

Kriminológiai kihívások a 21. században: AI és a modern technológia a bűnözők kezében

Összefoglalás: A 21. században a bűnözés is előszeretettel használja a modern technológia vívmányait: az internetet, a mesterséges intelligenciát (MI) és az általuk életre hívott szintetikus médiát. Válaszul a nyomozó hatóságok maguk is segítségül hívják az MI-t arra, hogy felkutassák és azonosítsák a bűncselekmények elkövetőit. A modern technológia alkalmazása azonban ambivalens: míg egyfelől kitágulni látszik a világ a globális online térben, másfelől felmerül az állampolgárok nagy számának személyiségi jogai megsértésének lehetősége is. A jelen tanulmány ezt a jelenséget mutatja be egy konkrét jogeset elemzésén keresztül.

Kulcsszavak: Modern technológia; internet; MI; bűnözés; nyomozó hatóságok; személyiségi jogok.

Abstract: In the 21st century, crime also makes great use of modern technology: the Internet, artificial intelligence (AI) and the synthetic media they bring to life. In response, law enforcement agencies themselves call on AI to help them track down and identify perpetrators of crimes. However, the use of modern technology is ambivalent: while on the one hand the world seems to be expanding in the global online space, on the other hand the possibility of violating the personal rights of a large number of citizens also arises. The aim of this study is to present this phenomenon through the analysis of a specific legal case.

Keywords: Modern technology; Internet; AI; crime; law enforcement agencies; personal rights.

* Pécsi Tudományegyetem, ÁJK,
PhD-hallgató
Email: czukor.akos@edu.pte.hu
ORCID: 0009-0006-0374-5560

** Dunaiújvárosi Egyetem,
Társadalomtudományi Intézet
Email: dosanpgy@gmail.com
ORCID: 0009-0006-3357-7625

Bevezetés

A 21. században a bűnözés is előszeretettel használja a modern technológia vívmányait: az internetet, a mesterséges intelligenciát (MI) és az általuk életre hívott szintetikus médiát. Válaszul a bűnüldöző szervek maguk is segítségül hívják az MI-t arra, hogy felkutassák és azonosítsák a bűncselekmények elkövetőit. A modern technológia alkalmazása azonban ambivalens: míg egyfelől kitágulni látszik a világ a globális online térben, másfelől felmerül az állampolgárok nagy számának személyiségi jogai megsértésének lehetősége is. A fenntartható jogalkotás [1] elvének figyelembevételével a jogalkotónak olyan választ szükséges adnia erre a jelenségre, amely várhatóan úgy iktatja ki a jogsértések lehetőségét, hogy a technológiák alkalmazásának társadalomra előnyös szegmenseit nem csak érintetlenül hagyja, de a fejlődésüket is elősegíti [2; 3].

Ezek a technikai újdonságok azonban Janus-arcú jelenségnek bizonyulnak: számos pozitív alkalmazási lehetőségük mellett alkalmasak súlyos emberijog-sértések előidézésére is [4; 5; 6; 7], méghozzá tömegesen. Logikus érveléssel egyértelműnek tűnik, hogy – mint minden jelenség – ez is kétoldalú, ezért az alkalmazási cél dönti el, hogy adott esetben az alkalmazás használata társadalmilag elfogadható-e, avagy jogsértő: vagyis a jó cél szentesíti az eszközt [8; 9], amelyet a társadalom kulturális adottságai is befolyásolhatnak [10; 11]. A különböző MI-platformok elérhetősége és megfizethetősége lehetővé tette a bűnözők számára, hogy kihasználják ezt a technológiát.

[1] Falus, Orsolya (2024): Thoughts on legal sustainability – ‘nihil sub sole novum.’ *Russian law journal*, 12., (2.), pp. 51–59.

[2] Józwiak, Piotr–Falus, Orsolya (2022/a): Legal regulations on autonomous vehicles. In: Poland And Hungary: The issue of criminal liability In: Balázs László–Rajcsányi-Molnár Mónika–András István (Szerk.): *Elektromobilitás és társadalom*. Dunajváros: DUE Press, pp. 125–136.

