



**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

„Idegen arcokat nézek...”

***A kiskorúak sérelmére a generatív mesterséges intelligencia
felhasználásával, online térben elkövetett jogsértések újabb
kárfelelősségi irányai az Amerikai Egyesült Államokban***

**Kézirat lezárásának dátuma:
2024. december 9.**

A dolgozat szerzőjeként kijelentem,
hogy dolgozatomhoz nem vettem igénybe mesterséges intelligenciát.

TARTALOMJEGYZÉK

BEVEZETÉS	4
1. A MESTERSÉGES INTELLIGENCIÁVAL PÁRHUZAMOSAN FEJLŐDŐ, A KISKORÚAKAT FENYEGETŐ VESZÉLY	5
2. A MESTERSÉGES INTELLIGENCIA VISSZAÉLÉSSZERŰ FELHASZNÁLÁSA	9
2.1 A mesterséges intelligencia által generált, gyermekekkel való szexuális visszaélést ábrázoló tartalom és a deepfake technológia.....	9
2.2 A generált visszaélésszerű tartalmak forrása: az ellenőrizetlen adatkészletek és a „sharenting”	11
2.2.1. A betanító adatbázisok lehetséges diszfunkciója, a LAION-adatkészlet.....	12
2.2.2. A sharenting-jelenség mint az MI-generált CSAM forrása	13
3. A GENERÁLT TARTALMAK FELHASZNÁLÁSA GYERMEKEK SÉRELMEIRE ELKÖVETETT JOGSÉRTÉSEKHEZ	14
3.1 A cyberbullying és online zaklatás újabb szintje, avagy a mesterséges intelligencia belépése a képletbe.....	15
3.2 A „sextortion”-jelenség és a fiatalokat érintő „bosszúpornó” új lépcsőfoka a generatív mesterséges intelligencia korszakában	16
4. AZ EGYESÜLT ÁLLAMOK JOGORVOSLATI GYAKORLATA, VAGY ANNAK HIÁNYA? A LEHETSÉGES KÁRFELELŐSSÉGI IRÁNYOK	18
4.1. Az „elkövető” felelőssége.....	19
4.1.1. A deliktuális, szerződésen kívüli károkozás lehetséges jogcímei (tort law)	21
4.1.2. Illinois Állam.....	25
4.1.3. Kalifornia Állam.....	25
4.1.4. Florida Állam.....	26
4.1.5. A United States Code rendelkezései.....	26
4.2. Az elkövető kiskorúsága esetén a törvényes képviselők felelőssége.....	27
4.3. Az iskola mint mulasztást megvalósító szereplő (diák áldozat és diák elkövető esetén).....	29
4.4. Az online platformok, a Communications Decency Act nyújtotta mentesség	31
4.5. A mesterséges intelligencia: avagy a készítőik és fejlesztők mint potenciális felelősök	33
5. A TÖRVÉNYJAVASLATOKRÓL: LÉPÉST TARTANI A MESTERSÉGES INTELLIGENCIÁVAL?	34
5.1. A generált, szexuálisan explicit tartalmak készítői és terjesztői vonatkozásában.....	35
5.1.1. A 2024. évi DEFIANCE Act	35
5.1.2. A 2023. évi Preventing Deepfakes of Intimate Images Act	36
5.1.3. A 2024. évi No AI FRAUD Act.....	37
5.1.4. A 2023. évi DEEPFAKES Accountability Act	38
5.2. A platformok felelősségre vonását és mentességük módosítását célzó törvényjavaslatok ..	38
5.2.1. SAFE TECH Act.....	38
5.2.2. EARN IT Act	39

6. KILÁTÁSOK, JAVASLATOK	40
6.1. Kilátások a változásra: Hogyan tovább?	40
6.2. Javaslat a megoldásra.....	41
IRODALOMJEGYZÉK	42

BEVEZETÉS

A dolgozat címében Ady Endre „Az idegen arcok” c. versének részletét idézem, amely arra a jelenségre kíván a költészet eszközével utalni, amikor a kiskorúról hétköznapi, ismert képmása alapján, visszaélésszerű, jogsértő céllal, az arckép felhasználásával készítenek generált ábrázolásokat, amelyek folytán saját arcának másolatait idegen testeken, mesterségesen előállított, idegen helyzetekben látja viszont, így azt érezheti: „idegen arcokat nézek...”.

A generatív mesterséges intelligenciával való visszaélés, illetve a kimeneti adatként előállított, generált, szexuálisan explicit képek és deepfake-ek egy olyan újszerű, korábban nem tapasztalt problémát jelentenek, amelyre az Egyesült Államok jogrendszere a bírói jogalkotás ellenére sem bírt megfelelően reagálni. A kutatás térbeli korlátozottsága ellenére a mesterséges intelligenciával való megbirkózás egy univerzális feladat és probléma. A generatív mesterséges intelligencia fejlődésével és térnyerésével párhuzamosan nő a modern társadalmat, így különösen a kiskorúakat fenyegető veszély, melynek fokozódása globális szinten zajló jelenség. E visszaélések, vagyis az explicit generált tartalmak komoly kihívást jelentenek az Amerikai Egyesült Államok jogrendszerével szemben már ma is. Ez a jelenség a világ technológiailag arra „felkészült” régióiban a közeljövő egyik legjelentősebb problémája lehet; amely nemcsak a társadalom, hanem a jogrendszer rezilienciájának, vagyis rugalmasságának, reagáló- és ellenállóképességének lesz az egyik próbaköve. Így mindezt nemcsak a társadalomnak, de a jogrendszernek is megfelelően fel kell készülnie annak érdekében, hogy a visszaélésszerű felhasználásra megfelelően reagálni tudjon és megoldást tudjon kínálni a „generatív mesterséges intelligencia károsultjai” számára.

Dolgozatomban szeretném ismertetni a gyermekek szexuális bántalmazását ábrázoló generált tartalmakat és deepfake-eket, azok meghatározását és ezzel összefüggésben, az explicit tartalom-generálás mibenlétét, alapjait és az ahhoz fűződő diszfunkciókat. Röviden bemutatom, hogy a generált felvételek hogyan súlyosbítják az online térben elkövetett jogsértések jelenlegi

helyzetét. Ezt követően pedig a lehetséges kárfelelősségi irányokat vizsgálom, majd az ezek megváltoztatására irányuló, már benyújtott szövetségi törvényjavaslatokat. Végezetül áttekintést adok a valószínűsíthető kilátásokról a probléma kezelését illetően, és javaslatot teszek egy mesterséges intelligencia specifikus jogszabály meghozatalára.

Kutatásom „színtere” az Amerikai Egyesült Államok jogrendszere; amelyet az aggodalomra okot adó eseteknek a sokszínű és szabad amerikai társadalom magas technológiai fejlettsége következtében történő megjelenése, és azzal párhuzamosan a szövetségi – és sok esetben a tagállami – jogrendszer relatív felkészületlensége indokol. Kutatásom célja feltárni a jelenleg rendelkezésre álló potenciális kárfelelősségi irányokat, ezen túlmenően pedig egy egységes, direkt megoldás keresése a sérelmet szenvedett kiskorúak kárának megtérítésére.

1. A MESTERSÉGES INTELLIGENCIÁVAL PÁRHUZAMOSAN FEJLŐDŐ, A KISKORÚAKAT FENYEGETŐ VESZÉLY

Kutatásom térben – miként említettem – az Amerikai Egyesült Államokra korlátozódik. Ennek az az oka, hogy jóllehet Magyarországon, a nemzeti törvények alkalmazhatósága mellett az Európai Unió AI Actnek köszönhetően már rendelkezésre áll egy viszonylag fejlett joganyag a mesterséges intelligencia felhasználásának és következményeinek szabályozására,¹ az MI-rendszerek felhasználásával elkövetett jogsértéseknek még nincs – a szakirodalom és a kutatható bírósági gyakorlat nyomán – világosan kimutatható gyakorlata.

Ezzel szemben az Egyesült Államokban – mint látni fogjuk – a helyzet pont az ellenkező: sem a szövetségi, sem a tagállami jogrendszerek, sem az ítélkezési gyakorlat nem fejlődött párhuzamosan az MI-technológiával. Ezt a lemaradást jelzi az elmúlt években megvalósuló, számos, aggodalomra okot adó eset is, amelyekben a technológia felhasználásával generálnak szexuális tartalmakat kiskorúakról. Az elmúlt években ilyen esetek történtek többek közt New

¹ Bár rendelkezései fokozatosan lesznek kötelezőek a tagállamokra. Lásd: Ma hatályba lép az EU AI Act: új korszak a mesterséges intelligencia szabályozásában. Jogászvilág (2024). (<https://jogaszvilag.hu/a-jovo-jogasza/ma-hatalyba-lep-az-eu-ai-act-uj-korszak-a-mesterseges-intelligencia-szabalyozasaban/>); az előrelépést jelentő törvény 2024. augusztus 1-jén hatályba lépett, amely meghatározza a deepfake fogalmát (Fogalommeghatározások 60.), rendelkezést tartalmaz a generált tartalmak megkülönböztetésének követelményéről (134) – Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete

Jersey Államban, egy westfieldi középiskolában,² a Washington Állambeli Issaquah egyik iskolájában,³ Észak-Karolinában,⁴ illetve Kaliforniában, egy beverly hills-i középiskolában.⁵

A jelenlegi hazai eset-szegény helyzet ellenére is fontos beszélni erről a problémáról, hiszen a generatív mesterséges intelligencia szoftverek világszerte, így Magyarországon is elérhetőek.⁶ Ezek visszaélészerű felhasználása csak az idő kérdése. Az Egyesült Államokban vizsgált problémát illetően prognosztizálható, hogy a technológiailag kellően fejlett államokban világszerte hasonlóan meg fog jelenni az MI-rendszerekkel való visszaélés. A jelenség nem fog megállni az államhatárokon és egy teljes mértékben globális problémává fogja kinőni magát. Ennek függvényében, az Egyesült Államokra korlátozódó vizsgálat szükségességét nagyon jól szemlélteti Pongó Tamás gondolata, miszerint „*a common law és a kontinentális jogcsaládok közötti különbségek bizonyos globálisan jelentkező problémák esetén csökkennek*”.⁷

Megállapítható tehát, hogy az USA-ban jelenleg megoldatlan probléma a világ más térségeiben, így Magyarországon is, a jövő problémáját, a jogrendszer következő kihívását jeleníti meg. Ezt előrejelzi többek közt egy a közelmúltban a sajtóban megjelent „botrány”, amelynek forrása egy magyar személyről generált és elterjedt deepfake videó.⁸

² Atherton, Daniel: Incident 597: Students Traumatized as AI-Generated Fake Nudes Are Circulated at New Jersey High School. Artificial Intelligence Incident Database (2023). (<https://incidentdatabase.ai/cite/597/>)

³ Atherton, Daniel: Incident 617: Male student allegedly used AI to generate nude photos of female classmates at a high school in Issaquah, Washington. Artificial Intelligence Incident Database (2023). (<https://incidentdatabase.ai/cite/617/>)

⁴ Atherton, Daniel: Incident 605: North Carolina Psychiatrist Used Artificial Intelligence to Produce Images of Child Sex Abuse. Artificial Intelligence Incident Database (2021). (<https://incidentdatabase.ai/cite/605/>)

⁵ Healey, Jon: Scandal over AI-generated nudes at Beverly Hills middle school exposes gaps in law. Los Angeles Times (2024). (<https://www.latimes.com/california/story/2024-03-03/scandal-over-ai-generated-nudes-at-beverly-hills-middle-school-highlights-gaps-in-law>)

⁶ Zách, Dániel: Pár ezer forintnyi összegért akár kiskorú lányokról is lehet hamis meztelen képeket generálni egy deepfake-alkalmazással. Telex (2024). (<https://telex.hu/techtud/2024/03/01/deepfake-spanyolorosz-egyesult-allamok-feheroroszsorszag-bunugy-ai-mesterseges-intelligencia>)

⁷ Pongó, Tamás: A cyberbullying és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére. Iurisperitus Kiadó: Szeged (2021) 20.

⁸ Lásd Flachner, Balázs: Mesterséges intelligenciával generált Schwab Richárd-hamisítvány népszerűsít fura csodaszert az interneten. Telex (2024). (<https://telex.hu/techtud/2024/11/18/schwab-richard-deepfake-kamu-video>)

Az előre jelezhető visszaélésekből szinte automatikusan mások jogainak sérelme következik, amely pedig a jogrendszer felkészültségét igényli. Hazánkban a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) személyiségi jogok védelmével kapcsolatos rendelkezései⁹ – absztrakt természetükből adódóan – alkalmazhatóak lesznek a probléma kezelésére, mégis valószínűsíthető, hogy az MI-visszaélések különlegessége miatt egyes jogfogalmak alkalmazása új normaértelmezési kihívás elé állítja majd a bíróságokat. E körben felmerülhet a „jogsértő” kifejezés – mint jelző és főnév (2:51. és 2:53. §) – értelmezése, amely problémás lehet akár a jogsértő személy megnevezése, meghatározása terén, akár a jogsértő jelleg körében a visszaélés sajátos jellemzői következtében figyelemmel az anonim tartalom-közzététel lehetőségére. További kérdés lehet a szankciók között a „jogsértést megelőző állapot helyreállítása” is, amely az internetről való „eltávolíthatatlanság” miatt egyes esetekben végrehajthatatlan ítéletet eredményezhet.¹⁰

Ennek ellenére dolgozatomban a magyar helyzetet két okból nem vizsgálom. Egyrészt tudomásom szerint és a sajtóban fellelhető információk alapján nem történt hazai viszonylatban kiskorúakról generált explicit tartalmak kapcsán nyilvánosságra hozott eset. Illetve a Bírósági Határozatok Gyűjteményében sem szerepel olyan jogerős ítélettel lezárt ügy, amelynek tárgya mesterséges intelligencia által generált tartalommal okozott sérelem. Másrészt pedig ezen kérdéskör vizsgálata szétfeszítette volna a dolgozat keretét, mely a központi, aktuálisan megoldatlan probléma minél kimerítőbben történő feltárására és bemutatására törekszik.

Az amerikai joganyag vizsgálata során figyelembe veszem az Egyesült Államok szövetségi szabályozását és az államok joganyagát. Bírói precedens, illetve olyan bíróság előtt zajló ügy a generált tartalmak felhasználásával elkövetett visszaélések kapcsán, amely bírósági kereteken belül kártérítéssel végződött volna nincs a témában,¹¹ így az esetjogot mélyebben nem vizsgálom. A fentebb jelzett, kimutatható ügyek forrása a sajtó, amely rámutatott arra is, hogy az ügyek egy része egyezséggel zárulhatott.

