon kívül valósul meg – súlyos következményekkel járhat, és kriminalizálása indokolt. A dokumentum külön nevesíti az internetes zaklatás ('cyberstalking') és a nemi alapú online erőszak formáit, mint amelyek félelmet, pszichológiai sérülést vagy társadalmi elszigeteltséget válthatnak ki az áldozatokból.

Különösen nagy hangsúlyt kap a női politikusok, újságírók és emberi jogi aktivisták fokozott védelme, akik gyakran célpontjai ilyen típusú digitális támadásoknak. Ezzel párhuzamosan az EU digitális piacokat szabályozó jogszabálysomagjának egyik kulcsfontosságú eleme, a Digital Services Act (DSA)¹⁰ 2024 elején lépett hatályba. A DSA a digitális szolgáltatók, különösen a tárhelyszolgáltatók és online platformok felelősségét szabályozza az illegális tartalmak eltávolítása, a felhasználók biztonsága és az átláthatóság terén. A rendelet célja, hogy a digitális szolgáltatók ne csupán passzív közvetítőként, hanem aktív kockázatkezelőként működjenek, különösen a gyermekek, fiatalok, illetve más veszélyeztetett csoportok védelme érdekében. A szabályozás bevezeti a „megbízható jelző” ('trusted flagger') intézményét, melynek keretében elismert szervezetek gyorsított eljárásban kérhetik a jogsértő tartalmak eltávolítását. A gyermekek védelmét szolgálja az új Child Sexual Abuse (CSA)¹¹ rendelettervezet, amely jelenleg vitás pontokat is tartalmaz. A szabályozás célja, hogy lehetővé tegye a gyermekekkel szembeni szexuális visszaélések dokumentumainak, képeinek, videóinak gyors és hatékony felismerését, valamint eltávolítását az internetről. Ez azonban számos adatvédelmi és jogi aggályt vet fel, különösen az end-to-end titkosítás (végponttól végpontig történő titkosított üzenetküldés) korlátozása tekintetében. A rendelet egyensúlyt próbál teremteni a felhasználók magánélethez való joga és a gyermekek biztonságához fűződő kollektív érdek között – egyensúly, amelyet a digitális jogalkotás egyik legnagyobb kihívásaként tartanak számon.

¹⁰ 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), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1751114269007>.

¹¹ Az Európai Parlament és a Tanács rendelete a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52022PC0209>.

4. GYERMEKEK VÉDELME ÉS ONLINE SZEXUÁLIS ZAKLATÁS AZ EURÓPAI UNIÓ JOGRENDSZERÉBEN

A digitális környezet fejlődése új típusú veszélyeket hozott magával, amelyek közül talán a legaggasztóbb a gyermekek elleni online szexuális visszaélések rohamos terjedése. Míg a gyermekvédelem hosszú ideje kiemelt célkitűzés az európai jogalkotásban, a technológiai változások olyan mélyreható kihívásokat támasztanak, amelyek új megközelítést, korszerű szabályozást és hatékony végrehajtási mechanizmusokat követelnek meg.

Az EUROPOL 2023-as jelentése¹² egyértelművé tette, hogy az online térben elkövetett szexuális visszaélések tekintetében az Európai Unió nemcsak célpont, de tárolási és terjesztési központként is funkcionál. A jelentés szerint a gyermekekkel szembeni szexuális visszaéléseket ábrázoló tartalmak több mint 60%-át az Európai Unió területén tárolják, vagy legalábbis innen elérhető szervereken található. Ráadásul ezek a tartalmak döntő többségében valódi, hús-vér gyermekeket ábrázolnak, ami morálisan és jogilag is különösen súlyos megítélés alá esik.¹³ E problémakörre válaszul az Európai Bizottság 2022 májusában előterjesztette a Child Sexual Abuse Regulation (CSA rendelettervezet) néven ismert új szabályozási javaslatát, amely 2024-re kulcsponttá vált az uniós digitális gyermekvédelmi politika formálásában. A jogalkotás célja az, hogy az EU területén működő szolgáltatók kötelesek legyenek észlelni, bejelenteni, és adott esetben eltávolítani minden olyan tartalmat, amely gyermekekkel szembeni szexuális visszaélésre utal. A rendelet több innovatív, ám vitákat kiváltó eszközt is tervez bevezetni. Talán a legnagyobb figyelmet az a szabályozási rész kapta, amely szerint a szolgáltatók – köztük a titkosított üzenetküldő rendszereket működtetők – kötelesek lennének a végponttól végpontig titkosított kommunikáció tartalmát is ellenőrizni bizonyos automatizált szűrőrendszerek segítségével. Ez a gyakorlatban azt jelentené, hogy olyan privát kommunikációs csatornákat is monitoroznának, amelyek eddig kívül estek a hatósági és vállalati betekintés hatókörén. Bár a cél világos – a gyermekbántalmazás visszaszorítása –, a jogvédő szervezetek és technológiai cégek részéről komoly ellenállást váltott ki ez az elképzelés. Az egyik fő ellenérv szerint a rendelet sértheti a magánélethez való jogot, amelyet az Európai Unió Alapjogi Chartája is garantál. Emellett technikaileg is vitatott, hogy a titkosítás gyengítése valóban növeli-e a biztonságot, vagy épp ellenkezőleg, sebezhetőbbé teszi a felhasználókat más típusú támadásokkal

¹² Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf.

