



37. Országos Tudományos Diákköri Konferencia

Állam- és Jogtudományi Szekció

Budapest, 2025. március 24–26.

Rendező intézmény:

Károli Gáspár Református Egyetem

Állam- és Jogtudományi Kar



Állam- és Jog-
tudományi Szekció

Hamis bizonyítékok, valós következmények:

A deepfake kihívásai a büntetőeljárásban

Kézirat lezárásának dátuma:

2024. november 08.

Bevezető gondolatok.....	3
I. A deepfake meghatározása	6
1.1. A deepfake működési alapjai.....	6
1.2. A deepfake jogi definiálása	8
II. A digitális bizonyítékok értékelése a deepfake korában	11
2.1. A képfelvételek értékelésének elméletei	11
2.2. A hamis bizonyítékok és a kognitív torzítás kapcsolata.....	14
2.3. A kép-, hang- és videófelvételek bizonyító erejének változása.....	17
III. A deepfake és a szakértői bizonyítás dilemmái.....	19
3.1. Szakértő alkalmazásának szükségessége	19
3.2. Szakértői megállapítások értékelése a deepfake technológiával szemben.....	24
IV. A hitelesség biztosítását, ellenőrzését segítő intézkedések	28
4.1. Vízjelek, egyéb megjelölések használata	29
4.2. Hitelesítő szoftverek alkalmazása	30
4.3. A bűnjelkezelés egyes kérdései	33
Záró gondolatok	36
Irodalomjegyzék	39

Bevezető gondolatok

Képzeljünk el a következő szituációt: a rendőrségen gyanúsítottként hallgatnak ki minket, és éppen egy videófelvételt mutatnak be nekünk. A felvétel szereplőjének az arca zavarba ejtően ismerős – hiszen ez a mi arcunk. Tudjuk, hogy valójában nem mi vagyunk ezen a felvételen, amelyen valaki éppen egy bűncselekményt követ el, azonban ezt nem tudjuk bizonyítani. A nyomozó hatóság informatikus szakértőt rendel ki a felvétel hitelességének megállapítása érdekében, azonban a szakértő nem tud megbízhatóan állást foglalni a hitelesség kérdésében, mindössze annyit állapít meg, hogy az elvégzett szakértői módszerek alapján nem találhatóak manipulációra utaló jelek.

Ez nem a távoli jövő disztópiája, hanem korunk egyik legnagyobb fenyegetése a büntetőeljárásra nézve: a deepfake technológia, amely képes hamis, de rendkívül valóságghű képek, videók és hangfelvételek létrehozására, vagy manipulálására.

A deepfake technológia elérkezett egy rendkívüli figyelmet érdemlő fordulóponthoz, hiszen már képes olyan tartalmakat létrehozni, hogy a szakértők sem képesek minden esetben a hamis és a valódi bizonyítékok megkülönböztetésére. A deepfake technológia mára olyan széleskörű hozzáféréssel rendelkezik, hogy különleges informatikai, grafikus vagy hangszerkesztői szaktudás nélkül is szinte bárki rövid idő alatt valóságghű tartalmakat tud létrehozni¹.

A dolgozatom azt a célt hivatott szolgálni, hogy feltárja a deepfake technológia büntetőeljárásra gyakorolt veszélyeit, valamint javaslatokat fogalmazzon meg a felmerülő kihívások hatékony kezelésére. Fontosnak tartom rögzíteni, hogy a deepfake technológia fejlődése természetesen nem kizárólag a büntető eljárásjogot fogja érinteni, hanem más jogterületeket és tudományterületeket is, melynek bemutatására e dolgozat keretei között nem vállalkozom, mindvégig a büntető eljárásjogi vonatkozások vizsgálatát tartom szem előtt.

A kutatási téma feldolgozásához több módszertani megközelítést alkalmazok, melynek során elengedhetetlen a kép-, hang- és videófelvelelek bizonyítékként történő értékelésére vonatkozó elméletek bemutatása, a releváns jogforrások, jogi és egyéb tudományterületről érkező szakmai anyagok értelmezése, valamint a téma specifikusságából adódóan egy igazságügyi informatikus szakértővel történő interjú elkészítése. Úgy vélem, hogy az igazságügyi szakértői megállapítások az egyik fontos kiindulópontját adják e dolgozatnak, ugyanis a szakmai tények

¹ BERNACIAK, Catherine and ROSS A. Dominic: *How Easy Is It to Make and Detect a Deepfake?* <https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/> (letöltés ideje: 2024. 09. 21.).

meghatározó szerepet játszhatnak abban, hogy milyen szabályozási megoldások válhatnak indokolttá. Utóbbi kapcsán ezúton is szeretném köszönetemet kifejezni Kiss Attila László igazságügyi informatikus szakértőnek, aki széleskörű szakmai tudásával hozzájárult egy szakmai interjú keretein belül e tanulmány elkészítéséhez. Nyilatkozom, hogy a tanulmány elkészítéséhez mesterséges intelligencia alapú szoftvert nem vettem igénybe.

A kutatásom során azzal a jelenséggel szembesültem, hogy még a szakirodalomban is eltérő definíciók keringenek a deepfake technológiával kapcsolatban. Úgy gondolom, ha nem tudjuk kristálytiszta módon meghatározni azt, hogy mivel állunk szemben, akkor nem láthatjuk tisztán a kihívások természetét sem, és nehezen képzelhető el a megfelelő jogi fogalmak és eljárásjogi szabályok kialakítása. Ennek fényében a dolgozat első részében arra vállalkozom, hogy jogi és technológiai szempontból meghatározzam a deepfake mibenlétét. A deepfake mögött álló technológia ismertetése más tudományterületeket is érint, amelynek teljeskörű feldolgozására ugyancsak nem törekszik e dolgozat, azonban fontosnak tartom a deepfake alapvető tételeinek áttekintését, amelyek segítenek, hogy közös logikai rendszerben gondolkodhassunk.

Fontosnak tartom tisztázni, hogy a deepfake technológia megváltoztathatja-e a kép-, hang- és videófelvevételek bizonyítékként való értékelésének jelenlegi gyakorlatát. Ennek fényében keresem a választ arra, hogy milyen elméletek alakultak ki a digitális bizonyítékok értékelésére vonatkozóan, valamint azok alkalmazhatóságát vizsgálom a deepfake technológiával szemben. Külön figyelmet igényel az a kérdés, hogy a bizonyítékokkal szemben megjelenő túlzott szkepticizmus befolyásolhatja-e a bizonyítékok értékelését, illetve, hogy mutatkoznak-e összefüggések a kognitív torzítások és a hamisított bizonyítékok között.

A deepfake hamisítás okozta kihívásoknak való megfelelés elképzelhetetlen az igazságügyi szakértők munkája nélkül. A hitelesség vizsgálata során kijelenthető, hogy a problémák egyre inkább multidiszciplinárisokká válnak, de már sokszor az sem egyértelmű, hogy hol kezdődik a különleges szakértelem mércéje. Ennek fényében a kutatásom során olyan szempontrendszer kidolgozására vállalkozom, amelyek iránymutatást adnak a legfontosabb kérdésekben:

- A kép-, hang-, és videófelvevételek kapcsán mi a különleges szakértelem mércéje, mikor indokolt a szakértő alkalmazása?
- A bizonyosság milyen szintjén tudnak a szakértők megállapításokat tenni a bizonyítékok hitelességének tekintetében? Hogyan értékelhető a büntetőeljárásban az a kép-, hang- vagy videófelvevételre vonatkozó szakértői vélemény, amely sem kategorikusan, sem a valószínűség magas szintjén nem tud megállapításokat tenni?

- A bizonyítékok beszerzésre, rögzítése kapcsán milyen kritériumokat kell követni, hogy azok hitelességét az eljárás során kétséget kizáróan meg lehessen állapítani?

Megítélésem szerint a deepfake technológia fejlődésének egyik el nem hanyagolható veszélye, hogy az egyébként valódi kép-, hang- és videófelvételek hitelessége könnyen és tömegesen vitathatóvá válhat. Annak érdekében, hogy a büntetőeljárásban megbízhatóan fel lehessen használni az ilyen bizonyítékokat, nélkülözhetetlen, hogy azok megszerzésére és rögzítésére vonatkozó előírások az eddigi feltételekhez képest magasabb szinten biztosítani tudják a hitelességet. Ezzel összefüggésben a dolgozatomban vizsgálom a hitelesítő szoftverek alkalmazásának, valamint a mesterséges intelligencia tartalmak kötelező megjelölésének lehetőségét is, mely utóbbival kapcsolatban szükséges az Európai Parlament és a Tanács 2024/1689. rendeletének (továbbiakban: AI Act) releváns rendelkezéseinek ismertetése.

Kétségtelen, hogy a mesterséges intelligencia számos kedvező hatással is bírhat mind az életünkre, mind pedig a büntetőeljárásra nézve. Kutatásom azonban – a célkitűzésével összhangban – kizárólag a deepfake technológia által jelentett kihívások vizsgálatára korlátozódik.

I. A deepfake meghatározása

Ahhoz, hogy a deepfake jogi meghatározása során megfelelő fogalmakat tudjunk alkotni, elengedhetetlen, hogy megértsük a technológia működésének legalapvetőbb tételeit. Ha nem tudjuk, hogy milyen potenciál rejlik a deepfake technológiában, akkor nehezen elképzelhető, hogy helyes jogi válaszokat tudjunk kidolgozni. Erre figyelemmel a technológiai alapvetések lefektetése után tartom indokoltnak a deepfake jogi meghatározásának tisztázását is.

1.1. A deepfake működési alapjai

A deepfake kifejezés a deep learning (mély tanulás) és a fake (hamis) szavakból ered. Az elnevezés arra utal, hogy valamilyen hamis tartalom jön létre a deep learning gépi tanulási technikával². A deep learning a mesterséges intelligencia (AI) egyik ága, melynek egyik legfontosabb jellemzője, hogy a rendelkezésre álló adatok alapján képes tanulni, fejlődni. Minél több adatot kap a mesterséges intelligencia, annál pontosabb eredményt tud produkálni³, hiszen a deepfake technológia ez alapján képes tökéletesíteni eredményeit⁴.

Fontos kiemelni, hogy a deepfake az AIM-nak (AI generated material) azaz mesterséges intelligencia által generált tartalomnak csak egy részét teszi ki, ugyanis a mesterséges intelligencia kép- és hangalkotási képességei nem minden esetben realisztikus tartalom elkészítésére használatosak⁵, például a Microsoft's Bing Image Creator könnyedén készít rajzfilmfigurát, vagy éppen névjegykártya dizájnt. Az AIM és a deepfake relációjában az AIM a tágabb kategória.

A deepfake technológia legelterjedtebb változata a GAN (Generative Adversarial Network), amely két versengő modellt tartalmaz. A generátor modell elkészíti a kívánt tartalmat, – például képet, videót – majd azt a diszkriminátor modell ellenőrzi. Amennyiben a diszkriminátor algoritmus szerint a tartalom hamisítvány, akkor azt visszaküldi a generátornak, majd ez a

² RANA, Md Shohel - NUR NOBI, Mohammad - MURALI Beddhu - SUNG, Andrew H.: *Deepfake Detection: A Systematic Literature Review*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9721302> (letöltés ideje 2024. 09. 17.).

³ MI Blog: *Mély tanulás a mesterséges intelligencia világában* <https://mesterseges-intelligencia.eu/mely-tanulas-a-mesterseges-intelligencia-vilagaban/> (letöltés ideje: 2024. 09. 25.)

⁴ DELFINO, Rebecca A.: *Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery*. *Hastings Law Journal*, 2023/2, 299. (<https://doi.org/10.2139/ssrn.4032094>) (letöltve: 2024. 09. 25.)

⁵ PFEFFERKORN, Riana: *'Deepfakes' in the Courtroom*. *Boston University Public Interest Law Journal*, 2020/2. 248. <https://www.bu.edu/pilj/archives/vol-29-2-summer-2020/> (letöltve: 2024.09.11.)

folyamat addig ismétlődik, amíg nem találja valódinak a tartalmat, így tökéletesítve az eredményt⁶.

A deepfake tartalmak különböző csoportjait különböztethetjük meg^{7,8}. Az egyik legismertebb csoport az arccsere (face swap), amely képes egy személy arcát kicserélni egy másik személy arcára egy képen, videón, vagy akár valós időben is. Ezt a technikát alkalmazta egy motoros vlogger, aki fiatal lányként bemutatva magát több tízezer Twitter követőt gyűjtött 2021-ben, mígnem kiderült, hogy a felhasználó egy 50 éves férfi, aki a Faceapp Iphone alkalmazását használta, hogy megtéve a közönségét⁹.

A másik nagy csoport az attribútum-szerkesztés (attribute editing), mely egy adott személynek egy konkrét külső tulajdonságát változtatja meg képeken vagy videókon. Ide sorolható például a hajszín vagy a bőrszín megváltoztatása.

A deepfake másik figyelemre méltó fajtája a Face re-enactment, mely képes arra, hogy egy ember arcmozgását, mimikáit leutánozva egy másik személy arcára átültesse azt, anélkül, hogy a célszemély arcán bármi mást megváltoztatna¹⁰. Figyelemre méltó a Face2Face projekt, amely valós időben képes megtartani az eredeti videóban végzett fejmozgásokat is, és úgy leutánozni a forrás arcmozgásait, hogy az a manipulált videóban lévő személy gesztusainak feleljen meg¹¹.

A Fully synthetic material (azaz teljesen mesterséges tartalom) esetén a mesterséges intelligencia által létrehozott képanyag teljesen mesterséges, nem egy meglévő felvételen hajt végre változtatásokat¹². Természetesen erre a csoportra is igaz, hogy az algoritmus arra törekszik, hogy a létrehozni kívánt képi tartalom realisztikus legyen, így jöhetett létre például egy olyan weboldal, amely képes minden egyes betöltéskor egy teljesen új emberi portrét létrehozni¹³.

⁶ Europol Innovation Lab (2022), *Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab*, Publications Office of the European Union, Luxembourg. 8. [Europol Innovation Lab Facing Reality Law Enforcement And The Challenge Of Deepfakes.pdf \(europa.eu\)](https://europa.eu/europol/innovation-lab/facing-reality-law-enforcement-and-the-challenge-of-deepfakes.pdf) (letöltés ideje: 2024. 09. 13.)

⁷ Ötödik csoportként a hangfelvételek manipulációja is ide sorolható, mint önálló kategória.

⁸ Europol Innovation Lab i.m. 9.

⁹ THE WASHINGTON POST: *A 'beautiful' female biker was actually a 50-year-old man using FaceApp. After he confessed, his followers liked him even more.* <https://www.washingtonpost.com/technology/2021/05/11/japan-biker-faceapp-soya-azusagakuyuki/> (letöltve: 2024. 09. 05.)

¹⁰ Europol Innovation Lab i. m. 9.

¹¹ Face2Face: *Real-time Face Capture and Reenactment of RGB Videos* https://vcai.mpi-inf.mpg.de/projects/MZ/Papers/CVPR2016_FF/page.html (letöltés ideje: 2024. 09. 16.).

