Mercz Mónika

Az állam védelmi kötelezettsége és a mesterséges intelligencia: új kihívások a gyermekek büntetőjogi védelmében

I. Bevezetés

A mesterséges intelligencia fejlődése alapjaiban alakítja át a digitális környezetet, amelyben a gyermekek szocializációja, kommunikációja és információfogyasztása zajlik.[1] Az új technológiák nem csupán lehetőségeket, hanem korábban nem ismert kockázatokat is hordoznak, különösen a gyermekek sérelmére elkövetett bűncselekmények[2] tekintetében, amelyek nem csupán egyéni, hanem társadalmi szinten is maradandó károkat okoznak.[3] E körben kiemelt jelentőséggel bírnak az úgynevezett *deepfake* technológiák, amelyek képesek valósághű, de ténylegesen meg nem történt események vizuális vagy audiovizuális megjelenítésére.[4]

A tanulmány központi kérdése, hogy a jelenlegi büntetőjogi eszközrendszer alkalmas-e az MI technológia, különösen a deepfake alapú tartalmak által közvetített gyermekveszélyeztetés kezelésére. A tanulmány módszertanát tekintve elsősorban dogmatikai és elemző megközelítést alkalmaz. A vizsgálat középpontjában a hatályos büntetőjogi szabályozás értelmezése áll, különös tekintettel arra, hogy az miként alkalmazható a mesterséges intelligencia által generált tartalmak, ezen belül a deepfake technológia által előidézett új típusú gyermekveszélyeztetési formák esetében. A kutatás ennek megfelelően a releváns büntetőjogi tényállások – különösen a gyermekpornográfiára, a kiskorú veszélyeztetésére, valamint a személy elleni és becsület elleni bűncselekményekre vonatkozó rendelkezések – értelmező elemzésére épül.

A dogmatikai vizsgálatot kiegészíti egy funkcionális és jogpolitikai megközelítés, amely az állam védelmi kötelezettségeinek tartalmát és határait vizsgálja a digitális környezetben. Ennek keretében a tanulmány figyelembe veszi az Emberi Jogok Európai Bíróságának (EJEB) releváns gyakorlatát is, különös tekintettel a gyermekek fokozott védelmére és az állam pozitív kötelezettségeire vonatkozó esetjogra. A nemzetközi jogi háttér bevonása lehetővé teszi annak értékelését, hogy a hazai büntetőjogi szabályozás mennyiben felel meg az európai emberi jogi standardoknak.

A tanulmány emellett korlátozott mértékben interdiszciplináris megközelítést is alkalmaz, amennyiben a technológiai háttér – különösen a deepfake rendszerek működési logikája és társadalmi hatásai – rövid ismertetésével hozzájárul a jogi értékelés megalapozásához. A kutatás nem törekszik a technológiai kérdések teljes körű feltárására, hanem azokat a büntetőjogi értékelés szempontjából releváns mértékre korlátozza.

E körben ugyanakkor szükséges utalni arra, hogy az Európai Unió mesterséges intelligenciára vonatkozó szabályozása, különösen az AI Act,[5] már tartalmaz a deepfake technológiára irányadó rendelkezéseket, elsősorban átláthatósági és tájékoztatási kötelezettségek formájában.[6] E szabályozás azonban alapvetően nem büntetőjogi jellegű, hanem preventív és piacszabályozási logikát követ, ráadásul rendelet formájában került megalkotásra, így közvetlenül nem alkalmas a büntetőjogi felelősség megállapítására, és nem ültethető át változtatás nélkül a nemzeti büntetőjog rendszerébe.[7]

A vizsgálat központi részét ezért a büntetőjogi elemzés képezi, amely a hatályos szabályozás alkalmazhatóságát, hiányosságait és értelmezési problémáit elemzi. Az elemzés megalapozásához azonban szükséges annak vizsgálata is, hogy az állam milyen szerepet tölt be a gyermekek védelmében, különösen a gyorsan változó digitális környezetben. A mesterséges intelligencia által generált új kockázatok ugyanis nem pusztán technológiai vagy kriminológiai kérdéseket vetnek fel, hanem az állam klasszikus funkcióinak és védelmi kötelezettségeinek újraértelmezését is szükségessé teszik.

A szerző PhD hallgató, KRE ÁJK

1 Staksrud, Elisabeth (2013): *Children in the Online World, Risk, Regulation, Rights,* Farnham, Taylor & Francis, doi:10.4324/9781315571508

2 Somogyi, Zsófia Borbála (2026): Gyermekvédelem, pedofília és szexuális bűncselekmények, *Belügyi Szemle* 74(3), 663-682. https://doi.org/10.38146/bsz-ajia-ajia.2026.v74.i3.pp663-682

3 Mehta, Divya et al. (2021): Child Maltreatment and Long-Term Physical and Mental Health Outcomes: An Exploration of Biopsychosocial Determinants and Implications for Prevention. *Child Psychiatry Hum Dev,* 54(2):421-435. doi: 10.1007/s10578-021-01258-8

4 Guo, Jinyi – Wang, Duola (2025): Deepfake: Understanding the Technology Background, Content Differences from Traditional Forgery, and Impact on Public Trust, *Advances in Economics Management and Political Sciences,* 213(1):265-273, DOI:10.54254/2754-1169/2024.26901

5 Az Európai Parlament és a Tanács 2024. június 13-i (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról.

6 AI Act Article 50(4).

7 Craig, Paul – de Búrca, Gráinne (2024): *EU Law: Text, Cases, and Materials* (8th edn), Oxford, Oxford University Press, https://doi.org/10.1093/he/9780198915522.001.0001.

Ennek megfelelően a tanulmány a továbbiakban az állam alapvető funkcióinak és a gyermekekkel kapcsolatos védelmi kötelezettségek elméleti kereteit vizsgálja, különös tekintettel arra, hogy ezek miként jelennek meg az európai jogrendben, és milyen követelményeket támasztanak a büntetőjogi szabályozással szemben.