¹³ GYURKÓ SZILVIA: A gyerekekkel szembeni online szexuális visszaélések és a készülő új EU rendelet háttere. *Családi jog*, 2023 (3), 10.

szemben. Mindemellett fontos hangsúlyozni, hogy a CSA rendelet különbséget tesz a gyermekpornográfia különféle kategóriái között: egyrészt célzottan a már ismert, jogsértő tartalmak gyors felismerésére koncentrál, másrészt lehetőséget teremt új, eddig azonosítatlan visszaélési anyagok feltárására is mesterséges intelligencia segítségével. E két mechanizmus különösen fontos, mivel az elkövetők folyamatosan új formákat keresnek az azonosítás elkerülésére.

A rendelettervezet egyik sarokpontja a bejelentési kötelezettség intézményesítése. Eszerint a digitális szolgáltatók számára kötelező lesz jelenteni a hatóságoknak minden olyan esetet, amikor gyermekkel szembeni szexuális visszaélés gyanúja merül fel. A rendszer kulcsszereplője a megbízható jelző (trusted flagger)¹⁴ – egy tanúsított, szakértői státuszú szereplő, aki gyorsított eljárás keretében kezdeményezheti a tartalom eltávolítását. Ez a mechanizmus a Digital Services Act-ből ismert koncepcióra épül, de a gyermekvédelem kontextusában sokkal szigorúbb határidőket és protokollokat ír elő. A rendelet a szolgáltatók számára átláthatósági követelményeket is megfogalmaz: éves jelentésekben kell beszámolniuk az észlelt tartalmak mennyiségéről, az alkalmazott technológiákról és a bejelentések eredményéről. Ez elősegíti a hatóságok munkáját, és a felhasználók számára is nyomon követhetővé teszi, milyen intézkedések történnek a gyermekek védelme érdekében. A CSA rendelet egy fontos felismerésre épül: az online szexuális zaklatás gyakran nem zárul le az interneten. Az esetek jelentős részében az online zaklatás és manipuláció (pl. 'grooming') előbb-utóbb fizikai visszaélésekhez vezet. A fiatalok sebezhetőségét súlyosbítja, hogy egyre fiatalabb korban kerülnek kapcsolatba az internetes közzeggel – az EUROPOL szerint a 12–17 éves korosztály 51%-a használ rendszeresen nyilvános chatszobákat és fórumokat, sőt 11–12%-uk már a dark neten is jelen van. A digitális zaklatás tehát nem pusztán adatvédelmi, hanem súlyos emberi jogi kérdés. A „digitális nyomok” maradandósága („az internet nem felejt”) különösen tragikus következményekkel járhat a gyermekek számára, akik gyakran képtelenek eltávolítani magukról az elkövetők által terjesztett tartalmakat. Ezért a szabályozás célja nem csupán a prevenció és az azonnali eltávolítás, hanem a hosszú távú rehabilitációs lehetőségek biztosítása is.

¹⁴ Trusted flaggers under the Digital Services Act (DSA), <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>.

4.1. Iskolai prevenció

A cyberbullying, vagyis az internetes zaklatás napjainkban az iskoláskorú gyermekeket és fiatalokat érintő egyik legsúlyosabb, ugyanakkor legnehezebben tetten érhető társadalmi problémává vált. A jelenség különösen aggasztó abban a tekintetben, hogy nem csupán a tanulók mentális egészségét veszélyezteti, hanem az iskolai közösségek egészét is megbontja. Míg korábban az iskolai zaklatás, azaz a klasszikus értelemben vett bullying elsősorban az intézmény falain belül zajlott, a digitális technológia térnyerésével és a mobil eszközök mindennapi használatával a zaklatás új, határokat nem ismerő dimenzióba lépett. A közösségi média, az üzenetküldő alkalmazások és az online játékelőterek olyan kommunikációs tereket hoztak létre, ahol a gyerekek állandó kapcsolatban maradhatnak egymással – és sajnos nemcsak pozitív, hanem destruktív módon is. Az iskolai közösségek, amelyek eredetileg a szocializáció, a tanulás és a személyiségfejlődés színterei, ma már egyre gyakrabban válnak a cyberbullying kiindulópontjává. Az osztálytársak közötti konfliktusok, versengések, kirekesztések és hatalmi viszonyok sokszor áttevődnek a virtuális térbe, ahol az agresszív viselkedésformák még nehezebben észlelhetők és kezelhetők. A pedagógusok és szülők gyakran csak utólag, a következményekből – például a gyerek visszahúzódozó viselkedéséből, tanulmányi eredményeinek romlásából vagy pszichoszomatikus tüneteiből – következtethetnek arra, hogy valamilyen online bántalmazás zajlik. A gyerekek ugyanis sok esetben nem merik vagy nem akarják elmondani, hogy zaklatás áldozatai lettek, részben a szégyen, részben pedig a megtorlástól való félelem miatt.

