UNIVERZITA MATEJA BELA
V BANSKEJ BYSTRICI

ZBORNÍK PRÍSPEVKOV
Z MEDZINÁRODNEJ ŠTUDENTSKEJ
VEDECKEJ KONFERENCIE

PRO-LEGAL Deň študentov práva a doktorandov 2026

2026

BELIANUM

Univerzita Mateja Bela v Banskej Bystrici
Právnická fakulta

Zborník príspevkov z medzinárodnej študentskej vedeckej konferencie PRO-LEGAL Deň študentov práva a doktorandov 2026

Recenzovaný zborník vedeckých príspevkov

Ľubica Saktorová
(eds.)

BELIANUM
Banská Bystrica
2026

Zostavovateľ (Editor) : JUDr. Ľubica Saktorová, PhD., LL.M., M.A.

Recenzenti (Reviewers) : doc. JUDr. Ivana Šošková, PhD., MBA
Mgr. Miroslava Dolíhalová, PhD.
JUDr. Peter Trajlinek, PhD.

Príspevky neprešli jazykovou korektúrou.
Za obsahovú a jazykovú stránku textu sú zodpovední autori publikovaných príspevkov.

ISBN 978-80-557-2337-2
EAN 9788055723372
https://doi.org/10.24040/2026.9788055723372

INTERNATIONAL LEGAL APPROACHES TO THE PROTECTION OF PERSONAL NON-PROPERTY RIGHTS IN THE CONTEXT OF AI TECHNOLOGIES

MAKSYMILIANA-ELLANTA ROMANIUK*

Abstract

We are currently experiencing a phase of rapid development of AI technologies, which can potentially be used with harmful intent. The article highlights the risks posed by the unauthorized use of a person's likeness and voice to create manipulative content, which can lead to violations of the rights to dignity, honour, privacy and the security of biometric data. The article also reviews attempts by various countries to regulate relations between users of such technologies and those affected by their use. Based on the analysis, the article proposes ways to improve Ukrainian civil legislation to ensure an effective legal order in the digital age.

Keywords: *personal non-property rights, likeness, artificial intelligence, deep synthesis technologies, deepfake.*

Introduction

The modern world lives not only in real life, but also in virtual. The number of hours spent on the Internet for some may significantly exceed the time devoted to live communication. In addition to consuming Internet content, many people are also engaged in its creation and filling the network with it.

Nowadays, artificial intelligence (AI) is gaining popularity. Because it is a great instrument, which was created to optimize certain processes. It can be useful in any field.

AI is already available to a wide variety of population groups. Consequently, it is becoming a tool not only for noble purposes, such as science or education, but also for entertainment and the commission of offenses. Some students use AI to "cheat" on exams. People also frequently turn to AI when writing texts, which sometimes leads to copyright infringement. However, it is also important to highlight that quite often users of AI violate the personal non-property rights of individuals.

Chapter 1

The Civil Code of Ukraine defines personal non-property rights belong to every natural person from birth or by law, have no economic content, are closely linked to the individual, and are inherent, inalienable, and are held by the natural person for life. The list of personal non-property rights is endless. The essence of a personal non-property right constitutes the ability

* 2nd year of study, Full-time, romaniuk.maksymiliana-ellanta@chnu.edu.ua Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Ukraine
Academic Supervisor Assoc. prof. Oksana Kiriiak, PhD. Associate Professor at the Department of Private Law

of an individual to freely, at their own discretion, determine their behavior in the sphere of their private life [1].

The Internet is saturated with photo and video materials created by AI using the appearance and voices of real people (deepfakes). Such content is usually created for entertainment. However, in this way users of AI spread false information that violates individuals' rights to respect for dignity and honor.

An interesting example is the exploitation of the likeness of Anila Bisha (an Albanian actress) by the government of Albania to create an "AI Minister" – a virtual member of the cabinet. Anila Bisha had not given consent for such use of her likeness. The actress filed a lawsuit against the government because such actions of the government led to unwanted attention on the street and online harassment [2].

