

KOKOLY ZSOLT  
OROSZ ANDREA

# A képmásvédelem jogi eszközei a deepfake jogsértő tartalmak esetében – a platformszabályozás novumai és a jogalkalmazás válaszai között

**Protecting One's Image Against Harmful Deepfake Content – Navigating Novelties in Platform Regulation and Legal Solutions by Law Enforcement**

**Abstract:** The paper examines the legal solutions against illegal online content created and broadcast using deepfake technologies, focusing on the interplay between personality rights (principally the right to one's image) and vulnerable groups (women). The extension of the normative framework for platform regulation by the European lawmaker (Digital Services Act, AI Act, completed by norms already in place like GDPR), as well as responses by national regulatory authorities offer the chance to assess the proficiency of these measures, confronting them with recent jurisprudential approaches. Nevertheless, the issue of deepfake pornography cannot be fully comprehended by studying various legal toolkit, as it represents an object of widespread social anxiety, and, as such, it goes beyond individual harm and poses a systemic risk in discriminating against social categories. Regulatory framework and public policies in the field of deepfake pornography (seen as a form of violence against women) are still evolving, but signal an ampler regime of preventive measures, completed by stricter regime of sanctions.

**Keywords:** deepfake, pornography, platform regulation, vulnerable groups, violence against women, AI

**Összefoglaló:** A tanulmány a deepfake technológiával készült és terjesztett jogsértő tartalmak elleni fellépés jogi lehetőségeit vizsgálja a személyiségi jogok (elsősorban a képmásvédelem) intézményére és egy sérülékeny csoportra (nők) gyakorolt hatását állítva fókuszba. A jogalkotói megoldások között vizsgáljuk a platformszabályozás új normatív rendelkezéseit (a digitális szolgáltatásokról és a mesterséges intelligenciáról szóló európai rendeletek, az európai adatvédelmi rendelettel kiegészítve), valamint a nemzeti szabályozó hatóságok intézményi válaszait, amelyeket a joggyakorlat alapján kristályosodó megoldások árnyalnak. A deepfake pornográfia kérdésköre ugyanakkor érdemben nem tárható fel kizárólag a jogi szabályozás alkalmazható/alkalmazandó eszközeinek vizsgálata révén, hiszen a jelenség a társadalmi aggályt keltő jelenségek közé tartozik, az egyéni személyiségi jogsértésen túlmutatóan társadalmi csoportokat képes hátrányos vagy kiszolgáltatott helyzetbe hozni. A kérdéskört övező szabályozási-közpolitikai keret még mindig képlékeny, azonban észlelhető a preventív

intézkedések hangsúlyosabbá válása, párhuzamosan a szankciók rendszerének kibővítésével és a deepfake cselekmények kriminalizálásával.

**Kulcsszavak:** deepfake, pornográfia, platformszabályozás, sérülékeny csoportok, nők elleni erőszak, mesterséges intelligencia

## 1. Bevezető

A deepfake technológiával való visszaélés nem új keletű, hiszen már az első deepfake technológiával létrejött videó is jogsértő tartalmat közvetített: erre 2017-ben került sor, amikor a Reddit-platform néhány felhasználója hamisított pornográf videókat készített azáltal, hogy mesterségesintelligencia-eszközök használatával hírességek arcát helyezték fel valódi pornográf videókra.<sup>1</sup>

Ami jelenleg akuttá tette a problémát, az a jogsértő tartalmak gyártását és terjesztését lehetővé tevő appok, beépített funkciók integrálása közösségimédia-oldalakra, az a jelenség, hogy a korábban fizetős vagy regisztráció alapú szolgáltatásként igénybe vett vagy a dark web felületén elérhető „meztelenítő” alkalmazások (nudifying apps), „pornó stílus funkciók” (pornifying features) 2025-ben már az online óriásplatformok szerkezetébe épülhettek be vagy reklámokat futtathatnak az óriásplatformok vagy keresők felületén, és ugyanolyan gyakori az oktatóvideók, tutorialok hirdetése arról, hogyan készíthet bárki otthon deepfake pornográf tartalmat.<sup>2</sup> Ugyanakkor ezen a ponton rendelkezésre áll már az uniós jogalkotó által kidolgozott platformszabályozás normatív kerete (elsősorban a digitális szolgáltatásokról<sup>3</sup> és a mesterséges intelligenciáról<sup>4</sup> szóló európai rendeletek, az európai adatvédelmi rendelettel<sup>5</sup> kiegészítve), amely tartalmaz a jogsértő deepfake tartalmakkal szembeni eljárásra vonatkozó rendelkezéseket.

1 Cellan-Jones, 2019.

2 Gondolunk itt az X (korábbi Twitter) óriásplatform Grok AI chatbotjára vagy a Meta felületein futó reklámokra, online tutorial hirdetésekre.

3 Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) PE/30/2022/REV/1. HL L 277., 2022. 10. 27, 1–102.

4 Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet) PE/24/2024/REV/1. HL L, 2024/1689, 2024. 07. 12.

5 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) HL L 119., 2016. 05. 04., 1–88.

Az uniós jogszabályi keretben kiemelten fontos a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről szóló irányelv átültetése,<sup>6</sup> amelyet 2027-re minden tagállamnak át kell ültetnie belső jogába, mivel különböző deepfake online tartalmak 99%-ban nőket ábrázolnak, míg a tartalomnak csak 1%-ában szerepelnek férfiak.<sup>7</sup> A deepfake videók 96%-a nem konszenzusos pornográf tartalomnak minősül, a deepfake pornográfia pedig az összes online deepfake videó 98%-át teszi ki.<sup>8</sup> A legnépszerűbb, szexualizált deepfake technológiával foglalkozó webhelyet havonta körülbelül 17 millióan látogatják – a tartalom alanyai pedig nők.

Mivel a deepfake technológiával való visszaélések nagyon széles távot fognak át, ebben az írásban kifejezetten azon deepfake technológiával készült és terjesztett jogsértő tartalmak elleni fellépés jogi lehetőségeit vizsgáljuk, amelyek a személyiségi jogok (elsősorban a képmásvédelem) intézményét érintik, egy sérülékeny csoportra (nőkre) gyakorolt hatását állítva fókuszba. A jogi szakirodalomban konszenzus van arra nézve, hogy a deepfake maga egy eszköz és nem a tartalom, azonban a technológia segítségével előállított tartalom vethet fel adatvédelmi, személyiségi jogi vagy büntetőjogi aggályokat.<sup>9</sup>

A képmásvédelemnek a deepfake pornográfiával szembeni többszintű jogi védelme nem merül ki a jogalkotói cselekményekben, hanem fejlesztő hatást gyakorol rá a jogalkalmazás és a bírói gyakorlat – ennek érdekében az esetjog és a szabályozói hatóságok intézményi fellépésének is vizsgáljuk néhány kiemelt jelentőséggel bíró mozzanatát.

---

## 2. Deepfake és AI – az online szexuális visszaélések egyik legaggasztóbb vetülete

A nők évek óta szembesülnek szexuális zaklatással az interneten, és a mesterséges intelligencia térnyerésével a jelenség rohamosan növekszik. A brit felsőház tagja, Charlotte Owen a deepfake visszaélést 2024-ben a „nők elleni erőszak új határának” nevezte – felvetése abba az irányba mozdul el, amely nemcsak a megosztást, hanem magát a létrehozást is kriminalizálja.<sup>10</sup>

Ez a fajta erőszak nem érint minden egyént egyformán, szinte teljes mértékben a nők jogait sérti. A nők, elsősorban közszereplők, gyakran szembesülnek deepfake képekkel és fenyegető üzenetekkel, megtévesztő vagy hamis információkat és képeket terjesztenek róluk. Ezeknek a képeknek, videóknak a terjedése világszerte rengeteg nőt

6 Az Európai Parlament és a Tanács (EU) 2024/1385 irányelve (2024. május 14.) a nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről. PE/33/2024/REV/1. HL L, 2024/1385, 2024. 05. 24.