¹² Europol i. m. 9.

¹³ <https://www.thispersondoesnotexist.com>

A deepfake körébe vonható továbbá az audio deepfake, amely egyrészt jelentheti egy hangfelvétel manipulálását – például egy férfi hangját női hanggá alakítja –, másrészt jelentheti egy teljesen mesterséges hang létrehozását¹⁴. Ez a fajta deepfake már évekkel ezelőtt is olyan jól működött, hogy tudósítások szerint 2019-ben egy energetikai cég vezérigazgatója több mint 70 millió forintnak megfelelő eurót utalt át egy számlára, ugyanis egy deepfake által manipulált hang elhitette vele, hogy az anyavállalatának vezetőjével beszél telefonon¹⁵.

1.2. A deepfake jogi definiálása

A jelenleg hatályos jogrendszerünk nem rendelkezik a deepfake pontos meghatározásával. A definiálás hiánya természetesen nem jelenti azt, hogy a deepfake használata nem járhat jogkövetkezményekkel, például a Büntető Törvénykönyvről szóló 2012. évi C. törvényben (a továbbiakban: Btk.) meghatározott törvényi tényállások egy része kimeríthető a deepfake használatával is, mint például a becsület csorbítására alkalmas hamis- hang vagy képfelvétel készítése, vagy éppen a zsarolás, ugyanakkor Herke Csongor szerint elképzelhető lenne olyan tényállások megalkotása is, amelyek a deepfake-hez kapcsolódnak, vagy éppen a meglévő tényállások minősített eseteit bővítené¹⁶. Ide sorolható még a Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:43.§-ban meghatározott nevesített személyiségi jogok – például a képmáshoz és hangfelvételhez való jog – megsértésével járó jogkövetkezmények is. Nyilvánvalóan a deepfake használata rendkívül sok jogkövetkezménnyel bírhat különböző területeken, azonban a dolgozat célkitűzésével összhangban kizárólag a büntetőeljárás oldaláról vizsgálom azt.

Ami a deepfake fogalmi meghatározását illeti, Lendvai Gergely Ferenc a következőképp fogalmazza meg: „a deepfake mesterséges intelligencián alapuló technológia, amely segítségével a felhasználó célzatosan és szándékosan hamisított, leginkább emberekről készített kép- és hangfelvétel-tartalmakat tud készíteni, oly módon, hogy a létrehozott tartalom

¹⁴ CHOI, Jeong-Eun – SCHÄFER, Karla – ZMUDZINSKI, Sascha: *Introduction to Audio Deepfake Generation*, Academic Insights for Non-Experts, 1. <https://dl.acm.org/doi/abs/10.1145/3643491.3660286> (letöltve: 2024. 09. 26.)

¹⁵ Molnár Csaba: Először csaltak ki pénzt deepfake hanggal, és rögtön van magyar szál, <https://index.hu/techtud/2019/09/05/eloszor-csaltak-ki-penzt-deepfake-hanggal-es-rogt-on-van-magyar-szal/> (letöltés ideje: 2024. 09. 22.).

¹⁶ HERKE Csongor: *Deepfake: áldás vagy átok? Jogi szabályozási szempontok*, Pro Futuro, 2023/1, 174. <https://doi.org/10.26521/profuturo/2023/1/13334> (letöltve: 2024. 09. 26.)

meggyőző módon képes a hamisított tartalmat valóságosnak érzékelteni.¹⁷ Más értelmezésben Sorbán Kinga hozzáfűzi azt, hogy „algoritmusok által manipulált felvételek”¹⁸.

Az Európai Parlament és a Tanács 2024/1689. rendelete (továbbiakban: AI Act) 3. cikkében úgy fogalmaz, hogy a deepfake „az MI által generált vagy manipulált kép, audio- vagy videotartalom, amely hasonlít létező személyekre, tárgyakra, helyekre, entitásokra vagy eseményekre, és amely egy személy számára megtévesztő módon autentikusnak vagy valóságosnak tűnne”. Ez a megfogalmazás eltér a jogalkotási eljárás során rögzített egyik megfogalmazástól, amely úgy hangzott, hogy „manipulált vagy szintetikus hang, kép vagy videótartalom, amely megtévesztő módon az eredetiség vagy hitelesség látszatát kelti, és amely úgy ábrázol személyeket, mintha olyasmit mondanának vagy tennének, amit soha nem mondtak vagy tettek, és amelyet mesterséges intelligencián alapuló technikákkal – beleértve a gépi tanulást és a mélytanulást is – állítanak elő”¹⁹.

Egy amerikai deepfake szabályozó törvénytervezet, a Deepfakes Accountability Act²⁰ a deepfake a következő módon írja le: „A deepfake olyan videofelvétel, mozgóképes film, hangfelvétel, elektronikus kép vagy fénykép, illetve a beszéd vagy magatartás bármely olyan technológiai ábrázolása, amely A) úgy tűnik, hogy hitelesen ábrázolja egy olyan személy beszédét vagy magatartását, aki valójában nem vett részt ilyen beszédben vagy magatartásban; és B) amelynek előállítása valójában technikai eszközökön múlik, és nem pedig egy másik személy azon képességén, hogy fizikailag vagy szóban megszemélyesítse az ilyen személyt.”

Minden ismertetett megközelítés tartalmazza, vagy utal arra, hogy a deepfake egy mesterséges intelligencián alapuló technológia, azonban a Deepfakes Accountability Act ködösen fogalmaz ebben a vonatkozásban miszerint: „előállítás valójában technikai eszközökön múlik, és nem pedig egy másik személy (...) képességén”. Az ismertetett technológiai háttér tükrében a deepfake jogi meghatározásakor indokoltnak tartom egyértelműen rögzíteni, hogy a deepfake egy mesterséges intelligencián alapuló technológia.

¹⁷ GOSZTONYI Gergely, LENDVAI Gergely: *Deepfake és dezinformáció*, Médiakutató 2024. tavasz, XXV. évf. 1. szám, 42.

¹⁸ SORBÁN Kinga: *A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről*, Belügyi Szemle 2020/10. 84.

¹⁹ Az Európai Parlament 2023. június 14-én elfogadott módosításai a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (a mesterséges intelligenciáról szóló jogszabály) (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

²⁰ Deepfakes Accountability Act H.R.5586. <https://www.congress.gov/bill/118th-congress/house-bill/5586/text> (megtekintve: 2024. 09. 26.)

Lendvai meghatározása kihangsúlyozza a deepfake fogalmi elemeként a hamisított tartalmak célzatos és szándékos készítését. A célzatos elkövetés büntetőjogi fogalom, amely arra utal, hogy a célzat a törvényi tényállásban megfogalmazott cél, amelynek elérésére törekszik az elkövető²¹. Lendvai természetesen nem a deepfake készítésének törvényi tényállását kívánta megfogalmazni, ezért elmondható, hogy a célzatosság azt jelenti, hogy a tartalom létrehozása mögött egy konkrét, előre meghatározott cél vagy célkitűzés áll. Például, ha azért hoz létre deepfake-t valaki, hogy befolyásolja a nyomozás eredményét, akkor a tartalom elkészítése e fogalom szerint célzatos. A célzatosság azonban álláspontom szerint nem tekinthető a deepfake meghatározásánál releváns szempontnak, mindinkább az esetleges büntetőjogi törvényi tényállások meghatározásánál bírhat jelentőséggel. A manipulátor és a tartalmat felhasználó személy elkülönülhet egymástól. Ha a manipulátor tudatát nem fogja át az a tény, hogy a másik személy mire szeretné felhasználni az általa hamisított tartalmat, akkor semmiképpen nem beszélhetünk célzatosságról, azonban a deepfake célzat nélkül is képes olyan tartalmat létrehozni, amely valódinak tűnik. Maga a megtévesztés pedig még inkább nem rendelhető a célzat fogalma alá, hiszen a megtévesztő képesség a deepfake technológia velejárója, ezért a célzatosság a megtévesztésen túli eredményt feltételez.

Ahogy a technológiai alapvetéseknél rámutattam a mesterséges intelligencia által generált tartalom és a deepfake közötti relációra, így e meghatározásoknál is hangsúlyos szerepet kap az a felismerés, hogy a deepfake tartalomnak alkalmasnak kell lennie arra, hogy a hamisított tartalom eredetinek hasson. Lendvai megfogalmazásában „meggyőző módon képes (...) valóságosnak érzékelteni”, az AI Act által rögzített meghatározásnál „megtévesztő módon autentikusnak vagy valóságosnak tűnne” kifejezés szerepel, míg a Deepfake Accountability Act „úgy tűnik, hogy hitelesen ábrázolja” megfogalmazást használja. Mindhárom értelmezésből kitűnik, hogy a tartalomnak nem kell, hogy tökéletes legyen, vagy teljesen valósághűként mutakozzon minden részletében, pusztán elegendő, ha meggyőző módon, az érzékek útján képes ezt a látszatot kelteni.

Az értelmezési nehézségek elkerülése miatt fontosnak tartom rögzíteni, hogy a deepfake kifejezés használatos egyszerre a deepfake technológia termékének megjelölésére, tehát a manipulált vagy mesterségesen kreált tartalomra, valamint magát a deepfake technológiát is

²¹ CSEMÁNÉ Váradi Erika–GÖRGÉNYI Ilona–GULA József–HORVÁTH Tibor–JACSÓ Judit–LÉVAY Miklós–SÁNTHA Ferenc: *Magyar büntetőjog - általános rész.* 2017, Budapest: Wolters Kluwer Kft. <https://doi.org/10.55413/9789632956282> Letöltve: https://mersz.hu/dokumentum/wk83_132/#wk83_129_p3 (2024.10.02.)

gyakran egyszerűen „deepfake” jelzővel illeti a szakirodalom. Bár az Ai Act által meghatározott deepfake fogalom irányadónak tekinthető, azonban az ismertetett fogalmi elemek és technológiai háttér figyelembevételével álláspontom szerint a deepfake technológia az alábbiak szerint definiálható a legpontosabban: A deepfake olyan mesterséges intelligencia alapú technológia, amely alkalmas kép-, hang- és videófelvevételek létrehozására vagy manipulálására oly módon, hogy azok megtévesztően hitelesnek és valóságosnak tűnjenek.

II. A digitális bizonyítékok értékelése a deepfake korában

Egyes tudósítások szerint Párizsban már 1841-ben lefényképeztek minden őrizetbe vett személyt, Magyarországon pedig 1887-ben kezdték meg a fényképnyilvántartás felállítását²². A 20. században széleskörben útnak indult a bűnügyi fényképezés, az elmúlt néhány évtizedre pedig egyre fontosabb szerepet játszott a büntetőeljárásban. Ezen bizonyítékok általában gyorsan és költséghatékonyan hozzáférhetőek, objektivitásuk igen kevés kétséget hagy maga után. A megbízhatóság ellenére már a 20. századi szakirodalom felismerte annak veszélyét, hogy a fénykép objektivitása és pártatlansága ki van téve a fényképész szándékának²³. Mindamellet a mesterséges képalkotás elterjedése kapcsán Kertész Imre 1992-ben felvetette annak lehetőségét, hogy „megcsappanhat” a fénykép bizonyítási jelentősége²⁴, sőt egyes szerzők azt jósolták az 1990-es években, hogy a Photoshop elterjedése az „igazság krízisét” fogja okozni²⁵. Az elmúlt néhány évtized tapasztalataiból kiindulva kijelenthetjük, hogy a képfelvevételek jelentősége az előrejelzések ellenére nem látszik csökkenni sem a büntetőeljárásban, sem az élet más területein.

2.1. A képfelvevételek értékelésének elméletei

A képfelvevételek értékelésére számos elmélet kialakult az igazságszolgáltatásban való elterjedése óta. Klasszikusan kettő elmélet állítható szembe egymással, a képikommunikáció-

²² KERTÉSZ Imre: *Kép- és hangtechnikai eszközök a büntető eljárásban*, Acta Universitatis Szegediensis: acta juridica et politica, 1992/41. 315. <https://acta.bibl.u-szeged.hu/6726/> (letöltve: 2024. 08. 01.)

²³ I. m. 317.

²⁴ I. m. 324.

²⁵ PFEFFERKORN i.m. 248.

elmélet (pictorial communication theory) és a néma tanú elmélet (silent witness theory)²⁶, azonban ezen elméletektől eltérő egyéb megközelítések is napvilágot láttak, például a múlt században megjelent angolszász értékelési módszer, amely a képfelvételek előítéletkeltő hatását mérlegeli az elfogadhatóság szempontjából²⁷.

2.1.1. A képikommunikáció-elmélet

A *képikommunikáció-elmélet* szerint a képfelvétel bizonyítékként történő értékeléséhez nem elegendő a képi tartalom rendelkezésre állása, hanem szükséges a hitelességének a megerősítése is egy tanú által. A tanúval szemben nem követelmény az, hogy ő készítse a fényképet, vagy hogy a fényképezés pillanatában jelen legyen a helyszínen, pusztán az is elegendő, ha igazolni tudja, hogy a felvétel a valóságot tükrözi²⁸. Kertész Imre rávilágít arra, hogy az elmúlt században az Egyesült Államokban ennek az elméletnek megfelelő eljárás alakult ki, viszont nem a fényképész tett tanúvallomást a kialakult gyakorlat szerint, hanem a helyszínre elsőként kiérkező rendőr, ugyanis ő hitelesebben tudott tanúskodni a fényképen látható dolgok valóságáról²⁹. Az elmélet szerint a vizuális tartalom elfogadhatóságának a hitelesítésen túl relevánsnak kell lennie a tényállás megállapítása vagy egy jogkérdés eldöntése szempontjából, valamint nem szabad, hogy félrevezető módon tüntesse fel a valóságot³⁰.

A szakértői bizonyítás kérdését részletesen a későbbiekben kívánom kifejteni, azonban azt leszögezhetjük, hogy a szakértő nem minden esetben tudja kétséget kizáróan megállapítani egy felvétel eredetiségét. Ebben az esetben – vagy szakértő kirendelésének hiányában – megítélésem szerint a képikommunikáció-elmélet adhat támpontot, hiszen egy tanú igazolni tudja a felvételen lévő tartalom valóságát, vagy a felvétel eljutását a hatóságokhoz, esetlegesen a bűnjelként lefoglalt felvétel hitelességi láncolatának a meglétét. Ebben az esetben a bíróság bizonyítást vehet fel, és a felvétel bűnjelként való kezeléséről, vagy a lefoglalást megelőző állapotáról tanúként kihallgathatja akár a hatóság tagjait is, hiszen a Be. 168.§ (1) bekezdésében meghatározott bizonyítandó tény éppen a hitelesség kérdése lehet.

²⁶ HERKE Csongor: *A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra*, Magyar Jog, 2024/6., 324.

²⁷ KETTERLING, Lester: *Photographs as Demonstrative Evidence in the Court Room*, North Dakota Law Review 1964. 195.

<https://commons.und.edu/cgi/viewcontent.cgi?article=2698&context=ndlr> (letöltve: 2024. 09. 15.)

²⁸ HERKE i.m. 325.

