



37. Országos Tudományos Diákköri Konferencia

Állam- és Jogtudományi Szekció

Budapest, 2025. március 24–26.

Rendező intézmény:

Károli Gáspár Református Egyetem

Állam- és Jogtudományi Kar



Állam- és Jog-
tudományi Szekció

A dolgozat címe

**A segítség egy kattintásnyira van!? A gyermekeket
érő cyberbullyinggal szembeni hatékony
reparációs megoldások szabályozási kerete**

Kézirat lezárásának dátuma:

2024.11.03.

Én, mint *A segítség egy kattintásnyira van!? A gyermekeket érő cyberbullyinggal szembeni hatékony reparációs megoldások szabályozási kerete* című dolgozat szerzője nyilatkozom, hogy a dolgozat megírásához semmilyen formában nem használtam mesterséges intelligenciát.

TARTALOMJEGYZÉK

BEVEZETÉS	1
1. A CYBERBULLYING FOGALMA ÉS TÍPUSAI	3
1.1. A CYBERBULLYING FOGALMA	3
1.2. A CYBERBULLYING JELLEMZŐ TÍPUSAI.....	8
2. CYBERBULLYING MEGOLDÁSOK NEMZETKÖZI KITEKINTÉSE	9
2.1. KITEKINTÉS AZ EURÓPAI UNIÓN KÍVÜLRE	9
2.1.1. Új-Zéland	9
2.1.2. USA	11
2.1.3. Egyesült Királyság.....	13
2.1.4. Ausztrália	14
2.2. IRÁNYADÓ SZABÁLYOK AZ EURÓPAI UNIÓBAN	15
2.2.1. <i>Digital Services Act</i>	15
2.2.2. <i>GDPR</i>	16
2.3. AZ EURÓPAI UNIÓ EGYES TAGÁLLAMAINAK GYAKORLATA	17
2.3.1. <i>Németország</i>	17
2.3.2. <i>Franciaország</i>	18
2.3.3. <i>Hollandia</i>	19
2.3.4. <i>Írország</i>	20
3. CYBERBULLYING TARTALOM ELTÁVOLÍTÁSA MAGYARORSZÁGON.....	22
3.1. AZ EKERTV. SZEREPE A SZEMÉLYISÉGI JOGOK VÉDELMEBEN A DIGITÁLIS PLATFORMOKON	22
3.2. MAGYARORSZÁGON ELÉRHETŐ HOTLINE-SZOLGÁLTATÁSOK	23
3.2.1. <i>Az Internet Hotline</i>	23
3.2.2. <i>Biztonsagosinternet.hu</i>	26
3.3. EGYES SOCIAL MÉDIA PLATFORMOK PANASZBEJELENTŐ RENDSZEREI MAGYARORSZÁGON	27
3.4. FELMÉRÉS A SZÜLŐK TUDATOSSÁGÁRÓL A CYBERBULLYINGOT ÉS A BÍRÓSÁGON KÍVÜLI TARTALOMELTÁVOLÍTÁSI ELJÁRÁSOKAT ILLETŐEN	29
ÖSSZEGZÉS.....	35
IRODALOMJEGYZÉK.....	1

BEVEZETÉS

A digitalizáció megjelenésével, illetve annak állandó fejlődésével a cyberbullying – különösen a gyermekeket és a serdülőket illetően – világszerte általános és folyamatosan növekvő problémát jelent.¹ Ez irányadó Európára és Magyarországra is, ahol az internet-penetráció meghaladja a 90 százalékot. A gyermekek már egészen kis koruktól kezdve digitális eszközök közt nőnek fel.² A felnőttekkel ellentétben a gyermekek még fejlődési szakaszban vannak, amely jobban sebezhetővé teszi őket a cyberbullying érzelmi és pszichológiai hatásaival szemben.³ A cyberbullying mélyreható kárt okozhat a fiatalok mentális jóllétét illetően, akár szorongáshoz, depresszióhoz vagy öngyilkosság gondolatának kialakulásához is vezethet,⁴ ezért létfontosságú a gyermekek online biztonságának megteremtése. A *K.U. kontra Finnország* ügyben az Emberi Jogok Európai Bírósága kimondta, hogy az államoknak megfelelő jogi eszközöket kell biztosítaniuk a személyiségi jogot sértő online tartalmak ellen, különösen, ha gyermekeket érint. Az anonim internethasználat védelme nem élvezhet prioritást az áldozat jogai és biztonsága felett.⁵

Kiemelt jelentősége van annak, hogy a szülők, a pedagógusok és a kiskorúak is tisztában legyenek azzal, hogy mit tudnak tenni cyberbullying jellegű online tartalom gyors és hatékony eltávolítása érdekében a közösségi médiában. A közhiedelemmel ellentétben a cyberbullyingnek nem kell ismétlődőnek lennie, hiszen megvalósulhat pusztán egy személyiségi jogot sértő fénykép vagy bejegyzés közzétételével is.

A dolgozat bemutatja a cyberbullying fontos fogalmi elemeit, valamint különböző fajtáit. A kutatás célja rávilágítani a személyiségi jogot sértő cyberbullying tartalmak online felületekről történő eltávolítási lehetőségeire bírósági eljáráson kívül, különös tekintettel a gyermekek védelme érdekében. A külföldi kitekintés keretében vizsgálja a tartalomeltávolításra vonatkozó jogi kereteket, illetve a civil szervezetek szerepét a folyamatban. Vizsgálja a tartalomeltávolításra vonatkozó jogi kereteket, illetve a civil szervezetek szerepét a törlési folyamatban. Az empirikus elemzés kitér arra is, hogy a magyar éves beszámolók alapján

¹ *The Canadian journal of psychiatry*, VAILLANCOURT – FARIS – MISHNA, 2017, 62.6: 368-373.

² Az alapvető jogok biztosának jelentése az AJB-686/2022.számú ügyben az online gyermekvédelem védelmi és jogorvoslati rendszerének működésével összefüggésben.

³ American Psychological Association: Social media brings benefits and risks to teens. Psychology can help identify a path forward.

⁴ Unicef: Protecting Children online.

⁵ European Court of Human Rights. *K.U. v. Finland*, Application No. 2872/02, 2008.

legveszélyesebbnek ítélt platformokon milyen tartalomjelentési opciók vannak, és ezeket felhasználói szemszögből nézve mennyire egyszerű, vagy éppen nehézkes elérni. A kiskorúakat érő cyberbullying és a káros tartalmak eltávolításával kapcsolatos szülői tudatosság felmérésére Google Forms segítségével kérdőíves kutatás készült. A kitöltés eredményessége érdekében az űrlap számos oktatási intézményhez lett eljuttatva, amelynek eredményei a kutatás végén ismertetésre kerülnek.

A releváns külföldi és magyar szakirodalmi források és jogszabályok mellett vizsgálat tárgyát képezték a hatáskörrel rendelkező külföldi és magyar szervek hivatalos honlapjain elérhető információk, továbbá tartalomeltávolítást végző vagy ahhoz kapcsolódóan a jogosultnak segítséget nyújtó szervek éves beszámolóit is.

A tanulmány kulcskérdése, hogy a különböző államok, különösen Magyarország, milyen eltávolítási mechanizmusokat alkalmaznak a cyberbullyinggal szemben, és ezek mennyire bizonyulnak eredményesnek a gyakorlatban. Arra keresi a választ, hogy ezek a gyakorlatok miként járulnak hozzá a gyermekek digitális környezetben történő védelméhez, illetve milyen hiányosságok tapasztalhatók az alkalmazásukban. A vizsgált államok megoldásainak górcső alá vételével kritikai észrevételek tehetők a szabályozás fejlesztése, valamint a szükséges intézményi keretek további erősítése érdekében.

1. A CYBERBULLYING FOGALMA ÉS TÍPUSAI

1.1. A CYBERBULLYING FOGALMA

A digitális ökoszisztémához tartozó egyes fogalmakhoz (például kibertér, kiberbiztonság) hasonlóan a cyberbullying is rendkívül nehezen határozható meg a jelenség rendkívül összetett jellege okán. Kutatók, nemzetközi szervezetek, az Európai Unió és a hozzá kapcsolódó Tubby Project is kísérletet tett a cyberbullying definiálásra, de pontosan a fentiek okán általánosan elfogadott meghatározása azonban nincs. E fejezet arra tesz kísérletet, hogy ezen fogalmak halmazából kiemeljen olyan jellemvonásokat, amelyek mentén a cyberbullying jelenség általános jellemzői rendszerezett formában áttekinthetővé váljanak.

Az ehhez kapcsolódó kutatás az alábbi fogalmakon alapszik:

1. A cyberbullying (online bántalmazás) az elektronikus kommunikációs technológiák használatát jelenti, olyan, egy másik személy ellen irányuló szándékos, ismételt, vagy sokak ellen (széles körben) kifejtett magatartást, amelynek eleme a kegyetlenség és az érzelmi terror. Az áldozat megközelítőleg csak az esetek felében tudja, hogy ki az elkövető (Tubby Project).⁶
2. A cyberbullying vagy elektronikus agresszió kegyetlen viselkedés másokkal szemben azáltal, hogy az internet vagy más digitális technológiák segítségével káros anyagokat küldenek vagy tesznek közzé, vagy a társadalmi agresszió más formáiban vesznek részt (Nancy Willard).⁷
3. A cyberbullying egy egyén vagy egy csoport által mások ellen elkövetett ismétlődő szóbeli vagy pszichológiai zaklatás. Ennek számos formája lehet: gúnyolódás, sértegetés, fenyegetés, pletyka, „happy slapping”, kellemetlen megjegyzések vagy rágalmazás (Európai Bizottság).⁸
4. Agresszív, szándékos cselekmény, amelyet egy csoport vagy egyén elektronikus kapcsolattartási formákat használva, ismételten és hosszabb időn keresztül követ el egy olyan áldozattal szemben, aki nem tudja könnyen megvédeni magát (Peter Smith).⁹
5. A cyberbullying a digitális technológiák felhasználásával történő zaklatás. Ez történhet a közösségi médiában, üzenetküldő platformokon, játékatplatformokon és mobiltelefonokon.

⁶ TABBY trip in Eu.

⁷ WILLARD: Educators guide to cyberbullying: Addressing the harm caused by online social cruelty.

⁸ Safer Internet Day 2009: Commission starts campaign against cyber-bullying.

⁹ *Journal of child psychology and psychiatry*, SMITH, 2008, 49.4: 376-385.

Ismétlődő viselkedés, amelynek célja, hogy megijessze, feldühítse vagy megszegyenítse azokat, akiket célba vesz (Unicef).¹⁰

6. A cyberbullying hasonló a zaklatás különböző típusaihoz azzal a különbséggel, hogy online, vagy szöveges üzenet küldésével történik (Commonwealth of Pennsylvania).¹¹
7. Egy csoport vagy individualizmus által végrehajtott szándékos károsító magatartás, amelyet a modern digitális technológiát használva egy olyan áldozat ellen, aki képtelen megvédeni magát, idővel ismételten elkövetnek, továbbá az agresszor valamilyen módon erősebb, mint a célszemély (Marylin Campbell).¹²
8. A cyberbullying az a törekvés, hogy egy személynek érzelmi és pszichológiai kárt okozzanak egy online zaklatási kampány révén (Julianne Klein).¹³
9. A cyberbullying a technológia használata egy másik személy zaklatására, fenyegetésére, zavarba hozására vagy célpontként való felhasználására (TeensHealth).¹⁴
10. Bármilyen szándékos és agresszív üzenet, amelyet időn keresztül ismételnék valakivel szemben, aki nem képes megvédeni magát elektronikus kommunikációs eszközök segítségével (Menesini és Nocentini).¹⁵
11. A cyberbullying olyan zaklatás, amely a technológia segítségével történik (Australian Human Rights Commission).¹⁶
12. A cyberbullying a digitális technológia – például telefon, táblagép, játékkonzol vagy számítógép – használata egy másik személy (vagy személyek) zaklatására e-mailen, közvetlen üzenetküldő platformokon, közösségi médián, hang- és videóplatformokon vagy szöveges üzeneteken keresztül. Ez magában foglalja olyan tartalmak megosztását vagy közzétételét, amelyek célja egy másik személy megalázásának vagy megszegyenítésének okozása (Kaspersky).¹⁷
13. A cyberbullying magában foglalja bántó vagy kegyetlen üzenetek vagy képek küldését vagy posztolását az internet vagy más digitális kommunikációs eszköz, mint a mobiltelefon segítségével (Ted Feinberg és Robey Nicole).¹⁸

¹⁰ Unicef: Cyberbullying: What is it and how to stop it.

¹¹ Commonwealth of Pennsylvania: Cyberbullying.

¹² *Journal of Psychologists and Counsellors in Schools*, CAMPBELL, 2005, 15.1: 68-76.

¹³ Study.com: Cyberbullying Definition, Effects & History.

¹⁴ TeensHealth: Cyberbullying.

¹⁵ *Zeitschrift für Psychologie/Journal of Psychology*, MENESINI – NOCENTINI. 2009, 217.4: 230-232.

¹⁶ Australian Human Rights Commission: Cyberbullying.

¹⁷ Kaspersky: What is cyberbullying?

¹⁸ *The education digest*, FEINBERG – ROBEY, 2009, 74.7: 26.

Ezen fogalmak áttanulmányozása után arra a következtetésre jutottam, hogy egyes elemek feltétlenül szükségesek a cyberbullying azonosításához, egyesek azonban csak eshetőlegesen kapcsolódnak a jelenséghez. Az általam vizsgált definíciók mindegyikében fellelhető a technológiai eszköz használata és a zaklatás valamilyen formája, ami nem meglepő a kifejezés elnevezését tekintve. A szándékosság, káros hatás, anonimitás, nyilvánosság, ismétlődés és a hatalmi különbség az elkövető és az áldozat között nem szükségszerű, de gyakori elemei a cyberbullyingnak. A továbbiakban ezen szükséges és eshetőleges elemek kerülnek kifejtésre.

Technológiai eszköz használata

A cyber szó jelentése a Cambridge szótár szerint minden olyan dologra utal, amely számítógépekkel kapcsolatos, számítógépeket használ, vagy azokhoz kapcsolódik, különösen az internet vonatkozásában.¹⁹ Tekintettel arra, hogy a cyberbullying kifejezés önmagában utal a tevékenység elektronikus úton történő kifejtésére, az elektronikus eszköz felhasználásával történő megvalósítás vitathatatlan.

Zaklatás

A zaklatás a cyberbullying tekintetében egy gyűjtőfogalom, amely többféle módon valósulhat meg. Ezt támasztják alá a következő pontban kifejtésre kerülő cyberbullying formái is, ahol az online megfélemlítésen belül egy további alpont szintén a zaklatás. Gyakran magában foglalhat közvetlen fenyegetéseket, mint például sértő üzenetek, zsarolás, vagy a személyes információk nyilvánosságra hozatala.²⁰ Másrészt agresszívnek tekinthető akkor is, ha nem egyszeri eseményként, hanem ismétlődő cselekvéssorozatként valósul meg, amely során az elkövető újra és újra támadja az áldozatot, így folyamatosan erősítve a félelem és a szorongás érzését.²¹ Emellett a cyberbullying gyakran magában foglalja az áldozat nyilvános megalázását, például kompromittáló képek, videók vagy információk megosztását nagy nyilvánosság előtt.²²

Szándékosság

A fogalmak egy része kifejezetten használja a szándékosság kifejezést, egy részük azonban nem is utal rá. A legtöbb esetben valóban elképzelhetetlen a cyberbullying szándékosság nélkül.

Azonban figyelembe véve azt, hogy például a mostani generáció már a digitalizált világba születik, a fiatalok koruknál fogva nincsenek feltétlenül tisztában azzal, hogy mi a bántó avagy vicces, nem is beszélve az egyének eltérő reagálását, így a kettő közötti határ nem választható

¹⁹ Cambridge Dictionary: Cyber.