A cyberbullying egyik legkritikusabb jellemzője éppen az, hogy időben és térben gyakorlatilag határtalan: míg a hagyományos iskolai bántalmazás tipikusan a tanítási órák között vagy az iskolaudvaron zajlott, a digitális zaklatás nem ér véget a csengő megszólalásával. Az online tér 0–24 órában elérhető, az üzenetek bármikor küldhetők, a posztok és megjegyzések bármikor olvashatók, újra megoszthatók, és az internetes közösségek tagjai – akár ismeretlenek is – pillanatok alatt részévé válhatnak az eseményeknek. Ez a folyamatos hozzáférés azt eredményezi, hogy az áldozatok számára szinte nincs menekvés: a tanítási idő után, otthon, a saját szobájukban sem érezhetik magukat biztonságban, mert az őket ért verbális vagy képi támadások a telefonjuk vagy számítógépük képernyőjén keresztül ott is eléri őket. Ez az állandó elérhetőség és kiszolgáltatottság rendkívül megterhelő pszichológiai hatással bír, különösen egy fejlődő személyiségű gyermek esetében. Az internetes zaklatás ezen túlmenően gyakran rejtett formát ölt. A bántalmazás nem minden esetben nyilvános, sokszor privát üzenetek, zárt csoportokban zajló beszélgetések, vagy akár anonim fiókok által

terjesztett tartalmak formájában valósul meg. A gyerekek gyakran nem is tudják pontosan, ki a zaklatójuk, vagy kik vesznek részt a bántalmazásban, ami tovább növeli a bizonytalanságot és félelmet. Ezenkívül a digitális tartalmak rendkívül gyorsan terjednek, így egy megszégyenítő fotó, sértő bejegyzés vagy gúnyos videó pillanatok alatt elérheti az egész osztályt, sőt, akár az egész iskolát is. Az online nyilvánosság felerősíti a szégyent, és az áldozat számára az események kontrollálhatatlanná válnak. Az iskolák és a pedagógiai közösségek számára komoly kihívást jelent, hogy miként kezeljék az ilyen jellegű konfliktusokat. A nevelési-oktatási intézmények hagyományos eszközei – mint a szóbeli figyelmeztetés, a fegyelmi eljárás vagy a szülőkkel való konzultáció – gyakran nem bizonyulnak elegendőnek vagy hatékonyak a cyberbullying eseteiben, különösen akkor, ha az iskolai hatáskör nem terjed ki az online térben történt eseményekre. A jogi eszközök alkalmazása pedig korlátozott, hiszen egyrészt a bizonyítás nehézkes, másrészt az elkövetők életkoruk miatt sok esetben még nem büntethetők. Ezért különösen fontos a prevenció, vagyis az olyan iskolai programok, amelyek a digitális etika, az empátia, az online viselkedés normái és a felelősségvállalás témáit integrálják a tanulók mindennapi nevelésébe. A cyberbullying tehát nem csupán egyéni tragédiák vagy személyes konfliktusok szintjén jelenik meg, hanem intézményi és társadalmi szinten is kihívásokat állít elénk. A gyermekek digitális térben való védelme nem csupán szülői vagy pedagógusi feladat, hanem közösségi felelősség is, amelyhez szükség van a jogrendszer, az oktatási intézmények, a technológiai szolgáltatók és a társadalmi tudatformálás szereplőinek összehangolt fellépésére.