²⁹ KERTÉSZ i.m. 318.

³⁰ HERKE i. m. 325.

2.1.2. A néma tanú elmélet

A *néma tanú elmélet* esetén ezen bizonyítékok elfogadhatóságának küszöbe alacsony, ugyanis itt nincs szükség külső hitelesítésre, az elmélet a képfelvételeket azok objektivitásából kiindulva tekinti megbízhatónak. Egyes vélemények szerint ma különösen akkor lehet jelentősége ezen elméletnek, amikor a felvételek biztonsági kamerák zárt rendszeréből származnak, vagyis olyan automatizált folyamat eredményei, amely során a felvételek közvetlen emberi közrehatás nélkül jöttek létre³¹. A néma tanú elmélet tehát nem kívánja meg, hogy egy tanú hitelesítse a vizuális tartalmat, hiszen maga a tartalom, mint „néma tanú” fogadható el bizonyítékként³².

Nyilvánvalóan ezen elméleteknek a vegyes alkalmazása jellemző, önmagában mindkettő feltételrendszer mára már meghaladottá vált. Egyes szakirodalmi álláspont szerint a néma tanú elmélet a deepfake korában nem alkalmazható megbízhatóan, hiszen a deepfake technológia túlságosan meggyőző tud lenni ahhoz, hogy hitelesítő tanú nélkül kellő legyen a felvétel valódiságába vetett bizalom³³. Mások megítélése szerint sem a képikommunikáció-elmélet, sem a néma tanú elmélet nem alkalmazható a deepfake korában, hiszen sem a felvétel nem lehet önmagában néma tanú, sem pedig egy tanú nem fogja tudni tanúsítani a felvétel valódiságát, ugyanis éppen a felvétel valódiságának megkérdőjelezése válik a bizonyítás kérdésének középpontjává³⁴.

A néma tanú elmélet alkalmazása álláspontom szerint is nehezen tűnik eredményesen alkalmazhatónak a deepfake hamisításokkal szemben, hiszen az elmélet éppen abból indul ki, hogy a felvételek objektív információkkal szolgálnak. Azonban a hitelesség megőrzése érdekében lehetséges ellátni a bizonyítékokat olyan adatokkal, amelyek segítségével biztosítható a hitelességük, így – bár némiképp „külső” hitelesítő forrásból származóan – a digitális korban is „néma tanúk” maradhatnak. Ilyen hitelesítő módszereknek tekinthető a hitelesítő szoftverek, hash kódok használata (lásd később).

³¹ LINNA JR, Daniel W. – DALAL, Abhishek – GAO, Chongyang – GRIMM, Paul W. – GROSSMAN, Maura R. – PULICE, Chiara - TUNHEIM Hon. John: *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases* 25. [Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases \(researchgate.net\)](#) (letöltve: 2024. 10. 09.).

³² i. m.

³³ Delfino i. m. 341.

³⁴ Herke i. m. 326.

2.2. A hamis bizonyítékok és a kognitív torzítás kapcsolata

2.2.1. Az angolszász értékelési módszer

Ahogy azt már korábban említettem, a Model Code of Evidence által az egyik legpontosabban leírt angolszász értékelési módszer nem helyezhető a néma tanú elmélet és a képi kommunikáció-elmélet logikai rendszerébe, ezért nem is helyezhető szembe ezen elméletekkel. Az értékelési módszer megfogalmazásának háttérében az a felismerés állt, hogy a fényképek elfogadhatóságának megítélésére különös figyelmet kell fordítani, ugyanis az esküdtek hajlamosak azokat a valósággal tökéletesen azonos ábrázolásnak tekinteni, valamint erős előítéletkeltő hatással bírhatnak, ezért minden felhasznált fényképnek releváns bizonyító erővel kell bírnia. Az elmélet szerint a fényképek relevanciája önmagában nem alapozza meg annak felhasználhatóságát, ugyanis, ha a fénykép előítéletkeltő hatása meghaladja a fénykép bizonyító erejét, akkor a bizonyítékot ki kell zárni. Az előítéletkeltő hatással szembeni óvatosság olyannyira meghatározó volt, hogy a Model Code of Evidence leírása alapján a korabeli bírói gyakorlatban találhatók precedensek arra, hogy olyan bizonyíték is kizárásra került, amelynek egy része releváns volt, másik része pedig irreleváns és előítéletes³⁵.

Ez az értékelési módszer a mai napig végigköveti az angolszász jogi gondolkodást, a deepfake kihívásait feldolgozó szakirodalomban egyes szerzők ma is arra az álláspontja helyezkednek, hogy a deepfake vonatkozásában kifogásolt bizonyítékot, ha a bíró úgy ítéli meg, hogy annak bizonyító erejét jelentősen felülmúlja az előítéletkeltő hatása, akkor nem szabad az esküdtszék elé terjeszteni³⁶. Az ilyesfajta óvatosságnak azonban nyomós oka van: tanulmányok számtalanszor kimutatták, hogy az esküdtek emlékezetére és további észlelésére akkor is jelentős hatást gyakorolnak az audiovizuális bizonyítékok, ha az esküdtek tisztában vannak azzal, hogy az adott bizonyíték valószínűsíthetően hamis³⁷.

2.2.2. A kognitív torzítás jelentősége

Az esküdtekre gyakorolt ezen hatást a szakirodalom kognitív torzításnak nevezi. A kontinentális jogrendszerben bár nem tudott meghonosodni az esküdtszék alkalmazása, de ezen ismeretek tükrében felmerül a kérdés: a kognitív torzítás hasonló hatással bírhat-e a jogilag

³⁵ KETTERLING i. m. 193-194.

³⁶ LINNA JR, Daniel W. – DALAL, Abhishek – GAO, Chongyang – GRIMM, Paul W. – GROSSMAN, Maura R. – PULICE, Chiara - TUNHEIM Hon. John: i.m. 31.

³⁷ i. m. 30.

képzett bírókra? A kognitív torzítás egy döntéshozatalt befolyásoló tényező, melynek egyik alfaja az „irreveláns információ” jelenség, melynek lényege, hogy az emberi agy hajlamos rá, hogy ne tudjon figyelmen kívül hagyni valamilyen információt, ha az már a tudomására jutott³⁸.

Jelen esetünkben ez az információ az olyan bizonyítékokat jelenti, amelyek nem játszhatnak releváns szerepet a döntéshozatal során. Az erre vonatkozó pszichológiai kutatások azt mutatják, hogy a jogilag felkészült bírók is hasonló kognitív torzításokkal szembesülnek, mint a laikusok, tehát nem zárható ki a torzító hatások érvényesülése a döntéshozatali folyamatban³⁹. Ilyen bizonyíték lehet például egy erőszak hatására tett vallomás, egy jogellenesen beszerzett bizonyíték, vagy esetünkben egy olyan audiovizuális tartalom, amelyről utóbb kiderül, hogy manipuláltak, vagy nem lehetett nagy valószínűséggel sem megállapítani, hogy hiteles. Különös aggodalomra adhatnak okot azok a tanulmányok, amelyek megerősítik, hogy az „audiovizuális bizonyítékok erőteljes hatással bírnak az emberi emlékezetre és a valóság érzékelésére”⁴⁰. Keleti Arthur is rámutat arra, hogy az információs rendszereket azért hoztuk létre, hogy tényeket tárolhassunk benne, ezért kialakulhatott bennünk az az érzés, hogy amik ebben a rendszerben szerepelnek, azok tények⁴¹. Maura Grossman úgy véli, hogy az esküdtek extrém módon érzékenyek a mesterséges intelligencia által generált anyagok általi manipulációra, és a bírók sem mentesek ezen hatás alól⁴². A tömegkommunikációs elmélet által is elismert tény, hogy „a képekkel illusztrált és audiovizuális tartalmak hatásosabb eszközök az egyén befolyásolására”⁴³.

2.2.3. A torzító hatás ellensúlyozása

Az emberi pszichében rejlő, az objektív döntéshozatalra nézve nem kívánatos természetszerűségeik kizárása azonban komoly kihívást jelenthet. Álláspontom szerint ezt a hatást ellensúlyozhatják egyrészt a Be. által előírt garanciális szabályok és az indokolási

³⁸ GÁBRI Angéla: *Kognitív tudományok az ítélkezési tevékenység szolgálatában*, Pro Futuro, 2020/1, 129.

³⁹ VIDMAR, Neil: *The Psychology of Trial Judging*. Current Directions in Psychological Science, 2011/1, 4. (<https://doi.org/10.1177/0963721410397283>) (letöltve: 2024. 10. 10.)

⁴⁰ BEAZLEY, Doug: *The challenge of AI in the courtroom* <https://www.nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2024/ai-in-the-courtroom> (letöltve: 2024. 10. 11.)

⁴¹ KELETI Arthur: *Nem minden az, aminek látszódnia akar – a deepfake és a hitelesség jelene és jövője*, in Deepfake: A valótlán valóság (szerk: Aczél Petra, Veszelszki Ágnes), Gondolat Kiadó, 2023, 62.

⁴² BEAZLEY, Doug i.m.

⁴³ KLEIN Tamás–TÓTH András: *Technológiai jog - Robotjog - Cyberjog*. 2019, Budapest, Wolters Kluwer Kft. <https://doi.org/10.55413/9789632958293> Letöltve: https://mersz.hu/dokumentum/YOV1766_207/#YOV1766_205_p1 (2024. 10. 11.)

kötelezettség, másrészt a döntéshozók megfelelő felkészítése és edukációja az ilyen helyzetek kezelésre.

A bizonyítékok mérlegelését tekintve a Be. számos garanciális rendelkezést tartalmaz. Ilyennek tekinthető a Be. a 167.§ (3) bekezdésében meghatározott rendelkezés, miszerint a bizonyítékoknak nincs törvényben előre meghatározott bizonyító erejük, vagy a Be. 167.§ (4) bekezdésében meghatározott bizonyítékok értékelésére vonatkozó általános szabályok is segítséget nyújthatnak, hiszen a bizonyítékokat egyenként és összességükben is értékelni kell, és a bizonyítás eredményét az így kialakult meggyőződés alapján kell megállapítani, azonban a kognitív torzítások kapcsán éppen az erre való képesség objektivitása torzulhat.

Megítélésem szerint a Be. által előírt indokolási kötelezettség egy jelentős garanciális szabálynak tekinthető, amelyről a kognitív torzítás relációjában vizsgálva elmondható, hogy egyszerre segíti elő a bizonyítékok mérlegelésére vonatkozó szabályok érvényesülését, és egyszerre ellenőrizhetőséget biztosít a döntési folyamatokat tekintve. Elek Balázs és Háger Tamás rámutatnak arra, hogy „az indokolás fő rendeltetése, hogy a kialakult bírói meggyőződést érvekkel alátámassza, elkerülve az önkényes ítélezés lehetőségét”, valamint elmondják, hogy „a meggyőződés belső folyamatának kialakulását jogi normával nem lehet szabályozni, és ennek során jogi normával nem lehet elhatárolni az objektív jellegű tényezőket.”⁴⁴ A szerzőkkel azonos álláspontra helyezkedve meglátásom szerint igaz, hogy a belső meggyőződési mechanizmusokat jogszabályok által nem lehet szabályozni, azonban az indokolási kötelezettség a bizonyítékok mérlegelése kapcsán mégis kedvező hatással bír a döntési folyamat objektivitására.

Csatlós Erzsébet az indokolási kötelezettségről, mint egyfajta „önkontrollról” számol be. Meglátása szerint az indokolási kötelezettség segíti a határozatok megalapozottságát, mert pusztán annak léte ösztönzi az eljáró szervet arra, hogy a tények felderítésénél és az alkalmazott jogszabályok tekintetében fokozott körültekintéssel járjon el⁴⁵. A meglátásom az, hogy az indokolási kötelezettség arra készíti az eljáró szervet, hogy a döntését racionalizálja, abból kizárja a szubjektív, torzító hatásokat és kizárólag a bizonyítékoknak, tényeknek és jogszabályoknak megfelelő döntést hozzon, amely a torzító hatások egyfajta ellensúlyozásaként is kifejeződik. Az indokolási kötelezettség jelentőségét felismerve a jogalkotó az Alaptörvény XXIV. cikkében is megjeleníti azt, miszerint a hatóságok törvényben meghatározottak szerint

⁴⁴ ELEK Balázs - HÁGER Tamás: *A megalapozott tényállás és az indokolási kötelezettség összefüggései*, Büntetőjogi Szemle 2023/1. 12.

⁴⁵ CSATLÓS Erzsébet: A hatóság indokolási kötelezettségéről, Közjogi Szemle 2024/1. 42.

kötelesek döntéseiket indokolni, valamint a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény 13.§ (1) bekezdésében előírja, hogy a bíróság a határozatát – ha törvény másképpen nem rendelkezik – indokolni köteles. A Be. számos helyen ír elő indokolási kötelezettséget, amelynek teljeskörű bemutatását jelen téma feldolgozásában szükségtelennek tartom, azonban utalnék a Be. 561.§ (3) bekezdés d) pontjára – amelyet bár a törvény az elsőfokú bíróság ügydöntő határozatai fejezetnél ír elő, azonban több helyen is utal rá – miszerint az ügydöntő határozat indokolásának tartalmaznia kell azoknak a bizonyítékoknak a megjelölését, amelyekre a bíróság a döntését alapozta, valamint annak rövid indokolását, hogy a bíróság a tényállás megállapításánál milyen bizonyítékokat és miért vagy miért nem fogadott el.

Más megközelítésből nézve, nem eljárásjogi megoldást kínálva Gábri Angéla megfogalmazza, hogy „minél több tudással rendelkezik a jogásztársadalom a kognitív tudományok által feltárt törvényszerűségekről, annál inkább biztosítható a pontosabb, torzításmentes döntéshozatal, így például a bizonyítás eredményének helyes alapokon nyugvó értékelése is⁴⁶”. Az oktatás felvetése nem idegen, ha a pszichológiai ismeretek és az ítélkezési tevékenység kapcsolatáról van szó: a Kúria *Az ítéleti bizonyosság elméleti és gyakorlati kérdései* című összefoglaló véleményében kifejti, hogy a bírói munka elősegítése érdekében pszichológiai oktatási anyagok, konzultációk szervezése lenne indokolt⁴⁷. A hivatkozott szerzőkkel azonos álláspontra helyezkedve úgy gondolom, hogy ezen kognitív torzítások kiküszöbölése vélhetően egy olyan probléma, amelynek megoldása nem kizárólag jogalkotói kompetencia, annál inkább a jogalkalmazók kognitív tudományokkal kapcsolatos edukációja is ebbe a körbe vonható.

2.3. A kép-, hang- és videófelvevételek bizonyító erejének változása

Ahogy a deepfake hatékonysága egyre inkább köztudomásúvá válik, annál inkább elmondható, hogy a társadalomnak az audiovizuális tartalmak hitelességébe vetett bizalma fokozatosan csökken. Delfino rámutat arra a veszélyre, hogy az angolszász jogrendszerben az esküdtek hajlamosak lesznek még a valódi kép- és hangfelvevételek hitelességét is

⁴⁶ GÁBRI i. m. 110.