7 Security Hero, 2025.

8 Badinszky, 2024, 18–38.

9 Lendvai, 2023, 121–138.

10 McGlynn, 2024.

és lányt használt és továbbra is használ ki. Az áldozatokra gyakorolt negatív hatás pedig káros a méltóságukra, a mentális egészségükre, képes önálló életvitelükben akadályozni őket, esetenként pedig az öngyilkosság gondolata is felmerül az áldozatokban.<sup>11</sup>

Jelentős különbséget jelent, hogy a hagyományos pornográf tartalmaktól eltérően a deepfake pornográfia esetében nem beszélhetünk beleegyezésről, ami egyenes utat jelent a személyiségi és más jogok megsértése felé, tételesen a képmással való visszaélés felé. Sem a pornósztárs esetében, sem az áldozat esetében, akinek a képét ebbe belekényszerítik, nem beszélhetünk konszenzusról, hiszen az áldozatok nem járulnak hozzá, hogy képmásukat ilyen módon használják fel.<sup>12</sup>

A technológia lehetővé teszi, hogy bárki beleegyezése nélkül szexuális tartalmak alanyává váljon, ami nemcsak a személyes integritás megsértését jelenti, hanem tággabb értelemben hatalmi pozíció fenntartását is egy adott társadalmi kategória fölött (ebben az esetben a férfiak hatalmi pozíciójának fenntartását a nők felett). A deepfake pornó ezenkívül a női test tárgyiasításának és kizsákmányolásának eszközeként is szolgál, ami tovább erősíti a nemek közötti hatalmi egyenlőtlenséget.<sup>13</sup>

A fentieket figyelembe véve, a cél jelen tanulmány keretén belül megvizsgálni, milyen módon történik a személyiségi jogok sérülése, amikor különböző platformokra deepfake pornográf tartalmakat töltenek fel, illetve milyen sajátosságokkal rendelkeznek ezek az oldalak, amelyek ezeket a tartalmakat tárolják. A hatálybalépésük óta eltelt idő azt is lehetővé teszi, hogy a DSA-AI Act-GDPR normatív keret platformszabályozási eszközeinek hatékonyságáról képet alkothassunk, és az is kiemelt fontossággal rendelkezik a kutatás tárgyában, hogy milyen jogorvoslati lehetőségek állnak az áldozatok rendelkezésére.

A nemzetközi és uniós normatívák vizsgálata mellett a belső jog doktrináris és joggyakorlati vonatkozásait összehasonlító jogi szempontból is vizsgáljuk, amelyben a román és a magyar jogalkotás és jogalkalmazás eredményeit hasznosítjuk.

---

## 3. A deepfake technológia az uniós jogszabályi környezetben

### 3.1. Az MI-rendelet (AI Act)

Az uniós jogalkotás 2024-ben hatályba léptetett, mesterséges intelligenciáról szóló jogszabálya (AI Act – MI Rendelet) három pilléren nyugszik: a rendszer emberközpontú, technológiásemleges és kockázatalapú, ezeket az elveket pedig különböző rendelkezések bontják ki részleteiben. A deepfake pornográfia szempontjából az első elv, azaz az emberközpontúság elve a leginkább releváns.<sup>14</sup>

A rendelet a harmadik csoportban, a korlátozott kockázatot képviselő megoldások között sorolja fel a generatív MI-megoldások egy részét, így a deepfake technológiát is.

11 Laffier és Rehman, 2023, 1–21.

12 McGlynn, 2024.

13 McGlynn, 2024.

14 Bővebben ld. Badinszky, 2024, 25.

A 134. preambulumbekzdésében az átláthatósági követelmények kapcsán rendelkezik a szintetikus tartalmak kötelező címkézéséről: „Az MI-rendszer szolgáltatói által alkalmazott műszaki megoldásokat illetően azon alkalmazóknak, akik MI-rendszert használnak olyan kép-, audio- vagy videótartalom létrehozására vagy manipulálására, amely érzékelhetően hasonlít meglévő személyekre, tárgyakra, helyekre, entitásokra vagy eseményekre, és egy személy számára megtévesztő módon autentikusnak vagy valóságosnak tűnhet (deep fake), egyértelműen és megkülönböztethetően fel kell tüntetniük, hogy a tartalmat mesterségesen hozták létre, vagy manipulálták az MI-kimenet megfelelő címkézésével és mesterséges eredetének közzétételével.”

Az MI Rendelet 3. cikkének 60. bekezdése nyújtja a deepfake definícióját: „az MI által generált vagy manipulált kép, audio- vagy videótartalom, amely hasonlít létező személyekre, tárgyakra, helyekre, entitásokra vagy eseményekre, és amely egy személy számára megtévesztő módon autentikusnak vagy valóságosnak tűnne”.

Az MI Rendelet deepfake rendelkezéseit a jogi szakirodalom több helyen hiányosnak, félreérthetően megfogalmazottnak tartja.<sup>15</sup> A nem konszenzuális deepfake tartalom létrehozása esetén a kár legtöbbször már a közzététellel bekövetkezik, hiszen a fizikai képmásnak a külvilágban történő ilyen materializálása megvalósítja a jogsérelmet, a kár jóvátételére pedig a reaktív intézkedések, szankciók kevésnek is bizonyulhatnak. Ennek érdekében magának a kárnak a megelőzése lehet az elérni kívánt cél, azaz a deepfake technológia jogellenes felhasználásainak elkerülése és a megakadályozásra irányuló intézkedések ösztönzése.<sup>16</sup>

### 3.2. A digitális szolgáltatásokról szóló európai rendelet (DSA)

A digitális szolgáltatásokról szóló, 2022-ben hatályba léptetett európai rendelet nem tartalmaz kifejezetten a deepfake tartalmakra vonatkozó rendelkezéseket, azonban jelentősége a jogellenes tartalmak eltávolítási gyakorlatának kidolgozásában, a tárhelyszolgáltatókra kirótt kötelezettségek rögzítésében válik relevánssá a kutatott téma szempontjából.

A DSA bejelentési és cselekvési mechanizmusokat biztosít, amelyek magasabb szintű fellépést jelentenek a jogellenes tartalmakkal szemben.

A 16. cikk. 1. bekezdésében a rendelet a következő kötelezettségeket rója a tárhelyszolgáltatókra: „A tárhelyszolgáltatók olyan mechanizmusokat alkalmaznak, amelyek lehetővé teszik bármely személy vagy szervezet számára az olyan konkrét, a szolgáltatás keretében elérhető információk bejelentését, amelyek a magánszemély vagy szervezet szerint jogellenes tartalomnak minősülnek. E mechanizmusoknak könnyen hozzáférhetőnek és felhasználóbarátnak kell lenniük, valamint lehetővé kell tenniük a bejelentések kizárólag elektronikus úton történő benyújtását.”

Az óriásplatformok és keresőprogramok feletti joghatóság teszi lehetővé, hogy az uniós jogalkotó eljárást indíthasson jogsértő online tartalmak esetében. Ugyanakkor a DSA a jogellenes tartalmak körét a lehető legtágabban határozza meg, a kritikai irodalom pedig a vonatkozó preambulumbekzdést úgy értelmezi, mint amelynek értelmében

<sup>15</sup> Badinszky, 2024, 28–30.