II.
Az állam funkciói és védelmi kötelezettsége a gyermekek vonatkozásában

Az Európai Unióról szóló szerződés (EUSZ) 4. cikk (2) bekezdése előírja, hogy az Európai Uniónak tiszteletben kell tartania a tagállamok nemzeti identitását, amely azok alapvető politikai és alkotmányos berendezkedésében gyökereznek, valamint alapvető állami funkcióikat is, ideértve a közrend fenntartását, a nemzetbiztonság védelmét és a területi integritás biztosítását. E rendelkezés központi szerepet tölt be az Európai Unió és a tagállamok közötti alkotmányos egyensúlyról szóló kortárs diskurzusban, mivel egyszerre jelöli ki a szupranacionális integráció határait és hangsúlyozza az államiság folyamatos jelentőségét az uniós jogrendben.[8]

Míg az EUSZ 4. cikk (2) bekezdésében szereplő nemzeti identitás klauzula elsősorban strukturális jellemzőkre fókuszál, addig az ugyanezen rendelkezésben megjelenő alapvető állami funkciókra vonatkozó rész inkább az állam működési, operatív képességeit emeli ki. Az alapvető állami funkciók ugyanis olyan tevékenységeket jelölnek, amelyek elengedhetetlenek az állam, mint politikai és jogi entitás hatékony működéséhez és fennmaradásához.[9] Az EUSZ 4. cikk (2) bekezdésének eredete az Európai Alkotmány létrehozásáról szóló szerződés I–5. cikkére vezethető vissza,[10] amelynek kialakítására jelentős hatást gyakorolt az V. munkacsoport kiegészítő hatáskörökről szóló zárójelentése. E jelentés amellett érvelt, hogy a „nemzeti identitás klauzula" és a „lényeges állami funkciók klauzulája" szoros összefüggésben értelmezendő. „Az uniós hatáskörök gyakorlásának elvei" cím alatt a munkacsoport célként tűzte ki annak tisztázását, hogy az Unió tiszteletben tartja a tagállamok bizonyos alapvető felelősségi területeit, mégpedig a nemzeti identitás tiszteletben tartásának alapelvének kibontásán keresztül.[11] A munkacsoport két fő területet határozott meg: egyrészt a tagállamok alapvető struktúráit és lényeges funkcióit – különösen politikai és alkotmányos berendezkedésüket, ideértve a regionális és helyi önkormányzatokat –, másrészt pedig olyan területeket, mint a nyelvhasználat, az állampolgárság, a terület, az egyházak és vallási közösségek jogállása, a nemzeti védelem és a fegyveres erők szervezete.[12]

Az EUSZ 4. cikk (2) bekezdésének tartalmából levezetve jelen tanulmány értelmezésében az alapvető állami funkciók olyan, az államisághoz inherensen kapcsolódó alapfunkciók, mint a területi integritás védelme, a nemzetbiztonság biztosítása, a közrend fenntartása,[13] a monetáris szuverenitás megőrzése, valamint az alkotmányos struktúrák fenntartása. E funkciók ellátása az állami intézményrendszer feladata, mivel ezek biztosítják az állam, mint hatékony kormányzati egység fennmaradását. Ennek megfelelően elsődleges felelősség terheli a tagállamokat, és e funkciókat az Európai Uniónak tiszteletben kell tartania.

Az EUSZ 4. cikk (2) bekezdésében nevesített körön túl az Európai Unió kontextusában az alapvető állami funkciók általában magukban foglalják az emberi jogok védelmét, a nemzeti szuverenitás biztosítását, a politikai és alkotmányos berendezkedés megválasztását, a regionális és helyi önkormányzati rendszer kialakítását, a demokratikus intézményrendszer működtetését, a fiskális és államadósság-kezelési kérdések irányítását, a hivatalos nyelv meghatározását, az állampolgárság szabályozását, a demográfiai kihívások kezelését, az adórendszer kialakítását, a jövedelemelosztás és a szociális ellátórendszerek meghatározását, valamint az egyházak és vallási közösségek jogállásának rendezését.

E felsorolás nem tekinthető kimerítőnek, ugyanakkor rávilágít, hogy az állam működésének középpontjában a közösség alapvető értékeinek és biztonságának megőrzése áll, amelynek egyik legfontosabb megnyilvánulása a jogrend fenntartása és az egyének – különösen a sérülékeny csoportok, így a gyermekek – védelme.

Az Emberi Jogok Európai Bíróságának gyakorlata is következetesen hangsúlyozza, hogy a gyermekek védelme az állam fokozott pozitív kötelezettségei közé tartozik. A *K. U. v. Finland*-ügyben a Bíróság kimondta, hogy az állam köteles olyan jogi és intézményi kereteket biztosítani, amelyek lehetővé teszik a gyermekeket érő online visszaélések hatékony kivizsgálását.[14] E követelmény a deepfake technológiák korában még hangsúlyosabbá válik, mivel az anonimitás és a technológiai komplexitás jelentősen megnehezíti az elkövetők azonosítását. Hasonlóképpen, a *X and Y v. Netherlands*-ügyben lefektetett elv szerint az állam nem maradhat passzív, ha az egyének – különösen a gyermekek – alapvető jogai sérülnek.[15] Ebből következően a büntetőjogi szabályozás hiányosságai önmagukban is felvethetik az állami felelősség kérdését, hiszen ez a védelmi feladat nemcsak erkölcsi, hanem jogi kötelezettség is, amely több szinten jelenik meg: büntetőjogi védelem (szankcionálás), preventív funkció (megelőzés), valamint

8 Boková, Terezie (2022): Exploring the Concept of Essential State Functions on the Basis of the CJEU's Decision on the Temporary Relocation Mechanism. *European Papers,* Vol. 7, No. 2, 773–979, doi: 10.15166/2499-8249/599.

9 Sulyok Tamás – Orbán Endre (2017): Az európai alkotmányos tér és az alkotmányos párbeszéd forgatókönyve. In Chronowski, Nóra et al. (eds.): *A szabadságszerető embernek. Liber Amicorum István Kukorelli.* Budapest: Gondolat, 116–125.

10 Angyal Zoltán (2007): Az Európai Alkotmányszerződés ratifikációs válsága, avagy a közvetlen demokrácia és az integráció kollíziója, *Sectio Juridica et Politica,* (1), 175–190

11 Guastaferro, Barbara (2012): Beyond the Exceptionalism of Constitutional Conflicts: The Ordinary Functions of the Identity Clause, Yearbook of European Law 263, 271–285.

12 Final Report of Working group V cit. 10–12.

13 Ezek a funkciók egyértelműen megnevezésre kerülnek az EUSZ 4. cikk (2) bekezdésben.

14 EJEB, K. U. kontra Finnország, 2872/02. sz. kérelem, 2008. december 2.

15 EJEB, X és Y kontra Hollandia, 8978/80. sz. kérelem, 1985. március 26.

intézményvédelmi kötelezettség (jogi és technikai keretek kialakítása) által.

