https://doi.org/10.63684/dk.2025.12.05

CZUKOR ÁKOS GELLÉRT*

New Criminological Challenges in the 21st Century

* *Pécsi Tudományegyetem, ÁJK, Phd-hallgató*
Email: czukor.akos@edu.pte.hu

Összefoglalás: Bár az emberiség történetében hosszú idő telt el az első orvosi és terápiás innovációktól az önvezető autók megjelenéséig, kevesen számítottak arra, hogy a 21. századra a generatív mesterséges intelligencia platformok és a *deepfake-as-a-service*-ajánlatok, valamint a hangszimuláció és a szintetikus média összes veszélyes „terméke” online elérhető lesz szinte bárki számára világszerte. A jelen tanulmány célja, hogy egy amerikai bírósági ügy alapján mutassa be ezt a jelenséget, választ keresve arra a kérdésre, hogy vajon szükséges-e tolerálni a személyiségi jogok megsértését a modern kriminológiai eszközök használatának „melléktermékeként”.

Kulcsszavak: Innováció; mesterséges intelligencia platformok; kriminológia; személyiségi jogok; bírósági ügy.

Abstract: Although a long time has passed in human history from the first medical and therapeutic innovations to the time when humanity’s cars became self-driving, few expected that by the 21st century, generative AI platforms and *deepfake-as-a-service* offerings, as well as all the dangerous “products” of voice simulation and synthetic media, would be available online to almost anyone worldwid The aim of this paper is to present this phenomenon through an American court case, seeking an answer to the question of whether is it necessary to tolerate personal rights’ violations as a "by-product" of the use of modern criminological tools.

Keywords: Innovation; AI platforms; criminology; personal rights; court case.

Introduction: The Dark Side of Innovation

In the ever-evolving environment of technology, especially with the rise of artificial intelligence (AI), law enforcement authorities are facing new challenges and opportunities. Although a long time has passed in human history from the first medical and therapeutic innovations [1, 2] to the time when humanity's cars became self-driving [3], few expected that by the 21st century, generative AI platforms and deepfake-as-a-service offerings, as well as all the dangerous "products" of voice simulation and synthetic media, would be available online to almost anyone worldwide. However, these technical innovations are proving to be a Janus-faced phenomenon: in addition to their numerous positive applications, they are also capable of causing serious human rights violations, and on a massive scale.

It seems logical that, like all phenomena, this is a two-sided phenomenon, and that the purpose of the application determines whether the use of the application is socially acceptable or illegal: the good purpose justifies the tool. The availability and affordability of various AI platforms have enabled criminals to exploit this technology. Recognizing the diversity of artificial intelligence and the synthetic media it generates, INTERPOL is committed to exploring this dynamically evolving environment in order to support its member states in addressing the current and future threats posed by synthetic media. This requires an approach that involves all stakeholders, including not only law enforcement agencies in member states, but also representatives of interested industries and academic institutions [4]. In response to cybercrime, police themselves are turning to AI tools such as facial recognition, automated license plate recognition, gunshot detection systems, social media analytics, and the use of police robots in crime prevention [5]. In parallel, AI has also infiltrated other sectors of the justice system, helping lawyers and judges in their daily work.

However, while AI has the potential to transform criminal justice by increasing operational efficiency [6] and improving public safety, it also poses risks to privacy and other human rights [7]. The aim of this study is to present one such downside of AI – the use of AI for purposes that are fundamentally criminologically useful, but which have proven to be legally problematic in their own right.

[1] Falus O. (2011): Lepra: Stigma a 21. században. *Orvosi Hetilap,* 152., (7.), pp. 246–251.

[2] Falus O. (2015): *Ispotályos keresztes lovagrendek az Árpád-kori Magyarországon.* Pécs: Publikon Kiadó.

[3] Jóźwiak, P.–Falus, O. (2022): 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.* Dunaújváros: DUE Press, pp. 125–136.