⁹ Lásd 2:42–2:54. §.

¹⁰ Lásd az elfeledtetéshez való jog sérelme kapcsán írtakat a 14. oldalon.

¹¹ A New Jersey Államban történt eset kapcsán a sérelmet szenvedett fél (és szülei) indítottak polgári pert (lásd Jane Doe v K.G.).

Vizsgálataim korosztály szerint az amerikai kiskorúakra (kiskorúakon belül is leginkább a tizenéves korosztályra) korlátozódnak. Az, hogy kik számítanak polgári jogi szempontból kiskorúnak, államonként differenciált, de az államok többségében a kiskorúság 18 éves korig terjed.¹² A kérdés vizsgálata több okból is kiemelten fontos ennek a korosztálynak a vonatkozásában. Felmérések alapján kimutatható, hogy az Egyesült Államokban alapvetően az internetes zaklatás és cyberbullying áldozatai között is magas a kiskorúak aránya.¹³ Ez a magas arány pedig összefüggésben van azzal, hogy majdnem minden amerikai tizenéves rendelkezik mindennapi internet-hozzáféréssel¹⁴ és több mint 70%-uk napi szinten látogat különféle közösségi média oldalakat.¹⁵ Ilyen magas internetes jelenlét mellett fokozottan ki vannak téve az online térben rejlő veszélyeknek, amelybe beletartoznak a generált szexuális tartalmak és deepfake-ek is. A közösségi platformok használatával nemcsak annak lehetősége magas, hogy káros tartalmakkal találkoznak böngészés közben, de az ezen felületeken keresztül könnyen áldozatává is válhatnak a visszaéléseknek.

Megjegyzendő továbbá, hogy az internetet is egyre inkább elárasztják a gyermekek szexuális visszaélését ábrázoló tartalmak.¹⁶ Csak az előző évben több mint százmillió ilyen tartalmat jelentettek a *National Center for Missing and Exploited Children* erre a célra létrehozott felületén.¹⁷ E magas szám mögött nemcsak a való életben történt visszaélésekről készült felvételek, hanem egyre több mesterségesen előállított kép és videó is áll. Ez jól jelzi azt a sokaságot, amely a jogrendszer rezilienciáját előbb-utóbb „párbajra” fogja hívni.

¹² Lásd Interstate Commission for Juveniles: Age Matrix. (<https://juvenilecompact.org/age-matrix>)

¹³ Vogels, Emilia A.: Teens and Cyberbullying 2022. Pew Research Center (2022). (A 13-17 éves fiatalok esetén 46% az arány). Vogels, Emilia A.: The State of Online Harrasmen. Pew Research Center (2021). (A felnőttek esetén 41% az arány.)

¹⁴ Vogels, Emilia A. – Gelles-Watnick, Risa – Massarat, Navid: Teens, Social Media and Technology 2022. Paw Research Center (2022).

¹⁵ Anderson, Monica – Faverio, Michelle – Gottfried, Jeffrey: Teens, Social Media and Technology 2023. Paw Research Center (2023).

¹⁶ O'Brien, Matt – Hadero Haleluya: AI-generated child sexual abuse images could flood the internet. Now there are calls for action. The Associated Press (2023). (<https://apnews.com/article/ai-artificial-intelligence-child-sexual-abuse-c8f17de56d41f05f55286eb6177138d2>)

¹⁷ National Center for Missing and Exploited Children: Cybertipline 2023 Report (<https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#files>)

2. A MESTERSÉGES INTELLIGENCIA VISSZAÉLÉSSZERŐ FELHASZNÁLÁSA

A mesterséges intelligencia (MI) szoftverek fejlődése tagadhatatlanul sok szempontból pozitív,¹⁸ ám előnyeit, az MI nyújtotta lehetőségeket könnyen „visszájára lehet fordítani”. Témám középpontjában is a generatív MI-rendszerek (ezen belül is a képgeneráló modellek) visszaélészerű felhasználása áll, vagyis a szexuálisan explicit tartalom generálása.

2.1 A mesterséges intelligencia által generált, gyermekekkel való szexuális visszaélést ábrázoló tartalom és a deepfake technológia

Alapvetésként megjegyezném, hogy nem minden CSAM deepfake,¹⁹ és nem minden deepfake CSAM (lásd alább).²⁰ Kutatásomban e két jelenség – pontosabban a generatív mesterséges intelligencia és a CSAM – metszete, vagyis a generált visszaélészerű tartalmak, illetve ezek szűkebb köre, a szexuálisan explicit deepfake-ek relevánsak. A „CSAM” (child sexual abuse material), azaz a gyermekek szexuális visszaélését, bántalmazását, kizsákmányolását ábrázoló tartalom alatt értünk minden olyan felvételt, amelyben a gyermekek valamilyen szexuális helyzetben, szexuális tevékenységet folytatva kerülnek ábrázolásra.²¹ E tartalmak között nem csak a megtörtént, valós visszaélésekről hang-, illetve képrögzítő eszközökkel készített

¹⁸ Lásd s.n. Applications of Artificial Intelligence Across Various Industries. Forbes (2023).
(<https://www.forbes.com/sites/qai/2023/01/06/applications-of-artificial-intelligence/>)

¹⁹ A gyermekek szexuális bántalmazását ábrázoló tartalmak fókuszában a kiskorúak kizsákmányolásának megjelenítése van. Ezek elsősorban valós visszaéléseket megjelenítő felvételek; a digitálisan módosított, illetve a mesterséges intelligencia segítségével generált CSAM a jelenség alkategóriái.

²⁰ A deepfake ábrázolások bármiről készülhetnek, nem feltétlenül jelenítenek meg szexuális tartalmat, magatartást, így például a választási deepfakek sem (Lásd Bondy, Meeka – Delaney, John – Ong, Jeff: AI-Generated Deepfakes and the Emerging Legal Landscape. Perkins Coie (2024).
(<https://www.ageofdisruptionblog.com/2024/04/ai-generated-deepfakes-and-the-emerging-legal-landscape/>).
O’Donell, Nicholas: Have We No Decency? Section 230 And The Liability of Social Media Companies For Deepfake Videos. University of Illinois Law Review 701 (2021). Illetve lehetnek teljesen ártalmatlanok is: például paródia, filmipari felhasználás. Lásd Tshimbalanga, Sydney: Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography. Tulane Journal of Technology and Intellectual Property, 26 (2024) 137–138.

²¹ National Center for Missing and Exploited Children: Child Sexual Abuse Material
(<https://www.missingkids.org/theissues/csam>)

felvételekről lehet szó. Ma már ennek kapcsán szükséges beszélnünk a mesterséges intelligencia felhasználásával generált tartalmakról,²² illetve ezek egy szűkebb, specifikusabb köréről, a deepfake-ekről is. A deepfake-ek olyan generatív mesterséges intelligencia felhasználásával létrehozott vagy módosított kép-, videó- és/vagy hangfelvételek, amelyek más személy képmását, illetve hangját használják fel oly módon, hogy azok teljesen valóságosnak tűnjenek.²³

A mesterséges intelligencia rendszerek térnyerésének köszönhetően egyre többen veszik igénybe a kifinomultabb algoritmusokat deepfake-ek létrehozására, illetve egyre többen élnek is vissza azokkal.²⁴ E szoftverek segítségével sokkal egyszerűbbé és gyorsabbá, ezáltal még szélesebb körben elérhetővé vált a szexuálisan explicit tartalmak készítése.²⁵ Az ebből adódó elterjedtségen túlmenően, a deepfake-ek jelentette különös veszély másik jelentős tényezője, hogy nehezen, esetenként egyáltalán nem megállapítható róluk, hogy nem valódiak.²⁶ Ebből következően jelenthető ki teljes biztossággal a gyermekeket ábrázoló explicit deepfake-ek CSAM volta. Egy átlagos, a technológia ismérveiben nem jártas ember nagy valószínűséggel ma már nem tudja megkülönböztetni a valós visszaélést és a generált bántalmazást. Ez az MI-rendszerek folyamatos fejlődésével hamarosan akár olyan formát is ölthet, aminél még a szakemberek is csak nehezen vagy egyáltalán nem lesznek képesek elhatárolni ezeket a valódi felvételektől.

A gyermekekkel való szexuális visszaélések ábrázolása alá sorolhatók alapvetően a valódi gyermekekről készített deepfake-ek, de emellett nem létező gyermekeket is megjelenítenek

²² Internet Watch Foundation: What has changed in the AI CSAM Landscape (2024). 7

²³ s.n. Definition of Deepfake from the Cambridge Advanced Learner's Dictionary And Thesaurus. Cambridge University Press). Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete: Fogalommeghatározások (60).

²⁴ Bondy, Meeka – Delaney, John – Ong, Jeff: AI-Generated Deepfakes and the Emerging Legal Landscape. Perkins Coie (2024). (<https://www.ageofdisruptionblog.com/2024/04/ai-generated-deepfakes-and-the-emerging-legal-landscape/>). Deepfakes: How to Protect Your Kids. Canopy (2024). (<https://canopy.us/2024/04/16/deepfakes-how-to-protect-your-kids/>)

²⁵ Aronashvili, Reuven: The Evolution Of Sextortion Attacks: How Generative AI Is Taking A Front Seat. Forbes Technology Council (2024). (<https://www.forbes.com/councils/forbestechcouncil/2024/02/20/the-evolution-of-sextortion-attacks-how-generative-ai-is-taking-a-front-seat/>)

²⁶ Deepfakes: How to Protect Your Kids. Canopy (2024).

szexuálisan explicit helyzetben.²⁷ Ennek vonatkozásában aggodalomra okot adó az elkészítés célja mellett az is, hogy ezek generálásához az MI-rendszer sok esetben, (habár képes a pornográfiáról és gyermekábrázolásokról tanultakat kombinálni) valós visszaélésekről készült ábrázolásokat vesz alapul.²⁸

2.2 A generált visszaélésszerű tartalmak forrása: az ellenőrizetlen adatkészletek és a „sharenting”

A gyermekek szexuális visszaélését megjelenítő, mesterségesen előállított tartalmakkal kapcsolatban érdemes megvizsgálni, hogy ezek generálása hogyan történik, mi az alapjuk. Habár a fejlett mesterséges intelligencia szoftverek képesek két külön területről; a felnőtt pornográfiáról és átlagos gyermekképekről tanultakat kombinálni,²⁹ nem mindig ez a helyzet. Sokszor ezen tartalmak forrása az interneten vagy a betanító adatbázisban fellelhető, gyermekek szexuális bántalmazásáról készült valós felvételek. Megemlítendő továbbá, hogy sok esetben alapvetően teljesen ártalmatlan, a gyermekekről nyilvánosan közzétett felvételek kerülnek felhasználásra a készítő által (vagy az interneten keresztül), az explicit tartalmak generálásához. Ez történhet egyrészt úgy, hogy az internetről táplálkozó alapmodellbe kerül be megosztott fénykép, másrészt pedig úgy, hogy a készítő használ fel nyilvánosan közzétett képet az internetről. Mindkét esetben a gyermek áldozattá válásának esélye arányosan nő a róla online fellelhető tartalmak mennyiségével. A generálás forrásainak vonatkozásában így a problémának két különböző oldalát érdemes megvizsgálni: azon jelenséget, amikor az MI-rendszer betanításhoz felhasznált adatkészletébe bekerülnek CSAM tartalmak, illetve amikor a sharenting által a szülők adatot szolgáltatnak az MI-rendszerekhez saját gyermekükről.

²⁷ Atherton, Daniel: Deepfakes and Child Safety: A Survey and Analysis of 2023 Incidents and Responses (2024). (<https://incidentdatabase.ai/blog/deepfakes-and-child-safety/>)

²⁸ Atherton (2024). Korte, Lara: California launches new broadside against tech over harmful AI content. Politico (2024). (<https://www.politico.com/news/2024/01/16/california-ai-generated-child-sex-abuse-material-bill-00135786>)

²⁹ Thiel, David: Identifying and Eliminating CSAM in Generative ML Training Data and Models. Stanford Internet Observatory (2023) 2.

2.2.1. A betanító adatbázisok lehetséges diszfunkciója, a LAION-adatkészlet

A gépi tanulási képgenerátor modellek a betanító adatbázisokban szereplő képekből táplálkoznak.³⁰ Ebből következően a nem megfelelően ellenőrzött adatbázisok fokozott veszélyt jelenthetnek a generált képeket illetően.³¹ Minél több szexuálisan explicit tartalom, illetve ezek között potenciálisan CSAM szerepel ezekben az adatkészletekben, annál jelentősebb mértékben befolyásolhatja, egyszerűbbé teheti az ilyen jellegű generálást és még realiztikusabbá a generált tartalmat.³² A CSAM jelenléte volt problémás a LAION 5B (Large-scale of Artificial Intelligence Open Network) adatbázis esetében is,³³ amelyet felhasználtak többek közt a népszerű képgenerátor modell, a Stable Diffusion betanításához.³⁴

Megemlítendő továbbá, hogy számos olyan modell van, amely az egész internetre kiterjedő adatbázisból táplálkozik, ami magában foglalja az interneten fellelhető már önmagukban is MI-generált tartalmakat, így a mesterségesen előállított CSAM-et is; amik így újra bekerülnek a „körforgásba” és a továbbiakban maguk is alapul fognak szolgálni újabb visszaélészerű képek kreálásához.³⁵

Ez a diszfunkció megfelelő szűrők, ellenőrzések alkalmazásával, ha teljesen elkerülhető nem is, de legalább jelentős mértékben leszűkíthető lenne.³⁶

³⁰ Thiel, David: Identifying and Eliminating CSAM in Generative ML Training Data and Models. Stanford Internet Observatory (2023) 2.

³¹ O'Brien, Matt – Hadero Haleluya: AI image-generators are being trained on explicit photos of children, a study shows. The Associated Press (2023). (<https://apnews.com/article/generative-ai-illegal-images-child-abuse-3081a81fa79e2a39b67c11201cfd085f>)

³² Thiel (2023) 3. O'Brien – Hadero (2023).

³³ Uo. Thiel (2023) 2-3, 7-8; O'Brien – Hadero (2023).

³⁴ O'Brien – Hadero (2023).

³⁵ Henderson, Peter – Hashimoto, Tatsunori – Lemley, Mark: Where's the liability in harmful ai speech? Journal of Free Speech Law 3/2 (2023) 589, 602, 604.

³⁶ O'Brien – Hadero (2023).