⁴⁷ Összefoglaló vélemény - Az ítéleti bizonyosság elméleti és gyakorlati kérdései
https://kuria-birosag.hu/hu/joggyak_csop/osszefoglalo-velemen-y-az-iteleti-bizonyossag-elméleti-es-gyakorlati-kerdesei 28. (letöltve: 2024. 08. 01.)

megkérdőjelezni, és csak akkor nem csökken az ilyen bizonyítékba vetett bizalom, ha van olyan hitelesítő tanú, aki meg tudja erősíteni a bizonyíték valódiságát⁴⁸. Xavier Rodriguez amerikai bíró szerint a deepfake létezése átalakíthatja az igazságszolgáltatási rendszert „még azokban az esetekben is, amelyek nem tartalmaznak hamis videókat, a deepfake-ek pusztán létezése bonyolultabbá teheti a valós bizonyítékok értékelését”⁴⁹. A hazai szakirodalomban Herke Csongor is utal arra, hogy „ahogyan egyre többet tudunk a hamisítványokról és ezáltal egyre szkeptikusabbá válunk az audiovizuális tartalmak hitelességét illetően, előbb-utóbb a valódi digitális tartalmak hitelességében is kételkedni fogunk, még akkor is, ha hitelesítik azt.” Álláspontja szerint ez a probléma jelentkezhet függetlenül attól, hogy a bűnösséget alátámasztó, vagy éppen cáfoló bizonyítékról van szó⁵⁰.

Részben ezzel a jelenséggel, részben az eljárásjogi szabályokkal mintegy „visszaélve” állíthatja a terhelt, hogy az egyébként teljesen hiteles és valódi ellene felmutatott bizonyíték hamis. Ezt az esetet a szakirodalom „deepfake védelem”, vagy a „hazug osztaléka” egyik lehetséges esetének nevezi⁵¹. A deepfake védelem másik esete, amikor a valós bizonyítékok megcáfolására, vagy „alibi” igazolására valaki hamis felvételt készít, illetve meglévőt hamisít⁵². A szakértői bizonyítás és az ítéleti bizonyosság kérdése a dolgozatomban külön részt érdemel, azonban az ismertetett jelenséggel összefüggésben megjegyzem, hogy a hazug osztaléka azért jelenthet jelentős hátrányt a büntetőeljárásra nézve, ugyanis gyakran lehetetlen megállapítani az ítéleti bizonyosság szintjén egy digitális bizonyítékról, hogy az valódi-e, de ha meg is lehet állapítani annak hitelességét, az esetleges szakértői bizonyítás miatt költséges lehet és az eljárás elhúzódásához vezethet.

A túlzott szkepticizmus veszélye azonban álláspontom szerint leginkább az angolszász esküdtszékes eljárásra jelenthet fenyegetést. Nehezen elképzelhetőnek tartom, hogy pusztán az audiovizuális tartalmakkal szemben meglévő általános társadalmi szkepticizmus kifejezésre juthatna egy jogalkalmazói mérlegelés során. Ahogy Herke Csongor fogalmaz, a bizonyítékok értékelése során alapvetés, hogy annak alapját „konkrét bizonyítékból származó tényszerű adat, körülmény kell képezze: az nem feltételezésen alapuló, fel nem merült ténybeliségre vonatkozó

⁴⁸ DELFINO i. m. 312.

⁴⁹ *Deepfakes in Legal Proceedings – A Strategic Framework for Collaborative Solutions* <https://www.jdsupra.com/legalnews/deepfakes-in-legal-proceedings-a-9816082/> (letöltve: 2024. 10. 12.)

⁵⁰ HERKE i. m. 329.

⁵¹ VENEMA E. Agnes – ZENO, Geradts J.: *Digital Forensics, Deepfakes, and the Legal Process*. https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/summer/digital-forensics-deepfakes-and-legal-process/ (letöltve: 2024. 09. 11.).

⁵² HERKE i. m. 325.

spekulatív tevékenység”⁵³. A túlzott szkepticizmus kapcsán pedig nem beszélhetünk a kognitív torzítás hatásáról, hiszen a szkepticizmus a tudatos kételkedés megnyilvánulása, míg a kognitív torzítás – ahogy az erre vonatkozó részben rámutattam – éppen az objektív mérlegelés és a tárgyilagos gondolkodás képességét befolyásolhatja.

A deepfake miatti túlzott bizalmatlanság hátrányos következményekkel járhatna a büntetőeljárásra nézve, egyrészt a kép- és hangfelvételek bizonyító erejének csökkenésében juthatna kifejezésre, másrészt előfordulhatna, hogy a bíróság vagy az eljáró hatóság mindenáron, és minél jobban meg akarná erősíteni az egyébként a valóságnak aggálytalanul megfelelő fénykép hitelességét más bizonyítékokkal, például tanúvallomásokkal vagy szakértő kirendelésével. Tekintve a deepfake technológia adta lehetőséget, az „egészséges szkepticizmus” viszont elfogadható és indokolt lehet. Annak a finom határvonalnak a meghatározása, amely még nem számít eltúlzottnak, már más kérdéskört feszeget, melynek során álláspontom szerint azt kell megvizsgálni, hogy indokolt lenne-e szigorúbb feltételeket támasztani a kép-, hang- és videófelvevételek bizonyítékként való elfogadhatóságára vonatkozóan, valamint a nyomozó hatóság által készített vagy beszerzett felvételek kezelésének szabályozásában. Tekintettel a kérdéskör összetettségére, valamint arra, hogy a korábban kifejtett és a továbbiakban tárgyalt témák szorosan kapcsolódnak hozzá, a válaszadást a szakértői bizonyítással foglalkozó rész után tartom ésszerűnek részletesen kifejteni.

III. A deepfake és a szakértői bizonyítás dilemmái

3.1. Szakértő alkalmazásának szükségessége

Az eddigi büntetőeljárásról szóló törvényeink szabályrendszerében a szakértő alkalmazásának oka töretlenül érvényesül, a Be. 188.§ (1) bekezdése, valamint a büntetőeljárásról szóló 1998. évi XIX. törvény (továbbiakban: régi Be.) 99.§ (1) bekezdése azonos tartalommal előírja, hogy ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni. Már az 1973. évi I. törvény is hasonlóképp fogalmazott, mindössze az „alkalmazni” szó helyett az „igénybe venni” kifejezést használta. Az új Be. miniszteri indokolásában olvashatjuk, „ha valamely tény megállapítása vagy megítélése különleges szakértelmet igényel, akkor a bizonyítás alanyainak kötelezettsége

⁵³ BARTKÓ Róbert – ELEK Balázs – FANTOLY Zsanett – HERKE Csongor: *A büntető eljárásjog tankönyve*, ORAC kiadó (2024) 133.

a szakértő alkalmazása”. A miniszteri indokolás szerint ez olyan átfogó szempontnak tekinthető, ami miatt az új Be. szakít az eddigi tendenciával és nem ad taxatív felsorolást, hogy mely esetekben kötelező szakértőt igénybe venni. Ezzel szemben a régi Be. indoklásában azt olvashatjuk, hogy „a bizonyítandó tény vagy az eldöntendő kérdés természete a különleges szakértelem szükségességét egyes esetekben vitathatatlaná teszi”. Tehát a régi jogalkotói álláspont szerint egyes kérdések eldöntése mindenképp szakértő igénybevételét tette szükségessé. Az új Be. szabályozásában a szakértő igénybevételének kötelezettségeként mindössze a „különleges szakértelem” meghatározás maradt.

A különleges szakértelem mércéjének pontos meghatározására azonban sem a törvényi megfogalmazás, sem a miniszteri indokolás nem vállalkozik, mindössze a régi Be. indoklásában került megfogalmazásra, hogy „a különleges szakértelem alsó határának megvonásakor a mindennapi, általános ismeretek szintjét meghaladó ismeretek szükségességéből kell kiindulni.” Ezzel ellentétben Erdei Árpád szerint a jelenlegi gyakorlat azt mutatja, hogy a különleges szakértelem alsó határának a büntetőeljárásban résztvevő bírónak, ügyésznek, nyomozó hatóság tagjainak általános szakmai ismerete tekinthető⁵⁴. A Kúria egyik összefoglaló véleményében⁵⁵ Csere Katalin fejti ki, hogy „Amennyiben a büntetőeljárásban jelentős tények és körülmények bizonyításához különleges szakértelem kell, mert a mindennapos élettapasztalat, a közönséges tudás, az általános ismeretanyag, valamint a speciális jogi szakismeret a bizonyításhoz nem elegendő, továbbá ha hiányoznak a bizonyított tényekből a nem bizonyított tényekre logikai úton való következtetés feltételei, szakértőt kell igénybe venni”. Csere Katalin megfogalmazásából tehát álláspontom szerint kitűnik, hogy a szakértő kirendelésének egyik lehetséges feltétele, hogy a rendelkezésre álló, bizonyított tények alapján logikailag ne lehessen a bizonyosság adott eljárásjogi szintjén következtetést levonni a nem bizonyított tényekre, amellyel természetesen nem a különleges szakértelem mércéjének meghatározására utal, hanem a bizonyítandó tény meglétére.

Egy gondolat erejéig megállva a logikai következtetés módszerével kapcsolatban fontosnak tartom rögzíteni, hogy a büntetőeljárásban mindvégig figyelemmel kell lennünk az *in dubio pro reo* elvére, amely Be. 7.§ (4) bekezdésében ölt testet, miszerint a kétséget kizáróan nem bizonyított tény nem értékelhető a terhelt terhére. Ennek az elvnek az alkalmazása alapjaiban

⁵⁴ NÉMETH János: *Szakértői bizonyítás indítványozása és elbírálása a büntetőeljárásban, különös tekintettel a magánszakértői vélemény igénybevételére* Büntetőjogi Szemle 2022/1. 71.

⁵⁵ Kúria Joggyakorlat-Elemző Csoport összefoglaló véleménye: *A szakértői bizonyítás a bírósági eljárásban*, Budapest (2014) 254.

határozza meg a büntetőeljárásban a bizonyítékok értékelése során a bizonyosság fokát, így tehát a logikai következtetés módszere is ilyen tekintetben értelmezhető.

A különleges szakértelem alsó mércéjéről megítélésem szerint elmondható, hogy az alapvetően az általános élettapasztalatban, evidens tényekben, speciális jogi ismeretekben, valamint köztudomású tényekben határozható meg, figyelembevételével azt a tényt, hogy az utóbbinak a szintje sem határozható meg általánosságban. Herke Csongor kifejti, hogy mindig az adott ügyben kell vizsgálni, hogy az adott kérdés köztudomásúnak tekinthető-e⁵⁶. Az eljáró hatóság vagy bíróság tagjainak adott szakterületen való személyes képzettsége, szakértelme ugyancsak nem játszhat releváns szerepet a szakértő alkalmazásának kérdésében, ugyanis, ha a kérdés eldöntése különleges szakértelmet igényel, akkor a szakértő igénybevétele nem csak lehetőség, hanem kötelezettség egyaránt⁵⁷.

A deepfake technológia által manipulált, vagy létrehozott bizonyítékok kapcsán annak meghatározásához, hogy mikor szükséges szakértő alkalmazása, a Be. ismertetett szabályozásából levezetve először azt kell megvizsgálnunk, hogy a tényállás tisztázásához szükséges-e különleges szakértelem igénybevétele. A bizonyítékok hitelességének vizsgálata során a különleges szakértelem mércéjének pontos meghatározására való törekvést rendkívül kockázatosnak tartom, éppen a deepfake technológia kiemelkedő megtévesztő képessége miatt. Ehelyett álláspontom szerint olyan esetkörök határozhatóak meg, amikor a jogalkalmazó megnyugtatóan foglalhat állást szakértő igénybevétele nélkül a hitelesség kérdésében.

Az egyik ilyen esetkörnek azt a helyzetet tartom, amikor a deepfake technológia által manipulált felvételen észlelhető tartalom megkérdőjelezhetetlenül és súlyosan ellentétben áll az általános élettapasztalattal. A deepfake technológiának nem minden változata tud kiváló tartalmakat létrehozni, így ilyen szituáció lehet, ha a felvételen súlyos grafikai hibák láthatóak, például a felvételen a vádlott több végtaggal, jelentősen eltorzult testalkattal és fejformával, vagy nem létező helyszínen látható, tehát olyan kategóriába esik, amely ténylegesen nem is vonható be a deepfake fogalma alá, csupán a technológiai háttér részénél kifejtett AIM (tehát a mesterséges intelligencia által alkotott tartalom) tágabb kategóriájába esik.

Egy másik esetkör a korábban ismertetett néma tanú elmélettel és a hash kódok használatával hozható szoros összefüggésbe. A hash kód leegyszerűsítve azt jelenti, hogy egy adott információból – esetünkben kép-, hang- vagy videófelvevételekből – a hash függvény készít egy

⁵⁶ BARTKÓ – ELEK – FANTOLY – HERKE: i.m. 129.

⁵⁷ NÉMETH i.m. 72.

meghatározott hosszúságú kódsort, amivel később azonosítható az eredeti fájl. Amennyiben az eredeti fájlban egy bitnyi adat (tehát az információ legkisebb egysége) is megváltozik, akkor annak a képzett hash kódja is⁵⁸. Ezáltal, ha rendelkezésre áll az eredeti hash kód, akkor annak összehasonlításával szakértő igénybevétele nélkül is könnyedén ellenőrizhető, hogy történt-e módosítás az elektronikus adatban. Ehhez természetesen az szükséges, hogy a hatóság a bizonyítékok rögzítése vagy beszerzése során hash kódokat generáljon az adott fájlhoz.

Herke Csongor rámutat arra, hogy egyes szakirodalmi álláspontok szerint a megfelelő metaadatokkal ellátott bizonyítékok önhibeletesnek tekinthetők, tehát nem igényelnek külső hitelesítést, valamint elmondja azt is, hogy a metaadatok annyira hétköznapi információknak tekinthetők álláspontja szerint, hogy azok vizsgálata önmagában nem szakkérdés, kivéve, ha felmerült annak a manipulációja⁵⁹. A felvételek készítésekor a rögzítő eszköz automatikusan hozzárendel különböző információkat a felvételhez (ezek a metaadatok), mint például az eszköz típusát, sorozatszámát, a felvétel létrehozásának pontos idejét, az eredeti fájlnevet, esetleges módosítás tényét és idejét, sőt egyes esetekben a felvétel készítésének helyét is GPS koordináták megadásával⁶⁰. Vannak olyan adatkinyerő módszerek, amikor teljesen hiányoznak a metaadatok, például a külső megfigyelésen alapuló vizuális adatkinyerés esetén, amikor technikai okok miatt egy készülék kijelzőjén látható adatok (például képek) csak egy külső eszköz kamerája segítségével rögzíthetők, így csak a rögzítést végző eszköz metaadatai lesznek elérhetők, az eredeti felvételé nem⁶¹, illetve más fájlformátumba való mentés vagy szakszerűtlen másolás, továbbítás miatt is bekövetkezhet adatvesztés a metaadatokat tekintve.