[4] Stock, J. (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 (2025. 09. 26.)

[5] Startari, A. V. (2025): Predictive Testimony: Compiled Syntax in AI-Generated Police Reports and Judicial Narratives. AI Power and Discourse. 1(1). Pp. 1-10.

[6] Pacchioni, F.–Flutti, E.–Caruso, P. –Fregna, L.–Attanasio, F. –Passani, C. –Colombo, C.–Travaini, G. (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.0319793

[7] Martin, K. D.–Zimmermann, J. (2024): Artificial intelligence and its implications for data privacy. *Current Opinion in Psychology,* 2024., (58.). https://doi.org/10.1016/j.copsyc.2024.101829.

The American Legal Case

Clearview AI was founded in Manhattan, New York, in 2017, before the use of artificial intelligence became significant worldwide. In 2020, an investigation by *The New York Times* (Hill, 2020) revealed and made public the fact that Clearview AI Inc. had built a facial recognition database using more than three billion images downloaded from the internet, including social media, without the consent of the users. The news spread like wildfire in the media that the company was collecting data not only from well-known social media sites such as Facebook, Instagram, Twitter, YouTube and LinkedIn, but also from other publicly available websites, such as news sites, educational institution websites and even criminal databases. In addition to facial images, the system also collects and stores metadata such as URLs or geolocation information to help identify wanted individuals [9].

Although Clearview AI has many advantages from a criminological perspective, such as enabling the identification of criminals, the illegal construction of the database and the disregard for data protection considerations still raise problems that in themselves violate certain human rights, and therefore may even be considered as a fact in criminal law. In view of this, although the program created for a good purpose is successfully used by police agencies around the world, it has nevertheless encountered public opposition in several countries. The data protection authorities of these states have determined that the company has violated data protection laws [10].

The first such procedure was launched in the United States of America on May 28, 2020. The *American Civil Liberties Union* (ACLU) and its Illinois State Office, as well as the Chicago Alliance Against Sexual Exploitation (CAASE), Sex Workers Outreach Project Chicago (SWOPChicago), Illinois State Public Interest Research Group, Inc. (Illinois PIRG), and Mujeres Latinas en Acción (Mujeres), represented by the law firm Edelson PC, have filed a class action lawsuit against Clearview AI, Inc., alleging violations of the privacy rights of Illinois residents under the Illinois Biometric Information Privacy Act (BIPA) (ACLU v. Clearview AI, Inc., 2021 Ill. Cir. LEXIS 292).

The lawsuit, filed in the Cook County District Court in Illinois, sought an injunction to prevent the defendant from making the plaintiffs' databases

[8] Hill, K. (2020): *The Secretive Company That Might End Privacy as We Know It.* New York: The New York Times. ISSN 0362-4331. January 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearviewprivacy-facial-recognition.html. (2025. 09. 27.)

[9] BBC (2020): *Clearview AI: Face-collecting company database hacked.* https://www.bbc.com/news/technology-51658111 (2025. 09. 26.)

[10] Kuru, T. (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

and platforms accessible to private companies, individuals, public institutions, and law enforcement agencies. The civil society organizations that filed the lawsuit were individuals whose images were obtained and processed by Clearview AI Inc. without their consent, exposing them to serious risks such as identity theft [11] – colloquially known as "personal theft" – as well as domestic violence and sexual harassment. This lawsuit was the first to specifically focus on the harmful and threatening effects of Clearview AI's unprecedented intelligence program on vulnerable communities and minorities. The ACLU argued that Clearview AI's algorithm clearly violated the local privacy law, BIPA, and asked the court to order the company to delete the images and data created without the consent of the subjects, in addition to restoring lawful operations. Clearview AI filed a motion to dismiss the lawsuit [12]. After lengthy litigation, which even required the Supreme Court to intervene to interpret the Constitution's privacy provisions, the parties finally reached a settlement on May 9, 2022, under which the defendant company deleted the images and other personal data it had unlawfully collected and stored [13].