²⁰ Commonwealth of Pennsylvania. i. m.

²¹ TeensHealth. i. m.

²² FEINBERG – ROBEY. i. m.

el élesen egymástól.²³ Tehát egyáltalán nem biztos, hogy a támadó tudatában van annak, hogy a másik fél az üzenetet megszégyenítőnek, megalázónak tartja és nem heccként értékeli.

Káros hatás

A cyberbullying célja az áldozat megalázása, megszégyenítése, vagy érzelmi bántalmazása, ami súlyos pszichológiai következményekkel járhat, és sok esetben azzal is járt, mint például szorongás, depresszió, vagy akár öngyilkossági gondolatok.²⁴

Nyilvánosság

Nyilvánosan valósul meg a cyberbullying, ha egy közösségi platformon, vagy bármilyen elektronikus felületen a nagy nyilvánosság előtt kerül sor az áldozat megszégyenítésére, jó hírnevének rontására.²⁵ A cyberbullying megtörténhet azonban privát üzenetek küldésével is, ahol azzal címzettént kizárólag az áldozat fog találkozni.²⁶

Anonimitás

Az anonimitás az elkövetés egy lehetséges módja, ebben az esetben az áldozat nem tudja, hogy ki a zaklatója, lehet egy teljesen ismeretlen személy, de akár egy ismerős vagy barát is.²⁷ A névtelenség azonban nem törvényszerű. Elképzelhető ugyanis, hogy a cyberbullying elszenvedője tisztában van a támadója kilétével. Az online térben az anonimitás azért lehet kedvelt, mert az agresszor nehezen azonosítható, különösen hamis felhasználónév használatával, illetve nem is kell korábbi kapcsolatban állnia az áldozattal.²⁸

Ismétlődés

Egyes szakirodalmi és szervezeti definíciók, mint amilyeneket a Smith-féle kutatások, az UNICEF, vagy az Európai Bizottság fogalmazott meg, valóban hangsúlyozzák, hogy a cyberbullying esetén az online megfélemlítésnek ismétlődő jellegűnek kell lennie. Ez a megközelítés arra összpontosít, hogy a rendszeres vagy folyamatos támadások jelentik a valódi problémát, mivel azok súlyosabb és tartósabb pszichológiai hatásokkal járhatnak az áldozatokra nézve. Azonban véleményem szerint ezzel a definíció túlságosan szűkre szabott, és nem veszi figyelembe a cyberbullying teljes spektrumát.

²³ *Human communication research*, FESTL – QUANDT 2013, 39.1: 101-126.

²⁴ *Computers & Education*, GUALDO et al. 2015, 82: 228-235.

²⁵ *Journal of youth and adolescence*, STICCA – PERREN, Sonja. 2013, 42: 739-750.

²⁶ HUDSON – INKELL, LLC: Cyber Bullying Stories: The Ryan Halligan Case (1989 – 2003). 2020.10.05.

²⁷ STICCA –PERREN. i. m.

²⁸ *Psychology of Popular Media Culture*, BARLETT, 2015, 4.2: 70.

Ha csak az ismétlődő támadások számítanak valódi zaklatásnak, akkor egyetlen fenyegető üzenet, vagy egy kompromittáló kép posztolása, amely egyszeri incidensként történik,²⁹ teljesen elfogadhatóvá válna ezen fogalmi keretek között. Ez komoly problémát jelenthet, hiszen az ilyen egyedi, de súlyos támadások is jelentős mentális és érzelmi hatásokat gyakorolhatnak az áldozatokra.³⁰

Hatalmi különbség

A cyberbullying esetén a hatalmi egyensúlyhiány nemcsak fizikai szempontból, hanem az elkövető népszerűsége és technológiai ismeretei alapján is mérhető. Az anonimitás további hatalmat adhat az elkövetőnek, mivel az áldozat nem képes azonosítani őt, így a zaklatás hatása még fokozottabbá válik a hatalmi egyensúlyhiány következtében.³¹ Hatalmi egyensúlytalanságot eredményezhetnek a nyelvi nehézségek, amelyhez már a cyberbullyingot megelőzően is fennálló szorongás, valamint depresszió társulhat,³² illetve szintén kiszolgáltatott helyzet állhat fenn súlyproblémákkal és figyelemzavarral való küzdés esetén.³³ Azonban nem csak népszerű személy, vagy technikai zseni lehet zaklató, és a bántalmazott személy sem feltétlenül népszerűtlen,³⁴ így hatalmi különbségnek nem szükséges fennállnia a cyberbullying elkövetéséhez.

Megvizsgálva ezen fogalmi elemeket, javasolt a cyberbullying szélesebb körű értelmezése a nélkülözhetetlen tartalmi komponenseket tartalmazó definícióval, amely a bullying digitális aspektusait középpontba helyezve elősegíti a különböző tényállások egyszerűbb integrálását. E szerint a cyberbullying digitális eszköz alkalmazásával megvalósított megfélemlítés. A további jellemzők, mint szándékosság, ismétlődő jelleg, anonim elkövetés, nyilvánosság, hatalmi erőfölény, illetve káros következmények opcionális tényezők a cyberbullying kapcsán. Ezzel a megközelítéssel a fogalom szélesebb körű alkalmazhatósága biztosított, miközben a bullying digitális aspektusai kerülnek középpontba.

²⁹ YMCA of greater brandywine: Cyberbullying: What You Need to Know.

³⁰ *Journal of Educational Administration*, HOFF – MITCHELL, 2009, 47.5: 652-665.

³¹ *ASEAN Journal of Psychiatry*, GUAN, 2016, 17.1: 104-115.

³² The Canadian Encyclopedia: Amanda Todd Case.

³³ Nowcomment: The Top Six Unforgettable CyberBullying Cases Ever.

³⁴ Laws: Who was Alexis Pilkington?

1.2. A CYBERBULLYING JELLEMZŐ TÍPUSAI

A cyberbullying-nak jelenleg tíz nevesített változata létezik. A technikai fejlődések újabb és újabb utat nyitnak a cyberbullying eddig nem ismert típusainak, így ezen felsorolás is bővíthet a jövőben.

Lángharcnak (flaming) nevezzük a dühös és durva hangvételű vitákat elektronikus üzeneteken keresztül. *Zaklatás* vagy *megfélemlítés* (harrassment) valósul meg ismételt bántó, durva online üzenetek küldésével. *Hírnévrontás* (denigration) alatt pletykák terjesztését vagy közzétételét értjük valakiről azzal a céllal, hogy rontsák a hírnevét vagy aláássák a baráti kapcsolatait. *Outing* valósul meg más titkainak, bizalmas információinak közzétételével az interneten. Az *átverés* (trickery) bizalmas információk megszerzése megtévesztéssel, majd ezek közzététele az interneten. *Kiközösítésről* (exclusion) beszélhetünk akkor, amikor valakit egy online közösségből szándékosan kiközösítenek. *Cyberstalking* valósul meg fenyegető tartalmú ismételt zaklatás vagy becsmérítés esetén. *Online fenyegetés* (cyberthreats) alatt olyan, közvetlen fenyegetéseket vagy nyugtalanító kijelentéseket értünk, amelyekből úgy tűnik, hogy az elkövető érzelmileg felkavart, és fontolgatja, hogy valaki mást, vagy magát bántja, illetőleg öngyilkosságot követ el. Végül *sexting* esetén a zaklató szexuálisan provokatív és saját maga által készített meztelen vagy félig meztelen képeket vagy nyíltan szexuális tartalmú szöveget küld el online valakinek.³⁵

Ebből is jól látható, hogy a cyberbullying számos formát ölthet. Lehet például sértő e-mailek vagy szöveges üzenetek küldése; sértések chatszobákon vagy üzeneten keresztül; fotók vagy videók megosztása mobiltelefonon vagy az interneten; kizárás a közösségi hálózatokból, vagy mások hitelesítő adatainak és személyazonossági adatainak ellopása.³⁶

³⁵ TUBBY trip in EU; WILLIARD, N. Educator's guide to cyberbullying, cyberthreats & sexting. 2010.

³⁶ *European Journal of Developmental Psychology*, MENESINI – SPIEL, 2012, 9.2: 163-167.

2. CYBERBULLYING MEGOLDÁSOK NEMZETKÖZI KITEKINTÉSE

E fejezet az egyes államok, valamint az Európai Unió cyberbullying tartalmak eltávolítására vonatkozó szabályozását és gyakorlati megoldásait vizsgálja. Minden ország egyedi megközelítésekkel válaszol a cyberbullying kihívásaira, amelyek a jogi keretek mellett a civil szervezetek szerepét, valamint a platformszolgáltatók felelősségét is magukban foglalják.

2.1. KITEKINTÉS AZ EURÓPAI UNIÓN KÍVÜLRE

2.1.1. Új-Zéland

Új Zélandon 2015-ben került elfogadásra a *Harmful Digital Communications Act* (HDCA). Főbb pontjai közé tartozik az a tíz alapelv, amely meghatározza, hogy mire tilos a digitális kommunikációt felhasználni. Az alapelvek között szerepel a személyes adatok nyilvánosságra hozásának, hamis állításoknak és megfélemlítésnek a tilalma, ezen felül nem lehet obszcén, és nem használható fel zaklatásra.³⁷ A jogszabály arra kötelezi a platformszolgáltatókat, hogy hatékony és könnyen elérhető panaszeljárást szolgáltassanak a felhasználók számára, így az online tárhelyszolgáltatóhoz lehet fordulni kompromittáló tartalom eltávolításának kérelme végett. A panasz megtehető az érintett által írásban, vagy a Netsafe közreműködésével, aki a panaszos nevében intézkedik a tartalom eltávolítása érdekében.³⁸ A panasznak tartalmaznia kell az érintett elérhetőségét, a konkrét tartalmat az azonosíthatóság érdekében, valamint hivatkozni kell arra is, hogy az online anyag miért jogellenes vagy miért ütközik az említett tíz alapelv legalább egyikébe. Végül nyilatkozni kell arról, hogy a panaszkezelés során a felelős személy előtt kívánja-e a személyazonosságának felfedését. Amennyiben a Netsafe-hez való fordulás nem vezetett eredményre, a kerületi bíróság intézkedése, mint végső eszköz vehető igénybe.³⁹ A bíróság ekkor széleskörű jogorvoslati lehetőségekkel élhet, például kötelezhet a tartalom eltávolítására, felszólíthat a jogsértés megszüntetésére, helyreigazítást rendelhet el. Ekkor még pénzbüntetés és börtönbüntetés elrendelésének nincs helye, azonban hat hónap elteltével, ha a bíróság döntésének nem tett eleget a kötelezett, cselekménye bűncselekménynek minősül, és akár hat hónap börtönbüntetés vagy 5.000 dollár pénzbüntetésre ítélték, a cégek 20.000 dollárig terjedő pénzbírsággal is sújthatók.⁴⁰

³⁷ Harmful Digital Communications Act 2015.

³⁸ Criminal & traffic law: Cyberbullying: Protections against online/digital harassment.

³⁹ New Zealand Parliament. (2015). *Harmful Digital Communications Act*.

⁴⁰ Justice.govt.nz: Applying for a Harmful Digital Communications order.

A *Netsafe* egy nonprofit online biztonsági szervezet, célja az online kihívások kezelése, biztonságos online élet minden korosztály számára, amely gyakorlati eszközök, támogatás és tanácsadás révén valósul meg. Független, amely együttműködik a kormánnyal és a bűnüldöző szervekkel. A Netsafe iskoláknak, szülőknek és fiataloknak szóló digitális forrásokat kínál, ilyen a Hector's World, amely 2024-ben indult újra, hogy jobban tükrözze a gyerekek számára releváns kortárs digitális problémákat, biztosítva, hogy a karakterek és a történetek a mai fiatalok számára is relevánsak legyenek. Sajnos az általuk közzétett videók Magyarországon nem elérhetők.⁴¹ A tanárok és iskolák számára a Kete nevezetű weboldaluk nyújt további segítséget az online biztonság megteremtése érdekében.⁴²

A Netsafe 2023-mas éves beszámoló alapján az adott évben összesen 23,213 bejelentés érkezett, a HDCA-val kapcsolatos panasz ebből 5023 volt. A legtöbb panasz képpel való visszaélésre és az adatvédelem megsértésére vonatkozott, és a bejelentők 72%-a maga jelentette a problémát, 12%-a pedig a szülőktől és a gyámoktól származott. A HDCA-val kapcsolatos sikerességi rátája igen ígéretes, 94%-os hatékonyságról számoltak be.⁴³

2024 első negyedéves jelentés szerint 6497 bejelentés történt, ebből 1396 érintette a személyiségi jogokat. A panaszok 41%-a 22 és 40 év közöttiektől, 29% 41 és 61 közöttiektől, és 16%-ban kiskorúaktól származik.⁴⁴ A második negyedévben 6768 bejelentés érkezett a Netsafe-hez, melyből 1769 panasz személyiségi jogsértéssel áll összefüggésben, így megjelenik a zaklatás, a szexuális tartalmú zaklatás és személyes információk engedély nélküli közzététele. A bejelentések 41%-át 22 és 40 év közötti személyek tették, azonban a kiskorúak által tett bejelentés is 15%.⁴⁵

Ezen arányokból nem lehet pontosan következtetni arra, hogy a személyiségi jogot sértő tartalmak hány százalékban érintettek kiskorú jogalanyokat. Ugyanakkor az egyértelműen látszik, hogy a kiskorúak is szép számmal tettek bejelentést. Továbbá elképzelhető, hogy a 22-40, valamint a 41-61 év közötti bejelentők közül többen a gyermekük nevében és védelme érdekében jelentettek káros tartalmat.

⁴¹ Hector's world: About Us.

⁴² Netsafe: About Netsafe.

⁴³ Netsafe: Annual Report 2022/2023.

⁴⁴ Netsafe: Quarterly Report January-March 2024.

⁴⁵ Netsafe: Quarterly Report April-June 2024.

2.1.2. USA

Az Egyesült Államokban nincs közvetlen szövetségi szintű törvény kifejezetten a cyberbullying-ra vonatkozóan, azonban a *Children's Online Privacy Protection Act*, (COPPA) egy olyan amerikai szövetségi törvény, amelyet a 13 év alatti gyermekek digitális térben való védelme érdekében alkottak meg. A COPPA előírja, hogy az adatokat gyűjtő weboldaloknak szülői hozzájárulást kell kérniük, mielőtt személyes adatokat gyűjtenének vagy tennének közzé a gyermekről. A szolgáltatóknak részletes adatvédelmi tájékoztatóval kell rendelkeznie, továbbá biztosítani kell az összegyűjtött adatok védelmét a jogosulatlan hozzáféréstől.⁴⁶

A szövetségi szintű szabályozás hiánya okán e terület rendezése elsősorban a tagállamok hatáskörébe tartozik.⁴⁷ Egyes esetekben, közvetetten alkalmazhatóak a szövetségi szabályozások, például a diszkriminációellenesek, azonban ezek csak anyagi jogorvoslatot biztosítanak, amelyek nem nyújtanak átfogó megoldást a cyberbullying kezelésére.⁴⁸ A tagállamok különböző intézkedéseket hoztak a gyermekek védelmére. Ennek részeként irányelveket vagy modellszabályokat dolgoztak ki iskolák és oktatási körzetek számára. A legtöbb állam előírja a cyberbullying elleni stratégiákat és eljárások bevezetését, néhányuk megelőző programokat és tanárok képzését is megköveteli.⁴⁹ Az eltérő tagállami megoldások miatt nem létezik egységes megközelítés a cyberbullying elleni fellépésre, amely megnehezíti a jogalkalmazást.⁵⁰

Számos államban terjesztették ki a zaklatásellenes törvények hatályát az elektronikus cselekményekre. Kalifornia egy ezen tagállamok közül, amely a cyberbullying elleni törvényt fogadott el. Többek között a *California Student Safety Prevention Act*, a *Safe Place to Learn Act* és a *Student Civil Rights* tartalmaz a cyberbullyingra és a diszkriminációra is vonatkozó szabályokat. A kiskorúak védelme érdekében Kaliforniában az iskolák is nagyobb autonómiát kapnak a cyberbullying elleni küzdelemben. Lehetőség van például egy tanuló felfüggesztésére, esetlegesen kizárására akár online akár offline bullying miatt.⁵¹ Texasban a *Texas Education Code* irányadó a kiskorúak által és kiskorúak ellen elkövetett cyberbullyingra.⁵² New Yorkban is kiemelkedő szerepük van az iskoláknak a különféle zaklató magatartások megelőzésében és kezelésében. 2012-ben például a bíróság több mint egy millió dollárt ítélt meg annak a New

⁴⁶ Federal Trade Commission. (1999). *Children's Online Privacy Protection Rule*.