Álláspontom szerint azonban óvatossá kell lennünk, ha a metaadatok hitelességéről szeretnénk állást foglalni, ugyanis Kiss Attila László rámutatott arra az interjú során, hogy még a metaadatokkal is bizonytalanná válhat egy felvétel hitelessége, ugyanis a megfelelő szoftverekkel azok módosíthatóak, törölhetők. Elmondta továbbá, hogy a metaadatok is utalhatnak manipulációra, ugyanis a metaadat mélysége, mennyisége eltérő különböző rögzítő eszközöknél. Ennek okán azt gondolom, hogy ha felmerül egy bizonyíték manipulálása egy eljárásban, akkor a metaadatok megléte és hatóság általi ellenőrzése nem indokolhatja az informatikus szakértő jelenlétének mellőzését, azonban a hash kódok összehasonlítása már

⁵⁸ MÁTÉ István Zsolt: *Az igazságügyi informatikai szakértő a büntetőeljárásban*, Doktori értekezés, Pécs, 2017.
⁶¹ <https://pea.lib.pte.hu/bitstream/handle/pea/16947/mate-istvan-zsolt-phd-2017.pdf> (letöltve: 2024. 08. 01.).

⁵⁹ HERKE i. m. 328.

⁶⁰ VENEMA – ZENO i. m.

⁶¹ MÁTÉ István Zsolt – SÁNDOR Gábor: *A mobilkommunikációs eszközök vizsgálatának általános eljárásaira vonatkozó módszertani leírás*: Budapest: NSZKK, 2019. – 27 p.13 (5/2019. (XII.17.) NSZKK főigazgatói körlevél) 14. <https://miszk.hu/index.php/tudastar/kamarai-modszertani-levelek> (letöltve: 2024. 09. 18.)

adott esetben igen. Azonban, ha a bizonyíték nem a rögzítéskor került ellátásra megfelelő hitelesítő információkkal, akkor a hash kód az azt megelőző módosítások észlelésében nem segíthet. Természetesen a metaadatok számtalan esetben hasznos információkkal szolgálnak, csak arra szerettem volna felhívni a figyelmet, hogy korántsem tekinthetők önmagukban olyan hitelesítő információnak, amely kizárná a szakértő alkalmazásának szükségességét.

A mesterséges intelligencia által létrehozott tartalmak kötelező megjelöléséről a dolgozat későbbi részében részletesen foglalkozom, azonban már itt is utalnék arra, hogy a mesterséges intelligencia alapú kép, hang és videó létrehozására vagy manipulálására alkalmas szoftverekkel szemben elő lehet írni, hogy a létrehozott felvételen kerüljön megjelölésre – például vízjelekkel, naplózási-, kriptográfiai módszerekkel –, hogy a tartalom mesterséges intelligencia terméke. Úgy vélem, ha a felvételen olyan jelölés található, ami tanúsítja, hogy azt mesterséges intelligencia hozta létre - és kizárólag ez a kérdés merül fel -, akkor mellőzhető a szakértő kirendelése. Felmerülhetnek azonban olyan esetek is, amikor a mesterséges intelligenciát mindössze arra használták, hogy az adott felvétel élesebb képminőséggel vagy tisztább hangzással rendelkezzen. Ilyen esetekben értelemszerűen indokolt lehet a szakértő bevonása, hiszen fontos lehet, hogy pontosan milyen módosításokat végeztek, esetleg történt-e egyéb, nem közölt manipuláció a felvételen.

A szakértő kirendelésének körében fontosnak tartom kiemelni a túlbizonyítás kérdését. A szakirodalom a túlbizonyításnak klasszikusan két esetét említi. Az egyik eset, amikor olyan tényt kíván az eljáró hatóság vagy bíróság bizonyítani, amely érdektelen a büntetőjogi főkérdés – esetlegesen a járulékos kérdések – eldöntése szempontjából⁶². A felvételek hitelességének relációjában ez azt jelenti, hogy teljesen irreveláns, bizonyító erővel nem bíró felvételek hitelességét azok manipulációjának felmerülése esetén sem indokolt vizsgálni. Természetesen szem előtt kell tartani, hogy a Be. 163.§ (2) bekezdése szerint a büntetőeljárásban a bíróság, az ügyészség és a nyomozó hatóság a döntését valósághű tényállásra alapozza, tehát szükséges a tényállás felderítése, kivéve, ha a döntéshozatal során az nem játszik semmilyen szerepet.

A túlbizonyítás másik esete, amikor a tényállás megállapításához rendelkezésre álló egyéb bizonyítékok alapján már kétséget kizáróan bizonyítható tény vonatkozásában törekszik a hatóság vagy a bíróság további bizonyítást felvenni⁶³. A túlbizonyítás ezen esete azonban álláspontom szerint igen szűk keresztmetszetben jelenhet meg a gyakorlatban, ugyanis egy tény kétséget kizáróan történő megállapíthatóságáról adott eljárási szakaszban ugyanazon eljáró

⁶² GÁRDONYI Gergely: *A bűnügyi szemle*, Ludovika Egyetem Kiadó, Budapest (2023), 90.

⁶³ i. m.

hatóságnak vagy bíróságnak kell állást foglalnia, mint amelyik éppen további bizonyítás felvételére törekszik – az elmélet szerint – a tényállás tisztázása érdekében, így természetesen, ha meggyőződött volna a bizonyítandó tény bizonyosságáról, akkor okafogyottá válna további bizonyítás felvétele. A szűk keresztmetszetben olyan esetek képzelhetők el, amikor például egy bíró az egyéb bizonyítékokat figyelembevéve, az eljárásjogi szabályok és a belső meggyőződése szerint kétséget kizáróan megállapíthatónak tart egy tényt, mégis helyt ad egy bizonyítási indítványnak, holott annak eredményétől függetlenül – például, ha ki is derülne, hogy az adott fényképfelvétel nem a valóságot tükrözi – az egyéb bizonyítékok mérlegelése alapján eljuthatna az ítéleti bizonyosság kialakulásához.

Bár a régi Be. nem sorolta a szakértő alkalmazásának kötelező esetei közé a kép- és hangfelvételek hitelességének vizsgálatát, azonban az új Be. hatálybalépésével – változtatva a korábbi jogalkotói állásponton – már nem is lenne elhelyezhető a törvény logikai rendszerében. Meglátásom szerint ez nem érinti hátrányosan a deepfake technológia kihívásainak való megfelelést, a fentebb leírt eseteket tekintve éppen a szakértő alkalmazásának kötelezővé tétele eredményezhetné a büntetőeljárás szükségtelen elhúzódását, vagy költségesebbé tételét.

3.2. Szakértői megállapítások értékelése a deepfake technológiával szemben

Az analóg technikával rögzített felvételek esetén a szakértők megbízhatóbban tudtak állást foglalni a hitelesség kérdésében, a digitális fényképfelvételek, videók megjelenésével azonban a hitelesség szakértői vizsgálata lényegesen nehezebbé vált⁶⁴. Kiss Attila László az interjú alatt kiemelte, hogy a problémák egyre inkább multidiszciplinárisok válnak, tehát több különböző szakterületről érkező szakértő munkája lehet szükséges egy adott kérdés megválaszolásához, valamint olyan szakterületek is előtérbe kerülnek, amelyekre az eddigi gyakorlat során ritkán volt szükség egy szakkérdés megválaszolásához. Ilyennek tekinthető például a nyelvész szakértő, aki egy hangfelvétel értékelése kapcsán egy személy beszédstílusát, hanglejtését, szóhasználatát értékeli, és az alapján tesz megállapításokat. Előfordulhat, hogy egy hangfelvétel úgy lett manipulálva, hogy azon a vádlott hangja legyen hallható, és még ha meg is tudja állapítani egy hangszakértő, hogy egy felvételen nagyon nagy valószínűséggel a vádlott hangja

⁶⁴ HERKE i.m. 324.

hallható, az egyáltalán nem biztos, hogy a hangfelvétel hitelességének kérdésében is ilyen kijelentést tud tenni, hiszen nem csak az a kérdés, hogy a vádlott hangja hallható-e a felvételen, hanem az is, hogy ténylegesen az ő szájából hangzottak el a felvételen hallottak, vagy az csak manipuláció eredménye.

A szakvélemények megállapításait tekintve megkülönböztethetjük egymástól a kategorikus (vagy teljes bizonyossággal határos valószínűség szintjén álló) szakvéleményeket és a lehetőség szintű bizonyítottságot meghatározó szakvéleményeket⁶⁵. Az egyik legnagyobb kihívást azt jelenti, hogy egy felvétel hitelességét nem mindig tudja egy szakértő teljes bizonyossággal, vagy a valószínűség magas fokán megállapítani, ami komoly bizonyítási problémákat jelenthet akár az in dubio pro reo elvét, akár a „hazug oszaléka” jelenséget tekintve. Herke Csongor kifejti, hogy a deepfake miatt a szakértők sokszor lehetetlen helyzetbe kerülnek, és a büntetőbírónak gondosan mérlegelni kell, hogy elrendeljen-e egy költséges és időigényes szakértői bizonyítást, ami nem biztos, hogy eredményre vezet⁶⁶. Természetesen nem ismeretlen az a jelenség, hogy bizonyos szakkérdésekben a szakértők csak a valószínűség egy szintjén tudnak megállapításokat tenni, például a DNS vizsgálatoknál is százalékos valószínűségi számítás a vizsgálati módszer eredménye⁶⁷, de elképzelhetőek olyan esetek is, amikor az informatikus szakértő az adott bizonyítékról azt ki tudja jelenteni, hogy a felvétel és a metaadatok alapján a vizsgálati módszerei szerint nem volt kimutatható manipulációra utaló jel, azonban ez korántsem jelenti azt, hogy bizonyosan hiteles a bizonyíték, hiszen – ahogy már említettem – a metaadatok is manipulálhatóak.

A Magyar Igazságügyi Szakértői Kamara 3/2020 módszertani levele beszélőazonosítási vizsgálatok esetén is egy 9 szintű skálát határoz meg, melynek legmagasabb valószínűségi szintje a „+4”-es skála, ami azt jelenti, hogy a két beszédhang nagyon nagy valószínűséggel azonos személytől származik, míg a „-4”-es skála jelentése, hogy a két beszédhang nagyon nagy valószínűséggel különböző személytől származik⁶⁸. A Kúria joggyakorlat elemző csoportjának egyik összefoglaló véleményében is azt olvashatjuk, hogy „a speciális szakértelmet igénylő

⁶⁵ BÁNYAI István: *Az igazságügyi szakértő helye, szerepe a döntéshozatalban*, Magyar Jog, 2020/2., 121.

⁶⁶ HERKE i.m. 328.

⁶⁷ Országos Igazságügyi Orvostani Intézet 22. számú módszertani levele polgári perekben és büntetőügyekben végzett DNS-vizsgálatokhoz és szakvéleményadáshoz, https://semmelweis.hu/igazsagugy/files/2012/06/22_mszlev.pdf 5. (letöltve: 2024. 10. 18.)

⁶⁸ Magyar Igazságügyi Szakértői Kamara 3/2020 módszertani levele a beszélőazonosító vizsgálatokról (2020), <https://miszk.hu/index.php/tudastar/kamarai-modszertani-levelek> 11. (letöltve: 2024. 09. 18.)

kérdések jelentős részében – a szakkérdés jellege miatt – ténylegesen nem is lehet kategorikus, vagy a teljes bizonyossággal határos valószínűség szintjén álló szakvéleményt adni”⁶⁹.

Felvetődik tehát a kérdés, hogy miként lehet összeegyeztetni a szakértő által megállapított valószínűségi mércéket az in dubio pro reo elvével és az ítéleti bizonyosság szigorú követelményével. Különösen a büntetőeljárásban történő bizonyítást tekintve lehet aggályos a valószínűség alacsony szintje, ugyanis a bizonyosság mércéjének követelménye itt a legmagasabb⁷⁰. Márpedig, ha a kétséget kizáróan nem bizonyított tény nem értékelhető a terhelt terhére, akkor a valószínűségi szinten történő szakértői meghatározások önmagukban nem nyújthatnak elegendő alapot a tényállás tisztázásához. Bányai István kifejti, hogy ha a szakértői megállapítás önállóan nem alkalmas a feltett szakkérdés aggálytalan eldöntésére, akkor egyéb bizonyítékokkal való összevetése adhat megoldást⁷¹, valamint kiemeli, hogy „a szakmai tények jellemzője, hogy kirendelő hatóság az adott tényt csak a szakértői értelmezés, átminősítés alapján tudja jogi sémába illeszteni”⁷².

Úgy vélem, hogy a szakértői megállapítások bizonyossága az adott szakterület szabályai szerint kerülnek megállapításra, ezért az adaptálni kell a büntetőeljárás fogalmi rendszerébe, amely egy elméleti síkon történő értékelési folyamat, nem pedig automatizmus. Kuhl Andrea is rámutat arra, hogy a szakvélemény valószínűsége nem esik mindig egybe a bírói bizonyosság fokával, ezért a hibalehetőségek elkerülése miatt mindig a többi bizonyítéknak és az eset egyéb körülményeinek körültekintő vizsgálatával kell a szakvélemény bizonyító erejét megítélni⁷³. Tehát elmondható, hogy a szakértői véleményt, mint bizonyítékot, a bíróságnak vagy a kirendelő szervnek az összes bizonyítékkal egybevetve is értékelni szükséges, amelybe beletartoznak a személyi és egyéb tárgyi bizonyítékok, valamint ide sorolhatóak a gyanújelek is⁷⁴. Ahogy az előző bekezdésben leírtak szerint is látható, több olyan eset is van, amikor nem várható el egy szakvéleménytől, hogy kategorikus megállapításokat tartalmazzon, viszont a bíróság a tényállás megállapítása során természetesen nem csak a szakvéleményre támaszkodik, így ez még nem feltétlenül jelenti akadályát a tényállás tisztázásának.

⁶⁹ Kúria Joggyakorlat-Elemző Csoport összefoglaló véleménye: *Az ítéleti bizonyosság elméleti és gyakorlati kérdései*, Budapest (2017) 101.

⁷⁰ i. m. 36.

⁷¹ BÁNYAI i.m. 121-122.

⁷² BÁNYAI István: *Az igazságügyi szakértői tevékenység módszertani kérdései*, Magyar Jog, 2016/7-8., 437.

⁷³ KUHL Andrea: *Az ítéleti bizonyosság és a szakvélemények értéke*, Miskolci Jogi Szemle, 2023/1., 99.

⁷⁴ Gyanújelnek nevezhetők azok az adatok, amelyek önmagukban bizonyítékoknak nem tekinthetők, de olyan tényeket igazolhatnak, amelyek a bizonyítékok megerősítésére vagy cáfolatára szolgálhatnak, forrás: BARTKÓ – ELEK – FANTOLY – HERKE i.m. 131-132.