Csak így biztosítható, hogy az iskolai közösségek újra olyan helyekké válhassanak, ahol a gyermekek biztonságban érezhetik magukat – nemcsak fizikailag, hanem a digitális világban is. Az internetes zaklatás különösen súlyos lelki és pszichológiai hatásokat válthat ki, mint például állandó szorongás, alvászavar, társas izoláció, sőt, súlyosabb esetekben öngyilkossági gondolatok vagy kísérletek is megjelenhetnek. A probléma súlyosságát felismerve az Európai Parlament 2018. szeptember 11-i állásfoglalása¹⁵ egyértelműen kiemeli a megelőzés fontosságát az oktatási intézményekben. Az állásfoglalás szerint szükséges, hogy az iskolák bejelentési rendszereket alakítsanak ki, melyek lehetővé teszik a tanulók, tanárok és szülők számára, hogy jelezhessék a zaklatásra utaló eseteket. Ezek a rendszerek nemcsak a visszaélések dokumentálását, hanem azok kezelését is segíthetik, hozzájárulva ahhoz, hogy az iskolai közösségek átláthatóbbá és biztonságosabbá

¹⁵ Az Európai Parlament 2018. szeptember 11-i állásfoglalása az Unión belüli, munkahelyen, nyilvános térben és a politikai életben elkövetett megfélemlítés és szexuális zaklatás megelőzését és az ellenük való küzdelmet szolgáló intézkedésekről (2018/2055(INI)), https://www.europarl.europa.eu/doceo/document/TA-8-2018-0331_HU.pdf.

váljanak. A hatékony prevencióhoz azonban önmagában a bejelentési csatornák kiépítése nem elegendő. Az oktatási intézményeknek pedagógiai, pszichológiai és jogi szempontból is felkészültnek kell lenniük arra, hogy az internetes zaklatással szemben megfelelő módon lépjenek fel. A tanároknak és iskolai dolgozóknak szükségük van megfelelő képzésekre, hogy felismerjék a zaklatás jeleit, valamint érzékenyen és hatékonyan tudjanak reagálni az esetekre. Az iskolai közösségekben a bizalom kiépítése és fenntartása kulcsszerepet játszik abban, hogy az áldozatok merjék jelezni, ha zaklatásban van részük. Az intézmények szerepe tehát nem csupán technikai, hanem szemléletformáló is: a gyermekeket meg kell tanítani a digitális tér veszélyeire, a felelős internethasználatra, valamint arra is, hogyan kérhetnek segítséget, ha bajban vannak. A prevenció részét kell képeznie az iskolai tantervnek, az intézményi kultúrának és a diákok közötti mindennapi interakcióknak is. Az a társadalmi közeg, amelyben a zaklatás, a megszegyenítés és a kirekesztés normalizálódik, hosszú távon képtelen védelmet nyújtani a gyermekeknek. Éppen ezért a cyberbullying elleni küzdelem egyik legfontosabb eleme a tudatosság erősítése, valamint a diákok, pedagógusok és szülők közötti együttműködés kialakítása.

5. INTERNETES ZAKLATÁS ÉS FENYEGETŐ ZAKLATÁS JOGI ÉRTELMEZÉSE

– UNIÓS ÉS MAGYAR SZABÁLYOZÁS ÖSSZEHASONLÍTÁSA

Az online térben megvalósuló zaklatás új kihívások elé állítja a modern jogrendszereket. Az Európai Parlament és a Tanács 2024/1385 irányelve (2024. május 14.)¹⁶ két külön fogalom mentén közelíti meg a kérdést: az „internetes fenyegető zaklatás” (6. cikk) és az „internetes zaklatás” (7. cikk) kategóriáin keresztül. Ezzel szemben a magyar jog a Btk.¹⁷ 222. § szerint egy általánosabb, cselekménysemleges zaklatási tényállást határoz meg. E három jogi konstrukció értelmezése és összevetése világosan rávilágít arra, hogy milyen irányban fejlődik a zaklatás jogi megítélése az európai jogrendszerben.

¹⁶ Az Európai Parlament és a Tanács (EU) 2024/1385 irányelve (2024. május 14.) a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről.

¹⁷ A Büntető Törvénykönyvről szóló 2012. évi C. törvény, <https://net.jogtar.hu/getpdf?docid=A1200100.TV&printTitle=2012.%20%C3%A9vi%20C.%20t%C3%B6rv%C3%A9ny>.

5.1. Internetes fenyegető zaklatás (6. cikk – EU 2024/1385)

Ez a tényállás kifejezetten az információs és kommunikációs technológia (IKT) révén megvalósuló, ismételt vagy folyamatos megfigyelésre koncentrál. A cél az adott személy tevékenységeinek, mozgásának nyomon követése, annak beleegyezése vagy jogi felhatalmazás hiányában. A jogalkotó külön kiemeli, hogy az ilyen magatartás csak akkor válik büntetendővé, ha súlyos kárt okozhat az érintett személynek. Ez a kár lehet pszichés, fizikai vagy akár szociális természetű is, és a törvény indokolása szerint nem szükséges annak bekövetkeznie – elegendő a veszélyeztetettség valószínűsége.