[3] Józwiak, Piotr–Falus, Orsolya (2022/B). Criminal liability of associations. In: *Polish and Hungarian law*. Poznan: Wydawnictwo Rys.

[4] András I.–Rajcsányi-Molnár M. (2014): Profit és filantropia: a CSR eszmétörténeti kérdései. *Civil Szemle*, 11., (2.), pp. 5–24.

[5] Balázs L. (2014): Az iskolai klíma hatása a tanulók teljesítményére. In: *A kommunikáció(s) képzésképzés és fenntarthatóság: globalizáció a 21. században*. Dunajváros: DUE Press, pp. 38–54.

[6] Kőkuti Tamás (2022): Mesterséges intelligencia és foglalkoztatás. In: Kesz-Szeremlei Andrea–Rajcsányi-Molnár Mónika–András István (Szerk.): *Gazdasági növekedés és fenntarthatóság: globalizáció a 21. században*. Dunajváros: DUE Press, pp. 39–51.

[7] Rajcsányi-Molnár, M.–Balázs, L.–András, I.–Czifra, S. (2024): Competition as an effective motivational tool in online education. In: *Proceedings of the IEEE 11th International conference on computational cybernetics and cyber-medical systems (ICCC 2024)*, pp. 83–88)p. IEEE. <https://doi.org/10.1109/ICCC62278.2024.10582987>

[8] András I.–Rajcsányi-Molnár M.–Füredi G. (2013): A vállalatilag felelős vállalat: a CSR- és a cafeteria-metszet értelmezési lehetőségei a gyakorlatban. In: *Metamorfózis: globális dilemmák három tételben*. Budapest: Új Mandátum, pp. 127–139.

[9] Kőkuti Tamás–Balázs László–Rajcsányi-Molnár Mónika (2022): A felsőoktatási felelősségvállalás egy sajátos módja: képzési életpályamenedzsment program a Dunajvárosi Egyetemen. *Civil Szemle*, 19., (4.), pp. 113–126.

[10] Kőkuti, Tamás (2020): Cultural Differences Of Human Resources In Eu Enlargement: Az emberi erőforrás kulturális különbségei az EU bővítésében. In: András, István–Rajcsányi-Molnár, Mónika (Eds.): *East-West cohesion iv.: strategic study volumes*. Subotica: Čikoš Group, pp. 106–117.

[11] Varga Anita (2023): A szervezeti kultúra versus esélyegyenlőség. *Civil Szemle*, 20(Special Issue 7), pp. 61–75.

Felismerve a mesterséges intelligencia és az általa generált szintetikus média sokféleségét, az INTERPOL elkötelezte magát amellett, hogy feltárja ezt a dinamikus fejlődő környezetet, annak érdekében, hogy támogassa tagországait a szintetikus média által jelentett jelenlegi és jövőbeni fenyegetések kezelésében. Ehhez valamennyi érdekelt fél bevonására irányuló megközelítésre van szükség, amely magában foglalja a tagországok bűnüldöző szervein túlmenően az érdekelt iparágak képviselőit és az akadémiai intézményeket egyaránt [12]. Az internetes bűnözéssel szemben a rendőrség válaszul maga is olyan MI-eszközökhöz fordul, mint az arcfelismerés, az automatizált rendszámfelismerők, a lövésérzékelő rendszerek, a közösségi média elemzése, továbbá rendőrségi robotok bevonása a bűnüldözésbe.

Ezzel párhuzamosan az igazságszolgáltatás más ágazataiba is beszivárgott már az MI-használata – így az ügyvédek és a bírák mindennapi munkáját is segíti. Míg azonban a MI lehetővé teszi a büntető igazságszolgáltatás átalakítását a működési hatékonyság növelésével [13] és a közbiztonság javításával, kockázatokkal is jár a magánélet védelme és egyes további az emberi jogok vonatkozásában [14]. A jelen tanulmány célja az AI egy ilyen – kriminológiai alapon alapvetően hasznos célok érdekében történő felhasználása – *árnyoldalának* bemutatása, amely aztán jogilag önmagában is aggályosnak bizonyult.