⁴⁷ *The Palgrave handbook of international cybercrime and cyberdeviance*, BOSSLER, 2020, 257-280.

⁴⁸ *World Medical & Health Policy*, YANG – GRINSHTEYN, 2016, 8.4: 458-477.

⁴⁹ stopbullying.gov: Laws, Policies & Regulations.

⁵⁰ BOSSLER: i. m.

⁵¹ LUEVANOS. A Policy Analysis on California's Cyber Bullying Laws Under the Education Code. 2014. PhD Thesis. California State University, Bakersfield.

⁵² stopbullying.gov: Texas Anti-Bullying Laws & Policies.

York-i diáknak, származása miatti cyberbullying okán beperelte az iskoláját, és a bíróság megállapította, hogy az iskola nem tett eleget, sőt szándékosan közömbös magatartást tanúsított a cselekmény jelentésére, amely elősegítette a zaklató magatartás folytatását.⁵³

A *Cyberbullying Reserach Center* 2005-ben kezdte meg működését az USA-ban. Célja naprakész információkat szolgáltatni a kiskorúak körében tapasztalható cyberbullying természetéről, mértékéről, okairól és következményeiről. Számadatok és részletes történetek találhatók az érintettektől. Az oldal számos olyan forrást tartalmaz, amelyek segítenek megelőzni a cyberbullying incidenseket, illetve reagálni rájuk.⁵⁴ Így az iskoláknak javasolja például, hogy az iskolai szabályzatban rögzítsék a megfélemlítés, zaklatás, cyberbullying egzakt fogalmát, fektessenek le arányos, például a magatartás típusához, időtartamához igazodó következményeket, illetve egyértelműen határozzák meg a jelentés menetét.⁵⁵

A *Stomp Out Bullying* szintén 2005-ben alapított nonprofit szervezet, amely az amerikai fiatalok körében tapasztalható offline és cyberbullying ellen küzd. Sokoldalú megközelítésével a szervezet felhívja a figyelmet a cyberbullying veszélyeire és megelőzésére, emellett támogató szolgáltatásokat, és oktatási anyagokat kínál diákoknak, pedagógusoknak és szülőknek. A legfontosabb kezdeményezések közé tartoznak az olyan országos kampányok, mint a National Bullying Prevention Month, és a Blue Shirt Day, továbbá a zaklatás áldozatai számára létrehozott bizalmas HelpChat vonal, valamint a megelőzési és beavatkozási stratégiákról szóló átfogó útmutatók. Munkája kulcsfontosságú mind a hagyományos zaklatás, mind a mai digitális környezetben egyre gyakoribbá váló cyberbullying kezelésében.⁵⁶

Az *End to Cyber Bullying* (ETCB) egy nonprofit szervezet, amelynek célja a cyberbullying elleni küzdelem. Az ETCB szerint kiemelt fontosságú a figyelem felkeltése, az átfogó információk megosztása, valamint a támogató és hozzáférhető szolgáltatások biztosítása. Fontos szerepet kap továbbá a diákok, oktatók, szülők és más közösségek mozgósítása. Az ETCB célja egy olyan globális közösségi hálózat létrehozása, amelyben minden felhasználó biztonságban érezheti magát. Önkéntesei az Egyesült Államokban és a világ különböző részein iskolákat látogatnak, és előadásokat tartanak iskoláskorú gyermekek. Ezeken az előadásokon a cyberbullying jeleinek felismeréséről, a megelőzés módjairól és arról adnak tanácsot, hogyan lehet az adott iskolákban saját ETCB-kezdeményezéseket indítani.⁵⁷

⁵³ *Implications for School Policy and Practice*. HINDUJA – PATCHIN, 2015, 5: 1-3.

⁵⁴ Cyberbullying Research Center.

⁵⁵ HINDUJA: i. m.

⁵⁶ Stomp Out Bullying.

⁵⁷ End to Cyber Bullying: About Us.

2.1.3. Egyesült Királyság

A 2023-as *Online Safety Act* átfogó szabályozási keretet vezet be az online megfélemlítés kezelésére, a gyermekek védelmére és az online platformok felelősségre vonására a káros tartalmak miatt. A törvény megkülönbözteti az elsődleges prioritású tartalmat, mint a zaklatás, sértő nyelvhasználat, pornográfia és önkárosítást népszerűsítő tartalom, valamint a priorizált tartalmat. A platformoknak intézkedéseket kell tenniük annak megakadályozására, hogy a gyermekek ilyen káros tartalommal találkozzanak. Ennek érdekében a szolgáltatóknak kockázatfelmérést kell végezniük, és következetesen alkalmazniuk kell az életkor-ellenőrzési rendszereket, hogy biztosítani tudják a korosztálynak megfelelő tartalomhoz való hozzáférést. Az OFCOM feladata, hogy figyelemmel kísérje és felülvizsgálja a gyermekeket érintő káros tartalom jelenlétét.⁵⁸

Az Egyesült Királyságban (EK) a *UK Safer Internet Centre* arra hivatott, hogy ingyenes tanácsot nyújtson az online káros tartalom bejelentésére. A szakemberek nemcsak áttekintik ezen tartalmat, hanem aktívan kommunikálnak az áldozatokkal, szükség esetén útmutatást és közvetítői támogatást nyújtanak. EK-ban a szervezetek – ideértve az iskolákat, egyetemeket is – maguk dönthetik el, hogy a weboldalaikra ingyenesen telepítik-e a káros tartalom bejelentése gombot, így a honlapon meg fog jelenni ez az opció, amely hatékonyabbá teszi a legális, de káros tartalmak jelentését a felhasználók számára.⁵⁹ A *Report Harmful Content* egy nemzeti alternatív vitarendezési szolgáltatás, amely lehetőséget biztosít az EK-ban élő, 13 éven felülieknek a káros tartalmak jelentésére az interneten.⁶⁰ A szolgáltatás csak akkor tud segítséget nyújtani, ha az általa partnerségben álló 25 platform valamelyikén tettek közzé káros anyagot, és már a platformszolgáltató felé megtették a bejelentést, de szeretnék, ha az eredményt felülvizsgálnák.

2023-ban 5101 bejelentést regisztráltak, ez azonban tartalmaz olyan panaszokat is, amelyek nem tartoznak a szolgáltatás hatáskörébe. A vitarendező szolgáltató nem kötelezheti, csak ösztönözheti a platformokat a tartalom eltávolítására, amely tavaly így is 86%-ban vezetett eredményre. A panaszok legnagyobb része, 45%-a zaklatás és megfélemlítés, 22% más személy nevében létrehozott profil miatt, 10% pedig visszaélések miatt érkezett, illetve a bejelentők 18%-a kiskorú volt.⁶¹ A panaszok többségét a személyiségi jogot sértő cyberbullying ellen

⁵⁸ UK Parliament. (2023). *Online Safety Act 2023*.

⁵⁹ UK Safer Internet Centre: Home.

⁶⁰ Report Harmful Content: Making a Report to Report Harmful Content.

⁶¹ Insights and Trends: Analysis of report Harmful Content 2023.

jegyzték, és azt ugyan nem tudjuk, hogy az összes bejelentésből mennyi került befogadásra, azonban a 86%-os sikerességi ráta mindenféleképpen nagyon jó aránynak mondható.

2.1.4. Ausztrália

Ausztráliában az *Enhancing Online Safety Act* hívta életre az eSafety Commissioner hivatalát, amely széleskörű jogosítványokkal rendelkezik az online biztonság megvalósítása érdekében, különösen a gyermekeket érintő cyberbullying tartalmak gyors eltávolítása érdekében. Amennyiben okkal feltehető, hogy egy gyermek cyberbullying áldozatává vált, akkor a biztosnál az ügyel kapcsolatban panasz tehető. A cyberbullying megfékezése érdekében a jogszabály alapvető követelményeket fogalmaz meg a közösségi médiaplatformokkal szemben is, így például kötelesek működtetni egy panaszrendszert, amelyen keresztül a felhasználók jelenthetik a bántalmazó tartalmakat. A platformoknak a panasz megtételétől számított 48 órán belül el kell távolítaniuk ezeket az online anyagokat.⁶² Az eSafety Commissioner rendelkezik saját online biztonsági oktatóanyagokkal is, amelyek lehetőséget biztosítanak a gyermekek számára, hogy megértsék, mi a teendő, ha zaklatás áldozatává válnak.⁶³

Az eSafety akkor tud segíteni, ha ausztrál állampolgárt sértő cyberbullying tartalom legalább 48 órája jelentve lett a platformon, azonban az továbbra is elérhető és egyértelműen beazonosítható a tartalom elérési helye. A bejelentést a hivatalos honlapon lehet megtenni, ahol a gyermeket ért cyberbullying opció után különböző kérdéseket kell megválaszolni.⁶⁴ Az eSafety Commissioner-hez négy bejelentési rendszere közül ez az egyik, az ausztrál gyermekekre vonatkozó cyberbullying rendszer, amelyen keresztül a biztos felelősségre vonhatja a platformokat a gyermekeket célzó, súlyosan káros tartalmak eltávolításáért. 2023-ban ezen rendszeren keresztül 2693 panasz érkezett, amely a jelentés szerint a korábbi évekhez képest 37%-os növekedést jelent. A beszámolóból nem tűnik ki azonban, hogy a panaszok alapján a platformszolgáltatók felé küldtek-e ki eltávolítási felszólítást. Következtetéseim szerint nem történt ilyen, ugyanis a felnőttekre vonatkozó rendszernél külön említi a beszámoló a szolgáltatókhoz intézett eltávolítási felszólítások számát, bár a bejelentésekhez képest nagyon elenyésző számban került erre sor.⁶⁵

Ausztráliában több hotline, például a *Lifeline Australia*, valamint a *Kids Helpline* nyújt ingyenes, 24 órás segítséget a válsághelyzetek kezelésében. A Lifeline különösen az

⁶² *Online Safety Act 2015*.

⁶³ eSafety Commissioner: Cyberbullying advice for educators and schools.

⁶⁴ eSafety Commissioner: Report online harm.

⁶⁵ Australian Communications and Media Authority eSafety Commissioner: Annual Report 2023-24.

öngyilkosság megelőzésére, a mentális egészség támogatására és az érzelmi segítségnyújtásra összpontosít. Mind telefonos, mind személyes tanácsadás és az online támogatás is rendelkezésre áll.⁶⁶ A Kids Helpline Ausztrália online és telefonos tanácsadási szolgáltatás kifejezetten az 5 és 25 év közötti fiatalok számára segít olyan problémák kezelésében, mint a párkapcsolati zavarok, a zaklatás, a mentális egészséggel kapcsolatos kihívások.⁶⁷

2.2. IRÁNYADÓ SZABÁLYOK AZ EURÓPAI UNIÓBAN

Az Európai Unió jogszabályai, különösen az adatvédelmi és digitális szolgáltatások szabályozása alapvető szerepet töltenek be a tagállamok online tartalomkezelésében. A Digital Services Act (DSA) központi jelentőségűek a közösségi média platformok működésében, különös tekintettel a jogsértő tartalmak kezelésére.

2.2.1. Digital Services Act

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete a digitális szolgáltatásokról (DSA) ésszerű, arányos és hatékony kockázatcsökkentő intézkedések alkalmazását írja elő az online óriásplatformok és népszerű keresőmotorokat működtető szolgáltatók számára. A rendelet tizenegy lehetséges intézkedést sorol fel, ezen felsorolás nem taxatív. A cyberbullying megelőzése szempontjából fontos a tartalommoderálási eljárások fejlesztése, amely lehetővé teszi a jogellenes tartalmak gyorsabb és hatékonyabb feldolgozását. Emellett lényegesek a célzott intézkedések a gyermekek jogainak védelme érdekében, mint például az életkor-ellenőrzés és a szülői felügyeleti eszközök bevezetése, amelyek segítik a gyermekeket abban, hogy jelenthessék a cyberbullyingot vagy segítséget kérhessenek. A tudatosságnövelő intézkedések is kulcsfontosságúak a felhasználók tájékoztatását illetően. A platformoknak figyelniük kell algoritmikus rendszereik és ajánlórendszereik módosítására is, hogy elkerülhető legyen a cyberbullying tartalmak ajánlása. A belső folyamatok és erőforrások megerősítése is elengedhetetlen a rendszerszintű kockázatok észleléséhez, így a platformok hatékonyabban reagálhatnak a cyberbullying problémáira. Ezen platformszolgáltatók minden évben független ellenőrzésen esnek át, melynek keretében a kötelező és vállalt kötelezettség teljesítését vizsgálják. A szolgáltatóknak emellett évente legalább egyszer átlátható, világos jelentést kell készíteniük az elvégzett tartalommoderálásokról. A tárhelyszolgáltatókra, így az online platformokra is vonatkoznak egyes további követelmények. A cyberbullying megelőzését célzó kritérium, hogy a szolgáltatóknak egyszerűen hozzáférhető és felhasználóbarát bejelentési

⁶⁶ Lifeline: Who we are.

⁶⁷ Kids Helpline: About.

mechanizmust kell működtetniük, amely lehetővé teszi a jogellenes tartalom jelentését. Az online platformoknak legalább hat hónapig biztosítaniuk kell a felhasználók számára egy hatékony belső panaszkezelési rendszert, amely lehetővé teszi, hogy a felhasználók elektronikusan és ingyenesen nyújtsanak be panaszokat a szolgáltató döntései ellen. A panasz benyújtása akkor lehetséges, ha a szolgáltató a felhasználó által közzétett tartalmat jogellenesnek minősítette, vagy ha az ellentétes a szolgáltató szerződési feltételeivel. A cyberbullying megelőzését és kezelését szolgálja az is, hogy előzetes figyelmeztetés után ésszerű időtartamra fel kell függeszteniük a szolgáltatásaik nyújtását azon felhasználók számára, akik rendszeresen osztanak meg nyilvánvalóan jogellenes tartalmakat. A kiskorúak védelmét szolgálja, hogy a platformoknak megfelelő és arányos intézkedéseket kell hozniuk annak érdekében, hogy a kiskorúak magas szintű magánéleti védelme és biztonsága biztosítva legyen a platform használata során. Nem jeleníthetnek meg profilalkotáson alapuló hirdetéseket, ha tisztában vannak azzal, hogy a felhasználó kiskorú. Ugyanakkor ez nem kötelezi a szolgáltatókat arra, hogy további személyes adatokat gyűjtsenek annak megállapítására, hogy a felhasználó kiskorú-e.⁶⁸

2.2.2. GDPR

Az *Általános Adatvédelmi Rendelet* (GDPR) 2018. május 25-én lépett hatályba, és az Európai Unió legfontosabb adatvédelmi jogszabályaként a személyes adatok védelmét biztosítja. A cyberbullying, mint egy súlyos társadalmi probléma különösen a fiatalok körében jelent komoly veszélyt, így elengedhetetlen, hogy a jogi keretek megfelelő védelmet nyújtsanak a személyes adatokkal kapcsolatos visszaélések ellen. A GDPR nemcsak a felhasználók jogait védi, hanem növeli az online platformok felelősségét is, biztosítva a felhasználók tájékoztatását adataik kezeléséről és a jogszerű adatkezelés betartását. Ezen jogszabály lehetőséget biztosít a felhasználóknak, hogy a platformoktól a személyes adataik törlését kérjék, amely hozzájárul a cyberbullying megelőzéséhez és a digitális környezet biztonságosabbá tételéhez.⁶⁹

A GDPR szerint a személyes adatok kezelésének alapvető elvei különösen fontosak a cyberbullying megelőzése szempontjából. Az adatkezelést jogszerűen, tisztességesen és átláthatóan kell végezni, így az érintettek tisztában vannak az adataik felhasználásával. Adatgyűjtés csak meghatározott, jogszerű célból történhet, más célokra nem használható fel.