Ez a típusú zaklatás lényegében az ún. ‘cyberstalking’-gal azonosítható, vagyis a digitális térben való zaklató, követő, megfigyelő magatartással. Kiemelendő, hogy az elkövető szándéka itt nem feltétlenül a közvetlen fenyegetés, hanem a célzott és tartós kontrollgyakorlás az áldozat felett, amely ugyanolyan mértékű félelmet vagy szorongást válthat ki.

5.2. Internetes zaklatás (7. cikk – EU 2024/1385)

Az internetes zaklatás fogalma szélesebb körű, és több altípust is felölel. A szabályozás négy különböző magatartásformát nevesít, amelyek önmagukban is bűncselekménynek minősülnek, ha azokat IKT révén hajtják végre. Az első altípus a klasszikus fenyegető magatartás, amely ismételt vagy folyamatos formában jelentkezik, és amely konkrét bűncselekménnyel való fenyegetést foglal magában. Itt az áldozat fizikai biztonsága kerül veszélybe – vagy legalábbis reális félelem alakul ki benne annak elvesztésétől. A második esetben nyilvánosan hozzáférhető, másokkal közösen tanúsított fenyegető vagy sértő magatartás történik, amely súlyos lelki sérülést okozhat. Itt a társas dimenzió – vagyis a közösség előtti megalázás – játszik központi szerepet. A harmadik pont egy viszonylag új keletű, de egyre gyakoribb online jelenséget – az intim képek kéretlen megosztását – bünteti. A képek nemi szerveket ábrázoló jellege, illetve azok kéretlensége kiemelt hangsúlyt kap. Az áldozat beleegyezésének hiánya, valamint a képek nemiségének megalázó volta indokolja a súlyosabb büntetőjogi fellépést. A negyedik magatartás az áldozat személyes adatainak nyilvánosságra hozatalát szankcionálja, ha ez mások buzdítását célozza fizikai vagy pszichikai sértés elkövetésére. E jelenség az ún. ‘doxxing’: az interneten való „kiárúsítása” az áldozat személyes adatainak, amelyet gyakran politikai, ideológiai vagy bosszúmotiváció kísér. Mind a négy altípus súlyos lelki sérelem lehetőségét feltételezi, és közös bennük a digitális tér manipulációs potenciálja: az, hogy a tartalmak

gyorsan terjednek, nem vagy nehezen kontrollálhatók, és az áldozatot a közösségi szintéren megalázzák vagy veszélybe sodorják.

5.3. Zaklatás a magyar Btk. szerint (222. §)

A magyar Büntető Törvénykönyv zaklatásra vonatkozó rendelkezése célzati bűncselekményként jelenik meg, amelynek lényege, hogy az elkövető célzatos magatartást tanúsít, vagyis szándékában kell állnia a sértett megfélemlítése vagy a magánéletébe történő önkényes beavatkozás. Ezt a jogi konstrukciót egészíti ki az a követelmény, miszerint az adott cselekménynek rendszeresnek vagy tartós-nak kell lennie, továbbá nem járhat súlyosabb bűncselekmény megvalósulásával. A törvény szövege tehát nem az elkövetés konkrét módjára, hanem a magatartás jellegére, a szubjektív szándéokra és az ismétlődésre, időbeliségre helyezi a hangsúlyt. Ugyanakkor a jogalkotó nem tesz különbséget aszerint, hogy a zaklatás milyen technikai eszközzel vagy kommunikációs csatornán keresztül valósul meg, így az információs és kommunikációs technológiák (IKT) használata sem jelenik meg sem súlyosító körülményként, sem önálló elkövetési sajátosságként. A Btk. 222. § technológiасemleges megfogalmazása azt jelenti, hogy az online zaklatás csak akkor értelmezhető a törvényi tényállás alá eső magatartásként, ha egyébként minden más feltétel – például a célzat, az ismétlődő jelleg és a súlyosság – megvalósul. Ez az általános megközelítés lehetővé teszi ugyan a szabályozás viszonylagos rugalmasságát, ugyanakkor komoly hátrányt jelent akkor, amikor a digitális tér egyedi jellemzői, visszaélésszerű lehetőségei és elkövetési formái kerülnek előtérbe.