A Clearview AI esete

A Clearview AI vállalatot Manhattanben, New Yorkban, alapították 2017-ben, még mielőtt a mesterséges intelligencia használata világviszonylatban is jelentőssé vált. 2020-ban a *The New York Times* vizsgálata [15] feltárta és nyilvánosságra hozta azt a tényt, hogy a Clearview AI Inc. több, mint hárommilliárd, az internetről, köztük a közösségi médiából a felhasználók beleegyezése nélkül letöltött képmás felhasználásával arcfelismerő adatbázist épített ki. A médiában futótűzként terjedt a hír, mely szerint cég az adatokat nem csak az olyan közismert közösségi média oldalakról szerzi, mint a Facebook, Instagram, Twitter, YouTube és LinkedIn, de egyéb nyilvánosan elérhető weboldalakról is, így híroldalokról, oktatási intézmények honlapjairól, sőt, bűnügyi adatbázisokból is meríti.

[12] Stock, Jürgen (2024): Beyond illusions unmasking the threat of synthetic media for law enforcement. *Interpol*. <https://www.interpol.int/en/how-we-work/innovation/interpol-innovation-centre> (Download: 2025. 09. 26.)

[13] Pacchioni, Federico Flutti, Emma–Caruso, Palmina, Fregna, Lorenzo–Attanasio, Francesco–Passani, Carolina–Colombo, Cristina–Travaini, Guido (2025): Generative AI and criminology: a threat or a promise? Exploring the potential and pitfalls in the identification of techniques of neutralization (Ton). *Plos one*, 20., (4.), E0319793. <https://doi.org/10.1371/Journal.Pone.031979>

[14] Martin, Kelly D.–Zimmermann, Johanna (2024): Artificial intelligence and its implications for data privacy. *Current opinion in psychology*, 58., <https://doi.org/10.1016/j.copsyc.2024.101829>.

[15] Hill, Kashmir (2020): *The secretive company that might end privacy as we know it*. The New York Times. <https://www.nytimes.com/2020/01/18/technology/clearviewprivacy-facial-recognition.html>. (Download: 2025. 09. 27.)

[16] BBC (2020): *Clearview AI: face-collecting company database hacked*. <https://www.bbc.com/news/technology-51658111> (Download: 2025. 09. 26.)

[17] Kuru, Taner (2024). Lawfulness of the mass processing of publicly accessible online data to train large language models. *International data privacy law*, 14., (3.), pp. 326–351. <https://doi.org/10.1093/Idpl/lpae013>

[18] ACLU.ORG (2022): *In big win, settlement ensures clearview ai complies with groundbreaking illinois biometric privacy law*. <https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois> (Download: 2025. 09. 26.)

[19] Sorbán Kinga (2015): Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. *Themis*, 2015/1. 343–375.
Startari, Augustin V. (2025). Predictive testimony: compiled syntax. In: *AI-generated police reports and judicial narratives*. *AI Power And Discourse*, 1., (1.), pp. 1–10.

A rendszer az arcképeken túlmenően az olyan metaadatokat is gyűjti és tárolja, mint az URL vagy a geolokációs információk, annak érdekében, hogy azok elősegítsék a keresett személyek azonosítását [16].

Noha kriminológiai aspektusból a Clearview AI számos előnnyel is rendelkezik, így például a bűnözők azonosításának lehetővé tételével, az adatbázis jogszerűtlen felépítése és az adatvédelmi megfontolások figyelmen kívül hagyása mégis olyan problémákat vet fel, amelyek önmagukban véne is sérteneek egyes emberi jogokat, ennek folytán akár büntetőjogi értelemben tényállás-szerűnek minősülhetnek. Erre figyelemmel – bár a jó cél érdekében megalkotott programot a rendőri szervek világszerte sikerrel alkalmazzák – több országban mégis nyilvános ellenállásba ütköztek. Ezen államok adatvédelmi hatóságai ugyanis megállapították, hogy a vállalat megsértette az adatvédelmi törvényeket [17].