<sup>16</sup> Sorbán, 2020, 81–104.

az olyan tartalmak jogellenesek, amelyek nem felelnek meg az uniós jognak vagy bármely tagállam – az uniós joggal összhangban álló – jogának, azaz alapvetően az uniós jognak megfelelő nemzeti jogot kell figyelembe venni a jogellenesség megítélésakor. Ennek kapcsán értelmezési nehézséget vet fel azon jogszabályok körének azonosítása, amelyek bár tagállami jogszabályok, de nincsenek összhangban az uniós joggal.<sup>17</sup>

*„A biztonságos, kiszámítható és megbízható online környezet biztosítására vonatkozó célkitűzés elérése érdekében e rendelet alkalmazásában a 'jogellenes tartalom' fogalmának nagyjából az offline környezetre vonatkozóan létező szabályokat kell tükröznie. A 'jogellenes tartalom' fogalmát tágran kell meghatározni, olyan módon, hogy az kiterjedjen a jogellenes tartalmakkal, termékekkel, szolgáltatásokkal és tevékenységekkel kapcsolatos információkra. Így különösen ezt a fogalmat úgy kell értelmezni, hogy az – formájától függetlenül – olyan információkra utal, amelyek az alkalmazandó jog értelmében vagy önmagukban is jogellenesek – mint például a jogellenes gyűlöletbeszéd vagy a terrorista tartalom és a jogellenes megkülönböztető tartalom –, vagy azokat az alkalmazandó szabályok teszik jogellenessé, mivel jogellenes tevékenységekhez kapcsolódnak. Szemléltető példa lehet erre a gyermekek szexuális bántalmazását ábrázoló képek megosztása, a magánjellegű képek jogellenes, beleegyezés nélküli megosztása, az online követéses zaklatás, a nem megfelelő vagy hamisított termékek értékesítése, a fogyasztóvédelmi jogszabályokba ütköző termékek értékesítése vagy ilyen szolgáltatások nyújtása, a szerzői jogi védelemben részesülő anyagok engedély nélküli felhasználása, a szálláshely-szolgáltatások jogellenes kínálata vagy az élő állatok jogellenes értékesítése.”*

A 34. cikk 1. bekezdése részletezi a rendszerek (ideértve az algoritmikus rendszereket is) kialakításából vagy működéséből vagy a szolgáltatásaik használatából eredő rendszerszintű kockázatokat, d) pontja alatt pedig a nemi alapú erőszakkal, a közegészség és a kiskorúak védelmével összefüggő tényleges vagy előre látható negatív hatások, valamint a személyek testi és szellemi jóllétére gyakorolt súlyos negatív következmények vonatkozásait taglalja.

A 35. cikk a 34. cikkkel köthető össze, mivel újdonságként jelenik meg a 34. cikkben a manipulált kép, audio- vagy videótartalommal (például deepfake) kapcsolatos kockázatok csökkenése. A deepfake tartalmakkal kapcsolatos intézkedések: jelzés, tartalom megjelölésének lehetősége az igénybe vevők számára, emellett számos más intézkedési lehetőséget sorol fel.<sup>18</sup>

Az uniós jogalkotó első ízben 2025 decemberében rótt ki büntetést a DSA alapján óriásplatformra.<sup>19</sup> A szankcióval illetett óriásplatform, az X (korábbi Twitter) deepfake pornográfiának minősíthető AI-chatbotja miatt ugyanakkor 2026 januárjában kivizsgálást is indított.<sup>20</sup>

A kivizsgálást az követelte meg, hogy az X óriásplatform AI chatbotja „pornográf stílusú” tartalom generálását lehetővé tevő funkciót nyújtott a felhasználók rendelkezésére.

17 Koltay et al., 2024, 27–28.

18 Koltay et al., 2024.

19 *Commission fines X €120 million under the Digital Services Act* [Online]. Elérhető: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_25\\_2934](https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934) (letöltés ideje: 2026. 01. 28.).

20 *Tackling AI deepfakes and sexual exploitation on social media* [Online]. Elérhető: <https://www.europarl.europa.eu/news/en/agenda/plenary-news/2026-01-19/8/tackling-ai-deepfakes-and-sexual-exploitation-on-social-media> (letöltés ideje: 2026. 01. 28.).

A Grok Imagine az előfizetéssel rendelkező felhasználóknak lehetővé tette, hogy a segítségével explicit képeket és videókat is készíthessenek. A rendszer szöveges utasítások és feltöltött képek alapján is képes szexuális tartalmú fotókat és videókat generálni, olyat is, amelyeken bizonyos mértékű meztelenség is látható (ezek egy részét moderálva látatja). Ezek egy részét moderálva (elhomályosítva) adja ki a rendszer.

A Grok chatbot által lehetővé tett funkció miatt heves vita indult, több országban korlátozták a platformhoz való hozzáférést, máshol pedig kivizsgálás indult a „pornográf stílust generáló” (pornification feature) vagy meztelenítő alkalmazásokat (nudifying apps) nyújtó szolgáltatók ellen, mivel ez a nők és kiskorúak esetében súlyos kockázati tényezőnek minősülhet. A Bizottság elítélte az X óriásplatform által bevezetett szexualizált képeket generáló funkciót, és elrendelte a chatbotra vonatkozó anyagok lefoglalását a kivizsgálás idejére.

### 3.3. Az általános európai adatvédelmi rendelet (GDPR)

Mivel 2016 óta alkalmazandó, az általános európai adatvédelmi rendelet nem tartalmazhatott a deepfake tartalmakra vonatkozó előírásokat, azonban a személyes adatok különleges kategóriáinak kezelésére vonatkozó rendelkezés vonatkoztatható erre is: 9. cikkének 1. bekezdésében a GDPR tiltja az alábbi személyes adatok kezelését: *„A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.”*

A GDPR által megkövetelt, a kezeléshez szükséges jogalap a nem konszenzuális deepfake tartalmak esetén értelemszerűen hiányzik: az érintett személy részéről nem beszélhetünk beleegyezésről, a létrehozó vagy harmadik személy jogos érdekéről sem.

A deepfake tartalmak akkor kerülhetnek a GDPR hatálya alá, hogyha a 9. cikk értelmében vett személyes adatok különleges kategóriájába tartozónak tekintjük, azaz amikor a deepfake biometrikus adatokat (képmás, hang) közöl a céllal, hogy a személlyel azonosítható váljék. A GDPR 51. preambulumbekkezdése értelmében a fényképek kezelését nem szükséges szisztematikusan különleges adatkezelésnek tekinteni, mivel azokra csak azokban az esetekben vonatkozik a biometrikus adatok fogalom meghatározása, amikor a természetes személy egyedi azonosítását vagy hitelesítését lehetővé tevő speciális eszközzel kezelik őket. *„Az ilyen adatok nem kezelhetők, kivéve, ha az adatkezelés az e rendeletben meghatározott egyedi esetekben megengedett, azt is figyelembe véve, hogy a tagállami jog különös rendelkezéseket állapíthat meg az adatok védelmére vonatkozóan annak érdekében, hogy kiigazítsák az e rendeletben foglalt szabályok alkalmazását valamely jogi kötelezettségnek való megfelelés vagy közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása tekintetében.”*

A képmásvédelem, online platformok és preventív intézkedések kötelezettsége összefüggésében az adatvédelmi jogi esetjog szolgáltató fontos fogódzót: a C-492/23

sz. ügyben<sup>21</sup> hozott ítéletében az Európai Bíróság kimondta, hogy az online platformok felelősséggel tartoznak a közzétett hirdetésekért, ekképpen meg kell vizsgálniuk, hogy tartalmazznak-e különleges adatokat, a felhasználók által beküldött tartalomról van-e szó, amennyiben igen, akkor le kell ellenőrizni, hogy megegyezik-e azzal a személlyel, akinek az adatai szerepelnek a tartalomban.

Az ügy alapeljárása nem deepfake pornográfia, hanem egy másik, a bosszúporno-hoz (revenge porn) hasonló jelenség, a bosszúhirdetés (revenge listing, revenge sexual ad) tényállását valósította meg: képmását és telefonszámát közzétéve, a hamis hirdetés, amely szexuális szolgáltatások nyújtását tulajdonította meg, megsértette a képmáshoz, a becsülethez és a magánélethez való jogát. Az online piactér üzemeltetője közösen felel a hirdetővel, mert közös adatkezelőnek minősülnek, és megfelelő biztonsági intézkedéseket kell bevezetniük annak érdekében, hogy ilyen jellegű tartalmakat ne lehessen átvenni, tovább terjeszteni.