A technológiai eszközökkel megvalósított zaklatás – így például az interneten keresztül történő fenyegetés, a közösségi média felületein történő nyilvános megalázás vagy az elektronikus levelezésben megvalósuló pszichológiai nyomás-gyakorlás – gyakran más dinamikát követ, mint a hagyományos fizikai vagy közvetlen kommunikációs eszközökkel elkövetett zaklatás. Ezt a különbséget azonban a jelenlegi jogi keretrendszer nem képes önállóan értékelni, mivel az eszköz vagy a médium nem válik releváns szemponttá a jogi minősítés során. Ezzel szemben az Európai Unió által elfogadott 2024/1385-ös irányelv már kifejezetten a digitális környezetre szabott jogi kategóriák kialakítására törekszik. Az irányelv részletesen körülírja az internetes megfigyelés és zaklatás különféle típusait, és finoman elkülöníti azokat egymástól az alapján, hogy milyen típusú sérelmet okoznak. E megközelítés révén külön jogi jelentőséget kapnak a pszichológiai károkozás, a nyilvános megszégyenítés, a fenyegetés, valamint az adatvédelem megsértése. Az ilyen típusú differenciálás jelentős előrelépést jelent a jogbiztonság

szempontjából, hiszen egyértelműbbé teszi, milyen magatartások tartoznak a büntetőjog által tilalmazott körbe, és ezáltal kiszámíthatóbbá, igazságosabbá és egységesebbé teszi az alkalmazandó jogot.

A magyar szabályozás ezzel ellentétben tágabb és elvontabb fogalmi keretekkel dolgozik, amelyek lehetővé teszik ugyan a rugalmas jogalkalmazást, de gyakran pontatlan jogértelmezéshez, illetve a digitális visszaélések alulminősítéséhez vezethetnek. A jelenlegi Btk. nem tudja kellő pontossággal megragadni azokat az új típusú magatartásokat, amelyek az online tér sajátosságain alapulnak, így például a közösségimédia-platformokon zajló ismétlődő lejáratás, a privát fényképek jogosulatlan megosztásával történő fenyegetés vagy a több felhasználó által egyszerre végzett zaklatás. Bár ezek a cselekmények súlyos pszichés és társadalmi következményekkel járhatnak az áldozat számára, a jogalkalmazó sokszor nem rendelkezik olyan jogi eszköztárral, amely lehetővé tenné a tényleges súlyuknak megfelelő szankcionálásukat. A digitális zaklatás gyakran rejtett, nehezen bizonyítható, ráadásul időben elhúzódó folyamat, amely nem mindig illeszthető be a hagyományos zaklatás büntetőjogi keretei közé. Az uniós irányelv egy másik jelentős újítása, hogy nem csupán a közvetlen pszichológiai sérelmet tekinti releváns káros hatásnak, hanem figyelembe veszi az áldozat társadalmi megítélésére, közösségi kapcsolataira és személyes biztonságérzetére gyakorolt hatásokat is. Az irányelv rendelkezései szerint az olyan magatartások, amelyek egy személy ellen irányulnak, de a közösség szeme előtt zajlanak – például nyilvános megszégyenítés vagy online lejárató kampány – különös súllyal esnek latba, hiszen a nyilvánosság előtti megalázás a pszichológiai terhek jelentős fokozódásával járhat.

A csoportosan megvalósított zaklatás is önálló jogi értékelést kap, mivel az elkövetők szervezettsége, száma és hatása az áldozatra sokkal intenzívebb, mint egy egyéni támadás esetén. E szempontok jelenleg nem tükröződnek a magyar büntetőjogi szabályozásban, noha a gyakorlatban egyre gyakoribbak az ilyen jellegű esetek, különösen a fiatalok körében. A magyar jogalkotás számára tehát a 2024/1385-ös irányelv végrehajtása nem pusztán törvénymódosítást igényel, hanem egy átfogó szemléletváltást is a büntetőjog területén. Ez a váltás magában kell, hogy foglalja a jogértelmezési gyakorlat korszerűsítését, a bírói döntéshozatal irányvonalainak pontosítását, az ügyészégi nyomozás kiterjesztését az online tér sajátosságaira, valamint az áldozatok hatékonyabb jogi és pszichológiai támogatásának kialakítását is. Fontos hangsúlyozni, hogy az új irányelvek beépítése nem csupán a törvénszöveg formális átvétele, hanem olyan gyakorlati intézkedések meghonosítása is, amelyek a digitális térben is biztosítani képesek az emberi méltóság, a magánélet és a személyes biztonság védelmét. Az irányelv implementálása során a magyar jogalkotásnak figyelembe kell vennie azt a társadalmi igényt is, amely egyre határozottabban lép fel a digitális visszaélésekkel szembeni