Az első ilyen eljárás az Amerikai Egyesült Államokban indult, 2020. május 28-án. Az Amerikai Polgári Szabadságjogok Uniója (American Civil Liberties Union = ACLU) és annak Illinois állami képviselője, valamint az Edelson PC ügyvédi iroda által képviselt Chicagói Szövetség a Szexuális Kizsákmányolás Ellen (Chicago Alliance Against Sexual Exploitation = CAASE), a Chicagói Szexmunkások Ismeretterjesztő Projektje (Sex Workers Outreach Project Chicago = SWOPChicago), az Illinois Állami Közérdekű Kutatócsoport (Illinois State Public Interest Research Group, Inc. = Illinois PIRG) és a „Latin Lányok Akcióban” Egyesület („Mujeres Latinas en Acción” = „Mujeres”), mint felperesi pertársaság, keresetet nyújtottak be a Clearview AI, Inc. ellen, az illinois lakosok adatvédelmi jogainak megsértésére hivatkozva az illinois biometrikus információk adatvédelmi törvénye (BIPA) értelmében [18].

Az illinois Cook megyei körzeti bíróságon indított perben a kereset arra irányult, hogy a bíróság tiltsa el az alperest attól, hogy a felperesek adatbázisait és platformjait a magáncégek, magánszemélyek, közintézmények és a bűnüldöző szervek számára hozzáférhetővé tegye. A keresetet benyújtó társadalmi szervezetek tagjai olyan magánszemélyek voltak, akiknek a képmását a Clearview AI Inc. a beleegyezésük nélkül szerezte meg és kezelte, és akiket ezzel olyan súlyos kockázatoknak tett ki, mint például a személyazonosságlopás [19] – köznapi szóhasználatlaltal „személyiséglopás” –, valamint a családon belüli erőszak és a szexuális zaklatás. Ez a per volt az első, amely kifejezetten a Clearview AI példa nélküli hírszerzési programjának a kiszolgáltatót közös-

ségekre és kisebbségekre gyakorolt káros és veszélyeztető hatásaira összpontosított. Az ACLU azt állította, hogy a Clearview AI algoritmusai egyértelműen sértette a helyben hatályos adatvédelmi törvényt, a BIPA-t, és azt kérte a bíróságtól, hogy kötelezze a vállalatot arra, hogy a törvényes működés helyreállításán túlmenően töröljék is az alanyok beleegyezése nélkül létrehozott képmásokat és adatokat. A Clearview AI indítványt nyújtott be a kereset elutasítására [20]. Hosszas pereskedés után, amelynek során még a Legfelsőbb Bíróság közbenső eljárása is szükségessé vált, az Alkotmánynak a magánélet védelmével kapcsolatos rendelkezései értelmezésének igénye folytán, a felek végül egyezséget kötöttek egymással 2022. május 9-én, amelynek értelmében az alperesi cég törölte a jogsértő módon begyűjtött és tárolt képmásokat és egyéb személyes adatokat [18].

A szoftver előnyei és hátrányai

Az alperes által elfogadott egyezség azt bizonyítja, hogy a szigorú adatvédelmi törvények valódi védelmet nyújthatnak a hasonló visszaélésekkel szemben. A Clearview többé nem kezelheti az emberek egyedi biometrikus azonosítóit korlátlan profitforrásként, akkor sem, ha alapvetően alappal hivatkozik arra a tényre, hogy a programja segítségével a bűnüldöző szervek munkáját is elősegíti. Mindössze néhány héttel a megállapodás aláírása és az egyezséget jóváhagyó bírósági végzés kihirdetése előtt a Clearview AI bejelentette ambiciózus tervét, mely szerint valamennyi, a Földön élő, személy képmását betáplálná az adatbázisába, és a mesterséges intelligenciát képessé tenné minden egyes személy felismerésére. A cégnek a saját bevallása szerint már 3 milliárdnál is több arckép szerepel az adatbázisában, továbbá jogosultja egy új amerikai szabadalomnak, amely egy rendkívül pontos, elfogulatlan arcfelismerő algoritmusra vonatkozik. Ezt az algoritmust jelenleg az orosz-ukrán háborúban használják, segítve az ukrán tisztviselőket a téves információk, álhírek, elleni küzdelemben és a halottak azonosításában. A szabadalmi joga alapján a Clearview AI-t abban sem akadályozza meg senki, hogy ugyanezeket az eszközöket Oroszország számára is biztosítsa [20].