2.2.2. A sharenting-jelenség mint az MI-generált CSAM forrása

A legtöbb generatív MI-szoftver alapmodellje részben vagy egészben az internet alapján kerül betanításra.³⁷ Ebbe az online felületekről származó fotókat is magában foglaló adatkészletbe bekerülhet bármilyen a közösségi médián nyilvánosan megosztott fotó.³⁸ Továbbá a generálás szempontjából fontos tényező az is, hogy a szabadon hozzáférhető fotókat bárki lementheti és bármilyen célra: például mesterséges CSAM készítésére is felhasználhatja.

Habár a publikus tartalmakkal való visszaélés nem újdonság, a mesterséges intelligencia fejlődésével, hasonlóan a többi jelenséghez, ez is minden eddiginél nagyobb mértéket öltött.³⁹ A szülőknek így még tudatosabbnak kell lenniük azzal kapcsolatban mit és milyen szinten osztanak meg gyermekeikről a nyilvánossággal. Ugyanis a gyermekeiket ábrázoló tartalmak túlzásba vitt megosztása akaratlanul fokozott veszélynek teszik ki őket.⁴⁰ Ez a közösségi médián történő „túlosztás” a sharenting jelenség.⁴¹

A generatív MI-rendszerek segítségével a gyermekeket ábrázoló teljesen hétköznapi képeket szexuálisan explicitté módosíthatják akár a gyermek ruházatának eltávolításával, akár csak az ábrázolt gyermek arcának felhasználásával.⁴² Természetesen az áldozattá váláshoz nem feltétlenül kell számtalan fotót közzétenni, mégis minél több adat áll rendelkezésre egy személyről online, a veszély annál inkább sokszorozódik.

³⁷ Henderson, Peter – Hashimoto, Tatsunori – Lemley, Mark: Where's the liability in harmful ai speech? *Journal of Free Speech Law* 3/2 (2023) 589, 602. Thiel, David: Identifying and Eliminating CSAM in Generative ML Training Data and Models. *Stanford Internet Observatory* (2023) 2.

³⁸ Saliba, Emmanuelle: Sharing photos of your kids? Maybe not after you watch this deepfake ad. *Abc News* (2023). (<https://abcnews.go.com/GMA/Family/sharing-photos-kids-after-watch-deepfake-ad/story?id=101730561>)

³⁹ Uo.

⁴⁰ Saliba (2023). Fineman, Melanie N.: Honey, monetized the kids: commercial sharenting and protecting the rights of consumers and the internet's child stars. *Georgetown Law Journal*, 111 /4 (2023) 860-863.

⁴¹ Fineman (2023) 848. Saliba (2023).

⁴² Saliba (2023). O'Brien, Matt – Hadero Haleluya: AI image-generators are being trained on explicit photos of children, a study shows. *The Associated Press* (2023). (<https://apnews.com/article/generative-ai-illegal-images-child-abuse-3081a81fa79e2a39b67c11201cfd085f>)

Az I. részben említett, kiskorúak online jelenlétének magas százalékához kiegészítésként megjegyzendő, hogy a szüleik tevékenysége folytán a legtöbb amerikai fiatal már kisgyermekkorban rendelkezik online jelenléttel.⁴³

3. A GENERÁLT TARTALMAK FELHASZNÁLÁSA GYERMEKEK SÉRELMERE ELKÖVETETT JOGSÉRTÉSEKHEZ

Mindenekelőtt megjegyezném, hogy önmagában a szexuális explicit generált tartalmak elkészítése, azok terjesztése is jogsértést valósít meg az ábrázolt kiskorúakkal szemben. Kutatásom középpontjában is ez a jelenség áll. Ezen fejezetben viszont kitérek a generált tartalmak online térben való, lehetséges felhasználására.

Megfelelő korlátozások nélkül a generatív MI-eszközök nagy eséllyel vannak kitéve a visszaélésszerű felhasználás veszélyének, ezáltal pedig hozzájárulhatnak többek között a cyberbullying, az online zaklatás, a sextortion és a bosszúpornográfia megvalósításához.⁴⁴

Az említett generált szexuálisan explicit tartalmak számos online térben történő jogsértés megvalósításához eszközül szolgálhatnak, tovább súlyosbítva ezáltal az internet jelentette különös veszélyeket a kiskorúakra nézve. Új szintre emelik e visszaélések lebonyolítását, ezzel hozzájárulva azok további térnyeréséhez.

⁴³ Fineman, Melanie N.: Honey, monetized the kids: commercial sharenting and protecting the rights of consumers and the internet's child stars. *Georgetown Law Journal*, 111/4 (2023) 850.

⁴⁴ Bialos, Noah – Natasha Amlani, Natasha – Klein, Samuel: Generative AI: How Existing Regulation May Apply to AI-Generated Harmful Content. Perkins Coie (2023). (<https://www.perkinsonprivacy.com/2023/10/generative-ai-how-existing-regulation-may-apply-to-ai-generated-harmful-content/#more-3243>). Deepfakes: How to Protect Your Kids. Canopy (2024). (<https://canopy.us/2024/04/16/deepfakes-how-to-protect-your-kids/>)

3.1 A cyberbullying és online zaklatás újabb szintje, avagy a mesterséges intelligencia belépése a képletbe

Habár a cyberbullyingnak nincs egységes definíciója az Egyesült Államokban;⁴⁵ általános fogalmi elemei alapján úgy lehet összefoglalni, mint hatalmi egyensúlytalanságban lévő felek között, elektronikus úton megvalósított valamilyen formájú (de leginkább érzelmi) szándékos károkozás, amely folyamatos vagy többször ismétlődő.⁴⁶ Bár az online zaklatás ezen elemeknek nem feltétlenül felel meg, ennél kevésbé „összetett” megvalósítási forma; gyakran értelmezik együtt a két alakzatot.⁴⁷ Mivel vizsgálatom szempontjából a két jelenség fogalmi elhatárolása nem releváns, viszont a mesterséges intelligencia felhasználása, ennek hatásai mindkét esetben ugyanolyan meghatározó tényező, így együtt vizsgálom őket.

A cyberbullying és a zaklatás, mint a legtöbb kiber-térben történő jogsértés, alapvetően számos sajátos veszélyt magában hordoz, amelyet a generatív mesterséges intelligencia felhasználása csak tovább terhel. A webes felületeken keresztül nincsenek korlátozva sem időben, sem térben,⁴⁸ illetve a legtöbb platformon akár csak a bejegyzések megosztása során, akár név nélkül vagy álneven működtetett felhasználói fiókkal, de adott az anonim tartalom-közzététel lehetősége.⁴⁹ Szintén az online jelenlét sajátossága az áldozat elfeledtetéshez való jogának („right to be forgotten”) sérelme: ami egyszer az internetre felkerült, azt onnan szinte lehetetlen eltávolítani, a tartalom újból megjelenhet a különböző platformokon.⁵⁰ Kiemelendő még az ún. virális terjedés, ami által az alapvetően is széles internetes közönség mértéke a közvéte

⁴⁵ Hallmark, Kirsten: Death by words: do united states statutes hold cyberbullies liable for their victims' suicide? *Houston Law Review* 60/3 (2023). 733. Pongó, Tamás: A cyberbullying és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére. *Iurisperitus* Kiadó: Szeged, 2021. 36.

⁴⁶ Ilin, Alexey: A New Cyberbullying Law? Extension of Legal Interpretations in China and Russia. *International Journal of Law, Ethics, and Technology* (2022). 62. Hallmark (2023). 733-734. De Lásd továbbá Pongó (2021) 14, 29–31, 62.

⁴⁷ Lásd például Ilin (2022) 64–65; Klein, Alyson: What a Proposed Ban on AI-Assisted 'DeepFakes' Would Mean for Cyberbullying. *Education Week* (2024). (<https://www.edweek.org/policy-politics/what-a-proposed-ban-on-ai-assisted-deep-fakes-would-mean-for-cyberbullying/2024/01>).

⁴⁸ Hallmark (2023) 732.

⁴⁹ Marcowitz-Bittont, Miriam – Sommer, Hillel: Remedying online shaming. *Cardozo International & Comparative Law Review* 5/2 (2022) 381.

⁵⁰ Uo. Marcowitz-Bittont – Sommer (2022) 379–380, 382, 410.

minden várakozását meghaladhatja.⁵¹ Mindennek újabb szintre lépése a generatív mesterséges intelligencia elterjedésével van összefüggésben.

A cyberbullying számos formája megvalósítható a generált képek felhasználásával, vagy azokkal összefüggésben, példaként említve itt a catfishinget (hamis személyazonosság létrehozása a közösségi oldalon egy konkrét áldozatot megcélózva), a cyber-mobbingot (megfélemlítő, csúfolódó, kiközösítő üzenet-áradat), vagy a sextinget (telefonon vagy interneten keresztül szexuális tartalmú képek és videók küldése).⁵²

További probléma a közösségi oldalakra feltöltött szexuális deepfake-kel, MI-generált meztelen képekkel kapcsolatban a kiskorúakat ért zaklatás, illetve a közzétett explicit képek kapcsán felmerülhet az is, hogy ezekre tekintettel válik egy kiskorú cyberbullying áldozatává a bántó, megalázó kommenteken keresztül.⁵³

3.2 A „sextortion”-jelenség és a fiatalokat érintő „bosszúpornó” új lépcsőfoka a generatív mesterséges intelligencia korszakában

A visszaélésszerű felhasználás másik kiemelendő területe az önmagukban is szexuális jellegű online jogsértések: a sextortion és a bosszúpornográfia.

A sextortion a gyermekek szexuális bántalmazásának olyan elektronikus úton megvalósított formája, amely során a kiskorúakat a róluk készült szexuális tartalmak nyilvánosságra

⁵¹ Marcowitz-Bittont, Miriam – Sommer, Hillel: Remediating online shaming. *Cardozo International & Comparative Law Review* 5/2 (2022) 377, 380–381.

⁵² Ilin, Alexey: A New Cyberbullying Law? Extension of Legal Interpretations in China and Russia. *International Journal of Law, Ethics, and Technology* (2022) 64–65.

⁵³ Fineman, Melanie N.: Honey, monetized the kids: commercial sharenting and protecting the rights of consumers and the internet's child stars. *Georgetown Law Journal*, 111/4 (2023) 862–863.

hozatalával fenyegetik, zsarolják különböző követelések teljesülése céljából.⁵⁴ Ennek alapesetében a zsaroló valós, a kiskorút ábrázoló képet, videót szerez meg a visszaéléshez.

A bosszúpornográfia egy online térben megvalósított, nem beleegyezéses pornográf jogsértés, amelynek megvalósítója azzal az indíttatással tesz közzé az ábrázolt személyről explicit tartalmat, hogy számára érzelmi sérelmet okozzon.⁵⁵ Alapesetben a felvételt terjesztő valós szexuális tartalmú képpel vagy videóval rendelkezik arról a személyről, akinek a sérelmet okozni szándékozta, akin valamilyen indíttatásból bosszút akart állni.

A generatív mesterséges intelligencia miatt ma már egyik jogsértés esetén sem feltétlenül szükséges, hogy a kiskorúról valódi meztelen képet, egyéb szexuális felvételt szerezzenek meg a jogsértők.⁵⁶ Teljesen valósághű tartalmat generálhat saját maga is néhány kattintással, amely ugyanúgy alkalmas arra, hogy a kívánt célt elérjék. Sextortion esetében a kiskorú kellően fenyegetve érzi magát a mesterségesen előállított kép potenciális nyilvánosságra hozatalától is.⁵⁷ Bosszúpornográfia esetén is, egy generált explicit fotó vagy videó közzétételével a jogsértés megvalósítója közel azonos helyzetbe hozhatja a sérteni szándékozott felet, mint egy valódi megosztásával.

Igaz, hogy az jogsértő feleknek az MI-szoftvereket megelőzően is megvolt a lehetősége képszerkesztő rendszerek igénybevételére, viszont a generálás ennél egyszerűbb és gyorsabb

⁵⁴ National Center for Missing and Exploited Children. Sextortion.

(<https://www.missingkids.org/theissues/sextortion>). s.n. Definition of Sextortion from the Cambridge Advanced Learner's Dictionary And Thesaurus. Cambridge University Press). Aronashvili, Reuven: The Evolution Of Sextortion Attacks: How Generative AI Is Taking A Front Seat. Forbes Technology Council (2024). (<https://www.forbes.com/councils/forbestechcouncil/2024/02/20/the-evolution-of-sextortion-attacks-how-generative-ai-is-taking-a-front-seat/>)

⁵⁵ Tshimbalanga, Sydney: Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography. Tulane Journal of Technology and Intellectual Property, 26 (2024) 140–141.

⁵⁶ Gieseke, Anne Pechenik: „The New Weapon of Choice”: Law's Current Inability to Properly Address Deepfake Pornography Vanderbilt Law Review, 73(5) (2020) 1480. Tshimbalanga (2024) 138. Deepfakes: How to Protect Your Kids. Canopy (2024). (<https://canopy.us/2024/04/16/deepfakes-how-to-protect-your-kids/>). Aronashvili (2024).

⁵⁷ Uo.

megvalósítási lehetőséget kínál.⁵⁸ Ezekben az esetekben sem új jelenségek alakultak tehát ki, hanem egy-egy meglévő probléma lépett magasabb szintre azáltal, hogy a jogsértők felfedezték a generatív MI nyújtotta lehetőségeket a visszaélések könnyebb kivitelezéséhez.

4. AZ EGYESÜLT ÁLLAMOK JOGORVOSLATI GYAKORLATA, VAGY ANNAK HIÁNYA? A LEHETSÉGES KÁRFELELŐSSÉGI IRÁNYOK

A polgári jogi jogorvoslat (lásd alább) lehetősége akár a büntetőjogi szankció mellett, akár ahelyett alkalmazva is lényeges, hiszen a sérelmet elszenvedett fél nem vagyoni sérelmének kompenzálása, esetleges vagyoni kárának megtérítése a cél. Éppen ezért mindenképp szükséges annak biztosítása, hogy az áldozat megfelelő jogalapra hivatkozással – nem a hazai jogfogalmi értelemben vett – kártérítési lehetőséggel tudjon élni. A téma vonatkozásában – újkeletű probléma lévén – még nincs kiforrott eszköze a kártérítésnek.

Röviden megjegyezném, hogy „jogorvoslat” kifejezés alatt a dolgozatban az anyagi jogi értelemben vett jogorvoslatot értem, az angolszász terminus technicus, a „remedy” magyar megfelelőjeként. A „jogorvoslat” kutatása tehát a kárigény-érvényesítés lehetséges jogcímeinek, a potenciális kárfelelősségi irányoknak a vizsgálatát célozza.