A digitális térben azonban az állami jelenlét korlátozottabb, miközben a veszélyek komplexebbé váltak.[16] Az állam pozitív kötelezettségei így kiterjednek arra is, hogy: felismerje az új típusú kockázatokat, megfelelő szabályozási környezetet alakítson ki és biztosítsa a hatékony jogérvényesítést.[17] Az MI által generált tartalmak új kihívást jelentenek: a deepfake technológia által generált gyermekpornográfia nem pusztán új elkövetési módot jelent, hanem a büntetőjog egyik alapvető kategóriáját – a sértett fogalmát – kérdőjelezi meg, ami indokolttá teszi a tényállások újragondolását vagy kifejezett kiterjesztését.

III. A deepfake technológia büntetőjogi vetületei

A deepfake technológia gépi tanulási algoritmusok – különösen neurális hálózatok – segítségével létrehozott vagy manipulált kép-, hang- vagy videótartalom. Sajátossága, hogy meglévő személyekre, tárgyakra, helyszínekre, szervezetekre vagy eseményekre hasonlít, és egy személy számára tévesen hitelesnek vagy valóságosnak tűnhet.[18] E technológia alkalmazása önmagában nem jogellenes, azonban visszaélésszerű használata komoly társadalmi és jogi problémákat vet fel.[19]

Büntetőjogi szempontból különösen problematikus, hogy a deepfake tartalmak olyan eseményeket jelenítenek meg, amelyek a valóságban nem történtek meg, mégis alkalmasak arra, hogy a befogadó számára valóságként hassanak. E sajátosság alapjaiban kérdőjelezi meg a bizonyítás hagyományos eszközeit és a tényállási elemek értelmezését. További nehézséget jelent, hogy a technológia egyre könnyebben hozzáférhető, amely az online térben biztosított anonimitás, valamint a tartalmak rendkívül gyors és kontrollálhatatlan terjedése mellett jelentősen megnehezíti a jogsértések felderítését és az elkövetők felelősségre vonását.[20]

A gyermekek vonatkozásában a deepfake technológia különösen súlyos kockázatokat hordoz. Az ilyen eszközök nem csupán szexuális tartalmak előállítására alkalmasak, hanem felhasználhatók zaklatásra, lejáratásra, illetve dezinformáció terjesztésére is.[21] Mindez a gyermekek személyiségfejlődésére, pszichés állapotára és társadalmi megítélésére egyaránt káros hatással lehet.[22]

Az online gyermekpornográfiával kapcsolatos szakirodalom már korábban rámutatott arra, hogy az internetes környezet sajátosságai – így különösen az anonimitás, a tömegesség és a határokon átnyúló jelleg – jelentősen megnehezítik a büntetőjogi fellépést, mivel a hagyományos nyomozási és bizonyítási eszközök sok esetben nem bizonyulnak hatékonynak az online térben megvalósuló jogsértések feltárása során. E kihívások a mesterséges intelligencia és a deepfake technológia megjelenésével tovább erősödnek. A gyermekpornográfia a kiberbűnözés egyik sajátos formájaként értelmezhető, amelynek jellemzője a nehezen körülhatárolható elkövetési kör, a tömegesség, valamint a jelentős és sok esetben hosszan fennálló károkozás. Ezzel párhuzamosan a bűncselekmények gyakran több joghatóságot érintenek, ami szükségessé teszi a nemzetközi bűnüldözési együttműködés erősítését. Ennek keretében kiemelt szerepet játszanak olyan szervezetek, mint az Europol vagy az Interpol, amelyek koordinációs és információmegosztási funkciójuk révén járulnak hozzá a hatékony fellépéshez.[23]

A jelenség kezelésére adott állami válaszok között megjelennek technikai jellegű eszközök is, így például az illegális tartalmakhoz való hozzáférés korlátozása vagy blokkolása. Ugyanakkor e megoldások hatékonysága korlátozott, tekintettel arra, hogy a digitális tartalmak könnyen újra előállíthatók és más platformokon ismételten közzétehetők.[24] Mindez arra utal, hogy a pusztán technikai eszközökre építő megközelítés nem elegendő, hanem komplex, büntetőjogi és preventív elemeket egyaránt magában foglaló szabályozás szükséges. Az online gyermekpornográfia kapcsán azonosított kockázatok – így különösen az anonimitás, a tömegesség és a gyors terjedés – a deepfake technológia révén tovább erősödnek, mivel a tartalmak előállítása még egyszerűbbé és szélesebb körben hozzáférhetővé válik. Ennek következtében a büntetőjogi szabályozás és a bűnüldözési gyakorlat előtt álló kihívások nemcsak fennmaradnak, hanem új dimenzióval is bővülnek, ami indokolttá teszi az állami fellépés újragondolását és megerősítését.

A probléma azonban két alapvető esetkört foglal magában: az első esetben valós gyermek arcképe vagy egyéb azonosításra alkalmas jellemzője kerül felhasználásra és manipulálásra egy pornográf tartalomban, míg a második esetben a deepfake által generált tartalomban szereplő személyek nem valósak. Amennyiben igazi gyermek arcképe került felhasználásra, a sérelem egyértelműen megállapítható, mivel a gyermek sze-

16 Ali, Waqar et al. (2025): Artificial Intelligence in crime prevention and detection: Enhancing predictive policing and public safety, *Advance Social Science Archive Journal,* 4(02), 1534–1543 https://doi.org/10.5281/zenodo.17577464.

17 Venier, Silvia (2022): Chapter 27 Positive Obligations under Human Rights Law to Protect against CBRN Risks, In: *International Law and Chemical, Biological, Radio-Nuclear (CBRN) Events* (eds: de Guttry, Andreas et al.), 481–500. DOI: https://doi.org/10.1163/9789004507999_028.

18 AI Act Article 3 (60) 'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.

19 Diel, Alexander et al. (2025): The harm of deepfakes: a scoping review of deepfakes' negative effects on human mind and behavior. *AI & Society,* 28(3), https://doi.org/10.1007/s00146-025-02774-0.

20 Herke Csongor (2013): Deepfake: áldás vagy átok? Jogi szabályozási szempontok, *Pro Futuro,* 2023/1., 157–178. DOI 10.26521/profuturo/2023/1/13334.

21 Gosztonyi Gergely – Lendvai Gergely (2024): Deepfake és dezinformáció. Mit tehet a jog a mélyhamisítással készített álhírek ellen? *Médiakutató,* 2024. (1), 41—49. DOI. https://doi.org/10.55395/MK.2024.1.3.

22 Kikerpill, Kristjan – Siibak, Andra – Valli, Suido (2021): Dealing with Deepfakes: Reddit, Online Content Moderation, and Situational Crime Prevention. In: Julie B. Wiest (ed.): *Theorizing Criminality and Policing in the Digital Media Age.* Leeds, Emerald Publishing Limited (Studies in Media and Communications, 20.) 25—45. DOI: https://doi.org/10.1108/S2050-206020210000020008.