⁶⁸ 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).

⁶⁹ Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), 2016. április 27., (GDPR).

Az adatkezelésnek relevánsnak és szükségesnek kell lennie, így csak a lényeges információkat tárolják, emellett az adatoknak pontosnak és naprakésznek kell lenniük, a pontatlan információkat haladéktalanul ki kell javítani. Végül a személyes adatok tárolása csak a szükséges ideig lehetséges, a megfelelő biztonsági intézkedések pedig védik az adatokat a jogosulatlan hozzáféréstől és visszaélésektől. A személyes adatok gyűjtése és kezelése csak meghatározott indokkal történhet, például a felhasználók beleegyezésével. A törléshez való jog meghatározott esetekben biztosítja, hogy az egyénről tárolt személyes adatok késedelem nélkül eltávolításra kerüljenek. Az adatkezelőknek és adatfeldolgozóknak megfelelő technikai és szervezési intézkedéseket kell alkalmazniuk a személyes adatok biztonsága érdekében, ezzel megakadályozható ezen adatok illetéktelenekhez kerülése. Kiemelt figyelmet kell fordítani a 16 éven aluliak személyes adatainak kezelésére, az ő személyes adataik csak szülői hozzájárulással kezelhetők jogszerűen.⁷⁰

2.3. AZ EURÓPAI UNIÓ EGYES TAGÁLLAMAINAK GYAKORLATA

2.3.1. Németország

Németországban a 2017-ben hatályba lépett *Netzwerkdurchsetzungsgesetz* (NetzDG) szabályozza az online platformok kötelezettségeit a káros tartalmak, köztük a cyberbullyinggal kapcsolatos bejegyzések eltávolítására. A felhasználók a platformokon tehetnek bejelentést. A törvény szűk határidőt szab a platformoknak a bejelentett panaszokra való reagálásra, így a nyilvánvalóan jogellenes tartalom eltávolítására 24 óra áll a szolgáltatók rendelkezésére. Amennyiben nem egyértelmű a jogellenesség, hét napon belül meg kell vizsgálni és el kell távolítani a kompromittáló tartalmat. A szabály megszegése akár 50 millió eurós bírsággal is járhat. Emellett a platformoknak félévente jelentéstételi kötelezettségük van az eltávolított tartalmak számáról és folyamatáról, amelyeket mindenki számára hozzáférhetővé kell tenni az interneten.⁷¹

A *Jugendschutzgesetz* számos elővigyázatossági követelményt fogalmaz meg a kiskorúak online védelmének érdekében. Ezek közé tartozik a gyermekbarát jelentési rendszerek biztosítása az integritás megsértése esetén, a tartalombesorolási és életkorellenőrző eszközök bevezetése, valamint a független tanácsadó szolgáltatások népszerűsítése. Kiemelt hangsúlyt kapnak a szülői felügyelet technikai szabályozásai és az alapértelmezett beállítások, amelyek

⁷⁰ GDPR. i. m.

⁷¹ Bundesministerium der Justiz. *Regeln gegen Hass im Netz – das Netzwerkdurchsetzungsgesetz (NetzDG)*.

korlátozzák a használati kockázatokat. Ezek közé tartozik a profil láthatóságának, a helymegosztásnak és az ismeretlen felhasználókkal való kommunikációnak a korlátozása.⁷²

Emellett Németországban több civil szervezet nyújt segítséget a cyberbullying áldozatainak. Az olyan szervezetek, mint a *Jugendschutz.net* és a *Nummer gegen Kummer* ingyenes telefonos és online tanácsadást nyújtanak az érintett fiataloknak és szüleiknek. Ezek a szolgáltatások nemcsak pszichológiai támogatást kínálnak, hanem gyakorlati tanácsokat is, például hogyan lehet blokkolni vagy jelenteni zaklatókat a közösségi médiában.⁷³ A *Jugendschutz.net* a kiskorúak érdekében állami szervekhez is fordulhat.⁷⁴

A *Jugendschutz.net*-en 2023-ban 7645 panaszt tettek, ennek 2%-a, vagyis 153 kifejezetten cyberbullyingra vonatkozik, és a beszámolóban tett megállapítás alapján az összes panasz 15%-a káros a gyermekekre. A forróvonal tájékoztatja a szolgáltatókat és az önszabályozó testületeket az ifjúsági médiavédelem megsértéséről. A cél a gyors korrekciós intézkedések megtétele, és ezáltal a gyermekek és fiatalok károsodásának vagy veszélyeztetettségének azonnali megszüntetése. Erre a tevékenységre tavaly 3210 jogsértés esetén került sor. A sérelmek 90%-a az év végére orvoslásra kerültek. A hotline arra is felhívja a figyelmet, a legnagyobb problémát az életkor-ellenőrzés hiánya eredményezi.⁷⁵

2.3.2. Franciaország

2020 május 13-án elfogadásra került a *Loi Avia* nevű törvény a gyűlöletkeltő online tartalmak elleni küzdelemről, amely előírta volna a platformok számára, hogy a bejelentést követő 24 órán belül távolítsák el ezeket a tartalmakat, egy órán belül pedig a terrorista vagy pedofil jellegű tartalmakat. 2020. július 1-jén lépett hatályba, azonban sok vitát váltott ki, különösen azzal kapcsolatban, hogy korlátozhatja a szólásszabadságot. A francia alkotmánybíróság, a Conseil Constitutionnel, 2020. június 18-án hatályon kívül helyezte a törvény legtöbb rendelkezését, köztük a platformokra vonatkozó szigorú eltávolítási határidőket is, az indoklás szerint ugyanis potenciálisan a szólásszabadság sérelmét eredményezhette volna, mivel a platformok esetleg túlzottan elővigyázatosan távolítottak volna el ezeket a tartalmakat. Az alkotmánybíróság szerint a törvény nem biztosított elegendő védelmet a jogszerű, ám vitatott tartalmak esetében.⁷⁶

⁷² Bundesministerium für Familie, Senioren, Frauen und Jugend. (2002). *Gesetz zum Schutz von Kindern und Jugendlichen in der Öffentlichkeit* [Jugendschutzgesetz]. BGBl. I S. 2730.

⁷³ NummergegenKummer.

⁷⁴ Jugendschutz.net: Was wir tun.

⁷⁵ Jugendschutz.net.

⁷⁶ Conseil Constitutionnel. (2020). *Décision n° 2020-801 DC du 18 juin 2020*.

A 2024-449. számú törvényt 2024. május 21-én fogadták el, amelynek célja a digitális tér biztonságának és szabályozásának növelése. Ez a 64 cikkelyből álló törvény a pornográf iparról és a nemzeti és európai digitális szuverenitásról szóló parlamenti jelentésekből származó ajánlások is beépítésre kerülnek. A törvény hatálya a digitális szféra szereplőinek széles spektrumát fogja át. Jelentősen kiterjeszti az érintett szabályozó hatóságok hatáskörét, és a hatékonyabb kormányzás érdekében koordinációs hálózatot hoz létre közöttük. Ezáltal a törvény célja, hogy megerősítse a digitális platformok elszámoltathatóságát, különösen a tartalom moderálása és a felhasználók védelme terén, kiemelt figyelmet fordítva a kiskorúak káros online tartalmaktól való védelmére. Így rendelkezéseket tartalmaz arra vonatkozóan, hogy a platformoknak életkorellenőrző intézkedéseket kell bevezetniük annak érdekében, hogy a kiskorúak számára ne legyenek elérhetők a pornográf tartalmak. A tárhelyszolgáltatók emellett kötelesek mechanizmusokat kialakítani az illegális tartalom bejelentésére, valamint értesíteni a hatóságokat az illegális tartalmak bizonyos típusairól, a különösen súlyosnak ítélt tartalmakra fókuszálva.⁷⁷

2.3.3. Hollandia

Hollandiában a gyermekek védelme érdekében a platformokhoz való regisztráció életkorhoz kötött. 16 éves kor alatt kizárólag szülő vagy gondviselő hozzájárulásával lehet csatlakozni az online felületekre. Ez a korhatár nem vonatkozik a hotline-okra, egyéb tanácsadó és támogató weboldalakra, ugyanis ezeken az oldalakon 16 év alatt is el lehet érni szülői felügyelet nélkül.⁷⁸

Külön szervezet, az *End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes* (ECPAT) foglalkozik a gyermekek szexuális kizsákmányolásával és a visszaélésekkel való küzdelemben. Az erre vonatkozó szabályok a *Child Protection Policy*-ben szerepelnek. Az ECPAT tevékenysége során fokozott figyelemmel jár el a gyermekek személyes adatait illetően. Az általuk működtetett bejelentési eljárás különösen a gyermekekkel szemben elkövetett bántalmazásra, így a platformokon található ilyen tartalmakra, mint például gyermekpornográfia is vonatkozik. Együttműködik hatóságokkal és civil szervezetekkel, valamint a nyilvánosságot is ösztönzi a tartalmak bejelentésére.⁷⁹

Hollandiában is elérhetők különböző forróvonalak, amelyek krízishelyzetek esetére támogatást nyújtanak a kiskorúaknak. A *Kindertelefoon* egy közérdekű szervezet, amely 8 éves kortól nyújt telefonos és chat-en elérhető ingyenes segítséget, tájékoztatást az adott problémával

⁷⁷ Hogan Lovells: French Legal and Regulatory Update, May 2024.

⁷⁸ BREITBARTH, *National Adaptations of the GDPR*, 2019.

⁷⁹ Defence for Children International Netherlands & ECPAT Netherlands: *Child Protection Policy*.

összhangban. Emellett tanító videói és elérhető olvasmányai is vannak, amelyek segítenek a probléma megértésében és kezelésében.⁸⁰

2.3.4. Írország

Írorszáiban a *Coimisiún na Meán* intézménye felügyeli az ország online biztonsági szabályozási rendszerét, amelynek sarkalatos pontja a digitális platformok felelőssége a felhasználók, kiemelten a gyermekek védelme terén. A szabályozás célja, hogy a digitális szolgáltatók olyan intézkedéseket vezessenek be, amelyek elősegítik az online környezet biztonságosabbá tételét és megelőzik a káros tartalmak terjedését. A keretrendszer három jogszabályt foglal magában, az első és legfontosabb az *Online Safety and Media Regulation Act 2022*, hiszen ez a bázisa az ír *Online Safety Code*-nak, valamint itt említhető az *EU Digital Services Act (DSA)* és az *EU Terrorist Content Online Regulation* is.⁸¹

A tárhelyszolgáltatóknak könnyen elérhető és felhasználóbarát mechanizmust kell alkalmazniuk az ártalmas tartalom jelentéséhez. Amennyiben a szolgáltató nem teljesítette az eltávolítási kötelezettségét, a felhasználó a Coimisiún de Meán-hoz (Médiabizottság) fordulhat, amelyet a 2022-es *Online Safety and Media Regulation Act* hozott létre. A Médiabizottság a kijelölt online szolgáltatásokat felelősségre vonhatja a kötelező erejű biztonsági kódexek révén. A bizottság hatáskörének megfelelően a káros tartalom eltávolítása vagy korlátozása végett a szolgáltatóhoz fordulhat. Az értesítőben szükséges konkrétan megjelölni a káros tartalmat, valamint annak kategóriáját, és a tartalom eltávolítására vonatkozó egyéb specifikus információkat. A szolgáltatónak az értesítés kézhezvételétől számított két napon belül gondoskodnia kell arról, hogy a tartalom feltöltője az értesítés egy példányát megkapja. A törvény nagy hangsúlyt fektet a gyermekek cyberbullying elleni védelmére, így a szolgáltatóknak intézkedéseket kell bevezetniük annak megakadályozására, hogy a gyermekek hozzáférjenek a káros tartalmakhoz. Biztosítaniuk kell, hogy egyes online anyagokhoz a 18 éven aluliak ne férhessenek hozzá, valamint gyermekbiztonsági kockázatértékeléseket is végezniük kell. A jogszabály szerint a korhatárnak nem megfelelő tartalom alatt azokat a tartalmakat érti, amelyek egy gyermek képességére, fejlődésére, jogaira és érdekeire tekintettel alkalmatlanok, különösen a pornográfia és az erőszak, valamint a kegyetlenkedés valóságghű ábrázolása.⁸²

⁸⁰ Kindertelefoon.

⁸¹ Coimisiún na Meán: Online safety.

⁸² *Online Safety and Media Regulation Act 2022*.

A Hotline.ie Írország nemzeti bejelentő szolgálata az illegális online tartalmakkal kapcsolatban. Elsősorban a gyermekek szexuális online bántalmazásával foglalkoznak, azonban a személyiségi jogot sértő, engedély nélkül posztolt képek és videók is jelenthetők, akár anonim, bizalmas módon. Amennyiben jogellenes tartalmat azonosítanak, a Hotline.ie lépéseket tesz annak eltávolítására, függetlenül attól, hogy a tartalom Írországban vagy külföldön található.⁸³ Írországnál említhető a CyberSafeKids non-profit szervezet is. A 2015-ben alapított intézmény elsősorban Írországban és az Egyesült Királyságban működik, és különösen a cyberbullying elleni küzdelemre, a gyermekek digitális tudatosságának növelésére, illetve a szülők és tanárok képzésére helyezi a hangsúlyt.⁸⁴ A CyberSafeKids évente készít jelentéseket és felméréseket például arról, hogy a gyerekek hogyan használják az internetet, milyen veszélyekkel találkoznak, és milyen hatása van a közösségi médiának a mentális egészségükre. A 2023-mas jelentés szerint a megkérdezett 4.325 8-12 év közötti diák 84%-ának saját profiljai vannak a közösségi oldalakon, elsősorban a YouTube-on, WhatsAppon, Tiktokon és a Snapchaten, annak ellenére, hogy a platformok elméletileg tiltják a 13 év alattiak csatlakozását a felülethez, a WhatsApp ezt az életkort 16 év alatt állapította meg. A jelentésből az is kitűnik, hogy a 8-12 év közötti megkérdezett kiskorúak többsége nincs tisztában a profilja adatvédelmi beállításával, ugyanis csak 39,1% állította tudatosan privátra a fiókját, a többiek profilja vagy nyilvános, vagy nincs tudatában az alkalmazott beállítást illetően. A 12-16 éves korosztály (930 diák) már tudatosabban alkalmazta ezt az opciót, ugyanis 47,8%-uk választott privát beállítást. Nem meglepő, hogy ezáltal a 8-12 év közötti korosztály 25%-a, a 12 és 16 év közötti korcsoport 40%-a legalább egyszer cyberbullying áldozatává vált.⁸⁵

⁸³ Hotline.ie: Home.

⁸⁴ CybersafeKids: Our Story.

⁸⁵ Keeping Kids Safer Online: Online. Safety. Matters. Trends and Usage Reports Academic Year 2022-2023.