A fejezet címében szereplő jogorvoslati „gyakorlat” megfogalmazás önmagában megtévesztő lehetne, hiszen bevett gyakorlat még nem létezik: egyrészt az egyre sokasodó esetek ellenére nem jellemző a bírósághoz fordulás (amely valószínűleg az egységes jogalap hiányának tulajdonítható), másrészt a bíróságok nehezen birkóznak meg önmagában a közösségi média világával is,⁵⁹ így különösen a mesterséges intelligenciával. Ezek vonatkozásában a már meghozott precedensek elveit vonakodnak kiterjesztve alkalmazni.⁶⁰

„Nehezítő tényező” továbbá a felelősségi alap keresése körében, hogy az online térben lezajló, általánosságban kontakt nélküli, generált tartalmak készítésével összefüggő jogsértések közvetlenül jellemzően érzelmi és azzal összefüggő lelki-testi sérelmet okoznak, vagyoni

⁵⁸ Aronashvili, Reuven: The Evolution Of Sextortion Attacks: How Generative AI Is Taking A Front Seat. Forbes Technology Council (2024). (<https://www.forbes.com/councils/forbestechcouncil/2024/02/20/the-evolution-of-sextortion-attacks-how-generative-ai-is-taking-a-front-seat/>)

⁵⁹ Tenzer, Garfield Leslie Y. Social media harms and the common law. Brooklyn Law Review, 88 /1 (2022) 228, 243, 245.

⁶⁰ Uo.

kárként *damnum emergens* (kezelési költség, tanulásból kiesés pótlásának költsége) és *lucrum cessans* (a tanulmányi eredmények esetleges romlása folytán a romló továbbtanulási kilátások); csak tovaggyűrűző, avagy áttételes kár keletkezik (a „long-tail liabilities” analógiájára).

Nem szabályozza szövetségi törvény specifikusan a generatív CSAM-t és szexuális explicit deepfake-eket, illetve a legtöbb állam jogrendszeréről sem mondható ez el. Ezen túlmenően nincsen e tárgykörre vonatkozó precedens sem. A témabeli precedensek hiányával kapcsolatban az eddig elmondottakon túl meg kell jegyezni, hogy az online elérhető és szabadon hozzáférhető esetjogi adatbázisok (lásd: Court Listener, Harvard Case Law Access Project) alapján nincs a témában jogerős ítélettel lezárt ügy. Viszont van folyamatban levő ügy, mégpedig a New Jersey Államban történt eset kapcsán.⁶¹ Továbbá nem zárható ki az sem, hogy peren kívüli megegyezés született több eset vonatkozásában (hiszen ezek általában nem nyilvánosan zajlanak).

Egységes szövetségi (és sok esetben állami) szabályozás hiányában, a téma különböző aspektusaiban csak lehetőségeket, lehetséges jogalapokat vizsgálok. A fejezet további részében megkísérlem az összes potenciális felelős, a visszaélések valamennyi, eltérő jogállású és cselekvőségű szereplője lehetséges polgári jogi felelősségének, illetve a felelősség alóli mentességének vizsgálatát. A fő kérdéskör tehát, hogy polgári jogi szempontból ki lehet felelős, illetve ki nem.

4.1. Az „elkövető” felelőssége

Ha szövetségi törvény vagy adott állam jogszabálya bünteti is a jogsértések elkövetőit magatartásukért; fontos, hogy emellett az áldozatnak lehetősége legyen kárigényét érvényesíteni velük szemben. A generált tartalmak vonatkozásában elkövető megnevezés alatt elsősorban ezen mesterségesen előállított felvételek készítői, terjesztői értendők.

Az Egyesült Államokban jelenleg nincsen olyan jogszabály föderális szinten, amely kifejezetten ezen szereplőkkel; vagyis az MI felhasználásával készített szexuális ábrázolások

⁶¹ Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

készítőivel, terjesztőivel szemben biztosítana polgári per indításához jogalapot a sérelmet szenvedett fél számára.

Ebből adódóan az elkövetővel szemben potenciálisan alkalmazható keresetindítási alapok vizsgálata során egyéb esetlegesen alkalmazható szövetségi és állami szinten meghozott jogszabályi rendelkezések mellett megvizsgáltam a *Restatement*-eket, kutatásomhoz pedig a *Restatement (Second) of Torts* című kötetet vettem alapul.

Ezúton megjegyezném, hogy habár a *Restatement*-ek nem minősülnek jogszabálynak (így nem is kötelező erejűek), illetve nem is a precedensrendszer részei; mégis nagy jelentőséggel bírnak. A korpulens kötetek olyan, a bírósági joggyakorlat harmonizációját célzó (és arra ható), tudományos testületek által kidolgozott és az *American Law Institute* által kiadott művek, amelyek a jogalkalmazók, a bíróságok által sűrűn hivatkozott forrásként tarthatók számon. Döntéseikhez a bíróságok gyakran (de erre való kötelezettség nélkül) figyelembe veszik ezeket.⁶² Tehát jelentőségük az amerikai jogrendszer vonatkozásában nem vonható kétségbe.⁶³

Az egységes szabályozás hiányának következtében dolgozatom során ún. kutatási nívumként, újszerű megoldást alkalmaztam az elkövetők lehetséges felelősségi alakzatainak vizsgálatára. Egyrészt kitérek a szerződésen kívüli károkozás (*tort*) potenciálisan alkalmazható jogcímeire, amelyekhez a *Second Restatement of Torts*-ot vettem alapul. Másrészt az MI-technológia szabályozásában fejlettebb államokban, tagállami szinten szabályozott, MI-specifikus keresetindítási alapokat vizsgálom, továbbá a U.S. Code lehetséges, elvileg alkalmazható rendelkezéseit.

⁶² Lásd s.n. Cornell Law School, Legal Information Institute: Wex Legal Dictionary – Restatement of the Law (https://www.law.cornell.edu/wex/restatement_of_the_law). Restatement (Second) of the Law: §708-End - Introduction. American Law Institute: St. Paul, Minn. (1979).

⁶³ Technikai megjegyzésként azt tudom megemlíteni, hogy a Restatement kötetek beszerzése jó néhány hetet vett igénybe könyvtárközi kölcsönzéssel is, mivel nagyon kevés helyén érhetőek el – illetve bocsátják rendelkezésre azokat – Európai szinten. A köteteket Berlinből, az egykori „Preußische Staatsbibliothek zu Berlin” állományából kaptuk meg.

4.1.1. A deliktuális, szerződésen kívüli károkozás lehetséges jogcímei (tort law)

Az említett MI-specifikus, egységes kereseti alap hiánya miatt a különböző, esetlegesen alkalmazható jogcímek vizsgálatára szorítkozom. Ennek keretein belül vizsgálom a szerződésen kívüli károkozás (*tort law*) egyes kereseti alapjait. Jóllehet a bíróságok sok esetben nem adnak helyt az online térben megvalósított szerződésen kívüli károkozásra hivatkozó kereseteknek,⁶⁴ mégis jelen esetben érdemes ezek vizsgálata, mert a New Jersey Állambeli ügy kapcsán indított polgári perben is részben ezek szolgáltak hivatkozási alapul.⁶⁵

4.1.1.1. Becsületsértési kereset

Becsületsértés megállapíthatóságához a *Restatement (Second) of Torts* alapján szükséges egy hamis, becsületsértő állítás közzététele az érintett személyre vonatkozóan, harmadik személy számára elérhető módon, amely vonatkozásában a sértő személy legalább hanyagsággal / gondatlanul járt el, és az állítás vagy önmagában peresíthető vagy különleges kár származik annak nyilvánosságra hozatalából.⁶⁶ Ez utóbbi feltételnél a generált explicit tartalmak vonatkozásában a különleges sérelem sok esetben helytálló lehetne, hiszen szexuális jellegű felvételek (hiába mesterségesen előállítottak) kerülnek ki az érintettekről az online térbe, és azt onnan nem lehet eltávolítani (lásd a „right to be forgotten”, az „elfeledtetési jog” említett lehetetlensége). De ezt sem szükséges bizonyítani a közzétett felvételek esetén, mivel a tartalmak publikálása (harmadik személy vagy személyek számára hozzáférhetővé tétele) önmagában is peresíthetővé teszi („*actionable per se*”) a cselekményt.⁶⁷ Ez alapján, aki becsületsértő tartalmat hamisan közzétesz olyan formában, hogy írásbeli becsületsértésnek („*libel*”) minősül, speciális sérelem eredményezése nélkül is felelősséggel tartozik.

⁶⁴ Tenzer, Garfield Leslie Y. Social media harms and the common law. Brooklyn Law Review, 88 /1 (2022) 242, 245–248.

⁶⁵ Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

⁶⁶ Restatement (Second) of Torts §558. American Law Institute: St. Paul, Minn. (1977). Lásd továbbá Tshimbalanga, Sydney: Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography. Tulane Journal of Technology and Intellectual Property, 26 (2024) 150.

⁶⁷ Restatement (Second) of Torts §569, §577. American Law Institute: St. Paul, Minn. (1977).

Az állítás ezen kontextusban nem kifejezetten egy szóbeli vagy írásbeli kijelentésre utal, hanem az angol szaknyelvben „*defamatory communication*”-ként meghatározott kifejezés, vagyis a hírnevet sértő, valamilyen módon való megjelenítése egy másik személynek.

A generált tartalmak szempontjából az írásbeli formájának („libel”) vizsgálata releváns. A *Restatement (Second) of Torts* szerint ehhez szükséges valamely hamis, akár írásbeli, akár kép általi, vagy egyéb módon a személyt megjelenítő publikálás, amely őt gyűlöletnek, megvetésnek teszi ki, hírnevét sérti.⁶⁸ Mivel képi formában is megvalósítható, így a becsületsértés egyéb feltételek teljesülése esetén alkalmas lehet a generált tartalmakból, deepfake-ekből eredő károk megtérítésére irányuló polgári per megindításához.

Mivel önmagában nem a generált tartalmak készítésére, terjesztésére nyújt megoldást, hanem az áldozat hírnevében esett sérelmet hivatott kompenzálni, teljeskörűen alkalmazható jogalapként semmiképpen nem tud szolgálni. Viszont a feltételek teljesülése esetén bizonyos mértékben megoldást nyújthat a generált tartalmakból következő sérelmek és károk megtérítésére. Bár ezen jogcímre hivatkozás esetleges hátránya lehet, hogy az online térben történt becsületsértés miatt indított polgári pereket sok esetben az alperesnek kedvezően bírálják el, a közösségi médiát megelőző precedensek alkalmazása miatt.⁶⁹

4.1.1.2. Érzelmi sérelem szándékos okozása (IIED)

Az érzelmi sérelem szándékos okozása (IIED, azaz „*intentional infliction of emotional distress*”) jelenleg az egyik legmegfelelőbb jogalap lehet, hiszen az említett online visszaélések mindegyikéről elmondható, hogy egyik legjelentősebb aspektusuk, hogy az áldozat számára (sok esetben kizárólag, vagy a perléskor egyelőre kizárólag) érzelmi sérelmet okoznak. A *Restatement (Second) of Torts* szerint, aki másnak extrém és súlyos magatartással szándékosan jelentős érzelmi sérelmet okoz, ezért felelősséggel tartozik.⁷⁰

⁶⁸ Restatement (Second) of Torts §568. American Law Institute: St. Paul, Minn. (1977). Tshimbalanga, Sydney: Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography. Tulane Journal of Technology and Intellectual Property, 26 (2024) 150.

⁶⁹ Tenzer, Garfield Leslie Y. Social media harms and the common law. Brooklyn Law Review, 88 /1 (2022) 247–248.

⁷⁰ Restatement (Second) of Torts 46.§. American Law Institute (1965). Lásd továbbá Tshimbalanga (2024) 147. Perry, Ronen: Civil Liability for Cyberbullying. UC Irvine Law Review (2020) 1228.

Természetesen ennek is megvan a maga nehézsége, mivel az elkövető szándékát bizonyítani szükséges,⁷¹ amely miatt ez sem teljesen hiánypótló hivatkozási alap a generált tartalmakból eredő kártérítési perek esetében. Habár az IIED leginkább kiegészítő, szubszidiárius jogalapként van számon tartva,⁷² az érzelmi sérelem megtérítésének vonatkozásában a szerződésen kívüli károkozások között mégis ez lehet az egyik legmegfelelőbb. Ennek ellenére mindenképp hangsúlyozandó, hogy a perindítási lehetőséget szintén nem az explicit tartalom terjesztése, generálása miatt biztosítja, hanem az ezzel okozott érzelmi sérelemből fakadóan.

4.1.1.3. A magánélet megsértése

A személyiségjegyek felhasználásával és magánjellegű tényeket sértő módon generált tartalmak vonatkozásában vizsgálható jogalap a magánélet megsértése. Ennek elemzéséhez ugyancsak a *Restatement (Second) of Torts*-ot vettem alapul.

Hivatkozási alapként szolgálhat azon típusa, amelyben a személy elvonultsága kerül megsértésre. Ez alapján, aki szándékosan, akár fizikailag, akár más értelemben megsérti más személy (vagy annak személyes ügyei) „elvonultságát” (seclusion, „*intrusion upon seclusion*”), ha ez egy átlagember számára is rendkívül sértő lenne, felelősséggel tartozik a személyes elvonultság sérelméért.⁷³

Alkalmazható lehet továbbá a magánélet megsértésének egy másik, a személyiség jogok (hang és képmás) felhasználásának kizárólagosságához fűződő alakzata. A *Restatement (Second) of Torts* alapján, aki saját előnyére felhasználja más személy nevét vagy képmását, felelőssé tehető az érintett személyiségi jogainak megsértéséért.⁷⁴ Ez a jogalap potenciálisan alkalmas lehet mindazon helyzetekben, amikor a generált tartalmak, illetve deepfake-ek előállítása során a készítő egy kiskorú képének megváltoztatásával vagy arcának alapul vételével hoz létre tartalmat, amelyet azt követően saját előnyére felhasznál. Habár ez felhasználás alapvetően nem

⁷¹ Tshimbalanga, Sydney: Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography. Tulane Journal of Technology and Intellectual Property, 26 (2024) 147–148.

⁷² Perry, Ronen: Civil Liability for Cyberbullying. UC Irvine Law Review (2020) 1229.