hatékonyabb fellépés érdekében. Az állampolgárok részéről egyre világosabb az elvárás, hogy az online tér ne legyen jogon kívüli zóna, hanem olyan közeg, ahol a jogrend érvényesül, és ahol a sértettek számára valódi védelem, az elkövetők számára pedig tényleges felelősségre vonás biztosított. A cyberbullying és más digitális visszaélések kezelése tehát nem csupán büntetőpolitikai kérdés, hanem a jogállamiság egyik próbája is. A magyar jogrendszernek ebben a folyamatban nem elég követnie az uniós irányelveket, hanem aktív, kezdeményező szerepet is vállalhat egy olyan jogi környezet kialakításában, amely valóban képes szembenézni a digitális társadalom kihívásaival. Összegzésként megállapítható, hogy a zaklatás jelenlegi magyar büntetőjogi szabályozása részben elavult eszközökkel próbálja kezelni a digitális térben megjelenő új típusú visszaéléseket. A technológiasemleges megközelítés egyes esetekben lehetővé teszi a rugalmas jogalkalmazást, ugyanakkor nem ad kielégítő választ az online zaklatás sajátos formáira. Az uniós szabályozás részletesebb, árnyaltabb és a gyakorlat igényeihez jobban illeszkedő megközelítést kínál, amelynek hazai adaptációja elkerülhetetlen, ha a magyar jogrendszer valóban reagálni kíván a 21. század digitális kihívásaira.

6. ZÁRÓGONDOLATOK

A cyberbullying, vagyis az online zaklatás nem pusztán egy újkori társadalmi jelenség, hanem egy olyan komplex és sokrétű probléma, amely a jogrendszerek számára is egyre nagyobb kihívást jelent világszerte. Ez a jelenség alapvetően kérdőjelezi meg a hagyományos jogi kategóriák érvényességét, illetve azok alkalmazhatóságát a 21. századi digitális környezetben, ahol az információáramlás sebessége, a technológiai eszközök elterjedtsége és az anonimitás lehetősége új típusú visszaélések előtt nyit kaput. Az online tér – amely sok esetben ellenőrizhetetlen, határok nélküli, és ahol a kommunikáció pillanatok alatt óriási közönséghez juthat el – radikálisan új helyzetet teremt nemcsak az áldozatok, hanem a jogalkalmazók, jogalkotók és szakpolitikák számára is. E tanulmány célja az volt, hogy feltárja, miként jelenik meg a cyberbullying a magyar jogrendszerben, és megvizsgálja, hogy a hazai szabályozás milyen mértékben képes kezelni az online zaklatás által felvetett problémákat. Ennek során különös figyelmet fordítottunk arra, hogy hol húzódnak a jelenlegi szabályozás határai, milyen jogi átfedések és hézagok tapasztalhatók a különböző jogterületek között, valamint, hogy milyen jogalkotási és jogalkalmazási lépések szükségesek annak érdekében, hogy a rendszer hatékonyabban tudjon reagálni egy ilyen érzékeny és dinamikusan változó társadalmi problémára. A vizsgálat rávilágított arra, hogy bár a magyar jog számos jogterülete – ideértve a büntetőjogot, az adatvédelmi

jogot, a polgári jogot, illetve a gyermekvédelmi rendelkezéseket – elviekben lehetőséget biztosít bizonyos online zaklatási formák kezelésére, az általános kép mégis meglehetősen széttagolt és töredezett. A jogalkalmazók gyakran nehézségekbe ütköznek az egyes esetek besorolása során, ugyanis hiányoznak azok az egységes fogalmi keretek és terminológiák, amelyek mentén a cyberbullying pontosan meghatározható és jogilag is megragadható lenne. A különböző jogágak közötti koordináció gyengesége, valamint a digitális környezet sajátosságainak – például az anonimitás, a határok nélküli kommunikáció, illetve a tartalmak gyors újraközlése – figyelmen kívül hagyása tovább nehezíti a hatékony jogérvényesítést. A tanulmány hangsúlyozta, hogy a digitális tér nem csupán egy új kommunikációs felület, hanem egy sajátos normarendszert és működési logikát követő társadalmi közeg, amelyhez a jogrendszernek alkalmazkodnia kell. Ezért nem elegendő pusztán jogtechnikai módosításokat végrehajtani, vagy az egyes jogszabályokat kiegészíteni bizonyos rendelkezésekkel. A cyberbullying elleni hatékony fellépés csak egy komplex, interdiszciplináris megközelítés mentén valósulhat meg, amely egyszerre épít a jogalkotás és jogalkalmazás eszközeire, a technológiai megoldásokra (pl. tartalomszűrők, jelentési rendszerek), az oktatási-nevelési programokra, valamint a társadalmi szemléletformálásra.