Now it is becoming increasingly difficult to distinguish AI from recordings of real people. This can be used to intentionally mislead content consumers, for example, for political campaigning. There is also the possibility of using AI to bypass security systems by forging person's biometric data, which can lead not only to the violation of personal non-property rights but also to the commission of more serious crimes.

Establishing norms at the legislative level to regulate such relationships is necessary to ensure the rule of law in every state.

Chapter 2

An important regulatory act governing relations in the field of AI is Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024 (the AI Act). This document classifies AI systems and defines various requirements for them depending on the level of risk. [3].

The Preamble (paragraph 10) and general provisions of the Act emphasize that this Regulation applies without prejudice to existing EU data protection legislation, in particular the GDPR (General Data Protection Regulation). A person's likeness and physiological characteristics are their personal (and often biometric) data. Creating a deepfake of a specific real individual involves the processing of this data. Under GDPR rules, such processing is unlawful by default without the explicit, informed, and revocable consent of the data subject.

Chapter IV, Article 50 of the AI Act defines transparency obligations for providers and users of certain AI systems. Paragraph 2 of this article obligates providers of systems that generate synthetic audio, image, video or text to ensure the machine-readable marking of outputs. Such marking must allow to detect artificially created or manipulated content.

Exceptions include systems for standard editing, algorithms that do not significantly alter the substance of input data, and law enforcement tools authorized by law.

Paragraph 4 concerns the use of AI to create deepfakes or manipulate images, audio, or video. Users of such systems must disclose that the content is of artificial origin. The Act makes an exception for obvious artistic, satirical (e.g., parodies) or fictional works, but even in such cases, transparency must be ensured in a manner that does not impede the display of the work while not misleading the audience [4].

The French approach is distinguished by harsh penalties. While European laws focus more on moderation and transparency, France directly criminalizes the creation and distribution of deepfakes without individual's permission.

In May 2024, a law was adopted amending Article 226-8 of the French Penal Code. The creation and distribution of deepfakes without the person's consent became a criminal offense. The rule applied if the artificiality of the material was not obvious or was not openly declared. Platforms must promptly remove illegal materials upon receiving notification of them [5]. Violation of these rules entails serious sanctions. The illegal creation or distribution of deepfakes is punishable by up to one year in prison and a fine of up to 15,000 euros. If the offense is committed via public online services, the penalty increases to two years in prison and a 45,000 euro fine. Enforcement of the law is monitored by the French judicial system with the support of regulatory bodies [6].

In June 2025, the Danish Ministry of Culture and several political parties agreed to amend the copyright law ("Agreement on Protection Against Digital Imitations Containing Personal Characteristics" (Aftale om et værn mod digitale efterligninger indeholdende personlige kendetegn)). They proposed two new levels of protection against the distribution of digital imitations without a person's consent.

The first mechanism will protect the general public from the unauthorized use of realistic forgeries of personal characteristics, such as appearance or voice. The second mechanism is designed specifically to protect performers from the distribution of generated imitations of their performances [7].

The main goal of these innovations is to create a clear legal framework that will allow anyone to demand that social networks and other platforms remove forged materials.

Ordinary users who distribute such materials will not be subject to criminal or administrative penalties, although victims will be able to seek damages through the courts. Instead, heavy fines may threaten the platforms themselves if they ignore complaints and requests to remove such content. These rules will apply exclusively within the territory of

Denmark; thus, content removed there may remain accessible from other countries. This law will enter into force on March 31, 2026 [8].

The Austrian Deepfake Action Plan (Aktionsplan Deepfake) is a government document developed by the Ministry of the Interior (BMI) in 2022 [9]. Protection of likeness is based on the right to one's own image according to Section 78 of the Copyright Act. This norm protects an individual against the publication of manipulations that affect a person's legitimate interests, degrade their dignity, or grossly interfere with their private life. Particular attention is paid to countering sexualized violence. Using a face to create fake pornography is defined as a direct violation of the rights to sexual self-determination, privacy and human dignity. The Deepfake Action Plan also extends the scope of protection to voice and speech, recognizing that audio deepfakes can violate the right to one's own speech and the privacy of communication.