⁷³ Restatement (Second) of Torts §652B. American Law Institute (1977). Lásd továbbá Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

⁷⁴ Restatement (Second) of Torts §652C. American Law Institute (1977).

korlátozódik kereskedelmi célú használatra, vannak államok, ahol kizárólag ezen kategóriára szűkítették.⁷⁵

Ezen túlmenően potenciálisan alkalmas jogcím lehet a magánjellegű (magánéletet érintő) tények nyilvánosságra hozatala („*publicity given to private life*”). A *Restatement (Second) of Torts* alapján, aki nyilvánosságra hoz más személy magánéletét érintő tényeket, felelősségre vonható a másik magánéletének megsértéséért, ha a közzétett tartalom egy átlagember számára is jelentősen sértő lenne és nem szolgálja a közérdeket.⁷⁶

A magánélet megsértése tehát a generált tartalmak szexuális jellege tekintetében nem nyújthat kimerítő megoldást, viszont a képmás felhasználása, a magánügyek sérelme és egyéb vonásai miatt potenciálisan alkalmazható lehet a sérelmet szenvedett fél mint felperes számára.

4.1.1.4. A „right of publicity”

A „right of publicity” lényegében a magánélet megsértése személyiségjegyek védelméhez fűződő alkategóriájának leszűkítése, annak állami szintén történő korlátozása kereskedelmi célú felhasználásra. Ez nem szövetségi szinten bevett jogalap (ehelyett ugyanezen célra használható a személyiségi jogok megsértése), de számos államban lehetséges ez alapján keresetet benyújtani.⁷⁷

A „right of publicity” olyan szellemi tulajdonjog, amely kereskedelmi haszonszerzéssel összefüggő visszaélésekkel szemben alkalmazható a személy nevének, képmásának, hangjának, illetve egyéb egyedi megkülönböztető jegyeinek vonatkozásában.⁷⁸

⁷⁵ Restatement (Second) of Torts §652C. American Law Institute (1977).

⁷⁶ Restatement (Second) of Torts §652D. American Law Institute (1977). Lásd továbbá Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

⁷⁷ International Trademark Association, Resources: Right of Publicity. Bondy, Meeka – Delaney, John – Ong, Jeff: AI-Generated Deepfakes and the Emerging Legal Landscape. Perkins Coie (2024). (<https://www.ageofdisruptionblog.com/2024/04/ai-generated-deepfakes-and-the-emerging-legal-landscape/>). s.n. Cornell Law School, Legal Information Institute: Wex Legal Dictionary - publicity. (<https://www.law.cornell.edu/wex/publicity>)

⁷⁸ Uo.

Így ez szintén egy általánosabb jellegű védelmet nyújthat a személyiségi jogok sérelmére, nem pedig kifejezetten a szexuális jellegű, beleegyezés nélkül generált tartalmakat illetően enged kártérítésért folyamodást. Természetesen ennek alkalmazhatósági köre a kereskedelmi cél miatt jelentősen korlátozott, de nem kizárt ilyen esetek előfordulása sem.⁷⁹

4.1.2. Illinois Állam

Illinois Államban egy 2023-ban elfogadott jogszabály a *Civil Remedies for Nonconsensual Dissemination of Private Sexual Images Act* módosításával határozott meg jogalapot a generált szexuális tartalmak károsultjai számára.⁸⁰ Meghatározza a digitálisan módosított szexuális felvétel fogalmát, amely magában foglal minden olyan vizuális ábrázolást, amelyet úgy készítettek vagy módosítottak, hogy egy átlagember számára valóságosnak tűnjön a személy megjelenítése vagy az illusztrált magatartás.⁸¹ Polgári keresetindítási alapot biztosít azon (egy átlagember számára) felismerhetően ábrázolt személyek számára, akik sérelmet szenvednek el digitálisan beleegyezés nélkül módosított szexuális felvétel szándékos terjesztéséből vagy azzal való fenyegetésből.⁸² A kártérítés mértékének meghatározásánál a törvény külön megnevezi az érzelmi sérelem elszenvedését is.⁸³

4.1.3. Kalifornia Állam

Kalifornia Államban 2019-ben elfogadtak egy jogszabályt (Assembly Bill No. 602), amely nem említi kifejezetten a generatív tartalmakat, a deepfake-eket, de alkalmazható lehet ezek vonatkozásában.⁸⁴ A Civil Code módosításával, új szakasz beillesztésével, biztosít jogalapot a készítővel és terjesztővel szemben. Az ábrázolt egyén, digitalizálás és szexuálisan explicit tartalom fogalommeghatározásokban jelenik meg a generált tartalom alkalmazhatósága.⁸⁵ Az

⁷⁹ Citron, Danielle K. – Chesney, Robert: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review* 107 (2019) 1753, 1794.

⁸⁰ Illinois Public Act 103-0294.

⁸¹ Remedies for Nonconsensual Dissemination of Private Sexual Images Act (740 ILCS 190/5) Sec.5.

⁸² Uo. 740 ILCS 190/10 Sec. 10.

⁸³ Uo. 740 ILCS 190/25 Sec. 25.

⁸⁴ California Civil Code – § 1708.86.

⁸⁵ Uo. (a)

ábrázolt személy keresetét indíthat az ellen, aki a nem-beleegyezés, szexuálisan explicit tartalmat készíti és szándékosan közzéteszi.⁸⁶ Továbbá a nem készítő, terjesztő ellen is keresettel fordulhat, aki a felvétel hozzájárulás nélküli voltáról tudott, vagy tudnia kellett.⁸⁷

4.1.4. Florida Állam

Florida Államban egy 2022-ben hatályba egy lépett jogszabály, amely a büntetőjogi rendelkezések között biztosít polgári jogalapot a nem beleegyezés generált explicit tartalmak károsultjai számára.⁸⁸ A sérelmet szenvedett félnek keresetindítási alapot biztosít az ellen, aki szándékosan hozzájárul valamilyen formában (így kiterjedhet készítőre, terjesztőre is) a módosított szexuális ábrázoláshoz, és tud vagy tudnia kellene annak ilyen voltáról.⁸⁹ A generált tartalmakra alkalmazhatósága a módosított szexuális ábrázolás definíciójából tűnik ki, amely bármilyen formában digitálisan, elektronikus úton vagy egyéb formában módosított, átalakított felvételre kiterjed; amely valósághűen jelenít meg más felismerhető személyt.⁹⁰

4.1.5. A United States Code rendelkezései

A szövetségi szinten jelenleg hatályos jogszabályok közül viszonylag szűk kör, a U.S. Code egyes rendelkezései szolgálhatnak potenciálisan alkalmas jogalapként a generált tartalmak készítőivel és terjesztőivel szemben.

Esetlegesen alkalmazható lehet ezek közül a 15. címének 6851. szakasza, amely polgári keresetindítási alapot biztosít az engedély nélkül közzétett intim ábrázoláson megjelenített

⁸⁶ California Civil Code – § 1708.86. (b). Lásd továbbá Bondy, Meeka – Delaney, John – Ong, Jeff: AI-Generated Deepfakes and the Emerging Legal Landscape. Perkins Coie (2024). (<https://www.ageofdisruptionblog.com/2024/04/ai-generated-deepfakes-and-the-emerging-legal-landscape/>)

⁸⁷ Uo.

⁸⁸ The 2024 Florida Statutes: Title XLVI. Chapter 836. – § 836.13. Lásd továbbá Bondy – Delaney – Ong (2024).

⁸⁹ Uo. (2), (5).

⁹⁰ Uo. (1).

személy számára azzal szemben, aki az ábrázolást úgy tette közzé, hogy egyenes vagy eshetőlegesen szándékkal figyelmen kívül hagyta annak nem-konszenzusos voltát.⁹¹

A U.S. Code 18. címének 2252. szakasza szerint polgári jogi kereset indítható azzal szemben, aki számítógép segítségével vagy egyéb módon, tudatosan olyan gyermekpornográfiát készít, amely felismerhető kiskorú képmásának felhasználásával, módosításával készült.⁹² Alkalmazhatóságára utal a U.S. Code ezen fejezetében található fogalom-meghatározásoknál a gyermekpornográfia meghatározása. Eszerint e körbe tartozik minden vizuális ábrázolás, amelybe beleértik a számítógépesen generált tartalmakat is.⁹³

Természetesen ezek esetében bírói értelmezés kérdése az MI-generált képekre való alkalmazhatósága, illetve egyedileg a tartalmak jellege is befolyásoló tényező lehet, viszont a New Jersey eset kapcsán folyamatban levő (anonimizált) ügyben mindkét rendelkezést hivatkozási alapként használták.⁹⁴

4.2. Az elkövető kiskorúsága esetén a törvényes képviselők felelőssége

A szülők, törvényes képviselők kárfelelősségének kérdése természetesen nem MI-specifikus probléma. A legtöbb, online térben megvalósított károkozás esetén azonos sémát lehet követni. A következő gondolatokról is ugyanez mondható el: azok általánosságban érvényesek az internetes sérelmekre.

A felelősségre vonás ezen lehetősége abból a szempontból is korlátozott, hogy az „elkövető”, vagyis a készítő, illetve a terjesztő személye itt – a szülői felelősség felmerülése folytán szükségképpen – a kiskorúakra szűkül. Az elkövető kiskorúsága mint tényállási elem előfordulása sajnálatosan gyakori az eddig megvalósult esetek körében. Ennek a felelősségi iránynak a rövid bemutatása tehát ugyancsak indokolt.

⁹¹ 15 U.S. Code § 6851 – Civil action relating to disclosure of intimate images (b). Lásd továbbá Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

⁹² 18 U.S. Code § 2252A – Certain activities relating to material constituting or containing child pornography (a) (7), (f). Lásd továbbá Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

⁹³ 18 U.S. Code § 2256 – Definitions for chapter (8).

⁹⁴ Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)

A szülők (gondnokok) felelőssége azokban az esetekben jöhet számításba, amikor a kiskorú sérelmére szintén vétőképtelen, azaz ugyanilyen korosztályú, vagy más (pl. mentális) okból önállóan felelősségre nem vonható személy valósítja meg a sérelemhez vezető magatartást.

A kiskorúság körében a szülők, törvényes képviselők felelősségre vonása két helyzetben lehetséges: közvetett (kiskorú gyermek károkozó cselekedete) és közvetlen (saját kötelezettség elmulasztása) felelősség fennállása esetén.

Bár az angolszász jogrendszerek, így az Egyesült Államok joga sem határoz meg általános jelleggel közvetett felelősséget a szülők vonatkozásában a gyermekeik által elkövetett jogsértésekért, bizonyos esetekben ez mégis lehetséges.⁹⁵ A sporadikus, már-már kazuisztikus szabályozás államonként és egyes törvények vonatkozásában is differenciált. A vegyes jogrendszerű Louisiana Államban például általános a szülők közvetett felelőssége,⁹⁶ de a legtöbb államban csak korlátok között rendelkeznek a törvényes képviselők ezen felelősségi formájáról.⁹⁷ Kalifornia Állam esetében a szabályozás a kártérítés összegének mértékére korlátozott.⁹⁸ A szülővel szemben jogalapként a saját mulasztásából fakadó közvetlen felelősségére is lehet hivatkozni.⁹⁹ Bár ennek megfelelő bizonyítása szükséges, de a kiskorú által generált tartalmak vonatkozásában (akárcsak általánosságban az online jogsértések esetében) a megfelelő felügyelet elmulasztása alapozhatja ezt meg.¹⁰⁰

Ennek rövid ismertetésére megfelelő a *Restatement Second of Torts*-ban meghatározott „szülői kötelezettség a gyermek magatartásának felügyeletére”. Eszerint a szülőnek kötelessége megfelelően gondoskodni a gyermeke felügyeletéről, különösen annak érdekében, hogy megakadályozza azt, hogy a gyermek másnak sérelmet okozzon.¹⁰¹

⁹⁵ Perry, Ronen: Civil Liability for Cyberbullying. UC Irvine Law Review (2020) 1235–1236.

⁹⁶ Louisiana Civil Code Title V. Article 2318. Lásd Perry (2020) 1236.

⁹⁷ Perry (2020) 1236. Buckner, Susan: Parental Liability. FindLaw (2023).

(<https://www.findlaw.com/family/parental-rights-and-liability/parental-liability.html>)

⁹⁸ California Civil Code §1714.1.

⁹⁹ Perry (2020) 1238.

¹⁰⁰ Butler, Des – Kift, Sally – Campbell, Marilyn: Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance? eLaw Journal, 16/1 (2009) 15.

¹⁰¹ Restatement (Second) of Torts. §316. American Law Institute: St. Paul, Minn. (1965).

Ennek érvényesüléséhez két feltétel teljesülése szükséges: (1) tudatában van annak vagy tudnia kellene arról, hogy képes a gyermek magatartását korlátozni, (2) tud vagy tudnia kellene az erre irányuló intézkedés megtételének szükségességéről és lehetőségéről.¹⁰²

4.3. Az iskola mint mulasztást megvalósító szereplő (diák áldozat és diák elkövető esetén)

A tankerületek, oktatási intézmények, tanárok felelősségének vizsgálatáról is ugyanaz mondható el, mint a szülők esetében. Az online jogsértések esetén az iskolával szembeni jogalap nagyjából azonos szempontok alapján vizsgálható, továbbá az elkövetők – és itt a jogsérelmet szenvedettek – köre is a korosztály alapján leszűkített. Ugyanis abban az esetben vizsgálható az iskola felelőssége, ha a diák sérelmére elkövetett jogsértés egy (vagy több) másik diák által lett megvalósítva.¹⁰³

Sok esetben történik a megbotránkoztató képek generálása kiskorúak között, ezen belül is olyan diákok közt, akik egy osztályba vagy egyazon iskolába járnak. Már több államban számos olyan eset történt, ahol adott iskola tanulói generáltak mesterséges intelligencia felhasználásával osztálytársaik hétköznapi fotóikból meztelen, szexuális tartalmú képeket.¹⁰⁴ A tankerületeknek jelenleg kihívást jelentenek a generatív MI-visszaélések és azok kezelése, nincsenek rá megfelelően felkészülve.¹⁰⁵

Habár szövetségi szinten nincs erre vonatkozó rendelkezés, minden államban törvény írja elő az iskolák számára, hogy határozzanak meg a diákok számára kötelezően betartandó irányelveket a zaklatásra, online zaklatásra és egyéb jogsértésekre vonatkozóan.¹⁰⁶ Példaként, Kalifornia Államban a Safe Place to Learn Act előírja irányelvek meghozatalának

¹⁰² Restatement (Second) of Torts. §316. American Law Institute: St. Paul, Minn. (1965).

¹⁰³ Lásd például a 2, 3. és 5. lábjegyzetben hivatkozott eseteket.

¹⁰⁴ Uo. Lásd továbbá Singer, Natasha: Teen Girls Confront an Epidemic of Deepfake Nudes in School. The New York Times (2024). (<https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html>)

¹⁰⁵ Uo.