[18] ACLU.ORG (2022): *In big win, settlement ensures clearview ai complies with groundbreaking illinois biometric privacy law*. <https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois> (Download: 2025. 09. 26.)

[20] Ahmed, Isra (2023): ACLU V. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292. *Depaul journal of art, technology & Intellectual property law*, 33., (1.), pp. 66–81.

[17] Kuru, Taner (2024). Lawfulness of the mass processing of publicly accessible online data to train large language models. *International data privacy law*, 14., (3.), pp. 326–351. <https://doi.org/10.1093/Idpl/Ipae013>

[22] European Data Protection Board/EDPB (2024): *Dutch supervisory authority imposes a fine on clearview because of illegal data collection for facial recognition*. https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en (Download: 2025. 09. 26.)

[23] (EU) 2024/1689 Rendelet

[24] European Data Protection Supervisor /EDPS (2020): *EDPS opinion on the possibility to use clearview ai and similar services at europol*. (Case 2020-0372). https://www.edps.europa.eu/system/files/2022-01/21-03-29_edps_opinion_2020-0372.pdf (Download: 2025. 09. 26.)

[25] Clearview AI (é.n.): *Success Stories*. <https://www.clearview.ai/success-stories> (Download: 2025. 09. 26.)

[26] Clearview AI (é.n.): Clearview AI launches justiceclearview, first facial recognition product for public defenders seeking justice. <https://www.clearview.ai/press-room/clearview-ai-launches-justiceclearview-first-facial-recognition-product-for-public-defenders-seeking-justice> (Download: 2025. 09. 27.)

A cég tevékenységével kapcsolatban más országok is jeleztek hasonló jogsértéseket, így például az Egyesült Királyság, Ausztrália és Kanada, már tettek lépéseket az adatvédelmi törvényeikre hivatkozva annak érdekében, hogy megakadályozzák a Clearview AI-t abban, hogy jogsértő módon kezelje az állampolgáraik adatait [17]. 2024. május 16-án a Holland Adatvédelmi Hatóság (DDPA) 30,5 millió eurós bírságot szabott ki a Clearview AI-ra, amiért az illegális adatbázist hozott létre. A DDPA megállapította a határozatában, hogy a cég jogellenesen gyűjtött arcképmásokat, beleértve holland állampolgárokat is, anélkül, hogy megszerezte volna beleegyezésüket [22]. Bár Clearview AI minden, ellene indult, eljárásban, hangsúlyozta, hogy terméke elősegíti a bűnüldöző szervek hatékony munkáját, az európai adatvédelmi biztos az Európai Unió mesterséges intelligenciáról szóló rendelete (Regulation (EU) 2024/1689 [23] laying down harmonised rules on artificial intelligence) 43. cikke (3) bekezdésének d) pontja értelmében mégis azt javasolta az EUROPOLNAK, hogy inkább ne vegye igénybe a Clearview AI szolgáltatásait, mivel ez valószínűleg sértené az EUROPOL szabályzatát [24]. A Clearview AI mindezek ellenére továbbra is működik, és olyan sikertörténetekre hivatkozik, mint például egy korábban ártatlanul elítélt személy felmentése egy bűncselekmény helyszínén látható tanú azonosításával; gyermekprostitúció elkövetőjének identifikálásával, vagy egy nemzetközi kábítószer-csempész hálózat tagjainak leleplezése az arcfelismerő programjának köszönhetően [25]. Hoan Ton-That, a cég társalapítója és ügyvezetője a társaság honlapján így nyilatkozik: „A Clearview AI küldetése az igazságszolgáltatásban és a közbiztonság támogatásában túlmutat a bűncselekmények elkövetőinek azonosításán, magában foglalja a jogtalanul vádoltak felmentését is. Ez ugyanazon érme két oldala, amelyek a bűncselekmények áldozatai és a nagyközönség számára egyaránt fontosnak tekinthetők a megfelelő igazságszolgáltatás szempontjából” [26]. A Clearview AI tevékenységével összefüggésben állandó aggodalmak merülnek fel azzal kapcsolatban is, hogy az arcfelismerő program hajlamos a téves eredményekre, különösen bőrszín alapján és más, faji alapon meghatározott emberek azonosítása során, amely súlyosbítja a rendszerszintű rasszizmust, az elfogultságot és a diszkriminációt [27].