Kiemelkedően fontos a spanyol adatvédelmi hatóság 2026. januári döntése, amely első ízben büntette az AI segítségével generált szexuális töltetű képek generálását és terjesztését.<sup>22</sup>

Az ügyben a meztelenítő appok használata és ezek segítségével létrehozott, valamint a közösségi médiában, felnőtt tartalmakat kínáló platformokon és csevegőprogramokban terjesztett jogellenes tartalmak miatt döntött a hatóság a büntetés kiszabásáról. Az ítélet érvelésében a spanyol szabályozó hatóság kimondta, hogy az ilyen típusú tartalmak nem tekinthetők egyszerű digitális montázsoknak, hanem személyes adatkezelésként kell elbírálni őket. Mivel a GDPR egyéni azonosítónak tekinti a személy képmását (arcképét és hangját), ezeknek a képeknek a digitális manipulálása (létrehozás, módosítás és ezt követően terjesztés) az adatvédelmi jog értelmében személyes adatkezelésnek minősül. További érv, hogy – amint fentebb is említettünk – nem konszenzuális deepfake tartalmak esetén nem beszélhetünk beleegyezésről, jogalapról vagy olyan törvényes érdekről, amely felülírná a célszemély jogait.

### 3.4. A nőkkel szembeni erőszak és a kapcsolati erőszak ellen szóló irányelv (EU) 2024/1385

Annak ellenére, hogy a nőkkel szembeni erőszak és a kapcsolati erőszak elleni irányelv átültetési határideje 2027, fontosnak tartottuk ebben a fejezetben ezt az uniós jogi aktust is megemlíteni – egyrészt, mivel abból a feltételezésből indultunk ki, hogy a deepfake pornográfia a nők elleni erőszak egyik manifesztációjának tekinthető, másrészt mivel a normaszöveg kifejezetten tartalmaz a deepfake tartalmakra vonatkozó rendelkezéseket.

A 3. preambulum bekezdésében az irányelv kimondja, hogy „a nőkkel szembeni erőszak és a kapcsolati erőszak sérti a Chartában és a gyermek jogairól szóló ENSZ-egyezményben

21 C492/23. sz. ügy X kontra Russmedia Digital SRL és Inform Media Press SRL. ECLI:EU:C:2025:935

22 El uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos visibles e invisibles [Online]. Elérhető: <https://www.aepd.es/guias/guia-aepd-uso-de-imagenes-de-terceros-en-sistemas-ia.pdf> (letöltés ideje: 2026. 01. 28.).

*foglalt olyan alapvető jogokat, mint az emberi méltósághoz való jog, a személy életéhez és sértetlenségéhez való jog, az embertelen vagy megalázó bánásmód vagy büntetés tilalma, a magán- és családi élet tisztelgetben tartásához való jog, a szabadsághoz és biztonsághoz való jog, a személyes adatok védelméhez való jog, a – többek között nemi alapon történő – megkülönböztetéstől való mentesség joga, valamint a gyermekek jogai.”*

Az 5. preambulumban bekezdésében felmerül a nőkkel szembeni erőszak sajátos jellege, amely átfogó igényű és célzott hatással bíró szabályokat követel meg: *„A nőkkel szembeni erőszak és a kapcsolati erőszak bűncselekményeihez kapcsolódó sajátosságokra tekintettel átfogó szabályokat kell megállapítani, amelyek célzottan kezelik a nőkkel szembeni erőszak és a kapcsolati erőszak továbbra is fennálló problémáját, és kielégítik az ilyen erőszak áldozatainak sajátos szükségleteit.”*

A deepfake tartalmak generálását és terjesztését, a jelenség szélesebb társadalmi negatív hatását és a fokozott védelem beiktatásának indokait a 19. cikk részletezi: *„Különösen a könnyű, gyors és széles körű terjesztést és elkövetést lehetővé tévő jellege, valamint intim jellege miatt a kifejezetten szexuális tevékenységeket vagy egy személy intim testrészeit ábrázoló képek, videók vagy hasonló anyagok IKT révén történő hozzáférhetővé tétele a nyilvánosság számára az említett személyek beleegyezése nélkül nagyon káros lehet az áldozatokra nézve. Az ezen irányelvben meghatározott releváns bűncselekménynek ki kell terjednie az ilyen anyagok valamennyi típusára, így a képekre, fényképekre és videókra, beleértve a szexualizált képeket, hangklipet és videoklipet is. Olyan helyzetekre kell kiterjednie, amikor az anyagnak a nyilvánosság számára az IKT révén történő hozzáférhetővé tétele az áldozat beleegyezése nélkül történik, függetlenül attól, hogy az áldozat beleegyezett-e az ilyen anyagok létrehozásába, vagy adott esetben továbbíthatta azt egy adott személynek. A bűncselekménynek ki kell terjednie az anyag beleegyezés nélküli előállítására vagy – például többek között mesterséges intelligenciát használó képszerkesztéssel történő – manipulálására vagy módosítására is, amelynek köszönhetően úgy tűnik, mintha egy személy szexuális tevékenységet folytatna, amennyiben az anyagot ezt követően IKT révén, az adott személy beleegyezése nélkül hozzáférhetővé teszik a nyilvánosság számára. Az ilyen előállítás, manipuláció vagy módosítás alá kell tartoznia a 'deepfake' előállításának is, amelynek esetében az anyag egyértelmű egyezést mutat egy létező személlyel, tárggyal, helyszínnel vagy más alánnyal vagy eseménnyel, egy személy szexuális tevékenységeit ábrázolja, és más személyekben azt a téves benyomást keltheti, hogy az anyag hiteles vagy valódi. Az áldozatoknak az ilyen magatartástól való hatékony védelme érdekében a szabályozásnak az ilyen magatartással való fenyegetésre is ki kell terjednie.”*

Az Irányelv egyik érdeme annak felismerése, hogy a kibertérben elkövetett erőszakos cselekményeket egységben fogja össze: ez a preambulumban is részletezett igénynek a megnyilvánulása, amely a sajátos jelleg és célzott hatás alapján gondolkodik jogi megoldásokban. A normaszöveg itt egyben tárgyalja az intim vagy manipulált anyagok nem beleegyezésen alapuló megosztását, 5. cikke 1. bekezdésében megkövetelve, hogy az alábbi szándékos cselekmények bűncselekményként büntetendők legyenek:

*a) „kifejezetten szexuális tevékenységeket vagy egy személy intim testrészeit ábrázoló képek, videók vagy hasonló anyagok információs és kommunikációs technológiák (a továbbiakban: IKT) révén történő hozzáférhetővé tétele a nyilvánosság számára az említett személy beleegyezése nélkül, amennyiben az ilyen cselekmény súlyos kárt okozhat az érintett személynek”;*

b) „IKT révén képek, videók vagy hasonló anyagok előállítása, manipulálása vagy megváltoztatása azt a benyomást keltve, hogy egy másik személy kifejezetten szexuális tevékenységet folytat, majd ezt követően az anyagok hozzáférhetővé tétele a nyilvánosság számára az említett személy beleegyezése nélkül, amennyiben az ilyen cselekmény súlyos kárt okozhat az említett személynek.”

Az Irányelv normaszövege a deepfake pornográf tartalmakat generáló jogsértő magatartást egységben látta olyan kriminalizálandó cselekményekkel, mint az internetes fenyegető zaklatás (cyber-stalking), internetes zaklatás (cyber-bullying) és az erőszakra vagy gyűlöletre való internetes uszítás (cyber-incitement).