Criminal and civil liability for such actions is provided by articles on cyberbullying – namely, persistent harassment via computer systems. Norms on defamation, insult to honor and damage to business reputation are also applied.

The Deepfake Action Plan provides for a simplified judicial protection procedure, known as mandate proceedings under Section 549 of the Code of Civil Procedure. This allows for a faster response to cases where a deepfake significantly degrades human dignity.

A separate priority is the development of technical tools for detecting manipulations, specifically through the Defalsif-AI project, so victims can obtain evidence for court. In addition, large online platforms are assigned obligations under the Digital Services Act regarding risk assessment and the removal of intentional manipulations that harm people.

Politicians and media figures have somewhat limited protection, as their lives are often the subject of public discussion, and satirical depictions may be protected by the freedom of art. However, this protection is not absolute: it ceases to apply if the deepfake has no factual basis, contains excessive insult, or interferes with a deeply personal, intimate sphere of an individual's life.

The British Data (Use and Access) Act 2025 (DUAA) significantly supplements the Online Safety Act 2023, filling a critical gap in the protection of personal rights. The most important innovation is Section 138 of the Data (Use and Access) Act 2025. It amends criminal legislation (specifically the Sexual Offences Act).

Now, the creation of an intimate deepfake of an adult without their consent is a standalone crime, even if the deepfake was never distributed and was kept only on the author's device. The article also prohibits ordering or asking another person (or an AI service) to create such content. The law uses the term "purported intimate image." This means it does not matter

if the image is a real photo. If AI generated content that "appears to be" an image of a particular person in an intimate context, it is a violation.

DUAA 2025 introduces changes to the UK General Data Protection Regulation (UK GDPR) that strengthen an individual's control over their digital identity. According to Articles 17 and 21 of the UK GDPR, as amended by the DUAA, an individual has the right to demand the deletion of their data (voice/face) from AI training datasets if they were collected without proper consent.

Articles 22A–22D of the UK GDPR establish a person's right to "human intervention" if an AI system uses their likeness or voice to create content that has a significant impact on their life.

The DUAA also amends the Data Protection Act 2018 (Sections 164A, 164B), thereby simplifying the procedure for filing complaints directly with the owners of AI models [10].

Chapter 3

The South Korea's Basic Act on the Development of Artificial Intelligence and the Establishment of a Foundation for Trustworthiness protects an individual's likeness through preventive mechanisms: transparency, labeling, and human rights impact assessment.

Article 31, paragraph 3 states that if an AI system generates virtual audio, images or video that are difficult to distinguish from real content, the AI operator is obliged to clearly notify the user (for example, by using watermarks or metadata) that this content is AI-generated. This makes it impossible or particularly hard to use another individual's likeness for fraud, creating fake news or discrediting a person as the content is immediately identified as artificial. This norm is a direct analogue of Article 50 of the EU AI Act, which also requires clear labeling of deepfakes and artificially generated content. Both jurisdictions make an exception for creative/artistic works.

According to Article 35, paragraph 1, business operators providing High-Impact AI systems must attempt to conduct an advance assessment of the potential impact on fundamental human rights (which include the right to privacy, appearence and voice).

The law stimulates corporate self-control instead of the direct censorship. According to Article 28, private autonomous AI ethics committees (which companies can create voluntarily) are empowered with the direct function of "investigating methods to prevent human rights violations." This means that a company developing a video or voice generator must internally block the possibility of cloning real people without their consent to comply with ethical principles.

Article 27, paragraph 1 says that the government establishes AI Ethical Principles, which explicitly require that the development and application of AI "do not cause harm to human life, physical well-being, or mental health" [11]. Creating intimate or defamatory deepfakes using a person's appearance causes exactly such severe psychological harm, making such tools violators of the basic principles of the law.