Az egyik legnagyobb probléma viszont az, hogy a deepfake technológia fejlődésével tömegessé válhat az a jelenség, hogy a szakértők lehetetlen helyzetbe kerülnek és nem tudnak a bizonyosság magas fokán sem állást foglalni a bizonyítékok hitelességét illetően, ezáltal jelentősen csökkenhet az kép-, hang- és videófelvevételek legnagyobb előnye, hogy nagyon pontos, objektív és megbízható adatokat szolgáltatnak, ami eddig kiemelkedő bizonyító erőt jelentett számukra. A deepfake technológia ezen hatásával kapcsolatban Herke Csongor kifejti, hogy a deepfake technológia megjelenésével a gyakran túlértékelt tárgyi bizonyítékok súlya csökkenni látszik, valamint azt is elmondja, hogy „még nem jelenthetjük ki, hogy ez a személyi jellegű bizonyítékok újbóli felértékelődéséhez és elsődlegességéhez vezet, azonban a tárgyi bizonyítékok értékét messzemenően meg fogja határozni, hogy mennyire lehet azok valódiságát igazolni és meghamisíttóságát cáfolni⁷⁵”.

Visszaautalva a *kép-, hang- és videófelvevételek bizonyító erejének változása* részhez, a szakértői bizonyítás kapcsán is hangsúlyozni kívánom, hogy álláspontom szerint a szakértői bizonyítás nehézségei még nem fogják eredményezni a felvevételek bizonyító erejének általános csökkenését, legfeljebb adott ügyben kell majd az adott elektronikus bizonyítékot kirekeszteni a bizonyítékok köréből, és kizárólag az egyéb bizonyítékokra támaszkodni. A szakértők számtalan esetben megnyugtató választ tudnak adni a bizonyítékok hitelessége kapcsán, ezért a deepfake technológia fejlődésével érkező kihívások leküzdésében is jelentős szerepet tölthetnek be a büntetőeljárásban, azonban mint láthattuk, gyakran ők sem fognak tudni állást foglalni a hitelesség kérdésében, ezért messzemenőleg nem tekinthető megoldottnak a bizonyítékok megbízhatóságának problémája. Elengedhetetlen, hogy a szakértői vélemények mellett egyéb bizonyítási eszközök is előtérbe kerüljenek, valamint olyan jogi és technológiai megoldások alkalmazása szükséges, amelyek a bizonyítékok hitelességének megőrzését és ellenőrizhetőségét elősegítik.

⁷⁵ HERKE i.m. 325.

IV. A hitelesség biztosítását, ellenőrzését segítő intézkedések

Megítélésem szerint a bizonyítékok hitelességének megőrzése a büntetőeljárásban egyfajta „új irányvonalként” kiemelkedő jelentőséget kell, hogy kapjon. Indokolt lenne a technológia fejlődése által érkező kihívások kezelésére olyan jogi és technológiai megoldások alkalmazása, amelyek a bizonyítékok hitelességének megőrzését és ellenőrizhetőségét aggálytalanul biztosítják. Elengedhetetlen annak vizsgálata, hogy a jog milyen követelményeket fogalmazzon meg a digitális bizonyítékok kezelésére vonatkozóan. Ezzel összefüggésben különös figyelmet érdemel a deepfake tartalmak kötelező megjelölésének kérdése, amely a jövőben álláspontom szerint jelentős mértékben megkönnyítheti a hamisított tartalmak felismerését és a hamisított tartalmak számának csökkentését.

A kutatásom során felmerült bennem az a kérdés, hogy hasznos lenne-e a bíróságoknak, hatóságoknak az automatikus deepfake detektáló szoftverek alkalmazása. A deepfake detektáló algoritmusok olyan mesterséges intelligencia alapú szoftverek, amelyek képesek meghatározni bizonyos tartalmakról, hogy azok mesterséges intelligencia által generált tartalmak-e, vagy valódiak, akár olyan apró jelekből is, amelyet az emberi érzékelés nem képes azonosítani. Ez a technológia koránt sem nevezhető megbízhatónak, ugyanis számtalan esetben hamis pozitív és hamis negatív eredményeket mutat⁷⁶, valamint miután a felismerő algoritmus nyilvánossá válik, könnyen előfordulhat, hogy egy deepfake tartalom készítő megkerüli az algoritmust, tehát annak hatékonysága és megbízhatósága dinamikusan változó⁷⁷. Mindezekre figyelemmel a felismerő szoftver alkalmazását kizárólag a szakértők eszköztárában tudom elképzelni, méghozzá olyan formában, hogy az algoritmus által megjelölt potenciális hamisításokra utaló jeleket a szakértő további vizsgálatoknak rendeli alá⁷⁸.

⁷⁶ Palmiotto, Francesca: *Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective*, 2023, 7-8. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384122 (letöltve: 2024.10.20.)

⁷⁷ VENEMA – ZENO i.m.

⁷⁸ Itt visszautalnék a dolgozat deepfake technológiai meghatározásával foglalkozó részéhez, ahol a diszkriminátor és a generátor modell versengését mutattam be, mint a deepfake egyik mozgatórugóját. A felismerő szoftver eredményessége elsősorban azon múlik, hogy az adott deepfake technológia diszkriminátor modelljétől fejlettebb-e, ezt nevezhetjük az „algoritmusok harcának” is.

4.1. Vízjelek, egyéb megjelölések használata

A deepfake technológia által létrehozott tartalom megjelölésére már nem csak szakirodalmi álláspontokat, hanem Európai Unió jogalkotási eredményeket is láthatunk. Az AI Act 50. cikk (2) bekezdése előírja, hogy „a szintetikus hang-, kép-, video- vagy szöveges tartalmat létrehozó MI-rendszerek (...) szolgáltatóinak biztosítaniuk kell, hogy az MI-rendszer kimeneteit géppel olvasható formátumban jelöljék meg, és azok mesterségesen létrehozottként vagy manipuláltként észlelhetők legyenek (...)” valamint a (4) bekezdés első felében rögzíti, hogy „az olyan MI-rendszerek alkalmazóinak, amelyek eredetinek vagy valóságosnak tűnő („deepfake”) kép-, hang- vagy videotartalmat hoznak létre vagy manipulálnak, közölniük kell, hogy a tartalmat mesterségesen hozták létre vagy manipulálták (...). Továbbá fontos kiemelni, hogy az AI Act. (133) preambulumbekkezdésében megfogalmazza, hogy a kötelező jelölés történhet vízjelekkel, metaadat-azonosításokkal, a tartalom eredetének és hitelességének bizonyítására szolgáló kriptográfiai módszerekkel, naplózási módszerekkel, ujjnyomatokkal és egyéb technikákkal is.

Egy gondolat erejéig megállva különösen hangsúlyozni kívánom, hogy az AI Act vonatkozó rendelkezéseit kizárólag a kötelező jelölések előírása és a hitelesség ellenőrzésének összefüggéseiben vizsgálom, még elméleti síkon sem kívánok elrugaszkodni a dolgozat célkitűzésétől, ezért a mesterséges intelligencia szabályozásának egyéb aspektusait és bőséges jogalkotási eredményeit tartalmi és célszerűségi okokból nem mutatom be. Mindössze utalni szeretnék arra, hogy az AI Act vonatkozó rendelkezései tesznek kivételt a kötelező mesterséges intelligencia jelölés alól, például, ha a tartalom nyilvánvalóan művészeti, fiktív stb.

Az AI Act rendelkezéseit – kivételekkel – 2026. augusztus 02. napjától kell alkalmazni, beleértve ebbe az ismertetett 50. cikket is. Ahogy a (133) preambulumbekkezdésben olvasható, a mesterséges intelligencia által létrehozott vagy manipulált tartalom nem csak vízjelekkel jelölhető. Ennek azért is van jelentősége, mert nem csak a képeken vagy videókon lehetséges vízjelek feltüntetése, hanem hanganyagok tekintetében is elő lehet írni egyéb kötelező jelölést, illetve fokozottabb védelmet jelenthet ezek együttes alkalmazása. Az 50. cikk vonatkozó rendelkezéseiben meghatározott jelölés azt a célt szolgálja, hogy egyértelműen meg lehessen állapítani egy tartalomról, hogy mesterséges intelligencia hozta létre, illetve, ha az már deepfake tartalomnak minősül (tehát ha valóság-hű tartalom jön létre) akkor a kvázi

felhasználókra (mesterséges intelligencia rendszert alkalmazókra) is közzéi kötelezettséget ír elő a rendelet.

A vízjelek és egyéb mesterséges intelligencia megjelölések azonban két okból sem jelenthetnek teljeskörű megoldást a hamis bizonyítékok tekintetében. Egyrészt, még ha az online mesterséges intelligencia szolgáltatások teljesen megfelelnek egy jelölési kötelezettségnek⁷⁹, akkor is lehetséges lenne vízjelek nélkül létrehozni deepfake tartalmakat némi informatikai ismeretek birtokában, ugyanis az internet különböző oldalain elérhető szoftverek és nyilvános forráskódok segítségével könnyedén produkálható jelölés nélküli deepfake tartalom⁸⁰. Másrészt elmondható, hogy a vízjelek és egyéb jelölések eltávolítása viszonylag könnyen megoldható, így akinek kifejezetten az a célja, hogy a deepfake technológia felhasználásával bizonyítékot hamisítson vagy hamis tartalmakat hozzon létre, az gondoskodni fog a jelölés eltávolításáról, vagy eleve nem tesz eleget a jelölési, közzéi kötelezettségének⁸¹.

Azonban nem szabad alábecsülnünk a vízjelek és egyéb jelölések kötelező alkalmazásában rejlő potenciált. A deepfake technológia egyik alapvető veszélye éppen abban rejlik, hogy bárki, speciális szaktudás nélkül képes professzionálisan bizonyítékot hamisítani, egy ilyen szabály alkalmazása pedig a laikus tömegek által előállított deepfake tartalmak könnyű ellenőrizhetőségét tenné lehetővé. Egy ilyen szabály széleskörű alkalmazása hatékony választ adhat a technológia egyik legnagyobb kihívására, ugyanis jelentősen mérsékelheti a mesterséges intelligencia által manipulált bizonyítékok megjelenését.

4.2. Hitelesítő szoftverek alkalmazása

A deepfake technológia rendkívüli megtévesztő képességét felismerve az elmúlt időszakban számtalan technológiai megoldás született a felvételek hitelességének megőrzése és későbbi bizonyítása érdekében. Ilyennek tekinthető például az „eyewitness to Atrocities” szoftver, amely több forrásból származó adat alapján hitelesen rögzíti a felvétel készítésének időpontját és helyszínét, valamint egy digitális ujjlenyomatot hoz létre, amely biztosítja a felvétel hitelességét. A rendszer felhőalapú, tehát a felvételek a felvevő eszköztől elkülönülten is rendelkezésre állnak, ami további védelmet biztosít a manipuláció és esetleges adatvesztés

⁷⁹ Úgy vélem, hogy az AI Act vagy egyéb jogforrások rendelkezései ellenére is a közeljövőben egyelőre messze fogunk állni ettől az állapottól, részben joghatósági akadályok miatt.

⁸⁰ LINNA JR, Daniel W. – DALAL, Abhishek – GAO, Chongyang – GRIMM, Paul W. – GROSSMAN, Maura R. – PULICE, Chiara – TUNHEIM Hon. John: i.m. 8.

⁸¹ HERKE i.m. 331.

ellen. A szoftver biztosítja a felügyeleti lánc követhetőségét, illetőleg a tárolt elektronikus adatok magas szintű kibervédelemmel vannak ellátva, megakadályozva ezzel, hogy az adatok hackertámadások áldozatául essenek⁸². Ezeknek a szoftvereknek az egyik legfontosabb hitelességet biztosító eleme a hash kódok használata. A hash kódok a dolgozatomban már ismertetésre kerültek, viszont fontos rögzíteni, hogy a hitelességet biztosító szoftverek a hash kódot már a felvétel rögzítésekor, amikor a fájl „lezárul” hozzárendelik az adott fájlhoz, így annak is kizárják a lehetőségét, hogy a felvétel készítése és a hash kód generálása között történik a manipuláció⁸³. Kiss Attila László is megerősítette az interjú alatt, hogy ha nem a rögzítéskor történik a hitelesítés, akkor a bizonyítékok hitelessége bizonytalanná válik, ezért elengedhetetlen, hogy ez a folyamat azonnal, már a rögzítéskor megtörténjen. Hozzáteszem, hogy a hitelesítő szoftverek széleskörben hozzáférhetőek, például az eyewitness to atrocities alkalmazás könnyedén letölthető okostelefonokra is, akár a Google Play áruházból⁸⁴.

A felvételek hitelesítő szoftver segítségével történő rögzítése kétségtelenül hatékony védelmet nyújt a deepfake technológia általi hamisítás ellen, valamint könnyedén cáfolhatóvá teheti egy eljárásban azt az állítást, hogy a bemutatott felvétel manipulált. Felmerül azonban annak a kérdése, hogy a bizonyítékok elfogadhatóságának szempontjából megfogalmazható-e olyan kritérium, amely kötelezővé tenné, hogy a bizonyítékok hitelesítő szoftverrel kerüljenek rögzítésre. Úgy gondolom, hogy e kérdés kapcsán azt érdemes vizsgálni, hogy a hitelesítő szoftver kötelező előírása konfliktusba kerülhet-e a fegyverek egyenlőségének elvével, valamint a tisztességes eljáráshoz való joggal.

A tisztességes eljárás követelménye az Alaptörvény XXVIII. cikkének (1) bekezdésében is megjelenik, miszerint „mindenkinek joga van ahhoz, hogy az ellene emelt bármely vádat vagy valamely perben a jogait és kötelezettségeit törvény által felállított, független és pártatlan bíróság tisztességes és nyilvános tárgyaláson, ésszerű határidőn belül bírálja el”. Az alkotmánybíróság kifejti a 22/2014. (VII. 15.) AB határozatának [49] bekezdésében, hogy „(...) nevesíthetők a tisztességes eljáráshoz való jog tartalmát kitöltő ún. részjogosítványok. Ezek különösen: a bírósághoz fordulás joga, a tárgyalás igazságossága, (...) a tárgyalás nyilvánosságának és a bírói döntés nyilvános kihirdetésének a követelménye, törvény által létrehozott bíróság, a bírói függetlenség és pártatlanság kívánalma, továbbá az ésszerű időn belüli elbírálás. A szabály de facto nem rögzíti, de az Alkotmánybíróság értelmezése szerint

⁸² <https://www.eyewitness.global/> (megtekintve 2024.10.22.)

⁸³ <https://www.eyewitness.global/Using-metadata> (megtekintve 2024.10.31.)

⁸⁴ <https://play.google.com/store/apps/details?id=com.camera.easy&pli=1> (megtekintve: 2024. 10. 23.)

része a tisztességes eljárásnak az is, hogy az eljárásban biztosítva legyen a fegyverek egyenlősége”, valamint egy bekezdéssel később visszautalva korábbi döntésére rögzíti az Alkotmánybíróság, hogy „a tisztességes eljáráshoz való jog abszolút jog, amellyel szemben nem létezik mérlegelhető más alapvető jog vagy alkotmányos cél, mert már maga is mérlegelés eredménye”. A tisztességes eljárás részeként a fegyverek egyenlőségének elvéről Elek Balázs kifejti, hogy az elv azt biztosítja, hogy vádnak és a védelemnek egyenlő esélye és alkalma legyen a büntetőper menetét alakítani⁸⁵.