---

## 4. A deepfake technológia és az alkalmazás által felvetett potenciális jogsértések – a manipulált tartalmak és az alapjogok viszonya

### 4.1. A deepfake által veszélyeztetett személyiségi jogok védelme a román nemzeti jogban

Románia Polgári Törvénykönyvének (Rptk.) az emberi lény és veleszületett jogainak tiszteletben tartására vonatkozó szabályozása a személyeket tárgyaló I. könyvben, a természetes személyről szóló II. címében található (58–81. cikkek). A természetes személyről szóló II. Cím II. Fejezete Az emberi lény és veleszületett jogainak tiszteletben tartása címet viseli és négy szakaszt ölel fel, melyek a természetes személy életéhez, egészséghez és testi épséghez való jogát, a magánélet és a személy méltóságának tiszteletben tartását, valamint a halottnak járó tisztelet kérdését tárgyalják. Az Rptk. megerősíti a magánélet védelmét, a véleménynyilvánítás szabadságát, ez pedig a személyes és családi életbe történő beavatkozásmentességet, a lakhely és levelezés sértetlenségét jelenti. Ezek a jogok csak a törvényben előírt esetekben korlátozhatók. A törvény szerint minden személyt megillet a saját képmáshoz való jog, melynek értelmében a személy megtilthatja vagy megakadályozhatja fizikai megjelenésének vagy hangjának bármilyen módon történő reprodukálását.<sup>23</sup>

A román Alkotmány az emberi méltóságot is védi, és mint legfőbb alkotmányos értéket jelöli meg, amelyről a Rptk. 72. cikke rendelkezik: „(1) Mindenkinek joga van méltósága tiszteletben tartásához. (2) Tilos valamely személy becsületét és hírnevét sérteni ennek beleegyezése vagy a 75. cikkben előírt korlátok betartása nélkül.” A becsület alatt az emberi lény olyan veleszületett tulajdonságát értjük, mely a természetes személyek közötti érintkezésben az érzelmek széles spektrumát, egy adott személynek az önmagáról alkotott felfogását öleli fel. A jó hírnév egy adott személy közvélemény általi megítélését jelenti, amely összhangban áll a személy társadalmi szerepével. A jó hírnév sérelme

<sup>23</sup> Kokoly, 2021, 69.

akkor következik be, ha valaki más személyre vonatkozó, azt sértő valótlan tényt állít, hírszél, vagy valós tény hamis színben tüntet fel.

A magánélethez való jogról, illetve ennek a jognak a gyakorlásáról és korlátairól az Rptk. 71. cikke rendelkezik. *„(1) Mindenkinek joga van a magánélet tiszteletben tartásához. (2) Senki sem vethető alá magán-, személyi vagy családi életébe, lakhelyére, tartózkodási helyére vagy levelezésébe történő beavatkozásnak az illető személy beleegyezése vagy a 75. cikkben előírt korlátok nélkül. (3) Tilos továbbá a levelezés, kéziratok vagy más személyes dokumentumok, valamint a személy magánéleti információinak bármilyen módon történő felhasználása az illető személy beleegyezése vagy a 75. cikkben előírt korlátok betartása nélkül.”* A 71. cikk értelmezése egy szélesebb értelemben vett intim magánterületet jelöl, amely felett az egyén kizárólagos jogokkal rendelkezik, és az indokolatlan behatolást mind a polgári jogi normák, mind az Alkotmány tiltja.

A képmás védelme kapcsán az Rptk. 73. cikke rögzíti: *„(1) Mindenkinek joga van a saját képmásához. (2) A saját képmáshoz való jog gyakorlásában az érintett személy megtilthatja vagy megakadályozhatja fizikai megjelenésének vagy hangjának bármilyen módon történő reprodukálását, illetve adott esetben az ilyen reprodukció felhasználását. A 75. cikk rendelkezéseit értelemszerűen kell alkalmazni.”*

Következtetésképpen elmondható, hogy Romániában az alapjogvédelem létezik és működik. A román jogrendszerben az emberi lény és a veleszületett jogaink tiszteletben tartása alapvető jogként jelenik meg, amit a jogrendszer átfogóan véd. Romániában a deepfake tartalmak áldozatainak jogai a meglévő személyiségi jogi védelem keretében érvényesülnek.

## 4.2. Alapjogvédelem a magyar jogrendszerben

Az alapjogok védelme, mint ahogy a magyar állam Alaptörvénye I. cikkében megfogalmazott elsőrendű kötelezettsége, a demokratikus jogállam működésének alapelve. Az alapjogok védelme jogi garanciákat biztosít az állampolgárok számára, az államnak pedig kötelezettséget. A személyiségi jogok között kiemelt szerepet kap a képmás védelme, amelyet a Polgári Törvénykönyv (Ptk.) is szabályoz.

A Ptk. 2:43. §-a kimondja, hogy mindenkinek joga van ahhoz, hogy a képmása és hangja védelmet élvezzen, és hogy mások csak a beleegyezésével készíthessenek vagy használhassanak fel ilyen felvételeket. A képmáshoz való jog az egyén személyiségének egyfajta kifejeződése, amely a személy intim szféráját érinti.<sup>24</sup>

Ezeknek a jogoknak a jogszerű felhasználás legfontosabb jogalapja a személy beleegyezése. A Ptk. szerint a képmás- vagy hangfelvétel elkészítése akkor jogszerű, ha azt az érintett személy engedélyezte. A beleegyezés akkor érvényes, ha az egyértelműen kifejezett beleegyezésen alapul és nem csupán hallgatólagos beleegyezésen, biztosítva az egyén számára, hogy szabad akaratából döntsön arról, hogy képmása vagy hangja rögzítésre vagy annak felvétele felhasználásra kerüljön. Mindezekből egyértelműen következik, hogy ilyen tartalmak jogellenes készítése vagy felhasználása a személyiségi jogok súlyos megsértésének minősül.

24 Boronkay, 2013, 111–132.

A jogellenes cselekmények, mint például a deepfake technológia használata által keletkezett jogsérelmek, nemcsak a képmáshoz való jogot sértik, hanem az emberi méltóságot is, amelyről az Alaptörvény II. cikke rendelkezik. Az emberi méltósághoz való jog megkülönbözteti az embert a jogi személyektől, az étellel együtt jár, oszthatatlan, korlátozhatatlan és egyenlő mindenkire nézve. Az emberi méltóság az a jogintézmény, amelytől fogva a személy emberi lény marad, és nem válhat eszközzé vagy tárgygyá. Az emberi méltóság elismerésével a jog a másik ember iránti minimális, őt emberi mivoltánál fogva megillető tiszteletet, elismerést követeli meg. Az emberi méltóság védelme és biztosítása az egész jogrend feladata.<sup>25</sup>

Az Alaptörvény kimondja a II. cikkben, hogy: „Az emberi méltóság sérthetetlen. Minden embernek joga van az élethez és az emberi méltósághoz, a magzat életét a fogantatástól kezdve védelem illeti meg.” A 8. § (1) bekezdése szerint a Magyar Köztársaság elismeri az ember sérthetetlen és elidegeníthetetlen alapvető jogait, ezek tiszteletben tartása és védelme az állam elsőrendű kötelessége.<sup>26</sup> Az emberi méltósághoz való jog az Alkotmánybíróság korábbi Alkotmányhoz kapcsolódó gyakorlatában a személyiségfejlődést védő relatív jogként jelenik meg (általános személyiségi jogként), másrészt szűkebb értelemben az emberi lét alapvető feltételeit védő, az alapjogi rendszert megalapozó abszolút jogot jelenti.<sup>27</sup> Egyes szakirodalmi források szerint „az emberi méltósághoz való jog azt jelenti, hogy van az egyén autonómiájának, önrendelkezésének egy olyan mindenki más rendelkezése alól kivont magja, amelynél fogva – a klasszikus megfogalmazás szerint – az ember alany marad, s nem válhat eszközzé vagy tárgygyá. A méltósághoz való jognak ez a felfogása különbözteti meg az embert a jogi személyektől, amelyek teljesen szabályozás alá vonhatók, nincs érinthetetlen lényegük.”<sup>28</sup>

A becsület és a jó hírnév védelme szintén fontos elemei a személyiségi jogoknak. A Ptk. 2:45. §-a a becsülethez és jó hírnévhez való jogot is védelem alá vonja. Az (1) bekezdés kimondja: „A becsület megsértését jelenti különösen a más személy társadalmi megítélésének hátrányos befolyásolására alkalmas, kifejezőmódjában indokolatlanul bántó véleménynyilvánítás. (2) A jó hírnév megsértését jelenti különösen, ha valaki más személyre vonatkozó és e személyt sértő, valótlan tényről állít vagy híresztel, vagy valós tényről hamis színben tüntet fel.”