¹⁰⁶ Patchin, J. W. – Hinduja, S.: Bullying Laws Across America. Cyberbullying Research Center. (2023). (<https://cyberbullying.org/bullying-laws>). Marcowitz-Bittont, Miriam – Sommer, Hillel: Remediating online shaming. Cardozo International & Comparative Law Review 5/2 (2022) 391.

szükségességét zaklatásra, bullyingra, cyberbullyingra.¹⁰⁷ Jóllehet ettől függetlenül nem kizárt, hogy az iskolák szabályzatában is legyenek rendelkezések a generált tartalmakkal való visszaélésekre vonatkozóan, ezeket a legtöbb állam törvényi szinten nem írja elő.

Az irányelvek megszegése esetén az iskolák megfelelő szankcióval sújthatják a diákokat:¹⁰⁸ szóba jöhet a diák elbocsátása, akárcsak a beverly hills-i ügy esetében,¹⁰⁹ ahol a tankerület határozottan fellépett a diákok közti, generált szexuális tartalmak készítése és terjesztése ellen.¹¹⁰ Viszont kifejezetten a mesterséges intelligencia felhasználásával elkövetett visszaélések, jogsértések vonatkozásában még nem minden tankerületben fogalmaztak meg irányelveket.¹¹¹ A szabályzatban megfogalmazott elvektől függetlenül az iskola köteles jelenteni a potenciális gyermekbántalmazásokat, ezen belül a CSAM-et is.¹¹²

Az iskola jogi felelőssége esetén legvalószínűbb a saját mulasztáson alapuló közvetlen felelősség alkalmazhatósága.¹¹³ Ennek alapja az oktatási intézmények azon kötelezettsége, hogy megfelelően felügyeljék a diákokat és azok tevékenységét.¹¹⁴ Ez a kötelesség viszont térben általában az iskola területére korlátozódik.¹¹⁵ Ugyanez mondható el például Kaliforniában, ahol az Education Code arról rendelkezik, hogy sem a tankerület, sem az iskola munkatársai nem tartoznak felelősséggel a diákok iskolán kívüli tevékenységéért, biztonságáért.¹¹⁶

¹⁰⁷ California Education Code: Safe Place to Learn Act.

¹⁰⁸ Klein, Alyson: What a Proposed Ban on AI-Assisted 'DeepFakes' Would Mean for Cyberbullying. Education Week (2024). (<https://www.edweek.org/policy-politics/what-a-proposed-ban-on-ai-assisted-deep-fakes-would-mean-for-cyberbullying/2024/01>). Patchin, J. W. – Hinduja, S.: Bullying Laws Across America. Cyberbullying Research Center. (2023). (<https://cyberbullying.org/bullying-laws>).

¹⁰⁹ Healey, Jon: Scandal over AI-generated nudes at Beverly Hills middle school exposes gaps in law. Los Angeles Times (2024). (<https://www.latimes.com/california/story/2024-03-03/scandal-over-ai-generated-nudes-at-beverly-hills-middle-school-highlights-gaps-in-law>).

¹¹⁰ Singer, Natasha: Teen Girls Confront an Epidemic of Deepfake Nudes in School. The New York Times (2024). (<https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html>)

¹¹¹ Uo.

¹¹² Uo.

¹¹³ Perry, Ronen: Civil Liability for Cyberbullying. UC Irvine Law Review (2020) 1240.

¹¹⁴ Uo.

¹¹⁵ Uo.

¹¹⁶ California Education Code – § 44808

Szövetségi törvények alapján lehetőség van még bizonyos többletfeltételek teljesülése esetén további jogalapon is perelni az iskolát. Ilyen többletfeltétel például az, hogy a zaklatás a diák alkotmányos jogait is sértette, így különösen diszkriminatív megkülönböztetés áldozatává vált.¹¹⁷ Így ez a jogalap nem feltétlenül alkalmas általános jelleggel a generált explicit tartalmakra.

Mivel az online generálás, az internetes közegben való terjesztés vonatkozásában az iskoláknak, a tanároknak valóban nem feltétlen lehet ráhatása a cselekmény megvalósítására, illetve annak elkerülésére, de mindennek az iskolában is tapasztalható, tetten érhető (iskolai IP-cím / wifi-használat) vonatkozásaira már kiterjedhet a felügyeleti kötelezettség, s így annak elmulasztása jogalapot teremthet. Leginkább azokban az esetekben merülhet fel a potenciális felelősség kérdése, amikor az iskola már tud az esetről, de nem tesz meg a szükséges lépéseket, nem intézkedik a diákokkal szemben, nem tájékoztatják a szülőket, nem jelentik a hatóságoknak.

4.4. Az online platformok, a Communications Decency Act nyújtotta mentesség

Az online platformok tárgyalása során különböző internetes és közösségi média oldalak potenciális felelősségre vonását vizsgálom, a mesterséges intelligencia szoftvereket működtető platformokról külön lesz szó.

Nincs sem szövetségi, sem állami törvény, amely kötelezné a platformokat a felületeiken közzétett káros bejegyzés eltávolítására,¹¹⁸ a megosztott tartalom szűrésére, ellenőrzésére.¹¹⁹ Ezt teljes mértékben önszabályozás keretein belül végzik.¹²⁰ Így ez vonatkozik a különböző online oldalakon publikált generált szexuális explicit tartalmakra, deepfake-ekre is.¹²¹

¹¹⁷ Perry, Ronen: Civil Liability for Cyberbullying. UC Irvine Law Review (2020) 1240–1244.

¹¹⁸ Marcowitz-Bittont, Miriam – Sommer, Hillel: Remediating online shaming. Cardozo International & Comparative Law Review 5/2 (2022) 383; Citron, Danielle K. – Chesney, Robert: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review 107 (2019) 1798.

¹¹⁹ Citron – Chesney (2019) 1795–1797.

¹²⁰ Marcowitz-Bittont – Sommer (2022) 400–405.

¹²¹ Citron – Chesney (2019) 1798.

A legtöbb, kiskorúakat érő online jogsértés esetén felmerülhet, hogy a szülő szeretné a platformot perelni kártérítésért, ám jelenleg az Egyesült Államokban szinte lehetetlen polgári pert indítani velük szemben.¹²² Pedig a perindítás lehetősége sok más tényező miatt is szükségesnek tűnik; megemlítve itt az anonim tartalom-közzététel lehetőségét, amelyből következik, hogy sok esetben az elkövetővel szemben a kártérítésért folyamodás eleve kizárt.¹²³

Jelenleg a platformok felelősségre vonása az említett visszaélések kapcsán nem lehetséges, ugyanis a Communications Decency Act (CDA) 230. szakasza mentességet biztosít minden internetes szolgáltatónak a polgári jogi felelősségre vonás alól, a felületeiken közzétett tartalmak vonatkozásában.¹²⁴ A CDA alapján ugyanis az internetes szolgáltatásokat biztosító felületek nem kezelhetők a más publikálótól származó információ vonatkozásában, annak közzétevőjeként.¹²⁵ Az önmagában is széleskörű védelmet biztosító rendelkezést ráadásul a bíróságok is kiterjesztően értelmezik.¹²⁶ Ebből az következik, hogy jelenleg a közösségi médiaoldalak hipotetikus felelősségéről csak abban az esetben beszélhetünk, ha feltételezzük, hogy ez a szakasz törvényhozás, törvénymódosítás, vagy lerontó precedens, bírói értelmezés által módosításra kerülne.¹²⁷

Az említett jogszabályi kötelezettség hiánya ellenére, önszabályozás keretein belül, a legtöbb platform irányelveket tart fenn a közzétett káros tartalmak kezelésére.¹²⁸ Így ennek keretein belül törekedhetnek a generált explicit tartalmak eltávolítására, de ez nem garanciális és sok

¹²² Perry, Ronen: Civil Liability for Cyberbullying. UC Irvine Law Review (2020) 1245.

¹²³ Citron, Danielle K. – Chesney, Robert: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. 107 California Law Review 1753 (2019) 1795.

¹²⁴ 47 U.S.Code § 230: Protection for private blocking and screening of offensive material c). Lásd továbbá O'Donnell, Nicholas: Have We No Decency? Section 230 And The Liability of Social Media Companies For Deepfake Videos. University of Illinois Law Review 701 (2021). 712-713.

¹²⁵ 47 U.S.Code § 230: Protection for private blocking and screening of offensive material c).

¹²⁶ Cyphert, Amy B. – Martin, Jena T.: "A Change is Gonna Come:" Developing a Liability Framework for Social Media Algorithmic Amplification, UC Irvine Law Review 13 /1 (2022) 171; O'Donnell (2021) 713. Citron – Chesney (2019) 1796.

¹²⁷ Cyphert – Martin (2022) 179.

¹²⁸ Marcowitz-Bittont, Miriam – Sommer, Hillel: Remediating online shaming. Cardozo International & Comparative Law Review 5/2 (2022) 400–405; Citron – Chesney (2019) 1798.

esetben nem is elégséges.¹²⁹ A belső szabályzatokban a legtöbb platform alkalmaz életkori korlátozást a fióklétrehozásra, bejegyzésre, képernyőidőre, adatvédelmi beállításra.¹³⁰

A platformokat védő mentesség megszüntetése mellett érvel több kutató.¹³¹ Továbbá ezen immunitás leszűkítésére különböző elméletek is születtek.¹³² Számos tanulmányban vizsgálták már a perindítási lehetőség megnyílásával potenciálisan alkalmazható jogalapokat,¹³³ ezekre bővebben nem térek ki.

A mentesség megváltoztatására irányuló szövetségi törvényjavaslatokról, így ennek vonatkozásában az online platformok potenciális felelősségéről továbbiakban még lesz szó.

4.5. A mesterséges intelligencia: avagy a készítőik és fejlesztők mint potenciális felelősök

A platformokhoz hasonlóan, nincs törvényi kötelezettsége a képgeneráló szoftvereket működtető szolgáltatóknak sem arra, hogy milyen módon korlátozzák a generált tartalmak, deepfake-ek készítését; erről önszabályozás keretén belül döntenek.¹³⁴ Ebből következően nem kizárt az olyan modellek működése, amelyek lehetővé teszik szexuális explicit kimeneti adat generálását, sőt kifejezetten mesterséges meztelen képek készítésére létrejött generatív MI-rendszer is létezik.¹³⁵ Bár a mentesség a generatív MI-vállalatok esetében kevésbé egyértelmű, többen vitatják.¹³⁶ Jelenleg a CDA 230. szakaszában biztosított széleskörű mentesség az MI-

¹²⁹ Citron, Danielle K. – Chesney, Robert: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. 107 California Law Review 1753 (2019) 1798.

¹³⁰ Cao, Juncheng: Safeguarding children's privacy: study of regulation and practice in the United Kingdom and the United States. International Journal of Law, Ethics, and Technology (IJLET) Issue 1 (2023) 58.

¹³¹ Citron – Chesney (2019) 1799; O'Donnell, Nicholas: Have We No Decency? Section 230 And The Liability of Social Media Companies For Deepfake Videos. University of Illinois Law Review 701 (2021) 711.

¹³² O'Donnell (2021) 713-714. Citron – Chesney (2019) 1799.

¹³³ Cyphert, Amy B. – Martin, Jena T.: "A Change is Gonna Come:" Developing a Liability Framework for Social Media Algorithmic Amplification, UC Irvine Law Review 13 /1 (2022) 179-201.

¹³⁴ O'Donnell (2021) 715.

¹³⁵ Lásd példaként Jane Doe v K. G. 19-26.: ClothesOff

¹³⁶ Shaheen, Louis M.: Section 230's Immunity for Generative Artificial Intelligence (2023) 16.

rendszerek készítőit és fejlesztőit mint internetes szolgáltatókat is védi egy polgári perrel szemben.¹³⁷

Az MI-rendszerek vonatkozásában is számos, elvileg alkalmas felelősségre vonási elmélet, lehetőség felmerült már a mentesség megszüntetésére.¹³⁸ Az MI-modellek készítői, illetve fejlesztői az említett önszabályozás során speciális korlátozásokkal igyekeznek akadályozni a visszaélést.¹³⁹ Bár tudnának bizonyos korlátokat adaptálni annak érdekében, hogy minél inkább megnehezítsék a szexuálisan explicit tartalmak generálását, a probléma akkor sem szűnne meg teljességgel,¹⁴⁰ így a jogorvoslat lehetősége mindenképpen szükséges.

5. A TÖRVÉNYJAVASLATOKRÓL: LÉPÉST TARTANI A MESTERSÉGES INTELLIGENCIÁVAL?

Jelenleg sem törvény, sem precedens nem biztosít konkrét, egységes kereseti alapot a generatív mesterséges intelligencia felhasználásával elkövetett sérelmek áldozatai számára. Az egységesség hiányának oka, hogy nem született még MI-specifikus szövetségi törvény és az államoknak is csak egy része rendelkezik ilyennel. Mindemellett a bíróságok sem terjesztették ki a korábbi precedensek elveit az újkeletű problémából eredő jogvitákra.¹⁴¹ A régebbi, nem közösségi média vonatkozású precedensek merev alkalmazása pedig nem szolgál elégséges megoldásként ezekre az ügyekre.¹⁴²

E helyzet megváltoztatása érdekében, a 2023-as és 2024-es évben is számos törvényjavaslat került benyújtásra a Kongresszushoz, amelyek a felelősségre vonás vonatkozásában változást,

¹³⁷ 47 U.S.Code § 230: Protection for private blocking and screening of offensive material f) (2)-(3). Lásd továbbá Shaheen (2023) 16, 23-33.

¹³⁸ Lásd például Henderson, Peter – Hashimoto, Tatsunori – Lemley, Mark: Where's the liability in harmful ai speech? Journal of Free Speech Law 3 /2 (2023) 626-635.

¹³⁹ De Guzman, Chad – Henshall, Will: As Tech CEOs Are Grilled Over Child Safety Online, AI Is Complicating the Issue. Time Magazin (2024). (<https://time.com/6590470/csam-ai-tech-ceos/>)

¹⁴⁰ Aronashvili, Reuven: The Evolution Of Sextortion Attacks: How Generative AI Is Taking A Front Seat. Forbes Technology Council (2024). (<https://www.forbes.com/councils/forbestechcouncil/2024/02/20/the-evolution-of-sextortion-attacks-how-generative-ai-is-taking-a-front-seat/>)

¹⁴¹ Tenzer, Garfield Leslie Y. Social media harms and the common law. Brooklyn Law Review, 88 /1 (2022) 227-228, 245.