3. CYBERBULLYING TARTALOM ELTÁVOLÍTÁSA MAGYARORSZÁGON

3.1. AZ EKERTV.SZEREPE A SZEMÉLYISÉGI JOGOK VÉDELMEBEN A DIGITÁLIS PLATFORMOKON

A 2001. évi CVIII. az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvényben (Ekertv.) lefektetett főszabály szerint a szolgáltató felel az általa rendelkezésre bocsátott, jogellenes információért, azonban 2024. február 17. napjától a jogszabály akképpen módosult, hogy ehhez a rendelkezéshez mentesülési lehetőséget fűzött. Így nem felel a platform, amennyiben nem tudott a tartalom jogellenességéről, vagy jogos érdek sérelemről, és a tudomásszerzést követően haladéktalanul eltávolítja, vagy hozzáférhetetlenné teszi azt. A Gyermekvédelmi Internet Kerekasztal szerepe kiemelt a kiskorúak online védelmében, különösen a káros tartalmakkal szemben. A szolgáltató azon információkat, amelyek egy gyermek fejlődésére károsan hathatnak – kiemelten az erőszakot és szexualitást ábrázoló tartalmak – csak a kiskorúak lehetséges veszélyeztetéséről szóló figyelmeztetéssel, és a tartalom kategóriájára utaló azonosítókkal tehetők közzé, amennyiben a szűrőszoftverek által így felismerhetővé válnak. A Kerekasztal figyelemmel kíséri ezen szabályok betartását, továbbá ösztönzi a szolgáltatókat és szakmai szervezeteket a kiskorúak védelmének biztosítására. Bárki fordulhat hozzájuk panasszal, amennyiben jogsértést észlel. Az ilyen bejelentések alapján ajánlásokat tehetnek, illetve javaslatokat dolgoznak ki a jogszabályok betartásának elősegítésére. Ha a szolgáltató nem tesz eleget a Kerekasztal ajánlásainak, először felhívja a platformot az ajánlásokban, állásfoglalásaiban megfogalmazott magatartások tanúsítására. Eredménytelenség esetén a szolgáltató nevét az éves beszámolójában nyilvánosságra hozza, jogsértő tartalom esetén pedig felhívja annak eltávolítására. Amennyiben a jogellenes információ öt napon belül nem kerül törlésre, a Kerekasztal az NMHH eljárását kezdeményezi. 2024. július 1-jétől módosult a törvény 13.§-a, amely meghatározza a kiskorúakra vonatkozó személyiségi jogot sértő tartalmak eltávolításával kapcsolatos eljárást. E szerint a szolgáltató által hozzáférhetővé tett, a kiskorú személyiségi jogát sértő online anyag eltávolítása végett a kiskorú törvényes képviselője, korlátozottan cselekvőképes kiskorú esetén maga az érintett is felhívhatja a szolgáltatót a tartalom eltávolítására a személyazonosságának igazolása mellett. Az értesítésben meg kell jelölni az indokokat, hogy az érintett tartalom miért sérti a kiskorú személyiségi

jogait.⁸⁶ A módosítás indokolása alapján az értesítés megtételére vonatkozó formai kritériumok mellőzésével így egyszerűbbé válik a kiskorúak személyiségi jogait sértő, cyberbullyingnak minősülő tartalmak bejelentése és eltávolítása, ugyanis kiskorú törvényes képviselője (kivételesen a kiskorú is) a jövőben elektronikus úton, egyszerű azonosítással kérheti a sértő tartalom eltávolítását, anélkül hogy ezt köz- vagy teljes bizonyító erejű magánokiratba kellene foglalni.⁸⁷

A videómegosztó platformokra külön szabályokat állapít meg a törvény. Ezen szolgáltatóknak figyelemmel kell lenniük a közzétett tartalmakra, és intézkedéseket kell tenniük, ha a tartalom kiskorúakat veszélyeztethet, vagy ha az emberi méltóságot sérti. Ha a közzétett tartalom bűncselekményre buzdít, vagy gyűlöletkeltő, akkor azt is el kell távolítaniuk. Emellett a kereskedelmi közleményeknek is meg kell felelniük a vonatkozó jogszabályoknak. Előírja továbbá a hatékony életkor-ellenőrző és szülői felügyeleti rendszer alkalmazását a videómegosztók számára, ezáltal elkerülhető, hogy a kiskorúak káros tartalommal találkozzanak. A személyes adatokat kereskedelmi célra nem kezelhetik, így a kiskorúaktól gyűjtött adatok nem használhatók fel marketing célokra. A Hivatal jogsértés esetén különböző szankciókat alkalmazhat, például bírságot szabhat ki, vagy meghatározott időtartamra felfüggesztheti az oldalt.⁸⁸

3.2. MAGYARORSZÁGON ELÉRHETŐ HOTLINE-SZOLGÁLTATÁSOK

3.2.1. Az Internet Hotline

Az Internet Hotline (IH) a Nemzeti Média- és Hírközlési Hatóság Hivatala (NMHH Hivatala) által 2011 óta működtetett közérdekű szolgáltatás, amelynek célja az internet biztonságosabbá tétele elsősorban tájékoztatással és segítségnyújtással. Az IH-nál bejelenthetők azok az online tartalmak, amelyek jogsértőek lehetnek, vagy káros hatással bírhatnak a kiskorúak fejlődésére. Az elmúlt közel 13 évben több mint 17.000 bejelentést dolgoztak fel.⁸⁹

A bejelentések nyolc különböző kategóriában tehetők meg: gyermekpornográfia, hozzájárulás nélkül közzétett tartalom, online zaklatás, adathalászat, rasszista vagy közösség ellen uszító tartalom, illegális pszichoaktív szerek népszerűsítésére felhívó tartalom, erőszakos vagy

⁸⁶ 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ekertv.).

⁸⁷ 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ekertv.) indokolása.

⁸⁸ Ekertv. i. m.

⁸⁹ Internet Hotline: Az Internet Hotline szolgálatról.

illegális cselekményekre ösztönző tartalom, illetve egyéb, kiskorúakra káros tartalom. A bejelentések benyújthatók online űrlapon vagy e-mailben, és anonim módon is megtehetők.⁹⁰

Fontos megjegyezni, hogy az IH-hoz benyújtott bejelentés nem számít hatósági ügynek, tehát senkit sem kötelezhetnek a tartalom eltávolítására, és bírság kiszabására sincs lehetőség a tartalom eltávolításának elmaradása esetén.⁹¹ Az NMHH elnöke azonban kifejtette, hogy bár az Internet Hotline bár nem rendelkezik törvényi felhatalmazással, ez a digitális világban előnyére válik, mivel így gyorsabban és hatékonyabban tud intézkedni a bejelentések esetében. A gyorsan terjedő online tartalmak azonnali reakciót követelnek, amit hatósági eljárás – a jogorvoslati kötelezettséggel – jelentősen lassítana, így az intézkedés lényegében elveszítené a hatékonyságát. Az alapvető jogok biztosa részben támogatta az NMHH elnökének véleményét, miszerint a gyorsan terjedő digitális jogsértések esetén az IH jelző- és jogsegélyszolgálati hatékonyabbak lehetnek a lassabb hatósági eljárásoknál. Ugyanakkor a hatósági ellenőrzés hiánya miatt nincs megfelelő rálátás és visszacsatolás arról, hogy a szolgáltatók valóban betartják-e a gyermekvédelmi szabályokat, pedig ennek monitorozása elengedhetetlen. Emellett az alacsony bejelentési számok és a látencia, valamint a hotline-ok ismertségének hiánya akadályozzák a rendszer eredményességének megítélését, és veszélyeztethetik a gyermekek jogainak védelmét, így jogsérelmek közvetlen kockázatát jelenthetik.⁹²

Mivel az IH nem vizsgálhat át teljes weboldalakat, kiemelten fontos a pontos link megadása a bejelentésnél. A bejelentést követően az IH ellenőrzi, hogy az adott weboldal vagy közösségi platform rendelkezik-e bejelentő űrlappal vagy panaszkezelési eljárással. Amennyiben ilyen eljárás létezik, az IH javasolja a bejelentőnek, hogy közvetlenül nyújtson be panaszt, és ha ez eredménytelen, akkor az IH veszi fel a kapcsolatot a szolgáltatóval. Anonim bejelentés esetén a bejelentőt nem tájékoztatják az eljárás kimeneteléről. Gyermekek online szexuális bántalmazása, vagy más, nem magánindítványra üldözendő bűncselekmény esetén az IH egy munkanapon belül felveszi a kapcsolatot a Nemzeti Nyomozó Irodával.⁹³

Statisztikai adatok szerint 2023-ig összesen 17.373 bejelentést regisztráltak, amelynek 2021 volt a csúcspontja, ekkor 5.508 panaszt dolgoztak fel, ami az összes bejelentés több mint egyharmadát tette ki. Bár a 2023-as évben a bejelentések száma csökkent, még így is jelentős, összesen 2.047 bejelentés érkezett. Ebből 42% (kb. 850 bejelentés) gyermekpornográfiával

⁹⁰ Internet Hotline beszámoló: A Nemzeti Média-és Hírközlési Hatóság kiadványa az Internet Hotline 2023. évi tevékenységéről.

⁹¹ Internet Hotline beszámoló. i. m.

⁹² Az alapvető jogok biztosa jelentése. i. m.

⁹³ Internet Hotline beszámoló. i. m.

kapcsolatos, amely továbbra is a legnagyobb arányú bejelentési kategória. A második leggyakoribb panasz az online zaklatás, amely a bejelentések 18%-át teszi ki, szám szerint 375 esetet.⁹⁴

Az IH gyakran kap bejelentést törvényes képviselőktől, különösen szülőktől, akik aggodalmukat fejezik ki olyan esetek kapcsán, amikor gyermeküket szexuális tartalmú képek kikérésére kényszerítették, különösen a Snapchat platformon. Számos esetben fenyegetőztek az elkövetők a képek közzétételével, amennyiben nem fizetnek. Egyes szülői bejelentésben az állt, hogy valaki a gyermekükről beleegyezés nélkül készített róluk profilt közösségi oldalakon. Ezen kívül Discordon és Messengeren is próbáltak szexuális tartalmú képeket kicsalni kiskorúaktól.⁹⁵

2023-ban a bejelentések közül minden ötödik közösségi médiával kapcsolatos volt, ezek közül a legtöbb, 186 bejelentés a Facebookon megjelenő tartalmak miatt érkezett, amelyet a YouTube és az Instagram követett. A TikTok, Reddit, Discord, Twitter és Snapchat is szerepel a listán.⁹⁶

További problémát vetnek fel a mesterséges intelligencia által generált szexuális tartalmak, bár ezek Magyarországon még kevésbé elterjedtek, a globális tendenciák alapján azonban várhatóan növekedni fog az ilyen jellegű tartalmak aránya hazánkban is. Ezen képek ugyan nem valós bántalmazást ábrázolnak, mégis károsnak és jogsértőnek minősülnek.⁹⁷

Az IH emellett az online veszélyek tudatosítása érdekében előadásokat tart közoktatási és felsőoktatási intézmények számára, valamint gyermekekkel foglalkozó szakembereknek és szülőknek is. 2023-ban több mint 60 előadás került megtartásra, amellyel összesen 1.700 embert értek el.⁹⁸

A gyermekek védelme érdekében egyes törvények módosításáról szóló 2024. évi XXX. törvény 57. §-a módosította a 2011. évi CXCV. nemzeti köznevelési törvény 25. § (5e) bekezdését.⁹⁹ Az új rendelkezés alapján a köznevelési intézmények számára kötelezővé vált, hogy minimum szabályként gondoskodjanak arról, hogy mind a tanulók, mind a hozzátartozók számára jól látható helyen ki legyen függesztve az NMHH által működtetett internetes hotline elérhetősége. Emellett az iskoláknak lehetőségük van más eszközökkel is támogatni az elérhetőség széleskörű

⁹⁴ Internet Hotline beszámoló. i. m.

⁹⁵ Internet Hotline beszámoló. i. m.

⁹⁶ Internet Hotline beszámoló. i. m.

⁹⁷ Internet Hotline beszámoló. i. m.

⁹⁸ Internet Hotline beszámoló. i. m.

⁹⁹ 2024. évi XXX. törvény a gyermekek védelme érdekében egyes törvények módosításáról.

megismertetését.¹⁰⁰ E rendelkezés célja a köznevelési intézmények felelősségének növelése a gyermekek online biztonságának támogatásában és az esetleges online fenyegetések felismerésében, illetve kezelésében.

3.2.2. *Biztonsagosinternet.hu*

A Biztonsagosinternet.hu hotline üzemeltetését a Nemzetközi Gyermeekmentő Szolgálat (NGYSZ) végzi 2009 óta. A hotline elsődleges célja, hogy a gyermekek testi, lelki és szellemi fejlődésére veszélyes káros és jogsértő online tartalmakat a lehető legrövidebb időn belül eltávolítsa. Ennek érdekében szoros együttműködést folytat a magyar hatóságokkal, tartalomszolgáltatókkal, közösségimédia-platfomokkal, valamint az INHOPE szervezet tagjaival. A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztályának közvetlenül továbbíthatnak illegális tartalmakat, míg szerzői jogi ügyekben a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóságához fordulhatnak. A hotline szakmai munkáját a Legfőbb Ügyészség is támogatja.¹⁰¹

Bejelentést tenni kizárólag a honlapjukon elérhető űrlap kitöltésével az alábbi kilenc kategóriában lehetséges: rasszista idegengyűlöletre uszító tartalmak; online zaklatás, hozzájárulás nélkül közzétett tartalom, erőszakos tartalom; gyermekek szexuális bántalmazását ábrázoló anyagok, drogfogyasztást kínáló, arra csábító tartalom; állatkínzással kapcsolatos tartalom; adathalászat, pénzügyi csalás, egyéb káros tartalom. Anonim módon is van lehetőség panasztételre, azonban e-mail cím megadásával az elemzők tájékoztatni tudják a megkeresőt az ügy állásáról, valamint további tanácsokat is tudnak nyújtani. A bejelentés során a bejelentőnek nyilatkoznia kell arról, hogy 18 év alatti vagy feletti, illetve arról, hogy személyesen érintett-e az ügyben. Ezt követően meg kell adnia, hogy a tartalom továbbítása megtörtént-e már a rendőrség felé. A bejelentőnek egy legördülő menü segítségével a kilenc kategória közül kell kiválasztania a megfelelő bejelentési típust, majd meg kell adnia a káros tartalom elérhetőségét (linkjét). Amennyiben további tájékoztatást igényel, e-mail címének megadása is szükséges.¹⁰²

Ahogy az előző hotline, a Biztonsagosinternet.hu sem kötelezhet senkit kötelezhet a tartalom eltávolítására, hatásköre a panaszok hatóságok felé történő értesítésben és továbbításban kimerül. Első sorba azt vizsgálják, hogy meg lehet-e állapítani jogsértést. Amennyiben igen, úgy többféle úton folytatódhat a hatóságok értesítése. Amennyiben magyar vonatkozású a

¹⁰⁰ 2011. évi CXCV. törvény a nemzeti köznevelésről.

¹⁰¹ Biztonsagosinternet.hu: Rólunk.