Következtetések és javaslatok

A büntető igazságszolgáltatással kapcsolatos magas kockázatú helyzetekben a legális és etikus mesterséges intelligencia iránti igény kiemelkedő fontosságú [28]. Kétségtelenül szükség van olyan új törvényekre, szabályozásokra és politikákra, amelyek kifejezetten az MI árnyoldalai okozta kihívások kezelésére szolgálnak. Az Európai Unió mesterséges intelligencia törvénye tiltja a mesterséges intelligencia olyan felhasználási módjait, mint a céltalan képek kimásolása az internetről vagy a CCTV-ből, valós idejű távoli biometrikus azonosítás nyilvános helyen (korlátozott kivételektől eltekintve), valamint a visszaesés kockázatának kizárólag profilalkotás vagy személyiségjegyek alapján történő felmérése [23].

A Clearview AI esete egyértelműen arra figyelmezteti a jogalkotókat és -alkalmazókat, hogy – mint oly sok jelenségnek az életben – az MI használatának is két oldala van. Míg a bűnüldözés és az igazságszolgáltatás számára a használata hasznos lehet, a személyes adatok védelme és az átláthatóság biztosítása olyan alapvető emberi jogok, amelyek biztosításától még a jó cél érdekében történő felhasználás esetén sem tekinthetünk el.

Mindenki, aki valaha képet osztott meg magáról vagy másokról az interneten, valószínűleg bekerült a Clearview AI-adatbázisába – és sajnos nincs egyértelmű védekezés ezen AI-rendszerek ellen, kizárólag az önkorlátozás, ha minél kevesebb adatot osztunk meg az online térben. A mesterséges intelligencia technológiájának gyors fejlődésével a szintetikus média egyre befolyásosabb tartalomformává válik. Könnyű elérhetősége lehetővé tette a bűnözők számára, hogy azt büntető törvénykönyvi tényállásba ütköző tevékenységekre használják fel. A szintetikus médiafájlok képesek megtéveszteni az emberi érzékelést, amely megnehezíti hitelességük meghatározását. A büntetőügyekben eljáró hatóságok számára kiemelten javasolható erre figyelemmel, hogy maguk is átfogó ismeretekkel rendelkezzenek a szintetikus média sokrétű természetéről, beleértve annak létrehozását, terjesztését és lehetséges hatásait, úgy, hogy mindezek mellett soha ne tévesszék szem elől a polgárok alapvető emberi jogait, hiszen, mint látható, még a jó cél sem szentesítheti az eszközt minden esetben.

[23] (EU) 2024/1689 Rendelet

[27] Ferreira, Marcos Vinicius –Almeida, Ariel–Canario, Joao Paulo Souza–Matheus, Nogueira–Tatiane, Rios, Ricardo (2021): Ethics of AI: do the face detection models act with prejudice?. In: Britto, A.–Valdivia Delgado, K. (Eds.): *Intelligent Systems*. BRACIS 2021. Lecture Notes In: *Computer Science*, 13074., Springer, Cham. https://doi.org/10.1007/978-3-030-91699-2_

[28] András, I.–Rajcsányi-Molnár, M. (2015): The Evolution of CSR and its reception in post-socialist environments: The Case Of Hungary. *Journal of environmental sustainability*, 4., (4.).