On November 25, 2022, People's Republic of China issued the Provisions on the Administration of Deep Synthesis Internet Information Services jointly by the Cyberspace Administration of China, the Ministry of Industry and Information Technology and the Ministry of Public Security of the PRC. The document regulates the activities of all services within PRC that use deep synthesis technologies (AI generation of text, voice, images, video, "deepfakes," virtual scenes). The main goal is the protection of national security, public interests and citizens' rights.

Developers of AI must implement a real-name user registration system (via phone number or state ID). They are obligated to monitor content: checking both input data and generation results. If harmful or illegal content is detected, the provider must immediately delete it, block the offender's account and inform regulatory authorities.

Furthermore, developers must create mechanisms for refuting rumors generated by their systems. If the technology allows for the editing of biometric information (face or voice), developers are obligated to remind users of the need to obtain separate consent from the individuals whose data is being used. Providers must also ensure the security of training data and regularly conduct assessments of the ethicality and safety of their algorithms.

Also developers of AI must take technical measures to add hidden identifiers (metadata) to all generated content. If an AI product can mislead people (e.g., realistic voice synthesis, face swapping, or creation of virtual scenes), it must bear a clear and prominent label. Users are strictly prohibited from removing, forging or hiding these marks.

App stores are obligated to check deepfake applications for compliance with safety norms before publication. The state conducts regular audits of algorithms. Administrative and criminal liability is provided for violations of the rules. In case of serious risks to information security, authorities may suspend the service's operation until violations are fully resolved [12].

Chapter 4

In the USA, Congress is implementing nationwide standards to combat disinformation. The TAKE IT DOWN Act (2025) criminalizes the distribution of intimate deepfakes or digital forgeries [13].

Referred to the House Committee on Financial Services (02/27/2025) the Preventing Deep Fake Scams Act is aimed at combating financial fraud using voice cloning [14].

The NO FAKES Act (2025) proposed to establish a federal right to protect voice and likeness, allowing for lawsuits over the unauthorized use of digital replicas. Fines for violating platforms could reach $750,000 [15].

Several states are implementing their own strict rules. For example, California acts AB 2655 and AB 2839 obligate platforms and politicians to remove or label election-related deepfakes. However in 2026 they are blocked by courts due to potential violations of freedom of speech and the right to satire. Parallelly, law SB 942 requires AI developers (such as Google or OpenAI) to implement digital watermarks and provide free tools to verify the origin of content [16].

New York updated its laws for 2025–2026. Now contracts cannot replace humans with digital replicas without special conditions, and advertisements with synthetic actors must contain a disclaimer (fine up to $5,000) [17].

Eleven states of the USA have restricted the usage of AI in political advertising.

Texas requires mandatory labeling for advertising creators.

Wisconsin introduced disclosure mandates for AI use.

Minnesota established liability for the dissemination of deepfakes [18].

Conclusion

The development of artificial intelligence and the emergence of realistic deepfakes have endangered fundamental human rights to individual's likeness and privacy, forcing the world's leading nations to develop various legal protection strategies.

The approaches of the European Union, South Korea and PRC are based on the principle of transparency, where AI developers are obligated to mark artificial content with metadata or watermarks to prevent users from being misled. The strategies, chosen by France, Great Britain and the USA, involves strict criminalization of creating intimate forgeries even without their distribution as well as protecting the digital identity of artists from commercial exploitation. The direction, represented by the experiences of Denmark and Austria, focuses on the liability of online platforms for removing illegal content and the implementation of special technical tools for judicial verification of manipulations.