The Two Sides of the Coin

The settlement the defendants have reached shows that strong privacy laws can provide real protection against such abuses. Clearview can no longer treat people's unique biometric identifiers as an unlimited source of profit, even if it makes a fundamental case that its software also helps law enforcement agencies.

However, other countries, in addition to the United States, have reported similar violations of the company's activities, such as the United Kingdom, Australia and Canada, which have already taken steps under their data protection laws to prevent Clearview AI from unlawfully processing the data of their citizens [10]. On 16 May 2024, the Dutch Data Protection Authority (DDPA) fined Clearview AI €30.5 million for creating an illegal database. The DDPA found in its decision that the company had unlawfully collected facial images, including those of Dutch citizens, without obtaining their consent [14].

[10] Kuru, T. (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

[11] Sorbán K. (2015): Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. *Themis,* 2015., (1.), pp. 343–375.

[12] Ahmed, I. (2023): ACLU v. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292. *DePaul Journal of Art, Technology & Intellectual Property Law,* 33., (1.), pp. 66–81.

[13] 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 (2025. 09. 26.)

[14] 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 (2025. 09. 26.)

Although Clearview AI emphasized in all proceedings brought against it that its product facilitates the effective work of law enforcement agencies, the European Data Protection Supervisor nevertheless recommended that EUROPOL, pursuant to Article 43(3)(d) of Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, not use Clearview AI's services as this would likely infringe EUROPOL's rules [15].

Despite all this, Clearview AI continues to operate and cites success stories such as the exoneration of a previously innocent person by identifying a witness at a crime scene; the identification of a child prostitution perpetrator; and the exposure of members of an international drug trafficking network thanks to its facial recognition program [16].

However, there are ongoing concerns about Clearview AI's activities that the facial recognition program is prone to erroneous results, especially when identifying people based on skin color and other racially defined characteristics, which exacerbates systemic racism, bias, and discrimination [17].

Conclusions

The need for legal and ethical AI in high-risk criminal justice situations is paramount. There is no doubt that new laws, regulations and policies are needed that specifically address the challenges posed by the downsides of AI. The European Union's AI law prohibits uses of AI such as the purposeless scraping of images from the internet or CCTV, real-time remote biometric identification in public places (subject to limited exceptions), and the assessment of the risk of recidivism based solely on profiling or personality traits (Regulation (EU) 2024/1689).

The Clearview AI case is a clear reminder to policymakers and practitioners that, like so many things in life, there are two sides to the use of AI. While its use can be beneficial for law enforcement and the administration of justice, the protection of personal data and transparency are fundamental human rights that cannot be ignored, even when used for good purposes. Everyone who has ever shared an image of themselves or others online has probably been included in Clearview AI's database – and unfortunately, there

[15] 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 (2025. 09. 26.)

[16] CLEARVIEW AI (é.n.): *Success Stories.* https://www.clearview.ai/success-stories (2025. 09. 26.)

[17] Ferreira, M. V.–Almeida, A. –Canario, J. P.–Souza, M. N. T. –Rios, R. (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,* vol 13074. Springer, Cham. https://doi.org/10.1007/978-3-030-91699-2_7

is no clear defense against these AI systems, except for self-restraint by sharing as little data as possible online. With the rapid development of artificial intelligence technology, synthetic media is becoming an increasingly influential form of content. Its easy availability has allowed criminals to use it for activities that violate criminal law. Synthetic media files are capable of deceiving human perception, which makes it difficult to determine their authenticity. In this regard, it is highly recommended for authorities dealing with criminal cases to have a comprehensive knowledge of the multifaceted nature of synthetic media, including its creation, distribution and potential effects, while never losing sight of the fundamental human rights of citizens, since, as can be seen, even a good purpose cannot justify the means in all cases.