Összességében megállapítható, hogy a deepfake tartalmak, amennyiben beleegyezés nélkül kerülnek elkészítésre és megosztásra, a magyar jogrendszerben jogellenesek, és a személyiségi jogok súlyos megsértését jelentik. Az érintett személy képmáshoz való joga, emberi méltósága, becsülete és jó hírneve egyaránt súlyosan sérülhet. Az állam elsőrendű kötelessége, hogy ezeket a jogokat az Alaptörvényben és a Ptk.-ban foglaltak szerint védje, és hogy a jogrendszer alkalmazkodjon a technológiai újításokhoz, biztosítva az áldozatok jogainak érvényesülését.

25 Kis, 2022, 67–85.

26 36/2000. (X. 27.) AB határozat.

27 Zakariás, 2019, 542.

28 Zakariás, 2019, 550.

### 4.3. Az alapjogvédelem nemzetközi jogi aspektusai

Az emberi méltóság sérthetatlensége és a személyiségi jogok védelme számos nemzetközi és európai jogi dokumentumban szerepet kap.

Az Egyesült Nemzetek Alapokmányának preambuluma az emberi méltóságot feltétlen érvényesülést kívánó elvként rögzíti, amely már itt az emberi jogokkal szoros összefüggésben jelent meg. Az Emberi Jogok Egyetemes Nyilatkozatának preambuluma is hangsúlyozza, hogy *„az emberiség családja minden egyes tagja méltóságának, valamint egyenlő és elidegeníthetetlen jogainak elismerése alkotja a szabadság, az igazság és a béke alapját a világon”*, ezért az 1. cikkében az emberi méltóság átfogó védelmét biztosítja, kimondva, hogy: *„Minden emberi lény szabadon születik és egyenlő méltósága és joga van.”*<sup>29</sup>

A Polgári és Politikai Jogok Nemzetközi Egyezségokmánya a preambulumban kifejezésre juttatta, hogy az emberi méltóság az emberi jogok alapja, kiemelve, hogy *„az emberi közösség valamennyi tagja veleszületett méltóságának, valamint egyenlő és elidegeníthetetlen jogainak az elismerése”*. Továbbá kimondta: *„ezek a jogok az emberi lény veleszületett méltóságából erednek”*.<sup>30</sup> A leírtakkal pedig szoros összefüggésben van az Emberi Jogok Európai Egyezményének rendszere,<sup>31</sup> amelyben megkülönböztethetjük az abszolút, erős és minősített jogokat. Az abszolút jogok az ember létét és méltóságát a legkomolyabb támadásoktól védik. Az Egyezmény 8. cikke 1. bekezdésében kimondja, hogy: *mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.*<sup>32</sup>

### 4.4. Alapjogvédelem az uniós jogban

Az Európai Unió Alapjogi Chartája 1. cikke is tartalmazza az emberi méltóság sérthetatlenségét, amit tiszteletben kell tartani és védelmezni kell: *„Az emberi méltóság sérthetetlen. Tiszteletben kell tartani, és védelmezni kell.”*<sup>33</sup>

Az Európai Unió Bírósága kimondta: *„Az Európai Unió Bíróságának kötelessége az intézmények jogi aktusai és a közösségi jog általános alapelvei összhangjának vizsgálata során az emberi méltósághoz és a személyi sérthetatlenséghez való jog biztosítása.”*<sup>34</sup>

### 4.5. A deepfake és az általa megvalósítható magyar és román büntetőjogi tényállások

Egyes esetekben a deepfake tartalmak létrehozása vagy terjesztése büntetőjogi felelősségre vonást vonhat maga után. Ezek a tartalmak magukban foglalhatják a személyazonosság-lopást, az internetes zaklatást vagy a csalást, rágalmazást, a becsület és a hírnév csorbitását.

29 Zakariás, 2019, 539.

30 Zakariás, 2019, 40.

31 Dudás, 2021, 55–56.

32 Egyezmény az emberi jogok és alapvető szabadságok védelméről, Róma, 1950. november 4., 8. cikk.

33 Európai Unió, Alapjogi Charta, Hivatalos Lap C 303/17 – 14.12.2007. I. cím 1. cikk.

34 Zakariás, 2019, 39.

Magyarországon és Romániában is egyaránt fontos kérdés, hogy a deepfake által okozott sérelmek milyen büntetőjogi tényállásokat merítenek ki. Magyarországon a Büntető Törvénykönyv (Btk.) nem tartalmaz kifejezetten a deepfake tartalmak feltöltésére, készítésére vonatkozó tényállásokat, viszont a meglévő jogszabályok alapján zaklatás, becsületsértés, rágalmozás stb. esetén felelősségre lehet vonni az elkövetőt. Romániában a törvénytervezet stádiumában rekedt meg egy javaslat, amely kifejezetten a deepfake tartalmakra vonatkozott volna.<sup>35</sup>

A deepfake tartalmak a becsület csorbítására is alkalmasak, amely mély nyomot hagyhat az áldozatban, és a társadalmi szerepére is hatással van. A becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítéséről a Btk. 226/A paragrafusá rendelkezik:

*„(1) Aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt készít, ha más bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő. (2) A büntetés három évig terjedő szabadságvesztés, ha a bűncselekményt a) nagy nyilvánosság előtt, vagy b) jelentős érdeksérelmet okozva követik el.”*

Ehhez pedig szorosan kapcsolódik a 227. §, mely kimondja: *„(1) Aki a 226. §-ban meghatározottakon kívül mással szemben a) a sértett munkakörének ellátásával, közmegegyezésének teljesítésével vagy közérdekű tevékenységével összefüggésben vagy b) nagy nyilvánosság előtt a becsület csorbítására alkalmas kifejezést használ, vagy egyéb ilyen cselekményt követ el, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő. (2) Az (1) bekezdés szerint büntetendő, aki a becsületsértést tettelesen követi el.”*

A román Büntető Törvénykönyv (Rbtk.) számos olyan tényállást tartalmaz, amelyek ezekre a jogsérelmekre alkalmazhatóak, ilyen például a 226. cikke, mely rendelkezik a magánszféra, magánélet megsértéséről: *„(1) A magánszféra jogtalan megsértése, ha valaki lakásban vagy ahhoz tartozó helyiségben vagy melléképületben tartózkodó személyt vagy magánbeszélgetést fényképez, képet vagy képfelvételt készít, technikai eszközzel lehallgat vagy hangfelvételt készít, egy hónaptól hat hónapig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő. (2) A (2) bekezdésben említett hangok, beszélgetések vagy képek jogtalan terjesztése, sugárzása, bemutatása vagy továbbítása.”*

A zsarolás is fontos tényállás, amelyet az MI-technológia segítségével könnyen el lehet követni, például a kompromittáló tartalmak terjesztése. A zsarolásról az Rbtk. a következőképpen rendelkezik 194. cikkében: *„(1) Aki erőszakkal vagy fenyegetéssel kényszerít valakit arra, hogy valamit adjon, tegyen, ne tegyen vagy tűrjön, ha a bűncselekményt azért követik el, hogy saját vagy más javára jogtalan előnyhöz jusson, 6 hónaptól 5 évig terjedő szabadságvesztéssel büntetendő. (2) Ha a kényszerítés abban áll, hogy a megfenyegetett személyt, házastársát vagy közeli hozzátartozóját kompromittáló valós vagy vélt tény felfedésével fenyegetik, a büntetés több évig terjedő szabadságvesztés.”*

35 Propunere legislativă privind interzicerea utilizării malițioase a tehnologiei și limitarea fenomenului Deepfake (Falsul Sever), Senat, L295/2023: 463/08.05.2023. A törvényjavaslat elfogadása ebben a formában nem valószínűsíthető.

## 5. Nők és női jogok a deepfake pornográfia árnyékában

Szükséges kifejtenuk ennek a jelenségnek a nőkre és a női jogokokra nézve felmerülő fokozott veszélyességét, valamint a beleegyezés hiányának következményeit és fontos aspektusait.