¹⁰² Biztonsagosinternet.hu hotline beszámoló 2023. A Nemzetközi Gyermeekmentő Szolgálat Magyar Egyesület kiadmánya a Biztonsagosinternet.hu hotline 2023. évi tevékenységéről.

tartalom, az illetékes nemzeti hatóságot értesítik, amely ezt követően lefolytatja a szükséges eljárást. Magyar illetékesség hiányában a gyermekek szexuális bántalmazását ábrázoló tartalmak esetén az illetékes INHOPE tagországokat értesítik az ICCAM platformon keresztül. Egyéb esetben a hotline magát a szolgáltatót keresi fel, és felhívja az anyag eltávolítására.¹⁰³

Az alapvető jogok biztosa a 2022-es jelentésében kifejtette, hogy az elmúlt évek távlataiban nézve a legtöbb panaszt 18 év alattiak törvényes képviselői tették online zaklatás miatt.¹⁰⁴ A forróvonalhoz 2023-ban 4.419 bejelentés érkezett, melyből 715-öt azonosítottak jogsértőnek. Ebből 76,8%, vagyis 549 panasz a gyermekek szexuális bántalmazását ábrázoló anyag volt. A második legtöbb bejelentés, 19,8%, az az 99 egyéb káros tartalomra irányult. Ezt követte az online zaklatás 3,9%-kal, amely 28 bejelentést jelent. Az éves jelentés kifejti, hogy az online zaklatás és a hozzájárulás nélkül közzétett tartalom egymással összefüggő, ugyanis sokszor az online zaklatás hatására kerül sor intim képek küldésére, amelyet a zaklató egy platformon majd engedély nélkül közzétesz. A hozzájárulás nélkül közzétett anyag a bejelentések 3,9%-át, azaz 24 bejelentést tesz ki. Ezen hotline vonatkozásában is felmerül a mesterséges intelligencia által generált képek veszélye. A jelentésből kiderül, hogy a panaszok 22,8%-a volt ilyen jellegű.¹⁰⁵

Megítélésem szerint nemcsak az online zaklatás és a hozzájárulás nélkül közzétett tartalom mutat összefüggést egymással, hanem ide sorolható a gyermekek szexuális bántalmazása is, amely magában foglalja a szexting jelenségét is. Ahogyan azt az első fejezetben tárgyaltam, a szexting a cyberbullying egyik formája. Úgy vélem, hogy a bejelentési kategóriák között jelentős átfedés tapasztalható, ami megnehezíti ezek egyértelmű elkülönítését és pontos meghatározását.

3.3. EGYES SOCIAL MÉDIA PLATFORMOK PANASZBEJELENTŐ RENDSZEREI MAGYARORSZÁGON

Az alábbiakban bemutatásra kerül, hogy a négy, személyiségi jogot sértő cyberbullying szempontjából legnagyobb veszélyt jelentő platformon hogyan működik a panaszbejelentési rendszer. Általánosságban elmondható, hogy az oldalak bejelentési folyamatai hasonlóak, és egyszerű, könnyen elérhető lehetőségeket biztosítanak a felhasználók számára a személyiségi jogsértések, zaklatás vagy megfélemlítés jelentésére.

¹⁰³ Biztonsagosinternet.hu hotline beszámoló 2023. i. m.

¹⁰⁴ Az alapvető jogok biztosaának jelentése. i. m.

¹⁰⁵ Biztonsagosinternet.hu hotline beszámoló 2023. i. m.

A 2023-mas hotline jelentések alapján a legveszélyesebb platform ebből a szempontból a Facebook volt. Ezen a felületen a bejegyzéseknél, sztoriknál, profiloknál közvetlenül elérhető a jelentési funkció, ahol a felhasználók kilenc különböző kategória közül választhatnak, amelyek közül a megfélemlítés, zaklatás, vagy visszaélés kifejezetten releváns cyberbullying esetén. Ezen túlmenően a Facebook Súlyközpontjában van lehetőség a személyiségi jogsértések bejelentésére is, amelyen keresztül a szülők gyermekeik jogait érintő tartalmakat jelenthetnek. Problémát vet fel azonban a Facebook-esetében, hogy 13 éven felüli gyermekek csak saját nevükben tehetnek panaszt az őket érő személyiségi jogsértések ellen, míg a szülők számára nincs külön eljárás a panaszok kezelésére, amely a kiskorúak személyiségi jogainak védelmében problémát okoz, hiszen a platformra a joghatóság alapján vonatkozó írás adatvédelmi törvény 31. pontja kimondja, hogy 16 év alattiak esetén szülői beleegyezés szükséges az adatfeldolgozáshoz.¹⁰⁶ A személyiségi jogok védelme szempontjából lényeges, hogy egy kiskorú személyes adatainak kezelése és védelme megfelelő szülői felügyelet alatt álljon. Az a korlátozás, amely szerint 13 év felettiek kizárólag önállóan jelenthetnek be sérelmeket, ellentmond ennek a célkitűzésnek, és így akadályozhatja a gyermekek személyiségi jogainak védelmét, nem beszélve arról, hogy az Ektv. legújabb módosítása révén a törvényes képviselő jogosult a platformhoz fordulni a tartalom eltávolításával kapcsolatban, a kiskorú maga csak akkor, amennyiben korlátozottan cselekvőképes. Így a Facebook személyiségi jogot sértő tartalomra vonatkozó panaszbejelentési eljárása szembe megy az írás, és a magyar szabályozással is.

Az Instagramon a tartalmak (bejegyzések és történetek) jelentése ugyanígy működik. A Súlyközpontban a felhasználók további lehetőségeket is találnak, például az üzenetek, élő közvetítések és jegyzetek jelentésére, amelyek az Instagram közösségi irányelveit sérthetik. A súly szerint az eltávolítás csak akkor garantált, ha a tartalom megsérti az Instagram irányelveit. Az oldalon kiemelten kezelik a zaklatást és a megfélemlítést, valamint bántó vagy sértő tartalmak jelentését, ez pedig megerősíti az online megfélemlítés elleni fellépés lehetőségét.

A YouTube-nál a videók mellett lehetőség van a short-videók, csatornák, indexképek, megjegyzések, valamint élő csevegési üzenetek és hirdetések jelentésére is. Itt is elérhető egy külön adatvédelmi és jogi bejelentés űrlap, amely személyiségi jogsértések esetén hasznos, például ha a videótartalom személyiségi jogokat vagy helyi törvényeket sért.

¹⁰⁶ Data Protection Act 2018.

A TikTokon szintén az adott tartalomnál lehet bejelentést tenni, ahol a gyűlölködés és zaklatás ponton belül a zaklatás és bullying közvetlenül választható kategória a jelentési felületen. Ez egyszerűsíti a problémás tartalmak gyors jelentését, azonban a platformon nem találtam további panaszkezelési lehetőségeket, így a személyiségi jogsértésekre vonatkozólag sem.

Összességében elmondható, hogy ezek a bejelentési lehetőségek egyszerűen és gyorsan elérhetők, és bár a tartalmak eltávolítása nem garantált, jelentős támogatást nyújthatnak a cyberbullying és személyiségi jogsértések elleni védelemben, amely a Facebook-ra nem teljeskörűen igaz, hiszen nincs összhangban az ír adatvédelmi előírásokkal a kiskorúak személyes adatainak védelmével kapcsolatban.

3.4. FELMÉRÉS A SZÜLŐK TUDATOSSÁGÁRÓL A CYBERBULLYINGOT ÉS A BÍRÓSÁGON KÍVÜLI TARTALOMELTÁVOLÍTÁSI ELJÁRÁSOKAT ILLETOEN

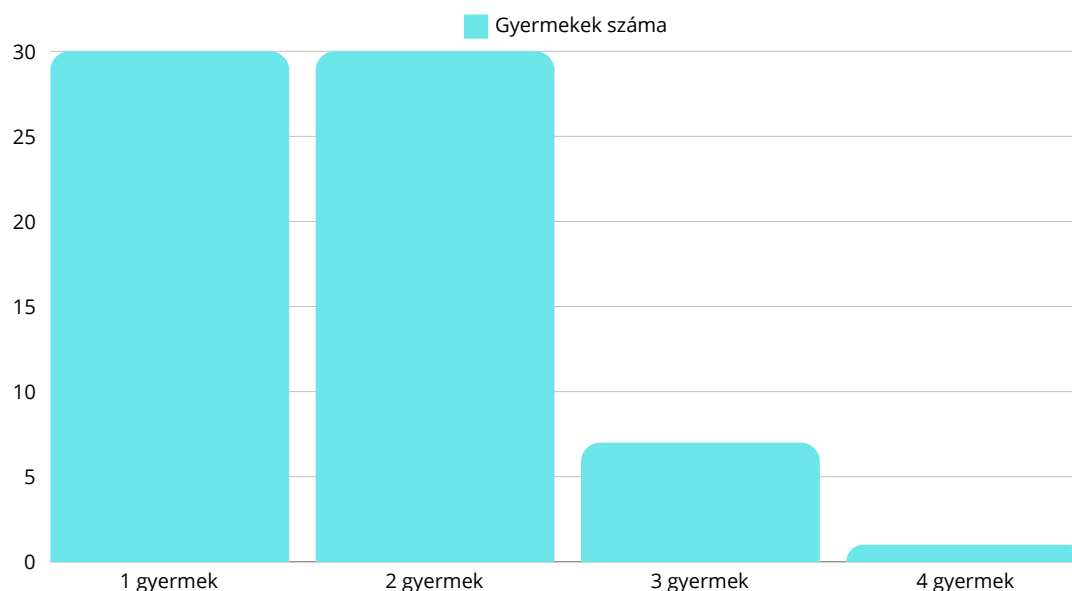
Magyarországon a jogszabályi keretek, illetve a gyermekek online védelmét elősegítő forróvonalak megpróbálták lekövetni a digitális világ adta negatív hatások, így a személyiségi jogot sértő cyberbullying tartalmak eltávolításának egyszerűbb leküzdését. A hotline-ok évek óta látogatnak iskolákat, és tartanak előadásokat gyermekek, szülők, pedagógusok és szakemberek számára, azonban ezen tevékenységeikkel is elenyésző számú embert tudnak elérni, például az Internet Hotline 2023-ban 60 előadással mindössze 1.700 embert ért el, és ahogy arra már utaltam korábban, az alapvető jogok biztosa is kifejtette a 2022-es jelentésében, ezek forróvonalak a mai napig szinte láthatatlanok, ahhoz képest, hogy az egyik 15, a másik 13 éve tevékenykedik. A jövőre nézve kérdéses, hogy a köznevelési intézmények számára előírt, az IH elérhetőségét kifüggeszteni rendelt kötelezettség mennyiben fogja növelni az érintettek jogtudatosságát és ezzel összefüggésben a hotline-nál tett éves bejelentések számát.

Emiatt készítettem egy Google Forms kérdőívet, amellyel a szülők tájékozottságát és tudatosságát szerettem volna felmérni a cyberbullying, illetve a tartalomeltávolítási mechanizmusok ismeretét illetően. A felmérésem sikerességéhez az ország több pontján lévő, összesen 58 általános és középiskola igazgatóját kerestem fel e-mailben annak reményében, hogy segíteni fognak a kérdőívem szülőkhöz való eljuttatásában, hiszen a cyberbullying kezelésében az oktatási intézményeknek is egyre nagyobb szerepük van. Az 58 megkeresésből mindösszesen öt választ kaptam. Egy iskola nem járult hozzá külsős kutatásokhoz, egy másik a tanárok és a diákok leterheltségére hivatkozással minden kutatási kérést elutasít. Egy iskolaigazgatótól azt a visszajelzést kaptam, hogy szülők felé nem szoktak kérdőíves vizsgálatokat továbbítani, azonban annyival segítette a munkámat, hogy néhány

osztályfőnökhöz eljuttatta a kérésem, akik belátásuk szerint tájékoztathatták a szülőket a felmérésemről. Személyes érintettségem okán két iskola támogatta aktívan a kutatásom.

A kérdőívem elkészítésekor sokkal nagyobb támogató közegre számítottam, hiszen a diákok érdekét, biztonságát és egészségét szolgálja az, ha nincsenek kitéve cyberbullyingnak, vagy ha mégis bekövetkezik ez az incidens, a szülők tisztában vannak a lehetőségeikkel a probléma kezelésében. Mivel az iskoláktól vagy elutasító választ, vagy főképp ignorálást kaptam, ezért közzétettük néhány szülői csoportban is, így 68 kitöltőhöz jutott el a kérdőívem.

A kitöltőknek tíz kérdésre kellett kötelezően, két kérdésre opcionálisan válaszolniuk, amelyet a következőkben ismertetek. Az első kérdés arra irányult, hogy a kitöltőnek mennyi kiskorú gyermeke van.

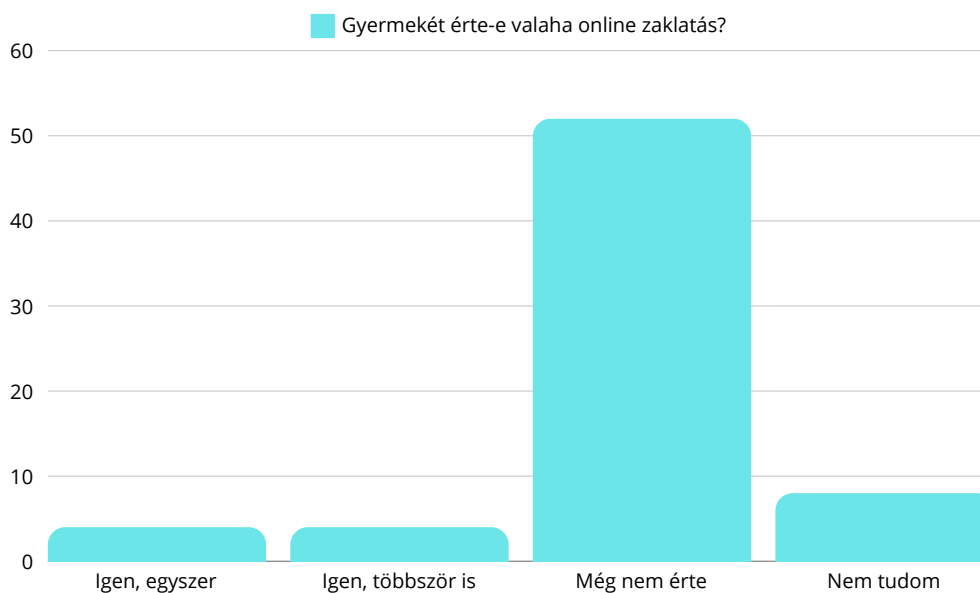


Forrás: Saját szerkesztés

A 68-ból 30 kitöltőnek egy, szintén 30-nak kettő, 7-nek három, és 1-nek négy gyermeke van, tehát a felmérés összesen 115 kiskorút érintett.

A második kérdésben a kitöltők megválaszolták, hogy hallottak-e már a cyberbullying kifejezésről. A válaszadók közül csupán egy szülő nem ismerte ezt a kifejezést korábban.

A harmadik kérdés arra vonatkozott, hogy a kitöltő gyermekét érte-e már valaha cyberbullying, ahol négy válaszlehetőség közül választhattak a szülők.



Forrás: Saját szerkesztés

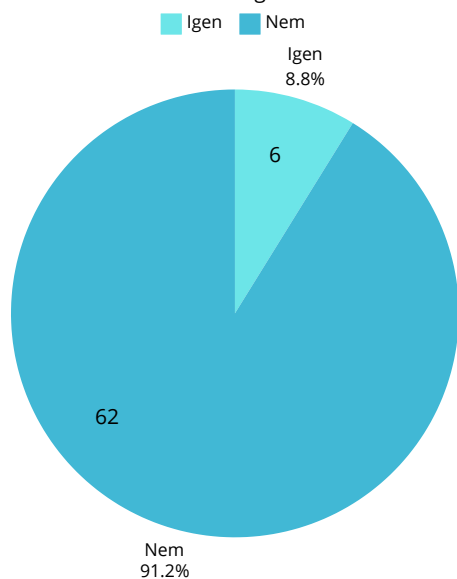
52 szülő azt válaszolta, hogy gyermekét még nem érte cyberbullying, 8 szülő nem tudja, hogy érte-e incidens a gyermekét, 4 szülő számolt be arról, hogy gyermeke egyszer már cyberbullying áldozatává esett, szintén 4 szülő hivatkozott arra, hogy gyermekét többször is érte cyberbullying.