Elmondható tehát, hogy a fegyverek egyenlőségének elve a tisztességes eljáráshoz való jog egyik részének tekinthető. A tisztességes eljáráshoz való jog kapcsán az Alkotmánybíróság vonatkozó határozataiból is kitűnik, hogy azt abszolút jognak tekinti, amely alapjogi védelmet élvez.

Elek Balázs kifejti, hogy a védelem nyilvánvalóan hátránnyal indul, emiatt szükséges az, hogy az államhatalom túlsúlyával szemben a felelősségre vont személy megfelelő eszközökkel rendelkezessen a vád vitatására. A kötelező hitelesítő szoftverek alkalmazása körében elmondható, hogy a hatóságok jelentős anyagi, technikai és személyi erőforrásokkal rendelkeznek, mely könnyedén lehetővé teszi a szükséges szoftverek telepítését, működtetését, valamint a hatóság tagjai nyilvánvalóan tudják, hogy a felvételeket bizonyítékként rögzítik. Ez a helyzet azonban ritkán mondható el a terheltről, illetve egy ilyen előírás alkalmazása sok esetben ellehetetleníthetné a védekezését, ha bizonyítékait nem az elvárt módon rögzítette, tehát nem lehetne biztosítani azt, hogy megfelelő eszközökkel rendelkezzen a vád vitatására. Egy kötelező hitelességi előírás álláspontom szerint nem összeegyeztethető a fegyverek egyenlőségének elvével és a tisztességes eljárás követelményével, hiszen ez olyan helyzetet teremtene, mintha a bíróságnak egy olyan előfeltevése lenne a terhelt vagy a védelem által benyújtott bizonyítékokról, hogy azok nem hitelesek, és a védelemnek kellene bizonyítania annak ellenkezőjét, – emiatt a bizonyítási teher is megfordulna – holott a nyomozó hatóság már a nyomozás vagy az előkészítő eljárás alatt olyan bizonyítékokat szerzett, amelyek kétségtelenül hitelesnek és elfogadhatónak tekinthetők.

Álláspontom szerint a szélsőséges megközelítések helyett olyan jogi normák kialakítására van szükség, amelyek hatékony védelmet biztosítanak a deepfake technológia okozta veszélyekkel szemben, ugyanakkor ezek a szabályok nem vezethetnek más garanciális

⁸⁵ ELEK Balázs: *A favor defensionis elv megjelenései az új büntetőeljárási törvény rendes perorvoslataiban*, Magyar Jog, 2021/10., 573.

szabályok sérelméhez vagy korlátozásához. Éppen ezért, a hitelesítő szoftverek kötelező alkalmazását nem a bizonyítékok elfogadhatóságának körében tartom indokoltnak előírni, hanem a nyomozó hatóság bizonyítékok rögzítésére, beszerzésére vonatkozó tevékenysége kapcsán. Amennyiben a nyomozó hatóság minden általa rögzített vagy beszerzett felvételt hitelesítő szoftver segítségével kezelne, akkor az egyrészt jelenthetne egy garanciális szabályt arra vonatkozóan, hogy a terhelt ellen felhozott bizonyítékok a nyomozó hatóság által biztosan nem kerültek hamisításra, másrészt a későbbi esetleges bizonyítási eljárás során is könnyebben cáfolhatóbbá tenné a terhelt azon állítását, hogy a bemutatott bizonyítékok hamisak.

Természetesen nem minden elektronikus adatot a nyomozó hatóság rögzít. Az elektronikus adatok beszerezhetőek kényszerintézkedés során, egyszerűen adatkéréssel vagy a hatóság önálló rögzítésével egyaránt⁸⁶. Így például a térfigyelő kamerarendszerek videói vagy a tanúk által benyújtott fényképek tekintetében ez a garanciális szabály csak attól az időponttól nyújthatna bizonyosságot a hitelesség kérdésében, amikor a nyomozó hatóság a beszerzett bizonyítékokat ellátja a szükséges hitelesítő információkkal⁸⁷. Az előzetes módosítás kiszűrésére ez a technikai megoldás nem alkalmas, viszont nem is erre hivatott.

4.3. A bűnjelkezelés egyes kérdései

Az elektronikus adatok lefoglalására, beszerzésére és kezelésére vonatkozó előírások és szakmai anyagok bőséges ismeretanyagot jelentenek, azonban e dolgozat keretei között kizárólag a hitelesség megőrzésének kérdésében kívánok kiemelni néhány kritikus pontot.

Az elektronikus adatok változatlanságának biztosításával kapcsolatban több jogi normával is találkozhatunk, például a 11/2003 (V. 8.) IM-BM-PM együttes rendelet (a továbbiakban: IM-BM-PM együttes rendelet) az elektronikus adatok lefoglalása kapcsán a 67/A. § (3) bekezdésében rögzíti, hogy ha az átmásolás utólag megváltoztatható adathordozóra történik, biztosítani kell az adatok változatlanságát, vagy azt, hogy a megváltoztatás nyomon követhető legyen, illetve a 100/2018. (VI. 8.) Korm. rendelet (a továbbiakban: Korm.rendelet) 86.§ (1) bekezdésében leírja, hogy az információs rendszer átvizsgálása során biztosítani kell az

⁸⁶ HERÉDI István: *Az elektronikus adatokat érintő eljárási cselekmények végrehajtása*, in: Kibernetizációs kézikönyv (szerk: Nagy Zoltán András), Ludovika Egyetemi Kiadó, 2022, 155.

⁸⁷ A jelenleg még a hash kódok használata sem vált gyakorlattá, viszont a hatóság vagy bíróság által elektronikusan kezelt adatok vonatkozásában most is van lehetőség biztosítani az adatok megváltoztathatatlanságát – például fokozott biztonságú elektronikus aláírás által –, azonban ez a művelet sem automatikus, szükséges hozzá az ügykezelő rendszerbe történő feltöltés.

információs rendszer útján – védelmi eszköz vagy informatikai megoldás megkerülése vagy kijátszása nélkül – hozzáférhető adatok megismerését és rögzítését is, függetlenül az adatok elhelyezkedésétől, illetve e bekezdés második fordulatóban előírja, hogy az információs rendszer útján hozzáférhető adatok megismerése és rögzítése során biztosítani kell a megismert adatok változatlanóságát. Fontosnak tartom még kiemelni az IM-BM-PM együttes rendelet 67/A.§ (2) bekezdését, amely arról rendelkezik, hogy az elektronikus adat lefoglalásakor az átmásolás lehetőleg utólag meg nem változtatható adathordozóra történhet, amely egyéb adatokat nem tartalmazhat.

Az elektronikus adatokkal összefüggésben Kiss Attila László is kiemelte az interjú alatt, hogy ha azok hitelességéről szeretnénk megbízhatóan állást foglalni, akkor mindvégig biztosítani kell azok „bitazonos” (tehát tökéletesen megegyező, például a metaadatokat tekintve is) rendelkezésre állását. Erre megfelelő megoldást nyújt a korábban ismertetett hash kódok és hitelesítő szoftverek használata, mellyel kapcsolatban a szakértő elmondta, hogy a szakmai ajánlások szerint legalább kettő különböző hash kóddal való biztosítás nevezhető megfelelőnek. Amikor a hatóság az elektronikus adatokat átmásolja egy tároló eszközre, már akkor nagyon fontos, hogy a másolás⁸⁸ bitazonosan történjen.

Herédi István is kiemeli, hogy alapvető követelmény, hogy a másolt adatállomány ne legyen megváltoztatható, biztosítani kell az eredetivel való megegyezést, így a másolás nem szabad, hogy az operációs rendszerbe beépített másolási algoritmusok használatával történjenek⁸⁹. Mezei Kitti álláspontja szerint, ha hagyományos módon történik az adathordozóra történő másolás, az problémás lehet a hitelesség érvényesülésének szempontjából. Úgy véli, hogy a digitális bizonyíték hitelességéhez hozzátartozik, hogy a későbbiekben pontosan meghatározható legyen, hogy az adat mely rendszerről származik, az elektronikus adat pontos és teljes másolatának lefoglalására került sor, amely változatlan maradt⁹⁰. Ennek fényében a hitelesség biztosításához hozzátartozik az IM-BM-PM együttes rendelet 67/A.§ (3) bekezdésének első fordulója is, amely előírja, hogy a hatóságnak fel kell tüntetni az átmásoláshoz használt adathordozó típusát, gyártási számát, illetve a rajta tárolt adat jellegét és

⁸⁸ Ebbe a körbe sorolható az áthelyezés is, ami technikailag egy másolási és az eredeti eszközről való törlési folyamatban tevődik össze.

⁸⁹ HERÉDI István: i.m. 160.

⁹⁰ MEZEI Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban*, Társadalomtudományi Kutatóközpont Jogtudományi Intézet – L'Harmattan, Budapest, 2020. 222.

tartalmát. Ezentúl biztosítani kell az átmásolás során, hogy az eredeti adatok ne változzanak meg, amihez írásvédő eszközök vagy szoftverek alkalmazása szükséges⁹¹.

A szakértő elmondta, hogy gyakran előfordul, hogy már az elektronikus adatok másolása sem bitazonosan történik, például a tárhelykapacitási okokból átkonvertálják az adott felvételt, azonban ez adatvesztéssel (például a metaadatok vesztesével) járhat. A szakértő szerint nagyon fontos, hogy amennyiben lehetséges, az eredeti rögzítő eszköz is rendelkezésre álljon, de ha ez nem biztosítható, akkor a lefoglalt adatok kapcsán fontos lenne legalább annak a rögzítése, hogy pontosan milyen eszközzel és mikor történt az adott kép-, hang- vagy videófelvétel rögzítése. Ha tudjuk, hogy milyen eszközzel történt a rögzítés, akkor az is meghatározható, hogy milyen mélységű és mennyire részletes metaadatoknak kell (vagy kellene) rendelkezésre állnia, például az Iphone telefonok több metaadatot rögzítenek egy felvétel készítésekor, mint az Android rendszerrel rendelkező készülékek. Ez a későbbiek során azért is fontos lehet, mert ha egy adott felvételhez tartozó metaadatok nem olyanok, mint amelyet a rögzítő eszköz generál, akkor az utólagos manipulációra utalhat. A szakértő olyan esettel is találkozott, amikor már bírósági eljárásban az ügykezelő rendszeren keresztül küldték meg a bíróságnak az adott felvételt, amit aztán CD-re másoltak és úgy küldték meg az informatikus szakértőnek, viszont a fájl metaadataiban a bíróságon keletkezett adatok voltak csak láthatóak, hiszen az elektronikus ügyintézésnek köszönhetően azok rögzültek, az eredetiek pedig nem voltak elérhetőek.

Az elektronikus adatok bűnjelként való kezelése természetesen sokkal több tényezőt foglal magában, mindössze arra szerettem volna rámutatni, hogy a hitelesség biztosításának szempontjából elengedhetetlen, hogy az elektronikus adatok az eljárás alatt mindvégig változatlanul rendelkezésre álljanak. Úgy vélem, hogy a deepfake korában különösen fontos, hogy a bizonyítékok hitelessége kétséget kizáróan igazolható legyen, ezért indokolt lenne előírni a hatóságoknak a hitelesítő eljárások alkalmazását.

⁹¹ i.m. 223.

Záró gondolatok

A deepfake technológia olyan lendületes fejlődésének lehetünk szemtanúi, amely egy dinamikusan változó környezetben állítja kihívások elé a büntető eljárásjogot. A kihívásoknak való megfelelés pedig feltételezi azt, hogy meg tudjuk ragadni a deepfake jelentésének lényegét. A technológiai ismeretek és különböző definiálási törekvések ismeretében kijelenthetjük, hogy a deepfake olyan mesterséges intelligencia alapú technológia, amely alkalmas kép-, hang- és videófelvevételek létrehozására vagy manipulálására oly módon, hogy azok megtévesztően hitelesnek és valóságosnak tűnjenek.

A technológia megtévesztő képességét tekintve szükségesnek tartottam a dolgozatban feltérképezni azt, hogy a deepfake milyen hatással lehet a bizonyítékok mérlegelésére, valamint a klasszikus értékelési elméletek alkalmazhatóságára.

A néma tanú elmélet abból a feltételezésből indul ki, hogy a képfelvevételek objektív információkat tartalmaznak, ezért nem szükséges az elfogadhatóságukhoz egy külső hitelesítő forrás, egy tanú, hanem a bizonyíték egyfajta „néma tanúként” ad megbízható információt a tényekről. Mára már meghaladottá vált ez az elmélet, azonban, ha megfelelő hitelesítő szoftverek, hash kódok alkalmazásával kerülnek rögzítésre a kép-, hang- és videófelvevételek, akkor olyan kétséget kizáró bizonyosságot adhatunk a bizonyítékoknak, amelyek a hitelességüket a régről ismert néma tanú elmélet szerinti bizonyítékok szintjére emelné. Azonban ezt az elvárást nem szabad a bizonyítékok elfogadhatóságának általános kritériumaként megfogalmazni, hiszen a hatóságok jelentős emberi, technikai és anyagi erőforrással rendelkeznek, valamint tisztában vannak azzal, hogy a felvételek bizonyítékként kerülnek rögzítésre, melynek köszönhetően könnyen meg tudnának felelni ilyen kritériumoknak, ellenben a fegyverek egyenlőségének elvét sértené az, ha a védelem, a terhelt nem tudna hatékonyan védekezni, nem tudná alakítani a büntetőeljárás menetét. Viszont a hatóság által rögzített bizonyítékok kötelező hitelesítése garanciális szabályt nyújtana a terheltnek arra vonatkozóan, hogy az ellene felhozott bizonyítékok a nyomozó hatóság által biztosan nem kerültek hamisításra, valamint könnyebben cáfolhatóbbá tenné azt az állítást, hogy az adott bizonyítékok hamisak.

A hitelesítő szoftverek, hash kódok alkalmazásán túl szükséges annak biztosítása, hogy az eredeti felvételek „bitazonosan” álljanak rendelkezésre, hiszen az elektronikus adatok átmásolása, konvertálása, elektronikus továbbítása során olyan adatokat veszíthetünk el, amelyek fontosak lehetnek a hitelesség megállapítása során, vagy a felvétel készítésével

kapcsolatos egyéb körülmények – például a felvétel készítésének pontos helye, ideje – tisztázásához.

A képi-kommunikáció elmélet szerint a felvételek bizonyítékként történő elfogadásához elengedhetetlen, hogy egy tanú megerősítése azok hitelességét. Azért tartottam fontosnak ezen elmélet bemutatását, hiszen még a hitelesítő szoftverek kötelező előírása esetén is lehetnek esetek, amikor a felvételek nem megfelelően kerültek rögzítésre, illetve még ha utóbb el is látjuk azokat hash kódokkal, az csak a hitelesítés pillanatától fogja tudni tanúsítani a bizonyíték változatlanosságát, azt megelőzően nem. Ekkor különösen fontos lehet, hogy egy tanú nyilatkozzon a felvétel készítésének körülményeiről és annak hitelességéről, vagy a felvétel által bemutatott tartalom valóságtartalmáról, hiszen a személyi bizonyítékok szerepéről sem szabad megfeledkeznünk.