23 Csapucha Bernadett (2019): A „világháló árnyoldala", avagy a gyermekpornográfia térnyerése az interneten, 2019. évi 4–5. lapszám, 55–68.

24 Harkai István (2020): *Az internet hatása a többszörözési és a nyilvánossághoz közvetítési jogra*. Pólay Elemér Alapítvány – A Pólay Elemér Alapítvány Könyvtára 87., Iurisperitus Kiadó, Szeged, ISBN 978-615-6268-07-5.

mélyiségi jogai és emberi méltósága közvetlenül sérülnek.[25] Ezzel szemben a második esetben teljes egészében mesterségesen generált, „nem létező" gyermek jelenik meg a tartalomban. Ez az eset dogmatikailag jóval összetettebb, mivel hiányzik a konkrét, azonosítható sértett, ugyanakkor a társadalmi veszélyesség továbbra is fennáll. Az ilyen tartalmak ugyanis hozzájárulhatnak a gyermekek szexuális tárgyiasításának normalizálásához, valamint közvetetten elősegíthetik a valós bűncselekmények elkövetését.[26]

Ezenfelül a deepfake technológia nemcsak szexuális visszaélések eszközeként jelenik meg, hanem a gyermekek sérelmére elkövetett egyéb jogsértések új formáit is lehetővé teszi. Különösen jelentős kockázatot jelent, hogy az ilyen technológiával könnyen előállíthatók kompromittáló vagy lejárató tartalmak, amelyek valótlan eseményeket tüntetnek fel valóságként. E körben a deepfake alkalmas, hogy gyermekekről olyan videófelvételek készüljenek, amelyek őket méltatlan, megalázó vagy társadalmilag hátrányos helyzetben ábrázolják. Emellett lehetőséget biztosít hamis narratívák kialakítására és terjesztésére, amelyek hosszú távon is káros hatást gyakorolhatnak az érintettek társadalmi megítélésére és pszichés állapotára. A jelenség különösen az iskolai közegben jelent fokozott veszélyt, ahol a digitális zaklatás (cyberbullying) a deepfake technológia révén új dimenziót nyer. A valósághű, de hamis tartalmak terjedése a közösségi médiában gyorsan és széles körben történik, ami a sérelmek súlyosságát és tartósságát jelentősen növeli.[27]

A mesterséges intelligencia fejlődése a klasszikus grooming jelenség új formáinak megjelenését is eredményezte. Az MI-alapú chatbotok és kommunikációs rendszerek képesek arra, hogy gyermekekkel interakcióba lépjenek, bizalmi kapcsolatot alakítsanak ki, és hosszabb távon fenntartsák azt. E rendszerek alkalmazása lehetővé teszi, hogy az elkövetők automatizált módon, akár tömegesen lépjenek kapcsolatba gyermekekkel, miközben a kommunikáció személyre szabottnak és hitelesnek tűnik. Az ilyen eszközök alkalmasak manipulációs technikák alkalmazására, érzelmi befolyásolásra, valamint a későbbi visszaélések előkészítésére.[28] Mindez a *grooming* jelenség technológiai evolúcióját jelenti, amely jelentősen növeli a kockázatok mértékét, és új kihívások elé állítja a büntetőjogi szabályozást és a gyermekvédelmi rendszereket egyaránt.

IV. Releváns tényállások

A mesterséges intelligencia és különösen a deepfake technológia által generált új típusú visszaélések értékelése során elsődleges kérdésként merül fel, hogy a hatályos büntetőjogi tényállások mennyiben alkalmasak e jelenségek megragadására. A tanulmány amellett érvel, hogy bár számos meglévő tényállás részben alkalmazható, azok több esetben értelmezési nehézségekbe ütköznek, illetve nem fedik le teljes mértékben az új technológiai környezetből fakadó magatartásokat.

1. Gyermekpornográfia – Btk. 204. §

A deepfake technológia büntetőjogi megítélése szempontjából központi jelentőségű a gyermekpornográfia tényállása. A jogszabály a gyermekről készült pornográf felvétel megszerzését, tartását, terjesztését és készítését rendeli büntetni, ezáltal komplex védelmet biztosít a gyermekek szexuális kizsákmányolásával szemben. A tényállás alkalmazása azonban dogmatikai szempontból problémássá válik a deepfake technológia esetében. A szabályozás implicit módon abból indul ki, hogy a felvétel valós gyermekről készült, vagy legalábbis valós személyhez köthető. Ezzel szemben a mesterséges intelligencia lehetővé teszi olyan tartalmak előállítását, amelyek esetében vagy egy valós gyermek arcképét manipulálják, vagy teljes egészében mesterségesen generált, „nem létező" gyermek jelenik meg.

Az előbbi esetben a tényállás alkalmazhatósága megalapozottnak tűnik, ugyanakkor a bizonyítás komoly nehézségekbe ütközhet, különösen a manipuláció ténye és mértéke tekintetében.[29] Az utóbbi esetben azonban felmerül a kérdés, hogy beszélhetünk-e egyáltalán gyermekpornográfiáról, amennyiben konkrét, azonosítható sértett nem állapítható meg. Ennek fényében a Btk. 204. § alkalmazhatósága kétséges olyan esetekben, amikor a felvétel nem valós gyermekről készült,[30] hanem mesterséges intelligencia által generált, „gyermek látszatát keltő" tartalom.[31]

2. Szexuális visszaélés – Btk. 198. §

A szexuális visszaélés tényállása a gyermek sérelmére elkövetett szexuális cselekményeket kriminalizálja, amelynek központi eleme a fizikai vagy közvetlen interakción alapuló magatartás. Ebből következően a deepfake technológia alkalmazása – amely tipikusan nem jár közvetlen fizikai érintkezéssel – e tényállás alá közvetlenül nem vonható.

Ugyanakkor a rendelkezés relevanciája nem zárható ki teljes mértékben. Az MI-alapú rendszerek által támogatott online grooming jelensége olyan előkészítő magatartásként értelmezhető, amely a későbbi szexuális visszaélések megalapozását szolgálja.[32] Ennek megfelelően a tényállás közvetett mó-

25 Némedi Márk (2016): *Változások a gyermekpornográfia szabályozásában Magyarországon és az Európai Unióban*. Pisa, 7—8.: https://www.jogiforum.hu/publikaciok/816

26 Lazaridou, Maria (2024): *Schrödinger's Crime: AI-generated Child Sexual Abuse Material as a Victimless Offense,* Master Thesis, Utrecht University, SN: 7465343.

27 Kowalski, Robin (2018): Cyberbullying, In: *The Routledge International Handbook of Human Aggression* (eds.: Jane Ireland, Philip Birch, Carol Ireland), Routledge, London, https://doi.org/10.4324/9781315618777.