Ebben az összetett folyamatban a jog szerepe kettős: egyrészt biztosítania kell a normatív garanciákat az áldozatok védelmére, valamint lehetőséget kell adnia az elkövetők felelősségre vonására, másrészt irányt kell mutatnia a társadalom számára abban, hogy mely viselkedésformák tekinthetők elfogadhatatlannak, akár az online térben, akár a fizikai világban. A cyberbullying nem csupán egyéni tragédiák forrása, hanem a társadalmi kohéziót, a közösségi normák stabilitását és az emberi méltóság védelmét is alapjaiban érintő kérdés. A tanulmány külön figyelmet szentelt annak, hogy a cyberbullying áldozatai döntően gyermekek, serdülők és fiatal felnőttek, akik fokozottan ki vannak téve az online bántalmazás különböző formáinak, és akik gyakran nincsenek tisztában azzal, milyen jogi vagy technikai lehetőségeik vannak a védekezésre. Az ő védelmük tehát nem csupán jogi, hanem mély erkölcsi és társadalmi felelősség is. Ennek megfelelően a megelőzés, a korai felismerés és a tudatosítás kiemelt jelentőséggel bír. Az iskolai nevelésben, a pedagógusok képzésében, a szülők felkészítésében, valamint a digitális kompetenciák fejlesztésében rejlő lehetőségek nélkülözhetetlenek a probléma gyökerének kezeléséhez. A jog itt nem öncélú szabályrendszer, hanem a társadalmi együttélés kereteit kijelölő eszköz, amelynek célja az egyéni és közösségi jogok védelme egyaránt.

Összegzőként megállapítható, hogy a cyberbullying jogi megközelítése a kortárs jogrendszerek egyik legfontosabb „lakmuspapírja”. Azt vizsgálja, hogy a jogi normák képesek-e lépést tartani azzal a gyors és gyakran kiszámíthatatlan

technológiai és társadalmi változással, amelyet a digitalizáció idézett elő. Magyarország számára e téren a kihívás kézzelfogható és sürgető, ám ugyanakkor lehetőséget is rejt magában. Lehetőséget arra, hogy a jelenlegi, részben még elaprózott és esetenként reaktív szabályozás helyett egy jól strukturált, koherens és előrelátó jogi környezet jöjjön létre, amely képes a jogbiztonság, az emberi méltóság és a közösségi normák hatékony védelmére – immár az online térben is, ahol a jövő generációi formálódnak.

IRODALOMJEGYZÉK

- ANNA COSTANZA BALDRY – ANNA SORRENTINO – DAVID P. FARRINGTON: The Efficacy of the Tabby Improved Prevention and Intervention Program in Reducing Cyberbullying and Cybervictimization among Students. *Int. J. Environ. Res. Public Health*, 2018 (15).
- DEÁK DOROTTYA: A cyberbullying problémája Magyarországon. *A NIT ifjúsági szakmai folyóirata*, 2022 (2), file:///C:/Users/felhaszn%C3%A1l%C3%B3/Downloads/NIT_Y.Z.+Folyoirat_2022-2.lapszam-25-35.pdf
- DOMONKOS KATALIN: Cyberbullying: Zaklatás elektronikus eszközök használatával. *Alkalmazott pszichológia*, 2014 (1).
- GYURKÓ SZILVIA: A gyerekekkel szembeni online szexuális visszaélések és a készülő új EU rendelet háttere. *Családi jog*, 2023 (3).
- KAREN LUMSDEN – HEATHER M. MORGAN: 'Cyber-Trolling as Symbolic Violence: Deconstructing Gendered Abuse Online'. In: NANCY LOMBARD (ed.): *Routledge Handbook of Gender and Violence*. Chapter 12. London, Routledge, 2018. https://www.researchgate.net/publication/317551298_Cyber_trolling_as_symbolic_violence_deconstructing_gendered_abuse_online
- BÁRBARA MOLAS: Doxing: A Literature Review. ICCT Project Report, December 2024, https://icct.nl/sites/default/files/2025-01/Molas_Doxing%20A%20Literature%20Review.pdf
- MONORI ZSUZSANNA ÉVA: Zaklatás-e a cyberbullying? *In Medias Res*, 2016 (2).
- A Büntető Törvénykönyvről szóló 2012. évi C. törvény, <https://net.jogtar.hu/getpdf?docid=A1200100.TV&printTitle=2012.%20%C3%A9vi%20C.%20t%C3%B6rv%C3%A9ny>
- Az Európai Parlament 2018. szeptember 11-i állásfoglalása az Unión belüli, munkahelyen, nyilvános térben és a politikai életben elkövetett megfélemlítés és szexuális zaklatás megelőzését és az ellenük való küzdelmet szolgáló intézkedésekről (2018/2055[INI]), https://www.europarl.europa.eu/doceo/document/TA-8-2018-0331_HU.pdf
- 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), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1751114269007>

Az Európai Parlament és a Tanács (EU) 2024/1385 irányelve (2024. május 14.) a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024L1385>

Az Európai Parlament és a Tanács rendelete a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52022PC0209>

Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

Trusted flaggers under the Digital Services Act (DSA), <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>