A kép-, hang- és videófelvelekkel kapcsolatban kijelenthetjük, hogy számtalan szakirodalmi álláspont és különböző kutatások szerint nagyobb hatással hatnak az emberi emlékezetre, a valóság érzékelésére és a döntéshozatalra, mint más jellegű bizonyítékok. Nem szabad alábecsülnünk azt a tényt, hogy kutatások szerint az emberi agy nehezen hagy figyelmen kívül olyan információt a döntéshozatal során, amely már ismertté vált számára. Ez különös aggodalomra adhat okot a deepfake technológia által hamisított bizonyítékok esetén, hiszen ez azt jelenti, hogy a manipulált tartalom még akkor is kedvezőtlen hatást tud kifejteni a döntéshozatalra, ha már bebizonyosodott annak valótlansága, vagy ha nem sikerült a bizonyosság magas fokán sem megállapítani a hitelességét. Egyes szerzők szerint nem csak a laikusokat érinti a mesterséges intelligencia által generált tartalmak manipulatív hatása, hanem a bírókat is a döntéshozatal során.

A kutatásom során arra az álláspontra jutottam, hogy ezen torzító hatást egyrészt ellensúlyozzák a Be. bizonyítékok értékelésére vonatkozó szabályai és az indokolási kötelezettség, azonban indokolt lenne a döntéshozók edukációja az ilyen helyzetek kezelésére. Az indokolási kötelezettség arra ösztönzi a döntéshozót, hogy döntését racionalizálja, abból kizárja a torzító hatásokat, és kizárólag a bizonyítékoknak, tényeknek és jogszabályoknak megfelelő döntést hozzon. A kognitív tudományok törvényszerűségeiről elmondhatjuk, hogy minél több tudással rendelkezünk róla, annál inkább biztosítható a torzító hatások felismerése és kizárása a döntéshozatal során, ezért kiemelten fontosnak tartom az edukációt ezen a területen.

A kutatásom során az egyik legnagyobb nehézséget az okozta, hogy a deepfake technológiával hamisított bizonyítékokkal összefüggésben nem találtam olyan szakirodalmat,

amely részletesebben foglalkozott volna az igazságügyi szakértők alkalmazásának kérdésével. A törvényi szabályozást, a jogelméleti megközelítéseket, valamint a deepfake technológiára vonatkozó szakmai ismereteket – Kiss Attila László informatikus szakértő szakértelmével kiegészítve – egybevetve meghatároztam azon esetköröket, amikor szakértő igénybevétele nélkül is megbízhatóan állást lehet foglalni egy bizonyíték hitelességének kérdésében. Az egyik ilyen eset, amikor a deepfake technológia által létrehozott tartalom súlyosan és megkérdőjelezhetetlenül ellentmond az általános élettapasztalatnak, ugyanis nem minden deepfake technológia – és nem mindig – képes realiztikus tartalom létrehozására. Nem tartom indokoltnak azon esetekben sem a szakértő kirendelését, amikor megfelelő hitelesítő szoftverekkel, hash kódokkal kerültek rögzítésre a bizonyítékok oly módon, hogy azok bizonyosan tudják a hitelességet igazolni, valamint akkor, amikor a felvételen mesterséges intelligencia által létrehozott tartalomra vonatkozó vízjelzés, egyéb jelölés található, hiszen ekkor maga a jelölés tanúsítja azt, hogy a tartalmat egy algoritmus kreálta.

A tanulmány készítésekor megfogalmazódott bennem annak a kérdése, hogy a deepfake technológia elterjedése indokolttá teheti-e bizonyos büntető eljárásjogi jogintézményeink szabályainak átgondolását – például a hamis, hamisított bizonyítékokra vonatkozó perújítási rendelkezéseket –, azonban ennek az elemzését a bevezető részben megfogalmazott hipotéziseket és a tartalmi korlátokat szem előtt tartva nem e dolgozat keretei között tartottam indokoltnak kifejteni.

A kutatásom zárásaként arra a következtetésre jutottam, hogy szükség van arra, hogy a büntetőeljárásban nagyobb hangsúlyt fektessünk a bizonyítékok hitelességének biztosítására, hiszen enélkül a hitelesség kérdésében a szakértők sem fognak tudni állást foglalni a modern hamisítási módszerekkel szemben. Itt az idő, hogy a büntetőeljárás lépést tartson a mesterséges intelligencia árnyoldalával, hiszen a jövő igazságszolgáltatása csak akkor maradhat eredményes, ha képes különbséget tenni a valódi és a hamis bizonyítékok között.

Irodalomjegyzék

Szakirodalom:

- BÁNYAI István: *Az igazságügyi szakértő helye, szerepe a döntéshozatalban*, Magyar Jog, 2020/2., 121-122.
- BÁNYAI István: *Az igazságügyi szakértői tevékenység módszertani kérdései*, Magyar Jog, 2016/7-8., 437.
- BARTKÓ Róbert – ELEK Balázs – FANTOLY Zsanett – HERKE Csongor: *A büntető eljárásjog tankönyve*, ORAC kiadó (2024) 129-133.
- BEAZLEY, Doug: *The challenge of AI in the courtroom* <https://www.nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2024/ai-in-the-courtroom> (letöltve: 2024. 10. 11.)
- CSATLÓS Erzsébet: *A hatóság indokolási kötelezettségéről*, Közjogi Szemle 2024/1. 42.
- CSEMÁNE Váradi Erika–GÖRGÉNYI Ilona–GULA József–HORVÁTH Tibor–JACSÓ Judit–LÉVAY Miklós–SÁNTHA Ferenc: *Magyar büntetőjog - általános rész*. 2017, Budapest: Wolters Kluwer Kft. <https://doi.org/10.55413/9789632956282> Letöltve: https://mersz.hu/dokumentum/wk83_132/#wk83_129_p3 (2024. 10. 02.)
- *Deepfakes in Legal Proceedings – A Strategic Framework for Collaborative Solutions* <https://www.jdsupra.com/legalnews/deepfakes-in-legal-proceedings-a-9816082/> (letöltve: 2024. 10. 12.)
- DELFINO, Rebecca A.: *Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery*. Hastings Law Journal, 2023/2, 299. (<https://doi.org/10.2139/ssrn.4032094>) (letöltve: 2024. 09. 25.)
- ELEK Balázs - HÁGER Tamás: *A megalapozott tényállás és az indokolási kötelezettség összefüggései*, Büntetőjogi Szemle 2023/1. 12.
- ELEK Balázs: *A favor defensionis elv megjelenései az új büntetőeljárási törvény rendes perorvoslataiban*, Magyar Jog, 2021/10., 573.
- Europol Innovation Lab (2022), *Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab*, Publications Office of the European Union, Luxembourg. 8-9.
https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf (letöltés ideje: 2024. 09. 13.)

- GÁBRI Angéla: *Kognitív tudományok az ítélkezési tevékenység szolgálatában*, Pro Futuro, 2020/1, 110., 129.
- GÁRDONYI Gergely: *A bűnügyi szemle*, Ludovika Egyetem Kiadó, Budapest (2023), 90.
- GOSZTONYI Gergely, LENDVAI Gergely: *Deepfake és dezinformáció*, Médiakutató 2024. tavasz, XXV. évf. 1. szám, 42.
- HERÉDI István: *Az elektronikus adatokat érintő eljárási cselekmények végrehajtása*, in: Kibernetizációs kézikönyv (szerk: Nagy Zoltán András), Ludovika Egyetemi Kiadó, 2022, 155-160.
- HERKE Csongor: *A bizonyítékok újraértékelése: a deepfake technológia hatása a büntető igazságszolgáltatásra*, Magyar Jog, 2024/6., 324-331.
- HERKE Csongor: *Deepfake: áldás vagy átok? Jogi szabályozási szempontok*, Pro Futuro, 2023/1, 174. <https://doi.org/10.26521/profuturo/2023/1/13334> (letöltve: 2024. 09. 26.)
- KELETI Arthur: *Nem minden az, aminek látszódnia akar – a deepfake és a hitelesség jelene és jövője*, in: *Deepfake: A valótlan valóság* (szerk: Aczél Petra, Veszelszki Ágnes), Gondolat Kiadó, 2023, 62.
- KERTÉSZ Imre: *Kép- és hangtechnikai eszközök a büntető eljárásban*, Acta Universitatis Szegediensis: acta juridica et politica, 1992/41. 315. <https://acta.bibl.u-szeged.hu/6726/> (letöltve: 2024. 08. 01.)
- KETTERLING, Lester: *Photographs as Demonstrative Evidence in the Court Room*, North Dakota Law Review 1964, 193-195.
<https://commons.und.edu/cgi/viewcontent.cgi?article=2698&context=ndlr> (letöltve: 2024. 09. 15.)
- KLEIN Tamás–TÓTH András: *Technológiajog - Robotjog - Cyberjog*. 2019, Budapest, Wolters Kluwer
Kft. <https://doi.org/10.55413/9789632958293> Letöltve: https://mersz.hu/dokumentum/YOV1766_207/#YOV1766_205_p1 (2024. 10. 11.)
- KUHL Andrea: *Az ítéleti bizonyosság és a szakvélemények értéke*, Miskolci Jogi Szemle, 2023/1., 99.
- Kúria Joggyakorlat-Elemző Csoport összefoglaló véleménye: *A szakértői bizonyítás a bírósági eljárásban*, Budapest (2014) 254.
- Kúria Joggyakorlat-Elemző Csoport összefoglaló véleménye: *Az ítéleti bizonyosság elméleti és gyakorlati kérdései*, Budapest (2017) 28., 101.

- LINNA JR, Daniel W. – DALAL, Abhishek – GAO, Chongyang – GRIMM, Paul W. – GROSSMAN, Maura R. – PULICE, Chiara - TUNHEIM Hon. John: *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases* 8-31. [Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases \(researchgate.net\)](#) (letöltve: 2024. 10. 09.).
- MÁTÉ István Zsolt: *Az igazságügyi informatikai szakértő a büntetőeljárársban*, Doktori értekezés, Pécs, 2017. 61. <https://pea.lib.pte.hu/bitstream/handle/pea/16947/mate-istvan-zsolt-phd-2017.pdf> (letöltve: 2024. 08. 01.)
- MEZEI Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban*, Társadalomtudományi Kutatóközpont Jogtudományi Intézet – L'Harmattan, Budapest, 2020. 222.
- NÉMETH János: *Szakértői bizonyítás indítványozása és elbírálása a büntetőeljárársban, különös tekintettel a magánszakértői vélemény igénybevételére* Büntetőjogi Szemle 2022/1. 71-72.
- PALMIOTTO, Francesca: *Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective*, 2023, 7-8. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384122 (letöltve: 2024.10.20.)
- PFEFFERKORN, Riana: *'Deepfakes' in the Courtroom*. Boston University Public Interest Law Journal, 2020/2. 248. <https://www.bu.edu/pilj/archives/vol-29-2-summer-2020/> (letöltve: 2024.09.11.)
- SORBÁN Kinga: *A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről*, Belügyi Szemle 2020/10. 84.
- VENEMA E. Agnes – ZENO, Geradts J.: *Digital Forensics, Deepfakes, and the Legal Process*. https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/summer/digital-forensics-deepfakes-and-legal-process/ (letöltve: 2024. 09. 11.).
- VIDMAR, Neil: *The Psychology of Trial Judging*. Current Directions in Psychological Science, 2011/1, 4. (<https://doi.org/10.1177/0963721410397283>) (letöltve: 2024. 10. 10.)

Egyéb források:

- BERNACIAK, Catherine and ROSS A. Dominic: *How Easy Is It to Make and Detect a Deepfake?* <https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/> (letöltés ideje: 2024. 09. 21.)
- CHOI, Jeong-Eun – SCHÄFER, Karla – ZMUDZINSKI, Sascha: *Introduction to Audio Deepfake Generation, Academic Insights for Non-Experts*, 1. <https://dl.acm.org/doi/abs/10.1145/3643491.3660286> (letöltve: 2024. 09. 26.)

- Deepfakes Accountability Act H.R.5586. <https://www.congress.gov/bill/118th-congress/house-bill/5586/text> (megtekintve: 2024. 09. 26.)
- Face2Face: *Real-time Face Capture and Reenactment of RGB Videos* https://vcai.mpi-inf.mpg.de/projects/MZ/Papers/CVPR2016_FF/page.html (letöltés ideje: 2024. 09. 16.)
- <https://play.google.com/store/apps/details?id=com.camera.easy&pli=1> (megtekintve: 2024. 10. 23.)
- <https://www.eyewitness.global/> (megtekintve 2024.10.22.)
- <https://www.eyewitness.global/Using-metadata> (megtekintve 2024.10.31.)
- Magyar Igazságügyi Szakértői Kamara 3/2020 módszertani levele a beszélőazonosító vizsgálatokról (2020), <https://miszk.hu/index.php/tudastar/kamarai-modszertani-levelek> 11. (letöltve: 2024. 09. 18.)
- MÁTÉ István Zsolt – SÁNDOR Gábor: *A mobilkommunikációs eszközök vizsgálatának általános eljárásaira vonatkozó módszertani leírás*: Budapest: NSZKK, 2019. – 27 p.13 (5/2019. (XII.17.) NSZKK főigazgatói körlevél) 14. <https://miszk.hu/index.php/tudastar/kamarai-modszertani-levelek> (letöltve: 2024. 09. 18.)
- MI Blog: *Mély tanulás a mesterséges intelligencia világában* <https://mesterseges-intelligencia.eu/mely-tanulas-a-mesterseges-intelligencia-vilagaban/> (letöltés ideje: 2024. 09. 25.)
- MOLNÁR Csaba: *Először csaltak ki pénzt deepfake hanggal, és rögtön van magyar szál*, <https://index.hu/techtud/2019/09/05/eloszor-csaltak-ki-penz-deepfake-hanggal-es-rogt-on-van-magyar-szal/> (letöltés ideje: 2024. 09. 22.).
- Országos Igazságügyi Orvostani Intézet 22. számú módszertani levele polgári perekben és büntetőügyekben végzett DNS-vizsgálatokhoz és szakvéleményadáshoz, https://semmelweis.hu/igazsagugy/files/2012/06/22_mszlev.pdf 5. (letöltve: 2024. 10. 18.)
- RANA, Md Shohel - NUR NOBI, Mohammad - MURALI Beddhu - SUNG, Andrew H.: *Deepfake Detection: A Systematic Literature Review*. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9721302> (letöltés ideje 2024. 09. 17.)
- THE WASHINGTON POST: *A 'beautiful' female biker was actually a 50-year-old man using FaceApp. After he confessed, his followers liked him even more.* <https://www.washingtonpost.com/technology/2021/05/11/japan-biker-faceapp-soya-azusagakuyuki/> (letöltve: 2024. 09. 05.)