28 Whittle, Helen – Hamilton-Giachritsis, Catherine – Beech, Anthony – Collings, Guy (2013): A review of young people's vulnerabilities to online grooming, *Aggression and Violent Behavior,* Volume 18, Issue 1, 135–146, https://doi.org/10.1016/j.avb.2012.11.008.

29 Somogyi Csilla (2025): A gyermekpornográfia felderítésének nehézségei, *Magyar Rendészet,* 2025/2. 103–123. DOI: 10.32577/MR.2025.2.7.

30 Tóth Mercédesz (2025): In: Békés Ádám – Kurunczi Gábor – Pogácsás Anett – Varga Ádám (szerk.): *'A tudomány fényénél egyre tisztábban látunk...': A Zlinszky János Szakkollégium első két éve*, Budapest, Magyarország : Pázmány Press, 141–153.

31 Petrini, Antonella – Belén Gauna, María (2024): Child Sexual Abuse Material provided by Artificial Intelligence, *EthAIca* 3:123, DOI:10.56294/ai2024123.

32 Köllő Dávid (2020): A gyermekek szexuális kizsákmányolása a kibertér felhasználásával, *Belügyi Szemle,* 2020/2, 59-87. DOI: 10.38146/BSZ.2020.2.5.

don kapcsolódhat a deepfake és más MI-alapú technológiák által előidézett veszélyekhez.

3. Gyermekprostitúció kihasználása – Btk. 203. §

A gyermekprostitúció kihasználására vonatkozó szabályozás elsősorban a gyermekek gazdasági célú szexuális kizsákmányolását célozza. A deepfake technológia ehhez a tényálláshoz közvetlenül ritkán kapcsolódik, ugyanakkor közvetett összefüggések azonosíthatók. Amennyiben a mesterséges intelligenciát gyermekek kizsákmányolását elősegítő rendszerek szervezésére, kommunikációjára vagy működtetésére használják, a tényállás alkalmazhatósága felmerülhet. Ez azonban inkább kivételes eset, és nem tekinthető a deepfake jelenség tipikus büntetőjogi kapcsolódási pontjának.

4. Zaklatás – Btk. 222. §

A zaklatás tényállása különösen jelentős a deepfake technológia kapcsán, mivel alkalmas lehet az ilyen eszközökkel megvalósított visszaélések megragadására, különösen a cyberbullying[33] jelensége kapcsán. A rendszeres háborgatás és a félelemkeltés mint tényállási elemek jól illeszkednek azokhoz az esetekhez, amikor valótlan, de valósághű tartalmak terjesztésével kívánják az érintettet megfélemlíteni vagy társadalmi helyzetét ellehetetleníteni.[34]

A technológiai fejlődés következtében e visszaélések új formái jelentek meg, amelyek közül kiemelendők a mesterséges intelligencián alapuló rendszerek – így például a Grok AI-hoz hasonló, széles körben hozzáférhető eszközök –, valamint az úgynevezett „nudifying" alkalmazások. Utóbbiak képesek arra, hogy valós személyekről készült képfelvételeket mesterségesen módosítsanak, és azokat szexuális tartalomként jelenítsék meg anélkül, hogy az érintett valójában ilyen helyzetben szerepelt volna. Különösen aggasztó, hogy e technológiák használata egyre alacsonyabb technikai tudást igényel, így gyermekek által is könnyen hozzáférhetővé válik.[35]

E jelenségek a zaklatás súlyosabb, kvalifikált eseteiként értelmezhetők, mivel a valósághű, de hamis tartalmak terjesztése alkalmas, hogy az érintettben tartós félelmet keltsen, valamint jelentős pszichés és társadalmi károkat idézzen elő. A „nudifying" alkalmazások különösen az iskolai környezetben jelentenek fokozott veszélyt, ahol az ilyen módon előállított és terjesztett képek a cyberbullying új, rendkívül káros formájaként jelennek meg, súlyosan sértve az érintett gyermek emberi méltóságát és társadalmi megítélését.

Mindezek alapján megalapozott az az álláspont, hogy a deepfake és más MI-alapú technológiák a zaklatás tényállásának új megjelenési formáit hozzák létre, amelyek a hagyományos értelmezési keretek kiterjesztését, illetve adott esetben a jogalkalmazási gyakorlat továbbfejlesztését teszik szükségessé.

5. Rágalmazás és becsületsértés – Btk. 226–227. §

A becsület elleni bűncselekmények szintén relevánsak a deepfake technológia alkalmazása során. A rágalmazás klaszszikusan valótlan tény állítását vagy híresztelését jelenti, amely más személy becsületének csorbítására alkalmas. A deepfake technológia ezt a magatartást új dimenzióba helyezi, mivel a hamis tényállítás vizuális, audiovizuális formában jelenik meg, ami annak meggyőző erejét jelentősen növeli. A jogsértés súlyosságát tovább fokozza, ha az érintett gyermek, illetve, ha a tartalom tömegesen terjed az online térben.[36] Ilyen esetekben a becsület elleni bűncselekmények alkalmazása indokolt lehet, ugyanakkor kérdéses, hogy e tényállások alkalmasak-e a technológia által előidézett komplex sérelmek teljes körű megragadására.

6. Kiskorú veszélyeztetése – Btk. 208. §

A kiskorú veszélyeztetésének tényállása tágabb értelmezési lehetőséget kínál a deepfake technológia kapcsán. A rendelkezés a gyermek testi, értelmi vagy erkölcsi fejlődésének veszélyeztetését rendeli büntetni, amely magában foglalhatja a pszichés károsodást és a társadalmi megbélyegzést is. A deepfake alapú visszaélések – különösen a lejárató vagy kompromittáló tartalmak – alkalmasak, hogy súlyos pszichológiai következményeket idézzenek elő, ezáltal veszélyeztetve a gyermek fejlődését.[37] Ebből következően a tényállás értelmezésének kiterjesztése releváns lehet az ilyen magatartások büntetőjogi megítélése során.

7. A „valós sérelem" dogmatikai problémája

A fentiek alapján megállapítható, hogy a jelenlegi büntetőjogi szabályozás több ponton képes reagálni a deepfake technológia által felvetett kihívásokra, ugyanakkor számos esetben értelmezési bizonytalanságokkal terhelt. Ennek egyik alapvető oka, hogy a büntetőjog hagyományosan a „valós sérelem" vagy legalábbis konkrét veszély fennállására épít.