Global trends indicate that an individual's likeness should now be considered as digital assets and critical biometric data requiring protection as a classic personal data. The effectiveness of each approach to protecting personal non-property rights can be assessed over

time by the action of regulatory legal acts adopted by different countries and the repeated application of their norms. However, in our opinion, ensuring transparency through a dedicated legal norm is the first step required to regulate these relations.Therefore, Ukraine ought to take an example from the European Union and South Korea, in particular, because they create an obligation to label content for both AI system providers and users. Moreover, the AI Basic Act of Korea, which encourages institutions that develop, research, and use AI to create ethics committees that must ensure that the activities of institutions are ethical, safe, and do not violate human rights, is also useful for implementation in Ukraine. Also such international experiences must become a basis for updating the Civil Code of Ukraine, particularly regarding the formalization of rights to a digital image and the establishment of consent withdrawal procedure for the use of biometrics.

Bibliography

1. Civil Code of Ukraine: Code of January 16, 2003. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text
2. Fatos Bytyci, Florion Goga. (February 13, 2026). Albanian actor sues government for using her image as "AI minister". Reuters. URL: https://www.reuters.com/business/media-telecom/albanian-actor-sues-government-using-her-image-ai-minister-2026-02-13/
3. Tambiama Madiega. (September, 2024). Artificial intelligence act (Briefing PE 698.792). European Parliamentary Research Service. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689.URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
5. LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (1). Legifrance. URL: https://www.legifrance.gouv.fr/loda/id/LEGIARTI000049565828/2024-05-23
6. Code pénal. Legifrance. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165310/#LEGISCTA000006165310
7. Værn mod deling af digitale efterligninger af personlige kendetegn. Kulturministeriet, 2025. URL: https://kum.dk/fileadmin/_kum/1_Nyheder_og_presse/2025/Vaern_mod_deling_af_digitale_efterligninger.pdf
8. Udkast. Forslag til Lov om ændring af lov om ophavsret (Indførelse af en præstationsbeskyttelse og beskyttelse mod digitalt genererede efterligninger mv.). Lovforslag. København. Kulturministeriet, 2025. URL: https://prodstoragehoeringspo.blob.core.windows.net/92ca118f-cd2c-4558-a6a9-f590c111bd67/Forslag%20til%20lov%20om%20%C3%A6ndring%20af%20lov%20om%20ophavsret%20(Indf%C3%B8relse%20af%20en%20pr%C3%A6stationsbeskyttelse%20og%20beskyttelse%20mod%20digitalt%20genererede%20efterligninger%20mv.).pdf
9. Aktionsplan Deepfake. Wien : Bundesministerium für Inneres, 2022. URL: https://www.bmi.gv.at/bmi_documents/2779.pdf
10. Data (Use and Access) Act 2025. URL: https://www.legislation.gov.uk/ukpga/2025/18/contents
11. AI Basic Act of Korea : Official Portal. 2025. URL: https://aibasicact.kr/explorer/#introduction
12. Order No. 12 of the State Internet Information Office, the Ministry of Industry and Information Technology of the People's Republic of China, and the Ministry of Public Security of the People's

13. TAKE IT DOWN Act, S. 146, 119th Cong. (2025). URL: https://www.congress.gov/bill/119th-congress/senate-bill/146/text
14. Preventing Deep Fake Scams Act, H.R. 1734 119th Cong. (2025). URL: https://www.congress.gov/bill/119th-congress/house-bill/1734/text
15. No Fakes Act of 2025, S. 1367, 119th Cong. (2025). URL: https://www.congress.gov/bill/119th-congress/senate-bill/1367/text
16. California AI Transparency Act, SB 942. (2024). URL: https://www.leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB942
17. New York State Senate Bill S8420A. (2025). URL: https://www.nysenate.gov/legislation/bills/2025/S8420/amendment/A
18. David Oxenford. (April 22, 2024). 11 States Now Have Laws Limiting Artificial Intelligence, Deep Fakes, and Synthetic Media in Political Advertising – Looking at the Issues. Broadcast Law Blog. URL: https://www.broadcastlawblog.com/2024/04/articles/11-states-now-have-laws-limiting-artificial-intelligence-deep-fakes-and-synthetic-media-in-political-advertising-looking-at-the-issues/