¹⁴² Uo. 251–255.

a mentesség megszüntetését, illetve egyéb újításokat céloznak. A probléma kapcsán fontosnak tartom megvizsgálni a lehetséges megoldásokat, vagyis azon benyújtott törvényjavaslatokat, amelyek valamilyen változtatásról rendelkeznek a felelősségi irányokkal kapcsolatban.

5.1. A generált, szexuálisan explicit tartalmak készítői és terjesztői vonatkozásában

Az elkövetők, így a generált tartalmak készítőinek és terjesztőinek felelősségre vonását érinti a DEFIANCE Act, a Preventing Deepfakes of Intimate Images Act, a No AI FRAUD Act és a DEEPFAKES Accountability Act, melyek főbb rendelkezéseit a következőkben ismertetem.

5.1.1. A 2024. évi DEFIANCE Act

A Distrust Explicit Forged Images and Non-Consensual Edits (=DEFIANCE) Act of 2024 a nem beleegyezéses, szexuálisan explicit deepfake-ek (és generált tartalmak) készítőit, terjesztőit célozza.¹⁴³ A javaslat a U.S. Code 6851. szakaszát módosítaná. Habár a tervezet magát a deepfake kifejezést konkrétan nem tartalmazza, beemelné a törvénybe a digitális hamisítvány definícióját, melynek meghatározása egyértelművé teszi alkalmazhatóságát. Minden virtuális ábrázolásra alkalmazható, amelyet szoftver, gépi tanulási mechanizmus, mesterséges intelligencia használatával vagy egyéb számítógépesen-generált módon készítettek (beleértve képek módosítását, megváltoztatását is).¹⁴⁴

Polgári per megindításához biztosítana jogalapot a beleegyezés nélkül intim ábrázoláson megjelenített, felismerhető személy számára.¹⁴⁵ A keresetindítást lehetővé tenné a hozzájárulás nélkül terjesztővel szemben, aki a beleegyezés nemlétéről tudott, vagy annak eshetőségét figyelmen kívül hagyta.¹⁴⁶ Ezen túlmenően biztosítaná még a felvételt továbbítási szándékkal készítővel és birtoklóval szemben,¹⁴⁷ illetve az azt kérő személy vonatkozásában is, ha egyenes vagy eshetőleges szándékkal figyelmen kívül hagyta a felvétel nem-konszenzusos

¹⁴³ 118th Congress (2023-2024): S.3696 – DEFIANCE Act of 2024.

¹⁴⁴ Uo. Sec. 2. (a) (3).

¹⁴⁵ Uo. Sec. 2. (b).

¹⁴⁶ Uo. Sec. 2. (b) (i).

¹⁴⁷ Uo. Sec. 2. (b) (ii).

voltát.¹⁴⁸ Továbbá az ugyanezen feltételeknek megfelelő készítővel szemben jogalapot biztosítana a digitális hamisítványok alanyának.¹⁴⁹

Kiemelendő, hogy a javaslatot Szenátus már elfogadta és jelenleg a Képviselőház előtt zajlik az egyeztetés.¹⁵⁰ Ha ez a javaslat elfogadásra kerülne, mindenképpen előrelépést jelentene az elkövetővel szembeni perindítási lehetőségek vonatkozásában, az ezen kárfelelősségi irány esetében fennálló problémát akár meg is tudná oldani.

5.1.2. A 2023. évi Preventing Deepfakes of Intimate Images Act

A Preventing Deepfakes of Intimate Images Act szintén nem-konszenzusos, szexuálisan explicit, generált tartalmak és deepfake-ek esetére biztosítana a perindításhoz jogalapot.¹⁵¹ A törvényjavaslat a The Violence Against Women Act Reauthorization Act of 2022-t módosítaná.

A fogalommeghatározások között szintén nem tartalmazza kifejezetten a deepfake definícióját. Digitálisan készített, illetve módosított intim ábrázolásokat nevesít, a U.S. Code fogalmainak módosítása tekintetében.¹⁵² Ezek vonatkozásában biztosítana a keresetindítási alapot a javaslat, az ilyen közzétett tartalmakban beleegyezésük nélkül ábrázolt személyek számára a terjesztővel szemben.¹⁵³ Habár a terjesztőre vonatkozóan a felvételek nem beleegyezéses voltának tudatán kívül egyéb követelményt nem fogalmazna meg, a készítőről egyáltalán nem rendelkezik, aki szintén jelentős szereplője a generálással való visszaélésnek.

Kiemelendő még a tervezettel kapcsolatban, hogy a kártérítési összeg meghatározásánál a tényleges kár esetén külön megnevezi az okozott érzelmi sérelmet.¹⁵⁴

¹⁴⁸ 118th Congress (2023-2024): S.3696 – DEFIANCE Act of 2024. Sec. 2. (b) (ii).

¹⁴⁹ Uo. Sec. 2. (b) (iii).

¹⁵⁰ Congress.gov: All Actions: S.3696 – 118th Congress (2023-2024).

¹⁵¹ 118th Congress (2023-2024): H.R.3106 – Preventing Deepfakes of Intimate Images Act.

¹⁵² Uo. Sec. 1309A (a).

¹⁵³ Uo. (b).

¹⁵⁴ Uo. (d).

5.1.3. A 2024. évi No AI FRAUD Act

A No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act of 2024 (No AI FRAUD Act) a személyiségi jogok (képmás és hang) védelmét célozza.¹⁵⁵ A javaslat indokolásában nevesítik más esetek mellett a New Jersey állambeli középiskolás lányokról generált deepfake-ek ügyét.¹⁵⁶

A tervezet definiálja a digitális ábrázolás, az ún. „egyéniessett klónozó szolgáltatás” (*personalized cloning service*) és a digitális technológia fogalmakat, amelyekből kitűnik a törvényjavaslat alkalmazhatósága számítógépes szoftverrel, mesterséges intelligenciával, gépi tanulási mechanizmussal, hasonló technológiával készített és módosított ábrázolásokra.¹⁵⁷

Ez alapján bárki, aki más személy hang és képmáshoz való jogát sérti azáltal, hogy beleegyezése nélkül ezen jogokat érintő felvételt közzétesz, megoszt, nyilvánosságra hoz felelősséggel tartozik az okozott károkért.¹⁵⁸ Ez a törvény tehát jogalapot nyújt a károsultak számára, hogy a terjesztővel szemben kártérítésért folyamodjanak, viszont a készítőkkal kifejezetten nem foglalkozik.

A kár kapcsán kiemeli, hogy abba a súlyos érzelmi sérelem okozására is beletartozik.¹⁵⁹ Az előző tervezet esetében a súlyos kikötés nem szerepelt, így ez egy szűkebb kört fed le. Külön rendelkezik „önálló kárként” (*per se harm*) minden digitális ábrázolásról, amely magában foglal CSAM-et, szexuális explicit vagy intim képet jelenít meg.¹⁶⁰

A javaslat célja, hogy a digitális személyiség védelmének biztosításával megakadályozza a mesterséges intelligencia felhasználását zaklatásra, bullyingra, bántalmazásra.¹⁶¹

¹⁵⁵ 118th Congress (2023-2024): H.R.6943 – No AI FRAUD Act.

¹⁵⁶ Uo. Sec. 2. (3).

¹⁵⁷ Uo. Sec. 3. (a).

¹⁵⁸ Uo. Sec. 3. (b), (c), (d).

¹⁵⁹ Uo. Sec. 3. (e) (2).

¹⁶⁰ Uo. Sec 3. (e) (3).

¹⁶¹ s.n. Salazar Introduces The No AI FRAUD Act. (2024) (<https://salazar.house.gov/media/press-releases/salazar-introduces-no-ai-fraud-act>).

5.1.4. A 2023. évi DEEPFAKES Accountability Act

A Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 (DEEPFAKES Accountability Act) a U.S. Code-ot módosítaná, új szakaszok beillesztésével.¹⁶² A javaslat alapvetően a tartalmakra vonatkozóan határoz meg követelményeket a generatív MI és egyéb hasonló technológia felhasználásával készített vagy módosított felvétel ilyen voltának megjelölése kapcsán.¹⁶³ Sikeres betartatása esetén a generált tartalmak megkülönböztethetősége a valódi felvételektől biztosítva lenne.

A téma szempontjából leglényegesebb rendelkezése viszont, hogy keresetindítási alapot biztosít azon sérelmet szenvedett fél számára, aki valóságosnak tűnő deepfake-en hozzájárulása nélkül került ábrázolásra.¹⁶⁴ A generált tartalom szexuális jellege ezen jogszabálytervezetben csak a kártérítés mértékének meghatározása során kerül értékelésre.¹⁶⁵ A törvényjavaslat meghatározza továbbá a deepfake fogalmát.¹⁶⁶

5.2. A platformok felelősségre vonását és mentességük módosítását célzó törvényjavaslatok

Az online platformokat érinti a SAFE TECH Act és az EARN IT Act. Bár nem általános jelleggel rendelkeznek polgári keresetindítási alapról a generált tartalmak vonatkozásában, fontos röviden említést tenni róluk, mivel az internetes szolgáltatók védelmét biztosító mentesség szűkítésére kevés esetben került eddig sor.

5.2.1. SAFE TECH Act

A 2023. évi Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act (SAFE TECH Act) a mentességet biztosító Communications Decency Act 230.

¹⁶² 118th Congress (2023-2024): H.R.5586 – DEEPFAKES Accountability Act.

¹⁶³ Uo. §1041. (c), (d), (e).

¹⁶⁴ Uo. (g)

¹⁶⁵ Uo. (g) (2) (D)

¹⁶⁶ Uo. (n)

szakaszát módosítaná.¹⁶⁷ Kizáró eseteket fogalmaz meg, amelyekre a mentesség nem vonatkozik.¹⁶⁸ Jogsértés megszüntetésére irányuló kérelem esetén a mentesítést biztosító rendelkezés nem alkalmazandó, ha ez abból ered, hogy az internetes szolgáltató elmulasztotta eltávolítani, hozzáférhetőségét korlátozni vagy elterjesztését megelőzni az olyan tartalomnak, amely valószínűsíthetően helyrehozhatatlan kárt okoz.¹⁶⁹ Ennek értelmezése bírósági kérdéskör lenne, viszont az online térben megvalósított jogsértések (különösen a szexuális jellegűek) az internetes közeg miatt általánosságban vissza nem fordítható hatással járnak.

5.2.2. EARN IT Act

Az Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2023 (EARN IT Act) a gyermekek online térben történő szexuális kizsákmányolásának megelőzését célozza.¹⁷⁰ A törvényjavaslatban célként tűzték ki annak elérését, hogy az internetszolgáltatók is intézkedéseket fogjanak a gyermekek szexuális kizsákmányolásának megelőzése, kezelése, leküzdése érdekében, külön kiemelve a CSAM terjedését.¹⁷¹

A javaslat szintén módosítaná a Communications Decency Act 230. szakaszát. A mentesség alól kivételt jelentenének a U.S. Code 2555. szakasza alapján biztosított, a gyermekek szexuális kizsákmányolására vonatkozó polgári jogi keresetek, jogalapot szolgáltatva az internetes szolgáltatókkal szemben.¹⁷²

Emellett a tervezet módosítaná a U.S. Code egyes rendelkezéseit is: a 2252. szakaszban használt a gyermekpornográfia fogalmat a CSAM megnevezéssel helyettesítené,¹⁷³ így az ezen alapuló polgári perindítási lehetőség az áldozatok számára az elkövetővel szemben is alkalmas lehetne.

¹⁶⁷ 118th Congress (2023-2024): S.560 – SAFE TECH Act.

¹⁶⁸ Uo. Sec. 2. (3).

¹⁶⁹ 118th Congress (2023-2024): S.560 – SAFE TECH Act. Uo. (3) (A)

¹⁷⁰ 118th Congress (2023-2024): S.1207 – EARN IT Act of 2023.

¹⁷¹ Uo. Sec. 3. (b).

¹⁷² Uo. Sec. 5. (6).

¹⁷³ Uo. Sec. 6. (7).

6. KILÁTÁSOK, JAVASLATOK

6.1. Kilátások a változásra: Hogyan tovább?

Az amerikai közvélemény állása, illetve a közelmúltban történt közéleti események arra engednek következtetni, hogy változás fog bekövetkezni a jogi szabályozást illetően.

Valószínűsíthető a helyzet azon irányba történő fordulása, hogy a platformokat, illetve a mesterséges intelligenciát széles körben védő mentesség megszűnjék, de legalábbis korlátozódjék. Erre enged következtetni többek közt a Szenátus Igazságügyi Bizottsága által tartott meghallgatása a nagyobb platformok mögött álló technológiai cégek vezérigazgatóinak a gyermekekkel való szexuális visszaélések megelőzésére tett intézkedéseikkel kapcsolatban.¹⁷⁴ Kiemelendő ehhez kapcsolódóan az is, hogy a Kongresszus mindkét pártja egyetért a Communications Decency Act 230. szakaszának módosításának szükségességében.¹⁷⁵

Mindezeken kívül az is valószínűsíthető, hogy szövetségi törvény meghozatalát szorgalmazzák MI-specifikus szabályozásként. Erre lehet következtetni az ötven állam ügyészei által a Kongresszusnak írt levélből is, amelyben azt sürgetik, hogy tanulmányozzák a mesterséges intelligencia felhasználását a gyermekek kizsákmányolására, és kezdjék meg a jogalkotást az azzal szembeni védekezésre.¹⁷⁶

¹⁷⁴ De Guzman, Chad – Henshall, Will: As Tech CEOs Are Grilled Over Child Safety Online, AI Is Complicating the Issue. Time Magazin (2024). (<https://time.com/6590470/csam-ai-tech-ceos/>). U.S Senate Committee on the Judiciary: Preview: Senate Judiciary Committee to Press Big Tech CEOs on Failures to Protect Kids Online During Landmark Hearing Today (2024). (<https://www.judiciary.senate.gov/press/releases/preview-senate-judiciary-committee-to-press-big-tech-ceos-on-failures-to-protect-kids-online-during-landmark-hearing-today>)

¹⁷⁵ Cyphert, Amy B. – Martin, Jena T.: "A Change is Gonna Come:" Developing a Liability Framework for Social Media Algorithmic Amplification, UC Irvine Law Review 13 /1 (2022) 168–169.

¹⁷⁶ Kinnard, Meg: Prosecutors in all 50 states urge Congress to strengthen tools to fight AI child sexual abuse images (2023) (<https://apnews.com/article/ai-child-pornography-attorneys-general-bc7f9384d469b061d603d6ba9748f38a>)

6.2. Javaslat a megoldásra

Egy újszerű probléma újszerű megoldást igényel. A generált, szexuálisan explicit tartalmak kezelése egy olyan lépést tesz szükségessé, amelyre korábban csak kezdeményezések születtek: egy föderális szinten meghozott MI-központú jogszabály megalkotását.