A következő kérdésben a kitöltők kiválasztották a szerintük legveszélyesebb közösségi oldalakat a cyberbullying szempontjából. A válaszok száma alapján a legveszélyesebbtől kezdve a következő a sorrend: Facebook, Instagram, Tiktok, Snapchat, Youtube, Twitter, Discord, Reddit.

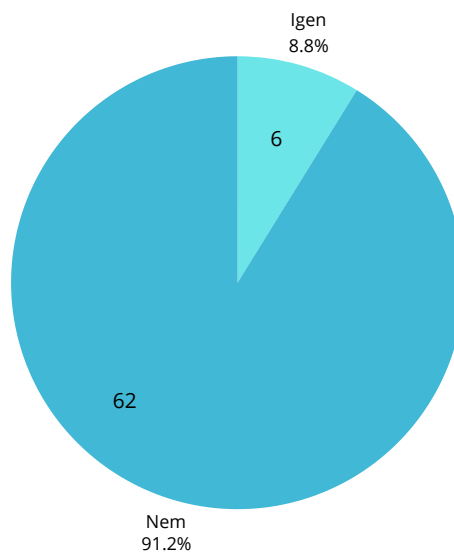
Ezt követően azok felé a szülők felé irányult a kérdés, akiknek a gyermekét érte már cyberbullying, ugyanis arra adtak választ, hogy ebben az esetben hogyan kezelték a helyzetet. Valamennyi szülő jelentette a platformon az incidenst, két szülő a rendőrséghez is fordult, egy megkereste a zaklató gyermek anyukáját, akivel megbeszélték a dolgot, egy szülő magához a zaklató gyerekhez fordult a tartalom eltávolítása végett azzal, hogy ha ennek a kérésnek nem tesz eleget, jelentik az iskolaigazgatónál, és a rendőrséghez is megteszik a feljelentést személyiségi jogok megsértése miatt, egy kitöltő pedig hotline segítségét is kérte.

A továbbiakban a hotline-okról való tájékozottságot és igénybevételi hajlandóságot került megvizsgálni. Így elsőként a szülők arra válaszoltak, hogy hallottak-e már a Biztonsagosinternet.hu és az Internet Hotline-ról.

Hallott már Ön a Biztonsagosinternet.hu hotline-ról?



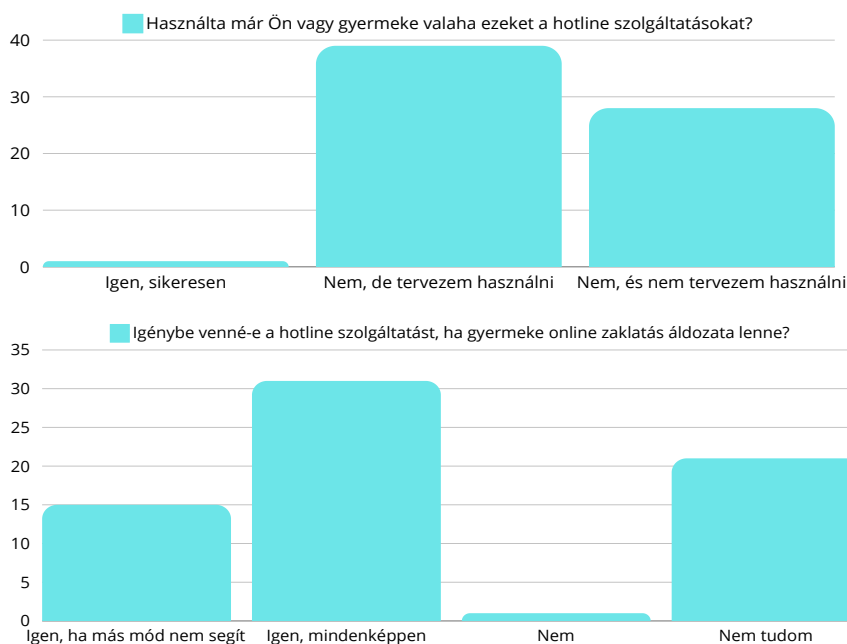
Hallott már Ön az Internet Hotline-ról?



Forrás: Saját szerkesztés

A megkérdezettek közül mindkét esetben 6-an ismerték az adott hotline-t, 62-en még nem hallottak róla. Ez is bizonyítja, hogy a forróvonalak még mindig alig ismertek, holott már több, mint egy évtizede működnek, előadásokat tartanak, és az idei évtől az iskolák is kötelesek az Internet Hotline elérhetőségét jól látható módon kifüggeszteni.

Ezután egy kérdés irányult arra, hogy a kitöltő vagy a gyermeke használta-e a két magyar hotline-t, egy másikban pedig arról, hogy használná-e, ha gyermekét cyberbullying érné.

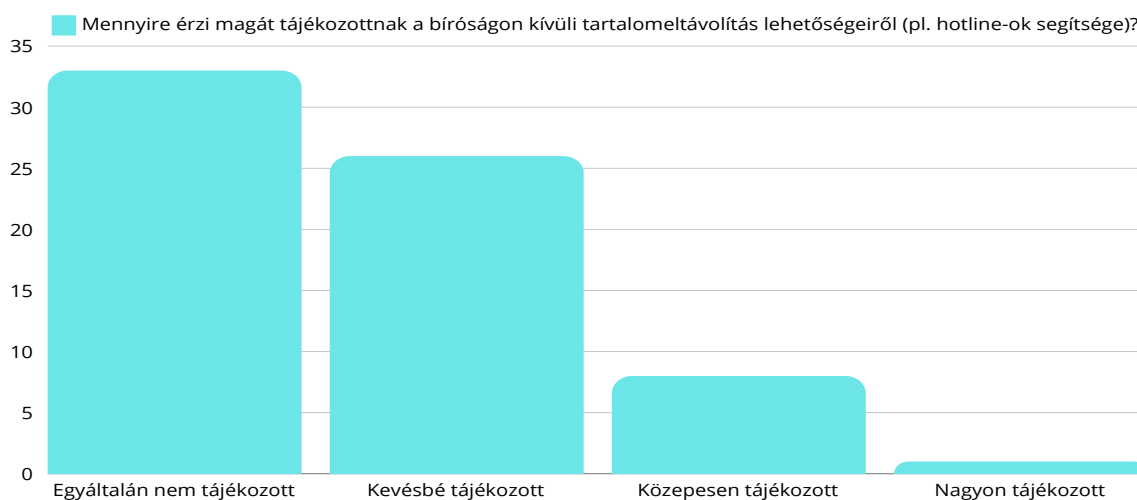


Forrás: Saját szerkesztés

A megkérdezett szülők közül 1 sikeresen alkalmazta a hotline nyújtotta segítséget, 39 tervezi, hogy használja, és 28 szülő elutasító ezen a téren. Egy esetleges incidens esetén a 86 szülőből 31 szülő, 45,6%, vagyis majdnem a szülők fele minden további nélkül hajlandó lenne alkalmazni a forróvonal eltávolítási mechanizmusát, 15 szülő, 22,1% pedig akkor alkalmazná, ha megpróbált már más opciókat, azonban azok nem vezettek eredményre. Így azok, akik valamilyen módon alkalmaznák a lehetőségeket, a megkérdezettek 65,7%-át teszik ki. 21 kitöltő, 30,9% kattintott a nem tudom válaszra, tehát nem biztos, hogy alkalmazná, de nem is utasítja el, és csupán 1 szülő gondolkodik akképp, hogy nem kívánja igénybe venni a hotline kínálta lehetőségeket. Úgy gondolom, hogy az arány nem rossz, hiszen kifejezetten elutasító válaszból csak egy érkezett, és a szülők több, mint a fele élne az eltávolítási mechanizmusokkal, azonban ebből is látszik, hogy a szülők nincsenek tisztában azzal, hogy ezek a hotline-ok hogyan tudnak segíteni cyberbullying esetén. Amennyiben tudatosabbak lennének a megoldási opciók vonatkozásában, úgy valószínűleg az arányok is módosulnának a hotline-ok javára.

Az utolsó előtti kötelezően megválaszolendő kérdésben a kitöltők megjelölték négy válaszlehetőség közül, hogy milyen eszközökkel próbálják megvédeni a gyermekeket a cyberbullyingtól. A megkérdezettek 73,5%-a, ami 50 szülőt jelent rendszeres beszélgetést folytat gyermekével az internetes biztonságról, 32 szülő, vagyis 47,1% korlátozza az internethez való hozzáférést, 28 szülő alkalmaz privát profilbeállításokat, valamint szűrőszoftvereket.

Végül arra irányult a kérdés, hogy mennyire tartják magukat a szülők tájékozottnak a bíróságon kívüli tartalomeltávolítási lehetőségek terén.



Forrás: Saját szerkesztés

33 szülő, amely a megkérdezettek 48,5%-át jelenti, egyáltalán nem tartja magát tájékozottnak az opciókat illetően, tehát majdnem a válaszadók fele semmilyen információval nem rendelkezik a bírósági eljárásen kívüli tartalomeltávolításról. További 26 szülő, 38,2% úgy gondolja, hogy kevésbé tájékozott a témát illetően. Valószínűleg hallott már róla, de nem nézett utána, hogy ez pontosan mit is jelent, illetve milyen lehetőségek adóttak. 8 kitöltő, 11,8 % saját bevallása szerint közepesen tájékozott, feltehetőleg hallott néhány lehetőségről, utána is nézett egy-két opciónak, esetleg alkalmazta is. Mindösszesen 1 válaszadó tartja magát nagyon tájékozottnak ezen a területen. Ez alapján az mondható el, hogy ezek az eltávolítási mechanizmusok, illetve a hotline-ok kevésbé vannak benne a köztudatban, amely összefüggésben áll az alkalmazási hajlandósággal is.

Az utolsó, opcionális kérdésben a szülők rövid szöveges válasz formájában kifejezheték a témával kapcsolatban felmerült észrevételeiket, megjegyzéseiket. Több szülő is hangsúlyozta a gyermekekkel való beszélgetést az internet veszélyeiről, illetve a szülői kontroll is szerepel két válaszban. Emellett szintén kiemelték azt is, hogy az iskoláknak kellene nagyobb szerepet vállalniuk, akár szakértő bevonásával abban, hogy tájékoztatást adjon mind a gyermekeknek mind a szülőknek az interneten található veszélyekről, és az eltávolítási mechanizmusokról.

A felmérés eredményeképpen megállapítom, hogy az iskoláknak sokkal aktívabb szerepet kellene vállalniuk a szülők és a gyermekek tájékozottságának gyarapításában, hiszen kevesen ismerik a személyiségi jogot sértő cyberbullying tartalmak elleni eltávolítási opciókat, és ezen kutatást sem kívánták támogatni, amellyel eljuthatott volna a szülőkhöz a kérdőív, így a témában kevésbé jártas szülő is utána tudott volna nézni ezeknek a lehetőségeknek a kérdések alapján. Emellett a szülőknek is javasolt volna behatóbban foglalkozni az online biztonság és védelem kérdésével, hiszen annak ellenére, hogy két iskola valamennyi szülővel megosztotta a felmérésem, a kitöltési hajlandóság nagyon alacsony szinten mozgott. Továbbá akik válaszoltak, ők sem ismerik a lehetőségeket, holott jelezte néhány szülő, hogy gyermekét már legalább egyszer cyberbullying érte, mégis csak egyetlen szülő tartotta magát a témában jártasnak, következésképpen a szülők nem néztek utána a lehetőségeknek. Végül szükséges volna maguknak a forróvonalaknak nagyobb reklámozást biztosítani akár a közösségi oldalakon (ha már úgyis annyi kiskorú van jelen ezeken a felületeken), illetve előadások keretében, ahol megismertetik a gyerekeket, szülőket, pedagógusokat a hotline tevékenységéről. Ez fokozhatná az eltávolítási eljárás iránti érdeklődést és alkalmazási hajlandóságot.

ÖSSZEGZÉS

A cyberbullying jelenségéhez számtalan szerző, szervezet által alkotott definíció és magyarázat fűződik, mégis egzakt, széleskörűen elfogadott meghatározása nincsen. Ez megnehezítheti a jogérvényesítést, hiszen nem tudjuk, hogy pontosan milyen elemek szükségesek a cyberbullying megvalósításához. Egyes fogalmak például magukban foglalják, hogy ismétlődő magatartásról van szó, azonban ezzel kizárják azokat az eseteket, amikor valakiről egyetlen alkalommal posztolnak megalázó üzenetet, vagy tesznek közzé személyiségi jogot sértő fényképet. A dolgozatban a meghatározások fogalmi elemekre lettek bontva, amelyeknek két csoportját lehet megkülönböztetni: a szükséges és eshetőleg fogalmi elemeket. Szükséges elem az interneten való elkövetés, hiszen ettől lesz online megfélemlítés, illetve a zaklatás, amely egyfajta gyűjtőkategóriaként fogható fel, így megnyilvánulhat agresszióként, például sértő üzenetek küldésével, vagy lehet nyilvánosság előtt, nyíltan megalázó üzenet, vagy akár fénykép. Lehetséges elem a szándékosság, káros hatás, nyilvánosság, anonimitás, ismétlődés és hatalmi különbség. Azért fontos a fogalom minél tágabb értelmezése, mert így valamennyi cyberbullying magatartásra kiterjed, ezáltal hatékonyabban lehet fellépni az incidensek ellen.

A cyberbullying tartalom eltávolítására nyitva áll egy bíróságon kívüli, alternatív megoldás, amely gyorsabbá, ezáltal hatékonyabbá teszi a zaklató tartalom törlését. A dolgozatban vizsgált államok mindegyikében kialakult jogi kerete van a tartalom ilyen típusú eltávolításának. Ezek a mechanizmusok több államban hasonló mechanizmust követnek, azonban az eredményesség és a részletszabályok tekintetében eltérőek. Előírják, hogy a platformszolgáltatók könnyen elérhető, felhasználóbarát panaszbejelentési rendszert biztosítsanak, így elősegítve a gyors reagálást. A civil szervezetek szintén fontos szereplők, mivel lelki támogatást nyújtanak és segítik a tartalmak eltávolítását, beleértve a jogorvoslati lehetőségek felkutatását és a hatóságokkal való kapcsolattartást. Egyes országok, mint Írország és Ausztrália, külön szervezetet is létrehoztak, amelyek közvetlenül a platformokkal lépnek kapcsolatba, ha a felhasználói panaszok nem vezetnek eredményre. Ezek az országok határidőket szabnak a tartalomeltávolításra, növelve ezzel a szabályozás hatékonyságát. Figyelemre méltóan eredményes gyakorlatot alakított ki Írország, ahol az erre létrehozott intézmény, a Comisiún de Meán jogosult a platformok felelősségre vonására. Új-Zélandon a Netsafe foglalkozik a tartalmak eltávolításával, akinek az eljárása az esetek nagy részében sikerrel zárul. Hasonló rendszer működik Ausztráliában is, ott azonban az eSafety fellépése a gyermekek védelme érdekében egyáltalán nem mondható sikeresnek, ugyanis tavaly több, mint 2600 panasz érkezett

az ausztrál gyermekekre vonatkozó cyberbullying rendszeren keresztül, azonban egy alkalommal sem történt eltávolítási felhívás. Az Egyesült Királyságban a Report Harmful Content, mint vitarendezési eljárás szolgálja a tartalmak eltávolítását, amely a platformokkal kötött megállapodása alapján léphet fel a felhasználók panaszára a platformszolgáltatóval szemben. Az USA cyberbullyingra vonatkozó szövetségi szintű szabályozás hiánya miatt a különböző államokban eltérő megoldásokkal, alacsonyabb vagy magasabb szintű jogszabállyal operálnak, illetve több államban főként az iskolákra hárítanak nagy felelősséget a cyberbullying megelőzés és kezelése érdekében.