A deepfake technológia ezzel szemben lehetővé teszi olyan tartalmak előállítását, amelyek esetében a sérelem nem feltétlenül közvetlen vagy individuálisan meghatározható, hanem közvetett, diffúz vagy akár társadalmi szinten jelentkezik. Ez a jelenség alapvető kihívást jelent a klasszikus tényállási elemek – különösen a sértett, a sérelem és az okozati összefüggés – értelmezése szempontjából, és indokolttá teszi a büntetőjogi dogmatika újragondolását vagy továbbfejlesztését.

A nemzetközi szakirodalom és joggyakorlat is rámutat, hogy a mesterséges intelligencia által generált, gyermekeket ábrá-

33 Alexander, Sergio (2025): Deepfake Cyberbullying: The Psychological Toll on Students and Institutional Challenges of AI-Driven Harassment. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas,* 98(2), 36–50. https://doi.org/10.1080/00098655.2025.2488777.

34 Serebrennikova, Anna V. (2020): Harassment: criminal law concept, *Economic problems and Legal Practice,* Vol 16, No 3, 198—201. https://journals.eco-vector.com/2541-8025/article/view/532605

35 Viola, M. – Voto, C. (2023): Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. *Synthese,* 201, *30*. https://doi.org/10.1007/s11229-022-04012-2.

36 Apolo, Yvonne – Michael, Katina (2024): Beyond A Reasonable Doubt? Audiovisual Evidence, AI Manipulation, Deepfakes, and the Law, *IEEE Transactions on Technology and Society,* vol. 5, no. 2, 156–168, doi: 10.1109/TTS.2024.3427816.

37 Laczi, Szandra – Póser, Valéria (2024): *Impact of Deepfake Technology on Children: Risks and Consequences*, Conference: 2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY), DOI:10.1109/SISY62279.2024.10737593.

zoló szexuális tartalmak esetében egyre gyakrabban merül fel a „sértett nélküli bűncselekmény” *(victimless offense)* problémája. Azokban az esetekben, amikor a tartalom teljes egészében mesterségesen generált, és nem köthető konkrét, azonosítható gyermekhez, a klasszikus értelemben vett sértetti pozíció hiányzik. Ugyanakkor több jogrendszerben és tudományos megközelítésben is megjelenik az az álláspont, hogy az ilyen tartalmak társadalmi veszélyessége önmagában megalapozhatja a büntetőjogi fellépést.

Ezt támasztják alá azok a nemzetközi példák is, amelyek szerint a deepfake alapú gyermekpornográfia terjedése nem csupán egyéni szinten okoz sérelmet, hanem hozzájárulhat a gyermekek szexuális kizsákmányolásának normalizálásához, valamint a valós visszaélések iránti kereslet fenntartásához vagy akár növeléséhez. Ebből következően a sérelem nem feltétlenül egy konkrét személyhez köthető, hanem a gyermekek, mint védendő társadalmi csoport kollektív érdekeit érinti.[38]

A gyakorlatban továbbá az is megfigyelhető, hogy a deepfake technológia sok esetben valós személyek képmásának felhasználásával működik, még akkor is, ha a végeredmény mesterségesen generált. Ilyen esetekben a sérelem már nem pusztán absztrakt, hanem konkrét személyhez köthető, ami tovább árnyalja a „valós” és „nem valós” sérelem közötti határvonalat. Emellett a tartalmak online terjedése révén a károkozás időben elhúzódóvá és nehezen kontrollálhatóvá válik, ami a sérelem súlyát és intenzitását is növeli.

Mindezek alapján megállapítható, hogy a deepfake technológia által előidézett jogsértések nem illeszthetők maradéktalanul a büntetőjog hagyományos dogmatikai keretei közé. A „valós sérelem” követelménye a digitális térben új tartalommal telítődik: a közvetett, diffúz és társadalmi szinten jelentkező károk is relevánssá válnak a büntetőjogi értékelés során. Ez indokolttá teszi a sértett fogalmának, a társadalmi veszélyesség értelmezésének, valamint a büntetőjogi beavatkozás határainak újragondolását, különös tekintettel a gyermekek fokozott védelmére.

V. Megoldási javaslatok

A mesterséges intelligencia és különösen a deepfake technológia megjelenése tehát rámutat, hogy a jelenlegi büntetőjogi szabályozás több ponton nem képes maradéktalanul kezelni az új típusú visszaéléseket. A fenti hiányosságokkal összefüggésben alapvető kérdésként merül fel a büntetőjogi beavatkozás határainak meghatározása, különösen a „valós sérelem nélküli” kriminalizáció tekintetében. Egyrészt érvek szólnak amellett, hogy az ilyen magatartások büntetendővé tétele indokolt lehet, mivel társadalmi veszélyességük fennáll: a gyermekek szexuális kizsákmányolásának normalizálásához vezethetnek, valamint előkészíthetik a későbbi, valós bűncselekményeket.[39] Másrészt azonban nem hagyható figyelmen kívül, hogy hiányzik a klasszikus sértetti pozíció,[40] fennáll a túlzott kriminalizáció veszélye,[41] és jelentős bizonyítási nehézségek is felmerülnek.[42] E kettősség rávilágít, hogy a büntetőjog hagyományos dogmatikai keretei nehezen alkalmazhatók az új technológiai környezetben.

A szabályozási hiányosságok kezelésére alapvetően két irány kínálkozik. Az egyik lehetőség a meglévő tényállások értelmezésének kiterjesztése, különösen oly módon, hogy azok kifejezetten magukban foglalják a „gyermek látszatát keltő” tartalmakat is. Ez a megközelítés lehetővé teszi a jogrendszer rugalmasságának megőrzését, ugyanakkor fennáll a veszélye, hogy az értelmezési bizonytalanságok továbbra is fennmaradnak. A másik lehetőség új, kifejezetten az MI által generált tartalmakra vonatkozó tényállás megalkotása. Ez nagyobb jogbiztonságot biztosíthat, ugyanakkor a technológia gyors fejlődése miatt fennáll a veszélye, hogy a szabályozás rövid időn belül elavulttá válik. A két megoldás közötti választás ezért nem kizárólag dogmatikai, hanem jogpolitikai kérdés is.

Az állam felelőssége e körben több szinten is megjelenik. Egyrészt jogalkotási felelősség terheli abban az értelemben, hogy a szabályozás képes legyen lépést tartani a technológiai fejlődéssel, és megfelelő módon kezelje az új típusú visszaéléseket. Másrészt a jogalkalmazás hatékonysága is kulcsfontosságú, különösen a felderítés és bizonyítás területén, ahol a technológiai komplexitás jelentős kihívásokat támaszt. Harmadrészt a preventív funkció is kiemelt jelentőséggel bír: az államnak szerepet kell vállalnia a tudatosságnövelésben, az oktatásban és a technológiai kockázatok megelőzésében.