### 5.1. Női jogok és a deepfake pornográfia

A deepfake és a mesterséges intelligencia által létrehozott manipuláció térhódításával aránytalanul megnőtt a negatív következmények és a célzott károkozás aránya, amellyel a nők szembesülnek a férfiakhoz képest. Ezek a következmények magukban foglalják a meglévő nemek közötti egyenlőtlenségek felerősödését, valamint a nők és testük tárgyiasítását és árucikké tételét. A deepfake-ek ilyen használata gyakran együtt jár a káros nemi sztereotípiákkal.

A Center for International Governance Innovation (CIGI)<sup>36</sup> által 2020-ban, 18 országban, 18 149 résztvevővel végzett online károkozásról szóló nemzetközi felmérésből kiderült, hogy a válaszadók 60%-a tapasztalt legalább egyet az online károkozás 13 formája közül. A vizsgált online ártalmak közül az intim képek nem beleegyezésen alapuló használata volt a leginkább károsnak tartott incidens, különösen a nők esetében.

A mesterségesintelligencia-alapú technológiák megnövekedett hozzáférése és gyors elterjedése miatt fennáll annak a veszélye, hogy a deepfake tartalmak az ilyen típusú bűncselekmények hatékony és veszélyes eszközévé válnak, mivel az elkövetőnek már nincs szüksége hiteles tartalomra, hanem olyan minőségben tudja előállítani, amely növeli annak valószínűségét, hogy az emberek valódinak hiszik. Az is megállapítható, hogy az áldozatok rendkívül kiszolgáltatott helyzetben vannak, mivel nehéz cáfolni ezeknek a videóknak a hitelességét, és a teljesen eltávolítás a kibertérből a nagy elterjedést követően szinte lehetetlen.<sup>37</sup>

### 5.2. Az egyes videómegosztó platformok által okozott jogsérelmek

A deepfake pornográfia használata azért is aggályos, mert a tartalom előállítói olyan anyagokat hoznak létre, amelyek a nők megszégyenítését, megalázását, lelki vagy akár fizikai bántalmazását keltik életre, és sokszor ezekhez a tartalmakhoz az erőszak támogatása is párosul.

A videómegosztó platformok működtetői a deepfake technológia megjelenése után röviddel felismerték a profitszerzési lehetőséget az ilyen tartalomgyártásban – az első alkalmazások már 2019-ben működőképeseek voltak.

Az első „meztelenítő” app 2019-ben már rendelkezésre állt (DeepNude néven), és lehetővé tette a felhasználók számára, hogy „meztelen” fotókat készítsenek felöltözött nőkről. Az algoritmusok nem tudtak hasonló fordítást végezni férfiak képein, mivel kifejezetten nők képein képezték ki őket. Ez a jelenség rávilágít a nemi alapú

<sup>36</sup> Dunn, Vaillacourt és Brittain, 2023.

<sup>37</sup> Hidalgo, 2023.

megkülönböztetés és a nők elleni erőszak rendszerszintű veszélyeire. Az alkalmazás eredetileg demó és letöltési lehetőséggel indult asztali számítógépes alkalmazásként (a letöltés ingyenes volt, azonban a generált képeket nagy vízjel takarta, amelynek eltávolításáért 50 dollárt lehetett fizetni). Az alkalmazás a fizetős verzióban is megőrzött egy kis vízjelet, amely címkézte a kép hamisítvány voltát.

A MrDeepfakes az egyik legnagyobb deepfake tartalmat kínáló pornóoldala, amely több mint 14 milliós havi látogatottsággal rendelkezik. „*Hírességeket ábrázoló deepfake pornócsatorna oldal*”-ként határozza meg magát, ahol a látogatók megtekinthetik a hírességek szexuális deepfake-eit, vásárolhatnak és eladhatnak deepfake-eket, és részt vehetnek a deepfake-ek készítésével kapcsolatos közösségi vitákban.

Az oldal felhasználói szabályzata rögzíti, hogy csak olyan szexuális deepfake tartalmakat engedélyez, amelyek hírességeket ábrázolnak. A weboldal szabályai többek között előírják, hogy a hírességnek „jelentős befolyással” kell rendelkeznie a közösségi médiában, több mint 200 ezer követővel a TikTok-on vagy 100 ezer követővel az Instagramon, YouTube-on, Twitteren vagy Twitchen. Viszont e szabályok mellett vannak olyan személyek, akik nem érik el ezeket a küszöbértékeket. Sok célszemély esetében nem található online jelenlét, továbbáknál pedig nem találhatóak olyan profilok a felsorolt közösségimédia-platformok egyikén sem, amelyek megfeleltek volna a következő minimális kritériumoknak.

A Motherless.com a felhasználók által létrehozott tartalomplatformok néven ismert webhelyek csoportjába tartozik, amely lehetővé teszi a felhasználók számára, hogy saját tartalmaikat töltsék fel a közönség számára.<sup>38</sup> Az oldal csak a dark weben volt elérhető, és magyar nőkről illegálisan megszerzett képekből álló állományt tartalmazott. A weboldal magyar influencerek és más nők levadászására és megkínzására buzdította a férfiakat. A tartalmak pornográf jellegűek is voltak, a forrásként használt képek egy része utcai környezetben, tömegközlekedési eszközökön vagy nyilvános WC-ben illegálisan elhelyezett kamerákkal készült. Arra is volt példa, hogy ablakon keresztül befényképezve, intim helyzetben lévő vagy zuhanyzó nőket mutattak.

A deepfake képek létrehozása mellett a platformra feltöltötték az ábrázolt nők személyes adatait is (név, közösségimédia-profilok neve), ami jelentősen megnövelte a beazonosíthatóság és felkutatás veszélyét. A képek csoportosítása egyrészt olyan témakörök szerint történt, amelyek kifejezetten a nőkkel szembeni kegyetlenséget és erőszakot promováltak, másrészt pedig „húspiac” témában, ahol a nők képei mellett személyes adataik is megjelentek és licitálni lehetett rájuk – az ár megadása után pedig erőszakra buzdító kommentárokat lehetett posztolni.<sup>39</sup>

A hasonló jellegű, felhasználók által generált tartalmaknak tárhelyet biztosító szolgáltatók jelentős számban vannak jelen Kelet-Európa és a Balkán térségében, ahol a nők elleni erőszak amúgy is rendszerszintű problémát jelent.<sup>40</sup> A magyar nők elleni erőszakot ábrázoló szexuális deepfake képeket feltöltő felhasználót – a közösségi médiában

38 Ibommahub, 2024.

39 Bálint, 2024.

40 Bavecic, 2024.

történi bejelentést követően – a magyar hatóságok német–magyar nemzetközi bűnügyi együttműködés eredményeként elfogták.<sup>41</sup>

Az eset kapcsán a Btk. módosítására került sor, bevezették az „internetes agresszió” törvényi tényállását, az új büntetőjogi tényállás 2025. január 1-jén lépett hatályba.<sup>42</sup>

---

## **6. A deepfake pornográfia áldozatai számára rendelkezésre álló jogorvoslati lehetőségek**

A deepfake létrehozásával és terjesztésével okozott károkat a bíróságok a meglévő polgári jogi és büntetőjogi eljárásokban kezelik. Keresetet lehet benyújtani személyiségi jogok sérülése (képmáshoz való jog sérülése, magánélethez való jog megsértése, méltósághoz és hírnévhez való jog megsértése stb.) miatt. A per sikeréhez az áldozatoknak be kell bizonyítaniuk, hogy a deepfake manipuláció eredménye, a valóság szándékolt figyelmen kívül hagyásával készült és kárt okozott.

A képi alapú szexuális visszaélések más formáihoz hasonlóan a deepfake-ek üldözése is jelentős joghatósági kihívásokkal néz szembe, hiszen teljes mértékben határon átlépő cselekményekről beszélünk. Az online platformok globális hozzáférhetősége azt eredményezi, hogy a világon bárki készíthet deepfake-et bárkiről, akinek az interneten elérhetőek a saját képei.