Magyarországon az Ekertv. módosításával bevezetésre került, hogy a kiskorú törvényes képviselője, korlátozottan cselekvőképes kiskorú esetén a kiskorú bejelentést tehet a platformoknál a személyiségi jogot sértő cyberbullying tartalmak eltávolítása végett, amelyhez már nem szükséges közokirat vagy teljes bizonyító erejű magánokirat, hanem személyazonosság igazolása mellett, az indokok ismertetésével fordulhat a platformokhoz, így sokkal gyorsabbá és egyszerűbbé válik a törlési eljárás. A Facebook szabályzata ezen rendelkezéssel, és az ír adatvédelmi szabályokkal is teljesen ellentétes, hiszen 13 év feletti gyermekek esetén csak akkor fogadják be a személyiségi jogot sértő tartalomra irányuló panaszt, amennyiben azt maga a kiskorú terjesztette elő. Az új magyar módosítás mellett segítik a tartalom eltávolítását a hotline-ok is, bár a megkeresésen kívül semmilyen jogosítványuk nincsen, így nem alkalmazhatnak a platformokkal szemben jogkövetkezményeket, amennyiben nem tesznek eleget az eltávolítási kérésnek. Az alapvető jogok biztosa kifejtette, hogy nehéz megmondani a rendszer eredményességét, hiszen még mindig láthatatlanok, ezáltal a bejelentési számok is alacsonyak. Az általam elvégzett kérdőíves vizsgálat is azt támasztja alá, hogy a szülők számára teljesen ismeretlenek a forróvonalak adta lehetőségek, ezért sokan szkeptikusak ezen megoldásokkal szemben, pedig, ha a felhasználó által történő bejelentés nem járt sikerrel, akkor is lehetne egy második opció a hotline mögött álló szervezet felkerése, aki felveszi a kapcsolatot a platformszolgáltatóval. Fontos lenne a forróvonalak ismertségének a növelése, amelyben az iskoláknak és a hotline-oknak is feladatuk van.

Megállapítható, hogy a vizsgált államok közül Írország szabályozása a leghatékonyabb, ugyanis a tartalom eltávolítása érdekében létrehozott szervnek sokkal szélesebb jogköre van, mint a többi elemzett államnak, ugyanis kötelezést tartalmazó döntést hozhat és joghátrányt alkalmazhat a platformokkal szemben. Az államoknak arra kellene törekedniük, hogy amennyiben nincs eltávolítási mechanizmusra feljogosított szervük, hozzanak létre egyet, vagy alakítsanak ki az eltávolítás vonatkozásában hatáskört és ehhez szükséges szabályozást,

amelyet a területtel foglalkozó szervhez lehet telepíteni, mint Magyarországon az NMHH. Ha van rá mód, tegyék lehetővé számukra a platformok felelősségre vonását is, ezzel biztosítható lenne a személyiségi jogot sértő cyberbullying tartalom hatékony eltávolítása. Amennyiben ez nem lehetséges, jó megoldás lehet egy akár állami, akár civil kezdeményezésre létrehozott vitarendezési eljárás, mint az Egyesült Királyságban, amelyhez a platformok önként csatlakozhatnak, ezzel, bár az adott államban nem kötelezhető a szolgáltató a tartalom eltávolítására, mégis nagy hajlandóságot mutatnak az online anyag törlését érintően. Ebben nagy szerepe van annak, hogy ehhez az eljáráshoz saját elhatározásból csatlakoztak, és így az önszabályozás elvén alapulva magukra nézve kötelezőnek ismerik el a mechanizmus eredményét. Ha tovább akarjuk erősíteni a sikerességet, akkor ezeknek a vitarendezési eljárásoknak ténylegesen is alávetethetnék magukat a csatlakozó platformok, de ez nem feltétlenül szükségszerű, hiszen az önkéntes belépésnek is van egyfajta ösztönző szerepe az eljárás eredményének végrehajtása szempontjából. Fontos szerepe lenne a forróvonalaknak is, nemcsak itthon, hanem valamennyi országban, hiszen azon kívül, hogy segítenek megoldást találni és felvenni a kapcsolatot a platformmal, egy nemzetközi cyberbullying esetén felveszik a kapcsolatot az illetékes hotline-nal, akik saját országukban intézkedhetnek a tartalom eltávolítása érdekében, ha szükséges, az illetékes szerv bevonásával. Ezért azon államok, akik nem csatlakoztak az INHOPE hálózatahoz, szükséges lenne ezt pótolniuk, hogy az internacionális incidensek is könnyebben kezelhetők legyenek.

Az USA-ban szükséges lenne legalább egy keretszintű szabályozás a cyberbullyingról, így annak fogalmáról, illetve kezelési lehetőségeiről, esetleg arról, hogy milyen szintű jogszabálynak kell lefektetnie a részletszabályokat, hogy az egyes államokban egy kicsit egységesebb legyen a rendszer, és egyszerűbbé váljon a jogérvényesítés. Több államban hatalmas felelősség van az iskolákon, akiknek tényleg kiemelt, vezető szerepe van a cyberbullying elleni küzdelemben, de végső soron nem nekik kellene teljesen megoldaniuk a problémát, hanem az államnak és a szakosodott szervezeteknek is nagyobb felelősséget kellene vállalniuk.

A magyar szabályozás jó úton halad, az új módosítás által a törvényes képviselők részére egyszerűbbé válik a panaszbejelentés a platformok felé. Két forróvonal segíti a jogérvényesítést, akiknek jobban kellene törekedniük arra, hogy az emberek megismerhessék munkásságukat és az általuk kínált lehetőségeket, ezen opciók hiánya a bejelentések alacsony számában is tetten érhető. Ebben segíthetne még több intézménylátogatás, szülőknek tartott előadás, hirdetések, esetleg egy csoportos konferenciahívás, ahol több iskola több osztálya

egyszerre becsatlakozik a hívásba, és egy óra keretén belül meghallgatják az előadást, szülők esetében szülői értekezlet címen, amely elsősorban hatékonyabb lenne, mint az intézménylátogatások, hiszen sokkal több gyermeket és szülőt lehetne elérni, és kevesebb erőforrást venne igénybe. Amennyiben kialakult a forróvonal ismertsége, utána egyszerűbb egyes intézményeknek előadásokat tartani. Ebben besegíthetnének az iskolák azáltal, hogy a kötelező elérhetőség kifüggesztése mellett a pedagógusok beszélnek a gyermekekkel és a szülőkkel a hotline lehetőségekről. Ehhez akár a forróvonalak is nyújthatnak oktatási segédanyagot, ezzel megkönnyítve a saját és a pedagógusok munkáját.

IRODALOMJEGYZÉK

Folyóiratok

BARLETT, Christopher P. Anonymously hurting others online: The effect of anonymity on cyberbullying frequency. *Psychology of Popular Media Culture*, 2015, 4.2: 70.

BOSSLER, Adam M. Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 2020, 257-280.

CAMPBELL, Marilyn A. Cyber bullying: An old problem in a new guise?. *Journal of Psychologists and Counsellors in Schools*, 2005, 15.1: 68-76.

FEINBERG, Ted; ROBEY Nicole. Cyberbullying. *The education digest*, 2009, 74.7: 26.

FESTL, Ruth; QUANDT, Thorsten. Social relations and cyberbullying: The influence of individual and structural attributes on victimization and perpetration via the internet. *Human communication research*, 2013, 39.1: 101-126.

GUALDO, Ana M. Giménez, et al. The emotional impact of cyberbullying: Differences in perceptions and experiences as a function of role. *Computers & Education*, 2015, 82: 228-235.

GUAN, Ng Chong, et al. Cyber bullying-a new social menace. *ASEAN Journal of Psychiatry*, 2016, 17.1: 104-115.

HINDUJA, Sameer; PATCHIN, Justin W. Cyberbullying legislation and case law. *Implications for School Policy and Practice. Pridobljeno*, 2015, 5: 1-3.

HOFF, Dianne L.; MITCHELL, Sidney N. Cyberbullying: Causes, effects, and remedies. *Journal of Educational Administration*, 2009, 47.5: 652-665.

MENESINI, Ersilia; NOCENTINI, Annalaura. Cyberbullying definition and measurement: Some critical considerations. *Zeitschrift für Psychologie/Journal of Psychology*, 2009, 217.4: 230-232.

MENESINI, Ersilia; SPIEL, Christiane. Introduction: Cyberbullying: Development, consequences, risk and protective factors. *European Journal of Developmental Psychology*, 2012, 9.2: 163-167.

SMITH, Peter K., et al. Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, 2008, 49.4: 376-385.

STICCA, Fabio; PERREN, Sonja. Is cyberbullying worse than traditional bullying? Examining the differential roles of medium, publicity, and anonymity for the perceived severity of bullying. *Journal of youth and adolescence*, 2013, 42: 739-750.

VAILLANCOURT, Tracy; FARIS, Robert; MISHNA, Faye. Cyberbullying in children and youth: implications for health and clinical practice. *The Canadian journal of psychiatry*, 2017, 62.6: 368-373.

YANG, Y. Tony; GRINSHTEYN, Erin. Safer cyberspace through legal intervention: A comparative review of cyberbullying legislation. *World Medical & Health Policy*, 2016, 8.4: 458-477.

Jogi normák és egyéb jogi dokumentumok

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

2011. évi CXC. törvény a nemzeti köznevelésről.

2024. évi XXX. törvény a gyermekek védelme érdekében egyes törvények módosításáról.

Az alapvető jogok biztosának jelentése az AJB-686/2022.számú ügyben az online gyermekvédelem védelmi és jogorvoslati rendszerének működésével összefüggésben.

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), 2016. április 27., (GDPR).

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).

Bundesministerium der Justiz. *Regeln gegen Hass im Netz – das Netzwerkdurchsetzungsgesetz (NetzDG)*.

Bundesministerium für Familie, Senioren, Frauen und Jugend. (2002). *Gesetz zum Schutz von Kindern und Jugendlichen in der Öffentlichkeit* [Jugendschutzgesetz]. BGBl. I S. 2730.

Conseil Constitutionnel. (2020). *Décision n° 2020-801 DC du 18 juin 2020*. <https://www.conseil-constitutionnel.fr>

Data Protection Act 2018, c. 12. (UK).

Defence for Children International Netherlands & ECPAT Netherlands. *Child Protection Policy*. <https://tinyurl.com/4kmjffvx>

European Court of Human Rights. *K.U. v. Finland*, Application No. 2872/02, 2008.

Federal Trade Commission. Children's Online Privacy Protection Rule, (1999). New Zealand Parliament. Harmful Digital Communications Act, (2015).

Online Safety and Media Regulation Act 2022, No. 44/2022. (Ireland).

UK Parliament. Online Safety Act 2023. <https://tinyurl.com/3uf298e4>

Beszámolók

Annual Report 2022/2023. Netsafe. <https://tinyurl.com/2pctazjy>

Australian Communications and Media Authority eSafety Commissioner. Annual Report 2023-24. <https://tinyurl.com/ydxjy6yk>

Biztonsagosinternet.hu hotline beszámoló 2023. A Nemzetközi Gyermeekmentő Szolgálat Magyar Egyesület kiadmánya a Biztonsagosinternet.hu hotline 2023. évi tevékenységéről. <https://tinyurl.com/8srdanw8>

Insights and Trends: Analysis of Report Harmful Content 2023. <https://tinyurl.com/bda6hsdb>

Internet Hotline beszámoló. A Nemzeti Média-és Hírközlési Hatóság kiadványa az Internet Hotline 2023. évi tevékenységéről. <https://tinyurl.com/yzp9wkup>

Keeping Kids Safer Online. Online. Safety. Matters. Trends and Usage Reports Academic Year 2022-2023. <https://tinyurl.com/t9ucnhzs>

Netsafe Quarterly Report April-June 2024. <https://tinyurl.com/4rr229ra>

Netsafe Quarterly Report January-March 2024. <https://tinyurl.com/4rr229ra>

Online források

American Psychological Association. Social media brings benefits and risks to teens. Psychology can help identify a path forward. <https://tinyurl.com/4rz8jx6t>

Australian Human Rights Commission. Cyberbullying. <https://tinyurl.com/2xyvwnuv>

Biztonsagosinternet.hu. <https://tinyurl.com/msv45ydc>

Cambridge Dictionary. Cyber. <https://tinyurl.com/29uc7bu4>

Coimisiún na Meán. <https://tinyurl.com/eynrx4hr>

Commonwealth of Pennsylvania. Cyberbullying. <https://tinyurl.com/mrxr8dk4>

Criminal & traffic law. Cyberbullying: Protections against online/digital harassment. <https://tinyurl.com/3uuc5ncx>

Cyberbullying Research Center. <https://cyberbullying.org>

CybersafeKids. <https://tinyurl.com/24697d3r>

End to Cyber Bullying. <https://tinyurl.com/ycy5wwzh>

eSafety Commissioner. Cyberbullying advice for educators and schools. <https://tinyurl.com/3u6a4tvh>

eSafety Commissioner. Report online harm. <https://tinyurl.com/42nha8fy>

Hector's world. <https://tinyurl.com/5fhmbmjik>

Hogan Lovells. French Legal and Regulatory Update, May 2024. <https://tinyurl.com/yt7wd28r>

Hotline.ie. <https://hotline.ie>

HUDSON, Castle; INKELL, LLC: Cyber Bullying Stories: The Ryan Halligan Case (1989 – 2003). 2020.10.05. <https://tinyurl.com/ywjr5v6v>

Internet Hotline. Az Internet Hotline szolgálatról. <https://tinyurl.com/3kzkv6tr>

Jugendschutz.net. <https://tinyurl.com/2r24aj8y>

Justice.govt.nz. Applying for a Harmful Digital Communications order. <https://tinyurl.com/auas7fdv>

Kaspersky. What is cyberbullying? <https://tinyurl.com/48j8t3me>

Kids Helpline. <https://tinyurl.com/yusk5bbm>

Kindertelefoon. <https://tinyurl.com/tzbu3dt8>

Laws. Who was Alexis Pilkington? <https://tinyurl.com/32ezpvjk>

Lifeline. <https://tinyurl.com/3f7z2vxv>

Netsafe. <https://netsafe.org.nz/netsafe>

Nowcomment. The Top Six Unforgettable CyberBullying Cases Ever. <https://tinyurl.com/y57hhyh2>

NummergegenKummer. <https://tinyurl.com/bdfm92nm>

Report Harmful Content. <https://tinyurl.com/4svu5c4u>

Safer Internet Day 2009: Commission starts campaign against cyber-bullying. <https://tinyurl.com/5ax24u64>

Stomp Out Bullying. <https://www.stompoutbullying.org>

stopbullying.gov. Laws, Policies & Regulations. <https://tinyurl.com/2utjxbtp>

stopbullying.gov. Texas Anti-Bullying Laws & Policies. <https://tinyurl.com/5ar77cxw>

Study.com. Cyberbullying Definition, Effects & History. <https://tinyurl.com/7stxrndv>

TABBY trip in Eu. <https://tinyurl.com/mr27xxm6>

TeensHealth.Cyberbullying. <https://tinyurl.com/mrx686mf>

The Canadian Encyclopedia. Amanda Todd Case. <https://tinyurl.com/3krfcmem>

UK Safer Internet Centre. <https://tinyurl.com/yc2mf5zv>

Unicef. Cyberbullying: What is it and how to stop it. <https://tinyurl.com/2s5p7xzz>

Unicef. Protecting Children online. <https://tinyurl.com/54xe2dze>

WILLARD: Educators guide to cyberbullying: Addressing the harm caused by online social cruelty. <https://tinyurl.com/5n78k5rc>

YMCA of greater brandywine: Cyberbullying: What You Need to Know. <https://tinyurl.com/m9edf36y>

Egyéb források

BREITBARTH, Paul. The GDPR Implementation Act in The Netherlands. *National Adaptations of the GDPR*, 2019.

LUEVANOS, Maria. A Policy Analysis on California's Cyber Bullying Laws Under the Education Code. 2014. PhD Thesis. California State University, Bakersfield.