Mindezek alapján több *de lege ferenda* javaslat is megfogalmazható. Indokolt lenne a „gyermek látszatát keltő” tartalmak egyértelmű bevonása a releváns büntetőjogi tényállások körébe, amely hozzájárulhat a jogbiztonság erősítéséhez. Emellett megfontolandó egy speciális, az MI által generált tartalmakra vonatkozó tényállás kialakítása, amely kifejezetten e technológia sajátosságaira reflektál. Szintén szükséges a platformok felelősségének erősítése, különös tekintettel a jogsértő tartalmak eltávolítására és terjedésének megakadályozására.

A hatékony fellépés érdekében elengedhetetlen a hatóságok technológiai felkészültségének fejlesztése, valamint a nemzetközi együttműködés fokozása, tekintettel arra, hogy az ilyen jellegű bűncselekmények gyakran határokon átnyúló jellegűek. Végül kiemelendő, hogy a jövőbeni szabályozásnak egyszerre kell technológiasemlegesnek maradnia, ugyanakkor képesnek kell lennie, hogy rugalmasan reagáljon az újonnan megjelenő kihívásokra.

38 Egyesült Államok, United States v. Holmes, 2019 (szövetségi bírósági ügy).
Egyesült Királyság, R v. John McKenzie, 2020 (büntetőügy).
Ausztrália (New South Wales), R v. S., 2021 (állami bírósági ügy).

39 Ciardha, Caoilte Ó. et al. (2026): AI-generated child sexual abuse material: what's the harm? *AI & SOCIETY,* DOI:10.1007/s00146-026-02932-y.

40 Kiss Anna (2017): A sértett szerepének változása az új büntetőeljárási törvényben, *Magyar Rendészet,* 2017/5. 11–21.

41 Amberg Erzsébet – Pallagi Anikó (2021): Mire jó a büntetőjog? Célszerűségi megfontolások kontra ultima ratio, *Belügyi Szemle,* Évf. 69 szám 1, 35–74. DOI:10.38146/BSZ.2021.1.2.

42 Badinszky Áron (2024): Hamis valóság, valós veszély: deepfake az AI Act-ben, *KözigazgatásTudomány,* 2024/2. 18–38. https://doi.org/10.54200/kt.v4i2.89.

VI. Összegzés

A mesterséges intelligencia fejlődése, különösen a deepfake technológia megjelenése alapvetően új kihívások elé állítja a gyermekek büntetőjogi védelmét. E technológiák sajátossága, hogy képesek valósághű, ugyanakkor ténylegesen meg nem történt események megjelenítésére, ezáltal elmosva a valóság és fikció közötti határvonalat. Ennek következtében nem csupán a bűncselekmények elkövetési módjai alakulnak át, hanem a büntetőjog hagyományos dogmatikai kategóriái – különösen a sértett, a sérelem és a társadalmi veszélyesség fogalma – is új értelmezési keretbe kerülnek.

A tanulmány rámutatott, hogy a hatályos büntetőjogi szabályozás több ponton képes reagálni az MI által közvetített gyermekveszélyeztetés jelenségére, ugyanakkor nem minden esetben nyújt kielégítő megoldást. Különösen a gyermekpornográfia tényállása esetében merülnek fel olyan értelmezési problémák, amelyek a mesterségesen generált, „gyermek látszatát keltő" tartalmak kezelését bizonytalanná teszik. Ezzel összefüggésben a „valós sérelem" hiánya új típusú dogmatikai dilemmákat vet fel, amelyek a büntetőjogi beavatkozás határainak újragondolását teszik szükségessé.

A vizsgálat továbbá megerősítette, hogy az állam védelmi kötelezettsége a digitális térben sem csökken, hanem a technológiai fejlődéssel párhuzamosan erősödik. Az Emberi Jogok Európai Bíróságának gyakorlata egyértelműen alátámasztja, hogy az állam nem maradhat passzív, hanem köteles hatékony jogi és intézményi kereteket biztosítani a gyermekeket érő visszaélésekkel szemben. Ez a kötelezettség a deepfake technológia kontextusában különösen hangsúlyossá válik, figyelemmel az anonimitásra, a tartalmak gyors terjedésére és a felderítés nehézségeire. Mindezek alapján megállapítható, hogy a jelenlegi szabályozási keret kiegészítésre és részben újragondolásra szorul.

Összességében a mesterséges intelligencia által generált tartalmak nem csupán új bűnözési formákat hoznak létre, hanem az állam szerepének újraértelmezését is szükségessé teszik. A modern állam egyik alapvető funkciója továbbra is a jogrend fenntartása és az egyének – különösen a sérülékeny csoportok, így a gyermekek – védelme, azonban e funkciók gyakorlása a digitális térben már csak aktív, proaktív és technológiailag megalapozott fellépéssel biztosítható.

Irodalomjegyzék

Alexander, Sergio (2025): Deepfake Cyberbullying: The Psychological Toll on Students and Institutional Challenges of AI-Driven Harassment. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas* 98(2), 36–50. https://doi.org/10.1080/00098655.2025.2488777.

Ali, Waqar et al. (2025): Artificial Intelligence in crime prevention and detection: Enhancing predictive policing and public safety, *Advance Social Science Archive Journal* 4(02), 1534–1543. https://doi.org/10.5281/zenodo.17577464.

Amberg Erzsébet – Pallagi Anikó (2021): Mire jó a büntetőjog? Célszerűségi megfontolások kontra ultima ratio, *Belügyi Szemle,* Évf. 69 szám 1, 35–74. DOI:10.38146/BSZ.2021.1.2.

Angyal Zoltán (2007): Az Európai Alkotmányszerződés ratifikációs válsága, avagy a közvetlen demokrácia és az integráció kollíziója, *Sectio Juridica et Politica,* (1), 175–190.

Apolo, Yvonne – Michael, Katina (2024): Beyond A Reasonable Doubt? Audiovisual Evidence, AI Manipulation, Deepfakes, and the Law, in *IEEE Transactions on Technology and Society,* vol. 5, no. 2, 156-168, doi: 10.1109/TTS.2024.3427816.

Badinszky Áron (2024): Hamis valóság, valós veszély: deepfake az AI Act-ben, *KözigazgatásTudomány,* 2024/2. 18–38. https://doi.org/10.54200/kt.v4i2.89.

Boková, Terezie (2022): Exploring the Concept of Essential State Functions on the Basis of the CJEU's Decision on the Temporary Relocation Mechanism. *European Papers,* Vol. 7, No. 2, 773-979, doi: 10.15166/2499-8249/599.