A deepfake visszaélések kezelésére a szakértők többoldalú megközelítést javasolnak, amely magában foglalja az áldozatsegítő szolgáltatások fokozását, a közvélemény figyelmének felhívását a deepfake-ek következményeire, valamint a technológiai vállalatok, jogi szakértők és bűnüldöző szervek közötti együttműködés előmozdítását.

A deepfake tartalmak terjedésének meggátolásában elsősorban az óriásplatformok saját ellenőrző mechanizmusait említenénk: a Facebook által alkalmazott „Deep Fake Detection Challenge”, a Google MI blogja a deepfake észleléséhez stb. Ezek az észlelő szoftverek azonban csak csökkentik, de nem szüntetik meg az ártalmas tartalmakat. Az észlelési technológiák csak a deepfake 65%-át tudják kiszűrni, azt is csak hitelességi százalékkal. Leginkább kontextuális szűrésre alkalmasak, technikailag nehéz, fizikailag lehetetlen ilyen mennyiségű digitális tartalmat szűrni.

---

## **7. Következtetések**

A rosszindulatú céllal készült deepfake tartalmak elterjedésének veszélye napról napra fokozódik. Ennek két meghatározó oka van: egyrészt, a világszerte egyre nagyobb

41 „archie147” – elfogtuk a Motherless ügy elkövetőjét [Online]. Elérhető: <https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/archie147-elfogtuk-a-motherless-ugy-elkovetojet> (letöltés ideje: 2025. 12. 28.).

42 Gáspár, 2025, 2499–2511.

felhasználószámmal és aktivitással rendelkező közösségimédia-platformoknak betudhatóan egyre több „nyersanyag” kerül az internetre, azaz szinte mindenkiről készülnek olyan kép- és videófelvételek, amelyek az interneten megtalálhatóak, és ezáltal nagyban elősegítik a deepfake tartalmak elkészítését és elterjedését. Másrészt az is megfigyelhető, hogy a technológia rohamosan fejlődik, így egyre kevesebb mások profiljairól letöltött fényképanyagra van szükség ahhoz, hogy szinte tökéletes, a valóságtól szinte megkülönböztethetetlen hamisított tartalmakat hozzanak létre.<sup>43</sup>

A kérdéskör eddigi evolúciója alapján az a következtetés körvonalazódik, hogy a deepfake pornográfia negatív társadalmi hatása a jövőben is kihívást fog jelenteni nem csak a női jogokra nézve, hanem számos alapjogra. A jogalkotás erre a problémára még nem talált teljes mértékben kielégítő választ, hiszen a jelenségre való tekintettel, nem létezik, nem létezhet konkrét, átfogó szabályozás. Az alapjogvédelmi eszközök peres érvényesítése túl lassú, és nem vagy csak nehezen tud lépést tartani a deepfake tartalmak gyors terjedésével, a nemzeti polgári jogi és büntetőjogi eszköztár egyelőre fennálló hiányosságai miatt (így sok esetben a hatóságok sem rendelkeznek még a szükséges eszközökkel és szakértelemmel ahhoz, hogy hatékonyan kezelhessék az ilyen ügyeket, és előrelépést érjenek el az esetek felderítésében és kezelésében). Láthattuk ugyanakkor, hogy létrejött az uniós szabályozási keret, illetve ugyanilyen jelentős az a tény is, hogy elvi szinten rögzültek azok a fogalmak, amelyeket mind a jogalkalmazás, mind a további jogalkotás alapul vehet: emberközpontúság és technológiasemlegesség, illetve kockázatkezelés és felelősségvállalás, már a preventív intézkedések szintjén.

## Irodalomjegyzék

- Badinszky, Á. (2024) 'Hamis valóság, valós veszély: deepfake az AI Act-ben', *Közigazgatás-Tudomány*, 4/2, 18–38. [Online]. Elérhető: <https://doi.org/10.54200/kt.v4i2.89>
- Bavcic, E. (2024) 'Digital Rights Review: Websites Promote and Profit from Abuse of Woman', *BalkanInsight* [Online]. Elérhető: <https://balkaninsight.com/2024/10/15/digital-rights-review-websites-promote-and-profit-from-abuse-of-women/> (letöltés ideje: 2025. 12. 28.)
- Boronkay, M. (2023) 'A képmáshoz és a hangfelvételhez fűződő jog', *In Medias Res*, 2013/1, 111–132.
- Cellan-Jones, R. (2019) *Deepfake videos' double in nine months* [Online]. Elérhető: <https://www.bbc.com/news/technology-49961089> (letöltés ideje: 2025. 12. 16.)
- Dudás, D. V. (2021) *Emberi Jogi kézikönyv az EJEB gyakorlata alapján*. Budapest: Wolters Kluwer.
- Dunn, S., Vaillacourt, T. és Brittain, H. (2023) *Supporting Safe Digital Spaces*. Centre for International Governance Innovation. [Online]. Elérhető: [https://www.cigionline.org/static/documents/SaferInternet\\_Special\\_Report.pdf](https://www.cigionline.org/static/documents/SaferInternet_Special_Report.pdf)
- Gáspár, Zs. (2025) 'Az internetes agresszió büntetőjogi megítélése', *Belügyi Szemle*, 73/12, 2499–2511. <https://doi.org/10.38146/BSZ-AJIA.2025.v73.i12.pp2499-2511>

43 Herke, 2023, 157–178.

- Hidalgo, N. (2023) *Gender-Based Violence in the Era of Artificial Intelligence* [Online]. Elérhető: <https://www.iadb.org/en/blog/gender-and-diversity/deepfakes-gender-based-violence-era-artificial-intelligence> (letöltés ideje: 2025. 12. 17.)
- Ibommahub (2024) *What is Motherless.com and the Importance of Internet Laws* [Online]. Elérhető: <https://ibommahub.com/what-is-motherless-com-and-the-importance/> (letöltés ideje: 2025. 03. 27.)
- Kis, J. (2022) 'A becsület és az emberi méltóság büntetőjogi védelme a román és a magyar jogban', *Erdélyi Jogélet*, 2022/4, 67–85. <https://doi.org/10.47745/ERJOG.2021.04.05>
- Kokoly, Zs. (2021) 'A személyiségi jogok szabályozása a hatályos román Polgári törvénykönyvben', *Erdélyi Jogélet*, 2021/2, 65–81. <https://doi.org/10.47745/ERJOG.2021.02.04>
- Koltay, A., Szikora, T., Lapsánszky A. és Tóth, A. (szerk.) (2024) *DSA Rendelet nagykommentár*. Budapest: Wolters Kluwer
- Laffier, J. és Rehman, A. (2023) 'Deepfakes and harm to women', *Journal of Digital Life and Learning*, 2023/3, 1–21.
- Lendvai, G. F. (2023) 'Deepfake a szólásszabadság tükrében – reflexiók a jog perspektívájából', in Aczél, P. és Veszelszki, Á. (szerk.) *Deepfake – a valótlan valóság*. Budapest: Gondolat Kiadó, 121–138.
- McGlynn, C. (2024) *Deepfake porn: why we need to make it a crime to create it, not just share it* [Online]. Elérhető: <https://theconversation.com/deepfake-porn-why-we-need-to-make-it-a-crime-to-create-it-not-just-share-it-227177> (letöltés ideje: 2025. 12. 17.)
- Security Hero. *2023 State of Deepfakes* [Online]. Elérhető: <https://www.securityhero.io/state-of-deepfakes/#advancements-in-deepfake-technology> (letöltés ideje: 2025. 12. 16.)
- Sorbán, K. (2020) 'A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről', *Belügyi Szemle*, 68/10, 81–104.
- Zakariás, K. (2019) *Az emberi méltósághoz való jog. Összehasonlító jogi elemzés a német és magyar alkotmánybíróági gyakorlat tükrében*. Budapest: Pázmány Press.