Véleményem szerint az ideális megoldás az lenne, ha szövetségi szinten születne egy MI-specifikus törvény, amelynek középpontjában a generatív MI diszfunkciói, a visszaélések állnának. Kifejezetten a kiskorúak védelmét is céloznia kellene, erre külön hangsúlyt fektetve, és „*per se harm*”-ként kiemelt jogvédelemben részesítve a generált CSAM által okozott sérelmeket. Emellett célszerű volna, ha a jogszabály elsődlegesen a nem beleegyezéses, szexuálisan explicit, generált ábrázolásokra koncentrálna, keresetindítási alapot biztosítva a károsult félnek a generált tartalom készítőjével, illetve terjesztőjével szemben.

Ezen túlmenően a DEFIANCE Act-ből merítve, a meghatározott feltételek teljesülése esetén, a jogalapnak a fogadóval szembeni biztosítása is megfontolandó.

Továbbá mindenképp szükségesnek tartom a törvénybe egy olyan rendelkezéssor beiktatását, amely átfedően meghatározná a különböző, egységesen nem tisztázott fogalmakat (például deepfake, CSAM), avagy a már meglévőket kiterjesztené a generatív mesterséges intelligencia felhasználásával megvalósított visszaélésekre.

Szükségesnek látom, hogy a jogszabály szűkítse a platformok mentességét. Egyrészt kötelezettségként előírja platformok számára, hogy használjanak megfelelő, kellően alapos szűrő (akár algoritmikus alapon működtetett) rendszereket, amelyek észlelik és eltávolítják ezen generált tartalmakat. Másrészt pedig keresetindítási alapot kellene biztosítson az ennek elmulasztása okán sérelmet szenvedett félnek a platformmal szemben.

IRODALOMJEGYZÉK

1. Tanulmányok, monográfiák

- Butler, Des – Kift, Sally – Campbell, Marilyn: Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance? *eLaw Journal*, 16(1) (2009).
- Cao, Juncheng: Safeguarding children's privacy: study of regulation and practice in the united kingdom and the united states. *International Journal of Law, Ethics, and Technology (IJLET)*, 2023 /1 (2023). 56–84.
- Citron, Danielle K. – Chesney, Robert: Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *107 California Law Review* (2019). 1753–1819.
- Cyphert, Amy B. – Martin, Jena T.: "A Change is Gonna Come:" Developing a Liability Framework for Social Media Algorithmic Amplification, *UC Irvine Law Review* 13 /1 (2022). 155–204.
- Fineman, Melanie N.: Honey, monetized the kids: commercial sharenting and protecting the rights of consumers and the internet's child stars. *Georgetown Law Journal*, 111 /4 (2023). 847–890.
- Gieseke, Anne Pechenik: "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography *Vanderbilt Law Review*, 73(5) (2020). 1479–1516.
- Hallmark, Kirsten: Death by words: do united states statutes hold cyberbullies liable for their victims' suicide? *Houston Law Review* 60 /3 (2023). 727–756.
- Henderson, Peter – Hashimoto, Tatsunori – Lemley, Mark: Where's the liability in harmful ai speech? *Journal of Free Speech Law* 3 /2 (2023). 589–650.
- Ilin, Alexey: A New Cyberbullying Law? Extension of Legal Interpretations in China and Russia. *International Journal of Law, Ethics, and Technology* (2022). 56–86.
- Marcowitz-Bittont, Miriam – Sommer, Hillel: Remedying online shaming. *Cardozo International & Comparative Law Review* 5 /2 (2022). 375–414.
- O'Donell, Nicholas: Have We No Decency? Section 230 And The Liability of Social Media Companies For Deepfake Videos. *University of Illinois Law Review* (2021). 701–740.
- Perry, Ronen: Civil Liability for Cyberbullying. *UC Irvine Law Review* 10/4 (2020). 1219–1272.

Pongó, Tamás: A cyberbullying és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére. Iurisperitus Kiadó: Szeged (2021).

Shaheen, Louis M.: Section 230's Immunity for Generative Artificial Intelligence (2023).

Tenzer, Garfield Leslie Y.: Social media harms and the common law. Brooklyn Law Review, 88 /1 (2022). 227–274.

Thiel, David: Identifying and Eliminating CSAM in Generative ML Training Data and Models. Stanford Internet Observatory (2023).

Tshimbalanga, Sydney: Not-So-Sexy Side of Porn: Examining the Legal Void for Victims of Deepfake Pornography. Tulane Journal of Technology and Intellectual Property, 26 (2024). 135–158.

Szerző megjelölése nélkül (sine nomine):

s.n. Internet Watch Foundation: What has changed in the AI CSAM Landscape (2024).

2. Internetes források

Anderson, Monica – Faverio, Michelle – Gottfried, Jeffrey: Teens, Social Media and Technology 2023. Paw Research Center (2023).
(<https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/>)

Aronashvili, Reuven: The Evolution Of Sextortion Attacks: How Generative AI Is Taking A Front Seat. Forbes Technology Council (2024).
(<https://www.forbes.com/councils/forbestechcouncil/2024/02/20/the-evolution-of-sextortion-attacks-how-generative-ai-is-taking-a-front-seat/>)

Atherton, Daniel: Deepfakes and Child Safety: A Survey and Analysis of 2023 Incidents and Responses (2024). (<https://incidentdatabase.ai/blog/deepfakes-and-child-safety/>)

Atherton, Daniel: Incident 597: Students Traumatized as AI-Generated Fake Nudes Are Circulated at New Jersey High School. Artificial Intelligence Incident Database (2023). (<https://incidentdatabase.ai/cite/597/>)

Atherton, Daniel: Incident 617: Male student allegedly used AI to generate nude photos of female classmates at a high school in Issaquah, Washington. Artificial Intelligence Incident Database (2023). (<https://incidentdatabase.ai/cite/617/>)

Atherton, Daniel: Incident 605: North Carolina Psychiatrist Used Artificial Intelligence to Produce Images of Child Sex Abuse. Artificial Intelligence Incident Database (2021). (<https://incidentdatabase.ai/cite/605/>)

Bialos, Noah – Natasha Amlani, Natasha – Klein, Samuel: Generative AI: How Existing Regulation May Apply to AI-Generated Harmful Content. Perkins Coie (2023). (<https://www.perkinsonprivacy.com/2023/10/generative-ai-how-existing-regulation-may-apply-to-ai-generated-harmful-content/#more-3243>).

Bondy, Meeka – Delaney, John – Ong, Jeff: AI-Generated Deepfakes and the Emerging Legal Landscape. Perkins Coie (2024). (<https://www.ageofdisruptionblog.com/2024/04/ai-generated-deepfakes-and-the-emerging-legal-landscape/>).

Buckner, Susan: Parental Liability. FindLaw (2023). (<https://www.findlaw.com/family/parental-rights-and-liability/parental-liability.html>)

De Guzman, Chad – Henshall, Will: As Tech CEOs Are Grilled Over Child Safety Online, AI Is Complicating the Issue. Time Magazin (2024). (<https://time.com/6590470/csam-ai-tech-ceos/>)

Flachner, Balázs: Mesterséges intelligenciával generált Schwab Richárd-hamisítvány népszerűsít fura csodaszert az interneten. Telex (2024). (<https://telex.hu/techtud/2024/11/18/schwab-richard-deepfake-kamu-video>)

Healey, Jon: Scandal over AI-generated nudes at Beverly Hills middle school exposes gaps in law. Los Angeles Times (2024). (<https://www.latimes.com/california/story/2024-03-03/scandal-over-ai-generated-nudes-at-beverly-hills-middle-school-highlights-gaps-in-law>)

Kinnard, Meg: Prosecutors in all 50 states urge Congress to strengthen tools to fight AI child sexual abuse images (2023) (<https://apnews.com/article/ai-child-pornography-attorneys-general-bc7f9384d469b061d603d6ba9748f38a>)

Klein, Alyson: What a Proposed Ban on AI-Assisted ‘DeepFakes’ Would Mean for Cyberbullying. Education Week (2024). (<https://www.edweek.org/policy-politics/what-a-proposed-ban-on-ai-assisted-deep-fakes-would-mean-for-cyberbullying/2024/01>).

Korte, Lara: California launches new broadside against tech over harmful AI content. Politico (2024). (<https://www.politico.com/news/2024/01/16/california-ai-generated-child-sex-abuse-material-bill-00135786>)

O’Brien, Matt – Hadero Haleluya: AI-generated child sexual abuse images could flood the internet. Now there are calls for action. The Associated Press (2023). (<https://apnews.com/article/ai-artificial-intelligence-child-sexual-abuse-c8f17de56d41f05f55286eb6177138d2>)

O'Brien, Matt – Hadero Haleluya: AI image-generators are being trained on explicit photos of children, a study shows. The Associated Press (2023).

(<https://apnews.com/article/generative-ai-illegal-images-child-abuse-3081a81fa79e2a39b67c11201cfd085f>)

Patchin, J. W. – Hinduja, S.: h Across America. Cyberbullying Research Center (2023).

(<https://cyberbullying.org/bullying-laws>)

Saliba, Emmanuelle: Sharing photos of your kids? Maybe not after you watch this deepfake ad. Abc News (2023). (<https://abcnews.go.com/GMA/Family/sharing-photos-kids-after-watch-deepfake-ad/story?id=101730561>)

Singer, Natasha: Teen Girls Confront an Epidemic of Deepfake Nudes in School. The New York Times (2024). (<https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html>)

Vogels, Emilia A.: Teens and Cyberbullying 2022. Pew Research Center (2022).

(<https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/>)

Vogels, Emilia A.: The State of Online Harrasmen. Pew Research Center (2021).

(<https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/>)

Vogels, Emilia A. – Gelles-Watnick, Risa – Massarat, Navid: Teens, Social Media and Technology 2022. Paw Research Center (2022).

(<https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/>)

Zách, Dániel: Pár ezer forintnyi összegért akár kiskorú lányokról is lehet hamis meztelen képeket generálni egy deepfake-alkalmazással. Telex (2024).

(<https://telex.hu/techtud/2024/03/01/deepfake-spanyoloroszag-egyeseult-allamok-feheroroszorszag-bunugy-ai-mesterseges-intelligencia>)

Szerző megjelölése nélkül (sine nomine):

s.n. Applications of Artificial Intelligence Across Various Industries. Forbes (2023).

(<https://www.forbes.com/sites/qai/2023/01/06/applications-of-artificial-intelligence/>)

s.n. Cornell Law School, Legal Information Institute: Wex Legal Dictionary – publicity.

(<https://www.law.cornell.edu/wex/publicity>)

s.n. Cornell Law School, Legal Information Institute: Wex Legal Dictionary – Restatement of the Law (https://www.law.cornell.edu/wex/restatement_of_the_law)

- s.n. Definition of Deepfake from the Cambridge Advanced Learner's Dictionary And Thesaurus. Cambridge University Press).
- s.n. Definition of Sextortion from the Cambridge Advanced Learner's Dictionary And Thesaurus. Cambridge University Press).
- s.n. Deepfakes: How to Protect Your Kids. Canopy (2024).
(<https://canopy.us/2024/04/16/deepfakes-how-to-protect-your-kids/>)
- s.n. International Trademark Association, Resources: Right of Publicity.
- s.n. Interstate Commission for Juveniles: Age Matrix. (<https://juvenilecompact.org/age-matrix>)
- s.n. Ma hatályba lép az EU AI Act: új korszak a mesterséges intelligencia szabályozásában. Jogászvilág (2024). (<https://jogaszvilag.hu/a-jovo-jogasza/ma-hatalyba-lep-az-eu-ai-act-uj-korszak-a-mesterseges-intelligencia-szabalyozasaban/>)
- s. n. National Center for Missing and Exploited Children: Child Sexual Abuse Material (<https://www.missingkids.org/theissues/csam>)
- s. n. National Center for Missing and Exploited Children: Cybertipline 2023 Report (<https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata#files>)
- s.n. National Center for Missing and Exploited Children. Sextortion.
(<https://www.missingkids.org/theissues/sextortion>).
- s.n. Salazar Introduces The No AI FRAUD Act. (2024).
(<https://salazar.house.gov/media/press-releases/salazar-introduces-no-ai-fraud-act>)
- s.n. U.S Senate Committee on the Judiciary: Preview: Senate Judiciary Committee to Press Big Tech CEOs on Failures to Protect Kids Online During Landmark Hearing Today (2024). (<https://www.judiciary.senate.gov/press/releases/preview-senate-judiciary-committee-to-press-big-tech-ceos-on-failures-to-protect-kids-online-during-landmark-hearing-today>)

3. Jogszabályok, törvényjavaslatok, esetek stb.

Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete

California Civil Code § 1708.86.

California Civil Code § 1714.1.

California Education Code: Safe Place to Learn Act

California Education Code § 44808

Illinois Public Act 103-0294.

Louisiana Civil Code § 2318.

The 2024 Florida Statutes: § 836.13

15 U.S. Code § 6851: Civil action relating to disclosure of intimate images

18 U.S. Code § 2252A: Certain activities relating to material constituting or containing child pornography

47 U.S. Code § 230: Protection for private blocking and screening of offensive material

118th Congress (2023-2024): H.R.3106 – Preventing Deepfakes of Intimate Images Act

118th Congress (2023-2024): H.R.5586 – DEEPFAKES Accountability Act

118th Congress (2023-2024): H.R.6943 – No AI FRAUD Act

118th Congress (2023-2024): S.560 – SAFE TECH Act

118th Congress (2023-2024): S.1207 – EARN IT Act of 2023

118th Congress (2023-2024): S.3696 – DEFIANCE Act of 2024

Restatement (Second) of Torts §46. American Law Institute: St. Paul, Minn. (1965)

Restatement (Second) of Torts §316. American Law Institute: St. Paul, Minn. (1965)

Restatement (Second) of Torts §558. American Law Institute: St. Paul, Minn. (1977)

Restatement (Second) of Torts §568. American Law Institute: St. Paul, Minn. (1977)

Restatement (Second) of Torts §569. American Law Institute: St. Paul, Minn. (1977)

Restatement (Second) of Torts §577. American Law Institute: St. Paul, Minn. (1977)

Restatement (Second) of Torts §652A, §652C, §652D. American Law Institute: St. Paul, Minn. (1977)

Jane Doe v K.G. (Civil Action No. 2:24-cv-00634)