Ciardha, Caoilte Ó. et al. (2026): AI-generated child sexual abuse material: what's the harm? *AI & SOCIETY,* DOI:10.1007/s00146-026-02932-y.

Craig, Paul – de Búrca, Gráinne (2024): *EU Law: Text, Cases, and Materials* (8th edn), Oxford, Oxford University Press, https://doi.org/10.1093/he/9780198915522.001.0001.

Csapucha Bernadett (2019): A „világháló árnyoldala", avagy a gyermekpornográfia térnyerése az interneten, 2019. évi 4-5. lapszám, 55–68.

Diel, Alexander et al. (2025): The harm of deepfakes: a scoping review of deepfakes' negative effects on human mind and behavior. *AI & Society,* 28(3), https://doi.org/10.1007/s00146-025-02774-0.

Gosztonyi Gergely – Lendvai Gergely (2024): Deepfake és dezinformáció. Mit tehet a jog a mélyhamisítással készített álhírek ellen? *Médiakutató,* 2024. (1), 41–49. DOI. https://doi.org/10.55395/MK.2024.1.3.

Guastaferro, Barbara (2012): Beyond the Exceptionalism of Constitutional Conflicts: The Ordinary Functions of the Identity Clause, *Yearbook of European Law,* 263, 271–285.

Guo, Jinyi – Wang, Duola (2025): Deepfake: Understanding the Technology Background, Content Differences from Traditional Forgery, and Impact on Public Trust, *Advances in Economics Management and Political Sciences,* 213(1): 265–273, DOI:10.54254/2754-1169/2024.26901.

Harkai István (2020): *Az internet hatása a többszörözési és a nyilvánossághoz közvetítési jogra*. Pólay Elemér Alapítvány – A Pólay Elemér Alapítvány Könyvtára 87., Iurisperitus Kiadó, Szeged, ISBN 978-615-6268-07-5.

Herke Csongor (2013): Deepfake: áldás vagy átok? Jogi szabályozási szempontok, *Pro Futuro,* 2023/1., 157-178. DOI 10.26521/profuturo/2023/1/13334.

Kikerpill, Kristjan – Siibak, Andra – Valli, Suido (2021): Dealing with Deepfakes: Reddit, Online Content Moderation, and Situational Crime Prevention. In: Julie B. Wiest (ed.): *Theorizing Criminality and Policing in the Digital Media Age*. Leeds, Emerald Publishing Limited (Studies in Media and Communications, 20.) 25–45. DOI: https://doi.org/10.1108/S2050-206020210000020008.

Kiss Anna (2017): A sértett szerepének változása az új büntetőeljárási törvényben, *Magyar Rendészet,* 2017/5. 11–21.

Kowalski, Robin (2018): Cyberbullying, In: *The Routledge*

International Handbook of Human Aggression (eds.: Jane Ireland – Philip Birch – Carol Ireland), Routledge, London, https://doi.org/10.4324/9781315618777.

Köllő Dávid (2020): A gyermekek szexuális kizsákmányolása a kibertér felhasználásával, *Belügyi Szemle,* 2020/2, 59–87. DOI: 10.38146/BSZ.2020.2.5.

Laczi, Szandra – Póser, Valéria (2024): *Impact of Deepfake Technology on Children: Risks and Consequences*, Conference: 2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY), DOI:10.1109/SISY62279.2024.10737593.

Lazaridou, Maria (2024): *Schrödinger's Crime: AI-generated Child Sexual Abuse Material as a Victimless Offense,* Master Thesis, Utrecht University, SN: 7465343.

Mehta, Divya et al. (2021): Child Maltreatment and Long-Term Physical and Mental Health Outcomes: An Exploration of Biopsychosocial Determinants and Implications for Prevention. *Child Psychiatry Hum Dev.,* 54(2): 421–435. doi: 10.1007/s10578-021-01258-8.

Némedi, Márk (2016): *Változások a gyermekpornográfia szabályozásában Magyarországon és az Európai Unióban*. Pisa, 7–8.: https://www.jogiforum.hu/publikaciok/816.

Orbán, Endre (2023): The Concept of Constitutional Identity as a Substantive Expression of the Principle of Subsidiarity, *Európai Tükör,* 2023/3, 23–42.

Petrini, Antonella – Belén Gauna, María (2024): Child Sexual Abuse Material provided by Artificial Intelligence, *EthAIca,* 3:123, DOI:10.56294/ai2024123.

Serebrennikova, Anna V. (2020): Harassment: criminal law concept, *Economic problems and Legal Practice,* Vol 16, No 3, 198–-201. https://journals.eco-vector.com/2541-8025/article/view/532605.

Somogyi Csilla (2025): A gyermekpornográfia felderítésének nehézségei, *Magyar Rendészet,* 2025/2. 103–123. DOI: 10.32577/MR.2025.2.7.

Somogyi Zsófia Borbála (2026): Gyermekvédelem, pedofília és szexuális bűncselekmények, *Belügyi Szemle,* 74(3), 663–682. https://doi.org/10.38146/bsz-ajia-ajia.2026.v74.i3.pp663-682.

Staksrud, Elisabeth (2013): *Children in the Online World, Risk, Regulation, Rights,* Farnham, Taylor & Francis, doi:10.4324/9781315571508.

Sulyok Tamás – Orbán Endre (2017): Az európai alkotmányos tér és az alkotmányos párbeszéd forgatókönyve. In Chronowski Nóra et al. (eds.): *A szabadságszerető embernek. Liber Amicorum István Kukorelli*. Budapest: Gondolat, 116–125.

Tóth Mercédesz (2025): In: Békés Ádám – Kurunczi Gábor – Pogácsás Anett – Varga Ádám (szerk.): *'A tudomány fényénél egyre tisztábban látunk…': A Zlinszky János Szakkollégium első két éve*. Budapest, Magyarország : Pázmány Press, 141–153.

Venier, Silvia (2022): Chapter 27 Positive Obligations under Human Rights Law to Protect against CBRN Risks, In: *International Law and Chemical, Biological, Radio-Nuclear (CBRN) Events* (eds: de Guttry, Andreas et al.), 481–500. DOI: https://doi.org/10.1163/9789004507999_028.

Viola, M. – Voto, C. (2023): Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. *Synthese,* 201, 30. https://doi.org/10.1007/s11229-022-04012-2.

Whittle, Helen – Hamilton-Giachritsis, Catherine – Beech, Anthony – Collings, Guy (2013): A review of young people's vulnerabilities to online grooming, *Aggression and Violent Behavior,* Volume 18, Issue 1, 135–146, https://doi.org/10.1016/j.avb.2012.11.008.